Quaternary quadratic forms of discriminant $4p$

by
Lisa Kaylor

Advisor: Wai Kiu Chan
Professor of Mathematics

Wesleyan University

Middletown, CT

May, 2019

A Dissertation in Mathematics

submitted in partial fulfillment of the

requirements for the degree of Doctor of Philosophy

In memory of my father

Abstract

A quadratic form is a homogeneous polynomial of degree 2 in n variables. One of the most fundamental questions in the study of quadratic forms is the classification problem. For rational quadratic forms, there is a complete solution to this question due to the local - global principle of Hasse; however, for integral quadratic forms, this principle does not hold in general. This leads to the study of invariants of integral quadratic forms and how they can be used for classification. In this thesis, we use the geometric language of quadratic spaces and lattices and restrict our attention to quaternary even positive definite integral $\mathbb{Z}$-lattices and their theta series. For such lattices with discriminant 389 and minimum 2, Kitaoka showed [11] that there is a linear dependence relation among the theta series corresponding to the classes of these lattices. However, Hsia and Hung showed [11] that the degree 2 theta series corresponding to the classes of positive definite even quaternary integral lattices of discriminant p a prime congruent to 1 mod 4 with minimum 2 are linearly independent. We consider those lattices with discriminant $4p$ where $p > 13$ is a prime congruent to 3 mod 4. There are two genera of lattices in this case, which are considered separately. We follow the strategy of Hsia and Hung to show that the degree 2 theta series of the classes with nontrivial orthogonal group are linearly independent within each genus.

Acknowledgements

First and foremost, I would like to express my sincere thanks to Professor Wai Kiu Chan. I feel honored to have him as my advisor not only because of his mathematical excellence, but also his exceptional teaching and advising. Without his patience, guidance, and support throughout my graduate studies, this work would not exist.

I would like express my gratitude to the mathematics faculty at Wesleyan. In particular, my committee members Professor David Pollack and Professor Chris Rasmussen for reading this work and providing useful commentary, and Professor Connie Leidy for being a mentor in both teaching and academic life.

I am happy to conclude my time at Wesleyan with the graduate students who have been there from the start, Miriam Parnes and Cameron Bishop. I thank the graduate students both past and present for their encouragement and motivating conversations. In particular, I would like to thank Freda Li and Noelle Sawyer for their genuine care and support, which has helped me in countless ways.

Finally, I thank my mother for her unending support in all of my pursuits.

Contents

Dedication **i**

Introduction **1**

1 Background and Definitions **4**

1.1 Quadratic Spaces 5

1.2 Lattices on Quadratic Spaces 7

1.3 Localization and Classification 9

2 Preliminaries **12**

2.1 Root Systems and Scaled Root Systems 12

2.2 Theta Series 15

2.3 Quaternary Lattices of Discriminant $4p$ 16

2.3.1 Minimum 4 or greater 17

2.3.2 Decomposability 22

3 The Principal Genus **25**

3.1 Root Systems 25

3.2 Scaled Root Systems and $O(L)$ 27

3.3 Linear Independence of Degree Two Theta Series 41

4 The Second Genus **55**

4.1 Root Systems 55

4.2 Scaled Root Systems and $O(L)$ 57

4.3 Linear Independence of Degree Two Theta Series 75

Introduction

The motivation for this work is the question of classification for integral quadratic forms. The Hasse-Minkowski principle [18, 66:4] gives a complete classification of quadratic forms over $\mathbb{Q}$, but it does not hold in general for quadratic forms over $\mathbb{Z}$. This leads to the study of invariants which can help classify quadratic forms over $\mathbb{Z}$. The invariant of interest we will be considering in this thesis is the theta series of an integral quadratic form.

We will conduct the subsequent discussion in the geometric language of quadratic spaces and lattices. The theta series of a positive definite lattice is a Fourier series whose nth coefficient is the number of representations of the positive integer n by the lattice. Since isometric lattices represent the same set of integers with the same multiplicity, the theta series is a class invariant. It was shown by Hecke [11] that the theta series of the classes of positive definite binary lattices with a fixed discriminant are linearly independent. Thus, the theta series provides a classification in this case.

In the ternary case, it was shown by Schiemann [20] that the theta series classifies positive definite ternary lattices. However, Gross provided an example in [10] of a linear dependence relation among the theta series of classes of ternary lattices. An explicit computation of the linear dependence relation was provided in the case of discriminant $32p^2$ where $p = 389$ by Kramer in [16]. Thus, although theta series classify positive definite ternary lattices, they are not always linearly independent.

Kitaoka [11] determined that in the case of positive definite even quaternary lattices of discriminant $p = 389$ there is a linear dependence relation among the theta series of those classes whose minimum is 2. An explicit computation can be found in [16]. Using a higher degree analogue of the theta series, Hsia and Hung [11] were able to show that the degree 2 theta series corresponding to those classes of positive definite even quaternary integral lattices of discriminant a prime p congruent to 1 mod 4 whose minimum is 2 are linearly independent. The degree 2 theta series of a positive definite lattice is a Fourier series whose coefficients are the numbers of distinct embeddings of binary lattices into the lattice. Thus, in this case, the degree 2 theta series provides the classification.

Here we note that in the result of Hsia and Hung, the minimum 2 condition is necessary. Schulze-Pillot gave an example in [21] of a linear dependence relation among the degree 2 theta series of the classes of positive definite even quaternary lattices of discriminant $p = 389$.

In this thesis, we consider positive definite even quaternary integral lattices of discriminant $4p$, where $p > 13$ is a prime congruent to 3 mod 4. These lattices fall into two genera which we will denote by $\mathcal{G}$ and $\mathcal{G}'$. Our goal is to show that the degree 2 theta series corresponding to classes of lattices with nontrivial orthogonal groups, in $\mathcal{G}$ and $\mathcal{G}'$ respectively, are linearly independent. We will follow the strategy used by Hsia and Hung in [11] with appropriate modifications specific to the aforementioned lattices in their respective genera.

The orthogonal groups of the lattices considered by Hsia and Hung are generated by symmetries with respect to the minimal vectors and -1. In [6], Chan investigated the class number of $\mathcal{G}$ and $\mathcal{G}'$. From this work, it is evident that the orthogonal groups of the lattices in $\mathcal{G}$ and $\mathcal{G}'$, if they are nontrivial, are generated not only by symmetries with respect to the minimal vectors but also symmetries with respect to some other primitive vectors. In adopting the strategy of proof in [5], we show that the orthogonal group of any lattice in $\mathcal{G}$ or $\mathcal{G}'$ is generated by symmetries and -1.

Once the structure of the orthogonal group is determined, we proceed with the proof of the linear independence of the degree 2 theta series. We consider an integer linear combination of the degree 2 theta series corresponding to the classes with nontrivial orthogonal group in either $\mathcal{G}$ or $\mathcal{G}'$. Without loss of generality, we assume that the coefficients of this linear combination are relatively prime. We then show in a systematic way that each coefficient is in fact even. This contradiction gives the desired result, that the degree 2 theta series associated to the classes with nontrivial orthogonal group, in either $\mathcal{G}$ or $\mathcal{G}'$, are linearly independent.

In the first Chapter, we will define quadratic spaces and lattices. Then, we will focus on the localization of lattices and the hierarchy of classification. Chapter 2 will introduce the notion of scaled root systems and theta series. Then, we will focus on the lattices of interest by examining both their decomposability and the structure of their orthogonal groups in the case when the minimum of the lattices is 4 or greater. In Chapters 3 and 4, we will consider the genera $\mathcal{G}$ and $\mathcal{G}'$ respectively. The root systems will first be determined, followed by the scaled root systems and the structure of the orthogonal groups. Finally, we will present the proof of the main result.

Chapter 1

Background and Definitions

Formally, an *n-ary quadratic form* $f(x_1, \ldots, x_n)$ over a field F of characteristic not 2 is a homogeneous polynomial of degree 2 over F in the n variables $x_1, \ldots, x_n$. In general, this polynomial takes the form:

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} b_{ij} x_i x_j.$$

To ensure that the coefficients of f are symmetric, we take $a_{ij} = (b_{ij} + b_{ji})/2$ and rewrite $f(x_1, \ldots x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$. The *Gram matrix* of f is defined to be the matrix $A_f = (a_{ij})$. Rewriting f in terms of matrix multiplication, we have:

$$f(\mathbf{x}) = \mathbf{x}^t A_f \mathbf{x}.$$

If f and g are n-ary quadratic forms, we say that f is *equivalent* to g, denoted $f \cong g$, if there exists an invertible matrix $P \in GL_n(F)$ such that $A_f = P^t A_g P$. In this way, the equivalence of forms can be viewed as the congruence of the associated Gram matrices.

There is a one to one correspondence between equivalence classes of quadratic forms as defined above and isometry classes of quadratic spaces [18, 41:2]. We will proceed by defining quadratic spaces and take the perspective of these more geometric objects for the remainder of this work. All content referred to in this chapter can be found in [9] and [18].

1.1 Quadratic Spaces

Let V be a finite-dimensional vector space over a field F of characteristic not equal to 2, and $B : V \times V \to F$ be a symmetric bilinear form. We call the composite object (V, B) a *quadratic space* and associate to it the *quadratic map* $Q : V \to F$ defined by $Q(x) = B(x, x)$. When our quadratic space is clear from context, we will use V to denote this composite object.

Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis for V and $v = a_1v_1 + \cdots + a_nv_n \in V$. Then

$$Q(v) = Q(a_1v_1 + \cdots + a_nv_n) = \sum_{i,j=1}^{n} B(v_i, v_j)a_ia_j.$$

We say that $a \in F$ is *represented by* V if $Q(v) = a$ for some $v \in V$. The polynomial

$$f(x_1, \ldots, x_n) := \sum_{i,j=1}^{n} B(v_i, v_j)x_ix_j,$$

is called the *quadratic form* of the quadratic space V in the basis $\mathcal{B}$.

The symmetric matrix $M = (B(v_i, v_j))$ is called the *Gram matrix* of V with respect to the basis $\mathcal{B}$, which is denoted by $V \cong M$. Note that for another basis $\mathcal{B}' = \{u_1, \ldots u_n\}$ of V and $N = (B(u_i, u_j))$, we have that $N = T^tMT$ where T is the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$. It is a fact [18, 42:1] that every nonzero quadratic space has an orthogonal basis, and hence a diagonal Gram matrix. When the Gram matrix of V is diagonal, we write $V \cong [a_1, \ldots, a_n]$ where $a_i = B(v_i, v_i) = Q(v_i)$ for all i. The *discriminant* of V, denoted dV, is the canonical image of $\det(M)$ in $F^\times/F^{\times 2} \cup \{0\}$. It is clear that dV is independent of the choice of the Gram matrix of V.

A quadratic space is said to be *nondegenerate* if $B(v, V) = 0$ for $v \in V$ only when $v = 0$. This is the same as requiring that $dV \neq 0$. All quadratic spaces considered in this thesis will be nondegenerate. We call a nonzero vector $v \in V$ *isotropic* if $Q(v) = 0$. Otherwise, we say that v is anisotropic. Further, if V contains an isotropic vector, then we say that V itself is isotropic. Otherwise, V is anisotropic. Two vectors u and w in V are *orthogonal* if $B(v, w) = 0$. Subsets U and W of V are said to be orthogonal if $B(u, w) = 0$ for all $u \in U$ and $w \in W$. Then, V is an *orthogonal sum* of U and W, written $V = U \perp W$, if V is the direct sum of U and W with U and W orthogonal. For a subspace U of V, we define the *orthogonal complement* of U in V, denoted $U^\perp$, to be the collection of vectors $v \in V$ such that $B(v, U) = 0$.

For a nonzero $\alpha \in F$, we define V^α to be the quadratic space (V, B^α) over F with $B^\alpha(x, y) = \alpha B(x, y)$. We call V^α the *scaling* of V by α. Note that $dV^\alpha = \alpha^n dV$ where n is the dimension of V.

Suppose (W, B') is another quadratic space and $\sigma : V \to W$ is a linear transformation. We say that σ is a *representation* of V into W if $B(v, v') = B'(\sigma(v), \sigma(v'))$ for all v and v' in V. We call a bijective representation an *isometry* and say that V is *isometric* to W, denoted $V \cong W$, if there exists an isometry between V and W.

The following theorem [18, 42:17] about quadratic spaces will be relevant in the proof of our main result:

Theorem (Witt's Extension Theorem)**.** *Let V and V' be nondegenerate isometric quadratic spaces, let U be any subspace of V, and let σ be an isometry of U into V'. Then, there is a prolongation of σ to an isometry of V onto V'.*

The *orthogonal group* of V, denoted $O(V)$, is the set of all isometries of V onto itself. Let v be an anisotropic vector in V. The *symmetry with respect to* v is the map $\tau_v : V \to V$ defined by

$$\tau_v(x) = x - \frac{2B(v,x)}{Q(v)}v.$$

It is easy to check that τ_v is an isometry of V. Note that $\tau_v(v) = -v$ and all vectors in $F[v]^\perp$ will be fixed by τ_v. Further, the Cartan-Dieudonné Theorem [9, p. 28] says that every $\sigma \in O(V)$ is a product of at most n symmetries .

1.2 Lattices on Quadratic Spaces

Let R be a principal ideal domain of characteristic not 2 and F be its field of fractions. A subset L of a quadratic space V over F is called an *R-lattice in V*, or simply a *lattice*, if there exists a linearly independent subset $\{v_1, \ldots, v_n\}$ of V such that $L = Rv_1 \oplus \cdots \oplus Rv_n$. In other words, a lattice in V is a finitely generated R-module. The integer n is called the *rank* of L. If $FL = V$, we say that L is a *lattice on* V. A nonzero vector $v \in L$ that can be extended to a basis of L is called a *primitive* vector of L. A lattice on V is nondegenerate if V is nondegenerate. Thus, the lattices we will consider are always nondegenerate.

Let L be an R-lattice on a quadratic space (V, B) and $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis of L. As with quadratic spaces, the symmetric matrix $A = (B(v_i, v_j))$ is called the *Gram matrix* of L with respect to the basis $\mathcal{B}$. The *discriminant* of L, denoted dL, is the canonical image of $\det(A)$ in $F^\times/R^{\times^2}$. If A' is another Gram matrix of L, we have that $A' = T^tAT$ for some $T \in GL_n(R)$. Then, $\det(A') \in \det(A)R^{\times^2}$, and hence dL is well-defined. Note that $\det(A) \neq 0$ because V is always assumed to be nondegenerate. We will often identify dL with

$\det(A)$ for convenience. Moreover, we will often define a lattice by specifying a Gram matrix associated to it. If A is a Gram matrix of L, we will write $L \cong A$. In the special case when $\{v_1, \ldots, v_n\}$ is an orthogonal basis, we will write $L \cong < a_1, \ldots, a_n >$ where $a_i = B(v_i, v_i) = Q(v_i)$ for all i.

If there exist nonzero sublattices L_i of L such that

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

then L is said to be *decomposable*, and $L_1 \perp \cdots \perp L_m$ is called an *orthogonal splitting* for L. Further, we say that each L_i *splits* L. If L has no such splitting, we say that L is *indecomposable*. For any integer $n \geq 1$, let nL denote a lattice which is the orthogonal sum of n copies of L.

The R-module generated by the subset $B(L, L)$ of F is called the *scale* of L, denoted $\mathfrak{s}(L)$, and the R-module generated by the subset $Q(L)$ of F is called the *norm* of L, denoted $\mathfrak{n}(L)$. A lattice L is called *integral* if $\mathfrak{s}(L) \subset R$. We say that a lattice L is *unimodular* if $\mathfrak{s}(L) \subset R$ and dL is a unit.

Let a be a nonzero element in F. Then, L^a denotes the lattice on the quadratic space V^a, whose underlying set is just L. We have the following relationships between the scale, norm, and discriminant of L and L^a:

$$\mathfrak{s}(L^a) = a\mathfrak{s}(L), \qquad \mathfrak{n}(L^a) = a\mathfrak{n}(L), \qquad \text{and} \qquad d(L^a) = a^n d(L),$$

where n is the rank of L. If $L^{a^{-1}}$ is unimodular, we say that L is (a)-*modular*. In general, we say L is *modular* if L is (a)-modular for some nonzero a in F.

For an R-lattice L on the quadratic space V, the *dual* lattice of L is the R-lattice given by

$$L^{\#} = \{v \in V | B(v, L) \subset R\}.$$

As the following properties of $L^{\#}$ will be relevant, we state them here. Justification can be found in [9, 6.25].

- If A is a Gram matrix of L, then A^{-1} is a Gram matrix of $L^{\#}$.

- The discriminant of $L^{\#}$, denoted $dL^{\#}$, is equal to $(dL)^{-1}$.

- If L is integral, then $L \subset L^{\#}$.

- L is unimodular if and only if $L = L^{\#}$.

- If K is another lattice on V and $L \subset K$, then $K^{\#} \subset L^{\#}$.

- If $L = M \perp N$, then $L^{\#} = M^{\#} \perp N^{\#}$.

Suppose that M is an R-lattice on a quadratic space W. Then, M is *represented* by L if there exists a representation σ of W by V such that $\sigma(M) \subset L$. Further, M is *isometric* to L, written $M \cong L$, if there exists an isometry $\sigma : W \to V$ such that $\sigma(M) = L$. The *orthogonal group* of L, denoted $O(L)$, is the set of isometries $\sigma \in O(V)$ such that $\sigma(L) = L$.

1.3 Localization and Classification

For an n-dimensional quadratic space U over $\mathbb{Q}_p$ such that $U \cong [\alpha_1, \ldots \alpha_n]$, we define the Hasse symbol

$$S_p(U) = \prod_{1 \leq i \leq n} \left(\frac{\alpha_i, d_i}{p} \right)$$

where $d_i = \alpha_1 \cdots \alpha_i$ and $\left(\frac{\alpha_i, d_i}{p} \right)$ is the Hilbert symbol [18, §63B]. The Hasse symbol is independent of the choice of diagonal Gram matrix for U. Properties useful for calculation of the Hasse symbol can be found in [18, p. 167].

Let V be a quadratic space over $\mathbb{Q}$ and p a prime. We define the *localization* of V, denoted V_p, to be $V \otimes_{\mathbb{Q}} \mathbb{Q}_p$. For a $\mathbb{Z}$-lattice L on V, the *localization*, denoted L_p, is the $\mathbb{Z}_p$-module generated by L on V_p. We have the following theorem [18, 63:19] on classification of quadratic spaces over $\mathbb{Q}_p$.

Theorem. *Let V and W be quadratic spaces over $\mathbb{Q}$ and p a prime. Then, V_p is isometric to W_p if and only if $\dim V_p = \dim W_p$, $dV_p = dW_p$ and $S_p(V_p) = S_p(W_p)$.*

The following classical theorem of Hasse [18, 66:4] gives a complete classification of quadratic spaces over $\mathbb{Q}$ up to isometry.

Theorem (Hasse-Minkowski)**.** *Let V and W be quadratic spaces over $\mathbb{Q}$. Then, V is isometric to W if and only if V_p is isometric to W_p for all primes p and $V \otimes \mathbb{R}$ is isometric to $W \otimes \mathbb{R}$.*

Unfortunately, the analogous statement for lattices is not true in general. If two lattices are locally isometric over all $\mathbb{Z}_p$ and over $\mathbb{R}$, the lattices are not necessarily isometric over $\mathbb{Z}$. This leads to the following definitions. The *genus* of L, denoted by $\text{gen}(L)$, is the collection of lattices M on V such that $L_p \cong M_p$ for all primes p. The *class* of L, denoted $\text{cls}(L)$, is the collection of lattices M on V such that $L \cong M$. It is clear that $\text{cls}(L) \subset \text{gen}(L)$ because every global isometry can be extended to a local isometry at every prime p.

Every $\mathbb{Z}_p$-lattice L_p can be written as an orthogonal sum $L_p = L_1 \perp \cdots \perp L_m$ where each L_i is a modular sublattice of L_p and $\mathfrak{s}(L_1) \supset \mathfrak{s}(L_2) \supset \cdots \supset \mathfrak{s}(L_m)$. We call this a *Jordan splitting* for L_p and the L_i are referred to as the *Jordan components*. If there exists another Jordan splitting of $L_p = L'_1 \perp \cdots \perp L'_t$, then it must be that $m = t$, $\text{rank}(L_i) = \text{rank}(L'_i)$, and $\mathfrak{s}(L_i) = \mathfrak{s}(L'_i)$ for all i.

When p is not equal to 2, each Jordan component has an orthogonal basis. For $p = 2$, if L_2 is (a)-modular and $\mathfrak{n}(L_2) = (2a)$, then L_2 is said to be *improper*.

Otherwise, $\mathfrak{n}(L_2) = (a)$ and L_2 is said to be *proper*. Further, if L_2 is unimodular and improper, we say that L_2 is *even*. Up to isometry there are precisely two binary even unimodular $\mathbb{Z}_2$ - lattices, and they are

$$\mathbb{H} \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad \mathbb{A} \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

The lattice $\mathbb{H}$ is the called the *hyperbolic plane*, which is isotropic. The lattice $\mathbb{A}$ is anisotropic. Both $\mathbb{H}$ and $\mathbb{A}$ are indecomposable $\mathbb{Z}_2$-lattices. Every even unimodular $\mathbb{Z}_2$-lattice is an orthogonal sum of binary sublattices isometric to $\mathbb{H}$ or $\mathbb{A}$ [18, 93:15]. If we have a $\mathbb{Z}_2$-lattice $L_2 \cong < \epsilon_0, \epsilon_1, \epsilon_2 >$ where $\epsilon_i \in \mathbb{Z}_2^\times$ for all i, then $L_2 \cong \mathbb{P} \perp < \epsilon >$ for some $\epsilon \in \mathbb{Z}_2^\times$ and an even unimodular lattice $\mathbb{P}$, where $\mathbb{P} = \mathbb{H}$ if and only if L is isotropic [18, 93:18(iv)].

For two lattices L and M on a quadratic space V over $\mathbb{Q}$ and a prime p not equal to 2, we have the following theorem of local classification [9, 8.5].

Theorem. *Let L_p and M_p have Jordan splittings $L_p = L_1 \perp \cdots \perp L_m$ and $M_p = M_1 \perp \cdots \perp M_t$ with $m = t$, rank(L_i) = rank(M_i), and $\mathfrak{s}(L_i) = \mathfrak{s}(M_i)$ for all i. Then $L_p \cong M_p$ if and only if $dL_i = dM_i$ for all i.*

For local classification when $p = 2$, we refer the reader to either [9, §8.3] or [18, §93].

Chapter 2

Preliminaries

In this chapter, we will introduce both the root system and the scaled root system of a lattice. Relevant examples pertaining to the lattices in $\mathcal{G}$ and $\mathcal{G}'$ will be given. Then, we will define the degree n theta series of a lattice. This will be followed by a discussion of the lattices in $\mathcal{G}$ and $\mathcal{G}'$ whose minimum is 4 or greater. We will conclude this chapter by determining the decomposability of the lattices in $\mathcal{G}$ and $\mathcal{G}'$.

2.1 Root Systems and Scaled Root Systems

Let L be an integral $\mathbb{Z}$-lattice on a quadratic space V over $\mathbb{Q}$. We say that L is *positive definite* if $Q(v) > 0$ for all nonzero $v \in L$. From now on, all $\mathbb{Z}$-lattices considered will be positive definite. The *minimum* of L is defined as

$$\min(L) = \min\{Q(v) : 0 \neq v \in L\}.$$

A nonzero vector v in L is said to be a *minimal vector* of L if $Q(v) = \min(L)$. The following theorem [9, 7.5] gives an upper bound on this value.

Theorem (Hermite's Inequality)**.** *Let L be an integral $\mathbb{Z}$-lattice of rank n. Then,*

$$\min(L) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} (dL)^{\frac{1}{n}}.$$

A *root system* in a quadratic space V over $\mathbb{Q}$ is a subset R of V satisfying the following properties [2, p.155]:

1. R is finite and does not contain zero.

2. For all $v \in R$, $\tau_v(R) = R$. That is, τ_v fixes R.

3. For all $v \in R$, $\dfrac{2B(u,v)}{Q(v)} \in \mathbb{Z}$ for all $u \in R$.

The *scaled root system* of a $\mathbb{Z}$-lattice L on V, denoted $R(L)^*$, is the collection of vectors v in L such that v is primitive and $\tau_v \in O(L)$. It was shown by Scharlau in [19] that the scaled root system is a root system as defined above. We call the vectors in the scaled root system the *scaled roots* of L. The *scaled root lattice* of L is the sublattice generated by the vectors in the scaled root system. We will denote the scaled root lattice of L by R_L^*.

The *root system* of L, denoted $R(L)$, is the subset of $R(L)^*$ containing vectors of length 2. Note that when referring to the length of a vector v, we mean the value $Q(v)$. We call the vectors in the root system the *roots* of L. It is clear that $R(L)$ itself is a root system. The *root lattice* of L is the sublattice generated by these vectors, which we will denote by R_L. The following root systems will appear in the later discussion of the lattices in $\mathcal{G}$ and $\mathcal{G}'$:

- The root system $\mathbf{A}_n$ is the collection of vectors of length 2 of the lattice

A_n with the following Gram matrix

$$\begin{pmatrix} 2 & 1 & 0 & \cdots & \cdots & 0 \\ 1 & 2 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 2 & 1 & \ddots & \vdots \\ \vdots & 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \vdots & \ddots & 1 & 2 & 1 \\ 0 & \cdots & \cdots & 0 & 1 & 2 \end{pmatrix}.$$

There are $n(n+1)$ roots in $\mathbf{A}_n$. Additionally, we have $\det(A_n) = n+1$.

- We will encounter the scaled root system $\mathbf{C}_n$ (commonly known as the root system $\mathbf{C}_n$) when $n = 2$ and $n = 3$. For $n = 2$, the scaled root system $\mathbf{C}_2$ is the collection of vectors of lengths 2 and 4 of the lattice C_2 with Gram matrix
$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$
There are 8 scaled roots in $\mathbf{C}_2$. When $n = 3$, the scaled root system $\mathbf{C}_3$ is the collection of vectors of lengths 2 and 4 of the lattice A_3. Although the lattice A_3 is spanned by the scaled root system $\mathbf{C}_3$, we will denote this lattice by C_3 to indicate that the scaled root system $\mathbf{C}_3$ is under consideration. There are 18 scaled roots in $\mathbf{C}_3$.

- The root system $\mathbf{D}_4$ is the collection of vectors of length 2 of the lattice D_4 with Gram matrix
$$\begin{pmatrix} 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}.$$
There are 24 roots in $\mathbf{D}_4$ and $\det(D_4) = 4$.

For a root system X in V and a positive integer α, X^α is the root system in V^α whose underlying set is just X. For two root systems X and Y on orthogonal quadratic spaces U and W, respectively, their union is a root system on $U \perp W$. We denote this root system by $X \perp Y$. For $n \geq 1$, let nX denote the orthogonal sum of n copies of X.

For the lattice L^α on V^α, we have $R(L^\alpha) = R(L)^\alpha$. The *Weyl group* of R_L^*, denoted $W(R_L^*)$, is the subgroup of $O(R_L^*)$ generated by symmetries with respect to the vectors in $R(L)^*$.

2.2 Theta Series

Let L be a $\mathbb{Z}$-lattice on a quadratic space V over $\mathbb{Q}$. We say that L is *even* if $Q(v) \in 2\mathbb{Z}$ for all $v \in L$. Recall that L is always assumed to be positive definite. All material referenced in this section can be found in [1] and [8].

Let Sym_n be the set of symmetric integral even (i. e. diagonal entries are even) positive semidefinite matrices of size $n \times n$. Let A be a Gram matrix of L and T be a matrix in Sym_n. The number of representations by L of the lattice with T as a Gram matrix is denoted by $r_L(A, T)$.

Let $\mathrm{Tr}(M)$ denote the trace of a matrix M. The *degree n theta series* of an even $\mathbb{Z}$-lattice L of rank m with Gram matrix A is defined to be

$$\theta^{(n)}(Z, A) = \sum_{X \in M_{m\times n}(\mathbb{Z})} e^{\pi i \mathrm{Tr}(X^t A X Z)} = \sum_{T \in \mathrm{Sym}_n} r_L(A, T) e^{\pi i \mathrm{Tr}(TZ)}$$

where $Z = X + iY$ is an $n \times n$ complex symmetric matrix with both X and Y real matrices and Y positive [1, §1.1.2]. It is clear that the degree n theta series is a class invariant.

To prove the main results of this work, we will make use of the following relationship between the degree n theta series of a lattice as above and that of its dual found in [8, 0.11 Satz]:

$$\theta^{(n)}(-Z^{-1}, A^{-1}) = \det(A)^{n/2}(\det(-iZ))^{m/2}\theta^{(n)}(Z, A). \tag{$\star$}$$

Note that A^{-1} is the Gram matrix of $L^{\#}$. Thus, when considering a linear relation among the theta series of a family of lattices of the same discriminant, by this transformation equation, we could switch the consideration to the theta series of the duals of those lattices, which should satisfy the same relation as well. It is this principle that we will make use of later.

2.3 Quaternary Lattices of Discriminant $4p$

Let L be a $\mathbb{Z}$-lattice on a quadratic space V of dimension 4 over $\mathbb{Q}$. Our assumption is that L is positive definite, even, and integral. We further assume that L has discriminant $4p$ where $p > 13$ is a prime congruent to 3 mod 4. For a fixed prime p, one can show that there are two genera of such lattices and that these genera are distinguished by the localizations of their lattices at the primes p and 2. Let $\mathcal{G}$ denote the genus containing those lattices L with $L_p \cong < 1, 1, \delta, \delta p >$ where 2δ is a nonsquare mod p and $L_2 \cong \mathbb{H} \perp < -2, 2p > \cong \mathbb{A} \perp < -2, -6p >$. In this case, the Hasse symbol is

$$S_q(\mathbb{Q}_q L_q) = \begin{cases} -(p, -2)_2 & \text{if } q = 2, \\ (-\delta, p)_p & \text{if } q = p, \\ 1 & \text{otherwise.} \end{cases}$$

Let $\mathcal{G}'$ denote the genus containing lattices L with $L_p \cong < 1, 1, \delta, \delta p >$ where 2δ is a square mod p and $L_2 \cong \mathbb{H} \perp < 2, -2p > \cong \mathbb{A} \perp < 2, 6p >$. In this case, the

Hasse symbol is

$$S_q(\mathbb{Q}_q L_q) = \begin{cases} -(p,2)_2 & \text{if } q = 2, \\ (-\delta, p)_p & \text{if } q = p, \\ 1 & \text{otherwise.} \end{cases}$$

2.3.1 Minimum 4 or greater

Let L be a lattice in $\mathcal{G}$ or $\mathcal{G}'$ such that $\min(L) \geq 4$. In this section, we prove a lemma analogous to that of [5, Lemma 2.2] and present the proof of the proposition [6, Prop 3.2].

First, we make the following definitions. A lattice L is *ambiguous* if L has an isometry σ of determinant -1. Otherwise, we say that L is *unambiguous.* The orthogonal group of L is said to be *trivial* if $O(L) = \{\pm 1\}$. For any $\sigma \in O(V)$, we define the *σ-fixed sublattice* of L to be $L^\sigma = \{v \in L : \sigma(v) = v\}$ and the *σ-variant sublattice* of L, denoted L_σ, to be the orthogonal complement of L^σ in L [15]. For a $\mathbb{Z}$-lattice (or $\mathbb{Z}_p$-lattice) L and a full rank sublattice M of L, we have $dM = dL[L : M]^2$. Further, for a sublattice N of L, we have that $dN^\perp$ divides $dL \cdot dN$ where $N^\perp$ is the orthogonal complement of N in L [9, 6.17(ii)].

Now, we are prepared to prove the following lemma.

Lemma 1. *Let L be a lattice in $\mathcal{G} \cup \mathcal{G}'$. If $\min(L) \geq 4$, then $O(L)$ does not have any element of odd order.*

Proof. Let $\sigma \in O(L)$ have order q where q is an odd prime. Then, considering L as a $\mathbb{Z}[\sigma]$-module, L can be written as $X^a \oplus \mathbb{Z}[\zeta_q]^b \oplus \mathbb{Z}^c$ for some $a, b, c \in \mathbb{Z}_{\geq 0}$ where X is a rank q indecomposable module, $\mathbb{Z}[\zeta_q]$ is the ring of integers in $\mathbb{Q}(\zeta_q)$, and $\mathbb{Z}$ is the trivial module [7]. Because L is a nontrivial $\mathbb{Z}[\sigma]$-module and has rank 4, q cannot be greater than 5.

Suppose that $q = 5$. Then, since the rank of L is 4 and L is a nontrivial $\mathbb{Z}[\sigma]$-module, we have that $L \cong \mathbb{Z}[\zeta_5]$. However, by [15, Proposition 3.1], this implies that $dL = 5 \cdot \alpha$ where α is a square. This is impossible because $dL = 4p$ and $p > 13$ is congruent to 3 mod 4. Thus, $q \neq 5$.

Suppose $q = 3$ and that $a = 0$. Then, $L \cong \mathbb{Z}[\zeta_3]^2$ or $L \cong \mathbb{Z}[\zeta_3] \perp \mathbb{Z}^2$. In the first case, [15, Proposition 3.1] implies that dL is a square, which is impossible. If $L \cong \mathbb{Z}[\zeta_3] \perp \mathbb{Z}^2$, then by [15, Proposition 3.1], dL is divisible by 3, which is again impossible. Thus, $a \neq 0$.

Suppose $a = 1$. Then, $L \cong X \perp \mathbb{Z}$. From the proof of [15, Proposition 3.1], $L_\sigma \cong \mathbb{Z}[\zeta_3]$ and $dL_\sigma = 3 \cdot \alpha$ where α is a square. Additionally, we know that $[L : L_\sigma \perp L^\sigma] = 3$, implying that $dL_\sigma \cdot dL^\sigma = 4p \cdot 3^2$. Therefore, $dL_\sigma = 3$ or 12. If $dL_\sigma = 3$, by Hermite's Inequality, we have that $\min(L_\sigma) \leq 2$, which is a contradiction. Suppose that $dL_\sigma = 12$. Then, $dL^\sigma = 3p$. This implies that $(L^\sigma)_2$ is an odd unimodular $\mathbb{Z}_2$-lattice, which is impossible for either genus. Therefore, with all cases considered, we can conclude that $q \neq 3$ and $O(L)$ has no elements of odd order. $\square$

Let $\sigma \in O(L)$ have order 2. In this situation, $L_\sigma = \{v \in L : \sigma(v) = -v\}$. Considering L as a $\mathbb{Z}[\sigma]$-module, L can be written as $T^a \oplus I^b \oplus \mathbb{Z}^c$ for some $a, b, c \in \mathbb{Z}_{\geq 0}$ where T is a rank 2 indecomposable module and I is a nontrivial rank 1 module [7]. Additionally, L^σ and L_σ have the following properties found in both [15] and [4]:

- L_σ has rank $(a + b)$ and L^σ has rank $(a + c)$.
- Both L^σ and L_σ are primitive sublattices of L with dL^σ and dL_σ divisible by 2^a.

- The quotient group $L/(L^\sigma \perp L_\sigma)$ is an elementary 2-group and $[L : L^\sigma \perp L_\sigma]$ is 2^a.

Now, we are prepared to prove the following proposition [6, Prop 3.2].

Proposition 1. *Let L be a lattice in $\mathcal{G} \cup \mathcal{G}'$. If $\min(L) \geq 4$ and $O(L)$ is nontrivial, then $O(L) = \langle -1_L, \sigma \rangle$ where $\sigma = \tau_v$ where v is a primitive vector of length 4 in L.*

Proof. Let σ be a nontrivial isometry of L. Then, by Lemma 1, the order of σ must be a power of 2. Suppose that σ has order 2^k. Now, for $k \geq 2$, the order of $\sigma^{2^{k-1}}$ is 2. Suppose that $\sigma^{2^{k-1}} = -1$. Then, $(\sigma^{2^{k-2}})^2 = -1$ and by [15, Lemma 2.1], this implies that dL is a square, which is not possible. Thus, there exists some $\sigma \in O(L)$ of order 2 such that $\sigma \neq -1$. We claim that either L_σ or $L_{-\sigma}$ is a rank one sublattice generated by a vector of length 4. To prove this claim, we consider all possible combinations of a, b, and c for L as the $\mathbb{Z}[\sigma]$-module $T^a \oplus I^b \oplus \mathbb{Z}^c$.

First, consider the case where $a = 0$. In this case, we have $L = L^\sigma \perp L_\sigma$. Since there are no even unimodular lattices of rank less than 8 [18, 106:1], neither dL^σ nor dL_σ can be 1. Further, if either L^σ or L_σ has discriminant p, then because L is even, both $\text{rank}(L^\sigma)$ and $\text{rank}(L_\sigma)$ equal 2. By changing σ to $-\sigma$ if necessary, we may assume that $dL^\sigma = p$, which means that $dL_\sigma = 4$. However, by Hermite's Inequality, $\min(L_\sigma) < 3$, which contradicts $\min(L) \geq 4$. Thus, dL^σ is either 2 or $2p$.

By changing σ to $-\sigma$ if necessary, we may assume that $dL^\sigma = 2$. Now, it must be that the rank of L^σ is 1 or 3. If the rank of L^σ is 1, then $\min(L^\sigma) = 2$, and if the rank of L^σ is 3, then $\min(L^\sigma) < 2$ by Hermite's Inequality. So, in both situations, we contradict the fact that $\min(L) \geq 4$. Therefore, a cannot equal 0.

Now, suppose that $a = 2$. Then, L^σ and L_σ are binary, and both dL^σ and dL_σ are divisible by 4. Furthermore,

$$dL^\sigma \cdot dL_\sigma = dL[L : L^\sigma \perp L_\sigma]^2 = 4p \cdot 16.$$

We may assume that p does not divide dL_σ by changing σ to $-\sigma$ if necessary. Then, by Hermite's Inequality and because $\min(L) \geq 4$, it follows that $dL_\sigma = 16$ and $\min(L_\sigma) = 4$. Thus, $L_\sigma \cong < 4 > \perp < 4 >$. Further, $dL^\sigma = 4p$ and $(L^\sigma)_2 \cong < 2\epsilon, 2\epsilon p >$ for some $\epsilon \in \{1, 3, 5, -1\}$. The Hasse symbol of the space $[4, 4, 2\epsilon, 2\epsilon p]$ at 2 is

$$S_2([4, 4, 2\epsilon, 2\epsilon p]) = \begin{cases} -1 & \text{if } p \equiv -1 \bmod 8, \\ 1 & \text{if } p \equiv 3 \bmod 8. \end{cases}$$

Since $\mathbb{Q}_2 L_2$ and $[4, 4, 2\epsilon, 2\epsilon p]$ are isometric, $S_2(\mathbb{Q}_2 L_2) = S_2([4, 4, 2\epsilon, 2\epsilon p])$; so $L \in \mathcal{G}'$. A direct computation shows that all choices of ϵ result in lattices isometric to $< -2, -2p >$ over $\mathbb{Z}_2$. Thus, we may simply take $\epsilon = -1$ and then $(L^\sigma)_2 \cong < -2, -2p >$.

Let e and f be vectors in L_σ such that $\mathrm{Mat}(e, f) = < 4, 4 >$ where $\mathrm{Mat}(e, f)$ denotes the Gram matrix $\begin{pmatrix} Q(e) & B(e, f) \\ B(e, f) & Q(f) \end{pmatrix}$. Let x and y be vectors in L^σ such that $\mathrm{Mat}(x, y) \equiv < -2, -2p > \bmod 64$. Then,

$$L = (L^\sigma \perp L_\sigma) + \mathbb{Z}\left[\frac{x + y}{2}, \frac{e + f + x + y}{2}\right].$$

However, this implies that $\frac{e+f}{2}$ is an element of L, which cannot be the case since $Q\left(\frac{e+f}{2}\right) = 2$. Thus, a cannot equal 2.

Finally, suppose that $a = 1$. Then, there are three cases. First, consider both b and c equal to 1. Then, both L^σ and L_σ are binary and their discriminants are divisible by 2. Further, $dL^\sigma \cdot dL_\sigma = 4p \cdot 4$. By changing σ to $-\sigma$ if necessary, we may assume that p divides dL^σ. Then, dL_σ is at most 8. However, by Hermite's

Inequality, this would imply that $\min(L_\sigma) = 2$, which is a contradiction. Thus, when $a = 1$, both b and c cannot equal 1.

Now, if $b = 2$ and $c = 0$, then $\text{rank}(L^\sigma) = 1$ and $\text{rank}(L_\sigma) = 3$, and if $b = 0$ and $c = 2$, then $\text{rank}(L^\sigma) = 3$ and $\text{rank}(L_\sigma) = 1$. So, without loss of generality, assume that the rank of L_σ is 1. Then, $\text{rank}(L^\sigma) = 3$ and both dL^σ and dL_σ are divisible by 2. Further, $dL^\sigma \cdot dL_\sigma = 4p \cdot 4$. If p does not divide dL^σ, then $\min(L^\sigma) \leq 2$ for all possible dL^σ by Hermite's Inequality. Thus, p must divide dL^σ. So, dL^σ is equal to one of $2p, 4p$, or $8p$.

If $dL^\sigma = 8p$, then $dL_\sigma = 2$. Since the rank of L_σ is 1, L contains a vector of length 2, which is impossible. So, dL^σ is not equal to $8p$. Now, if $dL^\sigma = 2p$, over $\mathbb{Z}_2$, $(L^\sigma)_2 \cong \mathbb{H} \perp < -2p > \cong \mathbb{A} \perp < 6p >$, and L is in $\mathcal{G}'$. Further, since $(L^\sigma \perp L_\sigma)_2 \cong \mathbb{H} \perp < -2p > \perp < 8 >$ is contained in $L_2 \cong \mathbb{H} \perp < 2, -2p >$,

$$L = (L^\sigma \perp L_\sigma) + \mathbb{Z}\left[\frac{x}{2}\right]$$

where x is the vector generating L_σ. However, $Q(\frac{x}{2}) = 2$, which contradicts the minimum of L. So, dL^σ cannot equal $2p$, and it must be that $dL^\sigma = 4p$ and $dL_\sigma = 4$. Therefore, $\sigma = \tau_v$ where v is the vector of length 4 generating L_σ. This proves our initial claim.

From above, it follows that $R(L)^*$ is nonempty, and further, if $u \in R(L)^*$, then $Q(u) = 4$. Therefore, $R(L)^*$ will be the orthogonal sum of $\mathbf{A}_n^2$ for some $n \geq 1$. However, if $n \geq 2$, then L has an isometry of odd order, which is impossible. So, $R(L)^*$ must be the orthogonal sum of m copies of $\mathbf{A}_1^2$. But, by the argument in the case of $a = 2$, if $m \geq 2$, we contradict the minimum of L. Thus, $m = 1$ and $R(L)^* = \mathbf{A}_1^2$.

It remains to show that $O(L) = \langle -1_L, \sigma \rangle$. Because L^σ is an even ternary lattice of discriminant $4p$,

$$(L^\sigma)_2 \cong \mathbb{H} \perp < -4p > \quad \text{or} \quad (L^\sigma)_2 \cong \mathbb{A} \perp < 12p >,$$

depending on the genus of L and whether $p \equiv -1$ or $3 \bmod 8$. Suppose that $(L^\sigma)_2 \cong \mathbb{H} \perp < -4p >$. Let v be a vector in L_σ with $Q(v) = 4$ such that $L_\sigma \cong \mathbb{Z}[v]$. Let x, y, and z be vectors in L^σ such that $\mathrm{Mat}(x, y, z) \equiv \mathbb{H} \perp < -4p >$ mod 64. Then,

$$L = (L_\sigma \perp L^\sigma) + \mathbb{Z}\left[\frac{v+z}{2}\right],$$

and L is uniquely determined by L_σ and L^σ. The same happens when $(L^\sigma)_2 \cong \mathbb{A} \perp < 12p >$. Note that $R_L^* \cong L_\sigma$ and so any isometry of L will stabilize $L_\sigma \perp L^\sigma$. Further, if ρ is an isometry of $L_\sigma \perp L^\sigma$, then $\rho(L)$ is a lattice containing $L_\sigma \perp L^\sigma$. Because there is only one lattice containing $L_\sigma \perp L^\sigma$, ρ is also an isometry of L. Thus, $O(L) = O(L_\sigma) \times O(L^\sigma)$. Now, suppose $O(L^\sigma)$ is nontrivial. By [15, Lemma 2.1], since the rank of L^σ is 3, there exists an isometry $\phi \neq -1_{L^\sigma}$ of order 2 in $O(L^\sigma)$. Then, the previous argument shows that $\phi = \tau_u$ or $-\tau_u$ for some vector $u \in L^\sigma$ of length 4. However, this implies that $\tau_v \circ \phi \neq -1_L$ is an isometry of order 2 in $O(L)$. In this case, both the fixed and variant sublattices of $\tau_v \circ \phi$ are binary, which we have shown cannot occur. Thus, $O(L^\sigma)$ is trivial and $O(L) =< -1_L, \tau_v >$. □

From the proof of Proposition 1, we have the following corollary.

Corollary 1. *Let L be a lattice in $\mathcal{G} \cup \mathcal{G}'$. If $\min(L) \geq 4$ and L has an isometry other than ± 1, then $\min(L) = 4$, $R(L)^* = \boldsymbol{A}_1^2$, and $|O(L)| = 4$.*

2.3.2 Decomposability

In this section, we determine the decomposability of the lattices in $\mathcal{G}$ and $\mathcal{G}'$.

Lemma 2. *If a lattice L in $\mathcal{G}'$ is decomposable, then L has $< 2 >$ as an indecomposable component. However, every lattice in $\mathcal{G}$ is indecomposable.*

Proof. Let L be a lattice in $\mathcal{G} \cup \mathcal{G}'$. Suppose that L is decomposable. Then, L can be written as the orthogonal sum of indecomposable components. Since L has rank 4, it can be the orthogonal sum of at most four indecomposable components. Suppose L is the orthogonal sum of four indecomposable components. The rank of each component must be 1. Since $dL = 4p$, at least one of these components is unimodular over $\mathbb{Z}_2$, which is impossible.

Suppose that L decomposes into two rank 1 components and one rank 2 indecomposable component. Then, since $dL = 4p$ and L is even, it must be that $L \cong < 2 > \perp < 2 > \perp N$ where N is an even binary lattice of discriminant p. By considering the localization of L at 2 in this case, we deduce that $L_2 \cong < 2, 2 > \perp \mathbb{P}$ where $\mathbb{P} = \mathbb{H}$ or $\mathbb{A}$ depending on $p \equiv -1$ or $3 \bmod 8$. Therefore, if L decomposes in this way, L is an element of $\mathcal{G}'$.

Now, suppose that L decomposes into one rank 1 component and one rank 3 indecomposable component. Then, there are two possible forms L can take:

- $< 2 > \perp K$ where K is an even ternary lattice of discriminant $2p$.
- $< 2p > \perp K$ where K is an even ternary lattice of discriminant 2.

Suppose L takes the second form. Then, since $dK = 2$, $\min(K) < 2$ by Hermite's Inequality and $\min(K) = 1$, which is impossible since K is even. If L takes the first form, then $K_2 \cong \mathbb{H} \perp < -2p > \cong \mathbb{A} \perp < 6p >$, which implies that L is in $\mathcal{G}'$.

Finally, suppose that $L = M \perp K$ where M and K are indecomposable binary even lattices. Without loss of generality, since $dL = 4p$ and there are no binary even unimodular lattices, we may assume that $dK = 2$ or 4. If $dK = 2$, then $\min(K) < 2$, which is impossible. On the other hand, if $dK = 4$, then $\min(K) < 3$; so $\min(K) = 2$. This implies that $K \cong < 2 > \perp < 2 >$, which contradicts the fact that K is indecomposable. Therefore, L cannot decompose into two indecomposable binary even lattices.

In conclusion, if $L \in \mathcal{G}'$ is decomposable, then L has an indecomposable component isometric to $< 2 >$. Further, L takes one of the following forms:

- $< 2 > \perp K$ where K is an indecomposable even ternary lattice of discriminant $2p$.
- $< 2 > \perp < 2 > \perp N$ where N is an even binary lattice of discriminant p.

It is now clear that if L is in $\mathcal{G}$, then L is indecomposable. $\square$

Chapter 3

The Principal Genus

Throughout this chapter, all lattices will be in the principal genus $\mathcal{G}$. We begin by determining all possible root systems of the lattices in $\mathcal{G}$. From there, we will determine the scaled root systems and show that the orthogonal group of a lattice in $\mathcal{G}$ is generated by symmetries with respect to the vectors in the scaled root system and -1_L. Finally, we prove the linear independence of the degree 2 theta series associated to the classes in $\mathcal{G}$ with nontrivial orthogonal group.

3.1 Root Systems

In this section, we will determine all possible root systems of the lattices in $\mathcal{G}$. Recall that for a lattice L in $\mathcal{G}$, $L_p \cong < 1, 1, \delta, \delta p >$ where 2δ is a nonsquare mod p and $L_2 \cong \mathbb{H} \perp < -2, 2p > \cong \mathbb{A} \perp < -2, -6p >$.

Let L be a lattice in $\mathcal{G}$. Since the rank of L is 4, the possible root systems of L are: $\emptyset$, $\mathbf{A}_1$, $2\mathbf{A}_1$, $\mathbf{A}_2$, $3\mathbf{A}_1$, $\mathbf{A}_2 \perp \mathbf{A}_1$, $\mathbf{A}_3$, $4\mathbf{A}_1$, $\mathbf{A}_2 \perp \mathbf{A}_2$, $\mathbf{A}_2 \perp 2\mathbf{A}_1$, $\mathbf{A}_3 \perp \mathbf{A}_1$, $\mathbf{A}_4$, and $\mathbf{D}_4$. The discriminant of each possible full rank root sublattice is given in the following table:

Root Sublattice	$4A_1$	$A_2 \perp A_2$	$A_2 \perp 2A_1$	$A_3 \perp A_1$	A_4	D_4
Discriminant	16	9	12	8	5	4

If R_L is full rank in L, then $dR_L = dL[L : R_L]^2$. However, $dL = 4p$ where $p > 13$ is a prime congruent to 3 mod 4. Thus, L cannot have a root sublattice of full rank.

Lemma 3. *If L is a lattice in $\mathcal{G}$, then $R(L)$ cannot equal $3\boldsymbol{A}_1$ or $\boldsymbol{A}_2 \perp \boldsymbol{A}_1$.*

Proof. Let L be a lattice in $\mathcal{G}$ and suppose that $R(L) = 3\mathbf{A}_1$. Then, $\mathbb{Q}L \cong [2, 2, 2, 2p]$. However, the Hasse symbol of $[2, 2, 2, 2p]$ at 2 is $(p, -2)_2$, while the Hasse symbol of $\mathbb{Q}_2 L_2 \cong \mathbb{H} \perp [-2, 2p]$ is $-(p, -2)_2$; a contradiction.

Now, suppose that $R(L) = \mathbf{A}_2 \perp \mathbf{A}_1$. Note that $(A_2 \perp A_1)_2 \cong \mathbb{A} \perp < 2 >$. Then, since $\mathbb{A}$ splits $L_2 \cong \mathbb{A} \perp < -2, -6p >$, 2 must be represented by $< -2, -6p >$ over $\mathbb{Z}_2$. Equivalently, 1 is represented by $< -1, -3p >$ over $\mathbb{Z}_2$. When $p \equiv 3 \mod 8$, $< -1, -3p > \cong < -1, -1 >$, which obviously does not represent 1. Similarly, when $p \equiv -1 \mod 8$, $< -1, -3p > \cong < -1, 3 >$, which represents 1 only if there exist $x, y \in \mathbb{Z}_2$ such that $-x^2 + 3y^2 \equiv 1 \mod 8$. However, through direct verification, we see that this is impossible. Thus, $R(L)$ cannot be $\mathbf{A}_2 \perp \mathbf{A}_1$. $\square$

Thus, for any lattice L in $\mathcal{G}$, $R(L)$ is equal to one of the following: $\emptyset$, $\mathbf{A}_1$, $2\mathbf{A}_1$, $\mathbf{A}_2$, or $\mathbf{A}_3$.

Lemma 4. *If L is a lattice in $\mathcal{G}$ and $R(L) = \boldsymbol{A}_3$ or $2\boldsymbol{A}_1$, then $p \equiv 3 \mod 8$.*

Proof. Let L be a lattice in $\mathcal{G}$ such that $R(L) = \mathbf{A}_3$. Over $\mathbb{Z}_2$, $(A_3)_2 \cong \mathbb{A} \perp < 12 >$. Therefore, over $\mathbb{Z}_2$, $< -2, -6p >$ represents 12, or equivalently,

$< -1, -3p >$ represents 6. When $p \equiv -1 \mod 8$, $< -1, -3p > \cong < -1, 3 >$ represents 6 only if there exist $x, y \in \mathbb{Z}_2$ such that $-x^2 + 3y^2 \equiv 6 \mod 8$. This is impossible by a direct verification. Thus, if $R(L) = \mathbf{A}_3$, then $p \equiv 3 \mod 8$.

Now, suppose that $R(L) = 2\mathbf{A}_1$. Then, $\mathbb{Q}_2 L_2 \cong [2, 2, \epsilon, \epsilon p]$ for some $\epsilon \in \{1, 3, 5, -1\}$. Then, $S_2([2, 2, \epsilon, \epsilon p]) = -1$ when $p \equiv -1 \mod 8$ no matter what the value of ϵ is. However, as noted earlier, the Hasse symbol of $\mathbb{Q}_2 L_2$ at 2 is $-(p, -2)_2$. So,

$$S_2(\mathbb{Q}_2 L_2) = \begin{cases} 1 & \text{if } p \equiv -1 \bmod 8, \\ -1 & \text{if } p \equiv 3 \bmod 8. \end{cases}$$

Thus, $\mathbb{Q}_2 L_2$ is not isometric to $[2, 2, \epsilon, \epsilon p]$ when $p \equiv -1 \mod 8$. This shows that $p \equiv 3 \mod 8$ if $R(L) = 2\mathbf{A}_1$. □

3.2 Scaled Root Systems and $O(L)$

In this section, we determine all possible scaled root systems of the lattices in $\mathcal{G}$ and show that the orthogonal group of a lattice in $\mathcal{G}$ is generated by symmetries with respect to the vectors in the scaled root system and -1_L.

Every positive definite $\mathbb{Z}$-lattice has a Minkowski reduced basis. A thorough discussion of the Minkowski reduced basis can be found in [3, §12.1]. We will make use of the following property of a Minkowski reduced basis. If $\{v_1, \dots, v_n\}$ is a Minkowski reduced basis of L, then $0 < Q(v_1) \le Q(v_2) \le \cdots \le Q(v_n)$ and $|2B(v_i, v_j)| \le Q(v_i)$ for $1 \le i < j \le n$. The *successive minima* [3, §12.2] of a positive $\mathbb{Z}$-lattice L are defined as follows: The *jth* minimum $\mu_j(L)$ of L is the positive number such that

- the set of integral $v \in L$ with $Q(v) \le \mu_j(L)$ spans a subspace of rank $\ge j$;
- the set of integral $v \in L$ with $Q(v) < \mu_j(L)$ spans a subspace of rank $< j$.

It follows from this definition that $\min(L) = \mu_1(L)$ and $\mu_1(L) \leq \cdots \leq \mu_n(L)$. Further, L contains a set of linearly independent vectors v_j such that $Q(v_j) = \mu_j(L)$. Both the successive minima and Minkowski reduced basis will be useful in determining the structure of lattices in $\mathcal{G}$.

Now, we determine the orthogonal complement of a root in L.

Lemma 5. *Let L be a lattice in $\mathcal{G}$ with $\min(L) = 2$ and $v \in L$ such that $Q(v) = 2$. Let K be the orthogonal complement of $\mathbb{Z}[v]$ in L. Then, $dK = 8p$, $K_2 \cong < -2, -2, 2p >$ and $K_p \cong < 1, 2\delta, \delta p >$.*

Proof. It is clear that K is an even, ternary lattice. Since $dK|(2 \cdot dL)$ and $2 \cdot dK = dL[L : \mathbb{Z}[v] \perp K]^2$, dK is either $2p$ or $8p$. Suppose that $dK = 2p$. Then, $[L : \mathbb{Z}[v] \perp K] = 1$, and L is decomposable, which is impossible by Lemma 2. Thus, we must have $dK = 8p$.

Since K is even, K_2 cannot have a unimodular component of odd rank. Further, K_2 cannot have a unimodular component of rank 2 or else this component would split L_2, implying that either $< -2, 2p >$ or $< -2, -6p >$ represents 2, which we have shown to be impossible. Thus, K_2 must be a (2)-modular $\mathbb{Z}_2$-lattice. Since $\mathbb{Q}_2 L_2 \cong [2] \perp \mathbb{Q}_2 K_2$, we have

$$S_2(\mathbb{Q}_2 L_2) = (2,2)_2 (2,8p)_2 S_2(\mathbb{Q}_2 K_2) = \begin{cases} S_2(\mathbb{Q}_2 K_2) & \text{if } p \equiv -1 \bmod 8, \\ -S_2(\mathbb{Q}_2 K_2) & \text{if } p \equiv 3 \bmod 8. \end{cases}$$

This forces $S_2(\mathbb{Q}_2 K_2) = 1$, which means that K_2 is anisotropic [9, Prop 4.21]. Thus, $K_2 \cong 2\mathbb{A} \perp < 6p > \cong < -2, -2, 2p >$.

Since $< 2 >$ is a unimodular $\mathbb{Z}_p$-lattice, it must split L_p. Therefore, $< 2 > \perp K_p \cong L_p \cong < 1, 1, \delta, \delta p >$, and hence $K_p \cong < 2, \delta, \delta p > \cong < 1, 2\delta, \delta p >$. $\square$

Lemma 6. *Let L be a lattice in $\mathcal{G}$ and K the orthogonal complement of R_L in L. Then,*

1. *If $R(L) = \boldsymbol{A}_1$, then $dK = 8p$, $K_2 \cong< -2, -2, 2p >$ and $K_p \cong< 1, 2\delta, \delta p >$.*
2. *If $R(L) = 2\boldsymbol{A}_1$, then $dK = 4p$, $K_2 \cong 2\mathbb{A}$, and $K_p \cong< \delta, \delta p >$.*
3. *If $R(L) = \boldsymbol{A}_2$, then $dK = 12p$, $K_2 \cong< -2, -6p >$, $K_p \cong< 3\delta, \delta p >$, and $K_3 \cong< p, 3 >$.*
4. *If $R(L) = \boldsymbol{A}_3$, then $dK = 4p$ and $K \cong< 4p >$.*

Proof. (1) This is a consequence of Lemma 5.

(2) Suppose that $R(L) = 2\mathbf{A}_1$. Then, $p \equiv 3 \bmod 8$ by Lemma 4 and K is a binary, even lattice. Since $dK|(4 \cdot dL)$ and $4 \cdot dK = dL[L : 2A_1 \perp K]^2$, it must be that $dK = p, 4p$, or $16p$. But $dK \neq p$; otherwise $[L : 2A_1 \perp K] = 1$, and L is decomposable, which is impossible by Lemma 2.

Recall that $2A_1 = A_1 \perp A_1 =< 2 >\perp< 2 >$. Then, $< 2 >\perp K$ is a sublattice of the orthogonal complement of a minimal vector in L. Lemma 5 implies that $< 2 >\perp K_2$ is represented by $< -2, -2, 2p >$. Then, since $< 2 >$ splits $< -2, -2, 2p >$ as $\mathbb{Z}_2$-lattices, it must be that $< 2 >\perp K_2 \cong< -2, -2, 2p >$, which forces $dK = 4p$.

If K_2 is a (2)-modular proper $\mathbb{Z}_2$-lattice, then $K_2 \cong< 2\epsilon, 2\epsilon p >$ for some $\epsilon \in \{1, 3, 5, -1\}$. However, $[1, \epsilon, \epsilon p]$ is not isometric to $[-1, -1, p]$ for any ϵ since their Hasse symbols are never equal. Thus, K_2 must be improper. Since $p \equiv 3 \bmod 8$, it follows that $K_2 \cong 2\mathbb{A}$.

Since $dK_p = 4p$, K_p must have a rank 1 unimodular component and a rank 1 (p)-modular component. Note that $(2A_1)_p \cong< 1, 1 >$, which is unimodular. Therefore, $(2A_1 \perp K)_p \cong < 1,1 > \perp K_p \cong < 1,1,\delta,\delta p >$, implying $K_p \cong < \delta, \delta p >$.

(3) Suppose $R(L) = \mathbf{A}_2$. Over $\mathbb{Z}_2$, A_2 is isometric to $\mathbb{A}$, which is even unimodular and splits L_2. Since $L_2 \cong \mathbb{A} \perp < -2, -6p >$, $K_2 \cong < -2, -6p >$. Over $\mathbb{Z}_p$, A_2 is isometric to $< 1, 3 >$ and $A_2 \perp K_p \cong L_p$. By comparing the Hasse symbols, we see that $K_p \cong < 3\delta, \delta p >$.

Finally, let us determine the structure of K_3. Note that $dK_3 = 3p$, $L_3 \cong < 1,1,1,p >$ and $S_3(\mathbb{Q}_3 L_3) = 1$. Through Hasse symbol calculations, we determine $\mathbb{Q}_3 K_3 \cong [p, 3]$, and hence $K_3 \cong < p, 3 >$.

(4) Suppose $R(L) = \mathbf{A}_3$. By Lemma 4, $p \equiv 3 \mod 8$; so $L_2 \cong \mathbb{A} \perp < -2, -2 >$. Since $(A_3)_2 \cong \mathbb{A} \perp < 12 >$, K_2 is the orthogonal complement of $< 12 >$ in $< -2, -2 >$, which is isometric to $< 12 >$. At $q \neq 2$, $(A_3)_q$ is unimodular and splits L_q. Therefore, $K \cong < 4p >$.

□

We can now proceed with the determination of the possible scaled root systems of L and the structure of $O(L)$. To do so, we need the following definitions. Let v be a nonzero vector in $\mathbb{Q}L$ and $\mathfrak{a}_v = \{a \in \mathbb{Q} : av \in L\}$ be the *coefficient of* v with respect to L, which is a fractional ideal. The positive generator of $\mathfrak{a}_v$ is called the *conductor* of v with respect to L.

A positive definite $\mathbb{Z}$-lattice L with $dL = \epsilon p$, where p is an odd prime, is called *primal* if (i) $\epsilon = 1$ and either L is odd or L is even of even rank, or (ii) $\epsilon = 2$ and L is even of odd rank [15, p. 78]. We will make use of the following property of primal lattices [15, Corollary 4.5].

Lemma 7. *Let L be a primal lattice, which is not necessarily indecomposable. If L is even (or odd) of rank less than 16 (or 13, respectively), then $O(L)$ is generated by -1 and symmetries with respect to the minimal vectors of length* 2 *in L.*

For other useful properties of primal lattices, we refer the reader to [15].

Proposition 2. *Let L be a lattice in $\mathcal{G}$ such that $O(L)$ is nontrivial. Then, $R(L)^*$ is one of the following: $\boldsymbol{A}_1^2$, $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, $\boldsymbol{A}_2 \perp \boldsymbol{A}_1$, $\boldsymbol{C}_2$, $\boldsymbol{C}_3 \perp \boldsymbol{A}_1^{2p}$, or $\boldsymbol{A}_1 \perp \boldsymbol{A}_1^2$. Further, $O(L)$ is generated by -1_L and symmetries.*

Proof. We will proceed with cases corresponding to the possible root systems of the lattices in $\mathcal{G}$.

- Suppose that $R(L) = \emptyset$. Then, $\min(L) \geq 4$ and by Corollary 1, $\min(L) = 4$ and $R(L)^* = \mathbf{A}_1^2$. Further, $O(L)$ is generated by -1_L and symmetries.

- Suppose that $R(L) = \mathbf{A}_3$. Note that $p \equiv 3 \bmod 8$ by Lemma 4. Then, the sublattice $M = R_L \perp \mathbb{Z}[z]$, where $Q(z) = 4p$, has index 2 in L. Moreover, any lattice in $\mathcal{G}$ containing R_L must also contain M. Let $\{v, x, y\} \subset R_L$ so that $\mathrm{Mat}(x, y, z) \equiv A_2 \perp < 12 > \bmod 64$. Then, to obtain a lattice in $\mathcal{G}$ containing M, we can adjoin only $\frac{y \pm z}{2}$ since these are the only vectors in $\mathbb{Q}M$ with conductor 2 with respect to M representing an even integer. However, $M + \mathbb{Z}[\frac{y+z}{2}]$ and $M + \mathbb{Z}[\frac{y-z}{2}]$ are the same lattice. Thus, we must have $L = M + \mathbb{Z}[\frac{y+z}{2}]$, and L is the only lattice in $\mathcal{G}$ that contains M.

Note that τ_z fixes every vector in R_L and sends $\frac{y+z}{2}$ to $\frac{y+z}{2} - z$, which is in L. So, τ_z is in $O(L)$. Since z is also primitive in L, z is in $R(L)^*$. Thus, if $R(L) = \mathbf{A}_3$, then $\mathbf{A}_3 \perp \mathbf{A}_1^{2p} \subset R(L)^*$.

Now, $O(L) < O(R_L) \times O(\mathbb{Z}[z])$, but since any $\sigma \in O(R_L) \times O(\mathbb{Z}[z])$ preserves $M = R_L \perp \mathbb{Z}[z]$ and L is the only one lattice in $\mathcal{G}$ containing M, it must be that $\sigma(L) = L$. Thus, $O(L) = O(R_L) \times O(\mathbb{Z}[z])$. But $O(R_L) = O(A_3) = O(C_3)$; therefore, $R(L)^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$ and $O(L) = O(R_L^*) = \langle -1_L, W(R_L^*)\rangle$.

• Suppose that $R(L) = \mathbf{A}_2$ and let K be the orthogonal complement of R_L in L. Then, the sublattice $M = R_L \perp K$ has index 3 in L. Let $\{v, x\}$ be a basis for R_L such that $\mathrm{Mat}(v, x) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and $\{y, z\} \subset K$ so that $\mathrm{Mat}(y, z) \equiv < 3, p >$ mod 27. Then, $\frac{v-2x+y}{3}$ and $\frac{v-2x-y}{3}$ are the only vectors in $\mathbb{Q}M$ with conductor 3 with respect to M that can be adjoined to M to obtain a lattice in $\mathcal{G}$. Note that $M + \mathbb{Z}[\frac{v-2x+y}{3}]$ is isometric to $M + \mathbb{Z}[\frac{v-2x-y}{3}]$ via the map $1_{R_L} \perp -1_K$. Thus, up to isometry, there is one lattice in $\mathcal{G}$ containing M. Further, this implies that $-1_K \notin O(L)$ for any L containing M.

Consider $\langle -1_L, W(R_L)\rangle < O(L) < O(R_L) \times O(K)$. If $O(K) = \{\pm 1_K\}$, we must have that $R(L) = R(L)^* = \mathbf{A}_2$. Further, since $-1_K \notin O(L)$ and $\langle -1_L, W(R_L)\rangle$ has index 2 in $O(R_L) \times O(K)$, we must have $O(L) = \langle -1_L, W(R_L)\rangle$ $= \langle -1_L, W(R_L^*)\rangle$.

Suppose that $O(K) \neq \{\pm 1_K\}$. If $O(K)$ contains some element σ of odd prime order q, then by an argument similar to the proof of Lemma 1, we can eliminate primes $q > 3$. If the order of σ is 3, then $dK = 3\alpha$ for some square α by [15, Lemma 2.2]. However, since $dK = 12p$, this is impossible. Thus, $O(K)$ contains no elements of odd order. Further, if $\sigma \in O(K)$ is an element of order 2 not equal to -1_K, then the rank of L^σ or L_σ is 1. Thus, σ or $-\sigma$ is a symmetry and all order 2 elements of $O(K)$ are either -1_K or $\pm 1_K$ composed with a symmetry.

Let $N = K^{1/2}$. Then, $dN = 3p$, $N_2 \cong < -1, -3p >$, $N_p \cong < 6\delta, 2\delta p >$, and $N_3 \cong < 6, 2p >$. Let u be an element of $R(N)^*$ and w be another element in N so that $N = \mathbb{Z}[u, w]$. Then, since τ_u is an isometry of N and $\tau_u(w) = w - \frac{2B(u,w)}{Q(u)}u$, it must be that $Q(u)$ divides $2B(u, w)$. Because

$$N \cong \begin{pmatrix} Q(u) & B(u,w) \\ B(u,w) & Q(w) \end{pmatrix},$$

we have $3p = Q(u)Q(w) - B(u, w)^2$. It follows that $Q(u)$ divides $6p$. Now, according to Gauss' Theory as described in [3, §14.4], since there are two distinct primes dividing $dN = 3p$ and $dN \equiv 1 \bmod 4$, there are four ambiguous classes of positive definite binary lattices with discriminant $3p$ when $p \equiv 3 \bmod 4$. Using the fact that the length of a vector in $R(N)^*$ divides $6p$, we determine the four ambiguous classes by their Gram matrices as follows:

$$\begin{pmatrix} 1 & 0 \\ 0 & 3p \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 \\ 1 & \frac{3p+1}{2} \end{pmatrix}, \quad \begin{pmatrix} 3 & 0 \\ 0 & p \end{pmatrix}, \quad \begin{pmatrix} 6 & 3 \\ 3 & \frac{p+3}{2} \end{pmatrix}.$$

Considering the localization at 2, we see that N is not in the first class since they are not in the same genus. Similarly, we can eliminate the third class by considering the localization at 3.

Suppose that $N \cong \begin{pmatrix} 6 & 3 \\ 3 & \frac{p+3}{2} \end{pmatrix}$. Then, $K \cong \begin{pmatrix} 12 & 6 \\ 6 & p+3 \end{pmatrix}$, which has only one pair of vectors of length 12. Let $y' \in K$ such that $Q(y') = 12$. Now, the vector $\frac{v-2x+y'}{3}$ can be adjoined to M to obtain a lattice in $\mathcal{G}$, which must be isometric to L. However, y' has length 2, which contradicts the fact that our root system is $\mathbf{A}_2$. Thus, if N is ambiguous, we must have $N \cong \begin{pmatrix} 2 & 1 \\ 1 & \frac{3p+1}{2} \end{pmatrix}$ and hence $K \cong \begin{pmatrix} 4 & 2 \\ 2 & 3p+1 \end{pmatrix}$. Over $\mathbb{Z}_2$,

$$\begin{pmatrix} 4 & 2 \\ 2 & 3p+1 \end{pmatrix} \cong \begin{cases} 2 < 5,5 > & \text{if} \quad p \equiv 3 \bmod 8, \\ 2 < -1,3 > & \text{if} \quad p \equiv -1 \bmod 8. \end{cases}$$

However, when $p \equiv 3 \bmod 8$, $K_2 \cong < -2, -6p > \cong 2 < -1, -1 >$, which is not isometric to $2 < 5,5 >$ since they are not isometric as quadratic spaces over $\mathbb{Q}_2$. Thus, $p \equiv -1 \bmod 8$. Over $\mathbb{Z}_3$,

$$\begin{pmatrix} 4 & 2 \\ 2 & 3p+1 \end{pmatrix} \cong < 4, 3p > \cong < 1, 3p > .$$

Since $K_3 \cong < 3, p >$, $S_3(\mathbb{Q}_3 K_3) = S_3([1, 3p])$. Because $S_3(\mathbb{Q}_3 K_3) = -(p,3)_3$ and $S_3([1,3p]) = -1$, it must be that $(p,3)_3 = 1$, which implies $p \equiv 1 \bmod 3$. Therefore, $p \equiv -1 \bmod 8$ and $p \equiv 1 \bmod 3$ in this case.

The symmetry with respect to the vector e of length 4 in K and 1_K are the only elements of $O(K)$ that extend to an isometry of a lattice L in $\mathcal{G}$ containing M. Because e is also primitive, $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1^2$. Consider $\langle -1_L, W(R_L^*) \rangle < O(L) < O(R_L) \times O(K)$. Then, since $\langle -1_L, W(R_L^*) \rangle$ has index 2 in $O(R_L) \times O(K)$ and $-1_K \notin O(L)$, $O(L) = \langle -1_L, W(R_L^*) \rangle$.

- Suppose that $R(L) = 2\mathbf{A}_1$. Note that $p \equiv 3 \bmod 8$ by Lemma 4. The sublattice $M = R_L \perp K$ has index 2 in L. Let $\{v, x\}$ be a basis for R_L such that $\mathrm{Mat}(v,x) = < 2, 2 >$ and $\{y, z\} \subset K$ such that $\mathrm{Mat}(y,z) \equiv \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}$ mod 32. Then, there are three vectors of conductor 2 with respect to M that can be adjoined to M to obtain a lattice in $\mathcal{G}$. These vectors are $\frac{v+x+y}{2}$, $\frac{v+x+z}{2}$, and $\frac{v+x+y+z}{2}$. None of the lattices obtained in this way are obviously isometric. However, the symmetries with respect to the vectors $\pm(v \pm x)$ will be isometries of each of these lattices respectively. Thus, $\mathbf{C}_2 \subset R(L)^*$ for any lattice L with $R(L) = 2\mathbf{A}_1$. Note also that $\pm 1_K \in O(L)$.

Now, if $O(K) = \{\pm 1_K\}$, then $R(L)^* = \mathbf{C}_2$ and $O(L) = O(C_2) \times \{\pm 1_K\} = \langle -1_L, W(R_L^*)\rangle$ as desired. Suppose that $O(K) \neq \{\pm 1_K\}$. Then, $dK^{1/2} = p$, $K^{1/2}$ is primal and does not represent 1. So, $O(K^{1/2})$ is generated by symmetries with respect to the vectors of length 2 in $K^{1/2}$ by [15, Cor. 4.5]. Thus, by scaling, $O(K)$ is generated by symmetries with respect to vectors of length 4 in K.

Using Gauss' theory of binary quadratic forms and considering the localizations of K at different primes, we obtain that there is only one ambiguous class of K, namely, the class represented by $\begin{pmatrix} 4 & 2 \\ 2 & p+1 \end{pmatrix}$. So, K has only two vectors of length 4.

Let $\{y', z'\} \subset K$ such that $K \cong \mathrm{Mat}(y', z') = \begin{pmatrix} 4 & 2 \\ 2 & p+1 \end{pmatrix}$. Then, there are three lattices containing M which are obtained by adjoining $\frac{v+x+y'}{2}$, $\frac{v+x+z'}{2}$, or $\frac{v+x+y'+z'}{2}$ to M. Let $L' = M + \mathbb{Z}[\frac{v+x+y'}{2}]$. Then, $Q(\frac{v+x+y'}{2}) = 2$ and L' will have $\mathbf{A}_3$ as its root system, a case we have already considered.

Let $L_0 = M + \mathbb{Z}[\frac{v+x+z'}{2}]$ and $L_1 = M + \mathbb{Z}[\frac{v+x+y'+z'}{2}]$. Then, $\tau_{y'}(L_0) = L_1$ and no vector of length 4 in K is in $R(L_0)^*$ or $R(L_1)^*$. Note that $\pm 1_K \in O(L_i)$ for $i = 0$ and 1.

Since $\langle -1_{L_i}, W(R_{L_i}^*)\rangle$ has index 2 in $O(R_{L_i}^*) \times O(K)$ and $\tau_{y'}$ is not in $O(L_i)$, the chain $\langle -1_{L_i}, W(R_{L_i})\rangle < O(L_i) < O(R_{L_i}^*) \times O(K)$ implies $O(L_i) = \langle -1_{L_i}, W(R_{L_i}^*)\rangle$ and $R(L_1)^* = R(L_2)^* = \mathbf{C}_2$.

- Suppose that $R(L) = \mathbf{A}_1$. The sublattice $R_L \perp K$ has index 2 in L. Let v be the vector generating R_L and $\{x, y, z\} \subset K$ so that $\mathrm{Mat}(x, y, z) \equiv < -2, -2, 2p >$ mod 64. Then, to obtain a lattice in $\mathcal{G}$ containing $R_L \perp K$ we can adjoin

$\frac{v+x}{2}$, $\frac{v+y}{2}$, or $\frac{v+z}{2}$. So, L is one of $(R_L \perp K) + \mathbb{Z}[\frac{v+x}{2}]$, $(R_L \perp K) + \mathbb{Z}[\frac{v+y}{2}]$ or $(R_L \perp K) + \mathbb{Z}[\frac{v+z}{2}]$. Note that $\pm 1_K$ is an isometry of each of these three lattices, and observe that $\langle -1_L, W(R_L^*)\rangle < O(L) < O(R_L) \times O(K)$. Now, if $O(K) = \{\pm 1_K\}$, then $O(L) = O(R_L) \times \{\pm 1_K\} = \langle -1_L, W(R_L^*)\rangle$ and $R(L)^* = R(L) = \mathbf{A}_1$.

Suppose $O(K) \neq \{\pm 1_K\}$. Then, $dK^{1/2} = p$, so $K^{1/2}$ is primal not representing 1. By [15, Cor. 4.5], $O(K^{1/2})$ is generated by symmetries with respect to the vectors of length 2 in $K^{1/2}$. Thus, by scaling, $O(K)$ is generated by symmetries with respect to vectors of length 4 in K, and K represents 4 when $O(K) \neq \{\pm 1_K\}$. Note that any vector of length 4 in K must be primitive in K.

Let e be a primitive vector of length 4 in K and $\{f, g\} \subset K$ such that $\mathrm{Mat}(e, f, g) \equiv \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix} \perp < 6p > \bmod 64$. There are three lattices in $\mathcal{G}$ containing $R_L \perp K$, and they are $L_0 = (R_L \perp K) + \mathbb{Z}[\frac{v+e+g}{2}]$, $L_1 = (R_L \perp K) + \mathbb{Z}[\frac{v+f+g}{2}]$, and $L_2 = (R_L \perp K) + \mathbb{Z}[\frac{v+e+f+g}{2}]$. The lattice L is one of these three lattices.

By Minkowski reduction, if K has another primitive vector of length 4 linearly independent of e, then K represents $\begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}$. In this case, we can take f to be one of the primitive vectors of length 4 linearly independent of e. Then, $\tau_e \in O(L_0)$, $\tau_f(L_0) = L_2$, and $\tau_{e-f}(L_0) = L_1$, so $R(L_0)^* = \mathbf{A}_1 \perp \mathbf{A}_1^2$. Similarly, $\tau_f \in O(L_1)$ and $\tau_e(L_1) = L_2$, while $\tau_{e-f} \in O(L_2)$. Thus, $R(L_1)^* = R(L_2)^* = \mathbf{A}_1 \perp \mathbf{A}_1^2$.

Now for each i, there exists some symmetry in $O(K)$ that does not extend to an isometry of L_i. The chain $\langle -1_{L_i}, W(R_{L_i}^*)\rangle < O(L_i) < O(R_{L_i}) \times O(K)$ implies that $O(L_i) = \langle -1_{L_i}, W(R_{L_i}^*)\rangle$ since $\langle -1_{L_i}, W(R_{L_i}^*)\rangle$ has index 2 in $O(R_{L_i}) \times O(K)$.

Suppose now that $\mu_2(K) > 6$. Then, by the same construction as above, τ_e is in $O(L_0)$ and $\tau_e(L_1) = L_2$. Thus, $R(L_0)^* = \mathbf{A}_1 \perp \mathbf{A}_1^2$ and $R(L_1)^* =$

$R(L_2)^* = \mathbf{A}_1$. Therefore, $\langle -1_{L_0}, W(R^*_{L_0})\rangle = O(R_{L_0}) \times O(K)$, which implies $O(L_0) = \langle -1_L, W(R^*_{L_0})\rangle$.

For $i = 1$ or 2, since the symmetry with respect to e in $O(K)$ does not extend to an isometry of L_i, the chain $\langle -1_{L_i}, W(R^*_{L_i})\rangle < O(L_i) < O(R_{L_i}) \times O(K)$ implies $O(L_i) = \langle -1_{L_i}, W(R^*_{L_i})\rangle$ since $\langle -1_{L_i}, W(R^*_{L_i})\rangle$ has index 2 in $O(R_{L_i}) \times O(K)$ for $i = 1$ and 2.

Now, suppose $\mu_2(K) = 6$. By Minkowski reduction, K must represent either $\begin{pmatrix} 4 & 2 \\ 2 & 6 \end{pmatrix}$ or $\begin{pmatrix} 4 & 0 \\ 0 & 6 \end{pmatrix}$. Suppose first that $K \cong \begin{pmatrix} 4 & 2 \\ 2 & 6 \end{pmatrix}$. Let $\{r, s, t\} \subset K$ such that $\mathrm{Mat}(r, s, t) \equiv \begin{pmatrix} 4 & 2 \\ 2 & 6 \end{pmatrix} \perp < 10p >$ mod 64 where $\mathrm{Mat}(r, s) = \begin{pmatrix} 4 & 2 \\ 2 & 6 \end{pmatrix}$. Now, the three lattices in $\mathcal{G}$ containing $R_L \perp K$ are $L_0 = (R_L \perp K) + \mathbb{Z}[\frac{v+s}{2}]$, $L_1 = (R_L \perp K) + \mathbb{Z}[\frac{v+t}{2}]$, and $L_2 = (R_L \perp K) + \mathbb{Z}[\frac{v+r+s}{2}]$. Note that $Q(\frac{v+s}{2}) = 2$ and $\{v, \frac{v+s}{2}\}$ generates a lattice isometric to A_2 in L_0. Further, $\tau_r(L_0) = L_2$. Thus, $R(L_0) = R(L_1) = \mathbf{A}_2$ and hence L must be L_1. Then, τ_r is an isometry of L, so $R(L)^* = \mathbf{A}_1 \perp \mathbf{A}_1^2$. Since $\pm 1_K \in O(L)$, we have $O(L) = O(R_L) \times O(K) = \langle -1_L, W(R^*_L)\rangle$.

Maintaining our assumptions that $\mu_1(K) = 4$ and $\mu_2(K) = 6$, if K does not contain the binary sublattice $\begin{pmatrix} 4 & 2 \\ 2 & 6 \end{pmatrix}$, then

$$K \cong \begin{pmatrix} 4 & 0 & 2 \\ 0 & 6 & 2 \\ 2 & 2 & \frac{p+5}{3} \end{pmatrix}.$$

By considering the localizations at 2 and 3, we see that $p \equiv -1$ mod 8 and $p \equiv 1$ mod 3.

Let $\{\alpha, \beta, \gamma\}$ be a basis of K which yields the above Gram matrix. Then, the three lattices in $\mathcal{G}$ containing $R_L \perp K$ are $L_0 = (R_L \perp K) + \mathbb{Z}[\frac{v+\beta}{2}]$, $L_1 =$

$(R_L \perp K)+\mathbb{Z}[\frac{v+\beta+\gamma}{2}]$, and $L_2 = (R_L \perp K)+\mathbb{Z}[\frac{v+\alpha+\beta+\gamma}{2}]$. Note that $Q(\frac{v+\beta}{2}) = 2$, so $R(L_0) \neq \mathbf{A}_1$. Thus, L cannot be L_0.

Finally, since $\tau_\alpha(L_1) = L_2$, α is not in $R(L_i)^*$ and $R(L_i) = R(L_i)^* = \mathbf{A}_1$ for $i = 1$ and 2. Further, the symmetry with respect to α does not extend to an isometry of L_i for $i = 1$ or 2. The chain $\langle -1_{L_i}, W(R^*_{L_i})\rangle < O(L_i) < O(R_{L_i}) \times O(K)$ implies $O(L_i) = \langle -1_{L_i}, W(R^*_{L_i})\rangle$ since $\langle -1_{L_i}, W(R^*_{L_i})\rangle$ has index 2 in $O(R_{L_i}) \times O(K)$ for $i = 1$ and 2.

□

Corollary 2. *There is only one class in $\mathcal{G}$ with scaled root system $\boldsymbol{C}_3 \perp \boldsymbol{A}_1^{2p}$.*

Proof. Let L be a lattice in $\mathcal{G}$ such that $R(L)^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$. Let $\{v, x, y\} \subset R^*_L$ such that $\mathrm{Mat}(v, x, y) \equiv \mathbb{A} \perp < 12 >$ mod 64. Then, L is either $R^*_L + \mathbb{Z}[\frac{y+z}{2}]$ or $R^*_L + \mathbb{Z}[\frac{y-z}{2}]$. However, these lattices are in fact the same. Thus, there is one class of lattices in $\mathcal{G}$ with scaled root system $\mathbf{C}_3 \perp \mathbf{A}_1^{2p}$. □

Using Proposition 2, we determine $|O(L)|$ corresponding to the scaled root system of a lattice L in $\mathcal{G}$:

$R(L)^*$	$\mathbf{A}_1^2$	$\mathbf{A}_1$	$\mathbf{A}_2$	$\mathbf{A}_2 \perp \mathbf{A}_1^2$	$\mathbf{C}_2$	$\mathbf{C}_3 \perp \mathbf{A}_1^{2p}$	$\mathbf{A}_1 \perp \mathbf{A}_1^2$
$\lvert O(L)\rvert$	4	4	12	24	16	96	8

We close this section with lemmas regarding the scaled root systems of the lattices in $\mathcal{G}$ which will be relevant in the proof of our main result.

Lemma 8. *There is only one class in $\mathcal{G}$ with scaled root system $\boldsymbol{A}_2 \perp \boldsymbol{A}_1^2$.*

Proof. Let L be a lattice in $\mathcal{G}$ such that $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1^2$ and let K denote the orthogonal complement of R^*_L in L. Note that $p \equiv 1$ mod 3 and $p \equiv -1$ mod 8 by the proof of the case $R(L) = \mathbf{A}_2$ in Proposition 2. Then, since

$12 \cdot dK = 4p[L : R_L^* \perp K]^2$ and $dK|(12 \cdot 4p)$, dK is one of $3p, 12p$, or $48p$. Note that $dK \neq 3p$ since K is an even rank 1 lattice.

By Lemma 5 and the fact that the orthogonal complement of a root in A_2 is a vector of length 6, $< 6, 4 > \perp K_2$ is represented by $< -2, -2, 2p >$. Since $< 6 >$ splits $< -2, -2, 2p >$, $< 6 > \perp N \cong < -2, -2, 2p >$ where N is a binary even lattice with $dN = 12p$. Then, K_2 is the orthogonal complement of $< 4 >$ in N, so $dK = 12p$.

Now, if $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1^2$, then L contains the full sublattice $M = R_L^* \perp \mathbb{Z}[z]$ where z is a vector of length $12p$ and $[L : M] = 6$. Let $\{v, x, y\}$ be a basis for R_L^* such that $\mathrm{Mat}(x, y, z) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp < 4 >$. Then, by considering the localizations at 2 and 3, L is equal to one of $M + \mathbb{Z}[\frac{y+z}{2}, \frac{v-2x+z}{3}]$ or $M + \mathbb{Z}[\frac{y+z}{2}, \frac{v-2x-z}{3}]$. However, these two lattices are isometric via τ_z. Thus, there is only one class in $\mathcal{G}$ with scaled root system $\mathbf{A}_2 \perp \mathbf{A}_1^2$. □

Lemma 9. *Let L be a lattice in $\mathcal{G}$ such that $R(L)^* = \boldsymbol{A}_1 \perp \boldsymbol{A}_1^2$ and let K be the orthogonal complement of R_L^* in L. Then, $dK = 8p$, $K_2 \cong < 12, 6p >$ and $K_p \cong < 2\delta, \delta p >$. Further, L is obtained by adjoining two vectors of conductor* 2 *to $R_L^* \perp K$.*

Proof. Since $8 \cdot dK = 4p[L : R_L^* \perp K]^2$ and $dK|8 \cdot dL$, dK equals one of $2p, 8p$, or $32p$. Note that $dK \neq 2p$ because K is binary and even. By Lemma 5, K_2 is the orthogonal complement of A_1^2 in $< -2, -2, 2p >$. Then, because $(\frac{dK}{4})|(2 \cdot p)$, $dK = 8p$.

Now, $K_2 \cong < 2\epsilon, 4\epsilon p >$ or $< 4\epsilon, 2\epsilon p >$ for some $\epsilon \in \{1, 3, 5, -1\}$. If $K_2 \cong < 2\epsilon, 4\epsilon p >$, then $\epsilon = 3$ or 5 when $p \equiv -1 \bmod 8$ and $\epsilon = 1$ or -1 when $p \equiv 3 \bmod 8$ so that $S_2(\mathbb{Q}_2 L_2) = S_2(\mathbb{Q}_2 R_L^* \perp \mathbb{Q}_2 K_2)$. Similarly, if $K_2 \cong < 4\epsilon, 2\epsilon p >$, then$\epsilon = 3$ or 5 when $p \equiv -1$ or $3 \bmod 8$. However, for each possible p, the lattices obtained by specifying different ϵ are isometric. Thus, we may take $\epsilon = 3$ and $K_2 \cong < 12, 6p >$. Since R_L^* is unimodular at p, $(R_L^*)_p \perp K_p \cong L_p \cong < 1, 1, \delta, \delta p >$. So, $K_p \cong < 2\delta, \delta p >$.

Consider the tower of lattices

$$\begin{array}{c} L \\ \Big| \\ R_L \perp R_L^{\perp} \\ \Big| \\ R_L^* \perp K \end{array}$$

where $R_L^{\perp}$ is the orthogonal complement of R_L in L. Let $\{v, x\} \subset L$ such that $\mathbb{Z}[v, x] = R_L^*$ and $\mathrm{Mat}(v, x) = < 2, 4 >$. Let $\{y, z\} \subset K$ such that $\mathrm{Mat}(y, z) \equiv < 12, 6p >$ mod 64. Then, $R_L^* \perp K$ has index 2 in $R_L \perp R_L^{\perp}$ and $R_L \perp R_L^{\perp} = (R_L^* \perp K) + \mathbb{Z}[\frac{x+y}{2}]$. Let $y' = \frac{x+y}{2}$. Then, $\mathrm{Mat}(v, x, y') \equiv < 2 > \perp \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}$ mod 64. Let z be a vector in $R_L \perp R_L^{\perp}$ such that $\mathrm{Mat}(v, x, y', z) \equiv < 2 > \perp \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix} \perp < 6p >$ mod 64. Now, $R_L \perp R_L^{\perp}$ has index 2 in L, and so L is one of

$$(R_L \perp R_L^{\perp}) + \mathbb{Z}\left[\frac{v + x + z}{2}\right], \ (R_L \perp R_L^{\perp}) + \mathbb{Z}\left[\frac{v + y' + z}{2}\right],$$

$$\text{or } \ (R_L \perp R_L^{\perp}) + \mathbb{Z}\left[\frac{v + x + y' + z}{2}\right].$$

However, from the proof of the case $R(L) = \mathbf{A}_1$ in Proposition 2, $L = (R_L \perp R_L^{\perp}) + \mathbb{Z}[\frac{v+x+z}{2}]$ since $R(L)^* = \mathbf{A}_1 \perp \mathbf{A}_1^2$. Further, $L = (R_L^* \perp K) + \mathbb{Z}[y', \frac{v+x+z}{2}]$. Thus, a lattice L in $\mathcal{G}'$ containing $R_L^* \perp K$ in this way is obtained by adjoining two vectors of conductor 2.

By the proof of the case $R(L) = \mathbf{A}_1$ in Proposition 2, there is only one class of lattices in $\mathcal{G}$ containing $R_L \perp K$ when K has two linearly independent primitive vectors of length 4. In this case, L is isometric to $(R_L^* \perp K)+\mathbb{Z}[y', \frac{v+x+z}{2}]$, which is obtained by adjoining two vectors of conductor 2 to $R_L^* \perp K$.

The remaining situation where $R(L)^* = \mathbf{A}_1 \perp \mathbf{A}_1^2$ occurs is when $R_L^\perp$ represents $\begin{pmatrix} 4 & 2 \\ 2 & 6 \end{pmatrix}$. Let $\{e, f\} \subset K$ such that $\mathrm{Mat}(e, f) \equiv < 20, 10p >$ mod 64. Then, $R_L^* \perp K$ has index 2 in $R_L \perp R_L^\perp$, and $R_L \perp R_L^\perp = (R_L^* \perp K) + \mathbb{Z}[\frac{x+e}{2}]$. Let $e' = \frac{x+e}{2}$. Then, let $f \in R_L^*$ such that $\mathrm{Mat}(v, x, e', f) \equiv < 2 > \perp \begin{pmatrix} 4 & 2 \\ 2 & 6 \end{pmatrix} \perp < 10p >$ mod 64. Now, $R_L \perp R_L^\perp$ has index 2 in L, and $L = (R_L \perp K) + \mathbb{Z}[\frac{v+f}{2}]$ by the proof of the case $R(L) = \mathbf{A}_1$ in Proposition 2 since $R(L)^* = \mathbf{A}_1 \perp \mathbf{A}_1^2$. Thus, $L = (R_L^* \perp K) + \mathbb{Z}[e', \frac{v+f}{2}]$, which is obtained by adjoining two vectors of conductor 2.

$\square$

3.3 Linear Independence of Degree Two Theta Series

Let $\mathscr{L}$ be a complete set of class representatives in $\mathcal{G}$ with nontrivial orthogonal groups and associate to each $L \in \mathscr{L}$ its degree 2 theta series, denoted θ_L. By Proposition 2, the scaled root system of an $L \in \mathscr{L}$ is one of the following: $\mathbf{A}_1^2$, $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_2 \perp \mathbf{A}_1^2$, $\mathbf{C}_2$, $\mathbf{C}_3 \perp \mathbf{A}_1^{2p}$, or $\mathbf{A}_1 \perp \mathbf{A}_1^2$. Further, $O(L) = \langle -1_L, W(R_L^*)\rangle$. In this section, we prove that the θ_L are linearly independent over $\mathbb{Z}$.

Our strategy is as follows. Suppose that there is a linear relation $\sum_{L \in \mathscr{L}} c_L \theta_L = 0$ such that the greatest common divisor of the c_L is 1. For a fixed L, we will construct a binary sublattice J, and for every $L' \in \mathscr{L}$, let $a_{JL'}$ denote the number of distinct isometric embeddings of J into L'. Then, for each L, we have the equality $\sum_{L' \in \mathscr{L}} c_{L'} a_{JL'} = 0$. Using these equations, we will show that $c_L \equiv 0 \mod 2$ for all $L \in \mathscr{L}$, contradicting our assumption that the gcd of the $c_{L'}$ is 1.

Lemma 10. *Let L be a lattice, and let J be a binary lattice. Fix $e \in R(L)^*$ and let S be a set of isometric embeddings $\phi : J \to L$ such that for all $\phi \in S$, $\phi(J)$ is not orthogonal to $\mathbb{Z}[e]$. If $\langle -1_L, \tau_e \rangle$ acts on S then, $|S|$ is divisible by 4.*

Proof. For any $\phi \in S$, since $\phi(J)$ is not orthogonal to $\mathbb{Z}[e]$, τ_e is not in the stabilizer of ϕ. Since the fixed space of $-\tau_e$ has dimension 1, $-\tau_e$ cannot stabilize ϕ. Thus, the stabilizer of ϕ is $\{1_L\}$ and hence $|\mathrm{orb}(\phi)| = 4$. Since this holds for all $\phi \in S$, we have $|S| \equiv 0 \mod 4$. □

Now we present the proof of our main result.

Theorem 1. *The degree 2 theta series of the classes in $\mathcal{G}$ with nontrivial orthogonal groups are linearly independent over $\mathbb{Z}$.*

Proof. We proceed with cases corresponding to the possible scaled root systems of a lattice $L \in \mathscr{L}$. In all cases, K is the orthogonal complement of R_L^* in L.

• Fix $L \in \mathscr{L}$ such that $R(L)^* = \mathbf{A}_1^2$ and let v be a vector of length 4 in $R(L)^*$. From the proof of Proposition 1, we have that $dK = 4p$ and hence $[L : R_L^* \perp K] = 2$. Further, by local considerations at 2 and p, we have $K_p \cong < 1, \delta, \delta p >$ and

$$K_2 \cong \begin{cases} \mathbb{H} \perp < -4p > & p \equiv 3 \bmod 8, \\ \mathbb{A} \perp < 12p > & p \equiv -1 \bmod 8. \end{cases}$$

By [13, Lemma 1.6], K contains a sublattice J such that $J_2 \cong \mathbb{P}$ where $\mathbb{P}$ denotes the even unimodular component of K_2, $J_p \cong < 1, \delta >$, and $dJ = q$ for some large prime q. Note also that $q \equiv -1 \bmod 8$ when $p \equiv 3 \bmod 8$, and $q \equiv 3 \bmod 8$ when $p \equiv -1 \bmod 8$.

Let N be the orthogonal complement of $R_L^* \perp J$ in L. Then, N is a rank 1 lattice generated by a vector z of length $4pq$. Let $M = R_L^* \perp J \perp N$, which has index $2q$ in L. Since J_2 splits L_2, we have $L_2 = M_2 + \mathbb{Z}_2[\frac{v+z}{2}] = M_2 + \mathbb{Z}_2[\frac{v-z}{2}]$. The map τ_z stabilizes L_2. Over $\mathbb{Z}_q$, $J_q \cong < \alpha, \alpha q >$ in a basis $\{e, f\}$ with $\alpha \in \mathbb{Z}_q^\times$. Then, L_q is equal to either $M_q + \mathbb{Z}_q[\frac{f+az}{q}]$ or $M_q + \mathbb{Z}_q[\frac{f-az}{q}]$ with $a \in \mathbb{Z}_q$ such that $\frac{1}{q}(Q(f) + a^2 Q(z)) \equiv 0 \bmod q$. These two lattices are isometric via τ_z. Thus, there are exactly two lattices in $\mathcal{G}$ which contain M, namely, $M + \mathbb{Z}[\frac{v+z}{2}, \frac{f'+az}{q}]$ and $M + \mathbb{Z}[\frac{v-z}{2}, \frac{f'+az}{q}]$, where $f' \in J$ locally approximates f, and they are isometric via τ_z. Thus, there is only one class of lattices in $\mathcal{G}$ containing M.

Suppose $\phi : J \to L$ is an isometric embedding such that $\phi(J)$ is orthogonal to $\mathbb{Z}[v]$. Then, there exists some $\sigma \in O(\mathbb{Q}L)$ such that $\sigma|_J = \phi$. Further, $\sigma^{-1}(L)$ contains $M = R_L^* \perp J \perp N$. Thus, $\sigma^{-1}(L) = L$ or $\sigma^{-1}(L) = \tau_z(L)$. Since $\sigma|_J = \phi$ and $(\sigma \circ \tau_z)|_J = \phi$, ϕ is in the orbit of the inclusion map $\iota : J \hookrightarrow L$ under the action of $O(L) = \langle -1_L, \tau_v \rangle$. Thus, this orbit has 2 embeddings; namely, ι and $-\iota$. By Lemma 10, the number of embeddings $\phi : J \to L$ with $\phi(J)$ not orthogonal to $\mathbb{Z}[v]$ is equivalent to $0 \mod 4$. Therefore, $a_{JL} \equiv 2 \mod 4$.

Now, suppose that $\phi : J \to L'$ is an isometric embedding of J into L' where $L \neq L'$ and $\min(L') = 2$. Let e be a vector of length 2 in L' and suppose that $\phi(J)$ is orthogonal to $\mathbb{Z}[e]$ in L'. Locally at 2, $L_2' \cong L_2 \cong \mathbb{H} \perp < -2, 2p > \cong \mathbb{A} \perp < -2, -6p >$. Since J_2 is even unimodular, it must split L_2' and hence 2 is represented by $< -2, 2p >$ or $< -2, -6p >$. However, this is impossible for either $p \equiv -1$ or $3 \bmod 8$. Thus, $\phi(J)$ is not orthogonal to any vector of length 2 in L'. Since ϕ is an arbitrary embedding of J into L' and $\phi(J)$ is not orthogonal to $\mathbb{Z}[e]$ for any minimal vector $e \in L'$, we can apply Lemma 10 to conclude that $a_{JL'} \equiv 0 \bmod 4$ for all $L' \neq L$.

Next, suppose that $\phi : J \to L'$ is an isometric embedding of J into L' where

$L \neq L'$ and $\min(L') = 4$. Let f be a vector of length 4 in $R(L')^*$ and suppose that $\phi(J)$ is orthogonal to $\mathbb{Z}[f]$ in L'. Then, ϕ can be extended to an embedding ϕ' of $\mathbb{Z}[v] \perp J$ into L' where $\phi'(v) = f$ and $\phi'|_J = \phi$. Then, by considering discriminants, the orthogonal complement of $\phi'(\mathbb{Z}[v] \perp J)$ in L' is isometric to N. Thus, ϕ' can be extended to an isometry Φ of the space $\mathbb{Q}L$ and $\Phi^{-1}(L')$ is a lattice in $\mathcal{G}$ which contains M. Since we have shown that there is only one class in $\mathcal{G}$ containing M, it must be that $L = L'$. Thus, when $L \neq L'$ and $\min(L') = 4$, $\phi(J)$ is not orthogonal to $\mathbb{Z}[f]$ in L', and by Lemma 10, $a_{JL'} \equiv 0 \bmod 4$ in this case.

Consider $\displaystyle\sum_{L' \in \mathscr{L}} c_{L'} a_{JL'} \equiv 0 \mod 4$. From above, we have that $a_{JL'} \equiv 0 \bmod 4$ when $L \neq L'$. Thus, $c_L a_{JL} \equiv 0 \mod 4$. But, $a_{JL} \equiv 2 \mod 4$; so, $c_L \equiv 0 \bmod 2$.

• Fix $L \in \mathscr{L}$ such that $R(L)^* = R(L) = \mathbf{A}_1$. Let v be a vector in $R(L)$ and let $\{x, y, z\} \subset K$ such that $\mathrm{Mat}(x, y, z) \equiv < -2, -2, 2p > \bmod 64$. A lattice in $\mathcal{G}$ containing $R_L \perp K$ will be obtained by adjoining one of $\frac{v+x}{2}$, $\frac{v+y}{2}$, or $\frac{v+z}{2}$ to $R_L \perp K$. One of these lattices is L. However, it is not clear if any two of these lattices are isometric. For this reason, we will make use of the transformation formula $(\star)$ in Section 2.2 relating θ_L and $\theta_L^{\#}$, the degree 2 theta series of $L^{\#}$, and proceed by using the dual of L in this case. Let $\mathcal{G}^{\#}$ and $\mathscr{L}^{\#}$ be the sets $\{L^{\#} : L \in \mathcal{G}\}$ and $\{L^{\#} : L \in \mathscr{L}\}$, respectively.

Note that $L_2^{\#} \cong \mathbb{H} \perp < \frac{-1}{2}, \frac{p}{2} > \cong \mathbb{A} \perp < \frac{-1}{2}, \frac{-3p}{2} >$. Let $\bar{L} = (R_L \perp K) + \mathbb{Z}[\frac{v+x}{2}]$. Then, the set $\{v, \frac{v+x}{2}, y, z\}$ is a basis for $\bar{L}_2$. Over $\mathbb{Z}_2$, $\mathrm{Mat}(v, \frac{v+x}{2}) \cong \mathbb{H}$ and $\mathrm{Mat}(y, z) \cong < -2, 2p >$. Therefore, $\{v, \frac{v+x}{2}, \frac{y}{2}, \frac{z}{2}\}$ is a basis for $\bar{L}_2^{\#}$ and $\mathrm{Mat}(\frac{y}{2}, \frac{z}{2}) \cong < \frac{-1}{2}, \frac{p}{2} >$.

Let $\hat{L} = (R_L \perp K) + \mathbb{Z}[\frac{v+y}{2}]$. Then, the set $\{v, \frac{v+y}{2}, x, z\}$ is a basis for $\hat{L}_2$.

Over $\mathbb{Z}_2$, $\mathrm{Mat}(v, \frac{v+y}{2}) \cong \mathbb{H}$ and $\mathrm{Mat}(x, z) \cong < -2, 2p >$. Therefore, $\{v, \frac{v+y}{2}, \frac{x}{2}, \frac{z}{2}\}$ is a basis for $\hat{L}_2^{\#}$ and $\mathrm{Mat}(\frac{x}{2}, \frac{z}{2}) \cong < \frac{-1}{2}, \frac{p}{2} >$.

Finally, let $\tilde{L} = (R_L \perp K) + \mathbb{Z}[\frac{v+z}{2}]$. Then, the set $\{v, \frac{v+z}{2}, x, y\}$ is a basis for $\tilde{L}_2$. Over $\mathbb{Z}_2$, $\mathrm{Mat}(v, \frac{v+z}{2}) \cong \mathbb{P}$ where $\mathbb{P} \cong \mathbb{H}$ if $p \equiv -1 \bmod 8$ and $\mathbb{P} \cong \mathbb{A}$ if $p \equiv 3 \bmod 8$, and $\mathrm{Mat}(x, y) \cong < -2, -2 >$. Therefore, $\{v, \frac{v+z}{2}, \frac{x}{2}, \frac{y}{2}\}$ is basis for $\tilde{L}_2^{\#}$ and $\mathrm{Mat}(\frac{x}{2}, \frac{y}{2}) \cong < \frac{-1}{2}, \frac{-1}{2} >$. Note that when $p \equiv -1 \bmod 8$, $\tilde{L}_2^{\#}$ has a component isometric to $< \frac{-1}{2}, \frac{p}{2} >$. Further, when $p \equiv 3 \bmod 8$, $\tilde{L}_2^{\#} \cong \mathbb{A} \perp < \frac{-1}{2}, \frac{-1}{2} >$, which is isometric to $\mathbb{H} \perp < \frac{-1}{2}, \frac{3}{2} >$. Thus, whether $p \equiv -1$ or $3 \bmod 8$, $\tilde{L}_2^{\#}$ contains a component isometric to $< \frac{-1}{2}, \frac{p}{2} >$.

Therefore, even though L could be equal to $\bar{L}, \hat{L}$, or $\tilde{L}$, $L_2^{\#}$ always contains a component isometric to $< \frac{-1}{2}, \frac{p}{2} >$.

Let K be the orthogonal complement of R_L in $L^{\#}$ and J a binary sublattice of K such that $J_2 \cong < \frac{-1}{2}, \frac{p}{2} >$, $J_p \cong < 2, \delta >$, and $dJ = \frac{q}{4}$ for some large prime q. Let $\{x, y\} \subset J$ such that

$$\mathrm{Mat}(x, y) \equiv \begin{cases} < \frac{-1}{2}, \frac{p}{2} > & \bmod 64, \\ < 2, \delta > & \bmod p^3. \end{cases}$$

Let N be the orthogonal complement of $R_L \perp J$ in $L^{\#}$. Then N is a rank 1 lattice generated by a vector z of length $\frac{2q}{p}$ and $M = R_L \perp J \perp N$ has index $2q$ in $L^{\#}$. Note that a lattice in $\mathcal{G}^{\#}$ containing $A_1 \perp J$ must also contain M.

Consider the localization at 2. Note that $q \equiv -p \bmod 8$ by the construction of J. Then, since J_2 splits $L_2^{\#}$, we have that $L_2^{\#} = M_2 + \mathbb{Z}_2[\frac{v+z}{2}] = M_2 + \mathbb{Z}_2[\frac{v-z}{2}]$, and τ_z is an isometry of $L_2^{\#}$. Since L_q is unimodular, $L_q^{\#} = L_q$. Suppose $J_q \cong < \alpha, \alpha q >$ in a basis $\{e, f\}$ with $\alpha \in \mathbb{Z}_q^{\times}$. Then, $L_q = M_q + \mathbb{Z}_q[\frac{f+az}{q}]$ or $M_q + \mathbb{Z}_q[\frac{f-az}{q}]$ where $a \in \mathbb{Z}_q$ and $\frac{1}{q}(Q(f) + a^2 Q(z)) \equiv 0 \bmod q$. These lattices are isometric to each other via τ_z. So, there are two lattices in $\mathcal{G}^{\#}$ containing M, and they are isometric via τ_z.

Suppose $\phi : J \to L^{\#}$ is an isometric embedding such that $\phi(J)$ is orthogonal to v in $L^{\#}$. Then, there exists some $\sigma \in O(\mathbb{Q}L^{\#}) = O(\mathbb{Q}L)$ such that $\sigma|_J = \phi$ and the orthogonal complement of $\mathbb{Z}[v] \perp \phi(J)$ in $L^{\#}$ is isometric to $< \frac{2q}{p} >$. Thus, $\sigma^{-1}(L^{\#})$ contains M. However, we have shown that $L^{\#}$ and $\tau_z(L^{\#})$ are the only lattices in $\mathcal{G}^{\#}$ containing M. Thus, $\sigma^{-1}(L^{\#}) = L^{\#}$ or $\sigma^{-1}(L^{\#}) = \tau_z(L^{\#})$. Since $\sigma|_J = \phi$ and $(\sigma \circ \tau_z)|_J = \phi$, ϕ is in the orbit of the inclusion map under the action of $O(L)$ and this orbit has only two elements. By Lemma 10, the other orbits of embeddings of J into $L^{\#}$ have size divisible by 4. Therefore, $a_{JL^{\#}} \equiv 2 \mod 4$.

Now, let $\phi : J \to L'^{\#}$ be an isometric embedding such that $L' \neq L$ and $\min(L') = 2$. Suppose that $\phi(J)$ is orthogonal to a vector e of length 2 in L'. Then, ϕ can be extended to an isometry ϕ' of $\mathbb{Q}L = \mathbb{Q}L^{\#}$ such that $\phi'(v) = e$ and $\phi'|_J = \phi$. Further, the orthogonal complement of $\mathbb{Z}[e] \perp \phi(J)$ in $L'^{\#}$ will be isometric to $< \frac{2q}{p} >$. Thus, $\phi'^{-1}(L'^{\#})$ contains M. However, since there is only one class of lattices in $\mathcal{G}^{\#}$ containing M, it must be that $L'^{\#} = L^{\#}$, which is impossible. Thus, $\phi(J)$ is not orthogonal to any vector of length 2 in L', and by Lemma 10, $a_{JL'^{\#}} \equiv 0 \mod 4$ for all $L \neq L'$ with $\min(L') = 2$.

For L' with $\min(L') = 4$, the previous case showed that $c_{L'} \equiv 0 \mod 2$. Since for each embedding ϕ, its negative will also be an embedding, so $a_{JL'^{\#}} \equiv 0 \mod 2$. Thus, $c_{L'} a_{JL'^{\#}} \equiv 0 \mod 4$ in this case.

From the discussion, $a_{JL'^{\#}} \equiv 0 \mod 4$ when $L \neq L'$. Then, the summation implies $c_L a_{JL^{\#}} \equiv 0 \mod 4$. But, $a_{JL^{\#}} \equiv 2 \mod 4$. Therefore, $c_L \equiv 0 \mod 2$.

- Fix $L \in \mathscr{L}$ such that $R(L)^* = R(L) = \mathbf{A}_2$. Then, $R_L \perp K$ has index 3 in L. Let $\{v, x\}$ be a basis for R_L such that $R_L \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ in $\{v, x\}$, and $\{y, z\} \subset K$

such that $\mathrm{Mat}(y,z) \equiv < 3, p >$ mod 27 and $\mathrm{Mat}(y,z) \equiv < -2, -6p >$ mod 64. Let J be the orthogonal complement of R_L in $L^\#$. Then, $L_2 \cong \mathbb{A} \perp J_2^\#$ implies that $L_2^\# \cong \mathbb{A} \perp J_2$ where $J_2 \cong < \frac{-1}{2}, \frac{-3p}{2} >$ and $(R_L)_2 \cong \mathbb{A}$ splits $L_2^\#$. Moreover, since $L_p^\# \cong < 1, 1, \delta, \frac{\delta}{p} >$ and $(R_L)_p$ is unimodular at p with discriminant 3, we have $J_p \cong < 3\delta, \frac{\delta}{p} >$. Finally, because L_3 is unimodular, $L_3^\# = L_3 \cong < 1, 1, 1, p >$. Because $\mathbb{Q}_3 L \cong \mathbb{Q}_3 R_L \perp \mathbb{Q}_3 J$, $J_3 \cong < 3, p >$.

Let N denote the orthogonal complement of $\mathbb{Z}[v]$ in $L^\#$. Then, $N = \mathbb{Z}[v - 2x] \perp J$ with $Q(v - 2x) = 6$. Note that $[L^\# : \mathbb{Z}[v] \perp N] = 6$. Over $\mathbb{Z}_2$, since J_2 splits $L_2^\#$, $L_2^\# = (\mathbb{Z}_2[v] \perp N_2) + \mathbb{Z}_2[v - x]$ and $1_{R_L} \perp -1_J$ is an isometry of $L_2^\#$. Over $\mathbb{Z}_3$, $\mathbb{Z}_3[v] \perp N_3 \cong < 2, 6 > \perp < 3, p >$ and has index 3 in L_3. Then, $L_3 = (\mathbb{Z}_3[v] \perp N_3) + \mathbb{Z}_3[\frac{v-2x+y}{3}]$ or $(\mathbb{Z}_3[v] \perp N_3) + \mathbb{Z}_3[\frac{v-2x-y}{3}]$. However, these lattices are isometric via $1_{R_L} \perp -1_J$. Therefore, $L^\#$ must be equal to $(\mathbb{Z}[v] \perp N) + \mathbb{Z}[v - x, \frac{v-2x+y}{3}]$ or $(\mathbb{Z}[v] \perp N) + \mathbb{Z}[v - x, \frac{v-2x-y}{3}]$. These lattices are isometric via $1_{R_L} \perp -1_J$, and up to isometry, there is exactly one lattice in $\mathcal{G}^\#$ containing $\mathbb{Z}[v] \perp N$.

Consider an isometric embedding $\phi : J \to L^\#$. First, suppose that $\phi(J)$ is orthogonal to R_L in $L^\#$. Then, ϕ is in $O(J)$ and $\sigma := 1_{R_L} \perp \phi$ is an isometry of $R_L \perp J$. If $\sigma(L^\#) = L^\#$, then $1_{R_L} \perp \phi \in O(L)$. Otherwise, $\sigma(L^\#) = (1_{R_L} \perp -1_J)(L^\#)$ by the above argument and $(1_{R_L} \perp -1_J) \circ \sigma = (1_{R_L} \perp -\phi)$ is in $O(L)$. However, since $O(L) = \langle -1_L, W(R_L^*) \rangle$ and $\pm 1_L$ are the only elements of $O(L)$ that stabilize R_L, it must be that $\phi = \pm 1_J$. Thus, there are exactly two isometric embeddings of J into $L^\#$ such that $\phi(J)$ is orthogonal to R_L. Suppose that $\phi(J)$ is orthogonal to the vector v in L. Then, by the previous argument, $L^\#$ is equal to $(\mathbb{Z}[v] \perp N) + \mathbb{Z}[v - x, \frac{v-2x+y}{3}]$ or $(\mathbb{Z}[v] \perp N) + \mathbb{Z}[v - x, \frac{v-2x-y}{3}]$. However, $Q(v - x) = 2$ and $\{v, v - x\}$ generates R_L in $L^\#$. Thus, if $\phi(J)$ is orthogonal to v, then $\phi(J)$ must be orthogonal to R_L. Finally, suppose that

$\phi(J)$ is not orthogonal to any vector of length 2 in $L^{\#}$. Then, by Lemma 10, the number of these embeddings will be divisible by 4. Thus, we have $a_{JL'^{\#}} \equiv 2 \mod 4$.

Now, let $\phi : J \to L'^{\#}$ be an isometric embedding such that $L' \neq L$ with $\min(L') = 2$. Suppose that $\phi(J)$ is orthogonal to a vector e of length 2 in L'. Then, ϕ can be extended to an isometry ϕ' on $\mathbb{Q}L = \mathbb{Q}L^{\#}$ such that $\phi'(v) = e$ and $\phi'|_J = \phi$, and by considering discriminants, the orthogonal complement of $\mathbb{Z}[e] \perp \phi(J)$ in $L'^{\#}$ will be isometric to $< 6 >$. Thus, the lattice $\phi'^{-1}(L'^{\#})$ contains a sublattice isometric to $\mathbb{Z}[v] \perp N$. However, since we have shown that up to isometry there is only one lattice in $\mathcal{G}^{\#}$ containing $\mathbb{Z}[v] \perp N$, it must be that $L'^{\#} = L^{\#}$. Thus, we have a contradiction and hence $\phi(J)$ is not orthogonal to any minimal vector e in L'. By Lemma 10, $a_{JL'^{\#}} \equiv 0 \mod 4$ for all $L' \neq L$ in $\mathscr{L}$.

For L' with $\min(L') = 4$, previous discussion shows that $c_{L'} \equiv 0 \mod 2$. Further, $a_{JL'^{\#}} \equiv 0 \mod 2$ since for each embedding ϕ, its negative will be a different embedding. Thus, $c_{L'}a_{JL'^{\#}} \equiv 0 \mod 4$ in this case. Similarly, for L' with $\min(L') = 2$ and $R(L')^* = \mathbf{A}_1$, the previous case shows that $c_{L'} \equiv 0 \mod 2$, and $c_{L'}a_{JL'^{\#}} \equiv 0 \mod 4$.

From above, we have that $a_{JL'^{\#}} \equiv 0 \mod 4$ when $L' \neq L$. Thus, $c_L a_{JL^{\#}} \equiv 0 \mod 4$. But, $a_{JL^{\#}} \equiv 2 \mod 4$, and we have $c_L \equiv 0 \mod 2$ as desired.

- Fix $L \in \mathscr{L}$ such that $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1^2$. In this case, $p \equiv 1 \mod 3$ and $p \equiv -1 \mod 8$ by the case $R(L) = \mathbf{A}_2$ in Proposition 2. By Lemma 8, L represents the only class in $\mathcal{G}$ with this scaled root system. Let $J = R_L$, which is isometric to A_2. Then, an embedding of J into L' will only exist if $R(L')^* = \mathbf{A}_2, \mathbf{A}_2 \perp \mathbf{A}_1^2$, or $\mathbf{C}_3 \perp \mathbf{A}_1^{2p}$.

When $R(L')^* = \mathbf{A}_2$, there are precisely 12 ways to embed J into L' since L' contains one copy of A_2 and $|O(A_2)| = 12$. Similarly, the number of embeddings of J into L is 12. If $R(L')^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$, then we count the number of distinct embeddings of J into L' in the following way. Let $\{v, x\}$ be a basis of J such that $\mathrm{Mat}(v, x) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and $\{e, f, g\}$ be a basis of C_3 such that $\mathrm{Mat}(e, f, g) = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$. The vector v can be sent to any one of the 12 vectors of length 2 in C_3. Without loss of generality, let us suppose that v is sent to e. Then, x can be sent to any vector of the set $\{f, e-f, f-g, e-f+g\}$ so that the image of $\{v, x\}$ in C_3 is a copy of A_2. Thus, there are 48 ways to embed J into L'.

Since it has been shown that $c_{L'} \equiv 0 \bmod 2$ and $a_{JL'} = 12$ when $R(L')^* = \mathbf{A}_2$, in this case, $c_{L'} a_{JL'} \equiv 0 \bmod 8$. Further, when $R(L')^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$, $c_{L'} a_{JL'} \equiv 0 \bmod 8$ since $a_{JL'} = 48$. Thus, $c_L a_{JL} \equiv 0 \bmod 8$. But $a_{JL} = 12$, so $c_L \cdot 4 \equiv 0 \bmod 8$, which implies $c_L \equiv 0 \bmod 2$ as desired.

• Fix $L \in \mathscr{L}$ such that $R(L)^* = \mathbf{C}_2$. Note that $p \equiv 3 \bmod 8$ by Lemma 4. Let J be the orthogonal complement of R_L^* in $L^{\#}$. We first determine the local structure of J at 2 and at p, respectively.

Let $\{v, x\}$ be a basis for R_L^* such that $\mathrm{Mat}(v, x) =< 2, 2 >$. Let K be the orthogonal complement of R_L^* in L. By Lemma 6, we have $dK = 4p$, $K_2 \cong 2\mathbb{A}$, and $K_p \cong < \delta, \delta p >$. Note that $R_L^* \perp K$ has index 2 in L. Let $\{y, z\} \subset K$ such that $\mathrm{Mat}(y, z) \equiv \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix} \bmod 64$. Then, L is equal to $(R_L^* \perp K) + \mathbb{Z}[\frac{v+x+y}{2}]$, $(R_L^* \perp K) + \mathbb{Z}[\frac{v+x+z}{2}]$ or $(R_L^* \perp K) + \mathbb{Z}[\frac{v+x+y+z}{2}]$. Note that $K \subset J \subset K^{\#}$ and that $[K^{\#} : K] = 4p$.

Since $L_p^{\#} \cong <1,1,\delta,\frac{\delta}{p}>$ and $(R_L^*)_p$ splits $L_p^{\#}$, $J_p \cong <\delta,\frac{\delta}{p}>$. Then, $J_p = K_p^{\#}$ since both $[J_p : K_p]$ and $[K_p^{\#} : K_p]$ equal p.

Now, $[J : K]$ equals $1, 2$ or 4. To determine this index, consider the localization at 2. Note that $K_2^{\#}$ is generated by $\{\frac{y}{2}, \frac{z}{2}\}$. If $L = (R_L^* \perp K) + \mathbb{Z}[\frac{v+x+y}{2}]$, then $B(\frac{y}{2}, L) \subset \mathbb{Z}$ and $\frac{y}{2} \in J_2 \backslash K_2$, since $\frac{y}{2}$ is orthogonal to R_L^* and has conductor 2 with respect to K. So, $[J : K]$ cannot be 1. Further, $B(\frac{z}{2}, L) \not\subset \mathbb{Z}$, so $\frac{z}{2} \in K_2^{\#} \backslash L_2^{\#}$, and $[K_2^{\#} : J_2]$ cannot be 1. Thus, $[J_2 : K_2]$ equals 2. A similar argument holds if L is equal to $(R_L^* \perp K) + \mathbb{Z}[\frac{v+x+z}{2}]$ or $(R_L^* \perp K) + \mathbb{Z}[\frac{v+x+y+z}{2}]$. Now, $[J : K] = 2p$, so $[L^{\#} : R_L^* \perp J] = 4$ and $dJ = \frac{1}{p}$.

Finally, since $dJ_2 = p$, $J_2 \cong \mathbb{A}$ (since $p \equiv 3 \mod 8$) or $<\epsilon, \epsilon p>$ for some $\epsilon \in \mathbb{Z}_2^{\times}$. Now, J_2 is not isometric to $\mathbb{A}$ since this would imply $(R_L^* \perp J)_2$ is represented by L_2. So, $J_2 \cong <\epsilon, \epsilon p>$. However, since $p \equiv 3 \mod 8$, the isometry class of $<\epsilon, \epsilon p>$ will not change no matter what the value of ϵ is. Thus, $J_2 \cong <1, p>$.

To summarize what we have just shown: $dJ = \frac{1}{p}$, $J_2 \cong <1,p>$, and $J_p \cong <\delta, \frac{\delta}{p}>$.

Now, let $\{\alpha, \beta\} \subset J$ such that $\mathrm{Mat}(\alpha, \beta) \equiv <1, p> \mod 64$. Let $M = R_L^* \perp J$. Then, $L^{\#}$ is obtained by adjoining any two vectors in the set $\{\frac{v+x}{2}, \frac{v+\alpha+\beta}{2}, \frac{x+\alpha+\beta}{2}\}$ to M. Note that adjoining any two of these three vectors to M will produce a lattice containing the third. Thus, we have exactly one lattice in $\mathcal{G}^{\#}$ containing M.

Let $\phi : J \to L^{\#}$ be an isometric embedding and suppose that $\phi(J)$ is orthogonal to R_L^* in $L^{\#}$. Then, ϕ is an isometry of J. If σ is the isometry $1_{R_L^*} \perp \phi$, then $\sigma(L^{\#}) = L^{\#}$ since $L^{\#}$ is the only lattice in $\mathcal{G}^{\#}$ containing M. Thus, $\sigma \in O(L^{\#}) = O(L)$. Because $O(L) = O(C_2) \times \{\pm 1_K\} = O(C_2) \times \{\pm 1_J\}$, we must have that $\phi = \pm 1_J$. Therefore, there are precisely two embeddings ϕ of J

into $L^\#$ such that $\phi(J)$ is orthogonal to R_L^*. Suppose $\phi(J)$ is not orthogonal to any vector v of length 2 in R_L^*. Then, by Lemma 10, we have that $|\mathrm{orb}(\phi)| = 4$ and the number of distinct embeddings with this property is divisible by 4. Finally, suppose that $\phi(J)$ is orthogonal to a vector of length 2 in $R(L)^*$ but is not orthogonal to another vector of length 2 in $R(L)^*$. Without loss of generality, we may assume that $\phi(J)$ is orthogonal to v but not x. Then, the group $\{\pm\tau_x, \pm 1_L\}$ acts on the set of embeddings with this property since v and x are orthogonal. The size of this set is divisible by 4, and we conclude that $a_{JL^\#} \equiv 2 \bmod 4$.

Suppose now that $\phi : J \to L'^\#$ is an isometric embedding such that $L' \neq L$ and $\min(L') = 2$. Further, suppose $\phi(J)$ is orthogonal to a minimal vector e of L'. Then, ϕ can be extended to an isometry ϕ' on $\mathbb{Q}L$ such that $\phi'(v) = e$ and $\phi'|_J = \phi$. Let N denote the orthogonal complement of $\mathbb{Z}[e] \perp \phi(J)$ in $L'^\#$ and K' be the orthogonal complement of $\mathbb{Z}[e]$ in $L'^\#$. Then, since $L_2'^\# \cong \mathbb{H} \perp < \frac{-1}{2}, \frac{3}{2} >$, K_2' is isometric to $< -2, \frac{-1}{2}, \frac{3}{2} >$. Further, $\phi(J_2) \cong < 1, 3 >$ is a sublattice of K_2' and $dN_2 = \frac{1}{2}, 2$, or 8.

Suppose that $dN_2 = \frac{1}{2}$. Then, $N_2 \cong < \frac{1}{2} >$ splits K_2' and hence $< 2, 6 >$ is represented by $< 4\epsilon, \gamma >$ for some 2-adic units ϵ and γ. However, this is impossible since $< 4\epsilon, \gamma >$ only represents even numbers that are multiples of 4. Next, suppose that $dN_2 = 8$. Then, the index of $\phi(J_2) \perp N_2$ in K_2' is 4. Let $\{r, s\}$ be a basis of $\phi(J)$ and t be the basis vector of N_2 such that $\mathrm{Mat}(r, s, t) = < 1, 3, 8 >$. Let $w = \frac{ar+bs+ct}{4}$ be a vector of conductor 4 with respect to K' and suppose that w is adjoined to $\mathbb{Z}_2[r, s, t]$ to obtain K_2'. Then, both a and b must be even so that $2a^2 + 6b^2 + 16c^2 \equiv 0 \mod 16$ and $2B(w, r)$ and $2B(w, s)$ are integers. Now, $2w$ is an element in $\mathbb{Z}_2[r, s, w] \cong K_2'$, implying $\frac{t}{2}$ is an element of K_2'. However, since t is primitive in K_2', this is impossible. So, we must adjoin two vectors of conductor 2 to obtain K_2'. A direct calculation shows that we must adjoin $\frac{r+s}{2}$ and $\frac{r+s+t}{2}$, but this again implies that $\frac{t}{2}$ is in K_2'. Thus, we cannot have dN_2 equal to 8, and so $dN_2 = 2$. Therefore, the orthogonal complement of $\mathbb{Z}[e] \perp \phi(J)$ in $L'^{\#}$ is isometric to $< 2 >$.

Now, $\phi'^{-1}(L'^{\#})$ contains M. However, since there is only one lattice in $\mathcal{G}^{\#}$ containing M, it must be that $\phi'(L^{\#}) = L^{\#}$ and hence $L' = L$, which is impossible. So, $\phi(J)$ is not orthogonal to any minimal vector e in L', and by Lemma 10, $a_{JL'^{\#}} \equiv 0 \bmod 4$ for all $L' \neq L$ in $\mathscr{L}$.

For L' with $\min(L') = 4$, previous consideration shows that $c_{L'} \equiv 0 \bmod 2$ and $a_{JL'^{\#}} \equiv 0 \bmod 2$. Thus, $c_{L'}a_{JL'^{\#}} \equiv 0 \bmod 4$. The same conclusion holds for all L' previously considered with minimum 2.

For $L' \neq L$, we have seen that $a_{JL'^{\#}} \equiv 0 \bmod 4$. Thus, $c_L a_{JL^{\#}} \equiv 0 \bmod 4$. But $a_{JL^{\#}} \equiv 2 \bmod 4$. Therefore, $c_L \equiv 0 \bmod 2$.

• Fix $L \in \mathscr{L}$ such that $R(L)^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$. Note that $p \equiv 3 \bmod 8$ by Lemma 4 and R_L^* has index 2 in L. By Corollary 2, L represents the only class in $\mathcal{G}$ with this scaled root system. Let J be a binary sublattice of L such that $J \cong C_2$. Then, there exists an embedding of J into $L' \in \mathscr{L}$ only if $R(L')^* = \mathbf{C}_2$ or $\mathbf{C}_3 \perp \mathbf{A}_1^{2p}$. If $R(L')^* = \mathbf{C}_2$, then there are 8 distinct ways to embed J into L' since $|O(C_2)| = 8$.

To determine the number of embeddings of J into L, we proceed in the following way. Let $\{v, x\}$ be an orthogonal basis for $J \cong < 2, 2 >$ and $\{e, f, g\}$ be a basis for R_L such that $\mathrm{Mat}(e, f, g) = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$. Then, there are 12 ways to send v into R_L. Once this choice is made, there are 2 ways to send x into R_L. One can see this by noting that the orthogonal complement of a minimal vector in R_L is isometric to $< 2, 4 >$. Thus, there are 24 ways to embed J into L.

Now, if $L' \neq L$ and $R(L')^*$ is neither $\mathbf{C}_2$ nor $\mathbf{C}_3 \perp \mathbf{A}_1^{2p}$, then $a_{JL'} = 0$. By the previous case, we have that $c_{L'} \equiv 0 \bmod 2$ when $R(L')^* = \mathbf{C}_2$, and from above $a_{JL'} = 8$, so $c_{L'} a_{JL'} \equiv 0 \bmod 16$ in this situation. Thus, $c_L a_{JL} \equiv 0 \bmod 16$. However, $a_{JL} = 24$, so $c_L \cdot 8 \equiv 0 \bmod 16$. Thus, $c_L \equiv 0 \bmod 2$.

• Fix $L \in \mathscr{L}$ such that $R(L)^* = \mathbf{A}_1 \perp \mathbf{A}_1^2$ and let K be the orthogonal complement of R_L^* in L. By Lemma 9, $dK = 8p$, $K_2 \cong < 12, 6p >$ and $K_p \cong < 2\delta, \delta p >$. Let $J = K$ and $\{y, z\} \subset J$ such that $\mathrm{Mat}(y, z) \equiv < 12, 6p > \bmod 64$ and $\{v, x\}$ be an orthogonal basis for $R_L^* \cong < 2, 4 >$. Let $M = R_L^* \perp K$. Then, L can only be obtained by adjoining two vectors in the set $\{\frac{x+y}{2}, \frac{v+x+z}{2}, \frac{v+y+z}{2}\}$ to M. However, by adjoining any two of these vectors to M, the lattice obtained will contain the third vector. Thus, L is the only lattice in $\mathcal{G}$ containing the full sublattice M.

Suppose $\phi : J \to L$ is an isometric embedding such that $\phi(J)$ is orthogonal to R_L^* in L. Then, $\phi(J) = J$. Note that $dJ^{1/2} = 2p$. By Gauss' theory, there are only two ambiguous classes of binary lattices with discriminant $2p$. They are represented by the Gram matrices $< 1, 2p >$ and $< 2, p >$, respectively. Because J does not represent 2, $J^{1/2}$ cannot be isometric to $< 1, 2p >$. By local consideration at p, since $J_p^{1/2} \cong < \delta, \delta 2p >$, $J^{1/2}$ cannot be isometric to $< 2, p >$. Thus, J is unambiguous and $O(J) = \{\pm 1_J\}$. So, $\phi = \pm 1_J$ and there are precisely two embeddings of J into L such that $\phi(J)$ is orthogonal to R_L^*. Now, suppose $\phi(J)$ is orthogonal to only one of v and x. In this case, we may apply Lemma 10 to determine that $|\mathrm{orb}(\phi)| = 4$ in each of these situations. Therefore, the number of distinct embeddings satisfying this property is divisible by 4. Consequently, $a_{JL} \equiv 2 \bmod 4$.

Let $\phi : J \to L'$ be an isometric embedding such that $L \neq L'$ and $\min(L') = 2$. Suppose that $\phi(J)$ is orthogonal to a vector e of length 2 in L'. Then, ϕ can be extended to an embedding ϕ' of $\mathbb{Z}[v] \perp J$ into L' where $\phi'(v) = e$ and $\phi'|_J = \phi$. Then, by considering the discriminant, the orthogonal complement of $\phi'(\mathbb{Z}[v] \perp J)$ in L' is isometric to $\mathbb{Z}[x]$. Thus, ϕ' can be extended to an isometry Φ of $\mathbb{Q}L$, and $\Phi^{-1}(L')$ is a lattice in $\mathcal{G}$ containing M. Since we have shown that there is only one class of lattices in $\mathcal{G}$ containing M, L must equal L', which is impossible. Thus, $\phi(J)$ cannot be orthogonal to any vector of length 2 in L', and by Lemma 10, $a_{JL'} \equiv 0 \bmod 4$.

From above, $a_{JL'} \equiv 0 \bmod 4$ when $L \neq L'$. Thus, $c_L a_{JL} \equiv 0 \mod 4$. But, $a_{JL} \equiv 2 \mod 4$, and we have $c_L \equiv 0 \mod 2$.

Finally, we have obtained a contradiction by showing that $c_{L'} \equiv 0 \mod 2$ for all $L' \in \mathscr{L}$. Therefore, the degree 2 theta series of the classes in $\mathcal{G}$ with nontrivial orthogonal groups are linearly independent over $\mathbb{Z}$.

$\square$

Chapter 4

The Second Genus

Throughout this chapter, all lattices will be in the second genus $\mathcal{G}'$. We proceed as we did in Chapter 3 by first determining all possible root systems of the lattices in $\mathcal{G}'$. Then, we determine the scaled root systems and show that the orthogonal group of a lattice in $\mathcal{G}'$ is generated by symmetries with respect to the vectors in the scaled root system and -1. We conclude with the proof of the linear independence of the degree 2 theta series associated to the classes in $\mathcal{G}'$ with nontrivial orthogonal groups.

4.1 Root Systems

We will now determine the possible root systems of a lattice in $\mathcal{G}'$. Recall that a lattice L in $\mathcal{G}'$ has $L_p \cong< 1, 1, \delta, \delta p >$ where 2δ is a square mod p and $L_2 \cong \mathbb{H} \perp< 2, -2p >\cong \mathbb{A} \perp< 2, 6p >$.

Considering only the rank of a lattice in $\mathcal{G}'$, we obtain the same list of possible root systems as for the lattices in $\mathcal{G}$: $\emptyset$, $\mathbf{A}_1$, $2\mathbf{A}_1$, $\mathbf{A}_2$, $3\mathbf{A}_1$, $\mathbf{A}_2 \perp \mathbf{A}_1$, $\mathbf{A}_3$, $4\mathbf{A}_1$, $\mathbf{A}_2 \perp \mathbf{A}_2$, $\mathbf{A}_2 \perp 2\mathbf{A}_1$, $\mathbf{A}_3 \perp \mathbf{A}_1$, $\mathbf{A}_4$ and $\mathbf{D}_4$. Again, we eliminate all full rank root systems by considering the discriminants of their corresponding root sublattices.

Lemma 11. *If L is a lattice in $\mathcal{G}'$ and $R(L) = \boldsymbol{A}_3$ or $2\boldsymbol{A}_1$, then $p \equiv -1 \mod 8$.*

Proof. Let L be a lattice in $\mathcal{G}'$ such that $R(L) = \mathbf{A}_3$. Over $\mathbb{Z}_2$, $(A_3)_2 \cong \mathbb{A} \perp < 12 >$. Since $L_2 \cong \mathbb{A} \perp < 2, 6p >$, 12 is represented by $< 2, 6p >$ over $\mathbb{Z}_2$, or equivalently, 6 is represented by $< 1, 3p >$ over $\mathbb{Z}_2$. If $p \equiv 3 \mod 8$, then $< 1, 3p > \cong < 1, 1 >$, which represents 6 only if there exist $x, y \in \mathbb{Z}_2$ such that $x^2 + y^2 \equiv 6 \mod 8$. However, this is impossible by direct verification. Thus, if $R(L) = \mathbf{A}_3$, then $p \equiv -1 \mod 8$.

Now, suppose $R(L) = 2\mathbf{A}_1$. Then, $\mathbb{Q}_2 L_2 \cong [2, 2, \epsilon, \epsilon p]$ for some $\epsilon = 1, 3, 5$, or -1. A direct computation shows that $S_2([2, 2, \epsilon, \epsilon p]) = (\epsilon, -p)_2 (p, -1)_2 = -1$ for both $p \equiv -1 \mod 8$ and $p \equiv 3 \mod 8$ no matter what the value of ϵ is. However, as noted earlier, the Hasse symbol of $\mathbb{Q}_2 L_2$ at 2 is $-(p, 2)_2$. Thus,

$$S_2(\mathbb{Q}_2 L_2) = \begin{cases} -1 & \text{if } p \equiv -1 \bmod 8, \\ 1 & \text{if } p \equiv 3. \bmod 8 \end{cases}$$

Therefore, $\mathbb{Q}_2 L_2$ is not isometric to $[2, 2, \epsilon, \epsilon p]$ when $p \equiv 3 \mod 8$. Consequently, if $R(L) = 2\mathbf{A}_1$, then $p \equiv -1 \mod 8$. □

Lemma 12. *If L is a lattice in $\mathcal{G}'$ and $R(L) = \boldsymbol{A}_2 \perp \boldsymbol{A}_1$, then $p \equiv -1 \mod 3$.*

Proof. Let L be a lattice in $\mathcal{G}'$ such that $R(L) = \mathbf{A}_2 \perp \mathbf{A}_1$. Over $\mathbb{Q}_3$, $(A_2 \perp A_1)_3 \cong [2, 2, 6]$, so $\mathbb{Q}_3 L_3 \cong [2, 2, 6, 6p]$. Then, $S_3([2, 2, 6, 6p]) = -(3, p)_3$ and since $S_3(\mathbb{Q}_3 L_3) = (p, -1)_3 = 1$, it follows that $p \equiv -1 \mod 3$. Therefore, if $R(L) = \mathbf{A}_2 \perp \mathbf{A}_1$, then $p \equiv -1 \mod 3$. □

Thus, for any lattice L in $\mathcal{G}'$, $R(L)$ is equal to one of the following: $\emptyset$, $\mathbf{A}_1$, $2\mathbf{A}_1$, $\mathbf{A}_2$, $3\mathbf{A}_1$, $\mathbf{A}_2 \perp \mathbf{A}_1$, $\mathbf{A}_3$.

4.2 Scaled Root Systems and $O(L)$

We now determine the possible scaled root systems for the lattices L in $\mathcal{G}'$ and show that $O(L)$ is generated by -1_L and symmetries with respect to the vectors in the scaled root system. As in Section 3.2, we first determine the orthogonal complement of the root sublattice R_L in L. Recall that if a lattice L in $\mathcal{G}'$ is decomposable, then L has an indecomposable component isometric to $< 2 >$ and has decomposition as described in Lemma 2.

Lemma 13. *Let L be a lattice in $\mathcal{G}'$ with $\min(L) = 2$ and $v \in L$ such that $Q(v) = 2$. Let K be the orthogonal complement of $\mathbb{Z}[v]$ in L. Then, one of the following holds:*

1. *$\mathbb{Z}[v]$ splits L (hence L must be decomposable), $dK = 2p$, $K_2 \cong \mathbb{H} \perp< -2p >\cong \mathbb{A} \perp< 6p >$, and $K_p \cong< 1, 2\delta, \delta p >$, or*
2. *$\mathbb{Z}[v]$ does not split L, $dK = 8p$, $K_2 \cong< -2, 2, -2p >$, and $K_p \cong< 1, 2\delta, \delta p >$.*

Proof. It is clear that K is an even, ternary lattice. Since $dK|(2 \cdot dL)$ and $2 \cdot dK = dL[L : \mathbb{Z}[v] \perp K]^2$, dK is either $2p$ or $8p$. Suppose $dK = 2p$. Then, $[L : \mathbb{Z}[v] \perp K] = 1$ and $L = \mathbb{Z}[v] \perp K$, so L is decomposable. Over $\mathbb{Z}_2$, since $L = \mathbb{Z}[v] \perp K$, $L_2 \cong< 2 >\perp K_2$. Then, since K is an even ternary lattice of discriminant $2p$ and $\mathbb{H} \perp< 2, -2p >\cong L_2 \cong< 2 >\perp K_2$, it follows that $K_2 \cong \mathbb{H} \perp< -2p >$.

Similarly, over $\mathbb{Z}_p$, $L_p \cong< 2 >\perp K_p$. Thus, since $< 1, 1, \delta, \delta p >\cong L_p \cong< 2 >\perp K_p$, we have $K_p \cong< 1, 2\delta, \delta p >$.

Suppose $dK = 8p$. Then, $[L : \mathbb{Z}[v] \perp K] = 2$ and $\mathbb{Z}[v]$ does not split L. Suppose that K_2 has a unimodular component $\mathbb{P}$ of rank 2. Then, $\mathbb{P}$ must be even and $K_2 \cong \mathbb{P} \perp < 8\epsilon >$ for some $\epsilon \in \mathbb{Z}_2^\times$. So, $\mathbb{P}$ splits L_2 and its orthogonal complement contains $\mathbb{Z}_2[v]$, which we know to be orthogonal to $< -2p >$ or $< 6p >$. Thus, $< 8\epsilon > \cong < -2p >$ or $< 6p >$, which is impossible since ϵ is a 2-adic unit. Thus, K_2 cannot have an even unimodular component, and hence it must be a (2)-modular $\mathbb{Z}_2$ lattice. This implies that $K_2 \cong 2\mathbb{P} \perp < 2\epsilon >$ for some $\epsilon \in \{1, 3, 5, -1\}$. Direct computation shows that K_2 is isotropic, which implies $\mathbb{P} \cong \mathbb{H}$. Thus, $K_2 \cong 2\mathbb{H} \perp < -2p > \cong < -2, 2, -2p >$.

Since $< 2 >$ is a unimodular $\mathbb{Z}_p$-lattice, it must split L_p. Therefore, $< 2 > \perp K_p \cong L_p \cong < 1, 1, \delta, \delta p >$, and hence $K_p \cong < 1, 2\delta, \delta p >$.

□

Lemma 14. *Let L be a lattice in $\mathcal{G}'$ such that $R(L) = 2\boldsymbol{A}_1$ and let K be the orthogonal complement of R_L in L. Then, one of the following holds:*

1. *$dK = p$, R_L splits L, $K_p \cong < \delta, \delta p >$, and $K_2 \cong \mathbb{H}$,*
2. *$dK = 4p$, $K_p \cong < \delta, \delta p >$, and $K_2 \cong < -2, -2p >$, and L is decomposable,*
3. *$dK = 4p$, $K_p \cong < \delta, \delta p >$, and $K_2 \cong 2\mathbb{H}$, and L is indecomposable.*

Proof. By Lemma 11, if $R(L) = 2\mathbf{A}_1$, then $p \equiv -1 \bmod 8$. Let v and x be orthogonal vectors in $R(L)$ such that $R_L = \mathbb{Z}[v, x]$. Since $dK | (4 \cdot 4p)$ and $4 \cdot dK = 4p[L : R_L \perp K]^2$, dK is either p, $4p$, or $16p$.

First, suppose that L is decomposable. Then, $L = \mathbb{Z}[v] \perp N$ where N is an even ternary lattice as in Lemma 13. Note that $\mathbb{Z}[x] \perp K$ is represented by N. Since $dK | (2 \cdot dN)$ and $2 \cdot dK = dN[N : \mathbb{Z}[x] \perp K]^2$, dK is either p or $4p$.

Suppose that $dK = p$. Then, $[L : R_L \perp K] = 1$ and $L = R_L \perp K$. So, R_L splits L. Over $\mathbb{Z}_2$, K is a binary even unimodular lattice with $dK_2 = p$.

Since $p \equiv -1 \bmod 8$, $K_2 \cong \mathbb{H}$. Over $\mathbb{Z}_p$, $(R_L)_p$ is unimodular and splits L_p, so $(R_L)_p \perp K_p \cong L_p \cong <1, 1, \delta, \delta p>$. Thus, $K_p \cong <\delta, \delta p>$.

Suppose now that $dK = 4p$. Then, $[L : R_L \perp K] = 2$ and N does not decompose as $\mathbb{Z}[x] \perp K$. So, K_2 is a (2)-modular lattice. Now, $<2> \perp K_2$ has discriminant $8p$ and by the argument in the proof of Lemma 13, $<2> \perp K_2 \cong < 2, -2, -2p > \cong < 2, -2, 2 > \cong <2> \perp 2\mathbb{H}$. Thus, $K_2 \cong < -2, -2p >$ or $2\mathbb{H}$.

Suppose that $K_2 \cong 2\mathbb{H}$. Let $\{y, z\} \subset K$ such that $\mathrm{Mat}(y, z) \equiv \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$ mod 64. Then, a lattice L in $\mathcal{G}'$ containing $R_L \perp K$ is obtained by adjoining $\frac{y}{2}, \frac{z}{2}$, or $\frac{v+x+y+z}{2}$ to $R_L \perp K$. If L were equal to either of the lattices obtained by adjoining $\frac{y}{2}$ or $\frac{z}{2}$, then R_L would split L, which is impossible. Further, if L were obtained by adjoining $\frac{v+x+y+z}{2}$, L would be indecomposable, which is also impossible. Thus, $K_2 \ncong 2\mathbb{H}$ when L is decomposable and R_L does not split L. Therefore, $K_2 \cong < -2, -2p >$. Over $\mathbb{Z}_p$, $(R_L)_p$ is unimodular and splits L_p, so $(R_L)_p \perp K_p \cong L_p \cong <1, 1, \delta, \delta p>$. Thus, $K_p \cong <\delta, \delta p>$.

Now, suppose L is indecomposable. Then, $<2> \perp K$ is a sublattice of the orthogonal complement of a vector of length 2 in L. Lemma 13 implies that $<2> \perp K_2$ is represented by $< -2, 2, -2p > \cong < -2, 2, 2 > \cong <2> \perp 2\mathbb{H}$. Therefore, $dK = 4p$ and $K_2 \cong < -2, -2p >$ or $2\mathbb{H}$.

Let $\{e, f\} \subset K$ such that $\mathrm{Mat}(e, f) \equiv < -2, -2p >$ mod 64. A lattice L in $\mathcal{G}'$ containing $R_L \perp K$ is obtained by adjoining $\frac{v+e}{2}$, $\frac{x+e}{2}$, or $\frac{e+f}{2}$ to $R_L \perp K$, and L is equal to one of the three lattices $(R_L \perp K) + \mathbb{Z}[\frac{v+e}{2}]$, $(R_L \perp K) + \mathbb{Z}[\frac{x+e}{2}]$, or $(R_L \perp K) + \mathbb{Z}[\frac{e+f}{2}]$. Now, $\{v, \frac{v+e}{2}, x, f\}$ is a basis for $(R_L \perp K) + \mathbb{Z}[\frac{v+e}{2}]$. However, if $L = (R_L \perp K) + \mathbb{Z}[\frac{v+e}{2}]$, then $L = \mathbb{Z}[x] \perp N$ where N is generated by $\{v, \frac{v+e}{2}, f\}$, which is impossible. A similar argument holds for L equal to both remaining lattices. Thus, if L is indecomposable, then $K_2 \ncong < -2, -2p >$. So,

$K_2 \cong 2\mathbb{H}$. Over $\mathbb{Z}_p$, $(R_L)_p$ is unimodular and splits L_p, so $(R_L)_p \perp K_p \cong L_p \cong <1, 1, \delta, \delta p>$. Thus, $K_p \cong <\delta, \delta p>$.

$\square$

Lemma 15. *Let L be a lattice in $\mathcal{G}'$ such that $R(L) = \boldsymbol{A}_2$ and let K be the orthogonal complement of R_L in L. Then, L is indecomposable, $dK = 12p$, $K_2 \cong <2, 6p>$, $K_p \cong <3\delta, \delta p>$, and $K_3 \cong <3, p>$.*

Proof. Suppose L is decomposable. Then, L has an orthogonal component isometric to $<2>$ by Lemma 2. However, since $R_L = A_2$, this is impossible. Thus, L is indecomposable. Since $dK|(3 \cdot dL)$ and $3 \cdot dK = dL[L : R_L \perp K]^2$, $dK = 12p$ and $[L : R_L \perp K] = 3$. Over $\mathbb{Z}_2$, $(R_L)_2 \cong \mathbb{A}$ and splits L_2. Therefore, since $\mathbb{A} \perp <2, 6p> \cong L_2 \cong (R_L)_2 \perp K_2$, $K_2 \cong <2, 6p>$.

Over $\mathbb{Z}_p$, $(R_L)_p \cong <1, 3>$ is unimodular and splits L_p. Thus, $<1, 3> \perp K_p \cong L_p \cong <1, 1, \delta, \delta p>$, so $K_p \cong <3\delta, \delta p>$. Finally, over $\mathbb{Z}_3$, $(R_L)_3 \cong <2, 6>$. Since $dK_3 = 3p$, $K_3 \cong <p\epsilon, 3\epsilon>$ for some ϵ in $\mathbb{Z}_3^\times$, and $\mathbb{Q}_3 L_3 \cong [2, 6, \epsilon p, 3\epsilon]$. By Hasse symbol calculation, $\epsilon = 1$. Thus, $K_3 \cong <p, 3>$. $\square$

Lemma 16. *Let L be a lattice in $\mathcal{G}'$ and K denote the orthogonal complement of R_L in L.*

1. *If $R(L) = 3\boldsymbol{A}_1$, then L is decomposable, $dK = 2p$ and $K \cong <2p>$.*

2. *If $R(L) = \boldsymbol{A}_2 \perp \boldsymbol{A}_1$, then L is decomposable, $dK = 6p$, and $K \cong <6p>$.*

3. *If $R(L) = \boldsymbol{A}_3$, then L is indecomposable, $dK = 4p$ and $K \cong <4p>$.*

Proof. (1) Suppose that $R(L) = 3\mathbf{A}_1$. Then,

$$L \cong \begin{pmatrix} 2 & 0 & 0 & * \\ 0 & 2 & 0 & * \\ 0 & 0 & 2 & * \\ * & * & * & * \end{pmatrix}.$$

By Minkowski reduction, the only L in $\mathcal{G}'$ with $R(L) = 3\mathbf{A}_1$ is

$$L \cong < 2 > \perp < 2 > \perp \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}.$$

Thus, if $R(L) = 3\mathbf{A}_1$, L is decomposable.

Further, since $2A_1$ splits L, $< 2 > \perp K$ is represented by $\begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}$. Then, because K is an even, rank 1 lattice and $dK|(2 \cdot p)$, $dK = 2p$. Thus, $K \cong < 2p >$.

(2) Suppose that $R(L) = \mathbf{A}_2 \perp \mathbf{A}_1$. Then,

$$L \cong \begin{pmatrix} 2 & 0 & 0 & * \\ 0 & 2 & 1 & * \\ 0 & 1 & 2 & * \\ * & * & * & * \end{pmatrix}.$$

Minkowski reduction implies that the only lattices L in $\mathcal{G}'$ with $R(L) = \mathbf{A}_2 \perp \mathbf{A}_1$ are decomposable.

Now, K is an even, rank 1 lattice. Since $dK|(6 \cdot dL)$ and $6 \cdot dK = dL[L : R_L \perp K]^2$, dK is either $6p$ or $24p$. Over $\mathbb{Z}_2$, $(R_L)_2 \cong \mathbb{A} \perp < 2 >$. By Lemma 13, since L is decomposable, $\mathbb{A} \perp K_2$ is represented by $\mathbb{A} \perp < 6p >$. But $\mathbb{A}$ splits $\mathbb{A} \perp < 6p >$, so $K_2 \cong < 6p >$. Thus, $dK = 6p$ and $K \cong < 6p >$.

(3) Suppose that $R(L) = \mathbf{A}_3$. Then,

$$L \cong \begin{pmatrix} 2 & 1 & 0 & * \\ 1 & 2 & 1 & * \\ 0 & 1 & 2 & * \\ * & * & * & * \end{pmatrix}.$$

By Minkowski reduction, the only lattices L in $\mathcal{G}'$ with $R(L) = \mathbf{A}_3$ are indecomposable.

Now, K is an even, rank 1 lattice. Since $dK|(4 \cdot dL)$ and $4 \cdot dK = dL[L : R_L \perp K]^2$, dK is equal to p, $4p$, or $16p$. Notice that $dK \neq p$ since K is even with rank 1. Over $\mathbb{Z}_2$, $(A_3)_2 \cong \mathbb{A} \perp < 12 >$, and because $\mathbb{A}$ splits L_2, K_2 is the orthogonal complement of $< 12 >$ in $< 2, 6p >$. Therefore, $dK = 4p$ and $K \cong < 4p >$.

□

Corollary 3. *There is only one class in $\mathcal{G}'$ with root system $3\boldsymbol{A}_1$. This class contains the lattice*

$$< 2 > \perp < 2 > \perp \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}.$$

Corollary 4. *If a lattice L in $\mathcal{G}'$ is decomposable, then $R(L) = \boldsymbol{A}_1, 2\boldsymbol{A}_1, 3\boldsymbol{A}_1$, or $\boldsymbol{A}_2 \perp \boldsymbol{A}_1$. Further, if L is indecomposable, then $R(L) = \emptyset, \boldsymbol{A}_1, 2\boldsymbol{A}_1, \boldsymbol{A}_2$, or $\boldsymbol{A}_3$.*

We now proceed with the determination of the possible scaled root systems and orthogonal group structure of the decomposable lattices in $\mathcal{G}'$.

Lemma 17. *Let L be a decomposable lattice in $\mathcal{G}'$ such that $O(L)$ is nontrivial. Then, $R(L)^*$ is one of the following: $\boldsymbol{A}_1$, $2\boldsymbol{A}_1$, $\boldsymbol{C}_2$, $\boldsymbol{C}_2 \perp \boldsymbol{A}_1 \perp \boldsymbol{A}_1^p$, or $\boldsymbol{A}_2 \perp \boldsymbol{A}_1$. Further, $O(L)$ is generated by -1_L and symmetries.*

Proof. By Corollary 4, if a lattice L in $\mathcal{G}'$ is decomposable, then $R(L) = \mathbf{A}_1, 2\mathbf{A}_1$, $3\mathbf{A}_1$, or $\mathbf{A}_2 \perp \mathbf{A}_1$. We will proceed with cases for each possible $R(L)$.

• Suppose $R(L) = \mathbf{A}_1$ and let K denote the orthogonal complement of R_L in L. By Lemma 13, since L is decomposable, K is an even ternary lattice of discriminant $2p$. Thus, by definition, K is primal. This implies that $O(K)$ is generated by symmetries with respect to the minimal vectors of K by [15, Cor. 4.5]. However, because $R(L) = \mathbf{A}_1$, K does not represent 2. So, $O(K) = \{\pm 1_K\}$. Therefore, $R(L) = R(L)^*$ and $O(L) = O(R_L) \times \{\pm 1_K\} = \langle -1_L, W(R_L^*)\rangle$.

• Suppose that $R(L) = 2\mathbf{A}_1$ and let K denote the orthogonal complement of R_L in L. By Lemma 11, $p \equiv -1 \bmod 8$. By Lemma 14, either $dK = p$ and R_L splits L or $dK = 4p$. First, suppose $dK = p$. Since K is a binary even lattice with $dK = p$, K is primal, and $O(K)$ is generated by symmetries with respect to the vectors of length 2 in K. However, since $R(L) = 2\mathbf{A}_1$, K does not represent 2. Thus, $O(K) = \{\pm 1_K\}$.

Now $L = R_L \perp K$ and $O(L) = O(R_L) \times O(K)$. Because $O(R_L) = O(2A_1) = O(C_2)$, we have $R(L)^* = \mathbf{C}_2$. Thus, $O(L) = O(R_L) \times \{\pm 1_K\} = \langle -1_L, W(R(L)^*)\rangle$.

Suppose $dK = 4p$. Let v and x be orthogonal basis vectors for R_L such that $\mathrm{Mat}(v, x) =< 2 > \perp < 2 >$ and let $L = \mathbb{Z}[v] \perp N$ where N is an even ternary lattice as in Lemma 13. Then, $R_L \perp K$ has index 2 in L and $K_2 \cong < -2, -2p >$ by Lemma 14. Let $\{y, z\} \subset K$ such that $\mathrm{Mat}(y, z) \equiv < -2, -2p > \bmod 64$. Then, to obtain a lattice in $\mathcal{G}'$ containing $R_L \perp K$, we must adjoin $\frac{v+y}{2}$, $\frac{x+y}{2}$, or $\frac{y+z}{2}$ to $R_L \perp K$. So, L is one of $L_0 = (R_L \perp K) + \mathbb{Z}[\frac{v+y}{2}]$, $L_1 = (R_L \perp K) + \mathbb{Z}[\frac{x+y}{2}]$, or $L_2 = (R_L \perp K) + \mathbb{Z}[\frac{y+z}{2}]$. Now, L_0 is isometric to L_1 via τ_{v-x}, so $\mathbf{C}_2$ is not contained in the scaled root system of either L_0 or L_1. The structure of L_2 implies that R_L splits L_2, and so L is either L_0 or L_1. Note that $\langle -1_L, W(R_L^*)\rangle < O(L) < O(R_L) \times O(K)$. We claim that K is unambiguous.

Suppose $O(K) \neq \{\pm 1_K\}$. Since $dK = 4p$, $dK^{1/2} = p$. Let u be an element of $R(K^{1/2})^*$ and w be another element in $K^{1/2}$ so that $K^{1/2} = \mathbb{Z}[u, w]$. Then, since τ_u is an isometry of $K^{1/2}$, $Q(u)$ divides $2B(u, w)$. Because

$$K^{1/2} \cong \begin{pmatrix} Q(u) & B(u,w) \\ B(u,w) & Q(w) \end{pmatrix},$$

it must be that $p = Q(u)Q(w) - B(u, w)^2$ and so $Q(u)$ divides $2p$.

According to Gauss' Theory as described in [3, §14.4], since there is one odd prime dividing $dK^{1/2} = p$, and $dK^{1/2} \equiv 3 \bmod 4$, there are two ambiguous classes of positive definite binary lattices with discriminant p where $p \equiv 3 \bmod 4$. Since the length of a vector in $R(K^{1/2})^*$ divides $2p$, the two ambiguous classes are represented by the following Gram matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}.$$

If $K^{1/2}$ were represented by the first Gram matrix, then K would represent 2, which is impossible. Further, if $K^{1/2}$ were represented by the second, then $(K^{1/2})_2 \cong \mathbb{H}$, which is false by Lemma 14. Thus, $K^{1/2}$ is unambiguous, and $O(K) = \{\pm 1_K\}$. Further, since τ_{v-x} is not an isometry of L, $R(L) = R(L)^*$ and $O(L) = \langle -1_L, W(R_L^*)\rangle$.

- Suppose that $R(L) = 3\mathbf{A}_1$. Then, by Corollary 3,

$$L \cong <2> \perp <2> \perp \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}.$$

Let $\{v, x, y, z\}$ be a basis of L which yields the above Gram matrix. Let $K =$

$\mathbb{Z}[y,z] \cong \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}$. Then, $dK = p$ and K is primal. Thus, $O(K)$ is generated by symmetries with respect to the minimal vectors of K, so $O(K) = \langle -1_K, \tau_y \rangle$.

Since the symmetries with respect to the vectors $\pm(v \pm x)$ of length 4 are in $O(L)$, we have $\mathbf{C}_2 \subset R(L)^*$. Further, the elements of $O(K)$ extend to isometries of L, and in particular, $-\tau_y = \tau_{y-2z}$ is an isometry of L. Since $y - 2z$ is primitive, $y - 2z \in R(L)^*$. Thus, $O(L) = O(\mathbb{Z}[v,x]) \times O(K) = \langle -1_L, W(R_L^*) \rangle$ and $R(L)^* = \mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_1^p$.

• Suppose that $R(L) = \mathbf{A}_2 \perp \mathbf{A}_1$ and let K denote the orthogonal complement of R_L in L. Let $\{v, x, y\}$ be a basis for R_L such that $\mathrm{Mat}(v,x,y) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp < 2 >$ and z a vector in L such that $K \cong \mathbb{Z}[z]$. Then, L is either $(R_L \perp K) + \mathbb{Z}[\frac{v-2x+z}{3}]$ or $(R_L \perp K) + \mathbb{Z}[\frac{v-2x-z}{3}]$. These lattices are isometric via τ_z, and so $\tau_z \notin O(L)$. Since $\langle -1_L, W(R_L^*) \rangle < O(L) < O(R_L) \times O(K)$ and the index of $\langle -1_L, W(R_L^*) \rangle$ in $O(R_L) \times O(K)$ is 2, we have $O(L) = \langle -1_L, W(R_L^*) \rangle$ and $R(L) = R(L)^*$. □

Now, we prove the analogous result for the indecomposable lattices in $\mathcal{G}'$.

Lemma 18. *Let L be an indecomposable lattice in $\mathcal{G}'$ such that $O(L)$ is nontrivial. Then, $R(L)^*$ is one of the following: $\boldsymbol{A}_1^2$, $\boldsymbol{A}_1$, $\boldsymbol{C}_2$, $\boldsymbol{A}_2$, $\boldsymbol{A}_2 \perp \boldsymbol{A}_1^2$, or $\boldsymbol{C}_3 \perp \boldsymbol{A}_1^{2p}$. Further, $O(L)$ is generated by -1_L and symmetries.*

Proof. By Corollary 4, if L is indecomposable, $R(L) = \emptyset, \mathbf{A}_1, 2\mathbf{A}_1, \mathbf{A}_2$, or $\mathbf{A}_3$. We will proceed with cases for each possible $R(L)$.

• Suppose $R(L) = \emptyset$. Then, $\min(L) \geq 4$ and L has a nontrivial isometry of order 2 not equal to -1_L. By Corollary 1, $\min(L) = 4$ and $R(L)^* = \mathbf{A}_1^2$. Further,

$O(L)$ is generated by -1_L and τ_v where v is a vector of length 4 in $R(L)^*$.

• Suppose that $R(L) = \mathbf{A}_3$. By Lemma 11, $p \equiv -1 \bmod 8$. Then, L contains a sublattice $M = R_L \perp \mathbb{Z}[z]$ where $Q(z) = 4p$ and M has index 2 in L. Let $\{v, x, y\} \subset R_L$ such that $\mathrm{Mat}(v, x, y) \equiv A_2 \perp < 12 >$ mod 64. Then, to obtain a lattice in $\mathcal{G}'$ containing M, we can only adjoin $\frac{y \pm z}{2}$ since these are the only vectors in $\mathbb{Q}M$ with conductor 2, with respect to M, representing an even integer. However, $M + \mathbb{Z}[\frac{y+z}{2}]$ and $M + \mathbb{Z}[\frac{y-z}{2}]$ are the same lattice. So, $L = M + \mathbb{Z}[\frac{y+z}{2}]$.

Notice that τ_z fixes every vector in R_L and sends $\frac{y+z}{2}$ to $\frac{y+z}{2} - z$, which is in L. So, τ_z is an isometry of L, and because z is also primitive in L, $z \in R(L)^*$. Note that $O(L) < O(R_L) \times O(\mathbb{Z}[z])$. Since there is only one lattice in $\mathcal{G}'$ containing M, any $\sigma \in O(R_L) \times O(\mathbb{Z}[z])$ must also be in $O(L)$. Thus, $O(L) = O(R_L) \times O(\mathbb{Z}[z])$. Further, $O(R_L) = O(A_3) = O(C_3)$. Therefore, $R(L)^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$ and $O(L) = \langle -1_L, W(R_L^*) \rangle$.

• Suppose that $R(L) = \mathbf{A}_2$ and let K denote the orthogonal complement of R_L in L. Then, the sublattice $M = R_L \perp K$ has index 3 in L. Let $\{v, x\}$ be a basis for R_L such that $\mathrm{Mat}(v, x) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and $\{y, z\} \subset K$ so that $\mathrm{Mat}(y, z) \equiv < 3, p >$ mod 27. Then, $\frac{v-2x+y}{3}$ and $\frac{v-2x-y}{3}$ are the only vectors of conductor 3, with respect to M, that can be adjoined to M to obtain a lattice in $\mathcal{G}'$. Note that $M + \mathbb{Z}[\frac{v-2x+y}{3}]$ is isometric to $M + \mathbb{Z}[\frac{v-2x-y}{3}]$ via the map $1_{R_L} \perp -1_K$. Thus, up to isometry, there is one lattice in $\mathcal{G}'$ containing M. Further, this implies that $-1_K \notin O(L)$ for any L containing M.

Consider the chain $\langle -1_L, W(R_L) \rangle < O(L) < O(R_L) \times O(K)$. If $O(K) = \{\pm 1_K\}$, then $R(L) = R(L)^*$. Since $-1_K \notin O(L)$ and $\langle -1_L, W(R_L) \rangle$ has index 2 in $O(R_L) \times O(K)$, $O(L) = \langle -1_L, W(R_L)\rangle = \langle -1_L, W(R_L^*)\rangle$.

Suppose that $O(K) \neq \{\pm 1_K\}$. If $O(K)$ contains some element σ of odd prime order q, then by an argument similar to the proof of Lemma 1, q cannot be greater than 3. If $q = 3$, by [15, Lemma 2.2], $dK = 3\alpha$ for some square α. However, $dK = 12p$, so this is impossible. Thus, $O(K)$ contains no elements of odd order. Further, if $\sigma \in O(K)$ is an element of order 2 not equal to -1_K, then the rank of L^σ or L_σ is 1. Thus, σ or $-\sigma$ is a symmetry, and all order 2 elements of $O(K)$ are either -1_K or $\pm 1_L$ composed with a symmetry.

Let $N = K^{1/2}$. Then, $dN = 3p$, $N_2 \cong < 1, 3p >$, $N_p \cong < 6\delta, 2\delta p >$, and $N_3 \cong < 6, 2p >$. Let $u \in R(N)^*$ and w be another element in N so that $N = \mathbb{Z}[u, w]$. Then, since τ_u is an isometry of N, $Q(u)$ divides $2B(u, w)$. Since

$$N \cong \begin{pmatrix} Q(u) & B(u,w) \\ B(u,w) & Q(w) \end{pmatrix},$$

it must be that $3p = Q(u)Q(w) - B(u, w)^2$, and so $Q(u)$ divides $6p$.

By Gauss' Theory as described in [3, §14.4], since there are two distinct primes dividing $dN = 3p$, and $dN \equiv 1 \bmod 4$, there are four ambiguous classes of positive definite binary lattices with discriminant $3p$ when $p \equiv 3 \bmod 4$. Since the length of a vector in $R(N)^*$ divides $6p$, the four ambiguous classes are represented by the following Gram matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 3p \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 \\ 1 & \frac{3p+1}{2} \end{pmatrix}, \quad \begin{pmatrix} 3 & 0 \\ 0 & p \end{pmatrix}, \quad \begin{pmatrix} 6 & 3 \\ 3 & \frac{p+3}{2} \end{pmatrix}.$$

If N is represented by the first matrix, then K would represent 2, which is impossible. Over $\mathbb{Z}_3$, we can eliminate the third matrix since $N_3 \ncong < 3, p >$.

Suppose that $N \cong \begin{pmatrix} 6 & 3 \\ 3 & \frac{p+3}{2} \end{pmatrix}$. Then, $K \cong \begin{pmatrix} 12 & 6 \\ 6 & p+3 \end{pmatrix}$. Let $y' \in K$ such that $Q(y') = 12$. Then, the vector $\frac{v-2x+y'}{3}$ must be adjoined to M to obtain a lattice in $\mathcal{G}'$ isometric to L. However, $\frac{v-2x+y'}{3}$ has length 2, which contradicts the fact that $R(L) = \mathbf{A}_2$. Thus, if N is ambiguous, we must have $N \cong \begin{pmatrix} 2 & 1 \\ 1 & \frac{3p+1}{2} \end{pmatrix}$ and hence $K \cong \begin{pmatrix} 4 & 2 \\ 2 & 3p+1 \end{pmatrix}$. Over $\mathbb{Z}_2$,

$$\begin{pmatrix} 4 & 2 \\ 2 & 3p+1 \end{pmatrix} \cong \begin{cases} 2 < 5, 5 > & p \equiv 3 \bmod 8, \\ 2 < -1, 3 > & p \equiv -1 \bmod 8. \end{cases}$$

However, when $p \equiv -1 \bmod 8$, $K_2 \cong < 2, 6p > \cong 2 < 1, -3 >$, which is not isometric to $2 < -1, 3 >$ since their underlying quadratic spaces are not isometric over $\mathbb{Q}_2$. Thus, $p \equiv 3 \bmod 8$. Similarly, over $\mathbb{Z}_3$,

$$\begin{pmatrix} 4 & 2 \\ 2 & 3p+1 \end{pmatrix} \cong < 4, 3p > \cong < 1, 3p > .$$

Since $K_3 \cong < 3, p >$, we should have $S_3(\mathbb{Q}_3 K_3) = S_3([1, 3p])$. Then since $S_3(\mathbb{Q}_3 K_3) = -(p, 3)_3$ and $S_3([1, 3p]) = -1$, it must be that $(p, 3)_3 = 1$. In other words, $p \equiv 1 \bmod 3$. Thus, additionally we have $p \equiv 3 \bmod 8$ and $p \equiv 1 \bmod 3$ in this case.

The symmetry with respect to the vector of length 4 in K along with 1_K are the only elements of $O(K)$ that extend to an isometry of a lattice L in $\mathcal{G}'$ containing M. Because this vector is also primitive, we have $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1^2$ in this case. Consider $\langle -1_L, W(R_L^*) \rangle < O(L) < O(R_L) \times O(K)$. Then, since $\langle -1_L, W(R_L^*) \rangle$ has index 2 in $O(R_L) \times O(K)$ and $-1_K \notin O(L)$, it follows that $O(L) = \langle -1_L, W(R_L^*) \rangle$.

• Suppose that $R(L) = \mathbf{A}_1$ and let K denote the orthogonal complement of R_L in L. The sublattice $R_L \perp K$ has index 2 in L. Let v be the vector generating R_L and $\{x, y, z\} \subset K$ so that $\mathrm{Mat}(x, y, z) \equiv < -2, 2, -2p > \bmod 64$. Then, to obtain a lattice in $\mathcal{G}'$ containing $R_L \perp K$, we must adjoin $\frac{v+x}{2}$, $\frac{x+y}{2}$, or $\frac{x+z}{2}$. However, the lattices obtained by adjoining $\frac{x+y}{2}$ or $\frac{x+z}{2}$ to $R_L \perp K$ are decomposable. Thus, there is only one indecomposable lattice containing $R_L \perp K$ given by $(A_1 \perp K) + \mathbb{Z}[\frac{v+x}{2}]$. Further, this implies $\pm 1_K \in O(L)$.

Note that $\langle -1_L, W(R_L^*)\rangle < O(L) < O(R_L) \times O(K)$. If $O(K) = \{\pm 1_K\}$, then $R(L) = R(L)^*$ and $O(L) = O(R_L) \times \{\pm 1_K\} = \langle -1_L, W(R_L^*)\rangle$. Suppose $O(K) \neq \{\pm 1_K\}$. Then, since $dK^{1/2} = p$, $K^{1/2}$ is primal and does not represent 1. By [15, Cor. 4.5], $O(K^{1/2})$ is generated by symmetries with respect to the vectors of length 2 in $K^{1/2}$. Thus, by scaling, $O(K)$ is generated by symmetries with respect to vectors of length 4 in K. Therefore, if $O(K) \neq \{\pm 1_K\}$, K represents 4.

Suppose that $\mu_1(K) = \mu_2(K) = 4$. Then, $\mu_1(K^{1/2}) = \mu_2(K^{1/2}) = 2$ and either $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ or $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ is represented by $K^{1/2}$. First, suppose $K^{1/2}$ represents $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$. Then, by Minkowski reduction,

$$K^{1/2} \cong \begin{pmatrix} 2 & 0 & * \\ 0 & 2 & * \\ * & * & * \end{pmatrix}.$$

However, there are no entries satisfying the inequalities of Minkowski reduction such that $dK^{1/2} = p$. Thus, $K^{1/2}$ does not represent $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, so K does not represent $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$.

Now, suppose $K^{1/2}$ represents $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Over $\mathbb{Z}_2$, this implies that $\mathbb{A}$ is represented by $< -1, 1, -p >$, but this is impossible since $< -1, 1, -p >$ is isotropic.

Thus, $K^{1/2}$ does not represent $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, so K does not represent $\begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}$. Therefore, both $\mu_1(K)$ and $\mu_2(K)$ cannot equal 4.

Suppose that $\mu_1(K) = 4$ and $\mu_2(K) = 6$. Then, $\mu_1(K^{1/2}) = 2$ and $\mu_2(K^{1/2}) = 3$ and either $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ or $\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$ is represented by $K^{1/2}$. Suppose $K^{1/2}$ represents $\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$. Then, over $\mathbb{Z}_2$,

$$< -1, 1, -p > \cong \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \perp < 5p > \cong < 3, -1 > \perp < 5p > .$$

However, $[-1, 1, -p]$ and $[3, -1] \perp [5p]$ are not isometric over $\mathbb{Q}_2$. Thus, $K^{1/2}$ does not represent $\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$, and so K does not represent $\begin{pmatrix} 4 & 2 \\ 2 & 6 \end{pmatrix}$. Now, suppose $K^{1/2}$ represents $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$. Then, by Minkowski reduction,

$$K^{1/2} \cong \begin{pmatrix} 2 & 0 & 1 \\ 0 & 3 & 1 \\ 1 & 1 & \frac{p+5}{6} \end{pmatrix}$$

where $p \equiv 1 \bmod 6$ and $p \equiv 3 \bmod 8$. Thus,

$$K \cong \begin{pmatrix} 4 & 0 & 2 \\ 0 & 6 & 2 \\ 2 & 2 & \frac{p+5}{3} \end{pmatrix}$$

where $p \equiv 1 \bmod 3$ and $p \equiv 3 \bmod 8$.

Let $\{\alpha, \beta, \gamma\}$ be a basis of K which yields the above Gram matrix. Then, there are three lattices in $\mathcal{G}'$ containing $R_L \perp K$, which are $L_0 = (R_L \perp K) + \mathbb{Z}[\frac{v+\beta}{2}]$, $L_1 = (R_L \perp K) + \mathbb{Z}[\frac{\gamma}{2}]$, and $L_2 = (R_L \perp K) + \mathbb{Z}[\frac{\alpha+\gamma}{2}]$. Notice, however, that L_1 and L_2 are decomposable, so the indecomposable lattice L containing $R_L \perp K$ is given by $L = L_0 = (R_L \perp K) + \mathbb{Z}[\frac{v+\beta}{2}]$. But, $Q(\frac{v+\beta}{2}) = 2$ and $\{v, \frac{v+\beta}{2}\}$ generates A_2. Thus, if $\mu_1(K) = 4$, then $\mu_2(K) > 6$.

Suppose that $\mu_1(K) = 4$ and e is a vector of length 4 in K. Let N denote the orthogonal complement of $\mathbb{Z}[e]$ in K. Then, since $4 \cdot dN = 8p[K : \mathbb{Z}[e] \perp N]^2$ and $dN | 4 \cdot 8p$, dN is either $2p$, $8p$, or $32p$. Note that $dN \neq 2p$ since N is a binary even lattice. Over $\mathbb{Z}_2$, $< 4 > \perp N_2$ is represented by $< -2, 2, -2p >$. Then, because $(\frac{dN}{4}) | (2 \cdot p)$, we have $dN = 8p$. Now, $N_2 \cong < 2\epsilon, 4\epsilon p >$ or $< 4\epsilon, 2\epsilon p >$ for some $\epsilon \in \{1, 3, 5, -1\}$. If $N_2 \cong < 2\epsilon, 4\epsilon p >$, then $\epsilon = 1$ or -1 when $p \equiv -1 \mod 8$ and $\epsilon = 3$ or 5 when $p \equiv 3 \mod 8$ so that K_2 and $\mathbb{Z}_2[e] \perp N_2$ are isometric over $\mathbb{Z}_2$. Similarly, if $N_2 \cong < 4\epsilon, 2\epsilon p >$, then $\epsilon = 1$ or -1 when $p \equiv -1$ or $3 \mod 8$. However, these lattices are isometric over $\mathbb{Z}_2$ no matter what the ϵ is. Thus, we can simply set $\epsilon = -1$ and $N_2 \cong < -4, -2p >$. Since $\mathbb{Z}_p[e]$ splits K_p, $N_p \cong < 2\delta, \delta p >$.

Consider the tower of lattices

$$\begin{array}{c} L \\ | \\ \mathbb{Z}[v] \perp K \\ | \\ \mathbb{Z}[v] \perp \mathbb{Z}[e] \perp N \end{array}$$

Let $\{f, g\}$ be vectors in K such that $\mathrm{Mat}(f, g) \equiv < -4, -2p > \mod 64$. Then, $\mathbb{Z}[v] \perp \mathbb{Z}[e] \perp N$ has index 2 in $\mathbb{Z}[v] \perp K$ and

$$\mathbb{Z}[v] \perp K = (\mathbb{Z}[v] \perp \mathbb{Z}[e] \perp N) + \mathbb{Z}\left[\frac{e+f}{2}\right].$$

Let $y' = \frac{e+f}{2}$. Then, $\{v, e, y', g\} \subset \mathbb{Z}[v] \perp K$ has $\mathrm{Mat}(v, e, y', g) \equiv < 2 > \perp \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \perp < -2p > \mod 64$. Now, $\mathbb{Z}[v] \perp K$ has index 2 in L, and since the only vectors of conductor 2 with respect to $\mathbb{Z}[v] \perp K$ representing an even integer are $\frac{e}{2}$, $\frac{y'}{2}$, and $\frac{v+e+y'+g}{2}$, L is equal to one of $(\mathbb{Z}[v] \perp K)+\mathbb{Z}[\frac{e}{2}]$, $(\mathbb{Z}[v] \perp K)+\mathbb{Z}[\frac{y'}{2}]$, or $(\mathbb{Z}[v] \perp K) + \mathbb{Z}[\frac{v+e+y'+g}{2}]$. However, the first two lattices are decomposable. Thus, the indecomposable lattice L containing $\mathbb{Z}[v] \perp \mathbb{Z}[e] \perp N$ is $L = (\mathbb{Z}[v] \perp \mathbb{Z}[e] \perp N) + \mathbb{Z}[y', \frac{v+e+y'+g}{2}]$.

Consider τ_e on L. Then, $\tau_e(\frac{v+e+y'+g}{2}) = \frac{v+e+y'+g}{2} - \frac{3}{2}e$, which is not in L since $\frac{e}{2}$ is not in L. Thus, e is not in $R(L)^*$ and $R(L) = R(L)^*$. Therefore, since $\langle -1_L, W(R_L^*)\rangle < O(L) < O(R_L) \times O(K)$ and the symmetry with respect to e in $O(K)$ does not extend to an isometry of L, $O(L) = \langle -1_L, W(R_L^*)\rangle$ since $\langle -1_L, W(R_L^*)\rangle$ has index 2 in $O(R_L) \times O(K)$.

• Suppose that $R(L) = 2\mathbf{A}_1$ and let K denote the orthogonal complement of R_L in L. Then, by Lemma 14, $dK = 4p$ and $R_L \perp K$ has index 2 in L. Let $\{v, x\}$ be orthogonal vectors of length 2 in $R(L)$ such that $R_L \cong \mathbb{Z}[v, x]$ and let $\{y, z\} \subset K$ such that $\mathrm{Mat}(y, z) \equiv \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \mod 64$. Then, a lattice L in $\mathcal{G}'$ containing $R_L \perp K$ is obtained by adjoining $\frac{y}{2}$, $\frac{z}{2}$, or $\frac{v+x+y+z}{2}$ to $R_L \perp K$, but only the lattice $(R_L \perp K) + \mathbb{Z}[\frac{v+x+y+z}{2}]$ is indecomposable. Thus, $L = (R_L \perp K) + \mathbb{Z}[\frac{v+x+y+z}{2}]$ is the only lattice in $\mathcal{G}'$ containing $R_L \perp K$. Notice that the isometries with respect to $\pm(v \pm x)$ will be in $O(L)$. Thus, $\mathbf{C}_2 \subset R(L)^*$.

Suppose $O(K) \neq \{\pm 1_K\}$. Then, $dK = 4p$ implies $dK^{1/2} = p$. Let u be an element of $R(K^{1/2})^*$ and w be another element in $K^{1/2}$ so that $K^{1/2} = \mathbb{Z}[u, w]$. Since τ_u is an isometry of $K^{1/2}$, it must be that $Q(u)$ divides $2B(u, w)$. Because

$$K^{1/2} \cong \begin{pmatrix} Q(u) & B(u,w) \\ B(u,w) & Q(w) \end{pmatrix},$$

it must be that $p = Q(u)Q(w) - B(u, w)^2$, and so $Q(u)$ divides $2p$.

According to Gauss' Theory as described in [3, §14.4], since there is one odd prime dividing $dK^{1/2} = p$, and $dK^{1/2} \equiv 3 \bmod 4$, there are two ambiguous classes of positive definite binary lattices with discriminant p where $p \equiv 3 \bmod 4$. Since the length of a vector in $R(K^{1/2})^*$ divides $2p$, the two ambiguous classes are represented by the following Gram matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}.$$

If $K^{1/2}$ were represented by the first of these matrices, then K would represent 2, which is impossible.

Suppose $K^{1/2} \cong \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}$. Then, $K \cong \begin{pmatrix} 4 & 2 \\ 2 & p+1 \end{pmatrix}$. Let $y' \in K$ such that $Q(y') = 4$. Then, the vector $\frac{v+x+y'}{2}$ can be adjoined to $R_L \perp K$ to obtain a lattice in $\mathcal{G}'$. But L is the only lattice in $\mathcal{G}'$ containing $R_L \perp K$ and $\frac{v+x+y'}{2}$ has length 2. This contradicts $R(L) = 2\mathbf{A}_1$. Thus, $K \not\cong \begin{pmatrix} 4 & 2 \\ 2 & p+1 \end{pmatrix}$ and so K is unambiguous.

Now, $O(K) = \{\pm 1_K\}$. Therefore, since $O(L) < O(R_L) \times O(K) = O(2A_1) \times \{\pm 1_K\} = O(C_2) \times \{\pm 1_K\}$ and both $\mathbf{C}_2 \subset R(L)^*$ and $-1_K \in O(L)$, $O(L) = O(C_2) \times \{\pm - 1_K\} = \langle -1_L, W(R_L^*)\rangle$. $\square$

Using Lemmas 17 and 18, we determine $|O(L)|$ corresponding to the scaled root system of a lattice L in $\mathcal{G}'$.

$R(L)^*$	$\mathbf{A}_1^2$	$\mathbf{A}_1$	$2\mathbf{A}_1$	$\mathbf{C}_2$	$\mathbf{A}_2$	$\mathbf{A}_2 \perp \mathbf{A}_1$	$\mathbf{A}_2 \perp \mathbf{A}_1^{(2)}$	$\mathbf{C}_3 \perp \mathbf{A}_1^{2p}$	$\mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_1^p$
$\lvert O(L)\rvert$	4	4	8	16	12	24	24	96	32

Lemma 19. *There is only one class in $\mathcal{G}'$ with $R(L)^* = \boldsymbol{C}_3 \perp \boldsymbol{A}_1^{2p}$.*

Proof. Let L be a lattice in $\mathcal{G}'$ such that $R(L)^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$. Let $z \in R(L)^*$ with $Q(z) = 4p$. Then, the sublattice $M = R_L^* = C_3 \perp \mathbb{Z}[z]$ has index 2 in L. Let $\{v, x, y\} \subset C_3$ such that $\mathrm{Mat}(v, x, y) \equiv \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp < 12 >$ mod 64. Then, to obtain a lattice in $\mathcal{G}'$ containing M, we must adjoin $\frac{y \pm z}{2}$ to M since these are the only vectors of conductor 2 with respect to M representing an even integer. Then, L is equal to one of $M + \mathbb{Z}[\frac{y+z}{2}]$ or $M + \mathbb{Z}[\frac{y-z}{2}]$, but they are the same lattice. Thus, there is only one class in $\mathcal{G}'$ with $R(L)^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$.

□

Lemma 20. *There is only one class in $\mathcal{G}'$ with scaled root system $\boldsymbol{A}_2 \perp \boldsymbol{A}_1^2$*

Proof. Let L be a lattice $\mathcal{G}'$ such that $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1^2$ and let K denote the orthogonal complement of R_L^* in L. Then, since $12 \cdot dK = 4p[L : R_L^* \perp K]^2$ and $dK | (12 \cdot 4p)$, dK is either $3p, 12p$, or $48p$. Notice that $dK \neq 3p$ since N is an even rank 1 lattice.

By Lemma 15, L is indecomposable, and by Lemma 13, $< 6, 4 > \perp K_2$ is represented by $< -2, 2, -2p >$. Since $< 6 >$ splits $< -2, 2, -2p >$, we have $< -2, 2, -2p > \cong < 6 > \perp N$ where $dN = 12p$. Then, K_2 is the orthogonal complement of $< 4 >$ in N. Through direct verification, $dK_2 = 12p$ and so $dK = 12p$.

Now, L contains the full sublattice $M = R_L^* \perp \mathbb{Z}[z]$ where z is a vector of length $12p$ and $[L : M] = 6$. Let $\{v, x, y\}$ be a basis for R_L^* such that $\mathrm{Mat}(x, y, z) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp < 4 >$. Then, by considering the localizations at 2 and 3, L is either $M + \mathbb{Z}[\frac{y+z}{2}, \frac{v-2x+z}{3}]$ or $M + \mathbb{Z}[\frac{y+z}{2}, \frac{v-2x-z}{3}]$. However, these two lattices are isometric via τ_z. Thus, there is only one class in $\mathcal{G}'$ with this scaled root system.

□

Lemma 21. *There is precisely one class in $\mathcal{G}'$ with scaled root system $\boldsymbol{A}_2 \perp \boldsymbol{A}_1$.*

Proof. Let L be a lattice in $\mathcal{G}'$ such that $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1$ and let K denote the orthogonal complement of R_L^* in L. Let $\{v, x, y\}$ be a basis for R_L^* such that $\mathrm{Mat}(v, x, y) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp < 2 >$ and let z be a vector of length $6p$ in L such that $K = \mathbb{Z}[z]$. Then, there are two lattices in $\mathcal{G}'$ containing $R_L^* \perp K$, and they are $(R_L^* \perp K) + \mathbb{Z}[\frac{v-2x+z}{3}]$ and $(R_L^* \perp K) + \mathbb{Z}[\frac{v-2x-z}{3}]$. These two lattices are isometric via τ_z. Thus, there is one class in $\mathcal{G}'$ with $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1$. $\square$

4.3 Linear Independence of Degree Two Theta Series

Let $\mathscr{L}'$ be a complete set of class representatives in $\mathcal{G}'$ with nontrivial orthogonal groups and associate to each $L \in \mathscr{L}'$ its degree 2 theta series, denoted θ_L. By Lemmas 17 and 18, the scaled root system of an $L \in \mathscr{L}'$ is one of $\mathbf{A}_1$, $2\mathbf{A}_1$, $\mathbf{C}_2$, $\mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_1^p$, or $\mathbf{A}_2 \perp \mathbf{A}_1$ if L is decomposable and one of $\mathbf{A}_1^2$, $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{C}_2$, $\mathbf{A}_2 \perp \mathbf{A}_1^2$, or $\mathbf{C}_3 \perp \mathbf{A}_1^{2p}$ if L is indecomposable. Further, $O(L) = \langle -1_L, W(R_L^*)\rangle$ for any $L \in \mathscr{L}'$. In this section, we prove that the θ_L are linearly independent over $\mathbb{Z}$.

We use the same strategy as in Section 3.3. Suppose that there is a linear relation $\sum_{L \in \mathscr{L}'} c_L \theta_L = 0$ such that the greatest common divisor of the c_L is 1. For a fixed L, we will construct a binary sublattice J and let $a_{JL'}$ denote the number of distinct isometric embeddings of J into L' for all $L' \in \mathscr{L}'$. Then, for each such J, we have the equality $\sum_{L' \in \mathscr{L}'} c_{L'} a_{JL'} = 0$. Using these equalities, we will show that $c_L \equiv 0 \bmod 2$ for all $L \in \mathscr{L}'$, contradicting our assumption that the gcd of the $c_{L'}$ is 1.

Theorem 2. *The degree 2 theta series of the classes in $\mathcal{G}'$ with nontrivial orthogonal groups are linearly independent over $\mathbb{Z}$.*

Proof. We proceed with cases corresponding the possible scaled root systems of a lattice L in $\mathcal{G}'$. For $L \in \mathscr{L}'$ with $R(L)^* = \mathbf{A}_1$, we will use $\mathbf{A}_1(D)$ to denote that L is decomposable and $\mathbf{A}_1(I)$ when L is indecomposable. In the same vein, we use the notation $\mathbf{C}_2(D)$ and $\mathbf{C}_2(I)$ for the lattices with scaled root system $\mathbf{C}_2$. In all cases, K is the orthogonal complement of R_L^* in L.

• Fix $L \in \mathscr{L}'$ such that $R(L)^* = \mathbf{A}_1(D)$. Let v be a vector in $R(L)^*$ generating R_L^*. Then, K is an even, ternary lattice with $dK = 2p$, $K_2 \cong \mathbb{H} \perp < -2p > \cong \mathbb{A} \perp < 6p >$, and $K_p \cong < 1, 2\delta, \delta p >$. By [13, Lemma 1.6], K contains a sublattice J such that $J_2 \cong \mathbb{P}$, $J_p \cong < 1, \delta >$, and $dJ = q$ for some large prime q. Suppose $\mathbb{P} = \mathbb{H}$ when $p \equiv 3 \bmod 8$ and $\mathbb{P} = \mathbb{A}$ when $p \equiv -1 \bmod 8$.

Let N be the orthogonal complement of $R_L^* \perp J$ in L. Then, N is a rank 1 lattice generated by a vector z of length $2pq$. Let $M = R_L^* \perp J \perp N$. Then, M has index q in L. Let $J_q \cong < \alpha, \alpha q >$ in a basis $\{e, f\}$ with $\alpha \in \mathbb{Z}_q^\times$. Then, L_q is equal to one of $M_q + \mathbb{Z}_q[\frac{f+az}{q}]$ or $M_q + \mathbb{Z}_q[\frac{f-az}{q}]$ where $a \in \mathbb{Z}_q$ such that $\frac{1}{q}(Q(f) + a^2 Q(z)) \equiv 0 \bmod q$. These lattices are isometric via τ_z. Thus, there are exactly two lattices in $\mathcal{G}'$ containing M, and they are $M + \mathbb{Z}[\frac{f'+az}{q}]$ and $M + \mathbb{Z}[\frac{f'-az}{q}]$, where $f' \in J$ which locally approximates f.

Suppose $\phi : J \to L$ is an isometric embedding such that $\phi(J)$ is orthogonal to R_L^*. Then, there exists some $\sigma \in O(\mathbb{Q}L)$ such that $\sigma|_J = \phi$. Further, by local consideration, $\sigma^{-1}(L)$ must contain $M = R_L^* \perp J \perp N$. Thus, $\sigma^{-1}(L) = L$ or $\sigma^{-1}(L) = \tau_z(L)$. Since $\sigma|_J = \phi$ and $(\sigma \circ \tau_z)|_J = \phi$, ϕ is in the orbit of the inclusion map $\iota : J \hookrightarrow L$ under the action of $O(L) = \langle -1_L, \tau_v \rangle$. Thus, this orbit has 2 embeddings; namely, ι and $-\iota$. By Lemma 10, the number of embeddings

$\phi : J \to L$ with $\phi(J)$ not orthogonal to R_L^* is equivalent to $0 \mod 4$. Therefore, $a_{JL} \equiv 2 \mod 4$.

Let $\phi : J \to L'$ be an isometric embedding such that $L \neq L'$. Suppose that $\min(L') = 2$ and $\phi(J)$ is orthogonal to a vector e of length 2 in L'. First, suppose L' is indecomposable. Then, by Lemma 13, over $\mathbb{Z}_2$, $< 2 > \perp \mathbb{P}$ is represented by $< -2, 2, -2p >$, which is impossible. Thus, if L' is indecomposable, $\phi(J)$ cannot be orthogonal to any minimal vector of L'. We can apply Lemma 10 to conclude that $a_{JL'} \equiv 0 \mod 4$ for all indecomposable $L' \neq L$ with minimum 2.

Now, suppose that L' is decomposable. Then, ϕ can be extended to an embedding ϕ' of $R_L^* \perp J$ into L' such that $\phi'(v) = e$ and $\phi'|_J = \phi$. By considering the discriminant, the orthogonal complement of $\phi(R_L^* \perp J)$ in L' is isometric to N. Thus, ϕ' can be extended to an isometry Φ of $\mathbb{Q}L$, and $\Phi^{-1}(L')$ is a lattice in $\mathcal{G}'$ containing M. Since we have shown that there is only one class of lattices in $\mathcal{G}'$ containing M, it must be that $\Phi(L) \cong L'$ and $L = L'$. Therefore, $\phi(J)$ cannot be orthogonal to a vector of length 2 in a decomposable $L' \neq L$. By Lemma 10, $a_{JL'} \equiv 0 \mod 4$ for all decomposable $L' \neq L$.

Suppose now that $\min(L') = 4$ and $\phi(J)$ is orthogonal to a vector f of length 4 in $R(L')^*$. Over $\mathbb{Z}_2$, the orthogonal complement of $\mathbb{Z}[f]$, denoted K', has structure

$$K'_2 \cong \begin{cases} \mathbb{H} \perp < -4p > & p \equiv -1 \bmod 8, \\ \mathbb{A} \perp < 12p > & p \equiv 3 \bmod 8, \end{cases}$$

by the proof of Proposition 1. Therefore, over $\mathbb{Z}_2$, $< 4 > \perp \mathbb{H}$ is represented by $< 4 > \perp \mathbb{A}$ when $p \equiv 3 \mod 8$ and $< 4 > \perp \mathbb{A}$ is represented by $< 4 > \perp \mathbb{H}$ when $p \equiv -1 \mod 8$. Both are impossible and hence $\phi(J)$ cannot be orthogonal to a vector of length 4 in $R(L')^*$. We can apply Lemma 10 to conclude that $a_{JL'} \equiv 0 \mod 4$ for all indecomposable $L' \neq L$ with minimum 4.

Consider $\sum_{L' \in \mathscr{L}'} c_{L'} a_{JL'} \equiv 0 \mod 4$. From above, $a_{JL'} \equiv 0 \mod 4$ for all $L' \neq L$. Therefore, $c_L a_{JL} \equiv 0 \mod 4$, and since $a_{JL} \equiv 2 \mod 4$, $c_L \equiv 0 \mod 2$.

• Fix $L \in \mathscr{L}'$ with $R(L)^* = \mathbf{A}_1(I)$. Let v be a vector in $R(L)^*$ generating $R(L)^*$ and let $\{x, y, z\} \subset K$ such that $\mathrm{Mat}(x, y, z) \equiv < -2, 2, -2p > \mod 64$. A lattice in $\mathcal{G}'$ containing $R_L^* \perp K$ will be obtained by adjoining one of $\frac{v+x}{2}$, $\frac{x+y}{2}$, or $\frac{x+z}{2}$ to $R_L^* \perp K$. Note that only the first of these lattices is indecomposable. We will proceed by using the dual of L in this case. Let $\mathcal{G}'^{\#}$ and $\mathscr{L}'^{\#}$ be the sets $\{L^{\#} : L \in \mathcal{G}'\}$ and $\{L^{\#} : L \in \mathscr{L}'\}$ respectively.

Note that $L_2^{\#} \cong \mathbb{H} \perp < \frac{1}{2}, \frac{-p}{2} > \cong \mathbb{A} \perp < \frac{1}{2}, \frac{3p}{2} >$. Let $\bar{L} = (R_L^* \perp K) + \mathbb{Z}[\frac{v+x}{2}]$. Then, $\{v, \frac{v+x}{2}, y, z\}$ is a basis for $\bar{L}_2$ where $\mathrm{Mat}(v, \frac{v+x}{2}) \cong \mathbb{H}$ and $\mathrm{Mat}(y, z) \cong < 2, -2p >$. So, $\{v, \frac{v+x}{2}, \frac{y}{2}, \frac{z}{2}\}$ as a basis for $\bar{L}_2^{\#}$ and $\mathrm{Mat}(\frac{y}{2}, \frac{z}{2}) \cong < \frac{1}{2}, \frac{-p}{2} >$. Thus, for a lattice in $\mathcal{G}'^{\#}$ with scaled root system $\mathbf{A}_1(I)$, the localization at 2 contains a component isometric to $< \frac{1}{2}, \frac{-p}{2} >$.

Let K be the orthogonal complement of R_L^* in $L^{\#}$ and J a binary sublattice of K such that $J_2 \cong < \frac{1}{2}, \frac{-p}{2} >$, $J_p \cong < 2, \delta >$, and $dJ = \frac{q}{4}$ for some large prime q. Further, let $\{x, y\} \subset J$ such that

$$\mathrm{Mat}(x, y) \equiv \begin{cases} < \frac{-1}{2}, \frac{p}{2} > & \mod 64, \\ < 2, \delta > & \mod p^3. \end{cases}$$

Let N be the orthogonal complement of $R_L^* \perp J$ in $L^{\#}$. Then N is a rank 1 lattice generated by a vector z of length $\frac{2q}{p}$ and $M = R_L^* \perp J \perp N$ has index $2q$ in $L^{\#}$. Note that a lattice in $\mathcal{G}'^{\#}$ containing $R_L^* \perp J$ must also contain M. Consider the localization at 2. Then, $L_2^{\#} = M_2 + \mathbb{Z}_2[\frac{v+z}{2}] = M_2 + \mathbb{Z}_2[\frac{v-z}{2}]$ since J_2 splits $L_2^{\#}$. Note that τ_z is an isometry of $L_2^{\#}$. Since L_q is unimodular, $L_q^{\#} = L_q$. Suppose $J_q \cong < \alpha, \alpha q >$ in a basis $\{e, f\}$ with $\alpha \in \mathbb{Z}_q^{\times}$. Then, $L_q = M_q + \mathbb{Z}_q[\frac{f+az}{q}]$

or $M_q + \mathbb{Z}_q[\frac{f-az}{q}]$ where $a \in \mathbb{Z}_q$ such that $\frac{1}{q}(Q(f) + a^2Q(z)) \equiv 0 \bmod q$. These lattices are isometric to each other via τ_z. Now, there are two lattices in $\mathcal{G}'^{\#}$ containing M, and they are isometric via τ_z.

Suppose $\phi : J \to L^{\#}$ is an isometric embedding such that $\phi(J)$ is orthogonal to R_L^*. Then, there exists some $\sigma \in O(\mathbb{Q}L^{\#}) = O(\mathbb{Q}L)$ such that $\sigma|_J = \phi$. Further, $\sigma^{-1}(L^{\#})$ contains M. Thus, $\sigma^{-1}(L^{\#}) = L^{\#}$ or $\sigma^{-1}(L^{\#}) = \tau_z(L^{\#})$ and either σ or $\sigma \circ \tau_z$ is an isometry of L. Since $\sigma|_J = \phi$ and $\tau_z \circ \sigma|_J = \phi$, ϕ is in the orbit of the inclusion map under the action of $O(L)$. Thus, we regard ϕ as the inclusion map in this situation and $a_{JL^{\#}} \equiv 2 \bmod 4$.

Now, let $\phi : J \to L'^{\#}$ be an isometric embedding such that $L \neq L'$. Suppose that $\min(L') = 2$ and $\phi(J)$ is orthogonal to a vector e of length 2 in L'. Then, ϕ can be extended to an isometry ϕ' such that $\phi'(v) = e$ and $\phi'|_J = \phi$. Further, ϕ' can be extended to an isometry Φ of $\mathbb{Q}L^{\#} = \mathbb{Q}L$, and so $\Phi^{-1}(L'^{\#})$ contains M. However, since there is only one class in $\mathcal{G}'^{\#}$ containing M, it must be that $\Phi(L^{\#}) = L'^{\#}$. Therefore, $L^{\#} = L'^{\#}$, which is impossible. Thus, $\phi(J)$ cannot be orthogonal to any minimal vector e in L'. Therefore, we apply Lemma 10 to conclude $a_{JL'^{\#}} \equiv 0 \bmod 4$ for all $L \neq L'$ when L' has minimum 2.

Suppose now that $\min(L') = 4$ and f is a vector of length 4 in $R(L')^*$. Recall that the orthogonal complement K' of $\mathbb{Z}[f]$ in L' satisfies $K'_p \cong < 1, \delta, \delta p >$ and

$$K'_2 \cong \begin{cases} \mathbb{H} \perp < -4p > & p \equiv -1 \bmod 8, \\ \mathbb{A} \perp < 12p > & p \equiv 3 \bmod 8. \end{cases}$$

Let $M = \mathbb{Z}[f] \perp K'$ and let $\{\alpha, \beta, \gamma\} \subset K'$ such that $\mathrm{Mat}(\alpha, \beta, \gamma) \equiv \mathbb{H} \perp < -4p > \bmod 64$ when $p \equiv -1 \bmod 8$ and $\mathrm{Mat}(\alpha, \beta, \gamma) \equiv \mathbb{A} \perp < 12p > \bmod 64$ when $p \equiv 3 \bmod 8$. Then, L'_2 will equal $M_2 + \mathbb{Z}_2[\frac{f+\gamma}{2}]$ in both cases, and $\{f, \frac{f+\gamma}{2}, \alpha, \beta\}$ is a basis for L'_2. Thus, $\{\frac{f}{2}, \frac{f+\gamma}{4}, \alpha, \beta\}$ is a basis for $L_2'^{\#}$ and the orthogonal complement of $\mathbb{Z}_2[f]$ in $L_2'^{\#}$ is $\mathrm{Mat}(\alpha, \beta, \frac{\gamma}{2}) \cong \mathbb{H} \perp < -p >$. Therefore, over $\mathbb{Z}_2$, if $\phi(J)$ were orthogonal to a vector of length 4 in $R(L')^*$, $< \frac{1}{2}, \frac{-p}{2} >$ would be represented by $\mathbb{H} \perp < -p >$ or $< \frac{1}{2}, \frac{-p}{2} >$ would be represented by $\mathbb{A} \perp < 3p >$, both of which are impossible. Therefore, $\phi(J)$ cannot be orthogonal to any vector of length 4 in $R(L')^*$. By Lemma 10, $a_{JL'^\#} \equiv 0 \mod 4$.

From above, $a_{JL'^\#} \equiv 0 \mod 4$ for all $L \neq L'$. Thus, the summation implies $c_L a_{JL^\#} \equiv 0 \mod 4$. But $a_{JL^\#} \equiv 0 \mod 2$. Thus, $c_L \equiv 0 \mod 2$.

• Fix $L \in \mathscr{L}'$ such that $R(L)^* = \mathbf{A}_2$. Then, $R_L^* \perp K$ has index 3 in L. Let $\{v, x\}$ be a basis for R_L^* such that $R_L^* \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and $\{y, z\} \subset K$ such that $\mathrm{Mat}(y, z) \equiv < 3, p > \mod 27$ and $\mathrm{Mat}(y, z) \equiv < 2, 6p > \mod 64$.

Let J be the orthogonal complement of R_L^* in $L^\#$. Then, since $L_2 \cong \mathbb{A} \perp J_2^\#$, $L_2^\# \cong \mathbb{A} \perp J_2$ where $J_2 \cong < \frac{1}{2}, \frac{3p}{2} >$ and $R_L^* \cong \mathbb{A}$ splits $L_2^\#$. Further, since $L_p^\# \cong < 1, 1, \delta, \frac{\delta}{p} >$ and $(R_L^*)_p$ is unimodular, $J_p \cong < 3\delta, \frac{\delta}{p} >$. Finally, because L_3 is unimodular, we have $L_3^\# = L_3 \cong < 1, 1, 1, p >$, and since $\mathbb{Q}L_3 \cong \mathbb{Q}_3 R_L^* \perp \mathbb{Q}_3 J$, we have $J_3 \cong < 3, p >$.

Let N denote the orthogonal complement of $\mathbb{Z}[v]$ in $L^\#$. Then, $N = \mathbb{Z}[v - 2x] \perp J$ with $Q(v - 2x) = 6$. Note that $[L^\# : \mathbb{Z}[v] \perp N] = 6$. Over $\mathbb{Z}_2$, since J_2 splits $L_2^\#$, $L_2^\# = (\mathbb{Z}_2[v] \perp N_2) + \mathbb{Z}_2[v - x]$. Notice that $1_{R_L^*} \perp -1_J$ is an isometry of $L_2^\#$. Over $\mathbb{Z}_3$, $\mathbb{Z}_3[v] \perp N_3 \cong < 2, 6 > \perp < 3, p >$ has index 3 in L_3. Then, L_3 is either $(\mathbb{Z}_3[v] \perp N_3) + \mathbb{Z}_3[\frac{v-2x+y}{3}]$ or $(\mathbb{Z}_3[v] \perp N_3) + \mathbb{Z}_3[\frac{v-2x\pm y}{3}]$. However, these lattices are isometric via $1_{R_L^*} \perp -1_J$. Thus, $L^\#$ must be equal to $(\mathbb{Z}[v] \perp N) + \mathbb{Z}[v - x, \frac{v-2x+y}{3}]$ or $(\mathbb{Z}[v] \perp N) + \mathbb{Z}[v - x, \frac{v-2x-y}{3}]$, but these lattices are isometric via $1_{R_L^*} \perp -1_J$. Thus, there is one class in $\mathcal{G}'^\#$ containing $\mathbb{Z}[v] \perp N$.

Consider an isometric embedding $\phi : J \to L^\#$. Suppose that $\phi(J)$ is orthogonal to R_L^* in $L^\#$. Then, ϕ is an isometry of J and $\sigma := 1_{R_L^*} \perp \phi$ is an isometry of $R_L^* \perp J$. If $\sigma(L^\#) = L^\#$, then $1_{R_L^*} \perp \phi$ is in $O(L)$. Otherwise, $\sigma(L^\#) = (1_{R_L^*} \perp -1_J)(L^\#)$ by the previous argument and $(1_{R_L^*} \perp -1_J) \circ \sigma = (1_{R_L^*} \perp -\phi)$ is in $O(L)$. However, since $O(L) = \langle -1_L, W(R_L^*) \rangle$ and $1_{R_L^*} \perp \pm 1_J$ are the only elements of $O(L)$ that stabilize R_L^*, it must be that $\phi = \pm 1_J$. Thus, there are exactly two embeddings ϕ of J into $L^\#$ so that $\phi(J)$ is orthogonal to R_L^*.

Now, suppose that $\phi(J)$ is orthogonal to $\mathbb{Z}[v]$ in $L^\#$. Then, by the previous argument, $L^\#$ is equal to $(\mathbb{Z}[v] \perp N) + \mathbb{Z}[v - x, \frac{v-2x+y}{3}]$ or $(\mathbb{Z}[v] \perp N) + \mathbb{Z}[v - x, \frac{v-2x-y}{3}]$. However, $Q(v - x) = 2$ and $\{v, v - x\}$ generates A_2 in $L^\#$. Thus, if $\phi(J)$ is orthogonal to a vector of length 2 in R_L^*, $\phi(J)$ is orthogonal to R_L^*. By Lemma 10, the number of embeddings such that $\phi(J)$ is not orthogonal to any vector of length 2 in R_L^* is divisible by 4. This discussion implies that $a_{JL^\#} \equiv 2 \mod 4$.

Let $\phi : J \to L'^\#$ be an isometric embedding such that $L \neq L'$ and $\min(L') = 2$. Suppose that $\phi(J)$ is orthogonal to a vector e of length 2 in L'. Then, there exists an isometry Φ on $\mathbb{Q}L^\# = \mathbb{Q}L'^\#$ such that $\Phi(v) = e$ and $\Phi|_J = \phi$. Thus, $\Phi^{-1}(L'^\#)$ contains $\mathbb{Z}[v] \perp J$, and further, by comparing discriminants, $\Phi^{-1}(L'^\#)$ contains $\mathbb{Z}[v] \perp N$. However, since we have shown that there is only one class in $\mathcal{G}'^\#$ containing $\mathbb{Z}[v] \perp N$, it must be that $\Phi(L^\#) = L'^\#$. Therefore, $L = L'$, which is impossible. Thus, $\phi(J)$ cannot be orthogonal to any minimal vector e in L', and by Lemma 10, $a_{JL'^\#} \equiv 0 \mod 4$ for all $L \neq L'$ where L' has minimum 2.

Suppose now that L' has $\min(L') = 4$ and let f be a vector of length 4 in $R(L')^*$. Then, as in the argument in the case of $R(L)^* = \mathbf{A}_1(D)$, if $\phi(J)$ is orthogonal to f in $L'^\#$, over $\mathbb{Z}_2$, $< \frac{1}{2}, \frac{3p}{2} >$ is represented by $\mathbb{H} \perp < -p >$ or $< \frac{1}{2}, \frac{3p}{2} >$ is represented by $\mathbb{A} \perp < 3p >$, both of which are impossible. Therefore, by Lemma 10, $a_{JL'^{\#}} \equiv 0 \bmod 4$ in this case.

From the above discussion, $a_{JL'^{\#}} \equiv 0 \bmod 4$ for all $L \neq L'$. The summation implies $c_L a_{JL^{\#}} \equiv 0 \mod 4$, but $a_{JL^{\#}} \equiv 0 \mod 2$. Therefore, $c_L \equiv 0 \mod 2$.

- Fix $L \in \mathscr{L}'$ such that $R(L)^* = 2\mathbf{A}_1$. By Lemma 11, $p \equiv -1 \bmod 8$ and $K_2 \cong < -2, -2p >$. Let $\{v, x\}$ be a basis for R_L^* such that $\mathrm{Mat}(v, x) =< 2, 2 >$. Let $\{y, z\} \subset K$ such that $\mathrm{Mat}(y, z) \equiv < -2, -2p > \bmod 64$. A lattice in $\mathcal{G}'$ containing $R_L^* \perp K$ is obtained by adjoining $\frac{v+y}{2}$, $\frac{x+y}{2}$, or $\frac{y+z}{2}$ to $R_L^* \perp K$. Then, L is one of $(R_L^* \perp K) + \mathbb{Z}[\frac{v+y}{2}]$, $(R_L^* \perp K) + \mathbb{Z}[\frac{x+y}{2}]$, or $(R_L^* \perp K) + \mathbb{Z}[\frac{y+z}{2}]$. Notice the first two of these lattices are isometric via the the map that sends v to x. Further, since R_L^* splits the third lattice, the scaled root system for this lattice would be $\mathbf{C}_2(D)$.

Let J be the orthogonal complement of R_L^* in $L^{\#}$. We first determine the local structure of J at 2 and p respectively. Note that $K \subset J$ and $[K^{\#} : K] = 4p$. Further, $J \subset K^{\#}$. Over $\mathbb{Z}_p$, since $L_p^{\#} \cong < 1, 1, \delta, \frac{\delta}{p} >$ and $(R_L^*)_p$ is unimodular, $J_p \cong < \delta, \frac{\delta}{p} >$. Thus, $J_p = K_p^{\#}$ since $[J_p : K_p] = p$ and $[K_p^{\#} : K_p] = p$.

Now, $[J : K]$ is equal to $1, 2$ or 4. Consider the localization at 2. Note that $K_2^{\#}$ is generated by $\{\frac{y}{2}, \frac{z}{2}\}$. Without loss of generality, let $L = (R_L^* \perp K) + \mathbb{Z}[\frac{v+y}{2}]$. Then, $B(\frac{z}{2}, L) \subset \mathbb{Z}$ and $\frac{z}{2} \in J_2 \backslash K_2$ since $\frac{z}{2}$ is orthogonal to R_L^* and has conductor 2. Therefore, the index cannot be 1. Now, $B(\frac{y}{2}, L) \not\subset \mathbb{Z}$ and so $\frac{y}{2} \in K_2^{\#} \backslash L_2^{\#}$, which implies $[K_2^{\#} : J_2]$ cannot be 1. Thus, $[J_2 : K_2] = 2$, and so $[J : K] = 2p$, which implies $[L^{\#} : R_L^* \perp J] = 4$. So, $dJ = \frac{1}{p}$. Finally, since $dJ_2 = p$ and by local consideration, $J_2 \cong < -2, \frac{-p}{2} >$.

Let $M = R_L^* \perp J$ and note that since $L^{\#}/M$ is an elementary 2-group, we must adjoin two vectors of conductor 2 to M to obtain a lattice in $\mathcal{G}'^{\#}$ containing M. Let $\{\alpha, \beta\} \subset J$ such that $\mathrm{Mat}(\alpha, \beta) \equiv < -2, \frac{-p}{2} > \bmod 64$.

Then, $L^{\#}$ is obtained by adjoining two of the vectors in the set $\{\frac{v+x}{2}, \frac{v+\alpha}{2}, \frac{x+\alpha}{2}\}$ to M. However, adjoining any two of these vectors to M will produce a lattice containing the third vector. Thus, there is precisely one lattice in $\mathcal{G}'^{\#}$ containing M.

Let $\phi : J \to L^{\#}$ be an isometric embedding. We consider three cases. First, suppose that $\phi(J)$ is orthogonal to R_L^*. Then, $\phi(J) = J$ and if $\sigma := 1_{R_L^*} \perp \phi$, then $\sigma(L^{\#}) = L^{\#}$ since there is only one lattice in $\mathcal{G}'^{\#}$ containing M. Thus, $\sigma \in O(L^{\#}) = O(L)$. Because $O(L) = O(R_L^*) \times \{\pm 1_J\}$, we must have that $\phi = \pm 1_J$. Therefore, there are precisely two embeddings of J into $L^{\#}$ such that $\phi(J)$ is orthogonal to R_L^*.

Now, suppose $\phi(J)$ is not orthogonal to $\mathbb{Z}[v]$ in $L^{\#}$. Then, by Lemma 10, the number of distinct embeddings with this property is divisible by 4. Finally, suppose that $\phi(J)$ is orthogonal to $\mathbb{Z}[v]$ in $L^{\#}$ but is not orthogonal to $\mathbb{Z}[x]$. Then, the set $\{\pm\tau_x, \pm 1_L\}$ acts on the set of embeddings of this type since v and x are orthogonal. Thus, the size of this set is also divisible by 4, and we can conclude that $a_{JL^{\#}} \equiv 2 \bmod 4$.

Let $\phi : J \to L'^{\#}$ be an isometric embedding such that $L \neq L'$ and $\min(L') = 2$. Suppose that $\phi(J)$ is orthogonal to a vector e of length 2 in L'. Then, ϕ can be extended to an isometry Φ on $\mathbb{Q}L'$ such that $\Phi(v) = e$ and $\Phi|_J = \phi$. Note that if $L'^{\#}$ contains $\mathbb{Z}[e] \perp \phi(J)$, then by comparing discriminants, $L'^{\#}$ must contain an isometric copy of M. Thus, $\Phi^{-1}(L'^{\#})$ contains M. However, since we have shown that there is only one lattice in $\mathcal{G}'^{\#}$ containing M, it must be that $\Phi(L^{\#}) \cong L'^{\#}$. Then, $L = L'$, but this is impossible. Therefore, $\phi(J)$ cannot be orthogonal to any minimal vector e in L'. By Lemma 10, $a_{JL'^{\#}} \equiv 0 \bmod 4$ for all $L \neq L'$ where L' has minimum 2.

Suppose now that L' has $\min(L') = 4$ and let f be a vector of this length in $R(L')^*$. Then, if $\phi(J)$ is orthogonal to $\mathbb{Z}[f]$ in $L'^{\#}$, over $\mathbb{Z}_2$, $< -2, \frac{-p}{2} >$ is represented by $\mathbb{H} \perp < -p >$ or $< -2, \frac{-p}{2} >$ is represented by $\mathbb{A} \perp < 3p >$, both of which are impossible. Therefore, $\phi(J)$ cannot be orthogonal to a vector of length 4 in $R(L')^*$ and by Lemma 10, $a_{JL'^{\#}} \equiv 0 \bmod 4$ in this case.

From above, $a_{JL'^{\#}} \equiv 0 \bmod 4$ for all $L \neq L'$. Thus, the summation implies $c_L a_{JL^{\#}} \equiv 0 \mod 4$. But $a_{JL^{\#}} \equiv 0 \mod 2$, and so $c_L \equiv 0 \mod 2$.

• Fix $L \in \mathscr{L}'$ such that $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1^2$. In this case, $p \equiv 1 \bmod 3$ and $p \equiv 3 \bmod 8$ by the case $R(L) = \mathbf{A}_2$ in the proof of Lemma 18. Let $\{v, x\}$ be a basis for $A_2 \subset R_L^*$ such that $\mathrm{Mat}(v, x) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Let $\{v, v - 2x\}$ be a basis for $J \subset A_2$ such that $\mathrm{Mat}(v, v - 2x) =< 2, 6 >$ and $u = v - 2x$.

We first show that if L' is indecomposable and there is an isometric embedding of J into L', then A_2 is represented by L'. Suppose $\phi : J \to L'$ is an isometric embedding and L' is indecomposable. Let K be the orthogonal complement of $\phi(J)$ in L'. Then, dK is either $3p, 12p$, or $48p$ by discriminant arguments. Notice that $dK \neq 3p$ since K is even. Since L' is indecomposable, over $\mathbb{Z}_2$, $< 6 > \perp K_2$ is represented by $< 6, 2, 6p >$, and K_2 is the orthogonal complement of $< 6 >$ in $< 6, 2, 6p >$. Thus, $K_2 \cong < 2, 6p >$ and $dK = 12p$.

Now, let $\{y, z\} \subset K$ such that $\mathrm{Mat}(y, z) \equiv < 2, 6p > \bmod 64$. Let $M = \phi(J) \perp K$. Then, a lattice in $\mathcal{G}'$ containing M is obtained by adjoining $\frac{\phi(v) \pm \phi(u)}{2}$. However, $\{\phi(v), \frac{\phi(v)+\phi(u)}{2}\}$ generates an isometric copy A_2. Thus, if L' is indecomposable and $\phi : J \to L'$ is an isometric embedding, then A_2 is represented by L'.

Now, we determine the number of embeddings of J into a lattice L'. From above, if L' is indecomposable and does not represent A_2, there are no embeddings of J into L'. Thus, for indecomposable lattices with $R(L)^* = \mathbf{A}_1(I)$,$\mathbf{C}_2(I)$, or $\mathbf{A}_1^2$, $a_{JL'} = 0$.

- Suppose $R(L')^* = \mathbf{A}_2$ or $\mathbf{A}_2 \perp \mathbf{A}_1^2$. Then, since there are 6 roots in $\mathbf{A}_2$, v can be embedded in R_L^* in 6 distinct ways. Now, the orthogonal complement of a vector of length 2 in A_2 is isometric to $< 6 >$, and so there are 2 ways to embed u in $R_{L'}^*$ for each embedding of v. Note that in the case of $R(L')^* = \mathbf{A}_2 \perp \mathbf{A}_1^2$, a vector of length 6 that is the sum of a vector of length 2 in $R_{L'}$ and a vector of length 4 in $\mathbf{A}_1^2$ will not be orthogonal to any vector of length 2 in $R(L')^*$. Thus, there are 12 distinct ways to embed J into L' and $a_{JL'} \equiv 0 \mod 4$.

- Suppose $R(L')^* = \mathbf{A}_2 \perp \mathbf{A}_1$. Then, there are the 12 distinct embeddings of J into A_2 as in the previous case. Additionally, there are two ways to send v to A_1, and for each choice of embedding, there are 6 ways to send u into A_2. Thus, there are an additional 12 embeddings of J into L' in this case. Therefore, there are 24 total embeddings of J into L' and $a_{JL'} \equiv 0 \mod 8$.

- Suppose $R(L')^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$. Then, since there are 12 roots in $R(L')^*$, v can be embedded in C_3 in 12 distinct ways. Note that the orthogonal complement of v in C_3 is isometric to $< 2, 4 >$. So, there are 4 ways to embed u so that the images of v and u are orthogonal. Thus, there are 48 distinct ways to embed J into L' and $a_{JL'} \equiv 0 \mod 4$.

- Suppose $R(L')^* = \mathbf{A}_1(D)$. Let K denote the orthogonal complement of $R_{L'}^*$ in L'. Then, if 6 is not represented by K, there are zero ways to embed J into L'. Suppose that K represents 6. Since there are 2 roots in $\mathbf{A}_1(D)$, there are precisely 2 ways to embed v into L'. For each representation of 6 by K, there are 2 ways to embed u into L' so that the images of u and v are orthogonal. Thus, $a_{JL'} \equiv 0 \bmod 4$.

- Suppose $R(L')^* = \mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_1^p$. Then,

$$L' \cong < 2, 2 > \perp \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}.$$

  Now, if $N = \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}$ represents 6, then $\mu_2(N) \leq 6$, but since $p > 13$, this is impossible. Similarly, if 4 is represented by N, then $\mu_2(N) \leq 4$, which is impossible. Therefore, since neither 4 nor 6 is represented by N. There are no embeddings of J into L' and $a_{JL'} = 0$.

- Suppose $R(L')^* = \mathbf{C}_2(D)$. Then, L' is of the form $< 2, 2 > \perp K$ where K is a binary lattice of discriminant p with $\min(K) > 2$. If $\min(K) > 6$, then there are no embeddings of J into L'. Further, if $\min(K) = 6$, then $K \cong \begin{pmatrix} 6 & 1 \\ 1 & \frac{p+1}{6} \end{pmatrix}$. Since there are 4 roots in $\mathbf{C}_2$, there are 4 distinct ways to embed v in L'. For each embedding of v, there are 2 ways to embed u in K. Thus, $a_{JL'} \equiv 0 \mod 8$.

  If $\min(K) = 4$, then $K \cong \begin{pmatrix} 4 & 1 \\ 1 & \frac{p+1}{4} \end{pmatrix}$. Again there are 4 distinct embeddings of v in L'. For each embedding, there are 4 possible ways to embed u into L' such that u is mapped to the sum of vectors of length 2 and 4. Therefore, $a_{JL'} \equiv 0 \bmod 8$ in this case.

- Suppose $R(L')^* = 2\mathbf{A}_1$ and e is a vector in $R(L')^*$ such that $L' \cong \mathbb{Z}[e] \perp K$ and K is an even ternary lattice with $dK = 2p$ and $\mu_1(K) = 2$. Note that if 6 is not represented by K, there are no embeddings of J into L', since the case of $2\mathbf{A}_1$ in the proof of Lemma 17 shows that the orthogonal complement of a vector of length 2 in K does not represent 4. Now, suppose K represents 6 and v is mapped to $\pm e$. Then, u can be mapped to any vector of length 6 in K so that the images of u and v are orthogonal. Thus, the number of embeddings of this kind is congruent to 0 mod 4. Because any additional embeddings will increase the total by a multiple of 4, we have $a_{JL'} \equiv 0 \mod 4$.

Since we have already shown $c_{L'} \equiv 0$ mod 2 when $R(L')^* = \mathbf{A}_1(D), \mathbf{A}_2$ and $2\mathbf{A}_1$, the above discussion implies that $c_{L'}a_{JL'} \equiv 0$ mod 8 in these cases. Further, for the remaining $L' \neq L$, $a_{JL'} \equiv 0$ mod 8 by the above arguments. Recall that for $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1^2$, $a_{JL} = 12$ and by Lemma 20, there is only class in $\mathscr{L}'$ with scaled root system $\mathbf{A}_2 \perp \mathbf{A}_1^2$. Thus, $c_L a_{JL} \equiv 0$ mod 8. So, $c_L \cdot 4 \equiv 0$ mod 8, and $c_L \equiv 0$ mod 2 as desired.

• Fix $L \in \mathscr{L}'$ with $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1$. Now, let $J = A_2$. Then, an embedding of J into L' with $L \neq L'$ will only exist if $R(L')^* = \mathbf{A}_2, \mathbf{A}_2 \perp \mathbf{A}_1^2$, or $\mathbf{C}_3 \perp \mathbf{A}_1^{2p}$.

Suppose $R(L')^* = \mathbf{A}_2$ or $\mathbf{A}_2 \perp \mathbf{A}_1^2$. There are precisely 12 ways to embed J into L' since there is one copy of A_2 in L' and $|O(A_2)| = 12$. Similarly, the number of embeddings of J into L is 12.

Now, suppose $R(L')^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$, then we count the number of distinct embeddings of J into L' in the following way. Let $\{v, x\}$ be a basis of J such that $\mathrm{Mat}(v, x) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and $\{e, f, g\}$ be a basis of C_3 such that $\mathrm{Mat}(e, f, g) =$

$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$. The vector v can be sent to any one of the 12 vectors of length 2 in C_3. Without loss of generality, suppose that v is sent to e. Then, x can be sent to any element of the set $\{f, e-f, f-g, e-f+g\}$ so that the image of $\{v, x\}$ in C_3 spans a copy of A_2. Thus, there are 48 ways to embed J into L.

Previous cases show that $c_{L'} \equiv 0 \bmod 2$ when $R(L')^* = \mathbf{A}_2$ and $\mathbf{A}_2 \perp \mathbf{A}_1^2$. By the above discussion, $a_{JL'} = 12$ for these L', and so $c_{L'}a_{JL'} \equiv 0 \bmod 8$ in these cases. When $R(L') = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$, $c_{L'}a_{JL'} \equiv 0 \bmod 8$ since $a_{JL'} = 48$. By Lemma 21, there is one class in $\mathscr{L}'$ with $R(L)^* = \mathbf{A}_2 \perp \mathbf{A}_1$. Thus, $c_L a_{JL} \equiv 0 \bmod 8$. But then $a_{JL} = 12$, so $c_L \cdot 4 \equiv 0 \bmod 8$ and $c_L \equiv 0 \bmod 2$.

• Fix $L \in \mathscr{L}'$ such that $R(L)^* = \mathbf{C}_2(D)$. Then, $L = R_L^* \perp K$ where K is a binary lattice of discriminant p with $\min(K) > 2$, $K_2 \cong \mathbb{H}$, $K_p \cong < \delta, \delta p >$, and $dK = p$. By the case $R(L) = 2\mathbf{A}_1$ in Lemma 17, $O(K) = \{\pm 1_K\}$, and by Lemma 11, $p \equiv -1 \bmod 8$. Let $\{v, x\}$ be a basis for R_L^* such that $\mathrm{Mat}(v, x) =< 2, 2 >$. Let $J = K$.

Let $L' \in \mathscr{L}'$ such that $L \neq L'$ and suppose that L' contains $< 2 > \perp J$. Let N denote the orthogonal complement of $< 2 > \perp J$ in L'. Suppose that L' is indecomposable with $\min(L') = 2$. Then, over $\mathbb{Z}_2$, by Lemma 13, $\mathbb{H} \perp N_2$ is represented by $< -2, 2, -2p >$ since $J_2 \perp N_2 \cong \mathbb{H} \perp N_2$. But this is impossible. Thus, if L' contains $< 2 > \perp J$, then L' cannot be indecomposable.

Suppose now that L' is decomposable and $L' \cong < 2 > \perp M$ where $dM = 2p$. Then, $J \perp N \subset M$. Since $p \cdot dN = 2p[M : J \perp N]^2$ and $dN | (p \cdot 2p)$, we have that either $dN = 2$ or $2p^2$. However, over $\mathbb{Z}_p$, J_p splits L'_p, so $< 2 > \perp N_p$ is represented by $< 1, 1 >$. Since N_p is the orthogonal complement of $< 2 >$, it must be that $dN = 2$. Therefore, $L' \cong < 2, 2 > \perp J \cong L$, and there is one class in $\mathcal{G}'$ containing $< 2 > \perp J$. Furthermore, if L' contains $< 2 > \perp J$, then L' contains $< 2 > \perp J \perp N$ and $L' \cong L$.

Let $\phi : J \to L$. Then, because J is chosen to be an indecomposable component of L, there are no embeddings of J into L such that $\phi(J)$ is not orthogonal to either v or x. Since $\phi(J) = J$ and $O(J) = \{\pm 1_J\}$, there are precisely two ways to embed J into L and $a_{JL} \equiv 2 \mod 4$.

Let $\phi : J \to L'$ be an isometric embedding such that $L \neq L'$ and $\min(L') = 2$. Suppose that $\phi(J)$ is orthogonal to a vector e of length 2 in L'. Further, suppose that L' is indecomposable. Then, by Lemma 13, over $\mathbb{Z}_2$, $\mathbb{H}$ is represented by $< -2, 2, -2p >$. But this is impossible. Thus, $\phi(J)$ cannot be orthogonal to any vector of length 2 in L', and by Lemma 10, $a_{JL'} \equiv 0 \mod 4$.

Now, suppose L' is decomposable. Then, ϕ can be extended to an isometry Φ on $\mathbb{Q}L$ such that $\Phi(v) = e$ and $\Phi|_J = \phi$, and so $\Phi^{-1}(L')$ contains $R_L^* \perp J$. However, since there is only one class of lattices in $\mathcal{G}'$ containing $R_L^* \perp J$, it must be that $\Phi(L) \cong L'$. Therefore, $L = L'$ and by Lemma 10, $a_{JL'} \equiv 0 \bmod 4$.

Suppose now that L' has $\min(L') = 4$ and let f be a vector of length 4 in $R(L')^* = \mathbf{A}_1^2$. Suppose that $\phi(J)$ is orthogonal to f in L' and let N denote the orthogonal complement of $\mathbb{Z}[f] \perp \phi(J)$ in L'. Since $4p \cdot dN = 4p[L' : \mathbb{Z}[f] \perp \phi(J) \perp N]^2$ and $dN|(4p \cdot 4p)$, dN is one of $1, 4, 16, p^2, 4p^2$, or $16p^2$. Notice that $dN \neq 1$ or p^2 since N is rank 1 and even.

Over $\mathbb{Z}_p$, $(\phi(J))_p$ splits L'_p, and so $< 1 > \perp N_p$ is represented by $< 1, 1 >$. Thus, N_p is the orthogonal complement of $< 1 >$ in $< 1, 1 >$, so $N_p \cong < 1 >$ and $dN_p = 1$. Now, $dN = 4$ or 16. Over $\mathbb{Z}_2$, $\mathbb{H} \perp N_2$ is represented by $\mathbb{H} \perp < -4p >$ by Lemma 13. Thus, since N_2 is the orthogonal complement of $\mathbb{H}$, $N_2 \cong < -4p > \cong < 4 >$ and $dN_2 = 4$. Therefore, $dN = 4$.

Now, the sublattice $M = \mathbb{Z}[f] \perp \phi(J) \perp \mathbb{Z}[z]$ has index 2 in L' where z is a vector of length 4 in L'. Let $\{x, y\} \subset \phi(J)$ such that $\mathrm{Mat}(x, y) \equiv \mathbb{H}$ mod 64. Then, $L' = M + \mathbb{Z}[\frac{f+z}{2}] = M + \mathbb{Z}[\frac{f-z}{2}]$. However, $Q(\frac{v+z}{2}) = 2$, which is a contradiction since $\min(L') = 4$. Thus, $\phi(J)$ cannot be orthogonal to a vector of length 4 in $R^*_{L'}$. By Lemma 10, $a_{JL'} \equiv 0$ mod 4 in this case.

Finally, since $a_{JL'} \equiv 0$ mod 4 for all $L' \neq L$, $c_L a_{JL} \equiv 0$ mod 4. Because $a_{JL} = 2$, we have $c_L \equiv 0$ mod 2.

• Fix $L \in \mathscr{L}'$ with $R(L)^* = \mathbf{A}_1^2$ and let v be a vector of length 4 in $R(L)^*$. Let K be the orthogonal complement of R^*_L in L. By the proof of Proposition 1, $dK = 4p$, $K_p \cong < 1, \delta, \delta p >$ and

$$K_2 \cong \begin{cases} \mathbb{H} \perp < -4p > & p \equiv -1 \bmod 8, \\ \mathbb{A} \perp < 12p > & p \equiv 3 \bmod 8. \end{cases}$$

By [13, Lemma 1.6], K contains a sublattice J such that $J_2 \cong \mathbb{P}$ where $\mathbb{P}$ denotes the even unimodular component of K_2, $J_p \cong < 1, \delta >$, and $dJ = q$ for some large prime q. Note also that $q \equiv -1$ mod 8 when $p \equiv 3$ mod 8 and $q \equiv 3$ mod 8 when $p \equiv -1$ mod 8.

Let N be the orthogonal complement of $R^*_L \perp J$ in L. Then, N is a rank 1 lattice generated by a vector z of length $4pq$. Let $M = R^*_L \perp J \perp N$. Then, M has index $2q$ in L. Since J_2 splits L_2, $L_2 = M_2 + \mathbb{Z}_2[\frac{v+z}{2}] = M_2 + \mathbb{Z}_2[\frac{v-z}{2}]$. The map τ_z stabilizes L_2. Over $\mathbb{Z}_q$, $J_q \cong < \alpha, \alpha q >$ in a basis $\{e, f\}$ with $\alpha \in \mathbb{Z}_q^\times$. Then, L_q is equal either $M_q + \mathbb{Z}_q[\frac{f+az}{q}]$ or $M_q + \mathbb{Z}_q[\frac{f-az}{q}]$ with $a \in \mathbb{Z}_q$ such that $\frac{1}{q}(Q(f) + a^2 Q(z)) \equiv 0$ mod q. These lattices are isometric via τ_z. Thus, there are exactly two lattices in $\mathcal{G}'$ containing M, and they are $M + \mathbb{Z}[\frac{v+z}{2}, \frac{f'+az}{q}]$ and $M + \mathbb{Z}[\frac{v-z}{2}, \frac{f'+az}{q}]$, where $f' \in J$ which locally approximates f. However, these lattices are equal, and so there is only one class in $\mathcal{G}'$ containing M.

Suppose $\phi : J \to L$ is an isometric embedding such that $\phi(J)$ is orthogonal to v in L. Then, there exists some $\sigma \in O(\mathbb{Q}L)$ such that $\sigma|_J = \phi$. Further, $\sigma^{-1}(L)$ must contain M. Thus, $\sigma^{-1}(L) = L$ or $\sigma^{-1}(L) = \tau_z(L)$ by the above discussion. Since $\sigma|_J = \phi$ and $\sigma \circ \tau_z|_J = \phi$, ϕ is in the orbit of the inclusion map under the action of $O(L) = \langle -1_L, \tau_v \rangle$, and this orbit has two embeddings. By Lemma 10, the number of embeddings $\phi : J \to L$ such that $\phi(J)$ not orthogonal to $\mathbb{Z}[v]$ is congruent to 0 mod 4. Thus, $a_{JL} \equiv 2 \bmod 4$.

Let $\phi : J \to L'$ be an isometric embedding such that $L \neq L'$ and $\min(L') = 4$. Suppose that $\phi(J)$ is orthogonal to a vector f of length 4 in $R(L')^*$. Then, ϕ can be extended to an embedding ϕ' of $\mathbb{Z}[v] \perp J$ into L' where $\phi'(v) = f$ and $\phi'|_J = \phi$. Further, ϕ' can be extended to an isometry Φ of $\mathbb{Q}L$, and so $\Phi^{-1}(L')$ is a lattice in $\mathcal{G}'$ which must contain M by local consideration. However, since there is only one class of lattices in $\mathcal{G}'$ containing M, it must be that $L = L'$, which is impossible. Thus, $\phi(J)$ cannot be orthogonal to any vector of length 4 in L', and by Lemma 10, $a_{JL'} \equiv 0 \bmod 4$.

Let $\phi : J \to L'$ be an isometric embedding such that $L \neq L'$ where $\min(L') = 2$ and L' is indecomposable. Suppose that $\phi(J)$ is orthogonal to a vector e of length 2 in L'. Over $\mathbb{Z}_2$, by Lemma 13, $\phi(J_2) \cong \mathbb{P}$ is represented by $< -2, 2, -2p >$, but this is impossible. Thus, $\phi(J)$ cannot be orthogonal to any vector of length 2 in L', and by Lemma 10, $a_{JL'} \equiv 0 \mod 4$ in this case.

Now, for all $L' \neq L$ with $\min(L') = 4$, $a_{JL'} \equiv 0 \mod 4$. Further, for all $L' \neq L$ with $\min(L') = 2$ and $R(L)^* \neq \mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_1^p$, from previous cases, $c_{L'} \equiv 0 \mod 2$. Note that $a_{JL'} \equiv 0 \mod 2$ since for each embedding, we will also have its negative. Thus, $c_{L'} a_{JL'} \equiv 0 \mod 4$.

Finally, let $\phi : J \to L'$ be an isometric embedding such that $R(L') = \mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_1^p$. Then, let $\{v, x, y, z\} \subset L'$ be vectors in $R(L')^*$ with $L' \cong$

$\mathrm{Mat}(v,x,y,z) =< 2,2 >\perp \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}$. Suppose that $\phi(J)$ is orthogonal to $\mathbb{Z}[v,x]$ but not $\mathbb{Z}[y]$. Then, $\phi(J)$ would be represented by $K' \cong \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}$. However, since $dJ = q$ and $dK' = p$, this is impossible. Thus, there are no embeddings of J into L' such that $\phi(J)$ is orthogonal to $\mathbb{Z}[v,x]$.

Next, suppose that $\phi(J)$ is orthogonal to $\mathbb{Z}[v,y]$. Then, $\phi(J)$ is represented by the orthogonal complement of $\mathbb{Z}[v,y]$, which is $\mathbb{Z}[x, y-2z] \cong< 2, 2p >$. However, by a discriminant argument, this is impossible. Thus, there are no embeddings of J into L' such that $\phi(J)$ is orthogonal to $\mathbb{Z}[v,y]$. A similar argument holds for $\mathbb{Z}[x,y]$.

Now, without loss of generality, suppose that $\phi(J)$ is orthogonal to $\mathbb{Z}[v]$ but not orthogonal to either $\mathbb{Z}[x]$ or $\mathbb{Z}[y]$. Then, the group $\{\pm\tau_x, \pm 1_{L'}\}$ acts on the set of embeddings with this property since both x and y are orthogonal to v. Thus, the number of embeddings with this property is divisible by 4. Finally, suppose that $\phi(J)$ is not orthgonal to any of v, x or y. Then, the group $\{\pm\tau_v, \pm 1_{L'}\}$ acts on the set of embeddings with this property since both x and y are both orthogonal to v. Therefore, $a_{JL'} \equiv 0 \mod 4$ for L' with $R(L') = \mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_1^p$. Now, $c_L a_{JL} \equiv 0 \mod 4$. But $a_{JL} \equiv 2 \mod 4$, and so $c_L \equiv 0 \mod 2$.

• Fix $L \in \mathscr{L}'$ with $R(L)^* = \mathbf{C}_2(I)$. By Lemma 11, $p \equiv -1 \mod 8$. Let v and x be orthogonal vectors of length 2 in $R(L)^*$ such that $R_L^* \cong \mathrm{Mat}(v,x) =< 2,2 >$ and let $\{y,z\} \subset K$ such that $\mathrm{Mat}(y,z) \equiv \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \mod 64$. Then, a lattice L in $\mathcal{G}'$ containing $R_L^* \perp K$ is obtained by adjoining $\frac{y}{2}, \frac{z}{2}$, or $\frac{v+x+y+z}{2}$ to $R_L^* \perp K$. However, if L was equal to either of the lattices obtained by adjoining $\frac{y}{2}$ or $\frac{z}{2}$, then R_L would split L, which is impossible. Thus, $L = (R_L^* \perp K) + \mathbb{Z}[\frac{v+x+y+z}{2}]$.

Let J be the orthogonal complement of R_L^* in $L^\#$. We first determine the local structure of J at 2 and p, respectively. Note that $K \subset J \subset K^\#$ and $[K^\# : K] = 4p$.

Since $L_p^\# \cong <1, 1, \delta, \frac{\delta}{p}>$, and $(R_L^*)_p$ splits $L_p^\#$, $J_p \cong <\delta, \frac{\delta}{p}>$. Then, $J_p = K_p^\#$ since $[J_p : K_p] = p$ and $[K_p^\# : K_p] = p$.

Now, $[J : K]$ is either $1, 2$ or 4. To determine this index, we consider the localization at 2. Note that $K_2^\#$ is generated by $\{\frac{y}{2}, \frac{z}{2}\}$. Then, since $L = (R_L^* \perp K) + \mathbb{Z}[\frac{v+x+y+z}{2}]$, $B(\frac{y+z}{2}, L) \subset \mathbb{Z}$ and $\frac{y+z}{2} \in J_2 \backslash K_2$ because $\frac{y+z}{2}$ is orthogonal to R_L^* and has conductor 2 with respect to K. So, $[J : K]$ cannot be 1. Now, $B(\frac{z}{2}, L) \not\subset \mathbb{Z}$ and so $\frac{z}{2} \in K_2^\# \backslash L_2^\#$. Thus, $[K_2^\# : J_2]$ cannot be 1, and so $[J_2 : K_2] = 2$. Now, $[J : K] = 2p$, and thus, $[L^\# : R_L^* \perp J] = 4$. So, $dJ = \frac{1}{p}$. Further, $J_2 = K_2 + \mathbb{Z}_2[\frac{y+z}{2}] \cong \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cong <1, -1>$, and so $J_2 \cong <1, -1> \cong <1, p>$.

To summarize what we have just shown: $dJ = \frac{1}{p}$, $J_2 \cong <1, p>$, and $J_p \cong <\delta, \frac{\delta}{p}>$.

Now, let $\{\alpha, \beta\} \subset J$ such that $\mathrm{Mat}(\alpha, \beta) \equiv <1, p> \bmod 64$. Let $M = R_L^* \perp J$. Then, $L^\#$ is obtained by adjoining any two vectors in the set $\{\frac{v+x}{2}, \frac{\alpha+\beta}{2}, \frac{v+x+\alpha+\beta}{2}\}$ to M. Note that adjoining any two of these three vectors to M will produce a lattice containing the third. Thus, there is exactly one lattice in $\mathcal{G}^\#$ containing M.

Let $\phi : J \to L^\#$ be an isometric embedding and suppose that $\phi(J)$ is orthogonal to R_L^* in $L^\#$. Then, ϕ is an isometry of J, and if σ is the isometry $1_{R_L^*} \perp \phi$, then $\sigma(L^\#) = L^\#$, since $L^\#$ is the only lattice in $\mathcal{G}^\#$ containing M. Thus, σ is in $O(L^\#) = O(L)$, and because $O(L) = O(C_2) \times \{\pm 1_K\} = O(C_2) \times \{\pm 1_J\}$, $\phi = \pm 1_J$. Therefore, there are precisely two embeddings ϕ of J into $L^\#$ such that $\phi(J)$ is orthogonal to R_L^*. Suppose $\phi(J)$ is not orthogonal to any vector of length 2 in R_L^*. Then, by Lemma 10, the number of distinct embeddings with this property is divisible by 4. Finally, suppose that $\phi(J)$ is orthogonal to only one of v and x but not both. Without loss of generality, we may assume $\phi(J)$ is orthogonal to v. Then, the group $\{\pm\tau_x, \pm 1_L\}$ acts on the set of these embeddings since v and x are orthogonal, and the size of this set is also divisible by 4. Therefore, we can conclude that $a_{JL^\#} \equiv 2 \bmod 4$.

Suppose now that $\phi : J \to L'^\#$ is an isometric embedding such that $L' \neq L$ and $\min(L') = 2$. Further, suppose $\phi(J)$ is orthogonal to a minimal vector e of L' and that $L' = \mathbb{Z}[e] \perp K'$. Then, the orthogonal complement of $\mathbb{Z}_2[e]$ in $L'^\#$ is isometric to $\mathbb{H} \perp < \frac{1}{2} >$. But this implies that $\phi(J_2) \cong < 1, p >$ is represented by $\mathbb{H} \perp < \frac{1}{2} >$, which is impossible. Thus, if L' is decomposable, $\phi(J)$ cannot be orthogonal to a vector of length 2 in $L'^\#$, and by Lemma 10, $a_{JL'} \equiv 0 \mod 4$.

Now, suppose that $\phi : J \to L'^\#$ is an isometric embedding such that $L' \neq L$, $\min(L') = 2$, and L' is indecomposable. Further, suppose $\phi(J)$ is orthogonal to a minimal vector f of L'. Then, ϕ can be extended to an isometry Φ on $\mathbb{Q}L'^\# = \mathbb{Q}L'$ such that $\Phi(v) = f$ and $\Phi|_J = \phi$. Further, by an argument analogous to the case $\mathbf{C}_2$ in Theorem 1, the orthogonal complement of $\mathbb{Z}[f] \perp \phi(J)$ in $L'^\#$ is isometric to $< 2 >$. Thus, $\Phi^{-1}(L'^\#)$ contains M. However, since there is only one lattice in $\mathcal{G}^\#$ containing M, it must be that $\Phi(L^\#) = L'^\#$ and hence $L' = L$, which is impossible. So, $\phi(J)$ is not orthogonal to any minimal vector f in L', and by Lemma 10, $a_{JL'^\#} \equiv 0 \bmod 4$ for all $L' \neq L$ with $\min(L') = 2$ in $\mathscr{L}'$.

For L' with $\min(L') = 4$, a previous discussion showed that $c_{L'} \equiv 0 \bmod 2$. Additionally, $a_{JL'^\#} \equiv 0 \bmod 2$, and so $c_{L'} a_{JL'^\#} \equiv 0 \bmod 4$. Now, $a_{JL'^\#} \equiv 0 \bmod 4$ for all $L' \neq L$, and thus, $c_L a_{JL^\#} \equiv 0 \bmod 4$. But $a_{JL^\#} \equiv 2 \bmod 4$. Therefore, $c_L \equiv 0 \bmod 2$.

• Fix $L \in \mathscr{L}'$ with $R(L)^* = \mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_1^p$. By Corollary 3, there is exactly one class in $\mathscr{L}'$ with this scaled room system and

$$L \cong <2> \perp <2> \perp \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}.$$

Let $\{v, x, y, z\}$ yield the above Gram matrix of L. Let $J \cong \mathrm{Mat}(y, z) = \begin{pmatrix} 2 & 1 \\ 1 & \frac{p+1}{2} \end{pmatrix}$. Now, suppose that $L' \in \mathscr{L}'$ such that $L \neq L'$ and L' contains $<2> \perp J$. Let N denote the orthogonal complement of $<2> \perp J$ in L'. If L' is indecomposable, over $\mathbb{Z}_2$, $\mathbb{H} \perp N_2$ is represented by $<-2, 2, -2p>$ by Lemma 13. However, this is impossible, and so L' cannot be indecomposable.

Suppose that L' is decomposable and $L' \cong <2> \perp M$ where $dM = 2p$. Then, $J \perp N$ is represented by M. Since $p \cdot dN = 2p[M : J \perp N]^2$ and $dN|(p \cdot 2p)$, dN is either 2 or $2p^2$. However, over $\mathbb{Z}_p$, J_p splits L'_p, and so $<2> \perp N_p$ is represented by $<1, 1>$. Therefore, N_p is the orthogonal complement of $<2>$ and $dN = 2$. Thus, $L' \cong <2, 2> \perp J \cong L$. Thus, there is one class in $\mathscr{L}'$ containing $<2> \perp J$. Furthermore, if L' contains $<2> \perp J$, then L' contains $<2> \perp J \perp N$ and $L' \cong L$.

Let $\phi : J \to L$ be an isometric embedding. Then, ϕ is an isometry of J because J is an indecomposable component of L not isometric to $<2>$. Since $|O(J)| = 4$, $a_{JL} \equiv 0 \mod 4$.

Let $\phi : J \to L'$ be an isometric embedding such that $L \neq L'$. First, suppose that $\min(L') = 2$ and $\phi(J)$ is orthogonal to a vector e of length 2 in $R(L')^*$. If L' is indecomposable, over $\mathbb{Z}_2$, $J_2 \cong \mathbb{H}$ is represented by $<-2, 2, -2p>$, which is impossible. Thus, $\phi(J)$ is not orthogonal to any minimal vector in L' and $a_{JL'} \equiv 0 \bmod 4$ by Lemma 10. Further, because all indecomposable classes with minimum 2, apart from L' with $R(L')^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$, have $c_{L'} \equiv 0 \mod 2$ by previous consideration, $c_{L'}a_{JL'} \equiv 0 \mod 8$.

Suppose now that L' is decomposable. Then, ϕ can be extended to an isometry Φ such that $\Phi(v) = e$ and $\Phi|_J = \phi$. Then, $\Phi^{-1}(L')$ contains $\mathbb{Z}[e] \perp J \perp N$. However, since there is one class in $\mathscr{L}'$ containing $\mathbb{Z}[e] \perp J \perp N$, it must be that $\Phi(L) \cong L'$. Therefore, $L = L'$ and $\phi(J)$ cannot be orthogonal to any vector of length 2. By Lemma 10, $a_{JL'} \equiv 0$ mod 4 in this case. Further, for all decomposable cases, apart from L' with $R(L')^* = \mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_p$, a previous discussion shows that $c_{L'} \equiv 0 \mod 2$, and so $c_{L'}a_{JL'} \equiv 0 \mod 8$.

Let $L' \in \mathscr{L}'$ such that $R(L')^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$. Consider the action of $\langle \tau_f, \tau_g, -1_{L'} \rangle$ where $f, g \in C_3$ such that $Q(f) = Q(g) = 2$ and $B(f, g) = 0$. Then, since $\phi(J)$ is not orthogonal to any vectors of length 2 in C_3, $\pm\tau_f$, $\pm\tau_g$, and $\pm 1_{L'}$ are not in the stabilizer of ϕ.

Suppose that $\sigma = \tau_f \tau_g$ stabilizes ϕ. Then, $\phi(J)$ is orthogonal to some vector of length 2 in L', which is impossible, and so σ does not stabilize ϕ. Similarly, suppose that $-\sigma = -\tau_f \tau_g$ stabilizes ϕ. Then, since the dimension of the fixed space is 2 and contains $\phi(J)$, $\phi(J)$ is contained in $\mathbb{Z}[f, g]$, which is not the case by construction. So, $-\sigma$ does not stabilize ϕ and $|\mathrm{orb}(\phi)| = 8$. Then, $a_{JL'} \equiv 0$ mod 8.

Finally, suppose that $\min(L') = 4$ and $\phi(J)$ is orthogonal to a vector of length 4 in $R(L')^*$. Then, there are no embeddings of J into L' since L' does not represent 2.

Now, $c_{L'}a_{JL'} \equiv 0$ mod 8 for all $L \neq L'$, and so $c_L a_{JL} \equiv 0 \mod 8$. Since $a_{JL} \equiv 0 \mod 4$, $c_L \equiv 0$ mod 2.

• Fix $L \in \mathscr{L}'$ such that $R(L)^* = \mathbf{C}_3 \perp \mathbf{A}_1^{2p}$. By Lemma 11, $p \equiv -1$ mod 8, and by Lemma 19, there is exactly one class in $\mathcal{G}'$ with this scaled root system. Let

$\{v, x\} \subset L$ such that $\mathrm{Mat}(v, x) =< 2, 2 >$ and let $J \cong \mathrm{Mat}(v, x)$. An embedding of J into L' where $L \neq L'$ will only exist if $R(L')^* = 2\mathbf{A}_1, \mathbf{A}_2 \perp \mathbf{A}_1, \mathbf{C}_2(D), \mathbf{C}_2(I)$ or $\mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_1^p$. Since $|O(2A_1)| = |O(C_2)| = 8$, $a_{JL'} \equiv 0 \mod 8$ for each $L' \neq L$ representing $2A_1$.

To determine the number of embeddings of J into L, we proceed in the following way. Let $\{e, f, g\}$ be a basis for $C_3 = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$. Then, v can be sent to any one of the 12 roots in C_3. Then, because the orthogonal complement of a vector of length 2 in C_3 is isometric to $< 2, 4 >$, there are 2 ways to send x into C_3. Thus, there are 24 embeddings of J into L.

Now, $a_{JL'} = 0$ when $R(L')^*$ is not equal to one of $2\mathbf{A}_1, \mathbf{A}_2 \perp \mathbf{A}_1, \mathbf{C}_2(D), \mathbf{C}_2(I)$, $\mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_1^p$ or $\mathbf{C}_3 \perp \mathbf{A}_1^{2p}$. By previous cases, we have that $c_{L'} \equiv 0 \mod 2$ when $R(L')^* = 2\mathbf{A}_1, \mathbf{A}_2 \perp \mathbf{A}_1, \mathbf{C}_2(D), \mathbf{C}_2(I)$, or $\mathbf{C}_2 \perp \mathbf{A}_1 \perp \mathbf{A}_1^p$. Therefore, $c_{L'}a_{JL'} \equiv 0 \mod 16$ for these L'. Thus, $c_L a_{JL} \equiv 0 \mod 16$. But $a_{JL} = 24$, so $c_L \cdot 8 \equiv 0 \mod 16$, and thus $c_L \equiv 0 \mod 2$.

Finally, we have obtained a contradiction by showing that $c_{L'} \equiv 0 \mod 2$ for all $L' \in \mathscr{L}'$. Therefore, the degree 2 theta series of the classes in $\mathcal{G}'$ with nontrivial orthogonal groups are linearly independent over $\mathbb{Z}$. $\square$

Bibliography

[1] A. N. Andrianov, Quadratic Forms and Hecke Operators, Springer-Verlag, (1987).

[2] N. Bourbaki, Elements of Mathematics: Lie Groups and Lie Algebras, Chapters 4 - 6., Springer-Verlag, (2002).

[3] J. W. S. Cassels, "Rational Quadratic Forms," Dover Publications, Inc., Mineloa, New York, 1978.

[4] W. K. Chan, *Quaternary Even Positive Definite Quadratic Forms of Discriminant* $4p$, J. Number Theory, **76**, (1999), 265-280.

[5] W. K. Chan, *Class Numbers of Quaternary Quadratic Forms of Discriminant* $4p$, Cont. Math., **249**, (1999), 29-41.

[6] W. K. Chan and Meinhard Peters, *Quaternary Quadratic Forms and Hilbert Modular Surfaces*, Cont. Math. **344**, (2004), 85-97.

[7] W. Curtis and I. Reiner, Representation Theory of Finite Groups and Associated Algebras, Interscience, New York, 1962.

[8] E. Freitag, Siegelsche Modulfunktionen, Springer-Verlag, (1983).

[9] L. J. Gerstein, Basic Quadratic Forms, American Mathematical Society, (2008).

[10] B. H. Gross, *Heights and the special values of L-series*, CMS Conf. Proc., **7**, (1985), 115-187.

[11] J.S. Hsia and D. C. Hung, *Theta Series of Ternary and Quaternary Quadratic Forms*, Invent. math. **73**, (1983), 151-156.

[12] J.S. Hsia and D. C. Hung, *Theta Series of Quaternary Quadratic Forms over $\mathbb{Z}$ and $\mathbb{Z}[(1+\sqrt{p})/2]$*, Acta Arith., **45**, (1985), 75-91.

[13] J. S. Hsia, Y. Kitaoka, and M. Kneser, *Representation of Positive Definite Quadratic Forms*, J. Reine Angew. Math. **301**. 1978, 132- 141.

[14] D.C. Hung, *Theta Series of Ternary Quadratic Forms*, J. Number Theory **26**, (1987), 1-7.

[15] M. H. Kim and B. K. Oh, *Generation of isometries of $\mathbb{Z}$-lattices by symmetries*, J. Number Theory, **83**, (2000), 76-90.

[16] J. Kramer, *On the linear independence of certain theta-series*, Math. Ann., **281**, (1988), 219-228.

[17] J. Martinet, Perfect Lattices in Euclidean Space, Springer-Verlag, (2003).

[18] O.T. O'Meara, Introduction to Quadratic Forms, Springer- Verlag, (1973).

[19] R. Scharlau, *Reflective Integral Lattices*, J. Algebra, **181**, No. 3 (1996), 934-961.

[20] A. Schiemann, *Ternary positive definite quadratic forms are determined by their theta series*, Math. Ann., **308**, (1997), 507-517.

[21] R. Schulze-Pillot. *A linear relation between theta series of degree and weight 2*, Number Theory, (Ulm, 1987), 197-201, Lecture Notes in Math., Springer, New York, 1989.