INFORMATION TO USERS

This reproduction was made from a copy of a document sent to us for microfilming. While the most advanced technology has been used to photograph and reproduce this document, the quality of the reproduction is heavily dependent upon the quality of the material submitted.

The following explanation of techniques is provided to help clarify markings or notations which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting through an image and duplicating adjacent pages to assure complete continuity.

2. When an image on the film is obliterated with a round black mark, it is an indication of either blurred copy because of movement during exposure, duplicate copy, or copyrighted materials that should not have been filmed. For blurred pages, a good image of the page can be found in the adjacent frame. If copyrighted materials were deleted, a target note will appear listing the pages in the adjacent frame.

3. When a map, drawing or chart, etc., is part of the material being photographed, a definite method of "sectioning" the material has been followed. It is customary to begin filming at the upper left hand corner of a large sheet and to continue from left to right in equal sections with small overlaps. If necessary, sectioning is continued again—beginning below the first row and continuing on until complete.

4. For illustrations that cannot be satisfactorily reproduced by xerographic means, photographic prints can be purchased at additional cost and inserted into your xerographic copy. These prints are available upon request from the Dissertations Customer Services Department.

5. Some pages in any document may have indistinct print. In all cases the best available copy has been filmed.
Hung, David Cheung-Yan

THETA SERIES OF QUADRATIC FORMS OVER Z AND Z((1 + SQRT.P)/2)

The Ohio State University

University Microfilms International 300 N. Zeeb Road, Ann Arbor, MI 48106
THETA SERIES OF QUADRATIC FORMS
OVER $\mathbb{Z}$ AND $\mathbb{Z}\left[\frac{1 + \sqrt{2}}{2}\right]$

DISSERTATION

Presented in Partial Fulfillment of the Requirements for
the Degree Doctor of Philosophy in the Graduate
School of The Ohio State University

By
David C. Hung, B.Sc., M.S.

* * * * *

The Ohio State University
1983

Reading Committee:  
John S. Hsia  
Paul Ponomarev  
Daniel Shapiro

Approved by

Adviser
Department of Mathematics
ACKNOWLEDGMENTS

I owe a great debt of gratitude to my adviser, Professor J. S. Hsia, for his invaluable guidance in the work which has gone into this dissertation. He has aided my development immeasurably by the presence of his own excellent example. I would like to express my appreciation to Professor Paul Ponomarev, who has always been available for consultation and offered assistance in constructing some arguments appearing on these pages. I thank Professor Daniel Shapiro for reading the manuscript, and Patricia Lyn Johnson for her efficient and accurate typing. Finally, I wish to thank my parents for their support and encouragement during this work.
V I T A

November 18, 1951 .......... Born - Hong Kong

June, 1974 .................... B.Sc., The Chinese University of Hong Kong

June, 1976 .................... M.Phil., The Chinese University of Hong Kong

1976-1983 .................... Teaching Associate, Department of Mathematics, The Ohio State University, Columbus, Ohio

PUBLICATIONS

"Theta Series of Ternary and Quaternary Quadratic Forms", Inventiones mathematicae, to appear, 1983.*

"Theta Series of Quaternary Quadratic Forms over \( \mathbb{Z} \left[ \frac{1 + \sqrt{p}}{2} \right]\)\), In preparation.*

FIELDS OF STUDY

Major Field: Mathematics
Studies in Quadratic Form Theory: Professor J.S. Hsia
Studies in Modular Forms: Professor M. Peters
Studies in Arithmetic of Quaternion Algebras:
Professor P. Ponomarev

* Joint paper with J. S. Hsia.
# TABLE OF CONTENTS

- **ACKNOWLEDGEMENTS** .......................................................... ii
- **VITA** .................................................................................. iii
- **INTRODUCTION** ................................................................. 1

## Chapter

0. **PRELIMINARIES** .............................................................. 6

- § 1 Quadratic Spaces and Orthogonal Groups .... 6
- § 2 Lattices on Quadratic Spaces ...................... 8
- § 3 Local Invariants of Lattices ...................... 10
- § 4 Class, Genus, and Roots Systems ............. 11
- § 5 Theta Series ................................................................. 12

I. **ARITHMETIC OF QUATERNION ALGEBRAS** ....................... 16

- §1.1 Quaternion Algebras ..................................................... 16
- §1.2 Maximal Orders and Ideals ................................. 18
- §1.3 Normal Ideals and Prime Ideals ..................... 20
- §1.4 Class Number, Type Number, and Idele Group .. 22
- §1.5 Quaternary Forms and Quaternion Algebras . . 23

II. **THETA SERIES OF QUADRATIC FORMS OVER Z** .......... 36

- §2.1 Dual Representations ................................................. 36
- §2.2 Characteristic Sublattices ...................................... 39
- §2.3 Nice Ternary Lattices ............................................. 47
- §2.4 The Genus $G(3, 2p)$, $p \equiv 3 \pmod{4}$ .............. 55
- §2.5 Even Positive Definite Ternary
  Lattices of Discriminant $2p^2$ ............................. 64
- §2.6 Nice Quaternary Lattices ................................. 70
- §2.7 Even Positive Definite Quaternary
  Lattices of Discriminant $p^2$ .............................. 81

III. **THETA SERIES OF QUADRATIC LATTICES OVER Z** 101

- §3.1 Theta Series of Degree Two ............................ 101
- §3.2 Theta Series of Degree One:
  Lattices of Type $A_1 \oplus A_1$ .......................... 119
3.3 Theta Series of Degree One:
   Lattices of Type $A_2$ ..................... 125
3.4 Theta Series of Ternary Lattices .......... 132

EPILOGUE: SUGGESTIONS FOR FURTHER RESEARCH ........ 137
APPENDIX: A COUNTEREXAMPLE ..................... 140
BIBLIOGRAPHY ........................................ 143
INTRODUCTION

One of the fundamental problems in the theory of quadratic forms is that of finding simple invariants which classify forms up to integral equivalence. Recent developments suggest the use of representation (of integers or of forms) to determine classification. Indeed, for positive binary forms of the same discriminant it is known that the set of integers represented by a form determines its class. See, for instance, [K₂], [Wa]. On the other hand, in the quaternary case these value-sets, in general, do not yield classification within a genus. An example was also found in the ternary case where two inequivalent positive forms in a genus represent the same integers [Hs]. Some progress has been made, however, toward using representation of forms for classification, notably the result of Kitaoka [K₂], which states that any n-ary form is classified by the (n-1)-ary forms it represents. Based upon some numerical evidence and representation results obtained in [HKK], Hsia conjectured that the n-ary positive definite forms of a fixed discriminant should be characterized (see [Hs], page 237) by the [½(n+1)]-ary forms they represent.
Furthermore, the theta series of degree \( d \geq \frac{1}{2}(n+1) \)
associated with forms in a genus should be linearly indepen-
dent. A related (weaker) question to the above is: what
degree theta series classify forms in a genus. In this case
\( d \) is expected to be roughly \( n/4 \) ([Hs], page 238). Some
positive evidences were established by Costello [Co] for
forms in 24 or fewer variables. For more details on the
development of this problem, see [Wi], [Kn], and [K₄].
The main objective of this work is to address the stronger
question of linear independence of theta series and, as a
consequence of this, the classification by theta series.
We provide some arithmetic methods for showing that the
theta series of certain explicitly described forms in a
genus are linearly independent.

Most of the work in Chapter II was inspired by two
conjectures: one of Kitaoka ([K₁], page 152) concerning
the theta series of even positive quaternary lattices of
prime discriminant \( p \ (p \equiv 1 \ (\text{mod} \ 4)) \) and their adjoints,
and a similar one of Ponomarev ([P₂], page 125) for discri-
minant \( p^2 \) (see also [P₄], page 362). In both conjectures
the theta series coming from quadratic forms which have an
improper automorphism are said to form a basis for their
corresponding space of modular forms (Nebentypus and Haupt-
typus, respectively). It is now known that this conjecture
is false, in general, as Kitaoka has provided a counter
example in the case of prime discriminant (communication with Hsia). He and Nashiro were able to find via computers ten classes in the genus of even quaternary forms of discriminant \( p = 389 \) for which there exists a nontrivial linear relation between their theta series (see Appendix). One naturally asks whether some reasonable subsets of forms in a genus can be found which have independent theta series. We will attempt to answer this by partitioning a genus into subsets according to the "roots system" types of the forms. We will also consider this problem for theta series of degree two.

Our methods are based upon the classical correspondence between representations by a form and those by its adjoint. This correspondence had already appeared in the works of Gauss, Smith, Minkowski, and others (see, e.g., [Pa]). In the language of lattices, it associates the primitive sublattices of codimension one in a lattice \( L \) with one-dimensional primitive sublattices of its reciprocal \( \hat{L} \) (see Section 2.1) with identical discriminant. By considering certain "characteristic sublattices" (in the sense of \([K_2]\)) of codimension one in \( L \), we are able to obtain the related coefficients in the theta series of \( \hat{L} \). We shall exploit this approach throughout Chapter II to show the independence of the theta series of \( \hat{L} \) coming from certain classes of quadratic lattices over \( \mathbb{Z} \). This will, in turn, yield the independence of the theta series of \( L \) by the classical
theta transformation formula. For an alternate approach, see [HH].

In Sections 2.3 through 2.5 we consider even positive definite ternary lattices over \mathbb{Z} of discriminant \(2p\) and \(2p^2\) (where \(p\) is an odd prime number). We find that, in each genus, the classes with nontrivial automorphism groups always have independent theta series. In the case of discriminant \(2p\), these classes correspond to those which represent \(2\), whereas in the case of discriminant \(2p^2\), they correspond to the classes which represent \(2p\). We then consider even positive quaternary lattices of discriminant \(p\) and \(p^2\) (where \(p\) is a prime \(\equiv 1 \pmod{4}\)) (Sections 2.6 and 2.7). In this case we obtain the independence only for some subsets of classes of a fixed roots system type. With regard to theta series of degree two, however, we are able to show the independence for all classes with improper (nontrivial) automorphism groups.

Our methods apply also to lattices over the ring of integers of a quadratic number field. In Chapter III we consider even unimodular quaternary lattices and even ternary lattices of discriminant \(2\) over \(\mathbb{Q}(\sqrt{p})\) (\(p \equiv 1 \pmod{4}\)). Some knowledge of the arithmetic structures of these lattices is needed, for example, their unit groups and roots system. Results from the arithmetic theory of quaternion algebra are employed to understand these structures.
There seems to be very little known in the literature about the linear independence of theta series associated with positive definite forms. The methods we use in this dissertation are purely arithmetic and can be applied to different genera as well as to theta series over number fields. However, it is still essential that one knows the technical features of the forms in these genera.

Several possible avenues for further research readily present themselves. One pertinent question is whether the forms we considered in this paper have independent theta series together with their adjoints. One may also consider this problem for forms with more variables (≥5). The Epilogue lists some specific suggestions along these lines.
Chapter 0
PRELIMINARIES

The purpose of this chapter is to establish notational conventions and to summarize some important concepts which shall be used throughout this dissertation. In order to achieve a more coherent exposition, other basic concepts will be introduced as they are needed. We will assume that the reader is familiar with the algebraic structure of groups, rings, and fields, and with the general theory of quadratic forms over arbitrary fields. In addition, an acquaintance with algebraic number fields, particularly the quadratic fields, is assumed. The notations and terminology used will generally be those of O'Meara's fundamental text [OM].

§ 1. Quadratic Spaces and Orthogonal Groups

Let \( F \) be a field of characteristic not equal to 2. A quadratic space is a pair \((V, Q)\), where \( V \) is a finite dimensional vector space over \( F \) and \( Q: V \rightarrow F \) is a map such that

\[
Q(\alpha x) = \alpha^2 Q(x) \quad \text{for } \alpha \in F, \, x \in V,
\]

\[
Q(x + y) = Q(x) + Q(y) + 2B(x, y),
\]

for some symmetric bilinear form \( B \). If \( x_1, \ldots, x_n \) is a
basis for $V$, then we denote by $d(x_1, \ldots, x_n)$ the determinant of the matrix $(B(x_i, x_j))$. The canonical image of $d(x_1, \ldots, x_n)$ in $O(U(F/F^2))$ (where $F$ is the multiplicative group of nonzero elements in $F$) is independent of the basis; we call it the discriminant of $V$ and denote it by $d_V$.

$V$ is said to be regular if $d_V \neq 0$. We shall assume that any space mentioned in this paper is regular.

An isotropic vector is a vector $x \in V$ such that $x \neq 0$, but $Q(x) = 0$. A quadratic space $V$ is called isotropic if it contains an isotropic vector; otherwise it is said to be anisotropic. A regular two-dimensional isotropic space is called a hyperbolic plane. If $H$ is a hyperbolic plane, there is a basis $\{x, y\}$ for $H$ with $Q(x) = Q(y) = 0$ and $B(x, y) = 1$.

The orthogonal group $O(V)$ is the group of bijective linear transformations $\sigma$ of $V$ such that $Q(\sigma x) = Q(x)$ for all $x \in V$. For any vector $y \in V$ with $Q(y) \neq 0$ the symmetry of $V$ with respect to $y$ is defined by

$$S_y(x) = x - \frac{2B(x, y)}{Q(y)} y.$$ 

Let $\sigma$ be an isometry of $V$ (i.e. $\sigma \in O(V)$), then $\det \sigma = \pm 1$. We say that $\sigma$ is proper (or a rotation) if $\det \sigma = 1$; $\sigma$ is improper (or a reflexion) if $\det \sigma = -1$. Every symmetry is improper.
§2. **Lattices on Quadratic Spaces**

Assume now that $F$ is a global or local field and $\mathfrak{O}$ the ring of integers of $F$. A lattice on $V$ is a finitely generated $\mathfrak{O}$-module $L$ such that $F \otimes_{\mathfrak{O}} L = V$. The rank of $L$ is the dimension of its underlying space $V$. Given any lattice $L$ on $V$, one can find a basis $\{x_1, \ldots, x_n\}$ for $V$ and fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ such that $L = \mathfrak{a}_1 x_1 + \mathfrak{a}_2 x_2 + \ldots + \mathfrak{a}_n x_n$. $L$ is said to be **free** if $L = \mathfrak{O} x_1 + \ldots + \mathfrak{O} x_n$ for some $\{x_1, \ldots, x_n\}$ (called a basis for $L$). When $\mathfrak{O}$ is a principal ideal domain, then every lattice will be free.

The **discriminant** of a free lattice $L$ is just $d(x_1, \ldots, x_n)$ for some basis $\{x_1, \ldots, x_n\}$ of $L$; its canonical image in $0 \cup (\hat{F}/\hat{U}^2)$ is independent of the basis chosen for $L$ (where $\hat{U}$ is the group of units in $\mathfrak{O}$).

We say that $L$ is the **orthogonal sum** of the sublattices $L_1, \ldots, L_r$ or that $L$ has the orthogonal splitting

$$L = L_1 \perp L_2 \perp \ldots \perp L_r$$

if $L$ is the direct sum of the $L_i$'s and $B(L_i, L_j) \neq 0$ for $i \neq j$. Whenever $L$ has an orthogonal splitting involving more than one nonzero component, $L$ is said to be **decomposable**; otherwise, it is **indecomposable**. Suppose that $L = L_1 \perp \ldots \perp L_r$, where $L$ and $L_i$ are free lattices, then it is clear that

$$dL = dL_1 \cdot dL_2 \cdot \ldots \cdot dL_r.$$ 

If $J$ is a sublattice of $L$, the **orthogonal complement** of $J$ in $L$ is defined to be $J^\perp = \{x \in L \mid B(x, J) = 0\}$.
The norm $n_L$ and scale $s_L$ of a lattice $L$ are the $\Theta$-modules generated by the sets $Q(L)$ and $B(L, L)$, respectively. A lattice $L$ is said to be integral if $s_L \subseteq \Theta$. An integral lattice $L$ is even if $n_L \subseteq 2\Theta$. If $L = a_1 x_1 + \ldots + a_n x_n$, then the volume of $L$ is defined to be $v_L = a_1^2 \cdot \ldots \cdot a_n^2 \cdot d(x_1, \ldots, x_n)$. A lattice $L$ is $Q$-modular whenever $Q = s_L = (v_L)^n$. $L$ is unimodular if it is $\Theta$-modular. We say that $L$ is $Q$-maximal on $V$ if $n_L \subseteq Q$ and $n_K \not\subseteq Q$ for any lattice $K$ properly containing $L$.

The dual of a lattice $L$ is defined to be
\[ L^\# = \{ x \in V \mid B(x, L) \subseteq \Theta \} \]
If $L = a_1 x_1 + \ldots + a_n x_n$ for some basis $\{x_1, \ldots, x_n\}$ of $V$ and fractional ideals $a_1, \ldots, a_n$, then $L^\# = a_1^{-1} y_1 + \ldots + a_n^{-1} y_n$, where $\{y_1, \ldots, y_n\}$ is the dual basis of $\{x_1, \ldots, x_n\}$ on $V$.
If $Q$ is a fractional ideal, then we define $L^Q$ as the sublattice $L^Q = \{ x \in L \mid B(x, L) \subseteq Q \}$ of $L$. Let $\alpha$ be a nonzero scalar. We shall use $L^\alpha$ to denote the lattice $L$ when regarded as a lattice in $V^\alpha$, where $V^\alpha = V$ is provided with a new bilinear form $B^\alpha(x, y) = \alpha B(x, y)$.

The automorphism group (or unit group) of $L$ is
\[ O(L) = \{ \sigma \in O(V) \mid \sigma L = L \} \]
We put $O^+(L) = O(L) \cap O^+(V)$, where $O^+(V)$ is the group of proper isometries of $V$. Similarly, $O^-(L) = O(L) \cap O^-(V)$ (where $O^-(V)$ consists of improper isometries). It is clear that $O(L) = O^+(L) \cup O^-(L)$. We have $1 \leq (O(L) : O^+(L)) \leq 2$. $(O(L) : O^+(L)) = 2$ when $O^-(L) \neq \emptyset$. 
§3. **Local Invariants of Lattices**

Let $F$ be a local field in which $\mathfrak{P}$ is the maximal ideal in the ring of integers $\mathfrak{O}$. An element $\alpha$ of $F$ can be written as a power of a prime element $\pi$ of $\mathfrak{P}$ times a unit. This power is the **order** of $\alpha$, denoted by $\text{ord} \, \alpha$. The **residue class field** $\overline{F}$ is defined by $\overline{F} = \mathfrak{O}/\mathfrak{P}$. The following result is very useful, a proof of which may be found in [OM].

**Local Square Theorem**: Let $\alpha$ be an integer in the local field $F$, then there is an integer $\beta$ such that

$$1 + 4\pi\alpha = (1 + 2\pi\beta)^2.$$

Every element $\alpha$ of $F$ can be written in the form $\alpha = \eta^2 + \zeta$, where $\eta, \zeta \in F$. The fractional ideal $\delta(\alpha) = \mathfrak{O} \mathfrak{O}$ taken over all $\zeta$ appearing in expressions of the above type, is the **quadratic defect** of $\alpha$. The local square theorem says that if $\delta(\alpha) \subset 4\mathfrak{P} = 4\pi\mathfrak{O}$, then $\alpha$ is a square. It can be shown that there is, up to squares, only one unit of defect $4\mathfrak{O}$; this element will be written $\Delta = 1 + 4\rho$, where $\rho$ is a unit of $\mathfrak{O}$.

Every local lattice can be decomposed into an orthogonal sum $L = L_1 \oplus \ldots \oplus L_t$ of modular components $L_i$ for which $sL_1 \supset \ldots \supset sL_t$. This decomposition is called a **Jordan splitting** of $L$.

If $L$ is a lattice over a dyadic local field, the **norm group** $gL$ is defined to be the additive group $\mathcal{O}(L) + 2sL$, 

and $mL$ denote the largest fractional ideal contained in $gL$.
The weight $wL$ is given by the equation $wL = \rho mL + 2sL$.
A norm generator and a weight generator are scalars of
largest value in $gL$ and $wL$, respectively.

Let $A(\alpha, \beta)$ denote the lattice having matrix $\begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$
with respect to some basis. It is well known that the
only even binary unimodular lattices over a dyadic field
are $A(0, 0)$ and $A(2, 2\rho)$ (where $\Delta = 1 + 4\rho$).

§4. Class, Genus, and Roots Systems

Let $F$ be a global field and $V$ a quadratic space over $F$.
If $L$ is a lattice on $V$, then the class of $L$ is defined by
$\text{cls } L = \{gL | \sigma \in O(V)\}$ and the proper class of $L$ by $\text{cls}^+ L = \{gL | \sigma \in O^+(V)\}$. A lattice $K$ on $V$ is isometric to $L$
(written $K \cong L$) if $K \in \text{cls } L$. If $K$ and $L$ are isometric over
a global field $F$, then locally at each prime $P$ of $F$, $K_P$ and
$L_P$ are also isometric. Unfortunately, there is no local-
global principle for lattices: $K$ and $L$ may not be isometric
even though $K_P \cong L_P$ for all primes $P$. This leads one to
define the genus of $L$, denoted by $\text{gen } L$, as the set of all
lattices $K$ with $K_P \in \text{cls } L_P$ for all $P$. All lattices in the
same genus have the same volume, scale, and norm. The genus
of an $\mathcal{A}$-maximal lattice on $V$ consists of all $\mathcal{A}$-maximal lattices
on the same space.
Let \( L \) be an even integral lattice over \( \mathcal{O} \), the ring of integers of \( F \). A vector \( x \in L \) is called a **minimal vector** (or 2-vector) if \( Q(x) = 2 \). A sublattice of \( L \) is a 2-lattice if it is generated by minimal vectors. The **roots system** of \( L \) is the maximal 2-lattice contained in \( L \).

The automorphism group of an even integral lattice \( L \) is often determined by the roots system of \( L \). The classification of all indecomposable 2-lattices over \( \mathbb{Z} \) and over any real quadratic integers have been completely determined ([Kn] [Oz], [Mi]). We now list a few of them which are useful in this paper.

<table>
<thead>
<tr>
<th>Name</th>
<th>( A_n, n &gt; 1 )</th>
<th>( D_4 )</th>
<th>( F_4 ) (over ( \mathbb{Q}(\sqrt{5}) ))</th>
</tr>
</thead>
</table>
| Matrix | \[
\begin{pmatrix}
2 & 1 \\
1 & 2 & 1 \\
1 & 2 & 1 \\
\end{pmatrix}
\] | \[
\begin{pmatrix}
2 & 0 & 1 & 1 \\
0 & 2 & 1 & 1 \\
1 & 1 & 2 & 1 \\
\end{pmatrix}
\] | \[
\begin{pmatrix}
2 & \zeta & \zeta & \zeta \\
\zeta & 2 & 1 & 1 \\
\zeta & 1 & 2 & 1 \\
\zeta & 1 & 1 & 2 \\
\end{pmatrix}
\] |
| Discriminant | \( n + 1 \) | 4 | \( \zeta = \frac{1 + \sqrt{5}}{2} \) |
| Number of minimal vectors | \( n(n + 1) \) | 24 | 120 |

§5. **Theta Series**

In this section we define the ordinary and then the generalized theta series for even positive definite lattices defined over \( \mathbb{Z} \) and then for free lattices defined over \( \mathbb{Z}\left[ \frac{1 + \sqrt{p}}{2} \right] \), where \( p \) is a prime \( \equiv 1 \) (mod 4).
The ordinary theta series (of degree one) associated with an even positive definite lattice $L$ defined over $\mathbb{Z}$ is given by

$$\theta_L^1(z) = \sum_{x \in L} e^{\pi i z Q(x)}$$

where $z \in \mathbb{H}$, the upper half complex plane. $\theta_L$ has a Fourier expansion of the form

$$\theta_L(z) = \sum_{m=0} a_L(2m) e^{2\pi i zm}$$

where $a_L(2m)$ is the number of vectors $x \in L$ with $Q(x) = 2m$.

The number $a_L(2m)$ and, in fact, the series $\theta_L$ are invariants of the class of $L$. If the dimension of $L$ is $n = 2k$, then $\theta_L$ is a modular form of weight $-k$ with a certain level $N$ and character ([0g], [E_2]). There is also an analogous property for theta series coming from odd dimensional lattices (see [Sh]).

The situation is a little more complicated when we define the theta series of higher degree. For any matrix $M$, let $\text{Tr}(M)$ be the trace of $M$. The theta series of degree $d$ associated with an even positive lattice $L$ defined over $\mathbb{Z}$ is

$$\theta_L^d(z) = \sum_{X} e^{i \pi \text{Tr}(XAXZ)}$$

where $X$ runs through all integral $n \times d$ matrices and $Z$ is a point of the Siegel upper half plane of degree $d$, i.e. $Z = X + iY$ is a $d \times d$ complex symmetric matrix, where $Y$ is positive definite; $A$ is the matrix of $L$ with respect to some
basis. The Fourier expansion of $\theta_L^{(d)}$ is

$$\theta_L^{(d)}(Z) = \sum_{T \geq 0} a_L(T) \ e^{\pi i \ Tr(TZ)}$$

where $T$ runs through all integral symmetric matrices of order $d$ with an even diagonal satisfying $T \geq 0$. It is shown in [AM] that $\theta_L^{(d)}$ is a Siegel modular form with respect to some congruence subgroup of the symplectic group of degree $d$ over $\mathbb{Z}$ and a multiplicator system. See also [Ra].

In order to define the generalized theta series associated with an even positive free lattice $\mathcal{L}$ over $\mathbb{Z} \left[ \frac{1 + \sqrt{d}}{2} \right]$ we let $Z = (Z_1, Z_2)$ be a pair of elements from the Siegel upper half plane of degree $d$. The generalized theta series of degree $d$ is defined by

$$\theta_{\mathcal{L}}^{(d)}(Z) = \sum_{X} e^{\pi i \ Tr(\tau XAXZ_1 + \bar{T}XAXZ_2)}$$

where $X$ runs through all integral $n \times d$ matrices; $A$ is the matric of $\mathcal{L}$ with respect to some basis. The Fourier expansion of $\theta_{\mathcal{L}}^{(d)}$ is

$$\theta_{\mathcal{L}}^{(d)}(Z) = \sum_{T \geq 0} a_{\mathcal{L}}(T) \ e^{\pi i \ Tr(TZ_1 + \bar{T}Z_2)}$$

where $T$ runs through all integral symmetric matrices of order $d$ with even diagonal. For even dimensional $\mathcal{L}$ ($n = 2k$), Lal ([LJ], page 237, Theorem 4) shows that $\theta_{\mathcal{L}}^{(d)}$ is a Hilbert-Siegel modular form of dimension $-k$ and certain level (stufe) belonging to some multiplicator system. If $d = 1$, then our
definition reduces to

$$\Theta_{\mathcal{F}}(z) = \sum_{x \in \mathcal{F}} e^{\pi i (Q(x)z_1 + \overline{Q(x)}z_2)}$$

$$= \sum_{c} a_{\mathcal{F}}(c) e^{2\pi i (cz_1 + \overline{c}z_2)}$$

where c runs through all totally positive integers in $\mathbb{Z}\left[\frac{1+i\sqrt{2}}{2}\right]$; $z_1$ and $z_2$ come from the upper half complex plane.
Chapter I
ARITHMETIC OF QUATERNION ALGEBRAS

In this chapter we give a brief account of some important concepts in the arithmetic theory of quaternion algebras which are useful to our study of quaternary quadratic forms. For proofs which are not provided in the following, refer to some standard texts on quaternion algebras (e.g. [R], [V]).

§1.1 Quaternion Algebras

Let \( F \) be an algebraic number field. An algebra \( \mathcal{A} \) over \( F \) generated by 1, \( u, v, \) and \( uv \) with multiplication \( u^2 = a, \ v^2 = b, uv = -vu, \) and \( a, b \in F \) is called a quaternion algebra and is denoted by \( (\frac{a,b}{F}) \). If \( \alpha \in \mathcal{A} \), then \( \alpha = a_0 + a_1u + a_2v + a_3uv, \) where \( a_i \in F \). The canonical involution of \( \alpha \) is given by \( (a_0 + a_1u + a_2v + a_3uv)^* = a_0 - a_1u - a_2v - a_3uv. \) The norm and trace of \( \alpha \) is defined in the usual way:

\[
N(\alpha) = \alpha \alpha^* = \alpha^* \alpha; \quad T(\alpha) = \alpha + \alpha^*, \quad \alpha \in \mathcal{A},
\]

Let \( \mathcal{A}^* \) denote the multiplicative group of all invertible elements in \( \mathcal{A} \). Then \( N: \mathcal{A}^* \rightarrow F \) is a group homomorphism.
T: $\sigma \rightarrow F$ is an $F$-linear mapping. Since $\alpha^2 - (\alpha + \alpha^*)\alpha + \alpha^*\alpha = 0$, the minimal polynomial for any $\alpha \in \sigma$, $\alpha \notin F$ is $x^2 - T(\alpha)x + N(\alpha)$.

1.1.1 Proposition ([OM], 57:2): $\sigma$ is a central simple algebra.

For each prime $\mathfrak{p}$ of $F$, we set $\sigma_{\mathfrak{p}} = \sigma \otimes_F F_\mathfrak{p}$. $\sigma_{\mathfrak{p}}$ is also a central simple algebra over $F_\mathfrak{p}$. By the Wedderburn's theorem, there are only two central simple algebras (up to isomorphism) of dimension 4 over $F_\mathfrak{p}$: the complete matrix algebra $M_2(F_\mathfrak{p})$ and the unique division algebra of dimension 4 over $F_\mathfrak{p}$. We say that $\sigma_{\mathfrak{p}}$ is split in the former case and non-split in the latter. We define a symmetric bilinear form $B$ on $\sigma$ by $B(x, y) = T(xy^*)$, $x, y \in \sigma$. The associated quadratic form satisfies $Q(x) = 2N(x)$. We have $\sigma_{\mathfrak{p}}$ is split if and only if $\sigma_{\mathfrak{p}}$ is isotropic with respect to $Q$, and this is equivalent to $(\frac{\alpha, b}{\mathfrak{p}}) = 1$, where $(\frac{\alpha, b}{\mathfrak{p}})$ is the Hilbert symbol at $\mathfrak{p}$. There are only finitely many primes $\mathfrak{p}$ with $(\frac{\alpha, b}{\mathfrak{p}}) = -1$. By the Hilbert Reciprocity Law, the number of non-split primes is even. If $F$ is a totally real algebraic number field, then $\sigma$ is definite if $(\frac{\alpha, b}{\mathfrak{p}}) = -1$ for all infinite primes $\mathfrak{p}$. By the Hasse local-global principle, if $(\frac{\alpha, b}{\mathfrak{p}}) = 1$ for all $\mathfrak{p}$, then $\sigma = M_2(F)$. Suppose that $\sigma = (\frac{\alpha, b}{F})$, $\sigma' = (\frac{\alpha', b'}{F})$ satisfy $(\frac{\alpha, b}{\mathfrak{p}}) = (\frac{\alpha', b'}{\mathfrak{p}})$ for all primes $\mathfrak{p}$, then $\sigma = \sigma'$ by the Hasse-Brauer-Noether-Albert
theorem ([R] 32.11). Therefore, any two quaternion algebras are isomorphic if and only if they have the same set of non-split primes. If \( T \) is a set consisting of an even number of finite or real primes, then there exists a quaternion algebra with \( T \) as its set of non-split primes ([OM], Theorem 71:19).

§1.2 Maximal Orders and Ideals

1.2.1 Definition: Let \( \mathcal{A} \) be a quaternion algebra over \( F \).
A subset \( \Omega \) of \( \mathcal{A} \) is an order if

(i) \( \Omega \) is an \( \Theta \)-lattice on \( \mathcal{A} \);

(ii) \( \Omega \) is a subring of \( \mathcal{A} \) which contains 1.

Orders in \( \mathcal{A}_\mathcal{P} \) are defined in exactly the same way.
If \( \Omega \) is an order in \( \mathcal{A} \), then \( \Omega_\mathcal{P} \) is an order in \( \mathcal{A}_\mathcal{P} \) for every finite prime \( \mathcal{P} \). Observe that if \( \omega \in \Omega \), then we have \( \omega \Omega \subseteq \Omega \); hence \( \omega \) is integral over \( \Theta \). It follows that the minimal polynomial must have integral coefficients, so \( N(\omega), T(\omega) \in \Theta \).

1.2.2 Definition: An order in \( \mathcal{A} \) (or in \( \mathcal{A}_\mathcal{P} \)) is said to be maximal if it is not properly contained in any other order.

1.2.3 Proposition ([R], 11.2): \( \Omega \) is a maximal order in \( \mathcal{A} \) if and only if \( \Omega_\mathcal{P} \) is a maximal order in \( \mathcal{A}_\mathcal{P} \) for all finite \( \mathcal{P} \).

The classification of maximal orders in the local case is fairly straightforward.
1.2.4 Proposition ([R], 12.8): If $\mathcal{O}_\mathfrak{p}$ is non-split, then there is a unique maximal order $\Omega_\mathfrak{p} = \{\omega \in \mathcal{O}_\mathfrak{p} \mid N(\omega) \in \mathfrak{p}\}$.

If $\mathcal{O}_\mathfrak{p}$ is split, then $\mathcal{O}_\mathfrak{p} = M_2(F_p)$. We show that $\Omega_\mathfrak{p} = M_2(\mathfrak{O}_\mathfrak{p})$ is a maximal order. $\Omega_\mathfrak{p}$ has a basis

$$x_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad x_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad x_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix};$$

hence, its discriminant is $d(\Omega_\mathfrak{p}) = \det \begin{pmatrix} T(x_i x_j^*) \end{pmatrix} =$

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = 1.$$  If $\Omega_\mathfrak{p}'$ is any maximal order containing $\Omega_\mathfrak{p}$ with basis elements $x_1', x_2', x_3', x_4'$, then we have

$$x_i = \sum \alpha_{ij} x_j'$$

for some $\alpha_{ij} \in \mathfrak{O}_\mathfrak{p}$. Therefore, $d(\Omega_\mathfrak{p}') = d(\Omega_\mathfrak{p}) (\det(\alpha_{ij}))^2$, so $d(\Omega_\mathfrak{p}')$ and $\det(\alpha_{ij})$ must both be units. Thus, $\Omega_\mathfrak{p}' = \Omega_\mathfrak{p}$.

1.2.5 Proposition ([R], 17.3(ii)): Let $\mathcal{O}_\mathfrak{p} = M_2(F_p)$ and $\Omega_\mathfrak{p} = M_2(\mathfrak{O}_\mathfrak{p})$. Then every maximal order in $\mathcal{O}_\mathfrak{p}$ is of the form

$$\alpha \Omega_\mathfrak{p} \alpha^{-1}$$

for some $\alpha \in \mathcal{O}_\mathfrak{p}$.

1.2.6 Definition: Let $\Omega$ be an order in a quaternion algebra $\mathcal{A}$. A subset $I$ of $\mathcal{A}$ is a left ideal of $\Omega$ if

(i) $I$ is an $\mathfrak{O}$-lattice on $\mathcal{A}$, and

(ii) $\Omega \cdot I = I$ (the product is defined as usual).

Similarly, we can define the notion of a right ideal of $\Omega$. The left and right ideal for a local order $\Omega_\mathfrak{p}$ is defined in the same way. $I$ is a two-sided ideal of $\Omega$ (or
1.2.7 Proposition ([R], 17.3(i)): Let \( \mathcal{O}_\rho = M_2(F_\rho) \) and \( \Omega_\rho = M_2(\mathcal{O}_\rho) \). The only two sided ideals of \( \Omega_\rho \) are the powers of

\[ \mathcal{T} = \left( \begin{array}{cc} \pi \mathcal{O}_\rho & \pi \mathcal{O}_\rho \\ \pi \mathcal{O}_\rho & \pi \mathcal{O}_\rho \end{array} \right) , \]

where \( \mathcal{P} = \pi \mathcal{O}_\rho \).

1.2.8 Proposition ([R], 17.3(iii)): Let \( \mathcal{O}_\rho = M_2(F_\rho) \) and \( \Omega_\rho = M_2(\mathcal{O}_\rho) \). Every left (right) ideal of \( \Omega_\rho \) is principal.

1.2.9 Corollary: Every right ideal with respect to a maximal order \( \Omega_\rho \) in \( \mathcal{O}_\rho = M_2(F_\rho) \) is a left ideal with respect to some maximal order \( \Omega_\rho' \).

1.2.10 Proposition ([R], 13.2): If \( \mathcal{O}_\rho \) is a division algebra (i.e. \( \mathcal{O}_\rho \) nonsplit), then the maximal order \( \Omega_\rho \) has a unique two-sided maximal ideal \( \mathcal{T} = \mathcal{P} \Omega_\rho', \mathcal{P}^2 = \pi \), where \( \mathcal{P} = \pi \mathcal{O}_\rho \), and all ideals of \( \Omega_\rho \) are two-sided and powers of \( \mathcal{T} \).

§1.3 Normal Ideals and Prime Ideals

1.3.1 Definition: If \( L \) is an \( \mathcal{O} \)-lattice in \( \mathcal{O} \), we set \( \Omega_L = \{ \alpha \in \mathcal{O} \mid \alpha L \subseteq L \} \) and \( \Omega_R = \{ \alpha \in \mathcal{O} \mid L \alpha \subseteq L \} \). It is easy to see that \( \Omega_L \) and \( \Omega_R \) are orders in \( \mathcal{O} \) ([R], page 109).

\( \Omega_L \) (respectively \( \Omega_R \)) is the largest order such that \( L \) is a left (respectively right) order. \( \Omega_L \) is called the left order of \( L \) and \( \Omega_R \) the right order of \( L \).
If \( L \) is a lattice with a maximal left order, then its right order is also maximal (and conversely). To see this, let \( \Omega_l, \Omega_r \) be the left and right orders of \( L \). Since \( L_\rho = (\Omega_l)_\rho \alpha_\rho \) for some \( \alpha_\rho \in \mathcal{A}_\rho^X \), we have \( (\Omega_r)_\rho = \alpha_\rho^{-1}(\Omega_l)_\rho \alpha_\rho \); hence, \( (\Omega_r)_\rho \) is maximal for all \( \rho \). By Proposition 1.2.3, \( \Omega_r \) is maximal.

1.3.2 Definition: A lattice \( L \) is called a normal ideal if the right or left order of \( L \) is maximal.

1.3.3 Definition: Let \( L \) be an \( \mathcal{Q} \)-lattice in \( \mathcal{A} \). We define \( L^{-1} = \{ \alpha \in \mathcal{A} \mid L_\alpha L \subseteq L \} \). If \( L \) is a normal ideal, then \( L^{-1} \) is also a normal ideal. The right order of \( L^{-1} \) is the left order of \( L \). We have \( L \cdot L^{-1} = \Omega_l \) and \( L^{-1} \cdot L = \Omega_r \), where \( \Omega_l, \Omega_r \) are the left and right orders of \( L \). Also, \( (L^{-1})^{-1} = L \) ([R], page 192).

The set of normal ideals form a groupoid (for definition see [R], page 201), with multiplication \( L \cdot L' \) defined whenever the left order of \( L' \) is the right order of \( L \). The left unit of \( L \) is just the left order of \( L \) (similarly for the right unit). The inverse of \( L \) is \( L^{-1} \).

1.3.4 Definition: Let \( \Omega \) be an order in a quaternion algebra \( \mathcal{A} \). A prime ideal of \( \Omega \) is a proper two-sided ideal \( \mathcal{P} \) in \( \Omega \) such that for every pair of two-sided ideals \( S,T \) in \( \Omega \),

\[
S \cdot T \subseteq \mathcal{P} = S \subseteq \mathcal{P} \quad \text{or} \quad T \subseteq \mathcal{P}.
\]
§1.4 Class Number, Type Number, and Idele Group

1.4.1 Definition: Let \( \Omega \) be a maximal order. Two left ideals \( I, J \) of \( \Omega \) are in the same left ideal class if there is an \( \alpha \in \mathcal{O}_X \) such that \( I\alpha = J \). Similarly, we can define right ideal class.

If \( I \) is a left ideal of \( \Omega \), then \( I^{-1} \) is a right \( \Omega \) ideal. It is easy to see that if \( I \) and \( J \) are in the same left ideal class, then \( I^{-1} \) and \( J^{-1} \) are in the same right ideal class.

1.4.2 Proposition ([R], 26.4): Let \( \Omega \) be a maximal order. The number of left ideal classes of \( \Omega \) is finite and is equal to the number of right ideal classes of \( \Omega \). The ideal class number \( h(\mathcal{O}) \) is independent of the choice of \( \Omega \).

1.4.3 Definition: Two maximal orders \( \Omega_1 \) and \( \Omega_2 \) in \( \mathcal{O} \) are conjugate if there exists \( \alpha \in \mathcal{O}_X \) such that \( \Omega_2 = \alpha \Omega_1 \alpha^{-1} \). We also say they are in the same conjugacy class.

Since every automorphism of \( \mathcal{O} \) is inner (i.e., \( \xi \mapsto \alpha \xi \alpha^{-1} \)), it follows that \( \Omega_1 \) and \( \Omega_2 \) are conjugate if and only if they are isomorphic.

1.4.4 Proposition ([R], page 232): Let \( \mathcal{O} \) be a quaternion algebra. The number of conjugacy classes of maximal order in \( \mathcal{O} \) is finite. We call this number the type number of \( \mathcal{O} \).
1.4.5 Definition: The idele group of \( \mathcal{O} \) is defined as 
\[ J_\mathcal{O} = \{ (a_\mathfrak{p}) \in \prod_a \mathcal{O}_\mathfrak{p}^\times \mid a_\mathfrak{p} \in \mathcal{U}(\mathfrak{O}_\mathfrak{p}) \text{ almost all } \mathfrak{p} \}, \]
where \( \Omega \) is any order of \( \mathcal{O} \) and \( \mathcal{U}(\mathfrak{O}_\mathfrak{p}) \) is the group of units of \( \mathfrak{O}_\mathfrak{p} \). Note that this definition is independent of the choice of \( \Omega \), since if \( \Omega' \) is any other order of \( \mathcal{O} \), then we have \( \mathfrak{O}_\mathfrak{p}' = \mathfrak{O}_\mathfrak{p} \) for almost all \( \mathfrak{p} \).

§1.5 Quaternary Forms and Quaternion Algebras

Since a quaternion algebra is a quaternary quadratic space, it is sometimes useful to study certain quaternary forms via the arithmetic of quaternion algebras. In this section, we shall investigate some connection between these two languages. We assume that \( p \) is a prime \( \equiv 1 \pmod{4} \), \( F = \mathbb{Q}(\sqrt{p}) \), and \( \mathcal{O} \) is the ring of integers of \( F \). The norm map of \( F \) is defined by \( n_{F/\mathbb{Q}}(a) = aa^* \), where \( a \mapsto a^* \) is the conjugation of \( F \). It is well known (see [Ha], page 589, for example) that (i) the norm of the fundamental unit of \( F \) is \(-1\), and (ii) the ideal class number of \( F \) is \( 1 \), and \( 2 \) is odd.

Let \( \mathcal{G} \) be the quaternion algebra over \( \mathbb{Q} \) which is non-split only at \( p \) and \( \infty \). We put \( \mathcal{G}_F = \mathcal{G} \otimes_{\mathbb{Q}} F \) and let \( N: \mathcal{G}_F \to F \) be the reduced norm. There are two infinite (real) primes for \( F \), and \( \mathcal{G}_F \) is nonsplit at these primes. Since \( p \) is a square in \( F \), \( \mathcal{G}_F \) is split for \( \sqrt{p} \) \((p)\); hence, \( \mathcal{G}_F \) is split for all finite primes. Let \( V = \{ a \in \mathcal{G}_F \mid a^* = a \} \).
1.5.1 Proposition: (i) $\mathcal{O}_F$ is a positive definite quaternary space over $F$ which supports the genus $G(4, 1)$ of even unimodular lattices over $\mathcal{O}$ of discriminant $1$.

(ii) $\mathcal{O}$ is a positive definite quaternary space over $\mathbb{Q}$ which supports the genus $G(4, \mathfrak{p}^2)$ of even quaternary lattices over $\mathbb{Z}$ of discriminant $\mathfrak{p}^2$.

(iii) $\mathcal{V}$ is a positive definite quaternary space over $\mathbb{Q}$ which supports the genus $G(4, \mathfrak{p})$ of even quaternary lattices over $\mathbb{Z}$ of discriminant $\mathfrak{p}$.

Proof: (i) Every maximal order $\mathfrak{O}$ of $\mathcal{O}_F$ is an even unimodular lattice of discriminant $1$. This is because $\mathcal{O}_F$ is split for all finite primes $\mathfrak{p}$; hence $\mathfrak{O}_\mathfrak{p}$ is unimodular for all $\mathfrak{p}$. Note that $\mathfrak{O}$ is free by Proposition in Appendix [K]; hence, $\mathfrak{O}$ has discriminant $1$.

(ii) If $\mathfrak{O}$ is a maximal order of $\mathcal{O}$, then $\mathfrak{O}_r$ is unimodular for all $r \neq \mathfrak{p}$. At the prime $\mathfrak{p}$, $\mathfrak{O}_\mathfrak{p} \cong \langle 1 \rangle \perp \langle -\Delta \rangle \perp \langle \mathfrak{p} \rangle \perp \langle -\Delta \mathfrak{p} \rangle$, since $\mathcal{O}_\mathfrak{p}$ is anisotropic. Hence, $\mathfrak{O}$ is an even quaternary lattice of discriminant $\mathfrak{p}^2$ over $\mathbb{Z}$.

(iii) See [P₁], Proposition 2, or [K₃], page 92.

Q.E.D.

1.5.2 Definition: Let $U$ be a quaternary quadratic space over a field $K$. A similitude $\sigma$ of $U$ is a linear automorphism of $U$ satisfying $Q(\sigma(x)) = a_\sigma Q(x)$ for every $x \in U$, where $a_\sigma \in K$. The number $a_\sigma$ is called the norm of $\sigma$. An orthogonal transformation of $U$ is a similitude of $U$ having norm $1$. 
If \( \sigma \) is a similitude, then \( \det \sigma = \pm a_0^2 \). We say that \( \sigma \) is proper or improper according as the plus or minus sign holds.

1.5.3 **Proposition** ([P] pages 4-6): (a) The proper similitudes of \( A \) (respectively \( A_P \)) are all the mappings of the form \( \xi \mapsto a\xi A \), where \( a, \beta \in A \) (\( a, \beta \in A_P \)).

(b) The proper orthogonal transformations of \( A \) (respectively \( A_P \)) are all the mappings of the form \( \xi \mapsto a\xi^{-1} \), where \( a, \beta \in A \) (\( a, \beta \in A_P \)) and \( N(a) = N(\beta) \).

(c) The proper similitudes of \( V \) are all the mappings of the form \( \xi \mapsto c a\xi A^* \), where \( c \in \{ \} \) and \( a \in A_P \).

(d) The proper orthogonal transformations of \( V \) are all the mappings of the form \( \xi \mapsto a\xi^{-1} \), where \( a \in A_P \) and \( N(a) \in \{ \} \).

1.5.4 **Definition**: Two lattices \( A_1 \) and \( A_2 \) (on \( A, A_P, \) or \( V \)) are similar if \( aA_1 = A_2 \) for some proper similitude \( a \). We say that \( A_1 \) and \( A_2 \) are in the same similitude class if they are similar.

Let \( \mathcal{L} \) be a lattice in \( J(4, 1) \), then by local consideration it is easy to show that \( \mathcal{L} \) is a normal ideal of \( A_P \). Furthermore, if \( \mathcal{L} \) represents 2, then \( \mathcal{L} \) is isometric to its left order (and its right order) (see Proposition 3.1.1). It follows that the isometry classes \( \{ \Omega \} \), where \( \Omega \) runs through the maximal orders of \( A_P \), are all the classes in
\( \mathcal{J}(4, 1) \) which represents 2. We denote by \( \mathcal{J}'(4, 1) \) the subset of \( \mathcal{J}(4, 1) \) consisting of all lattices which represent 2. There exist certain maximal orders in \( \mathcal{A}_F \) which are of special interest.

1.5.5 Definition: An \( \mathcal{O} \)-lattice \( \Lambda \) on \( \mathcal{A}_F \) is symmetric if \( \Lambda^* = \Lambda \).

1.5.6 Proposition ([H], page 170): Let \( \Omega \) be a symmetric maximal order of \( \mathcal{A}_F \), then \( L = \Omega \cap V \) is a lattice in \( G(4, p) \) which represents 2. Moreover, if \( \Omega_1 \) and \( \Omega_2 \) are two symmetric maximal orders of \( \mathcal{A}_F \) and \( L_i = \Omega_i \cap V \), \( i = 1, 2 \), then \( L_1 \cong L_2 \) if and only if \( \Omega_1 \cong \Omega_2 \).

If we start with a lattice \( L \) in \( G(4, p) \), then there is associated a unique lattice \( \hat{L} \) in \( \mathcal{J}(4, 1) \) such that \( \hat{L} \cap V = L \) by the following construction:

if \( p \) and \( P \mid r \), then \( \hat{L}_P \) is the closure of \( L_r \) in \( (\mathcal{A}_F)_P \);

at the prime \( \mathfrak{p} \mid p \), assume that \( L_p = \mathbb{Z}_{p^2} x_1 \bot \mathbb{Z}_{p^2} x_2 \bot \mathbb{Z}_{p^2} x_3 \bot \mathbb{Z}_{p^2} x_4 \approx \langle \varepsilon_1 \rangle \bot \langle \varepsilon_2 \rangle \bot \langle \varepsilon_3 \rangle \bot \langle \varepsilon_4 \rangle \), where \( \varepsilon_i \in \mathbb{Q}/\mathbb{Z} \); then

\( \hat{L}_\mathfrak{p} = \mathcal{O}_{\mathfrak{p}} x_1 \bot \mathcal{O}_{\mathfrak{p}} x_2 \bot \mathcal{O}_{\mathfrak{p}} x_3 \bot \mathcal{O}_{\mathfrak{p}}^{1/2} x_4 \).

1.5.7 Proposition ([P_2], page 137): Let \( L \) be a lattice in \( G(4, p) \), then \( \hat{L} \) is a symmetric normal ideal of \( \mathcal{A}_F \). Furthermore, \( \hat{L} \) is isometric to a symmetric maximal order of \( \mathcal{A}_F \) if and only if \( L \) represents 2.
Denote by $G'(4, p)$ the subset of $G(4, p)$ consisting of those lattices which represent 2.

1.5.8 Corollary: There is a one-to-one correspondence between the classes in $J'(4, 1)$ and those in $G'(4, p)$.

We now consider the lattices in $G(4, p^2)$.

1.5.9 Proposition: Let $L$ be any lattice in $G(4, p^2)$, then $L$ is a normal ideal of $\mathcal{Q}$. Furthermore, if $L$ represents 2, then $L$ is isometric to a maximal order of $\mathcal{Q}$.

Proof: Fix a maximal order $O$ of $\mathcal{Q}$. Since $L$ and $O$ are in the same genus, they are locally isometric; hence, $L_r = \alpha_r O_r \beta_r^{-1}$, where $\alpha_r, \beta_r \in \mathcal{Q}_r$ and $N(\alpha_r) = N(\beta_r)$. This shows that the left and right orders of $L$ are maximal; hence, $L$ is a normal ideal. The proof of the last statement is identical to Proposition 3.1.1. Q.E.D.

In Chapter II we will see that, in addition to the lattices which represent 2, there exist other lattices in $G(4, p^2)$ which have nontrivial automorphism groups. These are the lattices which represent $2p$. We shall describe them in the language of quaternion algebra.

1.5.10 Definition: Let $O$ be a maximal order of $\mathcal{Q}$, then there is a two-sided prime ideal $\mathfrak{P}$ associated with $O$ in the following canonical way: $\mathfrak{P}_r = O_r$ for all $r \neq p$ and $\mathfrak{P}_p = \rho O_p$, where $\rho^2 = p$ (i.e. $\mathfrak{P}_p$ is the unique two-sided prime
ideal of $\mathcal{O}_p$). We shall refer to $\mathfrak{p}$ loosely as the two-sided prime ideal of $\mathcal{O}$.

1.5.11 Proposition: Let $\mathfrak{p}$ be the two-sided prime ideal of $\mathcal{O}$, then $\frac{1}{\mathfrak{p}}$ is a lattice on the space $\mathcal{O}^\mathfrak{p}$ of discriminant $p^2$ such that $\frac{1}{\mathfrak{p}} \simeq \mathcal{O}$.

Proof: Let $\mathcal{O}_p = \mathbb{Z}_p x_1 + \mathbb{Z}_p x_2 + \mathbb{Z}_p x_3 + \mathbb{Z}_p x_4 \cong <1> \perp <\Delta> \perp <\mathfrak{p}> \perp <\mathfrak{p}^-> \perp <\mathfrak{p}^+>$, then $\mathfrak{p} = \mathbb{Z}_p x_1 + \mathbb{Z}_p x_2 + \mathbb{Z}_p x_3 + \mathbb{Z}_p x_4 \cong <\mathfrak{p}> \perp <\mathfrak{p}^-> \perp <\mathfrak{p}^+> <\mathfrak{p}^2> \perp <\mathfrak{p}^2>$; hence,

$\frac{1}{\mathfrak{p}} \cong <1> \perp <\Delta> \perp <\mathfrak{p}> \perp <\mathfrak{p}^-> <\mathfrak{p}^+> <\mathfrak{p}^2> <\mathfrak{p}^2>$. Clearly, $\frac{1}{\mathfrak{p}}$ has discriminant $p^2$. Now the dual lattice of $\mathcal{O}$ is just $\mathfrak{p}^{-1}$. Since $\mathfrak{p}^2 = p\mathcal{O}$, we have $\mathfrak{p} = p\mathfrak{p}^{-1} = p\mathcal{O}^\mathfrak{p}$. It follows that $\mathfrak{p}$ is similar to $\mathcal{O} = (\mathcal{O}^\mathfrak{p})^\mathfrak{p}$; hence, $\frac{1}{\mathfrak{p}} \cong \mathcal{O}$, because they both have discriminant $p^2$. Q.E.D.

Since $\alpha^{1/p} \cong \alpha$ by a computation of Hasse symbols, we may identify $\mathfrak{p}$ with a sublattice of $\mathcal{O}$. We can show that $\frac{1}{\mathfrak{p}}$ represents $2p$. (Note that $\mathcal{O}$ represents $2p$ by Lemma 2.7.1.) To provide another proof, observe that $\mathcal{O}$ contains the identity element $1$, so $\mathfrak{p}$ contains $p\cdot 1$ (an element in $\mathcal{O}$); therefore, $\mathfrak{p}$ represents $2p^2$. But this means that $\frac{1}{\mathfrak{p}}$ represents $2p$. Conversely

1.5.12 Proposition: Let $\mathcal{L}$ be a lattice in $G(4, p^2)$ which represents $2p$, then $\mathcal{L} \cong \frac{1}{\mathfrak{p}}$, where $\mathfrak{p}$ is the two-sided prime ideal of some maximal order $\mathcal{O}$.
Proof: If \( L \) represents \( 2p \), then \( \hat{L} \) represents \( 2 \) (by Lemma 2.7.11). Hence, \( \hat{L} \) is isometric to a maximal order \( \mathcal{O} \) of \( \mathcal{G} \) by Proposition 1.5.9. It follows that \( L \cong \mathcal{O} \) which is similar to \( \mathfrak{P} \), so \( L \cong \mathfrak{P}^{1/p} \). Q.E.D.

Therefore, the classes \( \{ \mathfrak{P}^{1/p} \} \), where \( \mathfrak{P} \) runs through all the two sided prime ideals of maximal orders, are all the classes in \( G(4, p^2) \) which represent \( 2p \), and they are essentially the reciprocals of those classes which represent \( 2 \). We show in the following lemma that different \( \mathfrak{P} \)'s corresponding to different conjugacy classes of maximal orders yield nonisometric classes \( \{ \mathfrak{P}^{1/p} \} \).

1.5.13 Lemma: Let \( \mathfrak{P}_1 \) and \( \mathfrak{P}_2 \) be two-sided prime ideals of the maximal orders \( \mathcal{O}_1 \) and \( \mathcal{O}_2 \), respectively, then \( \mathfrak{P}_1^{1/p} \cong \mathfrak{P}_2^{1/p} \) if and only if \( \mathcal{O}_1 \cong \mathcal{O}_2 \).

Proof: \((\Rightarrow)\) If \( \mathfrak{P}_1^{1/p} \cong \mathfrak{P}_2^{1/p} \), then \( \mathfrak{P}_1 \cong \mathfrak{P}_2 \), so \( \mathfrak{P}_1 = \alpha \mathfrak{P}_2^{\beta^{-1}} \) for some \( \alpha, \beta \in \mathcal{O}^* \) which satisfy \( N(\alpha) = N(\beta) \). Since the left order of \( \alpha \mathfrak{P}_2^{\beta^{-1}} \) is \( \alpha \mathcal{O}_2 \alpha^{-1} \), we have \( \mathcal{O}_1 = \alpha \mathcal{O}_2 \alpha^{-1} \); hence, \( \mathcal{O}_1 \cong \mathcal{O}_2 \).

\((\Leftarrow)\) If \( \mathcal{O}_1 \cong \mathcal{O}_2 \), then \( \mathcal{O}_1^{\#} \cong \mathcal{O}_2^{\#} \); hence, \( \mathfrak{P}_1 = p \mathcal{O}_1^{\#} \cong \mathfrak{P}_2 = p \mathcal{O}_2^{\#} \). This implies that \( \mathfrak{P}_1^{1/p} \cong \mathfrak{P}_2^{1/p} \). Q.E.D.

It follows that there are as many classes in \( G(4, p^2) \) which represent \( 2p \) as classes which represent \( 2 \). But there are some overlaps among these classes; that is, there are classes which represent both \( 2 \) and \( 2p \).
1.5.14 Proposition: Let $L \in G(4, p^2)$ represent both 2 and $2p$, then $L$ is isometric to a maximal order which is similar to its two-sided prime ideal. In this case, the prime ideal is principal.

Proof: By Proposition 1.5.9, $L \cong \mathfrak{O}$ for some maximal order $\mathfrak{O}$. Since $L$ also represents $2$, $L \cong \mathfrak{O}_1$ for a maximal order $\mathfrak{O}_1$. Now $L \cong \mathfrak{O}$ is similar to $\mathfrak{P}$, where $\mathfrak{P}$ is the two-sided prime ideal of $\mathfrak{O}$, so $\mathfrak{O}_1$ is similar to $\mathfrak{P}$. This means that $\mathfrak{O}$ and $\mathfrak{O}_1$ are in the same conjugacy class and $\mathfrak{O}$ is similar to $\mathfrak{P}$. To show that $\mathfrak{P}$ is principal, observe that $\mathfrak{P} = \alpha \mathfrak{O} \beta$ for some $\alpha, \beta \in \mathcal{O}^\times$; hence, $\mathfrak{O} = \alpha \mathfrak{O} \alpha^{-1}$. This means that $\alpha \mathfrak{O} = \mathfrak{O} \alpha$ is two-sided; therefore, $\mathfrak{P} = \mathfrak{O} \alpha \beta$. Q.E.D.

Denote by $G'(4, p^2)$ the subset of $G(4, p^2)$ consisting of those lattices which represent 2 or $2p$. We now investigate the relation between the classes in $G'(4, p^2)$ and the classes in $\mathcal{O}'(4, 1)$, and also with the classes in $G'(4, p)$.

1.5.15 Definition: An $\mathcal{O}$-lattice $\Lambda$ of $\mathcal{O}_F$ is reflexive if $\Lambda = \Lambda$.

For a maximal order $\mathfrak{O}$ of $\mathcal{O}_F$, we have $\mathfrak{O}^* = \mathfrak{O}$. Hence, $\mathfrak{O}$ is reflexive if and only if it is symmetric.

If we start with a lattice $L$ in $G(4, p^2)$, we can construct a unique lattice $\hat{L}$ in $\mathcal{O}(4, 1)$ such that $\hat{L} \cap \mathcal{O} = L$ in the following way:
If \( r \neq p \) and \( p | r \), then \( \hat{L}_p \) is the closure of \( L_r \) in \((\mathcal{A}_r)_p\).

At the prime \( p \), let \( L_p = \mathbb{Z}_{p_1} x_1 \uparrow \mathbb{Z}_{p_2} x_2 \uparrow \mathbb{Z}_{p_3} x_3 \uparrow \mathbb{Z}_{p_4} x_4 \cong <1> \uparrow <-\Delta> \uparrow <p> \uparrow <-\Delta_p> \), then \( \hat{L}_p = \mathcal{O}_{\mathcal{A}} x_1 \uparrow \mathcal{O}_{\mathcal{A}} x_2 \uparrow \mathcal{O}_{\mathcal{A}} \frac{1}{\sqrt{p}} x_3 \uparrow \mathcal{O}_{\mathcal{A}} \frac{1}{\sqrt{p}} x_4 \cong <1> \uparrow <-\Delta> \uparrow <1> \uparrow <-\Delta> \).

1.5.16 Proposition: Let \( L \) be a lattice in \( G(4, p^2) \), then \( L \) is a reflexive normal ideal of \( \mathcal{A}_F \). Furthermore, if \( L = \mathcal{O} \) is a maximal order, then \( \mathcal{O} \) is a symmetric maximal order of \( \mathcal{A}_F \).

Proof: Fix a symmetric maximal order \( \Omega \) of \( \mathcal{A}_F \), then \( \Omega \cap \mathcal{A} \) is a maximal order of \( \mathcal{A} \) and \( L = \hat{\Omega} (\Omega \cap \mathcal{A})^{\beta^{-1}} \) for some \( \hat{\alpha}, \hat{\beta} \in \mathcal{A} \), since \( L \) and \( \Omega \cap \mathcal{A} \) are locally isometric. At the prime \( p \), let \( (\Omega \cap \mathcal{A})_p = \mathbb{Z}_{p_1} x_1 \uparrow \mathbb{Z}_{p_2} x_2 \uparrow \mathbb{Z}_{p_3} x_3 \uparrow \mathbb{Z}_{p_4} x_4 \cong <1> \uparrow <-\Delta> \uparrow <p> \uparrow <-\Delta_p> \), then \( L_p = \mathbb{Z}_p \alpha x_1 \beta^{-1} \uparrow \mathbb{Z}_p \alpha x_2 \beta^{-1} \uparrow \mathbb{Z}_p \frac{1}{\sqrt{p}} x_3 \beta^{-1} \uparrow \mathbb{Z}_p \frac{1}{\sqrt{p}} x_4 \beta^{-1} \cong <1> \uparrow <-\Delta> \uparrow <p> \uparrow <-\Delta_p> \).

By definition, \( \hat{L}_p = \mathcal{O}_{\mathcal{A}} \alpha x_1 \beta^{-1} \uparrow \mathcal{O}_{\mathcal{A}} \alpha x_2 \beta^{-1} \uparrow \mathcal{O}_{\mathcal{A}} \frac{1}{\sqrt{p}} x_3 \beta^{-1} \uparrow \mathcal{O}_{\mathcal{A}} \frac{1}{\sqrt{p}} x_4 \beta^{-1} \), \( \mathcal{O}_{\mathcal{A}} \frac{1}{\sqrt{p}} x_4 \beta^{-1} = \alpha_p (\mathcal{O}_{\mathcal{A}} \alpha x_1 \uparrow \mathcal{O}_{\mathcal{A}} \alpha x_2 \uparrow \mathcal{O}_{\mathcal{A}} \frac{1}{\sqrt{p}} x_3 \uparrow \mathcal{O}_{\mathcal{A}} \frac{1}{\sqrt{p}} x_4) \beta^{-1} = \alpha_p \Omega \beta^{-1} \). Similarly for any prime \( p | r \), \( r \neq p \), \( \hat{L}_r = \alpha_r \Omega \beta^{-1} \); hence, \( \hat{L} = \hat{\Omega} \beta^{-1} \). It is clear that \( \hat{L} \) is reflexive. If \( L = \mathcal{O} \) is a maximal order and \( \mathcal{O} = \hat{\Omega} (\Omega \cap \mathcal{A})^{\beta^{-1}} \), then \( \mathcal{O} = \hat{\Omega} (\Omega \cap \mathcal{A})^{\beta^{-1}} \).

Therefore, \( \hat{\mathcal{O}} = \hat{\Omega} \beta^{-1} \) is a maximal order. Q.E.D.
It follows from Proposition 1.5.16 and Proposition 1.5.6 that to each class \{G\} in G'(4, p^2) which represents 2, we can associate a class \{\hat{G} \cap V\} in G'(4, p). By Proposition 4, [P_3], this association (not necessarily one-to-one) is the same as the correspondence we obtain in Proposition 2.7.9, Chapter II. We describe these two correspondences by the following picture:

```
Prop. 1.5.16  Prop. 1.5.6
\{G\}  \downarrow
\{\hat{D}\}  \{\hat{G} \cap V\}
```

The correspondence is one-to-one when \(\mathfrak{D}\) only represents 2 (or equivalently, the two-sided prime ideal \(\mathfrak{P}\) of \(\mathfrak{D}\) is non-principal). The correspondence is two-to-one when \(\mathfrak{D}\) represents both 2 and 2p (or when \(\mathfrak{P}\) is principal), except when the binary lattice \(\langle 2 \rangle \perp \langle 2p \rangle\) in \(\mathfrak{D}\) is ambiguous: \(\langle 2 \rangle \perp \langle 2p \rangle\) is ambiguous if it has a nontrivial automorphism group; this occurs only when \(p \equiv 5 \pmod{8}\). Since the correspondence in Proposition 1.5.6 is one-to-one, we have

1.5.17 Proposition: The correspondence \(\{D\} \mapsto \{\hat{G}\}\) in Proposition 1.5.16 is one-to-one when the two-sided prime ideal \(\mathfrak{P}\) of \(\mathfrak{D}\) is nonprincipal; otherwise, it is two-to-one, except in the ambiguous case.
We shall now consider a correspondence between the reciprocals of \( \{\mathcal{O}\} \) and those of \( \{\hat{\mathcal{O}} \cap V\} \).

1.5.18 Proposition: Let \( \mathfrak{p} \) be the two-sided prime ideal of a maximal order \( \mathcal{O} \) of \( A \). Then \( (\mathfrak{p} \cap V)^{1/p} \) is a lattice on \( V^{1/p} \) of discriminant \( p^3 \) which is isometric to the reciprocal of \( \hat{\mathcal{O}} \cap V \).

Proof: Since \( \mathfrak{p} = \sqrt{p} \hat{\mathcal{O}} \), we have \( \hat{\mathfrak{p}}^{-1} = \frac{1}{\sqrt{p}} \hat{\mathcal{O}} \). It is easy to see that \( (\hat{\mathfrak{p}}^{-1} \cap V)^r = (\hat{\mathcal{O}} \cap V)^r \) for all \( r \neq p \).

At the prime \( p \), assume that \( (\hat{\mathcal{O}} \cap V)^p = Z_p x_1 \perp Z_p x_2 \perp Z_p x_3 \perp Z_p x_4 \cong \langle \epsilon_1 \rangle \perp \langle \epsilon_2 \rangle \perp \langle \epsilon_3 \rangle \perp \langle \epsilon_4 \rangle \) for some \( \epsilon_i \in \hat{Z}_p \), \( 1 \leq i \leq 4 \).

Then \( \hat{\mathfrak{p}}_y = \epsilon_y x_1 \perp \epsilon_y x_2 \perp \epsilon_y x_3 \perp \epsilon_y x_4 \cong \langle \epsilon_1 \rangle \perp \langle \epsilon_2 \rangle \perp \langle \epsilon_3 \rangle \perp \langle \epsilon_4 \rangle \). Now \( \hat{\mathfrak{p}}_y^{-1} = 1/\sqrt{p} \hat{\mathcal{O}}_y = \epsilon_y 1/\sqrt{p} x_1 \perp \epsilon_y 1/\sqrt{p} x_2 \perp \epsilon_y 1/\sqrt{p} x_3 \perp \epsilon_y 1/\sqrt{p} x_4 \), so \( (\hat{\mathfrak{p}}^{-1} \cap V)^p = Z_p x_1 \perp Z_p x_2 \perp Z_p x_3 \perp Z_p x_4 \cong \langle \epsilon_1 \rangle \perp \langle \epsilon_2 \rangle \perp \langle \epsilon_3 \rangle \perp \langle \epsilon_4 \rangle \).

It follows that \( \hat{\mathfrak{p}}^{-1} \cap V \) is the dual lattice of \( \hat{\mathcal{O}} \cap V \). But \( \hat{\mathfrak{p}} = p\hat{\mathfrak{p}}^{-1} \), so \( \hat{\mathfrak{p}} \cap V = p(\hat{\mathfrak{p}}^{-1} \cap V) \); therefore, \( \hat{\mathfrak{p}} \cap V \) has discriminant \( p^7 \) and \( (\hat{\mathfrak{p}} \cap V)^{1/p} \) has discriminant \( p^3 \). Since \( \hat{\mathfrak{p}} \cap V \) and the dual of \( \hat{\mathcal{O}} \cap V \) are similar, \( (\hat{\mathfrak{p}} \cap V)^{1/p} \) is isometric to the reciprocal of \( \hat{\mathcal{O}} \cap V \). Q.E.D.

By Proposition 1.5.18 and Proposition 1.5.12, to each class \( \{\mathfrak{T}^{1/p}\} \) in \( G'(4, p^2) \) which represents \( 2p \), there is associated a class \( \{(\mathfrak{p} \cap V)^{1/p}\} \) of discriminant \( p^3 \) which is the reciprocal of the class \( \{\hat{\mathcal{O}} \cap V\} \).
1.5.19 Definition: If \( L \) is a lattice on \( V \), then the \textbf{reduced discriminant} of \( L \) is defined to be \( \det [v^{-1}B(v_i, v_j)] \), where \( \{v_i\} \) is a basis of \( L \) and \( v \) is the unique positive rational number which generates \( n(L) \).

If \( L \) has reduced discriminant \( p \), then clearly the lattice \( L^{1/v} \) has discriminant \( p \); therefore, any lattice \( L \)
with reduced discriminant $p$ is in the same similitude class of a lattice in $G(4, p)$. Suppose $L_1, \ldots, L_h$ are all nonisometric lattices in $G(4, p)$, then $L_1, \ldots, L_h$ are also not similar, otherwise they would be isometric. Hence, there are as many isometry classes of discriminant $p$ as similitude classes of reduced discriminant $p$. A similar argument applies for lattices of discriminant $p^3$. 
Chapter II

THETA SERIES OF QUADRATIC LATTICES OVER $\mathbb{Z}$

This chapter is devoted to a study of theta series of even positive definite lattices over $\mathbb{Z}$. First, we begin with some general discussions about dual representations and characteristic sublattices. These concepts are crucial to our proof of the linear independence of theta series, and we shall formulate them under a more general assumption of the ring. In the following, $F$ will denote a totally real algebraic number field with ring of integers $\mathcal{O}$, $\mathcal{U}$ the group of units of $\mathcal{O}$.

§2.1 Dual Representations

We assume in this section that $\mathcal{O}$ is a principal ideal domain; hence, every lattice over $\mathcal{O}$ is free. If $L$ is any $\mathcal{O}$-lattice and $\alpha \in F$, then $d_L = \alpha$ means that $L$ has a basis $L = \mathcal{O}x_1 + \ldots + \mathcal{O}x_n$ in which $d(x_1, \ldots, x_n) = \alpha$.

2.1.1 Proposition: Let $L$ be an integral $\mathcal{O}$-lattice of rank $n$ and discriminant $d_L = \alpha$. For any $\gamma \in \mathcal{O}$, there is a one-to-one correspondence between the primitive sublattices $M$ of $L$ of rank $n-1$ and discriminant $d_M = \gamma$ and the primitive sublattices $\mathcal{O}_y$ of $L^\#$ with $Q(y) = \gamma/\alpha$. 

36
Proof: Let \( M \) be a primitive sublattice of \( L \) with rank of \( M = n-1 \) and \( dM = \gamma \). Then there is a basis \( \{x_1, \ldots, x_{n-1}\} \) of \( M \) in which \( d(x_1, \ldots, x_n) = \gamma \). Extend it to a basis of \( L \) with the adjunction of some vector \( x_n \), and let \( A = (B(x_i, x_j)) \) be the matrix of \( L \) with respect to \( \{x_1, \ldots, x_n\} \) and \( \text{adj} \ A = (A_{ij}) \) be the matrix adjoint to \( A \). We may assume that \( \det A = \alpha \). It is clear that \( L^\# = \mathcal{O}y_1 + \cdots + \mathcal{O}y_n \), where \( \{y_1, \ldots, y_n\} \) is the dual basis of \( \{x_1, \ldots, x_n\} \). A routine calculation gives

\[
y_j = \frac{1}{\alpha} (A_{j1} x_1 + \cdots + A_{jn} x_n), \quad j = 1, \ldots, n.
\]

From the general matrix theory we know that

\[
\sum_{k=1}^{n} B(x_i, x_k) A_{jk} = \alpha \delta_{ij};
\]

hence, it follows that

\[
Q(y_n) = \frac{1}{\alpha^2} (A_{11}, \ldots, A_{nn}) (A_{11}, \ldots, A_{nn})^t = \frac{A_{nn}}{\alpha} = \frac{\gamma}{\alpha}.
\]

Conversely, let \( \mathcal{O}y \) be a primitive sublattice of \( L^\# \) with \( Q(y) = \gamma/\alpha \). Then \( M = L \cap (Fy)^\perp \) is a primitive sublattice of \( L \) of rank \( n-1 \). If \( \{x_1, \ldots, x_{n-1}\} \) is a basis of \( M \), we can again complete it to a basis of \( L \) by adjoining some vector \( x_n \). Since \( y \) is primitive in \( L^\# \), there is a vector \( u \) in \( L \) with \( B(u, y) = 1 \). By writing \( u = \sum_{i=1}^{n} \alpha_i x_i \), one sees that \( B(\alpha_n x_n, y) = 1 \) with \( \alpha_n \in U \). Let \( \{y_1, \ldots, y_n\} \) be the dual basis.
for \{x_1, \ldots, x_n\}. It is clear that \( y_n = y \) and  
\[
Q(y_n) = \frac{d(x_1, \ldots, x_n)}{d(x_1, \ldots, x_{n-1}, a_n x_n)}.
\]
Since \( \{x_1, \ldots, x_{n-1}, a_n x_n\} \) is a basis for \( L \), we have  
\[
d(x_1, \ldots, a_n x_n) = \alpha \epsilon^2 \quad \text{for some } \epsilon \in \mathbb{U}.
\]
Therefore,  
\[
d(x_1, \ldots, x_{n-1}) = \left(\frac{\gamma}{\alpha}\right) d(x_1, \ldots, x_{n-1}, a_n x_n) = \left(\frac{\gamma}{\alpha}\right) \alpha \epsilon^2 = \gamma \epsilon^2.
\]
Hence, \( dM = \gamma \). Q.E.D.

If \( \Theta' = \mathbb{Z} \), then we let \( \Omega \) denote the g.c.d. of the entries \( A_{ij} \) in the adjoint matrix to \( A \). It is clear that \( \Omega \) as well as the discriminant \( dL \) of \( L \) are independent of the choice of the basis.

2.1.2 Definition: Let \( L \) be an integral \( \mathbb{Z} \)-lattice of discriminant \( \alpha \). The reciprocal of \( L \) is the lattice \( (L^\#)^{\alpha/\Omega} \) obtained by scaling the dual lattice \( L^\# \) by \( \alpha/\Omega \). We shall denote it by \( \hat{L} \). Clearly, \( \hat{L} \) is integral with \( d\hat{L} = \alpha^{n-1}/\Omega^n \).

2.1.3 Corollary: Let \( L \) be an integral \( \mathbb{Z} \)-lattice of rank \( n \) and discriminant \( \alpha \). Suppose \( \Omega = 1 \), then for any \( \gamma \in \mathbb{Z} \), there is a one-to-one correspondence between the primitive sublattices \( M \) of \( L \) of rank \( n-1 \) and discriminant \( \gamma \) and the primitive sublattices \( \mathcal{L}^{-1} \) of \( \hat{L} \) with \( Q(\gamma) = \gamma \).

2.1.4 Remark: If \( L \) has the matrix \( A \) with respect to some basis, then \( \hat{L} \) has the matrix \( (\alpha/\Omega)A^{-1} = (1/\Omega)\text{adj } A \). Since  
\[
\text{adj}((1/\Omega)\text{adj } A) = (\alpha^{n-2}/\Omega^{n-1})A,
\]
the g.c.d. of its entries
is \((\alpha^{n-2}/\Omega^{n-1})\omega\), where \(\omega\) is the g.c.d. of \(a_{ij}\). It follows that
\[
L = \left(\frac{\omega^{n-1}}{\alpha^{n-2}} \cdot \Omega^{n-1} \cdot \frac{1}{\omega} \cdot \frac{\alpha}{\Omega} \cdot \frac{1}{\omega} \cdot \frac{\alpha}{\Omega} \right) \subset L.
\]
So if \(L\) is primitive, then \(L^G \cong L\).

\section*{2.2 Characteristic Sublattices}

The notion of characteristic sublattices was introduced by Kitaoka over \(\mathbb{Z}\) and its completions \(\mathbb{Z}_p\) (see [K2]). In this section we shall give a treatment of this for lattices over the ring \(\mathcal{O}\) and its completions \(\mathcal{O}_p\) at the finite primes \(p\) of \(F\). Let \(L\) be a lattice over \(\mathcal{O}_p\). Then \(L\) has a Jordan splitting \(L = L_1 \perp L_2 \perp \ldots \perp L_t\), where \(L_i\) is \(p^{a_i}\)-modular and \(a_1 < \ldots < a_t\).

\subsection*{2.2.1 Notation:}
Denote by \(t_p(L)\) the ordered \(n\)-tuple 
\((a_1, \ldots, a_1, \ldots, a_t, \ldots, a_t)\) in which \(a_i\) occurs with multiplicity \(\dim L_i\) and \(n = \dim L\). It is clear that \(t_p(L)\) is independent of the choice of the Jordan splitting. The set of \(n\)-tuples will be ordered by the lexicographic ordering.

Although the scale of each component in a Jordan splitting is invariant of the lattice \(L\), the same is not true for its norm. However, if we let \(s_i\) denote the scale of the \(i\)th component, then \(nL s_i\) is an invariant.
2.2.2 Lemma: Let \( L \) be an \( \mathcal{O}_p \)-lattice with \( t \) components in its Jordan splitting. For each \( 1 \leq i \leq t \), there exists a Jordan splitting \( L = L_1 \oplus L_2 \oplus \ldots \oplus L_t \) such that \( nL_i = nL_i \).

Proof: Fix \( 1 \leq i \leq t \) and let \( L = L_1 \oplus \ldots \oplus L_t \) be any Jordan splitting of \( L \). Then \( L_i \) is the first component of some Jordan splitting of \( L_i \). We consider the following cases:

Case (i). \( p \) non-dyadic. Since norm and scale are equal over nondyadic fields, it follows that \( s_i = nL_i \subseteq nL_i \).

Case (ii). \( p \) dyadic, \( \dim L_i \geq 3 \). By \( 93:21 \) [OM], we can find a splitting of \( L \) such that \( gL_i = gL_i \). But this implies that \( nL_i = nL_i \).

Case (iii). \( p \) dyadic, \( \dim L_i = 2 \). By scaling we may assume that \( L_i \) is unimodular; hence, \( L_i = A(a, \beta) \) with respect to some basis \( \{x, y\} \), where \( a \) is a norm generator of \( L_i \) and \( \beta \in nL_i \) (93:10 [OM]). If \( nL_i \not\subseteq nL_i \), then there exists a vector \( z \) in the orthogonal complement of \( L_i \) in \( L_i \) such that \( Q(z) \) generates \( nL_i \). Replace \( L_i \) by the lattice \( \mathcal{O}_p(x + z) + \mathcal{O}_p \). Since \( L_i \) splits \( L \), it is the \( i \)th component of some Jordan splitting of \( L \). Now we have \( |Q(x + z)| = |a + Q(z)| = |Q(z)| \) by the principle of domination; hence \( nL_i = nL_i \). Q.E.D.
2.2.3 **Lemma**: Let $L$ be an $\mathfrak{O}_p$-lattice with $t$ components in its Jordan splitting. Then $L$ contains a primitive regular sublattice $M$ of codimension 1 which satisfies:

(LC) If $L'$ is any $\mathfrak{O}_p$-lattice on $F_pL$ containing $M$ with $dL' = dL$, $t_p(L') \geq t_p(L)$ and $nL' = nL$, then $L' = L$.

**Proof**: We first consider the case that $L$ is modular. By scaling we may assume that $L$ is unimodular. Let $L'$ be a lattice as in the hypothesis. Then it is clear that $L'$ is also unimodular and $nL' = nL$. Suppose that $L$ has an orthogonal basis $L = \mathfrak{O}_p x_1 \perp ... \perp \mathfrak{O}_p x_n$. We can set $M = \mathfrak{O}_p x_1 \perp ... \perp \mathfrak{O}_p x_{n-1}$, which is a unimodular sublattice of codimension 1 in $L$. If $L' \supset M$, then $M$ splits $L'$, and $L' = M \perp \mathfrak{O}_p x_n$ for some $a \in F_p$. Since $L'$ is unimodular, $a$ is a unit; hence, $L' = L$. Now suppose that $L$ does not have an orthogonal basis, then $P$ is dyadic. We divide this into two cases:

Case (i). $L$ binary. By 93:10 [OM], there is a basis $L = \mathfrak{O}_p x + \mathfrak{O}_p y$ in which $L$ has the matrix $A(a, \beta)$, where $a$ is a norm generator of $L$ and $\beta \in \omega L$. Set $M = \mathfrak{O}_p x$. If $L' \supset M$, then $L' = \mathfrak{O}_p x + \mathfrak{O}_p z$ for some $z$ such that $B(x, z) = 1$. This is because $nL' = nL$. Write $z = \gamma x + \delta y$, where $\delta, \gamma \in F_p$. We have

$$B(x, z) = B(x, \gamma x + \delta y) = a\gamma + \delta = 1,$$

$$Q(z) = a\gamma^2 + 2\gamma\delta + \beta\delta^2 \in a\mathfrak{O}_p.$$  

Consider the following inequalities.
If $|a\gamma| \geq \delta$, then $|a\gamma^2| \geq |\gamma^2| > |2\gamma\delta|$. Also, since $nL \not\subseteq \Omega_p$, we have $|a| < 1$; hence, $|\gamma| > |\delta|$. This implies that $|a\gamma^2| \geq |\gamma^2| > |2\gamma^2|$. It follows that $|Q(z)| = |a\gamma^2|$. Since $Q(z) \in a\Omega_p$, we have $\gamma \in \Omega_p$.

If $|a\gamma| < \delta$, then $|\delta| = 1$. Assume that $\gamma \not\in \Omega_p$. Then we would have $|a\gamma^2| > |2\gamma\delta|$, and $|a\gamma^2| > |\delta\delta^2|$. Therefore, $|Q(z)|$ is again dominated by $|a\gamma^2|$. But this is impossible, since $Q(z) \in a\Omega_p$.

It follows that, in any case, we have $\gamma \in \Omega_p$; hence, also $\delta \in \Omega_p$.

Case (ii). $\dim L > 4$. By 93:18 [OM], one sees readily that $L = (\Omega_p x_1 + \Omega_p y_1) \perp \cdots \perp (\Omega_p x_m + \Omega_p y_m)$, where $\Omega_p x_i + \Omega_p y_i$ is a binary unimodular lattice for all $i$ and $\Omega_p x_m + \Omega_p y_m \cong A(a, *)$ for some $a$ which generates $nL$. We set $M = (\Omega_p x_1 + \Omega_p y_1) \perp \cdots \perp (\Omega_p x_m-1 + \Omega_p y_{m-1}) \perp \Omega_p x_m$. If $L' \supset M$, then each $\Omega_p x_i + \Omega_p y_1$, $1 \leq i \leq m-1$, splits $L'$, and we can reduce to Case (i).

We now come back to the general case. By Lemma 2.2.2 there is a Jordan splitting $L = L_1 \perp \cdots \perp L_t$ such that $nL_t = nL$. Let $M_t$ be a sublattice of $L_t$ as constructed in the modular case. We put $M = L_1 \perp \cdots \perp L_{t-1} \perp M_t$. If $L' \supset M$ satisfies $dL' = dL$, $t_p(L') \geq t_p(L)$ and $nL' \supset nL$, then each $L_i$ for $1 \leq i \leq t$ splits $L'$; hence, $L = L_1 \perp \cdots \perp L_t$ for some $L' \supset M$. This is reduced to the modular case if we show that $nL' = nL$. To see this, we observe that
\[ nM_t = nL_t \] by construction. Therefore, \[ nL_t' \leq nL_t \]
\[ nL_t' \leq nL_t = nM_t \leq nL_t' . \] Q.E.D.

2.2.4 **Remark:** The condition \( nL'_t = nL_t' \) in Lemma 2.2.3 is equivalent to \( nL' = nL \) when \( L \) is modular, since there is only one component in the Jordan splitting of \( L \). If 2 is unramified in \( F \), this condition is automatically satisfied, and hence may be dropped from the hypothesis.

2.2.5 **Definition:** The lattice \( M \) in Lemma 2.2.3 is called a **locally characteristic** sublattice of \( L \).

2.2.6 **Theorem:** Let \( L \) be a global lattice over \( \mathcal{O} \). Then \( L \) contains a primitive regular sublattice \( M \) of codimension 1 which satisfies:

(GC) If \( L' \) is any \( \mathcal{O} \)-lattice with rank \( L' = \text{rank } L \),
\[ dL'_\rho = dL_\rho , \quad t_\rho(L'_\rho) \geq t_\rho(L_\rho) \quad \text{and} \quad nL'_\rho = nL_\rho \] for any prime \( \rho \) of \( F \) (\( s \) being the scale of the last component of a Jordan splitting of \( L_\rho \)), and, if there is an isometry \( \phi \) from \( M \) into \( L' \), then \( L' \cong L \).

**Proof:** By scaling we may assume that \( sL \leq \mathcal{O} \). Let \( S = \{ \rho \text{ prime of } F \mid \rho \text{ dyadic or } L_\rho \text{ is not unimodular} \} \).

By Lemma 2.2.3, we can choose a locally characteristic sublattice \( M_\rho \) in \( L_\rho \) for each \( \rho \in S \). Let \( \{x_1, \rho , \ldots , x_n, \rho \} \) be a basis of \( M_\rho \). By Lemma 1.6 [HKK], there are vectors \( x_1 , \ldots , x_n \) in \( L \) satisfying:

\( x_i \) approximates \( x_i, \rho \) at each \( \rho \in S \);
\[ d(x_1, \ldots, x_n) \in U_\mathcal{P} \text{ for all } \mathcal{P} \neq S \text{ except at one prime } q, \text{ where } q = (d(x_1, \ldots, x_n)). \]

Set \( M = \mathcal{O}x_1 + \ldots + \mathcal{O}x_n \). Clearly, \( M_\mathcal{P} \) is locally characteristic in \( \mathcal{L}_\mathcal{P} \) for each \( \mathcal{P} \neq q \). Let \( L' \) be a lattice as in the hypothesis. By Witt's theorem, we may assume that \( L' \supset M; \) hence \( L'_\mathcal{P} = L_\mathcal{P} \) for all \( \mathcal{P} \neq q \). Let \( \pi \) be a prime element at \( q \). Since \( dM_q = \pi \), we have \( M_q = X \perp \mathcal{O}_q y \), where \( X \) is unimodular and \( Q(y) \in \pi U_q \). It follows that \( L_q = X \perp Y \), where \( Y \) is unimodular containing \( y \). Now \( y \) is primitive in \( Y \); therefore, there exists a vector \( z \) such that \( B(y, z) = 1 \) and \( Y = \mathcal{O}_q y + \mathcal{O}_q z \). One sees readily by computing its discriminant that \( Y \) is isotropic. Hence, there exists a basis \( \{u, v\} \) for which \( Y \cong A(0, 0) \). Let \( y = \alpha u + \beta v \), where \( \alpha, \beta \in \mathcal{O}_q \). Without loss of generality, we may assume that \( \alpha = 1 \) and \( \beta \in \pi U_q \). Since \( L'_q \supset M_q \), we have also \( L'_q = X \perp Y' \) for some unimodular \( Y' \) containing \( y \). Therefore, \( Y' = \mathcal{O}_q y + \mathcal{O}_q (\gamma u + \delta v) \), where \( \gamma, \delta \in \mathcal{F}_q \). Now

1. \( Q(\gamma u + \delta v) = 2\gamma \delta \in \mathcal{O}_q \);
2. \( B(y, \gamma u + \delta v) = \delta + \beta \gamma \in \pi U_q \).

Consider the following cases:

Case (i). If \( \gamma \notin \mathcal{O}_q \), then \( \delta \in \pi \mathcal{O}_q \) by (1); hence, \( \gamma \in \pi^{-1} U_q \) by (2). It follows that \( Y' = \mathcal{O}_q \pi^{-1} u + \mathcal{O}_q \pi v \) and \( Y' = S_{u - \beta v} Y \).
Case (ii). If $\delta \notin \mathcal{O}_q$, then $\gamma \in \mathcal{O}_q$ by (1). But this is impossible by (2).

Case (iii). If both $\gamma$ and $\delta \in \mathcal{O}_q$, then $Y' = Y$.

Let $w$ be a global element of $L$ which is orthogonal to $M$.

It is easy to see that the two symmetries $S_w$ and $S_{w^p}$ are identical at the prime $q$. Hence, by the above considerations, we have either $L'_q = L_q$ or $L'_q = S_wL_q$. For $p \neq q$, since $M_p \subseteq S_wL_p$ and $M_p$ is locally characteristic, we have also $S_wL_p = L_p = L'_p$. It follows, therefore, that $L' = L$ or $S_wL$.

2.2.7 Definition: The lattice $M$ in Theorem 2.2.6 is called a globally characteristic sublattice of $L$.

2.2.8 Proposition: Let $L$ be a lattice over $\mathcal{O}$ and $S = \{p \text{ prime of } F \mid p \text{ dyadic or } L_p \text{ is not unimodular }\}$.

If a sublattice $M$ of $L$ satisfies:

1. $M_p$ is locally characteristic in $L_p$ for each $p \in S$, and

2. $dM_p \in U_p$ for all $p \notin S$ except at one prime $q$ where $dM \in \pi U_q$, $\pi$ is a prime element of $q$, then every automorphism of $M$ lifts to an automorphism of $L$.

Furthermore, if $L$ is positive definite, then the number of sublattices of $L$ which are isometric to $M$ is given by $|O(L)|/|O(M)|$. 
Proof: Let $\sigma \in O(M)$. By Witt's theorem, $\sigma$ lifts to an automorphism of the space $FL$ (denoted again by $\sigma$). Since $\sigma L \supset M$ and $M$ is globally characteristic, we have either $\sigma L = L$ or $S_w L$, where $w$ is a vector in $L$ orthogonal to $M$. If $\sigma L = S_w L$, then $S_w \sigma L = L$ and $S_w \sigma = \sigma$ on $M$; hence, the first assertion follows.

To show the second assertion, let $X$ be the set of all sublattices of $L$ which are isometric to $M$. Thus, if $M' \in X$, then $M' = \sigma M$ for some automorphism $\sigma$ of $FL$. We claim that $\sigma$ can be so chosen that $\sigma \in O(L)$. It is clear that $\sigma M$ satisfies (1) and (2) with respect to the lattice $\sigma L$.

Since $L \supset \sigma M$, we have $L = \sigma L$ or $S_{w'} \sigma L$ for some $w'$ in $\sigma L$ orthogonal to $\sigma M$. If $L = S_{w'} \sigma L$, then $S_{w'} \sigma \in O(L)$ and $S_{w'} \sigma M = \sigma M = M'$; hence, we have proved our claim. One sees readily that there is a bijection from $X$ onto the left cosets of $O(L)$ modulo the subgroup $H = \{ \sigma \in O(L) \mid \sigma M = M \}$.

Now the restriction map $\sigma \mapsto \sigma|_M$ defines a homomorphism from $H$ to $O(M)$ whose surjectivity follows from the first statement. The injectivity follows from the fact that if $\sigma|_M$ is trivial, then $\sigma = 1$ or $S_w$. But $S_w$ is not a unit of $L$, which is guaranteed by the property (2). Therefore, $\sigma = 1$.

Q.E.D.
§2.3 Nice Ternary Lattices

We consider in this section even positive definite ternary \( \mathbb{Z} \)-lattices of discriminant \( 2p \), where \( p \) is a prime congruent to 1 (mod 4). For a fixed such \( p \), these lattices belong to a single genus. This follows easily by a computation of Hasse symbols: if \( K \) is any such lattice, then \( K_r \) is unimodular for all \( r \neq 2, p \); hence, \( S_r(\mathbb{Q}K) = 1 \). At the prime 2, we have \( K_2 \cong \mathbb{A}(0,0) \perp \langle -2p \rangle \), so \( S_2(\mathbb{Q}K) = -1 \). Since \( K \) is positive definite, \( S_\infty(\mathbb{Q}K) = 1 \); therefore, \( S_p(\mathbb{Q}K) = -1 \) by the Hilbert Reciprocity Law.

2.3.1 Notation: Let \( G(3, 2p) \) denote the genus of even positive definite ternary lattices of discriminant \( 2p \). The subset of \( G(3, 2p) \) consisting of those lattices which represent 2 is denoted by \( G'(3, 2p) \).

Lattices in \( G(3, 2p) \), \( p \equiv 1 \) (mod 4) have already been studied by Kitaoka in \([K_1]\) and are called nice ternary lattices. Our main objective here is to show the linear independence of the theta series associated with those lattices in \( G'(3, 2p) \).

We find it useful to partition the classes in \( G(3, 2p) \) according to their roots systems. It is well known \([Kn]\) that the only indecomposable 2-lattices over \( \mathbb{Z} \) of dimension \( \leq 3 \) are \( A_1 \), \( A_2 \), and \( A_3 \).
2.3.2 Proposition: The only possible types of roots system for lattices in \( G(3, 2p) \), \( p \equiv 1 \pmod{4} \), are \( \emptyset, A_1, \) and \( A_2 \).

Proof: It suffices to show that the types \( A_1 \oplus A_1 \), \( A_1 \oplus A_1 \oplus A_1 \), \( A_1 \oplus A_2 \), \( A_3 \) are impossible.

Let \( K \in G(3, 2p) \); if \( K \) belongs to any of the above types, then \( K \) contains two orthogonal minimal vectors \( e_1, e_2 \). Since the orthogonal complement of \( e_1 \) is an even positive binary lattice \( M \) (called a nice binary lattice) with Hasse symbol \( S_2(CM) = -\left(\frac{2}{p}\right) \), \( M \) cannot contain \( e_2 \).

Q.E.D.

2.3.3 Remark: Let \( h(\sqrt{m}) \) denote the ideal class number of \( \mathbb{Q}(\sqrt{m}) \). The class number of \( G(3, 2p) \) is \( \frac{1}{2} h(\sqrt{-p}) + \frac{1}{24}(p + 3 - \frac{p}{3}) \) (\([\text{Mo}], [K_1]\)) \). The number of classes in \( G'(3, 2p) \), however, is \( h(\sqrt{-p})/2 \). To see this, we observe that by the structures of nice ternary lattices as given in \([K_1]\), there is a correspondence between the classes in \( G'(3, 2p) \) and classes of even positive binary lattices of discriminant \( 4p \) and with Hasse symbol \( -\left(\frac{2}{p}\right) \) (called nice binary lattices). This correspondence is two-to-one, except when the binary lattice is ambiguous (i.e. when the binary lattice has an improper automorphism), in which case the correspondence is one-to-one. Now from classical theory (see, for example, \([J]\) Thm 65) the number of proper classes of even positive binary lattices of discriminant \( 4p \) is just
h(\sqrt{-p})$. Since $p \equiv 1 \pmod{4}$, there are two genera of this discriminant ([J], Theorem 75). It is clear that the nice binary lattices belong to the non-principal genus. (They do not represent 2.) If $a$ is the number of ambiguous classes in the non-principal genus, then there are $(\frac{1}{2}h(\sqrt{-p}) - a)/2$ number of classes with trivial automorphism group (note that the number of proper classes is the same for each genus [J], Theorem 75). Therefore, we have a total of $\frac{1}{2}h(\sqrt{-p})$ classes in $G'(3, 2p)$. The number $a$ is 0 or 1 as $p \equiv 1$ or 5 (mod 8), respectively ([K_1], page 152).

2.3.4 Proposition: Let $K \in G(3, 2p)$. The unit group $O(K)$ is generated by symmetries of $K$ and $\pm 1$. We have $O(K) = C_2$, $C_2 \times C_2$, or $S_3 \times C_2$ as the type of $K$ is $\emptyset$, $A_1$, or $A_2$, respectively. In particular, $|O(K)| = 2$, 4, or 12, respectively.

Proof: Case (i). Type of $K$ is $\emptyset$. Then $O(K) = \{\pm 1\}$ by Lemma 2.6 [K_1].

Case (ii). Type of $K$ is $A_1$. Let $\pm e$ be the unique minimal vectors of $K$. If $\sigma \in O(K)$, then $\sigma e = \pm e$; hence, $\sigma M = M$, where $M$ is the orthogonal complement of $e$ in $K$. Since $O(M)$ is trivial (except in the ambiguous case), $\sigma$ is either $\pm 1$ or $\pm S_e$. If $M$ is unambiguous, then there exist nontrivial automorphism $\pm \sigma$ of $M$. But $\sigma \neq \pm \sigma$ on $M$ (see Lemma 1.9 [K_1]). Therefore, $\sigma$ acts trivially on $M$. Thus, $\sigma = \pm 1$ or $\pm S_e$. 
Case (iii). Type of $K$ is $A_2$. There exists a unique binary sublattice $N \cong A(2, 2)$ in $K$. Since $N$ is globally characteristic in $K$, by Proposition 2.2.8 we have $|O(K)| = |O(N)| = 12$. Clearly, $O(K)$ is generated by symmetries of $K$ and $\pm 1$. In fact, if $N = Ze_1 + Ze_2 \cong A(2, 2)$, then $S_{e_1} S_{e_2}$, $-S_{e_1}$, $-S_{e_2}$, $-S_{e_1-e_2}$ are permutations of $\{e_1, -e_2, e_2-e_1\}$ and they generate $S_3$. One sees easily that $O(K) = S_3 \times C_2$.

Q.E.D.

2.3.5 Lemma: Let $K \in G'(3, 2p)$ and $e$ be a minimal vector of $K$. Then there exists a binary sublattice $J$ in $K$ containing $e$ with $dJ = q$, where $q$ a prime $\equiv 3 \pmod{4}$ and $(\frac{q}{p}) = -1$.

Proof: Let $S = \{2, p\}$. At the prime 2, we have $K_2 = X \bigoplus \mathbb{Z}_2 x_2$, where $X$ is unimodular containing $e$ and $Q(x_2) \in 2\hat{\mathbb{Z}}_2$. $p$-adically, $K_p = Y \bigoplus \mathbb{Z}_p x_p$, where $Q(x_p) \in p\hat{\mathbb{Z}}_p$ and $Y$ is unimodular. By Lemma 1.6 [HKK], there exists a global vector $x$ in $K$ satisfying:

$x$ approximates $x_r$ for $r = 2, p$, and

$Q(x) \in \hat{\mathbb{Z}}_r$ with precisely one exception $q$,

where $Q(x) \in q\hat{\mathbb{Z}}_q$.

If we set $J = (Zx)^\perp$, then we see that $e \subseteq J$ and $dJ = q$ by integral Witt's theorem. The prime $q$ is clearly $\equiv 3 \pmod{4}$. Since the Hasse symbol for $QK$ at $p$ is $-1$, it follows from a routine calculation that $(\frac{q}{p}) = -1$.

Q.E.D.
In order to show that the lattice classes in \( \mathcal{G}'(3, 2p) \) have linearly independent theta series, we shall have to appeal to their reciprocals. Since \( \Omega = 1 \) for any \( K \in \mathcal{G}(3, 2p) \), its reciprocal \( \tilde{K} = (K^\#)^{2p} \) is a positive definite ternary \( \mathbb{Z} \)-lattice of discriminant \( 4p^2 \).

2.3.6 Remark: Assume that \( \sum c_j \Theta_{L_j}(z) = 0 \), where \( c_j \in \mathbb{C} \) is a linear relation between the theta series of some positive definite \( \mathbb{Z} \)-lattices \( L_j \) of dimension \( n \) and discriminant \( d \). Then the same relation holds for the theta series of their reciprocals, i.e. \( \sum c_j \Theta_{L_j^\#}(z) = 0 \). This follows easily by applying the transformation formula [Se]

\[
\Theta_L(t) = t^{-\frac{kn}{2}} d \Theta_{L^\#}(t^{-1}),
\]

where \( \Theta_L(t) \) is the restriction of \( \Theta_L(z) \) on the positive imaginary axis \( z = it, t > 0 \).

We need the following technical lemma.

2.3.7 Lemma: Let \( M \) be an even positive definite binary lattice of prime discriminant \( q \) (\( q \equiv 3 \) necessarily).

Then \( \Theta(M) \cong C_2, C_2 \times C_2, \) or \( S_3 \times C_2 \) as the roots system of \( M \) are \( \emptyset, A_1, \) or \( A_2 \), respectively. In particular, \( |\Theta(M)| = 2, 4, \) or \( 12 \), respectively.
Proof: It is easy to see that $M$ has one of the above roots systems. If $M$ is $A_2$, then clearly $O(M) \cong S_3 \times C_2$ (see the proof of Proposition 2.3.4). Assume, therefore, that $M$ is not $A_2$. By Minkowski's reduction theory ([J] Theorem 76), we may assume that $M \cong \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ with respect to some basis $\{x, y\}$, where $2a$ is the minimum value represented by $M$ and $0 < b < a < c$. If $a = c$, then the roots system of $M$ is $A_2$, which is impossible; hence, we have $a < c$. If $b = a$, then we have $a = b = 1$ and $c = \frac{1}{2}(q + 1)$, so the roots system of $M$ is $A_1$. Clearly, $O(M)$ is generated by $S_x$ and $t_1$. Finally, we assume that $b < a$. We claim that $t_x$ are the only vectors with length $2a$. To see this, we suppose that $v$ satisfies $Q(v) = 2a$. Then $v = ax + by$ for some $a, b \in \mathbb{Z}$. We have $Q(v) = 2a^2 + 2ba + 2c^2 = (\sqrt{a} + \sqrt{b})^2 + (2a - b)a + (2c - b)b^2$. It is easy to see that $a = \pm 1$ and $b = 0$. Similarly, $t_y$ are the only vectors with length $2c$. Therefore, $O(M)$ is trivial. Q.E.D.

2.3.8 Theorem: The theta series for lattices $K$ coming from the classes in $G'(3, 2p)$ are linearly independent.

Proof: Let $K_1, \ldots, K_h$ be a full set of non-isometric lattices in $G'(3, 2p)$. Fix a minimal vector $e_i$ in $K_i$. By Lemma 2.3.5, there exists a binary sublattice $J_i$ in $K_i$ containing $e_i$ such that its discriminant is a prime $q_i \neq 2, p$. Suppose that there are $t_i$ pairwise inequivalent binary
sublattices of $K_i$ of discriminant $q_i$, say $M_1 = J_1, M_2, \ldots, M_t$. Then by the classical correspondence (Corollary 2.1.3), the number of primitive unary sublattices of $K_i$ of discriminant $q_i$ is \( \sum_{\ell=1}^{t_i} \alpha_{\ell} \), where $\alpha_{\ell}$ is the number of binary sublattices in $K_i$ which are isometric to $M_{\ell}$. Now each $M_{\ell}$ satisfies the hypothesis of Proposition 2.2.8; hence

\[
\alpha_{\ell} = \frac{|O(K_i)|}{|O(M_{\ell})|}.
\]

It follows that

\[
a_{K_i}^\gamma(q_i) = 2 \sum_{\ell=1}^{t_i} \alpha_{\ell} = 2 \sum_{\ell=1}^{t_i} \frac{|O(K_i)|}{|O(M_{\ell})|}.
\]

By Proposition 2.3.4, we know that $|O(K_i)| \equiv 0 \, (\text{mod } 2^2)$, but $|O(K_i)| \not\equiv 0 \, (\text{mod } 2^3)$. It is clear that each $M_{\ell}$ has a trivial automorphism group, except when $M_{\ell}$ contains a minimal vector. This can only occur when $\ell = 1$. Thus, we have

\[
|O(M_{\ell})| = 2 \text{ for } \ell = 2, \ldots, t_i \text{ and } |O(M_1)| \equiv 0 \, (\text{mod } 2^2).
\]

Hence, $a_{K_i}^\gamma(q_i) \equiv 2 \, (\text{mod } 2^2)$.

If we evaluate the coefficient of $\theta_{K_j}^\gamma(z)$ at $q_i$, we obtain

\[
a_{K_j}^\gamma(q_i) = 2 \sum_{\substack{N \text{ binary} \, \text{dN} = q_i}} \frac{|O(K_j)|}{|O(N)|} \equiv 0 \, (\text{mod } 2^2),
\]
since none of the binary sublattices of $K_j$ of discriminant $q_i$ can have nontrivial automorphism group.

Now to prove the linear independence of the theta series $0_{K_j}(z)$, it suffices to prove the linear independence of $\Theta_{K_j}(z)$ by the usual transformation formula (see Remark 2.3.6). Since theta series of quadratic forms are integral modular forms, linear independence over $\mathbb{Z}$ already implies linear independence over $\mathbb{C}$. To see this, one can write each theta series as a row matrix of Fourier coefficients. If $n$ theta series are independent over $\mathbb{Z}$, then by means of elementary row operations (over $\mathbb{Q}$) one can reduce the matrix $(n \times \infty)$ of Fourier coefficients to a matrix with the property $a_{ij} = 0$ for all $j < j_i$, $a_{ij} \neq 0$, $i = 1, \ldots, n$, $j_1 < j_2 < \ldots < j_n$. But this means that the theta series are independent over $\mathbb{C}$.

Suppose there is a non-trivial linear relation

\[
\sum_{j} c_j \Theta_{K_j}(z) = 0, \quad c_j \in \mathbb{Z}.
\]

We may assume the $c_j$'s are relatively prime. Let $a_{ij}$ denote the number of representations of $q_i$ by $K_j$. By evaluating (*) at $q_i$, we obtain $\sum_{j} c_j a_{ij} = 0$. Upon considering this equation modulo $2^2$, we have $c_i$ $\equiv$ 0 (mod 2) for all $i$. This is a contradiction. Q.E.D.
2.3.9 Remark: The above proof actually yields the following classification result: let $K_1, K_2 \in G'(3, 20)$, then $K_1 \sim K_2$ if and only if $\Theta_{K_1}(z) \equiv \Theta_{K_2}(z) \pmod{4}$. In particular, if $\Theta_{K_1}(z) = \Theta_{K_2}(z)$, then $K_1 \sim K_2$.

§2.4 The Genus $G(3, 2p)$, $p \equiv 3 \pmod{4}$

In this section we study the genus of even positive definite ternary $\mathbb{Z}$-lattices of discriminant $2p$, where $p$ is a prime $\equiv 3 \pmod{4}$. Unlike the nice ternary lattices, lattices in $G(3, 2p)$ ($p \equiv 3 \pmod{4}$) may be decomposable. If $K \in G(3, 2p)$ is decomposable, then $K = \mathbb{Z}e \perp M$ for some minimal vector $e$, where $M$ is an even positive binary lattice of discriminant $p$. Conversely, if $M$ is any even positive binary lattice of discriminant $p$, then $\mathbb{Z}e \perp M$ is a decomposable lattice in $G(3, 2p)$. Hence, there is a one-to-one correspondence between the decomposable lattices in $G(3, 2p)$ and even positive binary lattices of discriminant $p$. We now consider the indecomposable lattices in $G(3, 2p)$.

2.4.1 Proposition: Let $K$ be an indecomposable lattice in $G'(3, 2p)$ and let $e$ be a minimal vector in $K$. Then $M = (\mathbb{Z}e)\perp$ is an even positive binary lattice of discriminant $4p$ satisfying (1) $nM = sM = 2\mathbb{Z}$; (2) $M$ does not represent $2$. 
Proof: By Minkowski's reduction theory ([Ca], Chapter 12), there exists a basis \{x_1, x_2, x_3\} (x_1 = e) of K such that \(B(x_1, x_2) = 1\) and \(B(x_1, x_3) = 0\). Thus, \(M = \mathbb{Z}(x_1 - 2x_2) + 2x_3\); hence, \(dM = 4p\). Since \(Q(x_1 - 2x_2) = 6 \pmod{8}\), it is clear that \(nM = sM = 2\mathbb{Z}\). If \(M\) represents 2, then by 82:15 [OM], \(M = \langle 2 \rangle \perp \langle 2p \rangle\). But this implies that \(K\) is decomposable (see Corollary 2.4.3) which contradicts our hypothesis. Q.E.D.

2.4.2 Proposition: Let \(M\) be an even positive binary \(\mathbb{Z}\)-lattice of discriminant \(4p\) (\(p \equiv 3 \pmod{4}\)) satisfying \(nM = sM = 2\mathbb{Z}\). Then there exist exactly two different even maximal ternary quadratic lattices containing \(\mathbb{Z} \perp M\) \((Q(e) = 2)\), and they both belong to \(G'(3, 2p)\).

Proof: We have \(M_2 \cong \langle 2u \rangle \perp \langle 2up \rangle\) for some \(u \in \mathbb{Z}_2^*\). If \(p \equiv 3 \pmod{8}\), then \(M_2\) is isometric to either \(\langle 2 \rangle \perp \langle 2p \rangle\) or \(\langle 2\cdot 5 \rangle \perp \langle 2\cdot 7 \rangle\). Since \(2\cdot 5 + (2\cdot 7)2^2 = 2\cdot 33 = 2\varepsilon^2, \varepsilon \in \mathbb{Z}_2^*\), we may assume in any case that \(M_2 \cong \langle 2 \rangle \perp \langle 2p \rangle\). Similarly for \(p \equiv 7 \pmod{8}\). Hence, \((\mathbb{Z} \perp M)_2 \cong \langle 2 \rangle \perp \langle 2 \rangle \perp \langle 2p \rangle\). \(\mathbb{Z} \perp M\) is not maximal, so there is an even maximal lattice \(K\) containing \(\mathbb{Z} \perp M\). It follows that \([K : \mathbb{Z} \perp M] = 2\) and \(dK = 2p\); hence, \(K \in G'(3, 2p)\). We have \(K = \mathbb{Z} \perp M + 2u\), where \(u = \frac{1}{2}(\delta_1 e + \delta_2 y + \delta_3 z)\) for some basis \(\{y, z\}\) of \(M\) and \(\delta_1 = 0\) or 1. By a change of basis if necessary, we may assume that \(\delta_1 = \delta_2 = 1, \delta_3 = 0\), or \(\delta_1 = \delta_2 = 0, \delta_3 = 1\) (for example, if both \(\delta_2 = \delta_3 = 1\), we may change \(\{y, z\}\) to
\{y + z, z\}). In the first case, \(u = \frac{1}{2}(e + y)\). The evenness of \(K\) implies that \(Q(y) \equiv 6 \pmod{8}\) and \(B(y, z) \equiv 0 \pmod{2}\).

Since \(4p = Q(y)Q(z) - B(y, z)^2\), we have \(Q(z) \equiv 0\) or \(2 \pmod{8}\). If \(Q(z) \equiv 2 \pmod{8}\), then \(Q(y + z) \equiv 0 \pmod{8}\). Without loss of generality (replacing \(z\) by \(y + z\), if necessary), we may assume that \(Q(y) \equiv 6 \pmod{8}\), \(Q(z) \equiv 0 \pmod{8}\), and \(B(y, z) \equiv 2 \pmod{4}\).

Let \(K'\) be any even maximal quadratic lattice containing \(\mathbb{Z}e \perp M\). Then \(K' = \mathbb{Z}e \perp M + Zv\), where \(v = \frac{1}{2}(\delta_1' e + \delta_2' y + \delta_3' z)\) for some \(\delta_i' (\delta_i' = 0 \text{ or } 1)\). The evenness of \(K'\) implies that either \(\delta_1' = \delta_2' = 1, \delta_3' = 0\) or \(\delta_1' = \delta_2', \delta_3' = 1\). Clearly, \(\mathbb{Z}e \perp M + Z\frac{1}{2}z\) and \(\mathbb{Z}e \perp M + Z\frac{1}{2}(e + y)\) are different.

\[\text{Q.E.D.}\]

2.4.3 **Corollary:** Let \(M\) be as in Proposition 2.4.2. Suppose further that \(M\) does not represent 2. Then there is a unique indecomposable lattice in \(G'(3, 2p)\) containing \(\mathbb{Z}e \perp M\) (\(Q(e) = 2\)). If \(M\) represents 2, then both lattices containing \(\mathbb{Z}e \perp M\) are decomposable.

**Proof:** It suffices to show that the lattice \(K = \mathbb{Z}e \perp M + Z\frac{1}{2}(e + y)\) as constructed in Proposition 2.4.2 is indecomposable. If \(K\) is decomposable, then there exists a minimal vector \(e'\) in \(K\) which splits \(K\). \(e' \neq \pm e\), since \(e\) does not split \(K\). Also, \(B(e, e') \neq \pm 1\). It follows that \(B(e, e') = 0\); hence, \(e' \notin M\). This contradicts our assumption that \(Q(M) \notin 2\). \(\text{Q.E.D.}\)
2.4.4 Lemma: Let $M$ be as in Proposition 2.4.2 such that $Q(M) \nmid 2$, and let $K$ be the unique indecomposable lattice in $G(3, 2p)$ containing $Ze \perp M$. Then any element $u$ in $K$ with $Q(u) = 2$ is mapped onto $\pm e$ by some symmetry of $K$.

Proof: If $u \in K$ satisfies $Q(u) = 2$, then $B(e, u) \neq 0$ by assumption. Hence, we have $u = \pm e$ or $B(e, u) = \pm 1$.

If $B(e, u) = 1$, then $S_{u-e}(u) = e$. If $B(e, u) = -1$, then $S_{u+e}(u) = -e$. Q.E.D.

2.4.5 Proposition: Let $M_1, M_2$ be two binary lattices as in Corollary 2.4.3 and $K_1, K_2$ be the corresponding indecomposable lattices in $G'(3, 2p)$. If $K_1 \cong K_2$, then $M_1 \cong M_2$.

Proof: Immediate by Lemma 2.4.4.

It follows from Proposition 2.4.5 that the number of indecomposable lattices in $G'(3, 2p)$ is equal to the number of even positive binary lattices of discriminant $4p$ with norm $2\mathbb{Z}$ (hence the scale is also $2\mathbb{Z}$ necessarily) and not representing $2$. We now partition $G(3, 2p)$ into classes of the same roots system type.

2.4.6 Proposition: The only possible roots system types for lattices in $G(3, 2p)$, $p \equiv 3 \pmod{4}$, are $\emptyset, A_1, A_1 \oplus A_1, A_2, \text{ and } A_1 \oplus A_2$. The latter case only occurs at $p = 3$.

Proof: Easy.
2.4.7 **Lemma:** Let $K \in G(3, 2p)$, $p \equiv 3 \pmod{4}$. If $Q(K) \neq \{\pm 1\}$, then $Q(K) \ni 2$.

**Proof:** Let $\sigma$ be a nontrivial automorphism of $K$, then $\sigma$ has one of the following matrices with respect to some basis $\{x_1, x_2, x_3\}$ of $K$ by Theorem 74.3 [CR]

\[
\text{(i)} \begin{pmatrix} 0 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{(ii)} \begin{pmatrix} 0 & -1 & 1 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\text{(iii)} \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{(iv)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.
\]

In case (i) we have $B(x_i, x_j) = \begin{pmatrix} 2a & -a & 0 \\ -a & 2a & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

Since $d_K = \det(B(x_i, x_j)) = 2p$, we have $a = 1$, $b = 2$, and $p = 3$.

In case (iv), $K$ is decomposable; hence, $2 \in Q(K)$.

In case (ii), we have

$B(x_i, x_j) = \begin{pmatrix} 2a & -a & -a \\ -a & 2a & 0 \\ -a & 0 & b \end{pmatrix}$.

Since $d_K = \det(B(x_i, x_j)) = 2p$, we have $a = 1$.

In case (iii), we have

$B(x_i, x_j) = \begin{pmatrix} 2a & -a & 0 \\ -a & b & e \\ 0 & e & c \end{pmatrix}$,

and $\det(B(x_i, x_j)) = 2p$ implies that $a = 1$ or $p$. If $a = 1$, then $2 \in Q(K)$. If $a = p$, then $d(\sum(x_1 + 2x_2) + zx_3) = 4$.

It follows that $2 \in Q(K)$. Q.E.D.
2.4.8 Lemma: Let $M$ be an even positive binary lattice of discriminant $4p$ $(p \equiv 3 \pmod{4})$ satisfying $nM = sM = 2\mathbb{Z}$. Then $O(M)$ is trivial except when $M$ is decomposable, in which case $O(M)$ is generated by $S_\epsilon, \pm 1$ ($\pm \epsilon$ the unique minimal vectors in $M$).

Proof: If $M$ is decomposable, then $M = Ze \perp Zu$, where $Q(e) = 2$ and $Q(u) = 2p$. It is clear that $O(M) = \{\pm 1, \pm S_\epsilon\}$. So assume that $M$ is indecomposable. By Minkowski's reduction theory, we may assume that $M \cong \begin{pmatrix} 2a & 2b \\ 2b & 2c \end{pmatrix}$ with respect to some basis $\{w_1, w_2\}$, where $2a$ is the minimum value represented by $M$ and $0 < 2b \leq a \leq c$. If $a = c$, then $2a = 2c = p + 1$ and $2b = p - 1$, which is impossible, since $nM = 2\mathbb{Z}$. Hence, we have $a < c$. Similarly, one can show that $2b < a$.
Using the same proof as given in Lemma 2.3.7 one shows easily that $O(M)$ is trivial. Q.E.D.

2.4.9 Proposition: Let $K \in G(3, 2p)$ $(p \equiv 3 \pmod{4})$. Then $O(K)$ is generated by symmetries of $K$ and $\pm 1$. $O(K)$ is isomorphic to $C_2, C_2 \times C_2, C_2 \times C_2 \times C_2, S_3 \times C_2$, or $S_3 \times C_2 \times C_2$ as the type of $K$ is $\emptyset, A_1, A_1 \oplus A_1, A_2$, or $A_1 \oplus A_2$, respectively. The latter occurs only when $p = 3$. In particular, $|O(K)| = 2, 4, 8, 12, 24$, accordingly.

Proof: We divide into the following cases according to the roots system type of $K$.

Case (i). type $\emptyset$. Lemma 2.4.7.
Case (ii). type $A_1$. Let $\pm e$ be the unique minimal vectors of $K$ and $M = (Ze)$. $M$ has discriminant either $p$ or $4p$ according as $K$ is decomposable or not. If $\sigma$ is an automorphism of $K$, then $\sigma e = \pm e$ and $\sigma M = M$. Since $O(M)$ is trivial, we have $\sigma = \pm 1$ or $\pm S_e$.

Case (iii). type $A_1 \oplus A_1$. By Proposition 2.4.1, $K$ is decomposable; hence, $K = Ze \perp M$ for some minimal vector $e$. Since $M$ also contains a minimal vector $e'$, it follows that $O(M) = \{\pm 1, \pm S_{e'}\}$; hence, $O(K)$ is generated by symmetries $S_e, S_{e'}, \text{ and } \pm 1$. It is clear that $|O(K)| = 8$.

Case (iv). type $A_2$. Same as Proposition 2.3.4.

Case (v). type $A_1 \oplus A_2$. Easy.

Q.E.D.

2.4.10 Remark: We observe that Lemma 2.3.5 holds also for indecomposable lattices $K$ in $G'(3, 2p)$ ($p \equiv 3 \pmod{4}$).

Namely, if $e$ is a minimal vector in $K$, then there exists a binary sublattice $J$ of discriminant $q$ and containing $e$, where $q$ is an odd prime distinct from $p$.

We shall ignore the case $p = 3$ in the following theorem since there is only one class in $G(3, 6)$ (see [BI]).

2.4.11 Theorem: The theta series $\Theta_K(z)$ for $K$ coming from the classes in $G'(3, 2p)$, $p \equiv 3 \pmod{4}$, are linearly independent.
Proof: Let $K_1, \ldots, K_n$ be a full set of non-isometric lattices in $G'(3, 2p)$. For each indecomposable $K_i$, fix a minimal vector $e_i$. By Remark 2.4.10, there exists a binary sublattice $J_i$ in $K_i$ containing $e_i$ such that $dJ_i = q_i$ for some prime $q_i \neq 2, p$. If $M_1 = J_i, M_2, \ldots, M_{t_i}$ are all the pair-wise inequivalent sublattices in $K_i$ of the same discriminant $q_i$, then by Corollary 2.1.3

$$a_{K_i}^q(q_i) = 2 \sum_{\ell=1}^{t_i} a_{\ell}$$

where $a_{\ell}$ is the number of binary sublattices of $K_i$ which are isometric to $M_{\ell}$. By Proposition 2.2.8, we have

$$a_{K_i}^q(q_i) = 2 \sum_{\ell=1}^{t_i} \frac{|O(K_i)|}{|O(M_{\ell})|}.$$ 

Since $K_i$ is indecomposable, we have $|O(K_i)| \equiv 0 \pmod{2^2}$, but $|O(K_i)| \not\equiv 0 \pmod{2^3}$ by Propositions 2.4.1 and 2.4.9. Now each $M_{\ell}$ has a trivial automorphism group, except for $\ell = 1$, where $|O(M_1)| \equiv 0 \pmod{4}$. It follows that $a_{K_i}^q(q_i) \equiv 2 \pmod{2^2}$. If $j \neq i$, then $K_j$ cannot contain a sublattice isometric to $J_i$ since $J_i$ is globally characteristic in $K_i$. Hence, every sublattice $N$ in $K_j$ of discriminant $q_i$ has a trivial automorphism group. Since $|O(K_j)| \equiv 0 \pmod{2^2}$ for all $j$ by Proposition 2.4.9, we have

$$a_{K_j}^q(q_i) = 2 \sum_{N \text{ binary}} \frac{|O(K_j)|}{|O(N)|} \equiv 0 \pmod{2^2}.$$
Suppose there is a nontrivial linear relation

\[(1) \sum_j c_j \Theta_{K_j} (z) = 0,\]

where the \(c_j\)'s are relatively prime integers. By Remark 2.3.6, the same relation also holds for their reciprocals, i.e.

\[(2) \sum_j c_j \Theta_{K_j} (z) = 0.\]

By evaluating (2) at each \(q_i\), we obtain \(\sum_j c_j a_{K_j} (q_i) = 0.\)

Upon considering this equation modulo \(2^2\), we have \(c_i \equiv 0 \pmod{2}\) for all \(i\) where \(K_i\) is indecomposable.

Now if \(K_i\) is decomposable, then we fix \(e_i\) such that \(K_i = Z e_i \perp M_i\), where \(M_i\) has discriminant \(p\). Choose a globally characteristic sublattice \(J_i\) in \(M_i\) such that \(dJ_i = 2r_i\) for some prime \(r_i \neq 2,p\). If \(M_i\) is ambiguous, we may let \(r_i = 1\). We have \(a_{M_i} (2r_i) = 2\), but \(a_{M_j} (2r_i) = 0\) for \(j \neq i\). It is easy to see that \(a_{K_i} (m) \equiv a_{M_i} (m) \pmod{2^2}\) for any \(m\) which is not \(2\) times a square, because if \(e_i + x\) satisfies \(Q(e_i + x) = m\), then all four vectors \(\perp(e_i + x), \perp(e_i - x)\) have the same length \(m\). Hence, it follows that \(a_{K_i} (2r_i) \equiv 2 \pmod{2^2}\), but \(a_{K_j} (2r_i) \equiv 0 \pmod{2^2}, j \neq i, K_j\) decomposable.

For indecomposable \(K_j\), \(a_{K_j} (2r_i) \equiv 0\) or \(2 \pmod{2^2}\). We
evaluate (1) at \(2r_i\) and consider \(\sum_j c_j a_{K_j}(2r_i) \equiv 0 \mod 2^2\). Since \(c_j\) is already even for all indecomposable \(K_j\), we have \(c_j a_{K_j}(2r_i) \equiv 0 \mod 2^2\) for such \(j\). It follows that \(c_i \equiv 0 \mod 2\) for all decomposable \(K_i\) also. This is a contradiction.

Q.E.D.

2.4.12 **Corollary**: Let \(K_1, K_2 \in G'(3, 2p)\). Then \(K_1 \cong K_2\) if and only if \(\theta_{K_1}(z) = \theta_{K_2}(z)\).

§2.5 **Even Positive Definite Ternary Lattices of Discriminant** \(2p^2\)

In this section \(p\) is an arbitrary prime \(\neq 2\). Let \(K\) be an even positive ternary lattice of discriminant \(2p^2\). Then it is clear that \(K\) is \(2\mathbb{Z}\)-maximal and \(K_p \cong \langle -2\Delta \rangle \perp \langle p \rangle \perp \langle -\Delta p \rangle\), where \(\Delta\) is a nonsquare unit at \(p\), for if \(K_p\) were not \(2\mathbb{Z}_p\)-maximal, then by 81:14 [OM] we can construct an even positive ternary lattice over \(\mathbb{Z}\) of discriminant 2. Such a lattice does not exist (see [BI]). A routine computation shows that \(S_p(\mathbb{Q}K) = 1\). This implies that \(S_2(\mathbb{Q}K) = 1\) also by the Hilbert Reciprocity Law, since \(S_r(\mathbb{Q}K) = 1\) at all other primes \(r\). It follows that all such lattices belong to the same genus \(G(3, 2p^2)\). We will show in this section that there is a one-to-one correspondence between the classes in \(G(3, 2p^2)\) and those in \(G(3, 2p)\) by means of lattice theoretic methods. This recovers a result of Ponomarev [P3]. We will also show that the
classes of lattices in $G(3, 2p^2)$ with nontrivial automorphism group have linearly independent theta series.

2.5.1 Proposition: Let $K \in G(3, 2p^2)$. Then $K$ contains a unique sublattice $K'$ such that $[K : K'] = p$ and $n(K, p') = pZ_p$.

Proof: Put $K_p = \mathbb{Z}_p x_1 \perp \mathbb{Z}_p x_2 \perp \mathbb{Z}_p x_3$, where $Q(x_1) = -2\Delta$, $Q(x_2) = p$, and $Q(x_3) = -\Delta p$. By the lattice theory, there is a lattice $K'$ such that

$$K'_r = \begin{cases} K'_r, & r \neq p, \\ \mathbb{Z}_p(p x_1) \perp \mathbb{Z}_p x_2 \perp \mathbb{Z}_p x_3, & r = p. \end{cases}$$

Clearly, $K$ contains $K'$ with $[K : K'] = p$ and $n(K, p') = pZ_p$.

Let $J$ be any lattice contained in $K$ which satisfies the same properties as $K'$. Then $J_r = K_r = K'_r$ for all $r \neq p$. It suffices to show that $J_p = K'_p$. Let $u$ be any vector in $J_p$. Then $u = \alpha x_1 + \beta x_2 + \gamma x_3$ for some $\alpha, \beta, \gamma \in \mathbb{Z}_p$. Since $Q(u) = -2\Delta \alpha^2 + \beta^2 p - \Delta \gamma^2 p \in pZ_p$, we have $\alpha \in pZ_p$; hence, $u \in K'_p$. It follows that $J_p \subseteq K'_p$; hence, $J_p = K'_p$. Q.E.D.

If we now scale the lattice $K'$ by $p^{-1}$, say $K = K'_p p^{-1}$, we then obtain a lattice in $G(3, 2p)$. Conversely, given a lattice $K$ in $G(3, 2p)$, we let $K' = K^p$. Then $K'$ has discriminant $2p^4$. Since $K \cong <1> \perp <-\Delta> \perp <-2\Delta p>$, we have $K'_p \cong <p> \perp <-\Delta p> \perp <-2\Delta p^2>$. 
2.5.2 Proposition: Let \( K \in G(3, 2p) \) and \( K' = K^p \), then there exists exactly one lattice \( K \) containing \( K' \) such that \( [K : K'] = p \); hence, \( K \in G(3, 2p^2) \).

Proof: Put \( K'_p = \mathbb{Z}_p \cdot x_1 \perp \mathbb{Z}_p \cdot x_2 \perp \mathbb{Z}_p \cdot x_3 \), where \( Q(x_1) = p \), \( Q(x_2) = -\Delta p \), and \( Q(x_3) = -2\Delta p^2 \). By the lattice theory, there is a lattice \( K \) such that

\[
K_r = \begin{cases} 
K'_r, & r \neq p, \\
\mathbb{Z}_p \cdot x_1 \perp \mathbb{Z}_p \cdot x_2 \perp \mathbb{Z}_p \cdot (\frac{1}{p} \cdot x_3), & r = p.
\end{cases}
\]

Clearly, \( K \) contains \( K' \) and \( [K : K'] = p \). Let \( J \) be any lattice containing \( K' \) with \([J : K'] = p \), then \( J_r = K'_r = K_r \) for \( r \neq p \). It suffices to show that \( J_p = K_p \). Since \([J_p : K_p'] = p \), we have \( J_p = K'_p + \mathbb{Z}_p \cdot \frac{1}{p} (\alpha x_1 + \beta x_2 + \gamma x_3) \) for some \( \alpha, \beta, \gamma \in \mathbb{Z}_p \). We may assume that \( \alpha, \beta, \gamma \) are either units or zero. If both \( \alpha \) and \( \beta \) are units, then \( \alpha^2 - \beta^2 \Delta \in \mathbb{Z}_p \). This implies that \( \Delta \) is a square by the local square theorem, which is absurd. If either \( \alpha \) or \( \beta \) is 0, then both of them must be 0. Therefore, \( J_p = K_p \). Q.E.D.

2.5.3 Corollary: The mapping \( K \mapsto K = K^p \) induces a one-to-one correspondence between classes in \( G(3, 2p^2) \) and classes in \( G(3, 2p) \).

2.5.4 Remark: Let \( K, K', K \) be as above. It is easy to see from the proof of Proposition 2.5.1 that any vector \( u \) in \( K \) of length \( Q(u) \) which is divisible by \( p \) actually lies in \( K' \). In particular, any vector \( u \) in \( K \) with \( Q(u) = 2p \) lies in \( K' \).
hence, \( a_{K}(2p) = a_{K'}(2p) \). But it is clear that \( a_{K'}(2p) = a_{K}(2) \), since \( K \) is just \( K' \) scaled by \( p^{-1} \). Thus, we have \( a_{K}(2p) = a_{K}(2) \).

2.5.5 **Proposition:** Let \( K, K', K \) be as in Corollary 2.5.3, then we have \( O(K) = O(K') = O(K) \).

**Proof:** Since \( K' \) and \( K \) have the same underlying lattice structure, it is clear that \( O(K') = O(K) \). To see that \( O(K) = O(K') \), let \( \sigma \in O(K) \). Since both \( \sigma K' \) and \( K' \) are sublattices of index \( p \) in \( K \) and their norms are contained in \( p\mathbb{Z} \), it follows that \( \sigma K' = K' \) by Proposition 2.5.1. Conversely, if \( \sigma \in O(K') \), then \( \sigma K \) contains \( K' \) with \( [\sigma K : K'] = p \). Hence, \( \sigma K = K \) by Proposition 2.5.2. Q.E.D.

2.5.6 **Remark:** It is now clear from Proposition 2.5.5 that \( O(K) \) is generated by symmetries and \( \pm 1 \). A typical symmetry of \( O(K) \) is of the form \( S_{u} \), where \( u \) is a vector in \( K \) of length \( 2p \). By the results we obtained in Sections 2.3 and 2.4 for \( O(K) \), we see that \( |O(K)| = 2, 4, 8, 12 \), as \( a_{K}(2p) = 0, 2, 4, 6 \), respectively. We exclude the case \( p = 3 \).

2.5.7 **Notation:** Let \( G'(2, 2p^{2}) \) denote the subset of \( G(3, 2p^{2}) \) consisting of those lattices with a nontrivial automorphism group. One sees readily by Remark 2.3.6 that \( G'(3, 2p^{2}) \) is just the set of those lattices in \( G(3, 2p^{2}) \) which represent \( 2p \). Note that this notation is in coherence of our previous notation for \( G'(3, 2p) \).
We now investigate the binary sublattices of $K$ of discriminant $p^2q$, where $q$ is an odd prime distinct from $p$. Let $K$ be the lattice in $G(3, 2p)$ corresponding to $K$.

Clearly, if $K$ contains a binary sublattice $M$ of discriminant $q$, then $K$ contains the lattice $M' = M^p$, which has discriminant $p^2q$. Conversely, we have

2.5.8 Proposition: Let $K, K', K$ be as in Corollary 2.5.3. Suppose $K$ contains a binary sublattice $M$ of discriminant $p^2q$, then $M \subseteq K'$; hence, $K$ contains the lattice $M = M^{p-1}$.

Proof: We first show that $M_p$ is $p$-modular. Suppose this is not the case, then $M_p = \mathbb{Z}_p u \perp \mathbb{Z}_p v$, where $Q(u)$ is a unit at $p$ and $Q(v) \in p^2\mathbb{Z}_p$. It follows that $u$ splits $K_p$; hence, $K_p = \mathbb{Z}_p u \perp N$ for some binary $N$. It is easy to see that $N$ is $p$-modular and $Q_p N$ is anisotropic. By 63:15 [OM] $N$ represents only elements of odd order. This is absurd, since $v \in N$. Hence, $M_p$ is $p$-modular. Now we have $mM \subseteq 2p\mathbb{Z}$; hence, by Remark 2.5.4, $M \subseteq K'$. Q.E.D.

2.5.9 Remark: We now see that the binary sublattices of $K$ of discriminant $p^2q$ are just those in $K$ of discriminant $q$ scaled by $p$. In particular, if $K \in G'(3, 2p^2)$, then there exists a $q \neq 2, p$ such that $K$ contains a binary $M$ of discriminant $p^2q$ which represents $2p$.

2.5.10 Remark: Let $K, K$ be as in Corollary 2.5.3. It is easy to see that $K$ is decomposable if and only if $K$ is
decomposable. In this case, we have $p \equiv 3 \pmod{4}$ and $\mathbb{K} = \mathbb{Z} u \perp M$ for some $u$ with $Q(u) = 2p$ and binary $M$ of discriminant $p$.

2.5.11 Theorem: The theta series $\Theta_{\mathbb{K}}(z)$ for $\mathbb{K}$ coming from the classes in $G'(3, 2p^2)$ are linearly independent.

Proof: The proof proceeds in exactly the same way as that of Theorem 2.3.8 for $p \equiv 1 \pmod{4}$ and that of Theorem 2.4.11 for $p \equiv 3 \pmod{4}$ with minor changes. For each indecomposable $\mathbb{K}_i$ we choose a binary $M_i$ of discriminant $p^2q_i$ which contains a vector of length $2p$. If there is a nontrivial linear relation $\sum c_j \Theta_{\mathbb{K}_j}(z) = 0$, where the $c_j$'s are relatively prime, we evaluate at $p^2q_i$. Now $\frac{1}{2}a_{\mathbb{K}_j}(p^2q_i)$, being equal to the number of binary sublattices in $\mathbb{K}_j$ of discriminant $p^2q_i$, is exactly equal to the number of binary sublattices in $\mathbb{K}_j$ of discriminant $q_i$. Therefore, it follows that

$$a_{\mathbb{K}_j}(p^2q_i) \equiv 0 \pmod{2^2} \text{ for } j \neq i,$$

$$a_{\mathbb{K}_i}(p^2q_i) \equiv 2 \pmod{2^2}.$$

The rest of the proof is clear. Q.E.D.

2.5.12 Corollary: Let $\mathbb{K}_1$ and $\mathbb{K}_2$ be any lattices in $G'(3, 2p^2)$, then $\mathbb{K}_1 \cong \mathbb{K}_2$ if and only if $\Theta_{\mathbb{K}_1}(z) = \Theta_{\mathbb{K}_2}(z)$. 
§2.6 Nice Quaternary Lattices

We now turn to study the theta series of quaternary lattices. Let $L$ be an even positive definite quaternary $\mathbb{Z}$-lattice of prime discriminant $p$, where $p \equiv 1 \pmod{4}$. Then we have

$$L_2 \cong \begin{cases} A(0,0) \oplus A(0,0) & \text{if } p \equiv 1 \pmod{8}, \\
A(0,0) \oplus A(2,2) & \text{if } p \equiv 5 \pmod{8}; \end{cases}$$

hence, the Hasse symbol $S_2(\mathcal{O}L) = -\left(\frac{2}{p}\right)$. It is clear that $S_r(\mathcal{O}L) = 1$ for all $r \neq 2, p$ (including $\infty$); therefore, $S_p(\mathcal{O}L) = -\left(\frac{2}{p}\right)$, also by the Hilbert Reciprocity Law. Since all even positive quaternary lattices of discriminant $p$ are $2\mathbb{Z}$-maximal, they belong to the same genus $G(4, p)$. We denote also by $G'(4, p)$ the subset of $G(4, p)$ consisting of those lattices which represent 2. Lattices in $G(4, p)$ (also called nice quaternary lattices) have been studied in the works of Kitaoka, Ponomarev, and Hashimoto (see [K], [P], and [H]). For later references we summarize here some of their results.

Let $\mathcal{O}$ denote the quaternion algebra of discriminant $p^2$ over the field of rational numbers $\mathbb{Q}$. Let $F = \mathbb{Q}(\sqrt{p})$ and $\mathcal{O}$ be the ring of integers of $F$. Put $\mathcal{O}_F = \mathcal{O} \otimes \mathbb{Q} F$. Let $\alpha \mapsto \alpha^*$ be the canonical involution of $\mathcal{O}_F$ and $N: \mathcal{O}_F \to F$ the reduced norm, $N(\alpha) = \alpha\alpha^*$. The conjugation $x \mapsto \overline{x}$ of $F$ extends uniquely to a $\mathbb{Q}$-automorphism $\alpha \mapsto \overline{\alpha}$ of $\mathcal{O}_F$ having as its ring of fixed elements. Let $n_{F/\mathbb{Q}}$ be the norm map of
$F, n_{F/Q}(x) = x\bar{x}$ for $x \in F$. Let $L \in G(4, p)$ and $V$ be its underlying vector space. Then $V$ is isometric to the quaternary space $W = \{ \alpha \in \mathcal{A}_F \mid \alpha^* = \alpha \}$, the quadratic form on $W$ being the restriction of the norm form $2N$ ([P₁], Proposition 2(a)). We shall assume that $V = W$ and $Q = 2N$ in the following.

2.6.1 Proposition ([P₂], page 137): If $\Omega$ is a symmetric maximal order of $\mathcal{A}_F$, then $L = \Omega \cap V$ is a lattice in $G'(4, p)$. Conversely, if $L \in G'(4, p)$ is a lattice on $V$, then there exists a symmetric normal ideal $\hat{L}$ of $\mathcal{A}_F$ such that $L = \hat{L} \cap V$. $\hat{L}$ is similar to a symmetric maximal order. Moreover, let $\Omega_1$ and $\Omega_2$ be symmetric maximal orders of $\mathcal{A}_F$ and $L_i = \Omega_i \cap V$, $i = 1, 2$. We have $L_1 \cong L_2$ if and only if $\Omega_1 \cong \Omega_2$.

2.6.2 Proposition ([H], page 171): Let $L \in G(4, p)$. Then the roots system of $L$ can be $\emptyset$, $A_1$, $A_1 \oplus A_1$, $A_2$, $A_1 \oplus A_2$, $A_3$, or $A_4$ as the number of minimal vectors $\alpha_L(2)$ is $0, 2, 4, 6, 8, 12, \text{or } 20$, respectively. The latter case occurs only when $p = 5$.

2.6.3 Proposition ([K₁], page 152; [H], pages 170-171): Let $L \in G(4, p)$ with $p > 5$. Then the unit group $O(L)$ of $L$ is generated by symmetries. $O(L)$ is isomorphic to $C_2^2$, $C_2 \times C_2$, $C_2 \times C_2 \times C_2$, $S_3 \times C_2$, $S_3 \times C_2 \times C_2$, or $S_4 \times C_2$ as the type of $L$ is $\emptyset$, $A_1$, $A_1 \oplus A_1$, $A_2$, $A_1 \oplus A_2$, or $A_3$. 
respectively. In particular, \(|O(L)| = 2, 4, 8, 12, 24, \) or 48, respectively.

2.6.4 Proposition ([H], pages 168-171): The class number of \(G'(4, p), p > 5,\) is \(\left\lfloor \frac{p + 19}{24} \right\rfloor.\) The number of classes of type \(A_1 \oplus A_2\) is 0 or 1 as \(p \equiv 1 \) or 2 (mod 3), whereas the number of classes of type \(A_3\) is 0 or 1 as \(p \equiv 1 \) or 5 (mod 8).

Since the class number of \(G(4, 5)\) is 1, we shall henceforth assume that \(p > 5.\) There exists a certain correspondence between the lattices in \(G'(4, p)\) and those in \(G(3, 2p)\).

2.6.5 Proposition ([K_1], pages 147-148): Let \(L \in G'(4, p)\) and \(e\) be a minimal vector in \(L.\) Then \(K = (Ze)^{-1}\) is a lattice in \(G(3, 2p).\) Conversely, if \(K \in G(3, 2p),\) then there exists a unique nice quaternary lattice containing \(Ze \perp K\) (\(Q(e) = 2).\)

2.6.6 Proposition ([K_1], page 150): The map \(K \mapsto L \supseteq Ze \perp K\) as given in Proposition 2.6.5 induces a correspondence between the classes in \(G(3, 2p)\) and the classes in \(G'(4, p).\) This correspondence is one-to-one on the classes of \(K\) of type \(\emptyset.\) It is two-to-one on the classes of \(K\) of type \(A_1\) or \(A_2\) with an exceptional case: if the associated nice binary sublattice of \(K\) is ambiguous, then the correspondence is one-to-one. (This occurs when \(p \equiv 5 \) (mod 8).)
<table>
<thead>
<tr>
<th>Type of $K$</th>
<th>Type of $L$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\emptyset$</td>
<td>$\begin{cases} A_1 \ A_2 \end{cases}$</td>
</tr>
<tr>
<td>$\leftarrow$ 1-1 $\rightarrow$</td>
<td></td>
</tr>
<tr>
<td>$A_1$</td>
<td>$A_1 \oplus A_1$</td>
</tr>
<tr>
<td>$\leftarrow$ 2-1 $\rightarrow$</td>
<td></td>
</tr>
<tr>
<td>$A_1$</td>
<td>$A_3$ when $p \equiv 5 \pmod{8}$</td>
</tr>
<tr>
<td>$\leftarrow$ 1-1 $\rightarrow$</td>
<td></td>
</tr>
<tr>
<td>$A_1$</td>
<td>$A_2$ when $p \equiv 2 \pmod{3}$</td>
</tr>
</tbody>
</table>

2.6.7 Lemma: Let $L \in G'(4, p)$, then there exists a ternary sublattice $J$ in $L$ containing the roots system of $L$ with $dJ = 2q$ for some prime $q$ distinct from $p$, $(q \mid p) = -1$. In particular, if $L$ has the type $A_1 \oplus A_2$ or $A_3$, we can take $J \cong A_1 \oplus A_2$ or $A_3$, respectively. In the latter case, the prime $q = 2$.

Proof: Let $R_L$ be the roots system of $L$, then there exists a ternary 2-adic lattice $X \supset R_L$ such that $L_2 \supset X \perp \mathbb{Z}_2x_2$, where $dx \in \mathbb{Z}_2^3$ and $Q(x_2) \in \mathbb{Z}_2^3$. For if $R_L$ if of type $A_1$, then $K = R_L^\perp$ is a nice ternary lattice of discriminant $2p$ and $K_2 \cong A(2a, 2a) \perp <2up>$, where $a = 0$ or 1 and $u = -1$ or 3, respectively. Hence, we may take $X = R_L \perp N$, $N \cong A(2a, 2a)$. Similarly for $R_L$ of type $A_1 \oplus A_1$ (just choose $N$ to contain a minimal vector). If $R_L \cong A_2$, then $R_L$ splits $L_2$, so $L_2 \supset R_L \perp \mathbb{Z}_2x_2 \perp \mathbb{Z}_2x_2$ for some $x_2, x_2$ with $Q(x_2), Q(x_2) \in \mathbb{Z}_2^3$. In this case we choose $X = R_L \perp \mathbb{Z}_2x_2$. At the prime $p$, it is easy to see that $L_p = Y \perp \mathbb{Z}_p x_p$ for some ternary $p$-adic.
lattice $Y \supset R_L$ with $dY \in \mathbb{Z}_p^2$ and $Q(x_p)$ is a $p$-adic unit. By Lemma 1.6 [HKK] we can find a global vector $x$ in $L$ such that $x$ approximates $x_2$ and $x_p$ at the primes 2 and $p$, respectively, and $Q(x)$ is locally a unit everywhere with the exception of the primes 2 and $q$ for some $q \neq 2$ or $p$. We have $Q(x) \in \mathbb{Z}_2$ and $Q(x) \in \mathbb{Z}_q$. Put $J = (Zx)^i$. Then we see that $J \supset R_L$ and $dJ = 2q$ by the integral Witt's theorem [T]. Since the Hasse symbol for $QL$ at 2 and $p$ are both equal to $-(\frac{2}{p})$, it follows from a routine calculation that $(\frac{q}{p}) = -1$. Q.E.D.

2.6.8 Theorem: The theta series $\Theta_L(z)$ for lattices $L$ coming from the classes in $G'(4, p)$ which have roots system of type (a) $R_L \supset A_1 \oplus A_1$, or (b) $R_L \supset A_2$ are linearly independent.

Proof: Let $L_1, \ldots, L_h$ be a full set of nonisometric lattices in $G'(4, p)$ of fixed types (a) or (b). For each $i$, choose a ternary sublattice $J_i$ in $L_i$ of discriminant $2q_i$ according to Lemma 2.6.7. In particular, $J_i$ contains the roots system $R_i$ of $L_i$. Let $M_1 = J_i$, $M_2, \ldots, M_{t_i}$ be all pairwise inequivalent ternary sublattices of $L_i$ of discriminant $2q_i$. Then by the classical correspondence, we have

$$a_{\frac{L_i}{2q_i}}(2q_i) = \sum_{\ell=1}^{t_i} a_{\ell}.$$
where \( \alpha \) is the number of ternary sublattices in \( L \), isometric to \( M \). Since each \( M \) satisfies the hypothesis of Proposition 2.2.8, we have \( \alpha = \frac{|O(L)|}{|O(M)|} \); hence

\[
a_{L_i}^{2q_i} = 2 \sum_{\ell=1}^{t_i} \frac{|O(L_i)|}{|O(M_{\ell})|}.
\]

Now we have

\[
|O(L_i)| \equiv \begin{cases} 
0 \pmod{2^3} & \text{if } R_i \supset A_1 \oplus A_1 \\
0 \pmod{3} & \text{if } R_i \supset A_2.
\end{cases}
\]

Since \( M = J_i \) contains the roots system \( R_i \) of \( L_i \), it follows that \( |O(M_i)| = |O(L_i)| \) by Proposition 2.3.4 and Proposition 2.4.9. If \( \ell \neq 1 \), we have \( |O(M_{\ell})| = 2 \) or \( 4 \). It follows, therefore, that

\[
a_{L_i}^{2q_i} \equiv \begin{cases} 
2 \pmod{2^2} & \text{if } R_i \supset A_1 \oplus A_1 \\
2 \pmod{3} & \text{if } R_i \supset A_2.
\end{cases}
\]

If \( j \neq i \), then \( L_j \) cannot contain a sublattice isometric to \( J_i \), since \( J_i \) is globally characteristic in \( L_i \). Hence, if \( N \) is any ternary sublattice of \( L_j \) of discriminant \( 2q_j \), its unit group has order either 2 or 4. (Since \( A_1 \oplus A_2 \) and \( A_3 \) are the only even ternary lattices of discriminant 6 and 4, if \( L_j \) has roots system \( R_j \neq A_1 \oplus A_2, A_3 \), respectively, then \( L_j \) does not contain any such ternary lattice.) Thus, we have

\[
a_{L_j}^{2q_j} = 2 \sum_{N \text{ ternary}} \frac{|O(L_j)|}{|O(N)|} \equiv \begin{cases} 
0 \pmod{2^2} & \text{if } R_j \supset A_1 \oplus A_1 \\
0 \pmod{3} & \text{if } R_j \supset A_2.
\end{cases}
\]
Suppose there is a nontrivial linear relation

\[(*) \quad \sum_j c_j \Theta_{l_j} (z) = 0,\]

where the \(c_j\)'s are relatively prime integers. By evaluating \((*)\) at each \(2q_i\), we obtain \(\sum_j c_j a_{l_j}^{(2q_i)} = 0\). We take this equation modulo \(2^2\) for \(R_i \supset A_1 \oplus A_2\) and modulo \(3\) for \(R_i \supset A_2\).

This, however, implies that \(c_i \equiv 0 \pmod{2}\) for all \(i\) in the first case and \(c_i \equiv 0 \pmod{3}\) for all \(i\) in the latter case, which is a contradiction.

Q.E.D.

2.6.9 Remark: The number of classes in \(G'(4, p)\) having roots systems of type \(A_1 \oplus A_1\) or \(A_2\) is essentially \(h(\sqrt{-p})/4\) or \(h(\sqrt{-3p})/4\), respectively. See [H], page 171.

2.6.10 Remark: An alternate approach is given in [HH] to obtain independence of the theta series considered in Theorem 2.6.8 (see also Chapter III). In fact, we have shown that for each \(L_i\) with roots system \(R_i\) containing \(A_1 \oplus A_1\) there exists a prime \(q_i\) (\(\neq 2\) or \(p\)) such that \(a_{L_i}^{(2q_i)} \equiv 2 \pmod{4}\), but \(a_{L_i}^{(2q_i)} \equiv 0 \pmod{4}\) for \(j \neq i\). (Similarly, for \(L_i \supset A_2\) there is a prime \(r_i\) (\(\neq 2\) or \(p\)) such that \(a_{L_i}^{(2r_i)} \neq 0 \pmod{3}\) but \(a_{L_j}^{(2r_i)} \equiv 0 \pmod{3}\) for \(j \neq i\).) Hence, it follows that for any two lattices \(L_1\) and \(L_2\) in \(G'(4, p)\) having roots systems both containing \(A_1 \oplus A_1\) or \(A_2\), then \(L_1 \cong L_2\) if and only if \(\Theta_{L_1} (z) \equiv \Theta_{L_2} (z) \pmod{4}\) or \(\pmod{3}\), respectively.
The ordinary theta series coming from all the classes in $G'(4, p)$ are, in general, not linearly independent. See the example in the Appendix. However, the degree two theta series of these lattices do form an independent set.

2.6.11 Remark: Let $f$ be a (Siegel) modular form of degree 2. Then there is attached a modular form $\phi f$ of degree 1 by the process

$$\phi f(z) = \lim_{t \to \infty} f \left( \begin{array}{cc} z & 0 \\ 0 & \text{i}t \end{array} \right), \quad z \in H,$$

where $H$ is the upper half complex plane ( [M$_2$], page 187). $\phi$ is called the Siegel operator. It can be shown ( [M$_2$], page 188) that if $f$ has the fourier series

$$f(z) = \sum_{T \geq 0} a(T) e^{2\pi i \text{tr}(TZ)},$$

where $T$ is a 2 by 2 integral symmetric matrix, then

$$\phi f(z) = \sum_{T \geq 0} a \left( \begin{array}{cc} t & 0 \\ 0 & 0 \end{array} \right) e^{2\pi i \text{tz}} \quad \text{(the terms where } T \neq \begin{array}{cc} t & 0 \\ 0 & 0 \end{array} \text{ vanish under the limit).}$$

In particular, if $f$ is a theta series of degree two $\Theta_L^{(2)}(z)$, where $L$ is even positive definite, then $\phi f(z) = \Theta_L(z)$, the ordinary theta series associated with $L$, since $a_L \left( \begin{array}{cc} t & 0 \\ 0 & 0 \end{array} \right) = a_L(t)$.

2.6.12 Theorem: The theta series $\Theta_L^{(2)}(z)$ of degree 2 for lattices $L$ coming from the classes in $G'(4, p)$ are linearly independent.
Proof: Let \( L_1, \ldots, L_h \) be a full set of non-isometric lattices in \( G'(4, p) \). We first consider those lattices \( L_i \) which have roots system of type \( A_1 \) or \( A_2 \). For each \( i \), fix a minimal vector \( e_i \) in \( L_i \) and let \( K_i = (Ze_i)^1 \). Using Lemma 1.6 [HKK], we may construct a binary sublattice \( M_i \) in \( K_i \) of discriminant \( q_i \). Since \( M_i \) is nonambiguous, as \( K_i \) does not represent 2, the unit group \( O(M_i) \) is trivial. If \( N \) is any other binary sublattice of \( L_i \) isometric to \( M_i \) and \( N \not\subset K_i \), we will show that \( S_{e_i}N \) is also not contained in \( K_i \) and \( S_{e_i}N \neq N \).

To see this, let \( v \in N \) be a vector not contained in \( K_i \). Then \( v = \frac{a}{2}(e_i + x) + y \) for some \( x \) and \( y \in K_i \). We have \( a \neq 0 \). Since \( S_{e_i}v = \frac{a}{2}(-e_i + x) + y \), \( S_{e_i} \) does not act trivially on \( N \); hence, \( S_{e_i}N \neq N \). It is also clear that \( S_{e_i}N \not\subset K_i \). It follows that the number \( a_{L_i}(M_i) \) of representations of \( M_i \) by \( L_i \) is congruent to \( a_{K_i}(M_i) \pmod{2^2} \). Since \( M_i \) is globally characteristic in \( K_i \), we have, by Proposition 2.2.8,

\[
a_{K_i}(M_i) = \frac{|O(K_i)|}{|O(M_i)|} \times |O(M_i)| = |O(K_i)|.
\]

Now \( K_i \) does not represent 2; hence, \( |O(K_i)| = 2 \) by Proposition 2.3.4, and so

\[
a_{L_i}(M_i) \equiv 2 \pmod{2^2}.
\]
If $j \neq i$, then the above argument shows that

$$a_{L_j}^i(M_i) = a_{K_j}^i(M_i) \equiv 0 \pmod{2^2},$$

since $K_j$ cannot represent $M_i$. Suppose there exists an integral linear relation

$$\sum_j c_j \Theta_{L_j}(z) = 0. \tag{1}$$

We may assume that the greatest common divisor of the coefficients is 1. If we evaluate (1) at $M_i$, we obtain

$$\sum_j c_j a_{L_j}^i(M_i) = 0.$$

This implies that $c_i \equiv 0 \pmod{2}$ for those $L_i$ of type $A_1$ or $A_2$ by taking the equation modulo $2^2$. We now apply the Siegel operator to (1). By Remark 2.6.11, this gives a linear relation between the degree one theta series

$$\sum_j c_j \Theta_{L_j}(z) = 0. \tag{2}$$

Again, by applying the usual transformation formula, we obtain

$$\sum_j c_j \Theta_{L_j}(z) = 0.$$

We can repeat our argument for theta series of degree one on those lattices $L_i$ of roots systems $R_i \supset A_1 \oplus A_1$ and choose some prime $r_i$ such that

$$a_{L_j}^{2r_i}(2r_i) \equiv 2 \pmod{2^2}, \quad R_i \supset A_1 \oplus A_1$$
(See the proof of Theorem 2.6.8.). If $R_j$ has type $A_1$ or $A_2$, then we have

$$a_{L_j}^\nu(2r_i) \equiv 0 \pmod{2^2}, \quad j \neq i, \quad R_j \supset A_1 \oplus A_1.$$ 

which is irrelevant, since their corresponding coefficients are already even. Therefore, if we evaluate (2) at each $2r_i$, we have

$$\sum_j c_j a_{L_j}^\nu(2r_i) = 0.$$ 

Upon consideration modulo $2^2$, we see that $c_i \equiv 0 \pmod{2^2}$ also for $L_i$ which have roots system $R_i \supset A_1 \oplus A_1$. But this is a contradiction. Q.E.D.

2.6.13 Remark: A direct approach is adopted in [HH] by choosing a binary sublattice $J_i$ in each $L_i$ such that $a_{L_j}^\nu(J_i) \equiv 0 \pmod{2^{n_j}}$ for $j \neq i$. $(2^{n_j} \text{ is the exact power of } 2 \text{ dividing } |O(L_j)|.)$ But $a_{L_i}^\nu(J_i) \equiv 0 \pmod{2^{n_i-1}}, a_{L_i}^\nu(J_i) \equiv 0 \pmod{2^{n_i}}$. In particular, this yields the following classification result:

Let $L_1$ and $L_2$ be any two lattices in $G'(4, p)$, then $L_1 \cong L_2$ if and only if $\Theta_{L_1}^{(2)}(Z) \equiv \Theta_{L_2}^{(2)}(Z) \pmod{8}$. To see this, we first observe that $a_{L}^\nu(\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}) = 2, 4, 6, 8, \text{ or } 12$ as the type of $L$ is $A_1, A_1 \oplus A_1, A_2, A_1 \oplus A_2, \text{ or } A_3$, respectively. Hence, we have $\Theta_{L_1}^{(2)}(Z) \not\equiv \Theta_{L_2}^{(2)}(Z) \pmod{8}$ if $L_1$ and $L_2$ are not of the same type, except perhaps when
L_1 is of type A_1 \oplus A_1 and L_2 is of type A_3. In this case, we have \( a_{L_1}(J_1) \equiv 4 \pmod{8} \), but \( a_{L_2}(J_1) \equiv 0 \pmod{8} \).

If \( L_1 \) and \( L_2 \) are of the same type, we have

\[
\begin{align*}
& a_{L_1}(J_1) \equiv 2 \text{ or } 6 \pmod{8}, \quad a_{L_2}(J_1) \equiv 4 \pmod{8}, \\
& L_1 \text{ and } L_2 \text{ are both type } A_1 \text{ or } A_2; \\
& a_{L_1}(J_1) \equiv 4 \pmod{8}, \quad a_{L_2}(J_1) \equiv 0 \pmod{8}, \\
& L_1 \text{ and } L_2 \text{ are both type } A_1 \oplus A_2.
\end{align*}
\]

In any case, \( \Theta_{L_1}^{(2)}(z) \neq \Theta_{L_2}^{(2)}(z) \pmod{8} \).

§2.7 Even Positive Definite Quaternary Lattices of Discriminant \( p^2 \)

Let \( p \) be a prime \( \equiv 1 \pmod{4} \). Let \( L \) be an even positive definite quaternary lattice of discriminant \( p^2 \). Then \( L_2 \cong A(0, 0) \perp A(0, 0) \) and \( L \) is maximal, since there is no even unimodular lattice of dimension 4. It is easy to see that \( S_2(\mathbb{Q}L) = S_p(\mathbb{Q}L) = -1 \) and \( S_r(\mathbb{Q}L) = 1 \) for all \( r \) (including \( \infty \)) \( \neq 2 \) or \( p \); hence, there is exactly one genus \( G(4, p^2) \) of such quaternary lattices. Denote by \( G'(4, p^2) \) the subset of \( G(4, p^2) \) consisting of those lattices which represent 2 or \( 2p \). We consider in this section their associated theta series of degree one and degree two. Suppose that \( L \in G(4, p^2) \) contains a minimal vector \( e \), then it is clear that \( K = (2e)^\perp \) is a lattice in \( G(3, 2p^2) \).
2.7.1 Proposition: Let $\mathcal{K}$ be a lattice in $G(3, 2p^2)$, then there is a unique maximal even positive quaternary lattice $\mathcal{L}$ in $G(4, p^2)$ containing $Ze \perp \mathcal{K}$, where $e$ is a minimal vector.

Proof: Since $\mathcal{K}_2 \cong A(0, 0) \perp <2p^2>$, we have $Z_2 e \perp \mathcal{K}_2 \cong <2> \perp <2p^2> \perp A(0, 0)$. It suffices to show that there is only one even unimodular lattice containing $Z_2 e \perp \mathcal{K}_2$. Let $\{e, x, y, z\}$ be a basis of $Z_2 e \perp \mathcal{K}_2$ such that $Q(x) = -2p^2$ and $Z_2 y + Z_2 z \cong A(0, 0)$. Since $Z_2 e \perp Z_2 x$ is isotropic, there exists a unimodular lattice $\mathcal{N} \cong A(0, 0)$ containing $Z_2 e \perp Z_2 x$. Let $\{u, v\}$ be a basis of $\mathcal{N}$ such that $Q(u) = Q(v) = 0$ and $B(u, v) = 1$. Let $e = \epsilon u + \delta v$, where $\epsilon, \delta \in \hat{Z}_2$. If $\mathcal{M}$ is any unimodular lattice containing $Z_2 e \perp Z_2 x$, then $\mathcal{M} = Z_2 e + Z_2 (\alpha u + \beta v)$ for some $\alpha, \beta \in \hat{Z}_2$.

Since $Q(\alpha u + \beta v) = 2\alpha \beta \in 2\hat{Z}_2$ and $B(e, \alpha u + \beta v) = \epsilon \beta + \delta \alpha \in \hat{Z}_2$, it follows that both $\alpha$ and $\beta$ are contained in $\hat{Z}_2$.

Hence, $\mathcal{M} = \mathcal{N}$. Q.E.D.

2.7.2 Lemma: Let $\mathcal{K}$ be a lattice in $G(3, 2p^2)$, then $2t^2 \notin Q(\mathcal{K})$ for any $t > 0$, $(t, p) = 1$. In particular, $2 \notin Q(\mathcal{K})$.

Proof: Suppose that there exists a $v \in \mathcal{K}$ with $Q(v) = 2t^2$, then $\mathcal{N} = (Zv)^\perp$ is an even positive definite binary lattice satisfying $\mathcal{K}_p = Z_p v \perp N_p$. Since $dN_p$ is a square in $Z_p$ and $p \equiv 1 \pmod{4}$, $N_p$ is isotropic; hence, $\mathcal{K}_p$ is not maximal, which is impossible. Q.E.D.
2.7.3 Proposition: Let \( K \in G(3, 2p^2) \) and \( L \) be the unique lattice in \( G(4, p^2) \) containing \( \mathbb{Z}e \perp K \) (\( Q(e) = 2 \)), then any minimal vector \( u \) in \( L \) is mapped onto \( \pm e \) by some symmetry of \( L \).

Proof: The proof is easy; see Lemma 2.4.4.

2.7.4 Proposition: Let \( K_1 \) and \( K_2 \) be two lattices in \( G(3, 2p^2) \) and \( L_1 \) and \( L_2 \) be the corresponding lattices in \( G(4, p^2) \). If \( L_1 \cong L_2 \), then \( K_1 \cong K_2 \).

Proof: Immediate by Proposition 2.7.3.

It follows from Proposition 2.7.4 that the map \( K \mapsto L \supset \mathbb{Z}e \perp K \) induces a one-to-one correspondence between the classes of lattices in \( G(3, 2p^2) \) and those classes in \( G(4, p^2) \) which represent 2. It is well known ([Kn]) that the only indecomposable 2-lattices of dimension \( \leq 4 \) over \( \mathbb{Z} \) are \( A_1, A_2, A_3, A_4, \) or \( D_4 \). Since \( L \) cannot contain two orthogonal minimal vectors by Lemma 2.7.2, the only possible roots system for any \( L \in G(4, p^2) \) are \( \emptyset, A_1, \) and \( A_2 \).

2.7.5 Proposition: Let \( K \) be a lattice in \( G(3, 2p^2) \) and \( L \) be the unique lattice in \( G(4, p^2) \) containing \( \mathbb{Z}e \perp K \). Let \( K \) be the lattice in \( G(3, 2p) \) uniquely associated with \( K \) according to Corollary 2.5.3. Then \( L \) has roots system of type \( A_2 \) if and only if \( K \) has roots system of type \( A_2 \).
Proof: We first observe that \( L \) has type \( A_2 \) if and only if \( K \) contains a vector \( x \) satisfying \( Q(x) = 6 \) and \( B(x, K) \subseteq 2\mathbb{Z} \). For if \( L \) has type \( A_2 \), then there exists a basis \( \{e, f, u, v\} \) of \( \mathbb{L} \) such that \( Q(e) = Q(f) = 2, B(e, f) = 1, \) and \( B(e, u) = B(e, v) = 0 \) by the Minkowski reduction theory. We may take \( x = e - 2f \). Conversely, if there exists such a vector \( x \) in \( K \), then it is easy to see that \( L = (Ze \perp K) + \mathbb{Z}(e + x) \). Since \( 2e + 2\mathbb{Z}(e + x) = \left( \begin{array}{cc} 2 & 1 \\ 2 & 1 \end{array} \right) \), \( L \) has type \( A_2 \). We now show that \( K \) has type \( A_2 \) if and only if \( K \) contains a vector \( x \) satisfying \( Q(x) = 6 \) and \( B(x, K) \subseteq 2\mathbb{Z} \).

(\( \Rightarrow \)). If \( K \) has type \( A_2 \), then \( K \supset N \) for some ternary sublattice \( N \cong \left( \begin{array}{c} 2 \\ 1 \\ 2 \end{array} \right) \perp \langle 6p \rangle \). Since \( K \supset K^p \supset N^p \), where \( N^p \cong \left( \begin{array}{c} 2p \\ p \\ 2p \end{array} \right) \perp \langle 6p^2 \rangle \), it follows that \( K \supset J \perp \mathbb{Z}x \) for some \( J \cong \left( \begin{array}{c} 2p \\ p \\ 2p \end{array} \right) \) and \( Q(x) = 6 \). There exists \( v \in J \) such that \( K = (J \perp \mathbb{Z}x) + \mathbb{Z}^{\frac{1}{3}}(x + v) \). Clearly, \( x \) satisfies \( B(x, K) \subseteq 2\mathbb{Z} \).

(\( \Leftarrow \)). Suppose that \( K \) contains a vector \( x \) satisfying \( Q(x) = 6 \) and \( B(x, K) \subseteq 2\mathbb{Z} \). Then \( K \supset \mathbb{Z}x \perp J \) for some binary lattice \( J \) of discriminant \( 3p^2 \). Note that \( x \) splits \( K \) locally, since \( B(x, K^p) \subseteq 2\mathbb{Z} \). Now \( J_p \) is \( p \)-modular and anisotropic; hence, \( \mathbb{Z}px \perp J \) is contained in a sublattice of index \( p \) in \( K \). Therefore, \( \mathbb{Z}px \perp J \subseteq K^p \) and \( J^{-1} \subseteq K \). Since there is only one even positive binary lattice of discriminant \( 3 \), \( J^{-1} \cong \left( \begin{array}{c} 2 \\ 1 \\ 2 \end{array} \right) \); hence, \( K \) has type \( A_2 \).

Q.E.D.
2.7.6 Definition: Let $K$, $L$, and $K$ be as in the hypothesis of Proposition 2.7.5. $L$ is said to have type $A_1^0$ if the roots system of $L$ is $A_1$ and the roots system of $K$ is $\emptyset$. $L$ has type $A_1^1$ if the roots systems of $L$ and $K$ are both $A_1$.

2.7.7 Lemma: Let $L$ be a lattice in $G(4, p^2)$. Suppose that $L$ contains vectors $e$ and $u$ such that $Q(e) = 2$ and $Q(u) = 2p$, then $e \perp u$.

Proof: Let $K$ be the orthogonal complement of $u$ in $L$. Suppose that $e \notin K$, then $e \notin u \perp K$, also. It follows that $e = \frac{1}{2}(au + v)$ for some $a \neq 0$ and $v \in K$. Since $Q(\frac{1}{2}(au + v)) = \frac{1}{2}(2pa^2 + Q(v)) > 2 = Q(e)$, we obtain a contradiction.

Q.E.D.

2.7.8 Remark: Let $K$, $L$, and $K$ be as in the hypothesis of Proposition 2.7.5. It follows from Lemma 2.7.7 that the number of representations of $2p$ by $L$ is $a_L(2p) = a_K(2p)$. But $a_K(2p) = a_K(2)$ by Remark 2.5.4; hence, $a_L(2p) = 0$, 2, or 6 as $L$ has type $A_1^0$, $A_1^1$, or $A_2$, respectively. We say that the type of $L$ is $A_2^2$ if it has roots system $A_2$.

Combining Corollary 2.5.3, Proposition 2.6.6, and Proposition 2.7.4 we obtain:

2.7.9 Proposition: The map $L \mapsto K \mapsto L$ induces a correspondence between the classes of lattices in $G(4, p^2)$ which represent 2 and those classes in $G'(4, p)$. This correspondence is one-to-one on the classes of $L$ of type $A_1^0$. 
It is two-to-one on the classes of $L$ of type $A_1^1$ or $A_2^2$ with the exceptional case when $K$ contains an ambiguous nice binary lattice, which occurs only when $p \equiv 5 \pmod{8}$.

<table>
<thead>
<tr>
<th>Type of $L$</th>
<th>Type of $L$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_1^0$</td>
<td>$A_1^1$</td>
</tr>
<tr>
<td>$A_1$</td>
<td>$A_2$</td>
</tr>
<tr>
<td>$A_1^1$</td>
<td>$A_1 \oplus A_1$</td>
</tr>
<tr>
<td>$A_1$</td>
<td>$A_3$       when $p \equiv 5 \pmod{8}$</td>
</tr>
<tr>
<td>$A_1^1$, $A_2^2$</td>
<td>$A_1 \oplus A_2$ when $p \equiv 2 \pmod{3}$</td>
</tr>
</tbody>
</table>

**2.7.10 Remark**: The above correspondence has been obtained by Ponomarev in [P$_2$] through the arithmetic of quaternion algebra. Following the notation of Section 2.6, his result is a consequence of a correspondence between the maximal orders of $G$ and the symmetric maximal orders of $G_p$ and a correspondence between symmetric maximal orders of $G_p$ and the lattices in $G'(4, p)$ (see Proposition 2.6.1).

Let $L \in G(4, p^2)$. Recall that the reciprocal of $L$ is the dual $L^\#$ scaled by the factor $a/\Omega$, where $a = dL$ and $\Omega$ is the greatest common divisor of the entries in the adjoint matrix to $A$, where $A$ is the matrix of $L$ with respect to some basis. Since $L$ is unimodular for all $r \neq p$, we have $\Omega \in \mathbb{Z}_r$ for all such $r$. At the prime $p$, $L_p \cong <1> \perp <-\Delta> \perp <p> \perp <-\Delta p>$
since $Q_{L}$ is anisotropic; so $L^{\#} \cong \langle 1 \rangle \perp \langle -\Delta \rangle \perp \langle p^{-1} \rangle \perp \langle -\Delta p^{-1} \rangle$. It follows that $\Omega = p$ and $\hat{\mathcal{L}} = (L^{\#})^{\hat{p}}$. Hence, $d_{\hat{\mathcal{L}}} = p^{2}$ and $\hat{\mathcal{L}} \in G(4, p^{2})$.

2.7.11 Lemma: Let $L$ be a lattice in $G(4, p^{2})$, then $Q(L) \equiv 2$ if and only if $Q(\hat{L}) \equiv 2p$. Furthermore, we have $a_{L}(2) = a_{\hat{L}}(2p)$.

Proof: ($\Rightarrow$). Let $e$ be a minimal vector in $L$ and $K = (Ze)^{\perp}$. Then $K$ is a primitive sublattice of $L$ of discriminant $2p^{2}$. By the classical correspondence between primitive sublattices of codimension 1 in $L$ and primitive vectors in $\hat{L}$ (Proposition 2.1.1), we see that $\hat{L}$ represents $2p^{2}/\Omega = 2p$.

($\Leftarrow$). Let $u$ be a vector in $L$ with $Q(u) = 2p$, then $K = (Zu)^{\perp}$ is a nice ternary lattice of discriminant $2p$.

To see this, we consider $K$ locally at the primes 2 and $p$.

At the prime 2, there exists a vector $v$ in $L_{2}$ such that $B(u, v) = 1$; hence, $\hat{L}_{2} = (Z_{2}u + Z_{2}v) \perp N$ for some binary unimodular lattice $N$. Clearly, $d_{K_{2}} = 2Z_{2}$. $p$-adically, we have $d_{K_{p}} \equiv \langle 1 \rangle \perp \langle -\Delta \rangle \perp \langle p \rangle \perp \langle -\Delta p \rangle$ with respect to some basis $\{x, y, z, w\}$. There exist scalars $\alpha, \beta, \gamma, \delta \in Z_{p}$ such that $u = \alpha x + \beta y + \gamma z + \delta w$. Since $Q(u) = 2p$, we have $\alpha, \beta \in pZ_{p}$, so $Z_{p}u$ splits $\hat{L}_{p}$ by 82:15 [OM]. It follows that $d_{K_{p}} \in pZ_{p}$. Therefore, $d_{K} = 2p$. Again by the classical correspondence (Proposition 2.1.1), we have $\hat{L}$ represents $2p/\Omega = 2$. Since $\hat{L} \cong L$ by Remark 2.1.4, our proof is completed.
To prove the last statement, we observe that if \( K \) is any ternary sublattice of \( \mathbb{L} \) of discriminant \( 2p^2 \), then there is a minimal vector \( e \) in \( \mathbb{L} \) such that \( e \perp K \). This is clear, since, locally at \( p \), we have \( K_p \cong \langle -2A \rangle \perp \langle p \rangle \perp \langle -\Delta p \rangle \); hence, the \( p \)-modular component of \( K_p \) splits \( \mathbb{L}_p \). Therefore, if \( e \) is a primitive vector in the orthogonal complement of \( K \), then \( Q(e) \in \mathbb{Z}_p \). Thus, \( e \) is a minimal vector. Now we have the number of ternary sublattices of \( \mathbb{L} \) of discriminant \( 2p^2 \) exactly equals the number of pairs \( \{t^\perp e\} \) of minimal vectors in \( \mathbb{L} \). On the other hand, this number also equals the number of pairs \( \{t^\perp u\} \) of vectors in \( \mathbb{L} \) with \( Q(u) = 2p \) by the classical correspondence. Hence, \( a_{\mathbb{L}}(2) = a_{\mathbb{L}}(2p) \).

Q.E.D.

2.7.12 Definition: Let \( \mathbb{L} \in G(4, p^2) \). We say that \( \mathbb{L} \) has type \( A_0^1 \) if \( a_{\mathbb{L}}(2) = 0 \) but \( a_{\mathbb{L}}(2p) = 2 \). \( \mathbb{L} \) has type \( \emptyset \) if \( \mathbb{L} \) represents neither 2 nor 2p.

2.7.13 Remark: It follows immediately from Lemma 2.7.11 that \( \mathbb{L} \) has type \( A_0^1, A_1^1, \) or \( A_2^1 \) if and only if \( \mathbb{L}' \) has type \( A_0^1, A_1^1, \) or \( A_2^1 \), respectively. In the last two cases, we have \( \mathbb{L} \cong \mathbb{L}' \), for if \( \mathbb{L} \) has type \( A_2^2 \), then \( a_{\mathbb{L}}(2p) = 6 \) by Remark 2.7.8; hence \( a_{\mathbb{L}}(2) = 6 \). This means that \( \mathbb{L}' \) has type \( A_2^2 \), but there is only one lattice-class of type \( A_2^2 \) in \( G(4, p^2) \); therefore, \( \mathbb{L} \cong \mathbb{L}' \).

If the type of \( \mathbb{L} \) is \( A_1^1 \), then one can also show that \( \mathbb{L} \cong \mathbb{L}' \) (see \( [p_2] \), page 136).
In summary, we have partitioned the classes in $G(4, p^2)$ in the following way: $G'(4, p^2)$ consists of lattices which are of type $A_0^0, A_0^1, A_1^1, \text{ or } A_2^2$. Lattices not in $G'(4, p^2)$ have type $\emptyset$. We now investigate their groups of automorphisms.

2.7.14 Proposition: Let $L \in G'(4, p^2)$, then $O(L)$ is generated by symmetries of $L$ and $\pm 1$. We have $O(L) \cong C_2 \times C_2, C_2 \times C_2 \times C_2, \text{ or } (S_3 \times S_3) \times C_2$ as the type of $L$ is $A_0^0, A_0^1, A_1^1, \text{ or } A_2^2, \text{ respectively (hence, } |O(L)| = 4, 8, \text{ or } 72, \text{ respectively}).$

Proof: Case (i). $L$ has type $A_0^0$. $L$ contains a minimal vector $e$. Since $K = (Ze)\perp$ does not represent $2p$, $|O(K)| = 2$ by Remark 2.5.6. Hence, if $\sigma$ is any automorphism of $L$, then $\sigma e = \pm e$ and $\sigma$ acts trivially on $K$. Clearly, $O(L)$ is generated by $S_e$ and $\pm 1$.

Case (ii). $L$ has type $A_0^1$. $L$ contains a vector $u$ with $Q(u) = 2p$. Since $u$ splits $L$ locally, we have $2B(u, L) \subseteq \mathbb{Z}$; hence, $\pm S_u \in O(L)$. Put $K = (Zu)\perp$, then $K$ is a nice ternary lattice with no minimal vectors, so $O(K)$ is trivial. If $\sigma$ is an automorphism of $L$, then $\sigma u = \pm u$ and $\sigma$ acts trivially on $K$. Thus, $O(L)$ is generated by $S_u$ and $\pm 1$.

Case (iii). $L$ has type $A_1^1$. $L$ contains a minimal vector $e$ such that $K = (Ze)\perp$ contains a vector $u$ of length $2p$. By Remark 2.5.6, $|O(K)| = 4$. In fact, $O(K)$ is generated by $S_u$ and $\pm 1$ (see Proposition 2.5.5). Clearly, $S_u$ is an automorphism of $L$. If $\sigma \in O(L)$, then $\sigma e = \pm e$ and
\(\mathfrak{K} = \mathfrak{K}\). It follows that \(O(L)\) is generated by \(S_{e}, S_{u}\), and \(\dagger 1\).

Case (iv). \(L\) has type \(A_{2}^{2}\). \(L \supseteq (Ze_{1} + Ze_{2}) \perp (Zu_{1} + Zu_{2})\), where \(Ze_{1} + Ze_{2} \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\) and \(Zu_{1} + Zu_{2} \cong \begin{pmatrix} 2p & p \\ p & 2p \end{pmatrix}\).

Clearly, \(S_{e_{1}}, S_{e_{2}}, S_{e_{1} - e_{2}}, S_{u_{1}}, S_{u_{2}}, S_{u_{1} - u_{2}}\) are all automorphisms of \(L\). Together with \(\dagger 1\), they generate a group of order 72. On the other hand, if \(\sigma\) is any automorphism of \(L\), then \(\sigma\) takes \(e_{1}\) onto \(e_{1}, e_{2}\), or \(\dagger(e_{1} - e_{2})\) and \(\sigma(Ze_{1}) \perp (Ze_{1}) \perp (Ze_{2}) \perp Z(e_{1} - e_{2}) \perp\), respectively. It is clear that \(O(L)\) is generated by \(S_{e_{1}}, S_{e_{2}}, S_{e_{1} - e_{2}}, S_{u_{1}}, S_{u_{2}}, S_{u_{1} - u_{2}}\) and \(\dagger 1\).

Q.E.D.

2.7.15 Remark: If \(L \in G(4, p^{2})\) has type \(\emptyset\), then \(O(L)\) is trivial. See [P2], page 138. It follows that \(G'(4, p^{2})\) are precisely those lattices in \(G(4, p^{2})\) which have improper automorphism.

Since the classes of lattices in \(G'(4, p)\) having roots systems containing \(A_{1} \oplus A_{1}\) have linearly independent ordinary theta series, it is natural to ask whether their counterparts in \(G'(4, p^{2})\) also have linearly independent series. We saw in Proposition 2.7.9 that each \(L\) in \(G'(4, p)\) with \(R_{L} \supseteq A_{1} \oplus A_{1}\) corresponds to two lattices in \(G'(4, p^{2})\) of type \(A_{1}^{1}\) or \(A_{2}^{2}\). Let \(L\) be any such lattice in \(G'(4, p^{2})\), then \(L\) contains a minimal vector \(e\) and a vector \(u\) of length \(2p\), where \(e \perp u\). We have \(L \supseteq Ze \perp Zu \perp M\) for some nice
binary lattice $M$. Choose a vector $v$ in $M$ such that $Q(v) = 2q$, $q$ a prime (use Lemma 1.6, [HKK]). Let $Zf$ be the orthogonal complement of $v$ in $M$, then $Q(f) = 2pq$ and $\mathbb{L} \subset Zv \perp Zu \perp Zv \perp Zf$.

2.7.16 Lemma: There exist exactly four lattices in $G(4, p^2)$ containing $Zv \perp Zu \perp Zv \perp Zf$ ($Q(e) = 2$, $Q(u) = 2p$, $Q(v) = 2q$, $Q(f) = 2pq$) which are partitioned into two disjoint sets of isometric lattices (each set contains two lattices). Lattices from one set are not isometric to those from the other, except in the case when an even maximal lattice containing $Zv \perp Zf$ is ambiguous.

Proof: There exist two nice binary lattices containing $Zv \perp Zf$, namely $M_1$ and $M_2$ defined by

$$ (M_1)_r = \begin{cases} Z_r v \perp Z_f, & r \neq q \\ (Z_q v \perp Z_f) + \frac{1}{q} (v + a f), & a \in \mathbb{Z}_q \end{cases} $$

$$ (M_2)_r = \begin{cases} Z_r v \perp Z_f, & r \neq q \\ (Z_q v \perp Z_f) + \frac{1}{q} (v - a f), & a \in \mathbb{Z}_q \end{cases} $$

$M_1$ and $M_2$ are permuted by $S_f$; hence, they are isometric.

For each $i = 1, 2$, there exist two nice ternary lattices $K_i$ and $K_i'$ containing $Zv \perp M_i$. $K_i$ and $K_i'$ are not isometric, except when $M_i$ is ambiguous (Lemma 1.9, [K1]). Moreover, we may assume that $K_1 \cong K_2$ and $K_1' \cong K_2'$. By a similar argument as that given in Proposition 2.7.1, one can show
that for each $K_i$ (or $K_i'$) there is a unique even maximal lattice in $G(4, p^2)$ containing $Zu \perp K_i$ (or $Zu \perp K_i'$), say $\mathcal{L}_i$ or $\mathcal{L}_i'$, $i = 1, 2$. Again by a proof similar to that of Proposition 2.7.4, we see that $\mathcal{L}_1$ and $\mathcal{L}_1'$ are not isometric, except in the ambiguous case, but $\mathcal{L}_1 \cong \mathcal{L}_2$ and $\mathcal{L}_1' \cong \mathcal{L}_2'$.

Q.E.D.

It follows from Lemma 2.7.16 that $Ze \perp Zu \perp Zv \perp Zf$ classifies the lattices of type $A_1^1$ or $A_2^2$ up to "twins." Let $G_o$ be a subset of $G'(4, p^2)$ consisting of exactly one member from each twin set $\{[\mathcal{L}, \mathcal{L}']\}$. (The choice of $G_o$ is arbitrary.) We assume that all lattices in $G_o$ have type $A_1^1$.

2.7.17 Theorem: The theta series $\Theta_{\mathcal{L}}(z)$ for lattices $\mathcal{L}$ coming from the classes of $G_o$ are linearly independent.

Proof: Let $\mathcal{L}_1, \ldots, \mathcal{L}_{h_o}$ be a full set of non-isometric lattices in $G_o$. For each $i$ fix a minimal vector $e_i$ and a vector $u_i$ with $Q(u_i) = 2p$. Choose $v_i$ in $M_i = (Ze_i \perp Zu_i) \perp$ such that $Q(v_i) = 2q_i$, where $q_i$ is a prime $\neq 2$ or $p$. Consider an isometric embedding $\phi$ of $v_i$ into $\mathcal{L}_j$. If $\phi(v_i)$ is orthogonal to both $e_j$ and $u_j$, then by Lemma 2.7.16 and the choice of $G_o$, we have $\mathcal{L}_i \cong \mathcal{L}_j$, and so $i = j$. Now $O(\mathcal{L}_j)$ acts on the set of isometric embeddings of $v_i$ into $\mathcal{L}_j$; hence, the size of the orbit of $\phi$ is $|O(\mathcal{L}_j)| / |H_\phi|$, where $H_\phi$ is the stabilizer of $\phi$. Let $\sigma$ be an involution in $H_\phi$. Since $\mathcal{L}_j$ has type $A_1^1$ and $O(\mathcal{L}_j)$ is generated by symmetries,
\( \sigma \) is either a pure symmetry or a product of two symmetries. The latter case can occur only when \( i = j \) and \( \phi \) lies in the orbit of the inclusion map. When \( i \neq j \), the only possible involution in \( \Phi \) is a pure symmetry.

Summarizing the above, we have the number of elements in an \( |O(L_j)| \)-orbit is divisible by \( 2^2 \), except for the orbit of the inclusion map, where this number is divisible exactly by 2. Suppose \( a_{ij} \) is the number of isometric embeddings of \( v_i \) into \( L_j \), then we have

\[
a_{ij} = \sum_{\phi \text{ in distinct orbit}} \begin{vmatrix} O(L_i) \end{vmatrix} \frac{|O(L_j)|}{|H_\phi|} \equiv 0 \pmod{2^2}
\]

if \( i \neq j \);

\[
a_{ii} = \frac{|O(L_j)|}{|H_\alpha|} + \sum_{\phi \not\in \alpha} \frac{|O(L_i)|}{|H_\phi|} \equiv 0 \pmod{2},
\]

but \( a_{ii} \neq 0 \pmod{2^2} \), where \( \alpha \) is the inclusion map.

Suppose there is a nontrivial integral linear relation

\[
\sum_{j} c_j \Omega_{L_j}(z) = 0,
\]

where the \( c_j \)'s are relatively prime. Then by evaluating it at \( 2q_i \) for each \( i \), we obtain \( \sum_{j} c_j a_{ij} = 0 \). This implies that \( c_i \equiv 0 \pmod{2} \) by considering the equation modulo \( 2^2 \), which is a contradiction. Q.E.D.
2.7.18 Remark: It follows easily from the proof of Theorem 2.7.17 that for any two lattices \( L_1 \) and \( L_2 \) in \( G_\mathbb{Q} \), \( L_1 \cong L_2 \) if and only if \( \Theta_{L_1}(z) \equiv \Theta_{L_2}(z) \mod 2^2 \). In particular, if \( \Theta_{L_1}(z) = \Theta_{L_2}(z) \), then \( L_1 \cong L_2 \).

2.7.19 Remark: The number of classes in \( G_\mathbb{Q} \) is one-half the total number of classes of type \( \mathbb{A}_1 \), which is essentially \( h(\sqrt{-p})/4 \) (see Proposition 2.7.9 and Remark 2.6.9).

2.7.20 Lemma: Let \( K \) be a lattice in \( G(3, 2p^2) \), then there is a binary sublattice \( J \) of \( K \) such that \( dJ = pq \) for some prime \( q \neq 2 \) or \( p \). Moreover, if \( K \) contains a vector \( u \) of length \( 2p \), then \( J \) can be chosen to contain \( u \).

Proof: Suppose that \( K \) contains \( u \), \( Q(u) = 2p \). At the prime 2, we have \( K_2 = N \perp \mathbb{Z}_2 x_2 \) for some unimodular binary lattice \( N \) containing \( u \). This is clear, since \( u \) does not split \( K_2 \). \( p \)-adically, we have \( K_p = R \perp \mathbb{Z}_p x_p \) for some \( R \) containing \( u \) and \( Q(x_p) \in p^2 \mathbb{Z} \). By Lemma 1.6 [HKK], we can find a vector \( x \) in \( K \) such that \( x \) is close to \( x_2 \) and \( x_p \) and, for \( h \neq 2 \) or \( p \), \( Q(x) \in \mathbb{Z}_h \), with the exception of one prime \( q \), where \( Q(x) \in q \mathbb{Z}_q \). Let \( J \) be the orthogonal complement of \( x \) in \( K \), then \( J \) contains \( u \) and \( dJ = pq \). Q.E.D.

We now consider the theta series of degree 2 associated with lattices in \( G'(4, p^2) \). Let \( L_1, \ldots, L_h \) be a full set of non-isometric lattices in \( G'(4, p^2) \). For each \( i \), choose a
binary sublattice $J_i$ in $\mathbb{L}_i$ according to its type:

(i) $\mathbb{L}_i$ type $A_2^2$. Let $J_i$ be the unique sublattice of $\mathbb{L}_i$ which is isometric to $A(2, 2)$.

(ii) $\mathbb{L}_i$ type $A_0^1$. Let $\mathbb{L}_i$ be a minimal vector $u_i$ such that $Q(u_i) = 2p$ and let $K_i = (Zu_i)^\perp$. Since $K_i$ is a nice ternary lattice, we can choose $J_i \subset K_i$ of discriminant $q_i$ for some prime $q_i \neq 2$ or $p$.

(iii) $\mathbb{L}_i$ type $A_0^0$ or $A_1^1$. Let $e_i$ be a minimal vector and $K_i = (Ze_i)^\perp$. By Lemma 2.7.19, we can choose $J_i \subset K_i$ of discriminant $pq_i$, where $q_i$ is a prime $\neq 2$ or $p$. $J_i$ contains a vector of length $2p$ if $\mathbb{L}_i$ has type $A_1^1$.

2.7.21 Lemma: Suppose $\mathbb{L}_i$ has type $A_0^1$ and $\phi: J_i \rightarrow \mathbb{L}_j$ is an isometric embedding of $J_i$ into $\mathbb{L}_j$. Then we have

(1) $\phi(J_i)$ is not orthogonal to any minimal vector in $\mathbb{L}_j$;

(2) If $\phi(J_i)^\perp u$ for some vector $u$ of length $2p$, then $\mathbb{L}_i \cong \mathbb{L}_j$; hence, $i = j$.

Proof: (1) If $\phi(J_i)^\perp e$ for some minimal vector $e$ in $\mathbb{L}_j$, then $(\mathbb{L}_j)^p = \phi(J_i)^\perp Z_p e \perp Z_p w$ for some $w$ with $Q(w) \in p^2 Z_p$. This is impossible, since $(\mathbb{L}_j)^p$ is maximal.

(2) It suffices to show that $Z_{U_i} \perp J_i$ is a characteristic sublattice of $\mathbb{L}_i$. But this is clear, since $J_i$ is characteristic in $K_i = (Zu_i)^\perp$. Q.E.D.
2.7.22 Lemma: Let \( L_i \) be of type \( A \) and \( \phi: J_i \rightarrow L_j \) an isometric embedding of \( J_i \) into \( L_j \). If \( \phi(J_i) \perp e \) for some minimal vector \( e \) in \( L_j \), then \( L_i \cong L_j \); hence, \( i = j \).

Proof: It is enough to show that \( Z_{e_i} \perp J_i \) is characteristic in \( L_i \). At the prime \( p \), \( Z_{e_i} \perp (J_i)_p \) splits \( L_p \) (see the proof of Lemma 2.7.11); hence, it is locally characteristic. At the prime 2, \( (L_i)_2 = (J_i)_2 \perp N \) for some unimodular \( N \) containing \( e_i \). Clearly, \( Z_{2e_i} \) characterizes \( N \) (see the proof of Proposition 2.7.1); hence, \( (J_i)_2 \perp Z_{2e_i} \) is locally characteristic. The lemma follows by Theorem 2.2.6.

Q.E.D.

2.7.23 Lemma: Suppose that \( L_i \) has type \( A \) and \( \phi: J_i \rightarrow L_j \) is an isometric embedding of \( J_i \) into \( L_j \). Then we have

1. \( \phi(J_i) \) is not orthogonal to any vector \( u \) of length \( 2p \) in \( L_j \);

2. If \( \phi(J_i) \perp e \) for some minimal vector \( e \) in \( L_j \),
then \( L_i \cong L_j \); hence, \( i = j \).

Proof: (1) \( \phi(J_i) \) already contains a vector of length \( 2p \); hence, it is impossible to have \( \phi(J_i) \perp u \) for some \( u \) with \( Q(u) = 2p \).

(2) Done in Lemma 2.7.22.

Q.E.D.

2.7.24 Theorem: The theta series \( \Theta_L^{(2)}(Z) \) of degree two for lattices \( L \) coming from the classes of even positive definite
quaternary lattices of discriminant $p^2$ having an improper automorphism group are linearly independent.

**Proof:** Let $\mathbb{L}_i$ and $J_i$ be as before, $i = 1, \ldots, h$. Let $a_{ij}$ be the number of isometric embeddings of $J_i$ into $\mathbb{L}_j$. Let $2^j$ be the exact power of 2 in $|O(\mathbb{L}_j)|$. We want to measure the size of an $O(\mathbb{L}_j)$-orbit. Consider the following cases:

Case (i). $\mathbb{L}_i$ has type $A_1^1$, then no symmetries of $O(\mathbb{L}_j)$ can fix $\phi(J_i)$ by Lemma 2.7.21, unless $i = j$ and $\phi$ is in the orbit of the inclusion map, where $H_\phi = \{1, S_{ui}\}$; hence

$$\frac{|O(\mathbb{L}_j)|}{|H_\phi|} = \begin{cases} 2^j - 1 & \text{if } i = j \text{ and } \phi \in \text{orbit of inclusion} \\ 2^j & \text{otherwise.} \end{cases}$$

By Proposition 2.7.14 we have

$$a_{ij} = \sum_{\phi \text{ in distinct orbit}} \frac{|O(\mathbb{L}_j)|}{|H_\phi|} \equiv 0 \pmod{2^2}$$

if $i \neq j$.

$$a_{ii} = \frac{|O(\mathbb{L}_j)|}{|H_\alpha|} + \sum_{\phi \notin \text{orbit } \alpha} \frac{|O(\mathbb{L}_j)|}{|H_\phi|} \equiv 2 \pmod{2^2}$$

but $a_{ii} \not\equiv 0 \pmod{2^2}$, where $\alpha$ is the inclusion map.

Case (iii). $\mathbb{L}_i$ has type $A_0^1$. If $\mathbb{L}_j$ has type $A_2$ or $A_1^1$, then by Lemma 2.7.22, no symmetries of the kind $S_e$ for some minimal vector $e$ can fix $\phi(J_i)$, and at most one symmetry $S_{ui}$.
\( Q(u) = 2p \), can fix \( \phi(J) \). Similarly for \( L_j \) of type \( A_0^1 \).

If \( L_j \) has type \( A_1^0 \), then \( H_\phi \) is trivial, except when \( i = j \), and \( \phi \) lies in the orbit of the inclusion map, in which case we have \( H_\phi = \{1, S_{e_1}\} \). We have

\[
\frac{|O(L_j)|}{|H_\phi|} = \begin{cases} 
2^n & \text{if } L_j \text{ has type } A_2^2, A_1^1, \text{ or } A_0^1 \\
2^n_{ij} & \text{if } L_j \text{ has type } A_1^0, i \neq j, \text{ or } i = j, \text{ but } \phi \notin \text{orbit of inclusion} \\
2^n_{ij} & \text{if } i = j \text{ and } \phi \in \text{orbit of inclusion.} 
\end{cases}
\]

Hence

\[
a_{ij} \equiv 0 \pmod{2^2} \text{ for } i \neq j \text{ and } L_j \text{ of type } A_2^2, A_1^1, A_0^1; \\
a_{ij} \equiv 0 \text{ or } 2 \pmod{2^2} \text{ for } L_j \text{ of type } A_1^0; \\
a_{ii} \equiv 0 \pmod{2}, \text{ but } a_{ii} \neq 0 \pmod{2^2}.
\]

Case (iii). \( L_i \) has type \( A_1^1 \). By Lemma 2.7.23, no symmetries of \( O(L_j) \) can fix \( \phi(J) \) unless \( i = j \) and \( \phi \) is in the orbit of the inclusion map, in which case \( H_\phi = \{1, S_{e_1}\} \).

We have

\[
\frac{|O(L_j)|}{|H_\phi|} = \begin{cases} 
2^n_{ij} - 1 & \text{if } i = j, \phi \in \text{orbit of inclusion} \\
2^n & \text{otherwise.}
\end{cases}
\]

Thus

\[
a_{ij} \equiv 0 \pmod{2^3} \text{ for } L_j \text{ of type } A_2^2 \text{ or } A_1^1, i \neq j; \\
a_{ij} \equiv 0 \pmod{2^2} \text{ for } L_j \text{ of type } A_0^0 \text{ or } A_1^1; \\
a_{ii} \equiv 0 \pmod{2^2}, \text{ but } a_{ii} \neq 0 \pmod{2^3}.
\]
Case (iv). \( \mathbb{L}_i \) has type \( A_2^2 \), then \( a_{ij} = 0 \) if \( i \neq j \), but \( a_{ii} = 12 \), since \( J_1 \cong A(2,2) \).

Suppose now there is a non-trivial linear relation

\[
\sum_j c_j \theta_{\mathbb{L}_j}^{(2)}(Z) = 0,
\]

where the \( c_j \)'s are relatively prime integers. By evaluating at each \( J_i \), we obtain \( \sum_j c_j a_{ij} = 0 \).

1. If \( \mathbb{L}_i \) has type \( A_2^2 \), then \( c_i = 0 \).
2. If \( \mathbb{L}_i \) has type \( A_0^1 \), then \( \sum_j c_j a_{ij} \equiv 0 \pmod{2^2} \) yields \( c_i \equiv 0 \pmod{2} \).
3. If \( \mathbb{L}_i \) has type \( A_1^0 \), then \( \sum_j c_j a_{ij} \equiv 0 \pmod{2^2} \) also yields \( c_i \equiv 0 \pmod{2} \).
4. If \( \mathbb{L}_i \) has type \( A_0^1 \), then \( \sum_j c_j a_{ij} \equiv 0 \pmod{2^3} \) yields \( c_i \equiv 0 \pmod{2} \).

This is a contradiction, and our proof is completed.

Q.E.D.

2.7.25 Corollary: Let \( \mathbb{L}_1 \) and \( \mathbb{L}_2 \) be two lattices in \( G'(4, p^2) \), then \( \mathbb{L}_1 \cong \mathbb{L}_2 \) if and only if \( \theta_{\mathbb{L}_1}^{(2)}(Z) \equiv \theta_{\mathbb{L}_2}^{(2)}(Z) \pmod{8} \).

Proof: We have \( a_{\mathbb{L}}(2 0 0) = 0, 2, 6 \), as \( \mathbb{L} \) has type \( A_0^1, A_1^0 \) or \( A_1^1 \), or \( A_2^1 \), respectively. Also, \( a_{\mathbb{L}}(2p 0 0) = 0 \) or 2 as \( \mathbb{L} \) has type \( A_0^1 \) or \( A_1^1 \), respectively. It follows that

\( \theta_{\mathbb{L}_1}^{(2)}(Z) \not\equiv \theta_{\mathbb{L}_2}^{(2)}(Z) \pmod{8} \) if \( \mathbb{L}_1 \) and \( \mathbb{L}_2 \) are not of the same type. If \( \mathbb{L}_1 \) and \( \mathbb{L}_2 \) are of the same type, then we choose \( J_1 \) in \( \mathbb{L}_1 \) according to Theorem 2.7.24. We have \( a_{\mathbb{L}_1}(J_1) = 2 \) or 6
(mod 8), but \( a_{\mathbb{L}_2}(J_1) \equiv 0 \) or \( 4 \) (mod 8) if \( \mathbb{L}_1 \) and \( \mathbb{L}_2 \) have type \( A_0^1 \) or \( A_1^0 \). If \( \mathbb{L}_1 \) and \( \mathbb{L}_2 \) are both of type \( A_1^1 \), then \( a_{\mathbb{L}_1}(J_1) \equiv 4 \) (mod 8), but \( a_{\mathbb{L}_2}(J_1) \equiv 0 \) (mod 8). In any case, \( \Theta_{\mathbb{L}_1}(Z) \neq \Theta_{\mathbb{L}_2}(Z) \) (mod 8).

Q.E.D.

2.7.26 Remark: By Proposition 2.6.4 and Proposition 2.7.9, the number of classes in \( G'(4, p^2) \) is essentially

\[
\left[ \frac{p + 19}{24} \right] + \frac{h(\sqrt{p})}{4}.
\]
Chapter III

THETA SERIES OF QUADRATIC LATTICES OVER \( \mathbb{Z} \left[ \frac{1 + \sqrt{p}}{2} \right] \)

Let \( p \) be a prime \( \equiv 1 \pmod{4} \). Let \( F = \mathbb{Q}(\sqrt{p}) \) and \( \mathcal{O} \) be the ring of integers of \( F \), i.e. \( \mathcal{O} = \mathbb{Z} \left[ \frac{1 + \sqrt{p}}{2} \right] \). Denote by \( \mathcal{U} \) the group of units of \( \mathcal{O} \). In this chapter we shall consider theta series of ternary and quaternary lattices over the ring \( \mathcal{O} \).

§3.1 Theta Series of Degree Two

Let \( \gamma \) be a positive definite quaternion space of discriminant \( 1 \) over \( F \). We assume that there is a lattice \( \mathcal{L} \) over \( \mathcal{O} \) on \( \gamma \) such that \( \mathcal{L}_p \) is unimodular at each finite prime \( p \) of \( F \) and \( Q(x) \in 2\mathcal{O} \) for any \( x \in \mathcal{L} \). It is easy to see that \( \mathcal{L}_p \) is a hyperbolic space at each finite \( p \). If we let \( \mathcal{Q} \) denote the quaternion algebra of discriminant \( p^2 \) over \( \mathbb{Q} \) and \( \mathcal{Q}_F = \mathcal{Q} \otimes_{\mathbb{Q}} F \), then a routine calculation of Hasse symbols shows that \( \gamma \cong \mathcal{Q}_F \), with the quadratic map on \( \mathcal{Q}_F \) being \( 2N(x) \), where \( N \) is the reduced norm. We assume throughout this chapter that \( \gamma = \mathcal{Q}_F \) and \( Q(x) = 2N(x) \). For any notation not explained in the following concerning the arithmetic of quaternion algebra, we refer the reader to Chapter I of this paper.
Let $\mathcal{J}(4,1)$ be the genus of the lattice $\mathcal{L}$ on $\mathcal{Q}$. Suppose that $\Omega$ is a maximal order of $\mathcal{O}_p$. Then $\Omega_p = M_2(\Theta_p)$ at every finite prime $p$, since $(\mathcal{O}_p)_p$ is split. Hence, $\Omega_p$ is unimodular for every $p$. Clearly, $Q(x) \in 2\Theta$ for every $x \in \Omega$; hence, $\Omega \in \mathcal{J}(4,1)$. On the other hand, if $\mathcal{L}$ is any lattice in $\mathcal{J}(4,1)$ and $\Omega$ is any maximal order of $\mathcal{O}_p$, then there exist $\alpha = (\alpha_p), \beta = (\beta_p)$ in $J_{\mathcal{O}_p}$ satisfying $N(\alpha_p \beta_p) = 1$ such that $\mathcal{L} = \Omega \Omega^*$. In particular, $\mathcal{L}$ is a normal ideal. To see this, we observe that $\mathcal{L}_p$ and $\Omega_p$ are locally isometric; hence, there exist $\alpha_p, \beta_p \in (\mathcal{O}_p)_p^\times$ such that $\mathcal{L}_p = \alpha_p \Omega_p \beta_p$ (Proposition 1(b), $[P_1]$). Since $\mathcal{L}_p = \Omega_p$ for almost all $p$, we may assume that $\alpha_p$ and $\beta_p$ are units of $\Omega_p$ for almost all $p$. Hence, $\alpha = (\alpha_p)$ and $\beta = (\beta_p)$ belong to $J_{\mathcal{O}_p}$. Clearly, $\mathcal{L} = \Omega \Omega^*$. It is also clear that the isomorphism class (i.e. conjugacy class) of a maximal order is the same as its isometry class. For if $\Omega_1$ and $\Omega_2$ are in the same isometry class, then $\Omega_2 = \alpha \Omega_1 \beta$ for some $\alpha, \beta \in \mathcal{O}_p$ satisfying $N(\alpha) = N(\beta)^{-1}$. But the left order of $\alpha \Omega_1 \beta$ is $\alpha \Omega_1 \beta^{-1}$, hence, $\Omega_2 = \alpha \Omega_1 \beta^{-1}$. It is natural to ask if the maximal orders are the only lattices (up to isometry, of course) which represent 2. 

3.1.1 Proposition: Let $\mathcal{L} \in \mathcal{J}(4,1)$ represent 2. Then $\mathcal{L}$ is isometric to a maximal order.

Proof: Let $\gamma \in \mathcal{L}$ be such that $N(\gamma) = 1$ (i.e. $Q(\gamma) = 2$), and let $\Omega_\ell, \Omega_r$ be the left and right order of $\mathcal{L}$, respectively. $\Omega_\ell$ and $\Omega_r$ are maximal orders, since $\mathcal{L}$ is normal; hence,
Ω_l, Ω_r ∈ ℓ(4,1). We have ℓ(ℓ⁻¹γ) = Ω_lγ ⊆ ℓ, so ℓ⁻¹γ ⊆ Ω_r⁻¹. We claim that ℓ⁻¹γ = Ω_r⁻¹. It suffices to show that ℓ⁻¹γ ∈ ℓ(4,1).
Write ℓ = αΩβ for some maximal order Ω, α = (α_0), β = (β_0) in J_F, N(α_0β_0) = 1 for all ϕ. Locally at each ϕ, we have ℓ_ϕ = α_ϕΩ_ϕβ_ϕ; hence, ℓ⁻¹_ϕ = β⁻¹_ϕΩ_ϕα⁻¹_ϕ. It follows that ℓ⁻¹_ϕγ = β⁻¹_ϕΩ_ϕα⁻¹_ϕγ. Since N(β⁻¹_ϕΩ⁻¹_ϕγ) = 1, ℓ⁻¹_ϕγ and Ω_ϕ are locally isometric for every ϕ; hence ℓ⁻¹γ ∈ ℓ(4,1). Now ℓ⁻¹γ = Ω_r⁻¹ implies that ℓℓ⁻¹γ = Ω_r or Ω_r⁻¹γ = ℓ. But this means that ℓ is isometric to Ω_r⁻¹. Q.E.D.

3.1.2 Remark: Denote by h(α_0) and h(F) the ideal class numbers of α_0 and F, respectively. The number of lattice classes in ℓ(4,1) is \( \frac{1}{2}H(H + 1) \), where \( H = h(α_0)/h(F) \) ([K_3]). It is known that H is the type number of α_0 (i.e. the number of conjugacy classes of maximal orders of α_0). By Lemma 2 [K_3], H is equal to the number of classes in ℓ(4,1) which have nontrivial automorphism. It follows, therefore, (using Proposition 3.1.1) that the classes in ℓ(4,1) which represent 2 are precisely those classes which have improper automorphism groups. We denote by ℓ°(4,1) the set of all such classes. A formula for H can be found in [K_3] (H is also equal to the proper class number of nice quaternary lattices of discriminant p).

Since the class number of ℓ(4,1) is 1 when p = 5, we shall henceforth assume in our discussion that p > 5.
3.1.3 **Lemma:** Let $\Omega$ be a maximal order of $\mathcal{O}_F$ and $W$ the group of roots of unity of $\Omega$. Then $W = \{ \omega \in \Omega \mid N(\omega) = 1 \}$.

**Proof:** (1). If $\omega \in \Omega$ is a root of unity, then $\omega^n = 1$ for some $n$; hence, $N(\omega)^n = 1$. Since $N(\omega)$ is totally positive and the only roots of unity of $K$ are $\pm 1$, we have $N(\omega) = 1$.

(2). This is an immediate consequence of the fact that the group of all units of $\Omega$ having norm 1 is a finite group (see page 129). Q.E.D.

3.1.4 **Proposition:** Let $\Omega$ be a maximal order of $\mathcal{O}_F$, $W$ the group of roots of unity of $\Omega$, and $U$ the group of units of $F$. Then $\Omega^* \cong W \times U / \{ \pm 1 \}$. In particular, we have $|W| = 2|\Omega^*/U|$.

**Proof:** Define $\phi: W \times U \to \Omega^*$ by $\phi(\omega, \varepsilon) = \omega \varepsilon$, then $\phi$ is clearly a homomorphism. If $u \in \Omega^*$, then $N(u) = \varepsilon^2$ for some $\varepsilon \in U$ (note that $n_{F/Q}(\text{fundamental unit}) = -1$). Since $N(ue^{-1}) = 1$, it follows that $u = \omega \varepsilon$ for some $\omega \in W$; hence, $\phi$ is surjective. Now if $\omega \varepsilon = 1$, then $\omega = \varepsilon^{-1} \in W \cap U = \{ \pm 1 \}$. Therefore, we have $\omega = \varepsilon = \pm 1$; thus, $\ker \phi = \{ \pm 1 \}$. Q.E.D.

3.1.5 **Remark:** If $\Omega$ is a symmetric maximal order, then we know from [H] that $|\Omega^*/U| = 1, 2, 3, 6, \text{ or } 12$; hence, it follows from Lemma 3.1.3 and Proposition 3.1.4 that the number of minimal vectors in $\Omega$ is $a(2) = 2, 4, 6, 12, \text{ or } 24$. Note that the corresponding nice quaternary lattice $L = \Omega \cap V$ in $V = \{ \alpha \in \mathcal{O}_F \mid \bar{\alpha}^* = \alpha \}$ has number of minimal vectors
a_L(2) = 2, 4, 6, 8, or 12. We remind the reader of two extreme cases. There exists exactly one class of symmetric maximal orders \( \Omega \) with \( a_\Omega(2) = 12 \) or \( 24 \) when \( p \equiv 2 \pmod{3} \) or \( p \equiv 5 \pmod{8} \), respectively. Such maximal orders do not exist otherwise (see [H]).

We wish to determine the different types of roots system of the lattices \( \mathcal{L} \) in \( \mathcal{J}(4, 1) \). It is known ([Mi]) that the only (nonempty) indecomposable 2-lattices over \( \mathcal{O} \) are \( \mathcal{A}_n \), \( 1 \leq n \leq 4 \), and \( \mathcal{D}_4 \). Hence, if \( \mathcal{L} \in \mathcal{J}(4, 1) \), then the possible roots systems for \( \mathcal{L} \) are \( \mathcal{A}_1 \), \( \mathcal{A}_1 \oplus \mathcal{A}_1 \), \( \mathcal{A}_1 \oplus \mathcal{A}_1 \oplus \mathcal{A}_1 \), \( \mathcal{A}_1 \oplus \mathcal{A}_1 \oplus \mathcal{A}_1 \oplus \mathcal{A}_1 \), \( \mathcal{A}_2 \), \( \mathcal{A}_1 \oplus \mathcal{A}_2 \), \( \mathcal{A}_1 \oplus \mathcal{A}_1 \oplus \mathcal{A}_2 \), \( \mathcal{A}_2 \oplus \mathcal{A}_2 \), \( \mathcal{A}_3 \), \( \mathcal{A}_1 \oplus \mathcal{A}_3 \), \( \mathcal{A}_4 \), and \( \mathcal{D}_4 \). The cases \( \mathcal{A}_1 \oplus \mathcal{A}_1 \oplus \mathcal{A}_2 \), \( \mathcal{A}_1 \oplus \mathcal{A}_3 \), and \( \mathcal{A}_4 \) are impossible by consideration of the discriminant of \( \mathcal{L}_p \) locally for \( p \) dividing 3, 2, and 5, respectively.

We shall eliminate some more cases.

3.1.6 Proposition: Suppose there exists \( \mathcal{L} \in \mathcal{J}(4, 1) \) with roots system \( R_\mathcal{L} \supset \mathcal{A}_1 \oplus \mathcal{A}_1 \oplus \mathcal{A}_1 \). Then we have \( p \equiv 5 \pmod{8} \) and \( R_\mathcal{L} = \mathcal{D}_4 \).

Proof: Let \( e_1 \), \( e_2 \), and \( e_3 \) be mutually orthogonal minimal vectors in \( \mathcal{L} \) and let \( \eta \) be the orthogonal complement of \( \kappa e_1 \perp \kappa e_2 \perp \kappa e_3 \) in \( \mathcal{L} \). If \( p \) is nondyadic, then \( \kappa e_1 \perp \kappa e_2 \perp \kappa e_3 \) splits \( \mathcal{L}_p \); hence, \( d \eta_p = 2 \) with respect to some basis of \( \eta_p \). For dyadic prime \( p \), we claim that \( d \eta_p = 2 \) also for some basis. To see this, we consider \( \mathcal{L} \) locally at \( p \).
Since $e_1$ is primitive in $L_\mathfrak{p}$, we may assume that $L_\mathfrak{p} \cong A(2, 0) \perp A(2, 0)$ with respect to a basis $\{ e_1, u, v, w \}$. Let $K = \Theta_\mathfrak{p}(e_1 - 2u) \perp (\Theta_\mathfrak{p}v + \Theta_\mathfrak{p}w)$. If $e_2$ splits $K$, then the orthogonal complement of $e_2$ in $K$ would be a binary unimodular lattice of discriminant a unit square such that its norm is contained in $2\Theta_\mathfrak{p}$. This is impossible, since the only such binary lattices are $A(0, 0)$ and $A(2, 2)$, and they have discriminant $-1$ and $-\Delta$, respectively. (Note that $-1$ and $\Delta$ are nonsquare units of quadratic defects equal to $2\Theta_\mathfrak{p}$ and $4\Theta_\mathfrak{p}$, respectively.) It follows that $B(e_2, K) = \Theta_\mathfrak{p}$; hence, we may assume that $e_2 = v$. Now the orthogonal complement of $e_2$ in $K$ is $m = \Theta_\mathfrak{p}(e_1 - 2u) \perp \Theta_\mathfrak{p}(e_2 - 2w)$. By 82:15 [OM], $e_3$ splits $m$, so $\mathfrak{m} = (\Theta_\mathfrak{p}e_3)^{\perp}$ in $m$. Clearly, $d\mathfrak{m} = 2$.

Since the discriminant of $F\mathfrak{m}$ is obviously 2, we have, by a result of Kitaoka (Proposition in Appendix $[K_3]$), page 97), that $\mathfrak{m}$ is a free lattice; hence, $\mathfrak{m} = \Theta_\mathfrak{p}e_4$ for some $e_4$ in $L$.

The above argument already shows that $e_4$ is a minimal vector. It is easy to see that $S_{\mathfrak{m}}(\mathfrak{m}) = 1$ using the basis $\{ e_1, e_2, e_3, e_4 \}$. On the other hand, $\mathfrak{m} \cong A(0, 0) \perp A(0, 0)$, so its Hasse symbol $S_{\mathfrak{m}}(\mathfrak{m})$ is $-1$ or $1$ as $p \equiv 1$ or $5 \pmod{8}$. It follows, therefore, in our case that $p \equiv 5 \pmod{8}$. At the dyadic prime $\mathfrak{p}$, we have $L_\mathfrak{p} \cong \Theta_\mathfrak{p}e_1 \perp \Theta_\mathfrak{p}e_2 \perp \Theta_\mathfrak{p}e_3 \perp \Theta_\mathfrak{p}e_4$; hence, $L_\mathfrak{p}$ contains a vector $\frac{1}{2}(\alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4)$ not in $\Theta_\mathfrak{p}e_1 \perp \Theta_\mathfrak{p}e_2 \perp \Theta_\mathfrak{p}e_3 \perp \Theta_\mathfrak{p}e_4$. We may assume that $\alpha$, $\beta$, $\gamma$, and $\delta$ are either units or 0. Furthermore, if $\{ 0, 1, \omega, 1 + \omega \}$
is a representative set of the residue class field at \( \mathfrak{p} \), then we may assume that \( \alpha, \beta, \gamma, \delta \in \{0, 1, \omega, 1 + \omega\} \).

Since \( Q(\frac{1}{2}(\alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4)) \) \( \notin 2\mathfrak{p} \), we have \( \alpha = \beta = \gamma = \delta \). It follows that \( \frac{1}{2}(e_1 + e_2 + e_3 + e_4) \) \( \notin \mathfrak{p} \), and so

\( \frac{1}{2}(e_1 + e_2 + e_3 + e_4) \in \mathfrak{l} \). But this implies that \( R_\mathfrak{l} = D_4 \), since \( \mathfrak{l} \) contains the lattice \((e_1 \perp e_2 \perp e_3 \perp e_4) + 2(e_1 + e_2 + e_3 + e_4) \). Q.E.D.

3.1.7 Proposition: There exists at most one class of lattices \( \mathfrak{l} \) in \( \mathcal{J}(4, 1) \) such that the roots system \( R_\mathfrak{l} \supset A_3 \). In case it exists, we have \( p \equiv 5 \pmod{8} \) and \( R_\mathfrak{l} = D_4 \).

Proof: Suppose \( \mathfrak{l} \supset \Lambda = \mathfrak{e}_1 + \mathfrak{e}_2 + \mathfrak{e}_3 \), where \( \mathfrak{e}_1, \mathfrak{e}_2, \) and \( \mathfrak{e}_3 \) are minimal vectors and \( B(e_1, e_2) = B(e_2, e_3) = 1, B(e_1, e_3) = 0 \). If \( \mathfrak{l}' \) is any other lattice in \( \mathcal{J}(4, 1) \) containing \( \Lambda \), then we have \( \mathfrak{l}' \mathfrak{p} = \mathfrak{p} \) for all nondyadic primes \( \mathfrak{p} \). This is clear, since \( \Lambda \mathfrak{p} \) is unimodular, and therefore it splits both \( \mathfrak{l} \mathfrak{p} \) and \( \mathfrak{l}' \mathfrak{p} \). Consider \( \mathfrak{l} \) at a dyadic prime \( \mathfrak{p} \)

We have \( \mathfrak{l} \mathfrak{p} = \mathfrak{e}_1 \mathfrak{p} + \mathfrak{e}_2 \mathfrak{p} \perp X \) for some binary unimodular lattice \( X \cong A(2, 2) \) by the cancellation law. If \( p \equiv 1 \pmod{8} \), then \( F_\mathfrak{p} X \) is anisotropic, since \( d(F_\mathfrak{p} X) \notin 5 \mathfrak{p}^2 \). By 63:15(i) \([\text{OM}]\), \( Q(F_\mathfrak{p} X) \) is either \( \mathfrak{u}_5^2 \mathfrak{f}_\mathfrak{p}^2 \) or \( 2 \mathfrak{u}_\mathfrak{p}^2 \). This is impossible, since, on one hand, \( Q(X) \geq 2 \) and, on the other hand, \( X \) contains \( e_1 - 2e_2 + 3e_3 \); hence, \( Q(X) \geq 12 \). It follows that \( p \equiv 5 \pmod{8} \) and \( F_\mathfrak{p} X \) is isotropic. There exists a basis \( \{u, v\} \) of \( X \) such that \( Q(u) = Q(v) = 0 \) and \( B(u, v) = 1 \). Since \( e_1 - 2e_2 + 3e_3 \in X \), we have \( e_1 - 2e_2 + 3e_3 = \alpha u + \beta v \) for some
\(a, \beta \in \mathcal{O}_\mathbb{M}\). We may assume that \(a\) is a unit. By changing the basis \{\(u, v\)\} to \{\(au, a^{-1}u\)\} if necessary, we may assume that \(a = 1\); hence, we have \(e_1 - 2e_2 + 3e_3 = u + \beta v\), where \(\beta = 6\).

Now if \(L' \in \mathcal{L}(4, 1)\) contains \(\Lambda\), then \(L'_\mathbb{M} = (\mathcal{O}_\mathbb{M}e_1 + \mathcal{O}_\mathbb{M}e_2) + Y\) for some binary unimodular lattice \(Y\) containing \(e_1 - 2e_2 + 3e_3\).

Since \(e_1 - 2e_2 + 3e_3\) is primitive in \(Y\), there exists \(z = \gamma u + \delta v\), where \(\gamma, \delta \in \mathbb{F}_\mathbb{M}\) in \(Y\) such that \(B(e_1 - 2e_2 + 3e_3, z) = 1\). We have

\[
\begin{align*}
(1) \quad B(e_1 - 2e_2 + 3e_3, z) &= B(u + 6v, \gamma u + \delta v) \\
&= \delta + 6\gamma = 1, \text{ and}
\end{align*}
\]

\[
\begin{align*}
(2) \quad Q(z) &= Q(\gamma u + \delta v) = 2\gamma \delta \in 2\mathcal{O}_\mathbb{M}(\gamma \delta \in \mathcal{O}_\mathbb{M}).
\end{align*}
\]

Consider the following cases:

(i) \(\gamma \in 2^{-1}\mathcal{O}_\mathbb{M}\). By (2), we have \(\delta \in 4\mathcal{O}_\mathbb{M}\); hence \(|\delta + 6\gamma| = |6\gamma| > 1\) by the principle of domination, which contradicts (1).

(ii) \(\gamma \in \mathcal{O}_\mathbb{M}\). By (1), we have \(\delta \in \mathcal{U}_\mathbb{M}\); hence, \(Y \subseteq X\). Since both \(X\) and \(Y\) are unimodular, it follows that \(Y = X\) and, therefore, \(L'_\mathbb{M} = L'_\mathbb{M}\). But this means that \(L' = L\).

(iii) \(\gamma \in 2^{-1}\mathcal{U}_\mathbb{M}\). By (2), we have \(\delta \in 2\mathcal{O}_\mathbb{M}\); hence \(\gamma = 2^{-1}\epsilon u + 2\eta v\) for some \(\epsilon \in \mathcal{U}_\mathbb{M}\) and \(\eta \in \mathcal{O}_\mathbb{M}\). A routine calculation shows that \(S_{u-6v}(e_1 - 2e_2 + 3e_3) = e_1 - 2e_2 + 3e_3\) and \(S_{u-6v}(z) = 3^{-1}\eta u + 3\epsilon v\). Hence, \(S_{u-6v}(Y) = X\). Let \(w\) be a vector in the orthogonal complement of \(\Lambda\) in \(L\). Then the two symmetries \(S_w\) and \(S_{u-6v}\) are identical locally at \(\mathbb{M}\). It follows that \(S_w(X) = Y\), and so \(S_w(L'_\mathbb{M}) = L'_\mathbb{M}\). For nondyadic
P, we have \( \mathcal{L}'_{\mathcal{P}} = \mathcal{L}_{\mathcal{P}} = S_{\mathcal{L}} \mathcal{L}_{\mathcal{P}} \) since they all contain \( \Lambda \).

Therefore, \( \mathcal{L}' = S_{\mathcal{L}} \mathcal{L} \), and they are isometric. Note that \( A_3 \) is characteristic in \( \mathcal{L} \) while locally at \( \mathcal{B} = (2) \) the localization is not characteristic. Now we know that there exists a lattice \( \mathcal{L} \) in \( \mathcal{O}(4,1) \) with roots system \( R_{\mathcal{L}} = D_4 \) when \( p \equiv 5 \pmod{8} \) by Remark 3.1.5. Since the roots system \( D_4 \supset A_3 \), it follows that \( \mathrm{cls} \mathcal{L} \) is the only class in \( \mathcal{O}(4,1) \) roots system \( R_{\mathcal{L}} \supset A_3 \) by what we have just shown. Q.E.D.

3.1.8 Proposition: There is at most one class of lattices \( \mathrm{cls} \mathcal{L} \) in \( \mathcal{O}(4,1) \) such that the roots system \( R_{\mathcal{L}} \supset A_1 \oplus A_2 \).

In case such a class exists, we have \( p \equiv 2 \pmod{3} \) and 
\[ R_{\mathcal{L}} = A_2 \oplus A_2. \]

Proof: Let \( \mathcal{L} \supset (\sigma e_1 + \sigma e_2) \perp \sigma e_3 \) such that \( e_1, e_2, \) and \( e_3 \) are minimal vectors and \( B(e_1, e_2) = 1 \). Let \( \eta \) be the orthogonal complement of \( \sigma e_1 + \sigma e_2 \perp \sigma e_3 \) in \( \mathcal{L} \). Assume that \( \mathcal{P} \) does not divide 2 or 3, then \( (\sigma_{\mathcal{P}} e_1 + \sigma_{\mathcal{P}} e_2) \perp \sigma_{\mathcal{P}} e_3 \) splits \( \mathcal{L}_{\mathcal{P}} \) and so \( d \eta_{\mathcal{P}} = 6 \) with respect to some basis. If \( \mathcal{P} \) divides 2, then \( \mathcal{L}_{\mathcal{P}} = (\sigma_{\mathcal{P}} e_1 + \sigma_{\mathcal{P}} e_2) \perp X \) for some binary unimodular lattice \( X \) containing \( e_3 \). Clearly, \( \eta_{\mathcal{P}} = (\sigma_{\mathcal{P}} e_3) \perp \) in \( X \) has discriminant 6 with respect to some basis. If \( \mathcal{P} \) divides 3, then we have \( \mathcal{L}_{\mathcal{P}} = \sigma_{\mathcal{P}} e_1 \perp \sigma_{\mathcal{P}} e_3 \perp Y \) for some binary unimodular lattice \( Y \) containing \( e_1 - 2e_2 \). It is clear that \( \eta_{\mathcal{P}} = \sigma_{\mathcal{P}}(e_1 - 2e_2) \perp \) in \( Y \) and \( d \eta_{\mathcal{P}} = 6 \) with respect to some basis.

By [K_3], page 97 (since \( d(F\eta) = 6 \)), \( \eta \) is a free lattice and \( \eta = \sigma z \) for some \( z \) with \( Q(z) = 6 \). Suppose now that \( p \equiv 1 \).
(mod 3), then a calculation of Hasse symbol at any prime \( P \) dividing 3 using the basis \( \{e_1, e_1 - 2e_2, e_3, z\} \) (see also [B]) shows that \( S_P(\gamma) = -1 \), which is impossible, since \( \gamma = \sigma_F \) is split at \( P \). It follows that \( p \equiv 2 \pmod{3} \) and there exists a unique prime \( P \) dividing 3. By an argument similar to the proof of Proposition 2.7.1, one can show that 

\[
(\sigma_P e_1 + \sigma_P e_2) \downarrow \sigma_P e_3
\]

is locally characteristic at any dyadic prime \( P \). Hence, by Theorem 2.2.6, \( \sigma e_1 + \sigma e_2 \downarrow \sigma e_3 \) is globally characteristic in \( \mathcal{L} \); therefore, it uniquely determines the class of \( \mathcal{L} \). Now in Remark 3.1.5 we saw that there exists a symmetric maximal order \( \Omega \) with \( a_{\Omega}(2) = 12 \) when \( p \equiv 2 \pmod{3} \). The roots system of \( \Omega \), therefore, must be \( A_2 \oplus A_2 \). (It cannot be \( A_3 \) by Proposition 3.1.7.) Since \( A_2 \oplus A_2 \supseteq A_1 \oplus A_2 \), cls \( \Omega \) is the only class in \( \mathcal{J}(4,1) \) which has roots system containing \( A_1 \oplus A_2 \). Q.E.D.

3.1.9 Summary: We have determined all possible types of roots systems for lattices \( \mathcal{L} \) in \( \mathcal{J}'(4,1) \), namely, \( A_1, A_1 \oplus A_1, A_2, A_2 \oplus A_2, \) and \( D_4 \). The number of minimal vectors in \( \mathcal{L} \) corresponding to each type is 2, 4, 6, 12, 24, respectively. Note that there is no new type besides those which have already appeared in the types of symmetric maximal orders. When \( p = 5 \), \( \mathcal{J}(4,1) \) contains exactly one class which is of type \( F_4 \) (see [M], [Mi], and [Co]).
3.1.10 Proposition: Let $\mathcal{L}$ be a lattice in $\mathfrak{S}(4, 1)$ and $\Omega_\mathcal{L}$ and $\Omega_\mathcal{R}$ be the left and right orders of $\mathcal{L}$. Let $W_\mathcal{L}$ and $W_\mathcal{R}$ be the groups of roots of unity of $\Omega_\mathcal{L}$ and $\Omega_\mathcal{R}$, respectively. Then $O^+(\mathcal{L}) \cong W_\mathcal{L} \times W_\mathcal{R} / \{ \pm 1 \}$.

Proof: Every rotation $\sigma$ of $\mathcal{L}$ is of the form $x \mapsto \alpha x \beta^{-1}$ where $\alpha$ and $\beta \in \mathcal{G}$ satisfy $N(\alpha) = N(\beta)$ (Proposition 1 [P1]). Since $\alpha \beta^{-1} = \mathcal{L}$, we have $\alpha \Omega_\mathcal{L} \alpha^{-1} = \Omega_\mathcal{L}$ and $\beta \Omega_\mathcal{R} \beta^{-1} = \Omega_\mathcal{R}$. Hence, both $\Omega_\mathcal{L} \alpha$ and $\Omega_\mathcal{R} \beta$ are principal two-sided ideals in $\mathcal{G}$.

Since $\mathcal{G}$ is split at every finite prime $\mathcal{P}$, all two-sided $(\Omega_\mathcal{L})_\mathcal{P}$-ideals are of the form $(\Omega_\mathcal{L})_\mathcal{P} I_\mathcal{P}$ where $I_\mathcal{P}$ is an ideal of $\mathcal{F}_\mathcal{P}$ (similarly for two-sided $(\Omega_\mathcal{R})_\mathcal{P}$-ideals). It follows that $\Omega_\mathcal{L} \alpha = \Omega_\mathcal{L} I$ and $\Omega_\mathcal{R} \beta = \Omega_\mathcal{R} J$ for some ideals $I$ and $J$ in $\mathcal{F}$. Observe that the ideal in $\mathcal{F}$ generated by $N(\Omega_\mathcal{L} \alpha)$ is $(N(\alpha))$ and the ideal generated by $N(\Omega_\mathcal{L} I)$ is $I^2$. To see the latter, just consider $I$ locally at each prime $\mathcal{P}$. We have $I_\mathcal{P} = \Theta_\mathcal{P} a_\mathcal{P}$ for some $a_\mathcal{P} \in \mathcal{F}_\mathcal{P}$; hence, $I^2 = \Theta_\mathcal{P} a_\mathcal{P}^2$. Clearly, the ideal generated by $N((\Omega_\mathcal{L})_\mathcal{P} I_\mathcal{P})$ is also $\Theta_\mathcal{P} a_\mathcal{P}^2$. Therefore, we have $I^2 = (N(\alpha))$, and similarly $J^2 = (N(\beta))$. Since the class number of $\mathcal{F}$ is odd, $I$ and $J$ are principal; hence, there exist $a, b \in \mathcal{F}$ such that $\Omega_\mathcal{L} \alpha = \Omega_\mathcal{L} a$ and $\Omega_\mathcal{R} \beta = \Omega_\mathcal{R} b$. Now let $u \in \Omega_\mathcal{L}^\times$, $v \in \Omega_\mathcal{R}^\times$ be such that $\alpha = ua$ and $\beta = vb$. Since $N(u) \in \mathcal{U}$ and is totally positive, we have $N(u) = \varepsilon^2$ for some $\varepsilon \in \mathcal{U}$; hence, $u = \varepsilon w$ for some $w \in W_\mathcal{L}$. By replacing $a$ by $\varepsilon a$, we may assume that $u \in W_\mathcal{L}$. Similarly, we may assume that $v \in W_\mathcal{R}$. Now we have $N(\alpha) = N(u)N(\alpha) = a^2$ and $N(\beta) = b^2$. Since $N(\alpha) = N(\beta)$,
it follows that $a = \pm b$. Finally, we have $\sigma(x) = ax^{b^{-1}} = uaxb^{-1}v = \pm uxv^{-1}$; hence, the homomorphism $\phi: W_L \times W_x \rightarrow O^{+}(L)$ defined by $\phi(u, v) = \sigma (\sigma(x) = uxv^{-1})$ is clearly surjective.

To see that $\ker \phi = \{ \pm 1 \}$, suppose that there exist $u, v \in W_L$, $v \in W_x$ such that $uxv^{-1} = u_1xv_1^{-1}$, for all $x \in G_F$, then we have $u_1^{-1}ux = xv_1^{-1}v$; hence, $u_1^{-1}u$ and $v_1^{-1}v$ belong to the center of $G_F$, which is $F$. But these are also roots of unity; therefore, $u_1 = \pm u$ and $v_1 = \pm v$. It follows that $u_1xv_1^{-1} = \pm uxv^{-1}$.

**Q.E.D.**

**3.1.11 Corollary:** Let $L$ be a lattice in $\mathcal{L}(4, 1)$, then the order of the unit group of $L$, $|O(L)|$, is $4, 16, 36, 144,$ or $576$, as the type of $L$ is $A_1$, $A_1 \oplus A_1$, $A_2$, $A_2 \oplus A_2$, or $D_4$, respectively.

**Proof:** If $L \in \mathcal{L}(4, 1)$, then $L$ is isometric to a maximal order $\Omega$ of $G_F$ by Proposition 3.1.1; hence, $|W_L| = |W_x| = 2, 4, 6, 12,$ or $24$ as the type of $L$ is $A_1$, $A_1 \oplus A_1$, $A_2$, $A_2 \oplus A_2$, or $D_4$, respectively. By Proposition 3.1.10, the corresponding rotation group of $L$ has order $|O^{+}(L)| = 2, 8, 18, 72,$ or $288$, respectively. Since $L$ has improper automorphism, it follows that $|O(L)| = 2|O^{+}(L)| = 2, 16, 36, 144,$ or $576$, respectively. **Q.E.D.**

If $e$ is a minimal vector in the lattice $L \in \mathcal{L}(4, 1)$, then it is clear that $S_e$ is a symmetry of $L$. Conversely, we have
3.1.12 Proposition: Every symmetry of $\mathcal{L} \in \mathcal{L}'(4, 1)$ is of the form $S_e$, where $e$ is a minimal vector of $\mathcal{L}$.

Proof: Let $S_u, u \in \mathcal{L}'$, be a symmetry of $\mathcal{L}$. By replacing $u$ by a scalar multiple of itself, we may assume that $u \in \mathcal{L}$. We consider $\mathcal{L}$ locally at each finite prime $p$.

If $u$ is not maximal in $\mathcal{L}_p$, we can write $u = \pi_p \hat{u}$, where $\pi_p$ is a prime element at $p$ and $\hat{u}$ is maximal in $\mathcal{L}_p$. It is clear that $S \in O(\mathcal{L}_p)$, hence $\mathcal{B}(\hat{u}, \mathcal{L}_p) \subseteq Q(\hat{u})\mathcal{O}_p$. Since $\hat{u}$ is maximal in $\mathcal{L}_p$, we have $\mathcal{B}(\hat{u}, \mathcal{L}_p) = \mathcal{O}_p$. It follows, therefore, that $Q(\hat{u}) \in \mathcal{U}_p$ if $p$ is a non-integer prime, and if $p$ divides $2$, we have $Q(\hat{u}) \in 2\mathcal{U}_p$. Thus, $Q(u) \in 2\mathcal{U}_p$ for all finite primes $p$, and so $Q(u)\mathcal{O}_p = 2\prod_{p \nmid 2^s_p} \mathcal{U}_p$ (note that $s_p = 0$ for almost all $p$). Now $(\prod_{p \nmid 2^s_p})^2$ is a principal ideal; hence

$$
\prod_{p \nmid 2^s_p} \mathcal{O}_p
$$

is also principal, since $h(F)$ is odd, say $\prod_{p \nmid 2^s_p} \mathcal{O}_p = \mathcal{O}_F(a), a \in \mathcal{O}_F$. It is easy to see that $Q(a^-1_u) = 2e^2$ for some $e \in \mathcal{U}$; so by replacing $u$ by $a^-1_u$, we get $Q(e^-1a^-1_u) = 2$ and

$$
S_{e^-1a^-1_u} = S_u.
$$

Q.E.D.

Our immediate goal is to show that the classes of lattices in $\mathcal{L}'(4, 1)$ have independent theta series. Let $\mathcal{L}_1, \ldots, \mathcal{L}_h$ be a full set of non-isometric lattices in $\mathcal{L}'(4, 1)$. For each $i$, fix a minimal $e_i$ in $\mathcal{L}_i$ and denote by $\mathcal{V}_i$ the orthogonal complement of $e_i$ in $\mathcal{L}_i$. By a similar argument as
the one given in the proof of Proposition 3.1.6, it is easy
to see that $\mathcal{K}_i$ is a free lattice and $d\mathcal{K}_i = 2$ with respect to
some basis. We choose a binary lattice $\mathcal{I}_i$ in $\mathcal{K}_i$ according
to the following lemma. (We shall omit the subscript $i$.)

3.1.13 Lemma: There exists a principal prime ideal $\mathfrak{q} = \mathfrak{p}^r$
of $F$ such that $\mathcal{K}$ contains a binary free lattice $\mathcal{I}$ with
discriminant $d\mathcal{I} = \pi$, where $\pi$ is a totally positive prime
number in $F$.

Proof: Consider $\mathcal{K}$ locally at a dyadic prime $\mathfrak{p}$. Since
d$\mathcal{K} = 2$, we have $\mathcal{K}_\mathfrak{p} = \mathcal{X} \perp \mathcal{O}_\mathfrak{p}\mathcal{X}$ for some binary unimodular
lattice $\mathcal{X}$ and $Q(\mathcal{X}_\mathfrak{p}) \in 2U_\mathfrak{p}$. By Lemma 1.6 [HKK] generalized
to totally real number fields, we can find a vector $x$ in $\mathcal{X}$
such that $x$ is close to $x_\mathfrak{p}$ at each dyadic prime $\mathfrak{p}$ and that
$Q(x) \in U_\mathfrak{p}$ for all nondyadic $\mathfrak{p}$, except at one prime $\mathfrak{q}$ where
$Q(x)\mathfrak{q} = \mathfrak{q}$. Since $2^{-1}Q(x) \in U_\mathfrak{p}$ for all $\mathfrak{p} \neq \mathfrak{q}$, whereas
$2^{-1}Q(x)\mathfrak{q} = \mathfrak{q}$, it follows that $\mathfrak{q} = c2^{-1}Q(x)$ as a global
ideal. There exists $\pi \in \mathfrak{q}$ such that $Q(x) = 2\pi$. Let $\mathcal{I}$ be the
orthogonal complement of $x$ in $\mathcal{K}$. It is easy to see that
d$\mathcal{I}_\mathfrak{p} = \pi$ (with respect to some basis) for all primes $\mathfrak{p}$.
Since $F\mathcal{I}$ clearly has discriminant $\pi$ also, by $[K_3]$, page 97,$\mathcal{I}$ is a free lattice and $d\mathcal{I} = \pi$.

Q.E.D.

It is clear from Lemma 3.1.13 that the orthogonal
complement of $\mathcal{I}$ in $\mathcal{K}$ is a free lattice. We shall denote it
by $\mathcal{I}_f$. Hence, we have $\mathcal{I} \supset \mathcal{O} \perp \mathcal{I} \perp \mathcal{O}_f$, where $Q(f) = 2\pi$. 
3.1.14 **Lemma:** \( \Theta \parallel \mathcal{J} \) is a globally characteristic sublattice of \( \mathcal{L} \). There exist exactly two lattices in \( \mathcal{J}(4,1) \) containing \( \Theta \parallel \mathcal{J} \), and the two are interchanged by the symmetry \( S_f \).

**Proof:** By Theorem 2.2.6, it is sufficient to show that \( \Theta \parallel \mathcal{J} \) is locally characteristic in \( \mathcal{L}_p \) for all dyadic primes \( p \). But the proof is identical to that of Proposition 2.7.1. Q.E.D.

3.1.15 **Lemma:** If \( \phi: \mathcal{J}_i \rightarrow \mathcal{L}_j \) is an isometric embedding such that \( \mathcal{L}_j \) contains a minimal vector \( e \) perpendicular to \( \phi(\mathcal{J}_i) \), then \( \phi \) can be extended to an isometry of \( \mathcal{L}_i \) onto \( \mathcal{L}_j \).

In particular, \( i = j \).

**Proof:** Obvious by Lemma 3.1.14.

3.1.16 **Theorem:** The generalized theta series \( \Theta_{\mathcal{L}}^{(2)}(\mathbb{Z}) \) of degree 2 for lattices \( \mathcal{L} \) coming from the distinct classes in \( \mathcal{J}(4,1) \) are linearly independent.

**Proof:** Let \( \mathcal{L}_i, e_i, \mathcal{J}_i, d \mathcal{J}_i = p_i \) and \( q_i = \Theta_{\mathcal{L}_i} \) be as above. Denote by \( 2^{n_i} \) the exact power of 2 dividing \( |O(\mathcal{L}_i)| \).

Then \( n_i = 2 \) for \( \mathcal{L}_i \) of type \( A_1 \) or \( A_2 \); \( n_i = 4 \) for type \( A_1 \oplus A_1 \) or \( A_2 \oplus A_2 \); and \( n_i = 6 \) for type \( D_4 \). It is clear that \( O(\mathcal{L}_j) \) acts on the set of isometric embeddings of \( \mathcal{J}_i \) into \( \mathcal{L}_j \). If \( \phi: \mathcal{J}_i \rightarrow \mathcal{L}_j \) is any isometric embedding, then the number of elements in the \( O(\mathcal{L}_j) \)-orbit of \( \phi \) is given by \( |O(\mathcal{L}_j)| / |H_\phi| \), where \( H_\phi \) is the stabilizer of \( \phi \). We want to determine the exact power of 2 in this quotient. Let \( \sigma \) be an element of
order 2 in $H^\sigma$, i.e. $\sigma$ is an involution. By 42:14 [OM], there is a splitting $\nu = u \perp \Sigma$ for which $\sigma = -1_u \perp 1_\nu$.

We consider the following cases.

Case (i). If $\dim \nu = 3$, then $\sigma$ is a symmetry of $\Sigma_j$; hence, by Proposition 3.1.12, there is a minimal vector $e$ in $\Sigma_j$ such that $\sigma = S_e$. Since $e \perp \phi(\theta_1)$, we have $i = j$ and $\phi$ lies in the orbit of the inclusion map by Lemma 3.1.15.

Case (ii). If $\dim \nu = 2$, then $\nu = F(\phi(\theta_1))$. Let $X$ be the orthogonal complement of $\phi(\theta_1)$ in $\Sigma_j$. We have

$$\left(\Sigma_j\right)_{q_i} \supset \left(\phi(\theta_1)\right)_{q_i} \perp x_{q_i} = q_i u \perp q_i v \perp q_i x \perp q_i y,$$

where $\phi(\theta_1)_{q_i} = q_i u \perp q_i v$, $x_{q_i} = q_i x \perp q_i y$

$Q(u), Q(x) \in \Sigma_{q_i}$, and $Q(v) Q(y) \in \Sigma_{q_i} u_q_i$. It follows that

$$\left(\Sigma_j\right)_{q_i} = \left(\phi(\theta_1)\right)_{q_i} \perp x_{q_i} + q_i d_{q_i} (v + ay)$$

for some $d \in \Sigma_{q_i}$. Since $\sigma \Sigma_j = \Sigma_j$, we have $\left(\Sigma_j\right)_{q_i} = \left(\phi(\theta_1)\right)_{q_i} \perp x_{q_i} + q_i d_{q_i} (v - ay)$ also. Thus, $\frac{2v}{q_i} \in \Sigma_j$. But this is impossible, since $\Sigma_{q_i} Q(v)$.

We have therefore determined the exact power of 2 in

$\left| \sigma(\Sigma_j) \right| / \left| H^\sigma \right|$

<table>
<thead>
<tr>
<th>Type of $\Sigma_j$</th>
<th>When $i = j$ and $\phi$ lies in the orbit of the inclusion</th>
<th>When $i \neq j$ or $\phi$ does not lie in the orbit of inclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_1$ or $A_2$</td>
<td>$2^1$</td>
<td>$2^2$</td>
</tr>
<tr>
<td>$A_1 \oplus A_1$</td>
<td>$2^3$</td>
<td>$2^4$</td>
</tr>
<tr>
<td>$A_2 \oplus A_2$</td>
<td></td>
<td>$2^6$</td>
</tr>
<tr>
<td>$D_4$</td>
<td>$2^5$</td>
<td></td>
</tr>
</tbody>
</table>
Let $a_{ij}$ be the number of isometric embeddings of $g_i$ into $\mathcal{L}_j$.

It follows that if the type of $\mathcal{L}_j$ is $A_1$ or $A_2$, then

$$a_{ij} \equiv 0 \pmod{2^2} \text{ for } i \neq j,$$

$$a_{jj} \equiv 0 \pmod{2}, \ a_{jj} \neq 0 \pmod{2^2};$$

if the type of $\mathcal{L}_j$ is $A_1 \oplus A_1$ or $A_2 \oplus A_2$, then we have

$$a_{ij} \equiv 0 \pmod{2^4} \text{ for } i \neq j,$$

$$a_{jj} \equiv 0 \pmod{2^3}, \ a_{jj} \neq 0 \pmod{2^4};$$

if the type of $\mathcal{L}_j$ is $D_4$, we have

$$a_{ij} \equiv 0 \pmod{2^6} \text{ for } i \neq j,$$

$$a_{jj} \equiv 0 \pmod{2^5}, \ a_{jj} \neq 0 \pmod{2^6}.$$

Now let $\sum c_j \Theta^{(2)}_{\mathcal{L}_j}(z) = 0$, $c_j \in \mathbb{C}$, be a nontrivial linear relation. Again, since the generalized theta series of degree 2 are integral automorphic forms, it suffices to show that they are linearly independent over $\mathbb{Z}$. Hence, we may assume that the $c_j$'s are relatively prime integers. By evaluating this linear relation at each $g_i$, we obtain

$$\sum c_j a_{ij} = 0.$$ We consider this equation modulo various congruences:

$$\text{mod } 2^2 \Rightarrow c_j \equiv 0 \pmod{2} \text{ for } n_j = 2 \text{ (i.e. for } \mathcal{L}_j \text{ with type } A_1 \text{ or } A_2);$$

$$\text{mod } 2^3 \Rightarrow c_j \equiv 0 \pmod{2^2} \text{ for } n_j = 2.$$
mod $2^4 \Rightarrow c_j \equiv 0 \pmod{2}$ for $n_j = 4$ ($\mathcal{L}_j$ of type $A_1 \oplus A_1$ or $A_2 \oplus A_2$);

$\Rightarrow c_j \equiv 0 \pmod{2^3}$ for $n_j = 2$;

mod $2^5 \Rightarrow c_j \equiv 0 \pmod{2^2}$ for $n_j = 4$,

$\Rightarrow c_j \equiv 0 \pmod{2^4}$ for $n_j = 2$;

mod $2^6 \Rightarrow c_j \equiv 0 \pmod{2}$ for $n_j = 6$ ($\mathcal{L}_j$ of type $D_4$).

This is a contradiction; therefore, our proof is complete.

Q.E.D.

3.1.17 Corollary: Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be any two lattices in $\mathcal{S}'(4, 1)$. Then $\mathcal{L}_1 \cong \mathcal{L}_2$ if and only if $\Theta_{\mathcal{L}_1}^{(2)}(Z) \equiv \Theta_{\mathcal{L}_2}^{(2)}(Z)$ (mod 16). In particular, $\mathcal{L}_1 \cong \mathcal{L}_2$ if and only if $\Theta_{\mathcal{L}_1}^{(2)}(Z) = \Theta_{\mathcal{L}_2}^{(2)}(Z)$.

Proof: Since $a_{\mathcal{L}}^{(2)}(0, 0) = 2, 4, 6, 12,$ or 8 as the roots system type of $\mathcal{L}$ is $A_1$, $A_1 \oplus A_1$, $A_2$, $A_2 \oplus A_2$, or $A_3$, respectively, it is clear that $\Theta_{\mathcal{L}_1}^{(2)}(Z) \not\equiv \Theta_{\mathcal{L}_2}^{(2)}(Z)$ (mod 16) if $\mathcal{L}_1$ and $\mathcal{L}_2$ are not of the same type. If $\mathcal{L}_1$ and $\mathcal{L}_2$ are of the same type, but not equivalent, then we choose $\mathcal{G}_1$ in $\mathcal{L}_1$ according to Theorem 3.1.16. We have $a_{\mathcal{L}_1}(\mathcal{G}_1) \equiv 2, 6, 10,$ or 14 (mod 16), but $a_{\mathcal{L}_2}(\mathcal{G}_1) \equiv 0, 4, 8,$ or 12 (mod 16) if $\mathcal{L}_1$ and $\mathcal{L}_2$ are both of type $A_1$ or $A_2$. If $\mathcal{L}_1$ and $\mathcal{L}_2$ are both of type $A_1 \oplus A_1$, then $a_{\mathcal{L}_1}(\mathcal{G}_1) \equiv 8$ (mod 16), but $a_{\mathcal{L}_2}(\mathcal{G}_1) \equiv 0$ (mod 16).
In any case, \( \Theta_{S_1}(z) \neq \Theta_{S_2}(z) \) (mod 16). Therefore, \( S_1 \) and \( S_2 \) are classified by their theta series (mod 16).

Q.E.D.

§3.2 Theta Series of Degree One: Lattices of Type \( A_1 \oplus A_1 \)

We now consider lattices \( S \) in \( \mathcal{S}'(4, 1) \) of the type \( A_1 \oplus A_1 \). Let \( e_1 \) and \( e_2 \) be minimal vectors of \( S \) and \( M \) be the orthogonal complement of \( \Theta e_1 \| \Theta e_2 \) in \( S \). It is easy to see (by showing that \( d(FM) \) and \( dM_p \) are equal up to a square in \( U_p \) for each \( p \), \([K_3] \), page 97) that \( M \) is a binary free lattice of discriminant 4. \( M_p \) is proper \( p \)-modular locally at each dyadic prime \( p \) (see the proof of Proposition 3.1.6).

Apply Lemma 1.6 [HKK] to find a vector \( u \) in \( M \) and a principal prime ideal \( q = \Theta^p \) of \( F \) such that \( Q(u) = 2^p \).

(One could, for example, choose a binary free lattice \( \mathcal{G} \) in \( \kappa = (\Theta e_1)^\perp \) such that \( d\mathcal{G} = \pi \) and \( \mathcal{G} \) contains \( e_2 \) (Lemma 3.1.13). Then let \( \Theta u \) be the orthogonal complement of \( e_2 \) in \( \mathcal{G} \). The orthogonal complement of \( u \) in \( M \) is a free lattice \( \Theta v \) with \( Q(v) = 2^p \). Therefore, we have \( S \supset \Theta e_1 \| \Theta e_2 \| \Theta u \| \Theta v \). Define an isometry \( \tau \) on \( v \) by \( \tau(e_1) = e_2, \tau(e_2) = e_1, \tau(u) = u, \) and \( \tau(v) = v \).

3.2.1 Lemma: Let \( p \equiv 5 \) (mod 8), then there are exactly four lattices in \( \mathcal{S}(4, 1) \) which contain \( \Theta e_1 \| \Theta e_2 \| \Theta u \| \Theta v \), and they are transitively permuted by \( S_v \) and \( \tau \).
Proof: There is a unique dyadic prime \( \rho = (2) \). We may assume that \( \sigma_\rho e_2 \perp \sigma_\rho u \) is not maximal (see the preceding paragraph); hence, there exists a \( \epsilon \in U_\rho \) such that
\[
(\sigma_\rho e_2 \perp \sigma_\rho u \perp \sigma_\rho v) + \sigma_\rho^2 (e_2 + au) \text{ is maximal. Similarly,}
\]
\[
(\sigma_\rho e_2 \perp \sigma_\rho u \perp \sigma_\rho v) + \sigma_\rho^2 (e_2 + av) \text{ is maximal. Locally at } \rho \text{ these are the only maximal ternary lattices containing}
\]
\[
\sigma_\rho e_2 \perp \sigma_\rho u \perp \sigma_\rho v. \text{ To see this, suppose that } \Gamma_\rho \text{ is a maximal ternary lattice containing } \sigma_\rho e_2 \perp \sigma_\rho u \perp \sigma_\rho v. \text{ Since } \sigma_\rho u \perp \sigma_\rho v \text{ is already maximal (its discriminant being a square), there exist } \alpha, \beta \in \sigma_\rho \text{ such that } h(\epsilon_2 + au + \beta v) \in \Gamma_\rho. \text{ By reducing modulo } 2\sigma_\rho, \text{ we may assume that } \alpha, \beta \text{ are either } 0, 1, \gamma, \text{ or } 1 + \gamma, \text{ where } \{0, 1, \gamma, 1 + \gamma\} \text{ is a representative set of the residue class field at } \rho. \text{ We have } Q(h(\epsilon_2 + au + \beta v)) = h(2 + 2\pi \alpha^2 + 2\pi \beta^2) \in 2\sigma_\rho; \text{ hence, } 1 + \pi(\alpha^2 + \beta^2) \in 4\sigma_\rho. \pi \text{ is in the same square class as either } -1 \text{ or } -\Lambda \text{ (since } \sigma_\rho e_2 \perp \sigma_\rho u \text{ is contained in an even binary unimodular lattice); hence, we may assume that } \alpha^2 + \beta^2 = 1 \pmod{4\sigma_\rho}. \text{ But this can occur only when one of } \alpha \text{ or } \beta \text{ is } 0. \text{ Therefore, } \Gamma_\rho \text{ is equal to one of the two lattices mentioned above. For each such } \Gamma_\rho, \text{ there is a unique unimodular lattice (see the proof of Proposition 2.7.1) } \Lambda_\rho \supseteq \sigma_\rho \mathfrak{e}_1 \perp \Gamma_\rho, \text{ namely}
\]
\[
\Lambda_{1\rho} = (\sigma_\rho \mathfrak{e}_1 \perp \sigma_\rho e_2 \perp \sigma_\rho u \perp \sigma_\rho v) + \sigma_\rho^2 (e_2 + au) + \sigma_\rho^2 (e_1 + av),
\]
\[
\Lambda_{2\rho} = (\sigma_\rho \mathfrak{e}_1 \perp \sigma_\rho e_2 \perp \sigma_\rho u \perp \sigma_\rho v) + \sigma_\rho^2 (e_1 + au) + \sigma_\rho^2 (e_2 + av). \]
It is clear that \( \Lambda_{1\rho} \) and \( \Lambda_{2\rho} \) are permuted by the isometry }
At the prime $q$, $\varrho^q u \perp \varrho^q v$ is not maximal by its construction, so there exists $b \in U_q$ such that $\Lambda_{1q} = (\varrho^q e_1 \perp \varrho^q e_2 \perp \varrho^q u \perp \varrho^q v) + \varrho^\frac{1}{q}(u + bv)$ is unimodular. Similarly, $\Lambda_{2q} = (\varrho^q e_1 \perp \varrho^q e_2 \perp \varrho^q u \perp \varrho^q v) + \varrho^\frac{1}{q}(u - bv)$ is unimodular. If $\Lambda_q$ is any unimodular lattice containing $\varrho^q e_1 \perp \varrho^q e_2 \perp \varrho^q u \perp \varrho^q v$, then $\Lambda_q$ must contain a vector $\frac{1}{q}(u + cv)$ for some $c \in U_q$. Since $1 + b^2$ and $1 + c^2$ both belong to $\pi \varrho_q$, we have $c = b$ or $-b$ (mod $\pi \varrho_q$). Hence, $\Lambda_q$ is equal to one of $\Lambda_{1q}$ or $\Lambda_{2q}$.

$\Lambda_{1q}$ and $\Lambda_{2q}$ are permuted by the symmetry $S_v$. By lattice theory, there are four global lattices in $\mathcal{G}(4, 1)$ containing $\varrho^q e_1 \perp \varrho^q e_2 \perp \varrho^q u \perp \varrho^q v$. They are defined by $(\mathcal{L}_i)_\varpi = \varrho^q e_1 \perp \varrho^q e_2 \perp \varrho^q u \perp \varrho^q v$ for all $\varpi \neq \varrho, q$, $i = 1, 2, 3, 4$, and

$$
(\mathcal{L}_1)_\varpi = \begin{cases} 
\Lambda_{1\rho} & \varpi = \rho \\
\Lambda_{1q} & \varpi = q
\end{cases} \quad \quad (\mathcal{L}_2)_\varpi = \begin{cases} 
\Lambda_{1\rho} & \varpi = \rho \\
\Lambda_{2q} & \varpi = q
\end{cases} 
$$

$$
(\mathcal{L}_3)_\varpi = \begin{cases} 
\Lambda_{2\rho} & \varpi = \rho \\
\Lambda_{1q} & \varpi = q
\end{cases} \quad \quad (\mathcal{L}_4)_\varpi = \begin{cases} 
\Lambda_{2\rho} & \varpi = \rho \\
\Lambda_{2q} & \varpi = q
\end{cases} 
$$

It is easy to see that these four lattices are permuted by $S_v$ and $\tau$.

Q.E.D.

3.2.2 Remark: If $p \equiv 1$ (mod 8), then there are two dyadic primes $\rho_1$ and $\rho_2$ in $F$. Locally at each $\varrho_i$, there are two unimodular lattices $\Lambda_{1\rho_i}$ and $\Lambda_{2\rho_i}$ containing $\varrho^q e_1 \perp \varrho^q e_2 \perp \varrho^q u \perp \varrho^q v$. Hence, there are eight global lattices in...
A lattice of type $A_1 \oplus A_1$ such that $A \equiv A e_1 \perp A e_2 \perp A u \perp A v$ (where $e_1$ and $e_2$ are minimal vectors, $Q(u) = Q(v) = 2\pi$, and $q = \pi\sigma$ is a principal prime ideal). Then $O(A) = \langle S e_1^\sigma, S e_2^\sigma, \sigma \rangle \cong (C_2 \times C_2) \rtimes C_4$, where $S_{e_1}^\sigma = S_{e_2}$ and $\sigma$ is defined by $\sigma(e_1) = e_2$, $\sigma(e_2) = e_1$, $\sigma(u) = v$, and $\sigma(v) = -u$. 

One can show easily that $L_1$, $L_2$, $L_3$, and $L_4$ (and $L_5$, $L_6$, $L_7$, and $L_8$, respectively) are permuted by $S_v$ and $\tau$.
Proof: We will show that \( \sigma \in O(\mathcal{I}) \). It suffices to show that \( \sigma \mathcal{I}_P = \mathcal{I}_P \) for any dyadic prime \( P \) and \( \sigma \mathcal{I}_q = \mathcal{I}_q \).

Assume that \( \mathcal{I}_P = \Lambda_1 P = (\Theta^e_1 \perp \Theta^e_2 \perp \Theta^u \perp \Theta^v) + \Theta^u \perp (e_2 + au) \) + \Theta^v \perp (e_1 + av) \). Then we have \( \sigma \mathcal{I}_P = (\Theta^e_2 \perp \Theta^e_1 \perp \Theta^v \perp \Theta^u \perp (u)) + \Theta^v \perp (e_1 + av) + \Theta^u \perp (e_2 - au) \). It is clear that \( \sigma \mathcal{I}_P = \mathcal{I}_P \). Similarly for \( \mathcal{I}_q = \Lambda_2 q \). At the prime \( q \), we assume that \( \mathcal{I}_q = \Lambda_1 q = (\Theta^e_1 \perp \Theta^e_2 \perp \Theta^u \perp \Theta^v) + \Theta^u \perp (u + bv) \).

Then \( \sigma \mathcal{I}_q = (\Theta^e_2 \perp \Theta^e_1 \perp \Theta^v \perp \Theta^u \perp (u)) + \Theta^v \perp (v - bu) \).

Now \( \frac{1}{b^2}(v - bu) = \frac{1}{b^2}(bv - b^2u) = \frac{1}{b^2}(u + bv) - \frac{1}{b^2}(1 + b^2)u \).

Since \( 1 + b^2 \in \pi \Theta_q \), we have \( \frac{1}{b^2}(1 + b^2)u \) already lies in \( (\Theta^e_2 \perp \Theta^e_1 \perp \Theta^u \perp \Theta^v) \); hence \( \sigma \mathcal{I}_q = \mathcal{I}_q \). Similarly for \( \mathcal{I}_q = \Lambda_2 q \).

It follows, therefore, that \( \sigma \in O(\mathcal{I}) \). It is easy to see that \( O(\mathcal{I}) \) is generated by \( S_i, S_{e_2} \), and \( \sigma \) (see Corollary 3.1.11).

Q.E.D.

3.2.4 Theorem: Let \( p \equiv 5 \pmod{8} \), then the generalized theta series \( \Theta_\mathcal{I}(Z) \) of degree one for lattices \( \mathcal{I} \) coming from distinct classes in \( \mathcal{E}(4, 1) \) of type \( A_1 \oplus A_1 \) are linearly independent.

Proof: Let \( \mathcal{I}_1, \ldots, \mathcal{I}_h \) be a full set of nonisometric lattices in \( \mathcal{E}(4, 1) \) of type \( A_1 \oplus A_1 \). For each \( i \), let \( q_i = \pi_i \Theta \) be a prime ideal such that \( \mathcal{I}_i \supset \Theta e_{1i} \perp \Theta e_{2i} \perp \Theta u_i \perp \Theta v_i \), where \( e_{1i} \) and \( e_{2i} \) are minimal vectors and \( Q(u_i) = Q(v_i) = 2\pi_i \).

Put \( \mathcal{J}_i = \Theta u_i \). If \( \phi: \mathcal{J}_i \rightarrow \mathcal{J}_j \) is any isometric embedding such
that \( \mathfrak{L}_j \) contains minimal vectors \( e_1 \) and \( e_2 \) with \( \phi(e_1) = e_1 \cdot \phi(e_2) = e_2 \cdot \phi_0 \), then by Lemma 3.2.1, \( \phi \) can be extended to an isometry from \( \mathfrak{L}_i \) onto \( \mathfrak{L}_j \). In particular, \( i = j \). Consider the \( O(\mathfrak{L}_j) \)-orbit of any isometric embedding \( \phi: \mathfrak{L}_i \rightarrow \mathfrak{L}_j \). The number of elements in the orbit of \( \phi \) is \( \frac{|O(\mathfrak{L}_j)|}{|H_\phi|} \). Since \( O(\mathfrak{L}_j) \) is generated by \( S_{e_1j}, S_{e_2j}, \sigma_j, \) and \( \dagger \) (see Corollary 3.2.3), it is easy to see that the \( 2 \)-power in \( |H_\phi| \) is at most \( 2^1 \), unless \( \phi \) lies in the orbit of the inclusion map, in which case the exact power of 2 dividing \( |H_\phi| \) is \( 2^2 \). Hence, we have

\[
\frac{|O(\mathfrak{L}_j)|}{|H_\phi|} \equiv 0 \pmod{2^3}
\]

for any \( \phi \neq \dagger \) orbit of inclusion, whereas

\[
\frac{|O(\mathfrak{L}_j)|}{|H_\alpha|} \equiv 0 \pmod{2^2}, \quad \text{but} \quad \neq 0 \pmod{2^3},
\]

where \( \alpha \) is the inclusion map.

Let \( a_{ij} \) be the number of isometric embeddings of \( \mathfrak{L}_i \) into \( \mathfrak{L}_j \). It is clear that

\[
a_{ij} \equiv 0 \pmod{2^3} \quad \text{for} \quad i \neq j,
\]

\[
a_{jj} \equiv 0 \pmod{2^2}, \quad \text{but} \quad \neq 0 \pmod{2^3}.
\]

Hence, if \( \sum c_j \phi_j(z) = 0 \) is an integral linear relation with relatively prime coefficients \( c_j \)'s, we may evaluate it at each \( \mathfrak{L}_i \) and consider the equation \( \sum c_j a_{ij} = 0 \) modulo \( 2^3 \). One sees readily that \( c_j \equiv 0 \pmod{2} \) for all \( j \), and this is a contradiction. 

Q.E.D.
3.2.5 Corollary: Let \( p \equiv 5 \pmod{8} \) and \( L_1 \) and \( L_2 \) be two lattices in \( \mathbf{H}'(4,1) \) of the type \( A_1 \oplus A_1 \). Then \( L_1 \cong L_2 \) if and only if \( \Theta_{\mathbf{L}_1}(z) \equiv \Theta_{\mathbf{L}_2}(z) \pmod{8} \). Hence, \( L_1 \) and \( L_2 \) are isometric if and only if they have the same theta series.

3.2.6 Remark: If \( p \equiv 1 \pmod{8} \), then the proof of Theorem 3.2.4 would yield the independence for only half the classes of type \( A_1 \oplus A_1 \) (see Remark 3.2.2).

§3.3 Theta Series of Degree One: Lattices of Type \( A_2 \)

Let \( \mathbf{L} \in \mathbf{H}'(4,1) \) be a lattice of type \( A_2 \), then \( \mathbf{L} \) contains a sublattice \( \mathfrak{R} = \mathfrak{L}e_1 + \mathfrak{L}e_2 \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \). Let \( \mathfrak{J} \) be the orthogonal complement of \( \mathfrak{R} \) in \( \mathbf{L} \). It is easy to see (Proposition [K3], page 97) that \( \mathfrak{J} \) is a binary free lattice of discriminant 3. Apply Lemma 1.6 [HKK] to find a principal ideal \( q = \pi \mathfrak{L} \) such that \( \mathfrak{J} \) contains a vector \( u_1 \) with \( Q(u_1) = 2\pi \). The orthogonal complement of \( \mathfrak{L}u_1 \) in \( \mathfrak{J} \) is a free lattice \( \mathfrak{L}v \) such that \( Q(v) = 6\pi \). Let \( p \) be any dyadic prime in \( F \). Clearly, \( \mathfrak{L}u_1 + \mathfrak{L}v \) is not maximal; hence, it is contained in a binary unimodular lattice. This unimodular lattice is unique (see the proof of Proposition 2.7.1) and so must be \( \mathfrak{J}_p \). Let \( u_2 = \tfrac{1}{2}(u_1 - v) \). It is easy to see that \( \mathfrak{L}u_1 + \mathfrak{L}u_2 \) is a unimodular lattice containing \( \mathfrak{L}u_1 + \mathfrak{L}v \); hence, it is identical to \( \mathfrak{J}_p \). Since \( u_2 \in \mathfrak{J}_p \) for all finite
primes \( \mathfrak{p} \), we have \( u_2 \in \mathcal{J} \); hence \( \mathbb{R} \supset \mathbb{R} \cap \mathbb{R} \perp (\mathfrak{p} u_1 + \mathfrak{p} u_2) \cong (2 \ 1) \perp \begin{pmatrix} 2 \pi & \pi \\ \pi & 2 \pi \end{pmatrix} (2 \ 1) \).

3.3.1 Lemma: Let \( p \equiv 2 \pmod{3} \). There are exactly four lattices in \( \mathcal{O} (4, 1) \) containing \( \mathbb{R} \perp \mathfrak{p} u_1 \perp \mathfrak{p} v \), and they are transitively permuted by \( S_v \) and the isometry \( \rho \) defined by

\[
\rho e_1 = e_1, \quad \rho e_2 = e_2, \quad \rho u_1 = -u_1, \quad \text{and} \quad \rho v = -v.
\]

Proof: The orthogonal complement of \( \mathfrak{p} e_1 \) in \( \mathbb{R} \) is \( \mathfrak{p} f \), where \( f = e_1 - 2e_2 \). We have already seen that, at any dyadic prime \( \mathfrak{p} \), there is only one unimodular lattice containing

\( \mathbb{R} \perp \mathfrak{p} u_1 \perp \mathfrak{p} v \), namely, the lattice \( \mathbb{R} \perp \mathfrak{p} u_1 + \mathfrak{p} v \).

At the prime \( q \), there are two unimodular lattices containing

\( \mathbb{R} \perp \mathfrak{q} u_1 \perp \mathfrak{q} v \). They are

\[
\Lambda_1(q) = (\mathbb{R} \perp \mathfrak{q} u_1 \perp \mathfrak{q} v) + \mathfrak{q} \frac{1}{\pi} (u_1 + av)
\]

and

\[
\Lambda_2(q) = (\mathbb{R} \perp \mathfrak{q} u_1 \perp \mathfrak{q} v) + \mathfrak{q} \frac{1}{\pi} (u_1 - av),
\]

where \( a \) is some unit in \( \mathfrak{q} \) satisfying \( 1 + 3a^2 \in \pi \mathfrak{q} \).

Similarly, if \( \mathfrak{f} = (3) \) is the unique prime in \( \mathfrak{p} \) dividing 3, then there are two unimodular lattices containing \( \mathbb{R} \perp \mathfrak{f} u_1 \perp \mathfrak{f} v \):

\[
\Lambda_1(f) = (\mathbb{R} \perp \mathfrak{f} u_1 \perp \mathfrak{f} v) + \mathfrak{f} \frac{1}{3} (f + bv)
\]

and

\[
\Lambda_2(f) = (\mathbb{R} \perp \mathfrak{f} u_1 \perp \mathfrak{f} v) + \mathfrak{f} \frac{1}{3} (f - bv),
\]

where \( b \) is some unit in \( \mathfrak{f} \) satisfying \( 1 + b^2 \in 3 \mathfrak{f} \). It follows that there are four global lattices in \( \mathcal{O}(4, 1) \) containing \( \mathbb{R} \perp \mathfrak{f} u_1 \perp \mathfrak{f} v \):
\[(S_1)_\mathfrak{p} = \mathfrak{p} \perp (\mathfrak{p}_1 u_1 + \mathfrak{p}_2 u_2) \text{ for } \mathfrak{p} \neq q, \; i = 1, 2, 3, 4,\]

\[(S_2)_\mathfrak{p} = \begin{cases} \Lambda_1 q & \mathfrak{p} = q \\ \Lambda_1 f_1 & \mathfrak{p} = f_1 \\ \Lambda_1 f_2 & \mathfrak{p} = f_2 \end{cases}, \quad (S_3)_\mathfrak{p} = \begin{cases} \Lambda_2 q & \mathfrak{p} = q \\ \Lambda_2 f_1 & \mathfrak{p} = f_1 \\ \Lambda_2 f_2 & \mathfrak{p} = f_2 \end{cases}, \quad (S_4)_\mathfrak{p} = \begin{cases} \Lambda_2 q & \mathfrak{p} = q \\ \Lambda_2 f_1 & \mathfrak{p} = f_1 \\ \Lambda_2 f_2 & \mathfrak{p} = f_2 \end{cases} \]

It is easy to see that \(S_\nu S_1 = S_4, \; \rho S_1 = S_2, \; \text{and} \; S_\nu S_2 = S_3;\)

hence, \(S_1, S_2, S_3, \) and \(S_4\) are permuted transitively by \(S_\nu \) and \(\rho.\)

**Q.E.D.**

3.3.2 Remark: If \(p = 1 \text{ (mod 3)},\) then there are two primes \(f_1 \) and \(f_2 \) in \(F\) such that \((3) = f_1 f_2.\) At each \(f_i,\) there exist two unimodular lattices \(\Lambda_1 f_i \) and \(\Lambda_2 f_i \) containing \(\mathfrak{p} \perp \mathfrak{p}_1 u_i \perp \mathfrak{u}_1 f_i.\) Hence, there are eight global lattices in \(\tilde{J}(4, 1)\)

\[(S_1)_\mathfrak{p} = \mathfrak{p} \perp (\mathfrak{p}_1 u_1 + \mathfrak{p}_2 u_2) \text{ for } \mathfrak{p} \neq q, \; f_1, \; f_2, \; 1 \leq i \leq 8,\]

\[(S_2)_\mathfrak{p} = \begin{cases} \Lambda_1 q & \mathfrak{p} = q \\ \Lambda_1 f_1 & \mathfrak{p} = f_1 \\ \Lambda_1 f_2 & \mathfrak{p} = f_2 \end{cases}, \quad (S_3)_\mathfrak{p} = \begin{cases} \Lambda_2 q & \mathfrak{p} = q \\ \Lambda_2 f_1 & \mathfrak{p} = f_1 \\ \Lambda_2 f_2 & \mathfrak{p} = f_2 \end{cases}, \quad (S_4)_\mathfrak{p} = \begin{cases} \Lambda_2 q & \mathfrak{p} = q \\ \Lambda_2 f_1 & \mathfrak{p} = f_1 \\ \Lambda_2 f_2 & \mathfrak{p} = f_2 \end{cases} \]
One sees readily that $\mathcal{L}_1$, $\mathcal{L}_2$, $\mathcal{L}_3$, and $\mathcal{L}_4$ (and $\mathcal{L}_5$, $\mathcal{L}_6$, $\mathcal{L}_7$, and $\mathcal{L}_8$, respectively) are permuted by $S_v$ and $\rho$.

3.3.3 Corollary: Let $p$ be a prime $\equiv 1$ modulo 4. Let $\mathcal{L} \in \mathcal{S}'(4, 1)$ be a lattice of type $A_2$ such that $\mathcal{L} \supset H \cup (\Theta u_1 + \Theta u_2) \supset H \cup \Theta u_1 + \Theta v$, where $H = \Theta e_1 + \Theta e_2 \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, $\Theta u_1 + \Theta u_2 \cong \begin{pmatrix} 2\pi & \pi \\ \pi & 2\pi \end{pmatrix}$, and $v = u_1 - 2u_2$, then $O(\mathcal{L}) = \langle S_{e_1}, S_{e_2}, S_{e_1-e_2} \rangle \times \langle -S_{u_1}S_{u_2} \rangle \cong S_3 \times C_6$.

Proof: We first show that $S_{u_1}S_{u_2} \in O(\mathcal{L})$. Since $\mathcal{L}_p = \mathcal{L}_p \cup (\Theta_{q}u_1 + \Theta_{q}u_2)$ for all $p$ not dividing 3 and $p \neq q$, it is clear that $S_{u_1}S_{u_2} \mathcal{L}_p = \mathcal{L}_p$. If $p = q$, we assume that $\mathcal{L}_q = \Lambda_1q = (\mathcal{L}_q \cup (\Theta_{q}u_1 + \Theta_{q}u_2)) + \Theta_{q} \frac{1}{\pi}(u_1 + av)$ (the proof is similar if $\mathcal{L}_q = \Lambda_2q$). We have

$$S_{u_1}S_{u_2} \mathcal{L}_q = (\mathcal{L}_q \cup (\Theta_{q}u_1 + \Theta_{q}u_2)) + \Theta_{q} \frac{1}{\pi}(-u_2 + a(u_2 - 2u_1)).$$
We claim that $\frac{1}{\pi}(-u_2 + a(u_2 - 2u_1)) \in \mathbb{L}_q$. To see this, we compute

$$\frac{1}{\pi}(u_1 + av) - \frac{1}{\pi}(-u_2 + a(u_2 - 2u_1))$$

$$= \frac{1}{\pi}\left((u_1 + u_2) + 3a(u_1 - u_2)\right)$$

$$= \frac{1}{\pi}\left((-u_1 + u_2) + 3a^2(u_1 - u_2) + (u_1 - u_2) - (u_1 - u_2)\right)$$

$$= \frac{1}{\pi}\left((-1)u_1 + (a + 1)u_2 + (1 + 3a^2)(u_1 - u_2)\right)$$

Since $1 + 3a^2 \in \mathbb{Q}_q$, it is enough to show that

$$\frac{1}{\pi}\left((-1)u_1 + (a + 1)u_2\right) \in \mathbb{L}_q.$$ 

We have

$$\frac{1}{\pi}\left((-1)u_1 + (a + 1)u_2\right) = \frac{1}{\pi}\left((-1)u_1 + (a + 1)\frac{1}{2}(u_1 - v)\right)$$

$$= \frac{1}{2\pi}\left(2(-1)u_1 + (a + 1)(u_1 - v)\right)$$

$$= \frac{1}{2\pi}\left(3au_1 - v - (u_1 + av)\right)$$

Again, since $\frac{1}{2\pi}(u_1 + av) \in \mathbb{L}_q$, it suffices to show that

$$\frac{1}{2\pi}(3au_1 - v) \in \mathbb{L}_q.$$ 

But

$$\frac{1}{2\pi}(3au_1 - v) = \frac{1}{2\pi}(3a^2u_1 - av)$$

$$= \frac{1}{2\pi}\left((1 + 3a^2)u_1 - (u_1 + av)\right) \in \mathbb{L}_q;$$

hence, our claim is proved. Next, we show that $S_{u_1 u_2} \mathbb{L}_q = \mathbb{L}_q$ for any prime $\mathfrak{p}$ dividing 3. Again, we assume that $\mathbb{L}_q = \Lambda_{\mathfrak{p}} = \mathfrak{p}^{-1}(\mathfrak{p}u_1 + \mathfrak{p}u_2) + \mathfrak{p}^{-1/3}(f + bv)$, then

$$S_{u_1 u_2} \mathbb{L}_q = \mathfrak{p}^{-1}(\mathfrak{p}u_1 + \mathfrak{p}u_2) + \mathfrak{p}^{-1/3}(f + b(u_2 - 2u_1)).$$

Since $\frac{1}{3}(f + b(u_2 - 2u_1)) = \frac{1}{3}(f + bv) - b(u_1 - u_2) \in \mathbb{L}_q$, 

it is clear that $S_{u_1} S_{u_2} \Lambda_1 = \Lambda_1$. The proof is identical if
$\Lambda_1 = \Lambda_2$. Hence, we have proved that $S_{u_1} S_{u_2} \in O(\Lambda)$. One
can show easily by a routine calculation that $S_{e_1}, S_{e_2}, S_{e_1-e_2}, S_{u_1} S_{u_2}$,
and $e_1$ generate group of order 36. Since
$|O(\Lambda)| = 36$ by Corollary 3.1.11, it follows that $O(\Lambda)$ is
generated by the above isometries. Q.E.D.

Assume now that $p = 2 \pmod{3}$, and let $\Lambda_1, \ldots, \Lambda_h$ be
a full set of nonisometric lattices in $\Lambda'(4, 1)$ of the type
$A_2$. For each $i$, let $\Lambda_i \subseteq A(2, 2)$ be the roots system of $\Lambda_i$.
Choose $\mathcal{R}_i = \mathcal{W}_{u_1}$ in the orthogonal complement $\mathcal{T}_i$ of $\Lambda_i$ in $\Lambda_i$
such that $Q(u_1) = 2^{\tau_1}$. The following lemma is immediate
from Lemma 3.3.1.

3.3.4 Lemma: Let $\phi: \mathcal{R}_i \to \mathcal{R}_j$ be an isometric embedding of $\mathcal{R}_i$
into $\mathcal{R}_j$ such that $\mathcal{R}_j$ contains a roots system $\mathcal{R}$ perpendicular
to $\phi(\mathcal{R}_i)$, then $\phi$ can be extended to an isometry from $\mathcal{R}_i$ onto
$\mathcal{R}_j$. In particular, $i = j$.

If $\phi$ is any isometric embedding of $\mathcal{R}_i$ into $\mathcal{R}_j$, then the
number of elements in the $O(\mathcal{R}_j)$-orbit of $\phi$ is equal to
$|O(\mathcal{R}_j)| / |H_\phi|$, where $H_\phi$ is the stabilizer of $\phi$.

3.3.5 Lemma: There are no elements of order 3 in $H_\phi$ unless
$\phi$ lies in the orbit of the inclusion map ($i = j$).
Proof: The only elements of order 3 in $O(\mathfrak{L}_j)$ are

$\pm e_1 e_2', \pm e_2 e_1', \pm u_1 u_2', \pm u_2 u_1', \pm e_1 e_2 u_1 u_2', \pm e_2 e_1 u_1 u_2$, All except $u_1 u_2', u_2 u_1', e_1 e_2', e_2 e_1$ do not have fixed space.

Now if $u_1 u_2$ or $u_2 u_1 \notin H_\phi$, then we would have $\phi(\mathfrak{L}_i) \notin \mathfrak{R}_j$, which is impossible, since $\mathfrak{L}_i$ was chosen to be characteristic in $\mathfrak{L}_i$. If $e_1 e_2$ or $e_2 e_1 \notin H_\phi$, then $\phi(\mathfrak{L}_i) \perp \mathfrak{R}_j$; hence, by Lemma 3.3.4, $\mathfrak{L}_i = \mathfrak{L}_j (i = j)$, and $\phi$ is in the orbit of the inclusion map. Q.E.D.

3.3.6 Theorem: Let $p \equiv 2 \pmod{3}$, then the generalized theta series $\Theta_{\mathfrak{L}}(z)$ of degree one for lattices $\mathfrak{L}$ coming from distinct classes in $\mathfrak{L}'(4, 1)$ of the type $A_2$ are linearly independent.

Proof: Let $a_{ij}$ be the number of isometric embeddings of $\mathfrak{L}_i$ into $\mathfrak{L}_j$, then by Lemma 3.3.5, we have

\[
\begin{align*}
    a_{ij} &\equiv 0 \pmod{3^2} \text{ for } i \neq j, \\
    a_{jj} &\equiv 0 \pmod{3}, \text{ but } a_{jj} \neq 0 \pmod{3^2}.
\end{align*}
\]

If $\sum c_j \Theta_{\mathfrak{L}_j}(z) = 0$ is an integral linear relation with relatively prime coefficients $c_j$, then we evaluate it at each $\mathfrak{L}_i$ to get $\sum c_j a_{ij} = 0$. By taking this equation modulo $3^2$, we obtain $c_j \equiv 0 \pmod{3}$ for all $j$, which is a contradiction. Q.E.D.
3.3.7 Corollary: Let \( p \equiv 2 \pmod{3} \) and \( \mathcal{L}_1 \) and \( \mathcal{L}_2 \) be two lattices in \( \mathcal{G}'(4, 1) \) of the type \( A_2 \). Then \( \mathcal{L}_1 \cong \mathcal{L}_2 \) if and only if \( \Theta_1(Z) \equiv \Theta_2(Z) \pmod{3} \). Hence, \( \mathcal{L}_1 \) and \( \mathcal{L}_2 \) are classified by their theta series.

3.3.8 Remark: If \( p \equiv 1 \pmod{3} \), then our method yields only the linear independence for half the classes of type \( A_2 \) (see Remark 3.3.2).

Corollary 3.2.3 yields the following general result.

3.3.9 Lemma: Let \( \mathcal{L} \) be any lattice in \( \mathcal{G}'(4, 1) \), then the minimal vectors in \( \mathcal{L} \) are transitively permuted by its automorphism group \( O(\mathcal{L}) \).

Proof: Let \( e_1 \) and \( e_2 \) be any two minimal vectors in \( \mathcal{L} \). If \( B(e_1, e_2) = 0 \), then the automorphism \( \sigma \) as defined in Corollary 3.2.3 permutes \( e_1 \) and \( e_2 \). If \( B(e_1, e_2) \neq 0 \), then we may assume that \( B(e_1, e_2) = 1 \). Clearly, \( S_{e_1-e_2} \) permutes \( e_1 \) and \( e_2 \). Q.E.D.

§3.4 Theta Series of Ternary Lattices

The rest of this chapter is devoted to a study of even ternary lattices \( \mathcal{X} \) over \( \mathcal{O} \) on a space of discriminant 2 such that \( \mathcal{X}_p \) is unimodular at all non-dyadic primes \( p \) and \( d\mathcal{X}_p = 2 \) for dyadic primes. Such lattices \( \mathcal{X} \) are free by Proposition [\( [K_3] \), page 97, and belong to the same genus \( \mathcal{G}(3, 2) \). For
each $\kappa \in \mathcal{J}(3, 2)$, one can construct by the method of Proposition 2.7.1 a unique quaternary lattice $\mathcal{L}$ in $\mathcal{J}'(4, 1)$ containing $\Theta \mathcal{L} \perp \kappa$, where $\mathcal{L}$ is a minimal vector. Conversely, if $\mathcal{L} \in \mathcal{J}'(4, 1)$ and $\mathcal{L}$ is a minimal vector in $\mathcal{L}$, then $\kappa = (\Theta \mathcal{L})^\perp \in \mathcal{J}(3, 2)$. By Lemma 3.3.9, the mapping $\kappa \mapsto \mathcal{L} \supset \Theta \mathcal{L} \perp \kappa$ induces a one-to-one correspondence between classes in $\mathcal{J}(3, 2)$ and classes in $\mathcal{J}'(4, 1)$. The type of roots system of $\kappa$ can be easily determined by the type of the corresponding lattice $\mathcal{L}$. Namely, $\kappa$ is of type $\emptyset$, $A_1$, $A_2$, or $A_1 \oplus A_1 \oplus A_1$ as the type of $\mathcal{L}$ is $A_1$ or $A_2$, $A_1 \oplus A_1$, $A_2 \oplus A_2$, or $D_4$, respectively.

3.4.1 Proposition: Let $\kappa \in \mathcal{J}(3, 2)$ and $\mathcal{L} \supset \Theta \mathcal{L} \perp \kappa$ the corresponding lattice in $\mathcal{J}'(4, 1)$, then $|O(\kappa)| = \sqrt{|O(\mathcal{L})|}$.

Proof: By Lemma 3.2.9, $O(\mathcal{L})$ permutes the minimal vectors of $\mathcal{L}$, hence, if $e'$ is any minimal vector in $\mathcal{L}$, then there exists $\sigma \in O(\mathcal{L})$ such that $\sigma e = e'$ and $\sigma \kappa = \kappa'$, where $\kappa' = (\Theta e')^\perp$. Conversely, if $\eta$ is any isometry of $\kappa$ onto $\kappa'$ and $\sigma e = e'$, then $\sigma \mathcal{L} \perp \eta$ is an automorphism of $\mathcal{L}$, since $\mathcal{L}$ is the only lattice in $\mathcal{J}'(4, 1)$ containing $\Theta e' \perp \kappa'$. It is easy to see that the number of isometries from $\kappa$ onto $\kappa'$ is just $|O(\kappa)|$; hence, $|O(\mathcal{L})| = a_2(2) \cdot |O(\kappa)|$. But $a_2(2) = \sqrt{|O(\mathcal{L})|}$ by Corollary 3.1.11; hence, our result follows. Q.E.D.

3.4.2 Remark: We observe that not all ternary lattices $\kappa$ in $\mathcal{J}(3, 2)$ with empty roots system have trivial automorphism groups. In fact, if $\kappa$ comes from a lattice $\mathcal{L}$ of type $A_2$, then $|O(\kappa)| = 6$ by Proposition 3.4.1. A careful inspection of the proof of Corollary 3.3.3 shows that $O(\kappa)$ is generated by $S_u S_u$ and $\pm 1$; hence, $O(\kappa)$ is not generated
by 11 and symmetries. If the type of $\mathcal{K}$ is $A_1 \oplus A_1 \oplus A_1$, we let $\mathcal{K} = \ominus e_1 \perp \ominus e_2 \perp \ominus e_3$, where $e_1$, $e_2$, and $e_3$ are minimal vectors. It is easy to see that $O(\mathcal{K})$ is generated by $e_1$, $e_2$, $e_3$, and $\rho$, where $\rho$ is defined by $\rho e_1 = e_2$, $\rho e_2 = e_3$, and $\rho e_3 = e_1$. Hence, $O(\mathcal{K}) = (C_2 \times C_2 \times C_2) \rtimes C_3$ is a wreath product. In this case, $O(\mathcal{K})$ is also not generated by symmetries. We denote by $\mathcal{J}'(3, 2)$ the subset of $\mathcal{J}(3, 2)$ consisting of all lattices which have nontrivial roots system (not nontrivial automorphism group).

3.4.3 Theorem: The generalized theta serie $\Theta_{\mathcal{K}}(z)$ of degree one for lattices $\mathcal{K}$ coming from the classes in $\mathcal{J}'(3, 2)$ are linearly independent.

Proof: Let $\mathcal{K}_1, \ldots, \mathcal{K}_h$ be a full set of nonisometric lattices in $\mathcal{J}'(3, 2)$. For each $i$, $\mathcal{K}_i$ is a free lattice of scale $2^{-1}\sigma$ and discriminant $2^{-1}$. Let $e_i$ be a minimal vector of $\mathcal{K}_i$, then $\ominus e_i$ does not split $\mathcal{K}_i$. For if $\mathcal{K}_i = \ominus e_i \perp M_i$ for some $M_i$, then locally at any dyadic prime $\mathfrak{p}$, $(M_i)_{\mathfrak{p}}$ is a unimodular lattice; hence, it has discriminant $-1$ or $-\Delta$ (up to a unit square). Therefore, $d(\mathcal{K}_i)_{\mathfrak{p}} = -2$ or $-2\Delta$, which is impossible, since $-1$ and $-\Delta$ are not squares. It follows that $e_i$ is contained in a binary unimodular lattice $(B_i)_{\mathfrak{p}}$ such that $(\mathcal{K}_i)_{\mathfrak{p}} = (B_i)_{\mathfrak{p}} \ominus Qz'$, where $Q(z) \in \mathcal{S}_{2\mathfrak{p}}$. We have $(\mathcal{K}_i)_{\mathfrak{p}} = (B_i)_{\mathfrak{p}} \ominus Qz'$, where $Q(z') \in 2^{-1}U_{\mathfrak{p}}$. It is now easy to see that the orthogonal complement of $e_i$ in $\mathcal{K}_i$ is a binary free lattice $\mathcal{L}_i$ of scale $2^{-1}\sigma$ and discriminant 1. Apply Lemma 1.6 [HKK] to obtain a unary free lattice $\mathcal{L}_i$ in $\mathcal{K}_i$ of discriminant $2^{-1}\pi_i$ with $\omega_i = \mathfrak{P}_i$ a prime of $F$, $\mathfrak{P}_i \nmid 3$. We claim that $\ominus e_i \perp \mathcal{L}_i$ is a globally characteristic sublattice in $\mathcal{K}_i$. By Theorem
2.2.1. it suffices to show that \( e_1 \perp (\mathfrak{g}_1)_P \) is locally characteristic for every dyadic prime \( \mathfrak{p} \). It is clear that \( (\mathfrak{g}_1)_P \) splits \( \mathfrak{X}_P \); hence, we have only to show that \( e_1 \) characterizes \( (\mathfrak{g}_1)_P \). But this is immediate (see the proof of Proposition 2.7.1). Now let \( a_{ij} \) be the number of isometric embeddings of \( \mathfrak{g}_i \) into \( \mathfrak{X}_j \). If \( \phi \) is any isometric embedding of \( \mathfrak{g}_i \) into \( \mathfrak{X}_j \), then the \( O(\mathfrak{X}_j) \)-orbit of \( \phi \) has \( |O(\mathfrak{X}_j)|/|H_\phi| \) elements, where \( H_\phi \) is the stabilizer of \( \phi \). Let \( \sigma \) be an involution in \( H_\phi \), then \( \sigma \) must be a symmetry if \( \mathfrak{X}_j \) is of type \( A_1 \) or \( A_2 \) (note that \( \sigma \) cannot be \(-S_e\), \( Q(e) = 2 \), since otherwise the fixed space of \( \sigma \) is \( \mathfrak{Oe} \); but \( \sigma \) fixes \( \phi(\mathfrak{g}_i) \), which is a contradiction.).

This can occur only when \( \mathfrak{X}_j \) is of type \( A_1 \) or \( A_2 \) (hence \( i = j \)) and \( \phi \) lies in the orbit of the inclusion map. It follows that

\[
a_{ij} \equiv 0 \pmod{2^2}, \quad i \neq j,
a_{jj} \equiv 0 \pmod{2}, \text{ but } a_{jj} \equiv 0 \pmod{2^2},
\]

for \( \mathfrak{X}_j \) of type \( A_1 \) or \( A_2 \). If \( \mathfrak{X}_j \) is of type \( A_1 \oplus A_1 \oplus A_2 \), then we have

\[
a_{ij} \equiv 0 \pmod{2^3}, \quad i \neq j,
a_{jj} \equiv 0 \pmod{2^3}.
\]

Now let \( \sum c_j \Theta_{\mathfrak{X}_j}(z) = 0 \) be a nontrivial linear relation, where the coefficients \( c_j \) are relatively prime integers. By evaluating it at each \( \mathfrak{g}_i \), we obtain \( \sum c_j a_{ij} = 0 \).

Consider the equation modulo various congruences:
\[
\begin{align*}
\mod 2^2 &= c_j \equiv 0 \pmod{2} \text{ for } \chi_j \text{ of type } A_1 \text{ or } A_2; \\
\mod 2^3 &= c_j \equiv 0 \pmod{2} \text{ for } \chi_j \text{ of type } A_1 \oplus A_1 \oplus A_1.
\end{align*}
\]

This is a contradiction. \hspace{1cm} \text{Q.E.D.}

3.4.4 \textbf{Corollary:} The generalized theta series of degree one classify the lattices in \(\mathbb{L}'(3, 2)\).
The ultimate question which remains to be resolved is whether Hsia's conjecture concerning the independence of theta series is always true. For positive ternary and quaternary forms, this means that the theta series (or degree 2 theta series in the quaternary case) associated with the classes in a genus should be independent. With our present knowledge of theta series, a full proof of this conjecture seems hardly within our reach. However, for specific genera, a solution may still be possible by exploiting the various technical features pertaining to the classes in a genus. In this dissertation, we were able to accomplish this for classes in certain genera which have nontrivial automorphism groups. A deeper understanding of the structures of the classes (with trivial automorphism groups) seems necessary in order to give a complete solution. The situation is essentially the same with regard to the question of classifying forms by theta series. Some evidences were provided in [Co]. We suggest in the following a few other possible avenues for further investigation:
(1) For the genus $G(4, p)$, we were able to show that the classes which have the same type of roots systems (either $A_1 \oplus A_1$ or $A_2$) have independent theta series of degree one. The question still remains whether the theta series coming from classes of both types are jointly independent. More generally, one would like to obtain the largest subset of classes in $G(4, p)$ for which their associated theta series are independent. The same question also applies to the genera $G(4, p^2)$ and $G(4, 1)$.

(2) The theta series associated with the classes in $G(4, p)$ and their reciprocals belong to the same space $\mathcal{M}(2, \Gamma_0(p), (\frac{*}{p}))$ of automorphic forms of weight 2 and character $(\frac{*}{p})$ with respect to the group $\Gamma_0(p)$. In [K1] Kitaoka observed that the number of classes in $G'(4, p)$ is one-half the dimension of $\mathcal{M}(2, \Gamma_0(p), (\frac{*}{p}))$ and, therefore, asked whether the theta series of the forms in $G'(4, p)$ and their reciprocals constitute an explicit basis for $\mathcal{M}(2, \Gamma_0(p), (\frac{*}{p}))$. This conjecture turns out to be invalid in general (see the counterexample in the appendix); however, one may still ask if a basis can be found among the theta series coming from all the classes in $G(4, p)$ and their reciprocals. As a first step toward finding such a basis, we suggest that one show that the classes of type $A_1 \oplus A_1$ or $A_2$ and their reciprocals have jointly independent theta series. A similar question can be raised for the genus $G(4, p^2)$. 
The arithmetic methods provided in this dissertation seem potentially applicable to forms of more than four variables as well as forms over arbitrary totally real number fields. One therefore asks whether our results can be extended over these cases. Chapter III dealt with $F = \mathbb{Q}(\sqrt{p})$ for forms in at most four variables.

Although it seems quite natural to prove linear independence of theta series by considering their coefficients modulo different congruence relations, one may ask whether a more direct approach is possible. For example, in the genus $G(4, p)$, can one show that the binary lattices strongly characterize all the classes (i.e. for each class in $G(4, p)$, is there a binary lattice which is represented by this class alone and not by the others)? If this is true, then the theta series of degree 2 associated with these classes will certainly be independent. Even if this is not possible, one may still ask the following question: Is there a "small" set of binary lattices associated with each class in $G(4, p)$ so that every other class does not represent at least one binary lattice from this set? This, however, does not necessarily imply the independence of their corresponding theta series.
APPENDIX

A COUNTEREXAMPLE

As we mentioned earlier in the introduction, the theta series coming from the classes of lattices in \( G'(4, p) \) in general are not independent. An example was furnished by Kitaoka and Nashiro at the prime 389. This shows in particular, that the conjecture in \([K_1]\) concerning the theta series associated with the classes in \( G'(4, p) \) and their reciprocals is false (i.e. they do not form a basis of the space \( \mathcal{M}(2, \Gamma_0(p), \left(\frac{\cdot}{p}\right)) \)).

We shall reproduce this example in the following.

There are 18 classes of even positive quaternary lattices of discriminant 389, 17 of which belong to \( G'(4, 389) \). If we represent these 17 classes by matrices of the form

\[
\begin{pmatrix}
2 & 1 & 0 & 0 \\
1 & 2a & e & 0 \\
0 & e & 2b & d \\
0 & 0 & d & 2c
\end{pmatrix},
\]

then they are given by

<table>
<thead>
<tr>
<th>Lattices</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>( L_1 )</td>
<td>7</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( L_2 )</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

140
<table>
<thead>
<tr>
<th>Lattices</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>L&lt;sub&gt;3&lt;/sub&gt;</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>L&lt;sub&gt;4&lt;/sub&gt;</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>L&lt;sub&gt;5&lt;/sub&gt;</td>
<td>3</td>
<td>4</td>
<td>8</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>L&lt;sub&gt;6&lt;/sub&gt;</td>
<td>3</td>
<td>3</td>
<td>10</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>L&lt;sub&gt;7&lt;/sub&gt;</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>L&lt;sub&gt;8&lt;/sub&gt;</td>
<td>1</td>
<td>5</td>
<td>16</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>L&lt;sub&gt;9&lt;/sub&gt;</td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>L&lt;sub&gt;10&lt;/sub&gt;</td>
<td>2</td>
<td>4</td>
<td>27</td>
<td>19</td>
<td>1</td>
</tr>
<tr>
<td>L&lt;sub&gt;11&lt;/sub&gt;</td>
<td>33</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>L&lt;sub&gt;12&lt;/sub&gt;</td>
<td>1</td>
<td>1</td>
<td>49</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>L&lt;sub&gt;13&lt;/sub&gt;</td>
<td>5</td>
<td>1</td>
<td>12</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>L&lt;sub&gt;14&lt;/sub&gt;</td>
<td>3</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>L&lt;sub&gt;15&lt;/sub&gt;</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>L&lt;sub&gt;16&lt;/sub&gt;</td>
<td>1</td>
<td>3</td>
<td>13</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>L&lt;sub&gt;17&lt;/sub&gt;</td>
<td>1</td>
<td>9</td>
<td>4</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>
The 18th class in \( G(4, 389) \) which does not represent 2 is furnished by P. Ponomarev and J. Yang:

\[
L_{18} = 2(2X^2 + 2Y^2 + 3Z^2 + 3W^2 + XY + 2XZ + YZ + XW + 2ZW).
\]

There is a linear relation between the theta series of the first ten classes:

\[
\theta_{L_1}(z) + \theta_{L_3}(z) + \theta_{L_5}(z) + \theta_{L_7}(z) + \theta_{L_{10}}(z)
= \theta_{L_2}(z) + \theta_{L_4}(z) + \theta_{L_6}(z) + \theta_{L_8}(z) + \theta_{L_9}(z).
\]

However, if we delete \( L_{10} \) and its reciprocal \( L_{10}^* \), then the theta series of the 17 classes \( L_1, \ldots, L_9, L_{11}, \ldots, L_{17}, L_{18} \) and their reciprocals do provide a basis for \( M(2, \Gamma_0(389)), \ (\frac{*}{389}) \). This was checked with a computer, using the fact that a modular form \( f = \sum a_n q^n \) in the space \( M(2, \Gamma_0(389)), \ (\frac{*}{389}) \) is identically zero if and only if its first 65 coefficients are zero. See [He], page 954.
BIBLIOGRAPHY


[Co]  P. J. Costello: "Classification and construction of integral positive definite quadratic forms over \( \mathbb{Z} \left[ \frac{1 + \sqrt{5}}{2} \right] \)"., Dissertation, The Ohio State University, 1982.


A. Trojan: "The integral extension of isometries of quadratic forms over local fields", CJM, 18(1966), 920-942.
