THE UNIVERSITY OF CHICAGO

CLIFFORD ALGEBRAS AND SHIMURA'S LIFT FOR THETA-SERIES

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY
FEDOR A. ANDRIANOV

CHICAGO, ILLINOIS
JUNE 2000

To Yuliya, who made a wonderful difference in my life.

Abstract

Automorph class theory formalism is developed for the case of integral nonsingular quadratic forms in an odd number of variables. As an application, automorph class theory is used to construct a lifting of similitudes of quadratic $\mathbb{Z}$-modules of arbitrary nondegenerate ternary quadratic forms to morphisms between certain subrings of associated Clifford algebras. The construction explains and generalizes Shimura's correspondence in the case of theta-series of positive definite ternary quadratic forms. The relation between associated zeta-functions is considered.

Acknowledgments

I am greatly indebted to Professor A. Andrianov without whose constant inspiration this paper would never be possible. I would like to express my deep gratitude to Professor W. Baily for many stimulating conversations and also for his personal friendship. I wish to thank Professor N. Nygaard whose help, advice, and encouragement have been exceptional in every way. Finally, I would like to thank Professor P. Ponomarev for his interest and friendly support.

Table of contents

Chapter 1
Introduction

1.1 Statement of results

In his important paper [12] G. Shimura discovered a remarkable correspondence between modular forms of half-integral weight and forms of integral weight – the so-called “ Shimura lift ” (see [12, Main Theorem]). P. Ponomarev [10] determined the effect of Shimura's lifting on the theta-series $\Theta(z, \mathbf{q})$ of certain positive definite ternary quadratic forms $\mathbf{q}$. Using purely arithmetical approach he expressed the lift of $\Theta(z, \mathbf{q})$ as an explicit linear combination of theta-series associated with a certain system of quaternary quadratic forms coming from a quaternion algebra (see [10, Theorem 1]). Considering the Fourier coefficients of corresponding theta-series, we can interpret these results as a link between the numbers of representations of integers by positive definite quadratic forms in three and in four variables. But in accordance with the theory of automorph class rings (i.e., matrix Hecke rings of orthogonal groups) developed by A. Andrianov in [1] and [2], the majority of known multiplicative properties of the numbers of integral representations by quadratic forms turn out to be merely a reflection of certain relations between the representations themselves. Following the ideas of A. Andrianov and P. Ponomarev, one can look for a direct algebraic correspondence between the representations of integers by quadratic forms in three and four variables that is expected to underlie Shimura's lift in case of theta-series. In the present paper we examine such a correspondence constructed by means of Clifford algebras.

In the first part of the paper (Chapters 2, 3, and 4) we develop automorph class theory formalism for the case of arbitrary integral nonsingular quadratic forms in an odd number of variables. Because of the impossibility of applying the methods of [1] directly, we introduce and study *isotropic sums* of a special type, computation of which is an essential technical prerequisite for determination of action of classes of automorphs (or of Hecke operators) on integral representations by quadratic forms in an odd number of variables (or on their theta-series respectively). Our principal technical result on isotropic sums can be stated as follows.

Theorem . *Let* $\mathbf{q}$ *be an arbitrary integral nonsingular quadratic form in an odd number of variables* $m = 2k+1 \geq 3$, *and let* p *be a rational prime not dividing the determinant* $\det \mathbf{q}$ *of the form* $\mathbf{q}$. *Let* $\{\mathbf{q}_1, \ldots, \mathbf{q}_h\}$ *be a complete system of representatives of different equivalence classes contained in the similarity class of* $\mathbf{q}$. *Then for each integral column* $K \in \mathbb{Z}^m$ *such that* $\mathbf{q}[K] \equiv 0 \pmod{p^2}$ *we have*

$$\sum_{i=1}^{h} \sum_{\substack{M \in R^*(\mathbf{q}, p^2\mathbf{q}_i)/E(\mathbf{q}_i) \\ M|K}} 1 =$$

$$c_p \cdot \left\{ 1 + \left(\varepsilon_p \chi_{\mathbf{q}}(p) p^{k-1} + c_p^{-1} \beta_p \right) \cdot \delta_{(p^{-1}K)} + p^{m-2} \cdot \delta_{(p^{-2}K)} \right\},$$

where

$$c_p = c_p(\mathbf{q}) = \sum_{a=1}^{k} \prod_{i=1}^{a-1} \frac{p^{2(k-i)} - 1}{1 - p^{-i}} \cdot p^{1-a},$$

$$\beta_p = \beta_p(\mathbf{q}) = \sum_{a=1}^{k} \left(\prod_{i=1}^{a-1} \frac{p^{2(k-i)} - 1}{1 - p^{-i}} \cdot \frac{p^{m-2} - p^{a-1}(p+1) + 1}{p^{a-1}(p^a - 1)} \right),$$

the symbol $\varepsilon_p = \varepsilon_p\left(\mathbf{q}(p^{-1}K)\right)$ *and the quadratic character* $\chi_{\mathbf{q}}(p)$ *are given by the Legendre symbols*

$$\varepsilon_p(a) = \left(\frac{2a}{p}\right), \ a \in \mathbb{N} \quad \text{and} \quad \chi_{\mathbf{q}}(p) = \left(\frac{(-1)^k \det \mathbf{q}}{p}\right),$$

respectively and $\delta_{(X)}$ *is the generalized Kronecker symbol*

$$\delta_{(X)} = \begin{cases} 1 & , \text{if } X \text{ is an integral matrix,} \\ 0 & , \text{if matrix } X \text{ is not integral.} \end{cases}$$

(See also Theorems 2.9 and 2.11).

Our method of computation is purely algebraic – based on consideration of certain quadratic modules over residue class rings – and can be easily generalized to forms over arbitrary Dedekind domains. In view of Shimura's formula for the action of Hecke operators $T(p^2)$ on modular forms of half-integral weight, as a corollary of the above Theorem we obtained a new proof of Eichler's commutation relations for the theta-series of positive definite quadratic forms in an odd number of variables, see (3.2). Moreover, the above Theorem allowed us to derive an automorph class theory analog of Eichler's commutation relations for arbitrary nonsingular integral quadratic forms in an odd number of variables which explains and generalizes the classical relations, see (4.4). We show further that the derived multiplicative decompositions of classes of integral representations imply similar relations between the numbers of such representations that resemble Shimura's well-known factorizations of zeta-functions of modular forms of half-integral weight (see [12]), and explain the latter in the case of theta-series of positive definite quadratic forms.

Corollary . *With the notation and under the assumptions of the above Theorem,*

$$\sum_{(n,\det \mathbf{q})=1} \frac{\mathfrak{R}(n^2a)}{n^s} = \prod_{p \nmid \det \mathbf{q}} \Big(\frac{[1] - \chi_{\mathbf{q}}(p)(\frac{2a}{p})[p]p^{k-1-s}}{[1] - c_p^{-1}(\mathfrak{T}^*(p^2) - \beta_p[p])p^{-s} + [p^2]p^{m-2-2s}}\Big) \cdot \mathfrak{R}(a) \ ,$$

where $m = 2k+1 \geq 3$ is odd and a is a square-free integer.

The second part of the present paper (Chapters 5, 6, and 7) contains an application of the techniques developed to an explicit construction of certain algebraic correspondence between ternary and quaternary quadratic forms. We use automorph class theory to construct a lifting of similitudes of quadratic $\mathbb{Z}$-modules of arbitrary nonsingular ternary quadratic forms to morphisms between certain subrings of associated Clifford algebras. Our main result is contained in Theorems 7.5 and 7.7 together with Corollary 7.8. In the notation of Chapter 1, all this can be summarized as follows.

Proposition . *Let $\mathbf{q}$ be an integral nonsingular ternary quadratic form and let $\mathbf{n}$*

be the integral quadratic form defined (up to integral equivalence) by the norm on the even subalgebra of the Clifford algebra $C(\mathbf{q})$ *. Take* $\{\mathbf{q}_1, \ldots, \mathbf{q}_h\}$ *and* $\{\mathbf{n}_1, \ldots, \mathbf{n}_H\}$ *to be complete systems of representatives of different equivalence classes of the similarity classes of* $\mathbf{q}$ *and of* $\mathbf{n}$ *respectively. Let* p *be a prime number coprime to* $\det \mathbf{q}$ *. Denote by*

$$\mathcal{T}^*_{\mathbf{q}}(p^\iota) = \bigcup_{i=1}^{h} E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^\iota \mathbf{q}) \quad \textit{and} \quad \mathcal{T}^*_{\mathbf{n}}(p^\iota) = \bigcup_{j=1}^{H} E(\mathbf{n}_j)\backslash R^*(\mathbf{n}_j, p^\iota \mathbf{n})$$

the sets of classes of (primitive) automorphs of $\mathbf{q}$ *and of* $\mathbf{n}$ *respectively (with multiplier* p^ι*). Then there exists an injection* $\Psi : A \mapsto \Psi_A,\ \mathcal{T}^*_{\mathbf{q}}(p^2) \to \mathcal{T}^*_{\mathbf{n}}(p^2)$ *, that admits natural extension to an injection* $\Upsilon : A \mapsto \Upsilon_A,\ \mathcal{T}^*_{\mathbf{q}}(p^2) \to \mathcal{T}^*_{\mathbf{n}}(p)$ *, in such a way that* Υ_A *divides* Ψ_A *from the right. Conversely, for any* $\mathcal{M} \in \mathcal{T}^*_{\mathbf{n}}(p)$ *there exists a unique* $A \in \mathcal{T}^*_{\mathbf{q}}(p^2)$ *such that* $\mathcal{M}$ *divides* Ψ_A *from the right. This construction turns the set* $\cup_j E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\,\mathbf{n})$ *of classes of quaternary automorphs into a 2-fold covering of the set* $\cup_i E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q}))$ *of classes of ternary automorphs .*

In view of Eichler's commutation relations (3.5), (4.3), and (4.4), the above construction corresponds to Shimura's lift (5.1) for generic theta-series of ternary positive definite quadratic forms and generalizes the latter in a purely arithmetical way to the case of arbitrary indeterminate (nonsingular) ternary quadratic forms.

Corollary . *With the notation and under the assumptions of the above proposition, let* $\mathbf{q}$ *be positive definite. Then Shimura's lift of the generic theta-series* $\Theta_{\{\mathbf{q}\}}(z)$ *and the generic theta-series* $\Theta_{\{\mathbf{n}\}}(z)$ *of the norm* $\mathbf{n}$ *on the even Clifford subalgebra* $C_0(E, \mathbf{q})$ *have the same eigenvalues* $p+1$ *for all Hecke operators* $T(p)$ *with* $p \not| \det \mathbf{q}$. (See also Theorem 7.3 and Corollary 7.4.)

Defined in this way, the *automorph class lift* (6.28) raises numerous questions which still await solution. Some of the possibilities, including relations that involve associated zeta-functions, will be discussed in Concluding Remarks (Chapter 8).

1.2 Notation and terminology

As usual, the letters $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{C}$ denote the ring of rational integers, the field of rational numbers and the field of complex numbers, respectively. We put $\mathbb{H} = \{z \in \mathbb{C}\ ;\ Im\ z > 0\}$ to be the upper half plane. $\mathbb{A}_n^m$ is the set of all $(m \times n)$–matrices with entries in a set $\mathbb{A}$, $\mathbb{A}^m = \mathbb{A}_1^m$, $\mathbb{A}_n = \mathbb{A}_n^1$. We let $\Lambda^m = GL_m(\mathbb{Z})$ denote the group of all integral invertible matrices of oder m and 1_m stand for the unit matrix of oder m. If M is a matrix, then ${}^tM$ denotes its transposed, $\tilde{M}$ is its adjoint and $|M|$ stands for the absolute value of its determinant (for square matrices M). We write

$$L[M] = {}^tMLM\ ,$$

if the product of matrices on the right makes sense. We consider a quadratic form

$$\mathbf{q}(X) = \sum_{1 \le i \le j \le m} q_{ij} x_i x_j\ , \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}\ ,$$

in m variables with rational integral coefficients q_{ij}. The symmetric matrix

$$Q = (q_{ij}) + {}^t(q_{ij})$$

is called the *matrix* of the form $\mathbf{q}$ and its determinant $\det Q = \det \mathbf{q}$ is the *determinant* of $\mathbf{q}$. A quadratic form $\mathbf{q}$ is *nonsingular* if $\det \mathbf{q} \neq 0$. Clearly,

$$2\mathbf{q}(X) = Q[X]\ .$$

Note that Q is an *even* matrix (i.e., an integral symmetric matrix whose diagonal elements are even). The *level* of $\mathbf{q}$ (and of Q) is defined to be the least positive integer ℓ such that ℓQ^{-1} is even. It should be noted that ℓ and $\det \mathbf{q}$ have the same prime divisors. If $A \in \mathbb{Q}_n^m$ with some $m, n \in \mathbb{N}$, then $\mathbf{q}[A]$ denotes the quadratic form

$$\mathbf{q}'(Y) = \frac{1}{2}Q'[Y] = \mathbf{q}(AY) = \frac{1}{2}Q[AY]\,, \quad Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \,,$$

resulting from $\mathbf{q}$ by the linear change of variables $X = AY$. The matrix A is called a *representation* (over $\mathbb{Q}$) of the form $\mathbf{q}'$ by the form $\mathbf{q}$. In case $A \in \mathbb{Z}_n^m$, we call it an *integral representation* of $\mathbf{q}'$ by $\mathbf{q}$ and denote by

$$R(\mathbf{q}, \mathbf{q}') = \{A \in \mathbb{Z}_n^m \ ; \ \mathbf{q}[A] = \mathbf{q}'\} = \{A \in \mathbb{Z}_n^m \ ; \ Q[A] = Q'\} \ ,$$

the set of all such integral representations. In particular, if $n = 1$ and $\mathbf{q}' = ay^2$ then the set $R(\mathbf{q}, \mathbf{q}')$ coincides with the set $R(\mathbf{q}, a)$ of (integral) representations of the number a by $\mathbf{q}$:

$$R(\mathbf{q}, ay^2) = R(\mathbf{q}, a) = \{X \in \mathbb{Z}^m \ ; \ \mathbf{q}(X) = a\} \ .$$

In case $\mathbf{q} = \mathbf{q}'$ we get $E(\mathbf{q}) = R(\mathbf{q}, \mathbf{q}) \cap \Lambda^m$, the *group of units* of the form $\mathbf{q}$. Subset of $R(\mathbf{q}, \mathbf{q}')$ consisting of matrices whose entries are coprime is denoted by $R^*(\mathbf{q}, \mathbf{q}')$, and its elements are called *primitive (integral) representations of* $\mathbf{q}'$ *by* $\mathbf{q}$. We set

$$r(\mathbf{q}, \mathbf{q}') = |R(\mathbf{q}, \mathbf{q}')| \ , \ r^*(\mathbf{q}, \mathbf{q}') = |R^*(\mathbf{q}, \mathbf{q}')| \ , \ r(\mathbf{q}, a) = |R(\mathbf{q}, a)| \ ,$$
$$e(\mathbf{q}) = |E(\mathbf{q})|$$

to be the corresponding cardinalities. Finally, the abbreviation gcd stands for *greatest common divisor.*

Chapter 2

Isotropic sums

If $\mathbf{q}$ and $\mathbf{q}'$ are integral quadratic forms in the same number of variables with equal determinants, we say that $\mathbf{q}'$ is *similar* to $\mathbf{q}$ if $R(\mathbf{q}, a\mathbf{q}')$ is not empty for some a prime to $\det \mathbf{q}$. The set of all quadratic forms similar to $\mathbf{q}$ is called the *similarity class* of $\mathbf{q}$. The Minkowski reduction theory of quadratic forms (see [3], for example) shows that the similarity class of a nonsingular integral quadratic form in m variables is a finite union

$$\bigcup_{i=1}^{h} \{\mathbf{q}_i[U] \ ; \ U \in GL_m(\mathbb{Z})\} \ ,$$

of mutually disjoint classes of integrally equivalent quadratic forms. (The similarity class may be compared with the *genus* of $\mathbf{q}$. Although in general the two sets are different, both consist of quadratic forms with arithmetical invariants equal to those of $\mathbf{q}$. Moreover, both sets are finite disjoint unions of classes modulo integral equivalence.)

For similar quadratic forms $\mathbf{q}$ and $\mathbf{q}'$ the elements of the set $R(\mathbf{q}, a\mathbf{q}')$ are called *automorphs* (of $\mathbf{q}$ to $\mathbf{q}'$) with *multiplier* a.

LEMMA 2.1. *For any integral nonsingular quadratic forms $\mathbf{q}$ and $\mathbf{q}'$ and for any nonzero number $a \in \mathbb{Z}$ the set $R(\mathbf{q}, a\mathbf{q}')$ of automorphs with multiplier a is a finite union of left cosets modulo $E(\mathbf{q})$.*

Proof. Let m denote the rank of $\mathbf{q}$ and $\mathbf{q}'$ and let Q, Q' be their respective matrices. If $M \in R(\mathbf{q}, a\mathbf{q}')$ then $Q[M] = aQ'$. Considering corresponding determinants we have $|M| = \left(a^m \det \mathbf{q} \,/\, \det \mathbf{q}'\right)^{1/2} = |a|^{m/2} \in \mathbb{Z}$ which means that $R(\mathbf{q}, a\mathbf{q}') \subset \Delta^m\left(|a|^{m/2}\right)$, where

$$\Delta^m(d) = \{D \in \mathbb{Z}_m^m \ ; \ |\det D| = d\} \qquad (2.1)$$

for a positive integer d. We claim that $\Delta^m(d)$ is a finite union of left cosets modulo Λ^m (see Notations). To establish this we note first that according to the theory of elementary divisors (see [3, Lemma 3.2.2]) each double coset $\Lambda^m D \Lambda^m$, $D \in \Delta^m(d)$ has a unique representative of the form $\mathrm{ed}(D) = \mathrm{diag}(d_1, \ldots, d_m)$ with $d_i > 0$, $d_i | d_{i+1}$ and so the cardinality $|\Lambda^m \backslash \Delta^m(d) / \Lambda^m|$ is bounded above by number of factorizations $d = \prod_{i=1}^m d_i,\ d_i > 0,\ d_i | d_{i+1}$, which means that $\Delta^m(d)$ is a finite disjoint union of double cosets modulo Λ^m. Next we note that each of these double cosets is a finite (disjoint) union of left cosets:

$$\Lambda^m D \, \Lambda^m = \bigcup_{D' \in D \cdot \left((D^{-1} \Lambda^m D \,\cap\, \Lambda^m) \backslash \Lambda^m \right)} \Lambda^m D' \,,$$

because $\Lambda^m D U = \Lambda^m D$ with $U \in \Lambda^m$ if and only if $U \in D^{-1} \Lambda^m D \cap \Lambda^m$ and the latter subgroup has finite index in Λ^m. To justify the last claim consider the principle congruence subgroup of level d of Λ^m:

$$\Lambda^m(d) = \{ M \in \Lambda^m \ ; \ M \equiv 1_m \pmod d \} \ .$$

Clearly $\Lambda^m(d)$ has a finite index in Λ^m as the kernel of reduction modulo $d : \Lambda^m \to GL_m(\mathbb{Z}/d\mathbb{Z})$. On the other hand $\Lambda^m(d) \subset D^{-1} \Lambda^m D$ since entry-wise $D \, \Lambda^m(d) \tilde{D} \equiv D \tilde{D} \equiv 0 \pmod d$ and so $D \, \Lambda^m(d) D^{-1} = (\pm d)^{-1} D \, \Lambda^m(d) \tilde{D} \subset \Lambda^m$, here $\tilde{D}$ is the matrix adjoint to D. Thus $D^{-1} \Lambda^m D \cap \Lambda^m$ contains subgroup $\Lambda^m(d)$ of finite index in Λ^m, which means that $D^{-1} \Lambda^m D \cap \Lambda^m$ is itself of finite index in Λ^m. Summing up, we see that $\Delta^m(d)$ is a finite (disjoint) union of double cosets each of which is a finite (disjoint) union of left cosets modulo Λ^m and thus $\Delta^m(d)$ is indeed a finite union of left cosets modulo Λ^m.

It remains to note that $R(\mathbf{q}, a\mathbf{q}') \subset \Delta^m \left(|a|^{m/2} \right)$ is therefore also a finite union of left cosets modulo Λ^m. But each left coset $\Lambda^m M \cap R(\mathbf{q}, a\mathbf{q}')$ consists of a single left coset $E(\mathbf{q}) M$ (if not empty), because if $UM = M' \in R(\mathbf{q}, a\mathbf{q}')$ with $U \in \Lambda^m$ then $Q[U] = Q[M' M^{-1}] = aQ'[M^{-1}] = Q$, i.e. $U \in E(\mathbf{q})$. We conclude that $R(\mathbf{q}, a\mathbf{q}')$ is a finite union of left cosets modulo $E(\mathbf{q})$. □

The above property of automorphs will allow us to construct certain Hecke algebras of orthogonal groups in section 3. Then the obvious inclusion

$$R(\mathbf{q}, a\mathbf{q}') \cdot R(\mathbf{q}', b) \subset R(\mathbf{q}, ab)$$

for any quadratic forms $\mathbf{q}, \mathbf{q}'$ and for any integers a, b (the dot refers to the usual matrix multiplication) will help us to define an action of these Hecke algebras on representations of integers by quadratic forms. In order to prepare for later quantitative investigation of that action, we first need to address the question of inverse inclusion, i.e. we need to factor a given element $K \in R(\mathbf{q}, ab)$ into a product of an automorph $M \in R(\mathbf{q}, a\mathbf{q}')$ and a representation $L \in R(\mathbf{q}', b)$. We also want to find total number of such factorizations. For our purposes it is enough to restrict attention to the case when the automorph multiplier a is a power of a fixed prime p and quadratic forms $\mathbf{q}, \mathbf{q}'$ are similar. Moreover, it appears that consideration of just two automorph multipliers $a = p$ or $a = p^2$ is completely sufficient for all situations (see [2]). The case of quadratic forms in an even number of variables and automorph multiplier p was treated in great detail in [1]. Our first goal is to conduct a similar investigation for the case of quadratic forms in and odd number of variables and automorph multiplier p^2 (it is easy to see that p^2 is the least power of an automorph multiplier possible for quadratic forms in an odd number of variables, see the proof of the Lemma 2.1).

Thus, given $K \in R(\mathbf{q}, p^2 b)$ we seek to find total number of factorizations $K = ML$ with $M \in R(\mathbf{q}, p^2\mathbf{q}')$, $L \in R(\mathbf{q}', b)$, where $\mathbf{q}, \mathbf{q}'$ are similar integral quadratic forms in an odd number of variables $m = 2k + 1 \geq 3$ and p is a prime coprime to $\det \mathbf{q}$. Following general method of investigation of questions of this type developed in [1], we will view a matrix $M \in R(\mathbf{q}, p^2\mathbf{q}')$ as a solution of quadratic congruence

$$\mathbf{q}[M] \equiv 0 \pmod{p^2} ,$$

whose matrix of elementary divisors D_p has a specific form.

Lemma 2.2. *Let $\mathbf{q}, \mathbf{q}'$ be similar integral quadratic forms in an odd number of* *variables $m = 2k+1 \geq 3$ and let p be a prime coprime to $\det \mathbf{q}$. Then*

$$R(\mathbf{q}, p^2\mathbf{q}') = \begin{cases} R^*(\mathbf{q}, p^2\mathbf{q}') & , \textit{if } \mathbf{q} \textit{ and } \mathbf{q}' \textit{ are not integrally equivalent,} \\ R^*(\mathbf{q}, p^2\mathbf{q}') \cup pR(\mathbf{q}, \mathbf{q}') & , \textit{otherwise,} \end{cases}$$

where $R^*(\mathbf{q}, p^2\mathbf{q}')$ is the set of primitive automorphs, $R(\mathbf{q}, \mathbf{q}') \subset \Lambda^m$, and the union on the right hand side is disjoint. Furthermore, the matrix of elementary divisors of an automorph from $pR(\mathbf{q}, \mathbf{q}')$ is equal to $p1_m$ and the matrix of elementary divisors of a primitive automorph has the form

$$D_p = D_p(d) = \begin{pmatrix} 1_d & & \\ & p1_b & \\ & & p^2 1_d \end{pmatrix} \tag{2.2}$$

for some d, $1 \leq d \leq k$, here $k = (m-1)/2$ and $b = m - 2d$.

Proof. Let $M \in R(\mathbf{q}, p^2\mathbf{q}')$ be an automorph and let μ denote the greatest common divisor of its entries. Since $\mathbf{q}[M] = p^2\mathbf{q}'$ then $|\det M| = |M| = p^m$, which implies that $\mu | p$ and so either $\mu = 1$ and $M \in R^*(\mathbf{q}, p^2\mathbf{q}')$ or $\mu = p$ and $p^{-1}M \in R(\mathbf{q}, \mathbf{q}')$. We also note that any elementary divisor of M is a power (at most m^{th}) of p. Next, since $\mathbf{q}$ and $\mathbf{q}'$ are similar, and in particular have equal determinants, then $R(\mathbf{q}, \mathbf{q}') \subset \Lambda^m$ and therefore this set is empty if $\mathbf{q}$ and $\mathbf{q}'$ are not integrally equivalent. It is also clear that any double coset from $\Lambda^m pR(\mathbf{q}, \mathbf{q}')\Lambda^m \subset p\Lambda^m$ coincides with $\Lambda^m p1_m \Lambda^m$. Furthermore, if $M \in R^*(\mathbf{q}, p^2\mathbf{q}')$, then $p^2M^{-1} = (p^2/\det M) \cdot \tilde{M} = (\det \mathbf{q})^{-1}\tilde{Q'}\, {}^tMQ$ is an integral matrix since $\det M$ and $\det \mathbf{q}$ are coprime. Therefore the matrix D_p of elementary divisors of M has the form $\operatorname{diag}(1_{s_0}, p1_{s_1}, p^2 1_{s_2})$ with $s_0 + s_1 + s_2 = m$ and $s_1 + 2s_2 = m$, which leaves us with $s_o = s_2 = d$ and $1 \leq d \leq (m-1)/2$. □

Thus if $M \in R^*(\mathbf{q}, p^2\mathbf{q}')$, then $\mathbf{q}[M] \equiv 0 \pmod{p^2}$ and $M \in \Lambda^m D_p \Lambda^m$ for a matrix D_p of the form (2.2). Next, since at the moment we do not want to distinguish a particular form $\mathbf{q}'$ in its equivalence class $\{\mathbf{q}'[U]\ ;\ U \in \Lambda^m\}$, we will be interested only in different cosets $M\Lambda^m \in \Lambda^m D_p \Lambda^m / \Lambda^m$ (and thus only in cosets $R^*(\mathbf{q}, p^2\mathbf{q}')/E(\mathbf{q}')$ after a choice of particular form $\mathbf{q}'$). Finally, because our interest is in factorizations of a particular column $K \in \mathbb{Z}^m$ such that $\mathbf{q}(K) \equiv 0 \pmod{p^2}$, we will consider only those M which divide from the left such a K. To this end we introduce *isotropic sums* of the form

$$\mathcal{S}_{p^2}(\mathbf{q}, D_p, K) = \sum_{\substack{M \in \Lambda^m D_p \Lambda^m / \Lambda^m \\ \mathbf{q}[M] \equiv 0 \pmod{p^2}\,,\, M|K}} 1\ . \tag{2.3}$$

We will use geometric methods to compute the above sum. The following notions and results will help us to reinterpret it in geometric terms.

Lemma 2.3. *Let δ be a positive integer and p be a rational prime. For a matrix $M \in \mathbb{Z}_n^m$ with $m > n$ the following statements are equivalent:*

i) There exists a primitive matrix $M' \in \mathbb{Z}_n^m$ such that $M' \equiv M \pmod{p^\delta}$.

ii) Columns of M are linearly independent modulo p.

iii) The matrix M can be complemented to a matrix $(MM'') \in \mathbb{Z}_m^m$ such that $(MM'') \equiv U \pmod{p^\delta}$ with $U \in \Lambda^m$.

Proof. First of all, recall that an integer matrix is called *primitive* if and only if the greatest common divisor of its principal minors is equal to 1. Note that if M' is primitive then not all of its principal minors are zero and so its $\operatorname{rank}_{\mathbb{Z}}$ is equal to n. Then $\operatorname{rank}_{(\mathbb{Z}/p^\delta\mathbb{Z})} M = \operatorname{rank}_{(\mathbb{Z}/p^\delta\mathbb{Z})} M' = n$, i.e. columns of M are linearly independent modulo p^δ. It remains to note that for an arbitrary δ, linear independence modulo p^δ is equivalent to linear independence modulo p. Thus *i)* implies *ii)*. Conversely, suppose that columns of M are linearly independent modulo p (and thus modulo p^δ). Then $\operatorname{rank}_{(\mathbb{Z}/p^\delta\mathbb{Z})} M = n$ and using elementary transformations over $\mathbb{Z}/p^\delta\mathbb{Z}$ one can find $A \in \Lambda^m$ such that

$$AM \equiv \begin{pmatrix} a_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_n \\ p^\delta & \dots & p^\delta \\ 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} = L \pmod{p^\delta}$$

with $\prod a_i \not\equiv 0 \pmod{p}$. Moreover, choosing appropriate representatives modulo p^δ one can assume that a_i's are pairwise coprime. Clearly such L is primitive. Then $M' = A^{-1}L$ is congruent to M modulo p^δ and also primitive since multiplication by an invertible matrix preserves primitiveness. (Indeed, using Binet-Cauchy formula, one can see that any principal minor of L has the form

$$\left|(A \cdot M')^{1,\dots,n}_{\gamma_1,\dots,\gamma_n}\right| = \left|(A)^{1,\dots,m}_{\gamma_1,\dots,\gamma_n} \cdot (M')^{1,\dots,n}_{1,\dots,m}\right| = \sum_{1\le\alpha_1<\ldots<\alpha_n\le m} \left|(A)^{\alpha_1,\dots,\alpha_n}_{\gamma_1,\dots,\gamma_n}\right| \cdot \left|(M')^{1,\dots,n}_{\alpha_1,\dots,\alpha_n}\right|$$

i.e. it is an integral linear combination of minors of oder n of M'. Therefore gcd of principal minors of M' divides gcd of those of L which is equal to 1 since L is primitive.) This establishes equivalence of *i)* and *ii)*.

To prove equivalence of *i)* and *iii)* it is enough to show that a matrix $U' \in \mathbb{Z}^m_n$ is primitive if and only if it can be complemented to $U = (U', U'') \in \Lambda^m$. This was done in a much more general setting (for matrices over arbitrary Dedekind rings) in [1, Lemmas 2.3, 2.4 and 2.5]. Here we will present another explanation of this fact for our particular case of integral matrices. If $U' \in \mathbb{Z}^m_n$ can be complemented to $U = (U', U'') \in \Lambda^m$, then there exists $U^{-1} = {}^t({}^tA\,{}^tB)$ with $A \in \mathbb{Z}^n_m, B \in \mathbb{Z}^{m-n}_m$. So we have:

$$U^{-1} \cdot U = \begin{pmatrix} AU' & AU'' \\ BU' & BU'' \end{pmatrix} = 1_m ,$$

in particular $AU' = 1_n$. Applying Binet-Cauchy formula one has:

$$\sum_{1\le\gamma_1<\ldots<\gamma_n\le m} \left|(A)^{\gamma_1,\dots,\gamma_n}_{1,\dots,n}\right| \cdot \left|(U')^{1,\dots,n}_{\gamma_1,\dots,\gamma_n}\right| = \det(A \cdot U') = 1 ,$$

which means that an integral linear combination of principal minors of U' is equal to 1, i.e. their gcd is 1 and U' is primitive.

Conversely, assume first that $n = 1$ and $U' \in \mathbb{Z}^m$ is a primitive column. Using induction on $m \geq 2$ we want to prove that U' can be complemented to an invertible matrix. In the base case $m = 2$ one has $U' = {}^t(u_1, u_2)$ with $\gcd(u_1, u_2) = 1$.

Therefore $xu_1 + yu_2 = 1$ for some $x, y \in \mathbb{Z}$ and then

$$\begin{pmatrix} u_1 & -y \\ u_2 & x \end{pmatrix} \in \Lambda^2$$

as intended. If $m > 2$ and $U' = {}^t(u_1, \ldots, u_m)$ is primitive, then either $u_2 = \ldots = u_m = 0$ and we can take

$$U = \begin{pmatrix} u_1 & \ldots & 0 \\ \vdots & 1_m & \\ 0 & & \end{pmatrix} \in \Lambda^m$$

since $u_1 = \pm 1$, or some of $u_2, \ldots, u_m$ are not zero and by induction hypothesis we can complement the primitive column $V' = {}^t(u_2/d, \ldots, u_m/d) \in \mathbb{Z}^{m-1}$ to an invertible matrix $(V'V'') \in \Lambda^m$, here $d = \gcd(u_2, \ldots, u_m)$. Note that $\gcd(u_1, d) = 1$ as U' is primitive, so $xu_1 + yd = 1$ for some $x, y \in \mathbb{Z}$ and then

$$U = \begin{pmatrix} u_1 & 0 & y \\ dV' & V'' & xV' \end{pmatrix} \in \Lambda^m$$

since $\det U = xu_1(-1)^{m-1} + yd(-1)^{m+1} = \pm 1$. Thus any primitive column can be complemented to an invertible matrix. Next assume that $n > 1$, $U' \in \mathbb{Z}_n^m$ is primitive and ${}^t(u_1, \ldots, u_m)$ is the first column of U' . For any selection $1 \leq i_1 < \ldots < i_n \leq m$, $\gcd(u_{i_1}, \ldots, u_{i_n})$ divides the minor $\left|(U')^{1,\ldots,n}_{i_1,\ldots,i_n}\right|$ and so $\gcd(u_1, \ldots, u_m) = 1$ as gcd of minors of oder n of U' is equal to 1. Therefore $\sum_{i=1}^m x_i u_i = 1$ for some $x_i \in \mathbb{Z}$. The column ${}^t(x_1, \ldots, x_m)$ is primitive, and as we already know it can be complemented to a matrix $X \in \Lambda^m$. Then ${}^tXU'$ is primitive with $({}^tXU')_{11} = 1$. Applying elementary transformations to rows of ${}^tXU'$ we can find matrix $Y \in \Lambda^m$, such that

$$YU' = \begin{pmatrix} 1 & \ldots & * \\ \vdots & V' & \\ 0 & & \end{pmatrix} \in \mathbb{Z}_n^m$$

is again a primitive matrix whose minors of oder n are either 0 (in case the minor does not include the first row), or have the form $\left|(V')^{1,\ldots,n-1}_{i_1,\ldots,i_{n-1}}\right|$, $1 \leq i_1 < \ldots < i_{n-1} \leq m$. The latter implies that gcd of principal minors of V' is 1, i.e. $V' \in \mathbb{Z}^{m-1}_{n-1}$ is also primitive and we can recursively apply the above procedure to it. Continuing in this fashion one can find a matrix $Z \in \Lambda^m$ such that

$$ZU' = \begin{pmatrix} 1 & \dots & * \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix} \in \mathbb{Z}_n^m \ ,$$

then the matrix $W = \left(ZU' \mid {0 \atop 1_{m-n}} \right)$ is clearly invertible and we can take $U = (U', U'') = Z^{-1} \cdot W$ to complement U' to an invertible matrix. □

We will consider quadratic modules of the form

$$V_{p^\delta}(1_m) = \left((\mathbb{Z}/p^\delta \mathbb{Z})^m \, , \, \mathbf{q} \bmod p^\delta \right) \tag{2.4}$$

obtained by reduction modulo p^δ of quadratic module $(\mathbb{Z}^m, \mathbf{q})$ whose Gramm matrix with respect to the standard basis of $\mathbb{Z}^m$ is Q , the matrix of $\mathbf{q}$. For a matrix $M \in \mathbb{Z}_n^m$ we will denote by $V_{p^\delta}(M)$ the quadratic submodule of $\left((\mathbb{Z}/p^\delta \mathbb{Z})^m \, , \, \mathbf{q} \bmod p^\delta \right)$ spanned by the columns of M modulo p^δ .

Lemma 2.4. *Let $D_p = D_p(d)$ be a matrix of the form (2.2) and let $M \in \Lambda^m D_p \Lambda^m$. Then the map $M \mapsto V_{p^2}(M)$ defines a bijection of the set of right cosets $M\Lambda^m \subset \Lambda^m D_p \Lambda^m / \Lambda^m$ to the set of all subgroups of $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^m$ whose invariants are $(\underbrace{p^2, \dots, p^2}_{d} \, , \, \underbrace{p, \dots, p}_{b})$, here $b = m - 2d$.*

Proof. First of all we note that if $M' \in M\Lambda^m$ then clearly $V_{p^2}(M') = V_{p^2}(M)$ as generators of any of these two groups are integral linear combinations of generators of the other. Thus our map is defined coset-wise. Next, let $M = UD_pV$ with $U, V \in \Lambda^m$ and let U_i's denote the columns of U . Then each $V_{p^2}(U_i)$, $1 \le i \le d$ is a cyclic group of oder p^2 and each $V_{p^2}(pU_i)$, $d \le i \le d + b$ is a cyclic group of oder p . (To see this note that if n is the oder of a column $W \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^m$ then $nW \equiv 0 \pmod{p^2}$ and so $W \equiv 0 \pmod{p^2/n}$. But the greatest common divisor of elements of any of U_i's is equal to 1 , since $U \in \Lambda^m$. Thus the oder of $W = U_i$ is p^2 and the oder of $W = pU_i$ is p .) Next we claim that

$$V_{p^2}(M) = V_{p^2}(U_1) \oplus \ldots \oplus V_{p^2}(U_d) \oplus V_{p^2}(pU_{d+1}) \oplus \ldots \oplus V_{p^2}(pU_{d+b}) \ ,$$

i.e. $V_{p^2}(M)$ is a direct sum of d cyclic subgroups of oder p^2 and b cyclic subgroups of oder p . Indeed,

$$V_{p^2}(M) = V_{p^2}(UD_p) = V_{p^2}(U_1, \ldots U_d, pU_{d+1}, \ldots, pU_{d+b}) = \\ V_{p^2}(U_1) + \ldots + V_{p^2}(U_d) + V_{p^2}(pU_{d+1} + \ldots + V_{p^2}(U_{d+b})$$

and we just need to show that the above sum is direct. To see this, consider the following: if

$$\sum_{i=1}^{d} \alpha_i U_i + p \sum_{j=d+1}^{d+b} \alpha_j U_j \ \equiv \ 0 \ (\operatorname{mod} p^2)$$

then $U^{-1} \cdot (U_1, \ldots, U_{d+b}) \cdot {}^t(\alpha_1, \ldots, \alpha_d, p\alpha_{d+1}, \ldots, p\alpha_{d+b}) \ \equiv \ 0 \ (\operatorname{mod} p^2)$, which implies that $p^2 | \alpha_i$ for $1 \leq i \leq d$ and $p | \alpha_j$ for $d \leq j \leq d + b$. Thus the zero of the group can be written only as the sum of zeros of the subgroups, i.e. the sum is indeed direct. Therefore the invariants of $V_{p^2}(M)$ are $(p^2, \ldots, p^2, p, \ldots, p)$.

Conversely, assume that $G \subset \left(\mathbb{Z}/p^2\mathbb{Z}\right)^m$ is a subgroup with this set of invariants, i.e.

$$G = V_{p^2}(K_1) \oplus \ldots \oplus V_{p^2}(K_d) \oplus V_{p^2}(L_1) \oplus \ldots \oplus V_{p^2}(L_b) \ ,$$

where the oder of each K_i is p^2 and the oder of each L_i is p . Since $pL_i \ \equiv \ 0 \ (\operatorname{mod} p^2)$ then $p | L_i$ for $1 \leq i \leq b$. The integral columns $K_1, \ldots, K_d, p^{-1}L_1, \ldots, p^{-1}L_b$ are linearly independent modulo p (because the sum of the cyclic groups generated by K_i's and L_j's is direct). Therefore, according to the Lemma 2.3 there exists a primitive matrix $A \in \mathbb{Z}^m_{d+b}$ such that $A \ \equiv \ K_1, \ldots, K_d, p^{-1}L_1, \ldots, p^{-1}L_b) \ (\operatorname{mod} p^2)$ which can be complemented to an integral invertible matrix $A' \in \Lambda^m$ for which

$$G = V_{p^2}(K_1, \ldots, K_d, L_1, \ldots, L_b) = V_{p^2}(A_1, \ldots, A_d, pA_{d+1}, \ldots A_{d+b}) = V_{p^2}(A'D_p) \ .$$

Thus any $G \subset \left(\mathbb{Z}/p^2\mathbb{Z}\right)^m$ with invariants $(p^2,\dots,p^2,p,\dots,p)$ has the form $V_{p^2}(A'D_p)$ for some $A' \in \Lambda^m$. □

The above Lemma allows us to replace summation over $M \in \Lambda^m D_p \Lambda^m/\Lambda^m$ in (2.3) by summation over different submodules $V_{p^2}(M) \subset \left(\mathbb{Z}/p^2\mathbb{Z}\right)^m$ with $M \in \Lambda^m D_p \Lambda^m$. Furthermore, conditions $\mathbf{q}[M] \equiv 0 \pmod{p^2}$, $M|K$ in (2.3) mean exactly that $V_{p^2}(M)$ should be an isotropic submodule of quadratic module $V_{p^2}(1_m) = \left((\mathbb{Z}/p^2\mathbb{Z})^m, \mathbf{q} \bmod p^2\right)$ containing a fixed vector K. In order to find the total number of such submodules (and thus to compute the isotropic sum (2.3)), we will first determine the total number of bases of certain kind which generate modules of type $V_{p^2}(M)$, $M \in \Lambda^m D_p \Lambda^m$ and then factor this number by the number if different bases generating the same module. We start with exhibiting the bases of $V_{p^2}(M)$ we are interested in. We choose

$$\{U \cdot D_p \;;\; U \in \Lambda^m/(D_p \Lambda^m D_p^{-1} \cap \Lambda^m)\}$$

as a complete system of representatives from classes $M\Lambda^m \in \Lambda^m D_p \Lambda^m/\Lambda^m$ and let U_i, $1 \le i \le m$ denote the columns of matrix a U. Then any isotropic module

$$V_{p^2}(M) = V_{p^2}(UD_p) = V_{p^2}(U_1,\dots,U_d,pU_{d+1},\dots,pU_{d+b}), \text{ where } b = m-2d\ .$$

Using Lemma 2.3 we replace condition $U \in \Lambda^m$ with requirement that $U_1,\dots,U_{d+b}$ should be linearly independent modulo p. Then the condition $\mathbf{q}[M] \equiv \mathbf{q}[UD_p] \equiv 0 \pmod{p^2}$ should be replaced with

$$\begin{cases} {}^tU_iQU_j \equiv 0 \pmod{p^2}, & \text{if } 1 \le i \le j \le d\,, \\ {}^tU_iQU_j \equiv 0 \pmod{p}, & \text{if } 1 \le i \le d \text{ and } d+1 \le j \le d+b\,. \end{cases} \tag{2.5}$$

Conversely, it is easy to see that any (ordered) collection $\{U_1,\dots,U_{d+b}\} \subset (\mathbb{Z}/p^2\mathbb{Z})^d \times (\mathbb{Z}/p\mathbb{Z})^b$ of linearly indepemdent modulo p vectors satisfying (2.5) defines a basis

$$U_1,\dots,U_d,pU_{d+1},\dots,pU_{d+b} \tag{2.6}$$

of an isotropic module of the form $V_{p^2}(M),\ M \in \Lambda^m D_p \Lambda^m$. From now on, when referring to a basis of the form (2.6), we will always assume that vectors $\{U_1, \dots, U_{d+b}\} \subset (\mathbb{Z}/p^2\mathbb{Z})^d \times (\mathbb{Z}/p\mathbb{Z})^b$ are linearly independent modulo p and satisfy (2.5). Let us find the total number of such bases.

Lemma 2.5. *Under the above notations there exist*

$$p^{d(m+b-1)} \cdot \left|GL_b(\mathbb{F}_p)\right| \cdot \prod_{s=0}^{d-1} (p^{2(k-s)} - 1)\,, \ \textit{where}\ \ k = (m-1)/2\ ,$$

different (ordered) bases of the form (2.6).

Proof. We note first that $U_1, \dots, U_d$ should form an *isotropic system* of vectors of the quadratic module $V_{p^2}(1_m)$, see (2.4), i.e. a system of linear independent modulo p vectors spanning an isotropic submodule. In particular they should also form an isotropic system of d vectors in $V_p(1_m)$. The number of isotropic systems in $V_p(1_m)$ consisting of d vectors was computed in [3, Proposition A.2.14] and equals to

$$p^{d(d-1)/2}(p^{2k} - 1)(p^{2(k-1)} - 1) \cdot \ldots \cdot (p^{2(k-d+1)} - 1)\ .$$

It remains to compute in how many ways such a system modulo p can be lifted to an isotropic system in $V_{p^2}(1_m)$. Note that any vector $L \in (\mathbb{Z}/p\mathbb{Z})^m$ splits into p^m different vectors of the form $L + pX$ in $(\mathbb{Z}/p\mathbb{Z})^m$. Therefore, if $\{L_1, \dots, L_d\}$ is an isotropic system in $V_p(1_m)$, then $\{L_1 + pX_1, \dots, L_d + pX_d\}$ would form an isotropic system in $V_{p^2}(1_m)$ if and only if

$${}^t(L_i + pX_i)Q(L_j + pX_j) \equiv {}^tL_iQL_j + p({}^tL_iQX_j + {}^tX_iQL_j) \equiv 0 \pmod{p^2}$$

for $1 \le i \le j \le d$. (We do not worry about linear independence of the vectors because linear independence modulo p^δ is equivalent for any δ to linear independence modulo p , as we already noted in the proof of Lemma 2.3.) The above congruences form a system of $d(d+1)/2$ linear equations (over $\mathbb{F}_p$) with respect to md unknowns – elements of columns X_i . Since columns L_i , $1 \le i \le d$ are linearly independent modulo p , the rank of the matrix of this linear system as well as the rank of its extended matrix is equal to $d(d+1)/2$ and therefore the system has

$$p^{dm-d(d+1)/2} \tag{2.7}$$

solutions in $\mathbb{F}_p$. (Note that this is exactly the number of different isotropic systems in $V_{p^2}(1_m)$ which lie above a fixed isotropic system in $V_p(1_m)$.) We conclude that there exist

$$p^{md-d(d+1)/2} \cdot p^{d(d-1)/2} \cdot \prod_{s=0}^{d-1} (p^{2(k-s)} - 1) = p^{d(m-1)} \cdot \prod_{s=0}^{d-1} (p^{2(k-s)} - 1)$$

different isotropic systems $\{U_1, \ldots, U_d\} \subset V_{p^2}(1_m)$. In how many ways such a system can be extended to an isotropic basis of the form (2.6)? From (2.5) one can see that each U_j, $d \leq j \leq d+b$ should be orthogonal to the linear span of $U_1, \ldots, U_d$, i.e. it should satisfy the following system of linear equations

$$\begin{pmatrix} {}^tU_1Q \\ \vdots \\ {}^tU_dQ \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \equiv 0 \pmod{p}$$

over $\mathbb{F}_p$. The above system has $m-d = d+b$ linear independent (modulo p) solutions. Besides, each of U_i, $1 \leq i \leq d$ is its solution. Therefore the remaining (ordered) set U_i, $d+1 \leq i \leq d+b$ can be chosen in

$$p^{db} \cdot \left|GL_b(\mathbb{F}_p)\right| \tag{2.8}$$

different ways. Multiplying (2.8) by the number of different isotropic systems of d vectors in $V_{p^2}(1_m)$ computed above, we deduce the result of the Lemma. □

Next we need to determine which of the bases in question generate the same isotropic module. Assume that $\{U_1, \ldots, pU_{d+b}\}$ and $\{V_1, \ldots, pV_{d+b}\}$ are two (ordered) bases of the form (2.6) such that $V_{p^2}(U_1, \ldots, pU_{d+b}) = V_{p^2}(V_1, \ldots, pV_{d+b})$. Then

$$(V_1, \ldots, pV_{d+b}) \equiv (U_1, \ldots, pU_{d+b}) \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix} \pmod{p^2},$$

where $A \in \mathbb{Z}_d^d$, $B \in \mathbb{Z}_b^d$, $C \in \mathbb{Z}_d^b$, $D \in \mathbb{Z}_d^d$. Because $(U_1, \ldots, U_{d+b}) \cdot \begin{pmatrix} B \\ pD \end{pmatrix} \equiv 0 \pmod{p}$, then necessarily $B \equiv 0 \pmod{p}$. Since vectors

$$(V_1, \ldots, V_{d+b}) \equiv (U_1, \ldots, U_{d+b}) \cdot \begin{pmatrix} A & p^{-1}B \\ pC & D \end{pmatrix} \pmod{p^2}$$

are linearly independent modulo p, then the system of congruences

$$\begin{pmatrix} A & p^{-1}B \\ pC & D \end{pmatrix} \cdot \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{d+b} \end{pmatrix} \equiv 0 \pmod{p}$$

should have only trivial solution, for which it is necessary and sufficient that

$$\begin{pmatrix} A & p^{-1}B \\ pC & D \end{pmatrix} \in GL_{d+b}(\mathbb{F}_p) \ ,$$

i.e. $A \in GL_d(\mathbb{F}_p)$ and $D \in GL_b(\mathbb{F}_p)$. Therefore two sets of vectors $\{U_1, \ldots, pU_{d+b}\}$ and $\{V_1, \ldots, pV_{d+b}\}$ generate the same isotropic module only if they differ by a matrix from the group

$$\Gamma = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GL_{d+b}(\mathbb{Z}/p^2\mathbb{Z}) \ ; \right.$$
$$\left. A \in GL_d(\mathbb{Z}/p^2\mathbb{Z}), \ D \in GL_b(\mathbb{Z}/p^2\mathbb{Z}), \ B \equiv 0 \pmod{p} \right\} . \qquad (2.9)$$

Clearly the converse is also true. Thus Γ acts transitively on the set of bases of the form (2.6) of an isotropic module of type $V_{p^2}(UD_p)$. Let Γ' denote stabilizer of a basis $(U_1, \ldots, U_d, pU_{d+1}, \ldots, pU_{d+b})$ under this action and let $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma'$, i.e.

$$(U_1, \ldots, U_d, pU_{d+1}, \ldots, pU_{d+b}) \cdot \begin{pmatrix} 1_d - A & B \\ C & 1_b - D \end{pmatrix} \equiv 0 \pmod{p^2} \ .$$

Because U_i's are linearly independent over $\mathbb{F}_p$, the last congruence is equivalent to the set of conditions:

$$A \equiv 1_d \ (\operatorname{mod} p^2)\,,\ B \equiv 0 \ (\operatorname{mod} p^2)\,,\ C \equiv 0 \ (\operatorname{mod} p)\,,\ D \equiv 1_b \ (\operatorname{mod} p)\ .$$

Combining this with (2.9) one can see that the cardinality of Γ modulo the stabilizer Γ' is given by

$$\left|\Gamma/\Gamma'\right| = p^{d(d+2b)} \cdot \left|GL_b(\mathbb{F}_p)\right| \cdot \left|GL_b(\mathbb{F}_p)\right|$$

and this is the number of different bases of form (2.6) generating some fixed isotropic module of the type $V_{p^2}(UD_p)$, $U \in \Lambda^m$. Using Lemma 2.5 we conclude that the number of different isotropic modules of the type we are interested in is equal to

$$\mathcal{S}_{p^2}(\mathbf{q}, D_p, 0) = p^{d(d-1)} \cdot \left|GL_d(\mathbb{F}_p)\right|^{-1} \cdot \prod_{s=0}^{d-1} (p^{2(k-s)} - 1)\ , \tag{2.10}$$

where $k = (m-1)/2$ and $0 \in \mathbb{Z}^m$ is the zero vector. We note also that since the zero vector belongs to any submodule of $V_{p^2}(1_m)$, then $\mathcal{S}_{p^2}(\mathbf{q}, D_p, K) = \mathcal{S}_{p^2}(\mathbf{q}, D_p, 0)$ in case $K \equiv 0 \ (\operatorname{mod} p^2)$, see (2.3).

In order to finish our computation of isotropic sums (2.3), we still need to find the number of isotropic modules of the form $V_{p^2}(UD_p)$, $U \in \Lambda^m$, which contain a fixed nonzero isotropic vector $K \in (\mathbb{Z}/p^2\mathbb{Z})^m$. It will be more convenient to consider two separate cases: either $K \not\equiv 0 \ (\operatorname{mod} p)$, or $K \equiv 0 \ (\operatorname{mod} p)$ but $K \not\equiv 0 \ (\operatorname{mod} p^2)$.

Lemma 2.6. *Under the above notations, assume that $K \not\equiv 0 \ (\operatorname{mod} p)$. Then there exist*

$$\mathcal{S}_{p^2}(\mathbf{q}, D_p, K) = (p^d - 1) \cdot p^{(d-1)^2} \cdot \left|GL_d(\mathbb{F}_p)\right|^{-1} \cdot \prod_{s=1}^{d-1} (p^{2(k-s)} - 1)$$

different isotropic modules of the form $V_{p^2}(UD_p)$, $U \in \Lambda^m$, which contain the vector K.

Proof. If $K \in V_{p^2}(UD_p) = V_{p^2}(U_1, \ldots, pU_{d+b})$ and $K \not\equiv 0 \ (\operatorname{mod} p)$ then this vector can be complemented to a basis $\{V_1, \ldots, K, \ldots, V_d, pV_{d+1}, \ldots, pV_{d+b}\}$ of $V_{p^2}(UD_p)$. As we already know, such a basis differs from $\{U_1, \ldots, pU_{d+b}\}$ only by a matrix from Γ , see (2.9). Moreover, if

$$K \equiv \sum_{i=1}^{d} \gamma_i U_i + p \sum_{j=d+1}^{d+b} \gamma_j U_j \pmod{p^2} , \tag{2.11}$$

then among the first d columns of a matrix from Γ which transforms $\{U_1, \ldots, pU_{d+b}\}$ into $\{V_1, \ldots, K, \ldots, V_d, pV_{d+1}, \ldots, pV_{d+b}\}$ there should be a column of the form

$${}^t(\gamma_1, \ldots, \gamma_d, \gamma'_{d+1}, \ldots, \gamma'_{d+b}) \text{ with } \gamma'_j \equiv \gamma_j \pmod{p} \text{ for } d+1 \le j \le d+b .$$

Since there exist exactly

$$\frac{d}{p^d - 1} \cdot \Big|GL_d(\mathbb{F}_p)\Big| \cdot \Big|GL_b(\mathbb{F}_p)\Big| \cdot p^{d^2+b^2+3db-d-b}$$

different matrices from Γ with this property, then dividing by the oder of the stabilizer $|\Gamma'|$ we deduce that a fixed isotropic module $V_{p^2}(UD_p)$ contains

$$\frac{d}{p^d - 1} \cdot \Big|GL_d(\mathbb{F}_p)\Big| \cdot \Big|GL_b(\mathbb{F}_p)\Big| \cdot p^{d^2+2db-d-b} \tag{2.12}$$

different bases of the form $\{V_1, \ldots, K, \ldots, V_d, pV_{d+1}, \ldots, pV_{d+b}\}$. Now we just need to find the total number of bases of the form (2.6) which contain K among their first d vectors. We will proceed in a fashion similar to the proof of Lemma 2.5: first we compute the number of isotropic systems of d vectors in $(\mathbb{Z}/p^2\mathbb{Z})^m$ containing the column K and then multiply the result by the number of ways such an isotropic system can be extended to an isotropic basis of the form we are interested in (the latter was already computed in the course of proof of Lemma 2.5, see (2.8)).

We already have noted above that any isotropic system modulo p^2 is also an isotropic system modulo p . Therefore we start with computation of the number of isotropic systems of d vectors in $(\mathbb{Z}/p\mathbb{Z})^m$ containing $K \bmod p$. We use induction: assume that $X_1, \ldots, X_{n-1} \in (\mathbb{Z}/p\mathbb{Z})^m$ form an isotropic system. In how many ways it can be complemented to an isotropic system of n vectors? Since $X_1, \ldots, X_{n-1}$ form a basis of the isotropic subspace $V_p(X_1, \ldots, X_n)$ of nondegenerate quadratic space $V_p(1_m)$ then there exist vectors $X'_1, \dots X'_{n-1} \in V_p(1_m)$ such that each pair X_i, X'_i, $1 \le i \le i-1$, is hyperbolic, i.e. vectors X_i, X'_i are isotropic, linear independent and ${}^tX_iQX'_i \equiv 1 \pmod p$, see [3, proposition A.2.12] or [9, Satz 2.24]. Then the spaces $V_p(X_i, X'_i)$, $1 \le i \le n-1$ are (nondegenerate) hyperbolic planes and

$$V_p(1_m) = V_p(X_1, X'_1) \oplus V_p(X_{n-1}, X'_{n-1}) \oplus V$$

is a direct sum of pairwise orthogonal subspaces. Therefore a vector $Y \in V_p(1_m)$ can be isotropic and orthogonal to each of X_i's only if

$$Y \equiv \sum_{i=1}^{n-1} \alpha_i X_i + v \pmod p ,$$

where v is an isotropic vector of V. The vectors $X_1, \dots, X_{n-1}, Y$ will be linearly independent only if $v \not\equiv 0 \pmod p$. Since V is nondegenerate and $\dim V = m - 2(n-1)$ then the number of nonzero isotropic vectors in it equals to $p^{m-2n+1} - 1$ (see [3, Proposition A.2.14]). Thus the vector X_n complementing $\{X_1, \dots, X_{n-1}\}$ to an isotropic system of n vectors can be chosen in $p^{n-1}(p^{m-2n+1} - 1)$ ways. Using induction on n we conclude that a fixed isotropic vector $K \not\equiv 0 \pmod p$ can be complemented to

$$p^{d(d-1)/2} \cdot \prod_{s=1}^{d-1} (p^{2(k-s)-1})$$

different (ordered) isotropic systems $\{K, X_2, \dots, X_d\} \subset V_p(1_m)$. Clearly, the total number of isotropic systems of d vectors in $V_p(1_m)$ containing K is d times that. Next we need to lift our solution to $V_{p^2}(1_m)$ keeping in mind that K is fixed modulo p^2. Since any vector $X \in (\mathbb{Z}/p\mathbb{Z})^m$ splits in $(\mathbb{Z}/p^2\mathbb{Z})^m$ into p^m different vectors $X + pY$, $Y \in (\mathbb{Z}/p\mathbb{Z})^m$, we need to look for isotropic systems of the form

$$\{X_1 + pY_1, \dots, K = X_i, \dots, X_d + pY_d\} \subset (\mathbb{Z}/p^2\mathbb{Z})^m .$$

Such a system will be isotropic modulo p^2 if and only if

$$\begin{aligned} {}^tKQY_j &\equiv -\frac{1}{p}{}^tX_jQK \pmod{p} \quad ; \\ {}^tX_sQY_j + {}^tX_jQY_s &\equiv -\frac{1}{p}{}^tX_sQX_j \pmod{p} \text{ for } s, j \neq i \quad . \end{aligned}$$

This is a system of $(d-1)(d+2)/2$ linear nonhomogeneous equations in $m(d-1)$ variables (elements of columns U_j, $j \neq i$) over $\mathbb{F}_p$. Since the columns $X_1, \ldots, X_i = K, \ldots, X_d$ are linearly independent modulo p, so are the columns $QX_1, \ldots, QX_d$, and therefore the rank of the matrix of the above system as well as the rank of its extended matrix is equal to $(d-1)(d+2)/2$, which implies that it has $p^{(d-1)(m-(d+2)/2)}$ solutions. We conclude that $V_{p^2}(1_m)$ contains

$$dp^{(m-1)(d-1)} \cdot \prod_{s=1}^{d-1} (p^{2(k-s)})$$

different isotropic systems of d vectors one of which is K. According to (2.8), each of these systems can be complemented to a basis of the form (2.6) of some isotropic module $V_{p^2}(UD_p)$, $U \in \Lambda^m$ in $p^{db}|GL_b(\mathbb{F}_p)|$ different ways. Multiplying the last two numbers we get the total number of bases of the form (2.6) which contain K among their first d vectors. Dividing the latter by (2.12) we finally deduce the result of the Lemma. □

It remains to consider the isotropic sum $\mathcal{S}_{p^2}(\mathbf{q}, D_p, K)$ in the case when $K \equiv 0 \pmod{p}$ but $K \not\equiv 0 \pmod{p^2}$. Let $K \in V_{p^2}(UD_p)$ for some $U = (U_1, \ldots, U_m) \in \Lambda^m$ and assume (2.11). Then ${}^t(\gamma_1, \ldots, \gamma_d) \equiv 0 \pmod{p}$ and we are faced with two possibilities:

(i) $\quad (\gamma_{d+1}, \ldots, \gamma_{d+b}) \not\equiv 0 \pmod{p}$;

(ii) $\quad (\gamma_{d+1}, \ldots, \gamma_{d+b}) \equiv 0 \pmod{p}$, $(\gamma_1, \ldots, \gamma_d) \not\equiv 0 \pmod{p^2}$.

In the first case the column ${}^t(\gamma_1, \ldots, \gamma_{d+b})$ can be complemented to a matrix from Γ, see (2.9), and in the second case this is impossible. Note that the type of representation (2.11) of the vector K does not depend on the choice of basis of $V_{p^2}(UD_p)$.

Therefore, if $K \equiv 0 \pmod p$ but $K \not\equiv 0 \pmod{p^2}$ then there exists two distinct types of isotropic modules which contain K : in modules of the first type there exist a basis of the form $\{V_1, \dots, V_d, pV_{d+1}, \dots, K, \dots, pV_{d+b}\}$, but in the modules of the second type there are no such bases. In the two following Lemmas we compute the number of isotropic modules of each these two types.

Lemma 2.7. *Under the above notations, assume that* $K \equiv 0 \pmod p$ *but* $K \not\equiv 0 \pmod{p^2}$. *Then the number of isotropic modules of the form* $V_{p^2}(UD_p)$, $U \in \Lambda^m$, *for which (2.11) implies case* (i) *above, is equal to*

$$\begin{cases} \frac{\eta_p}{p^d} \cdot (p^k - \chi_{\mathbf{q}}\varepsilon_p)(p^{k-d} + \chi_{\mathbf{q}}\varepsilon_p) \prod\limits_{s=1}^{d-1} (p^{2(k-s)} - 1) \,, & \textit{if } \mathbf{q}(p^{-1}K) \not\equiv 0 \pmod p \,, \\ \eta_p \cdot \prod\limits_{s=1}^{d} (p^{2(k-s)} - 1) \,, & \textit{if } \mathbf{q}(p^{-1}K) \equiv 0 \pmod p \,. \end{cases}$$

Here $\eta_p = p^{(d^2+b-1)}(p^b - 1)|GL_{b-1}(\mathbb{F}_p)||GL_d(\mathbb{F}_p)|^{-1}|GL_b(\mathbb{F}_p)|^{-1}$, *the quadratic character* $\chi_{\mathbf{q}} = \chi_{\mathbf{q}}(p)$ *of the form* $\mathbf{q}$ *is defined via (3.4) below, and* $\varepsilon_p = \varepsilon_p\left(\mathbf{q}(p^{-1}K)\right)$ *is given by the Legendre symbol*

$$\varepsilon_p(a) = \left(\frac{2a}{p}\right) \,, \; a \in \mathbb{N} \,. \tag{2.13}$$

Proof. As we already noted above, if an isotropic module satisfies conditions of the Lemma, then it has a basis of the form $\{V_1, \dots, V_d, pV_{d+1}, \dots, K, \dots, pV_{d+b}\}$. Thus we need to compute the total number of bases of the form (2.6) which have K among the last b vectors, and then divide it by the number of such bases generating the same isotropic module. The latter is equal to the number of matrices in Γ (2.9) one of whose last b columns is fixed modulo $(\mathbb{Z}/p^2\mathbb{Z})^d \times (\mathbb{Z}/p\mathbb{Z})^b$ divided by the oder of stabilizer $|\Gamma'|$:

$$b(p^b - 1)^{-1}|GL_d(F_p)| \cdot |GL_B(\mathbb{F}_p)|p^{d^2+2db-d} \,. \tag{2.14}$$

Now we need to compute the total number of bases of the form (2.6) which have K

among their last b vectors. Assume first that $\mathbf{q}(p^{-1}K) \not\equiv 0 \pmod{p}$, i.e. the column $p^{-1}K$ is anisotropic. Then $V_p(1_m) = V_p(p^{-1}K) \oplus V$, where V is an orthogonal complement of $V_p(p^{-1}K)$ (see [9, Satz 1.15]). The module V is nondegenerate and its dimension $\dim V = m-1$ is even. Any vector orthogonal to $p^{-1}K$ belongs to V and in particular is linear independent (modulo p) with $p^{-1}K$. Therefore first d columns of a basis of the type in question should form an isotropic system in V. According to [3, Proposition A.2.14], the number of such systems is equal to

$$p^{d(d-1)/2}(p^k - \chi_{\mathbf{q}}(p)\varepsilon_p)(p^{k-d} + \chi_{\mathbf{q}}(p)\varepsilon_p)\prod_{s=1}^{d-1}(p^{2(k-s)}-1)\,, \tag{2.15}$$

where $\varepsilon_p = \varepsilon_p\left(\mathbf{q}(p^{-1}K)\right)$ is the Legendre symbol (2.13). Each of these systems splits into $p^{dm-d(d+1)/2}$ different isotropic systems in $V_{p^2}(1_m)$, see (2.7), any of which can be chosen as first d columns of a basis of the form (2.6). Now we need to find in how many ways an isotropic system $U_1, \ldots, U_d, K$ can be complemented by $b-1$ vectors from $(\mathbb{F}_p)^m$ to form a basis of the type (2.6). Orthogonality conditions imply that elements of each of the complementary columns should satisfy the following system of linear homogeneous equations:

$$\begin{pmatrix} {}^tU_1Q \\ \vdots \\ {}^tU_dQ \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \equiv 0 \pmod{p}$$

This system of d equations in m variables over $\mathbb{F}_p$ has $d+b$ linear independent modulo p solutions which can be chosen in the form $\vartheta = (U_1, \ldots, U_d, p^{-1}K, V_2, \ldots, V_b)$. Any other set of linear independent solutions has the form $\vartheta \cdot M$ with $M \in GL_{d+b}(\mathbb{F}_p)$. Among such matrices M there are exactly $b|GL_{b-1}(\mathbb{F}_p)|p^{(b-1)(d-1)}$ matrices which do not change the first d columns of the basis and leave $p^{-1}K$ intact (possibly changing its position). And this is exactly the number of different (modulo p) sets of vectors $pU_{d+1}, \ldots, K, \ldots, pU_{d+b}$ which complement a given isotropic system $U_1, \ldots, U_d$ to a basis of the form (2.6). Therefore, multiplying this number by (2.15) times (2.7) and dividing by (2.14), we deduce the statement of the Lemma in the case when

$\mathbf{q}(p^{-1}K) \not\equiv 0 \pmod{p}$.

We turn to the case of an isotropic vector $p^{-1}K \in \mathbb{Z}^m$. Assume that $\mathbf{q}(p^{-1}K) \equiv 0 \pmod{p}$ and let $V \subset V_p(1_m)$ again denote its orthogonal complement. We see that $\dim V = m-1$ again but now V is degenerate: it has nontrivial radical $\operatorname{rad} V = V_p(p^{-1}K)$. Nevertheless, $V = \operatorname{rad} V \oplus W$, where W is a nondegenerate subspace orthogonal to $\operatorname{rad} V$. The first d vectors of a basis of the type we are interested in should form an isotropic system in V. Suppose that $U_1, \dots, U_d$ is a set of elements of V. Each of these vectors can be uniquely represented in the form

$$U_i \equiv \alpha_i p^{-1}K + w_i \pmod{p}, \ \text{ where } \alpha_i \in \mathbb{F}_p,\, w_i \in W\,.$$

Naturally, each of U_i's is orthogonal to $p^{-1}K$. They will be isotropic an pairwise orthogonal if and only if ${}^t w_i Q w_j \equiv 0 \pmod{p}$ for $1 \le i \le j \le d$. Furthermore, the columns $U_1, \dots, U_d, p^{-1}K$ will be linearly independent (modulo p) if and only if $w_1, \dots, w_d \in W$ are linearly independent. We conclude that $U_1, \dots, U_d$ will be an isotropic system if and only if $w_1, \dots, w_d$ form an isotropic system. The number of isotropic systems of d vectors in W is equal to

$$p^{d(d-1)/2} \cdot \prod_{s=1}^{d} (p^{2(k-s)} - 1)$$

(see [3, Proposition A.2.14]). Multiplying this number by p^d we get the number of different isotropic systems in V consisting of d vectors linear independent with $p^{-1}K$. The rest of the computations completely coincide with the case of anisotropic $p^{-1}K$ and lead to the result stated in the Lemma. □

Let us turn to the second case.

Lemma 2.8. *Under the above notations, assume that $K \equiv 0 \pmod{p}$ but $K \not\equiv 0 \pmod{p^2}$. Then the number of isotropic modules of the form $V_{p^2}(UD_p)$, $U \in \Lambda^m$*

for which (2.11) implies case (ii) above is equal to

$$\begin{cases} 0\,, & \text{if } \mathbf{q}(p^{-1}K) \not\equiv 0 \pmod{p}\,, \\ p^{(d-1)^2}|GL_{d-1}(\mathbb{F}_p)|^{-1}\cdot\prod_{s=1}^{d-1}(p^{2(k-s)}-1)\,, & \text{if } \mathbf{q}(p^{-1}K) \equiv 0 \pmod{p}\,. \end{cases}$$

Proof. Let $\{U_1, \ldots, pU_{d+b}\}$ be a basis of the form (2.6). Assume that (2.11) holds for some column ${}^t(\gamma_1, \ldots, \gamma_{d+b})$. Then the conditions $(\gamma_1, \ldots, \gamma_{d+b}) \equiv 0 \pmod{p}$ and $(\gamma_1, \ldots, \gamma_d) \not\equiv 0 \pmod{p^2}$ will hold if and only if $p^{-1}K \in V_p(U_1, \ldots, U_d)$. But the subspace $V_p(U_1, \ldots, U_d) \subset V_p(1_m)$ is isotropic, therefore the column ${}^t(\gamma_1, \ldots, \gamma_{d+b})$ satisfies (ii) if and only $\mathbf{q}(p^{-1}K) \equiv 0 \pmod{p}$, otherwise there exist no isotropic modules which would satisfy the conditions of the Lemma. This proves its first case.

Suppose now that $\mathbf{q}(p^{-1}K) \equiv 0 \pmod{p}$. In order to find the number of isotropic modules we are interested in, we need to divide the number of different bases of the form (2.6) for which $p^{-1}K \in V_p(U_1, \ldots, U_d)$ by the number of different bases of the form (2.6) which generate the same isotropic module, i.e. by $|\Gamma/\Gamma'|$ computed above, see discussion immediately following (2.9). Next, the number of bases of the form (2.6) with the property in question is equal to the product of the number of different isotropic systems $\{U_1, \ldots, U_d\} \in V_{p^2}(1_m)$ for which $p^{-1}K \in V_p(U_1, \ldots, U_d)$ multiplied by the number of ways an isotropic system of d vectors can be complemented to a basis of the form (2.6), i.e. by $p^{db}\cdot|GL_b(\mathbb{F}_p)|$, see (2.8). According to (2.7), the number of isotropic systems $\{U_1, \ldots, U_d\} \in V_{p^2}(1_m)$ for which $p^{-1}K \in V_p(U_1, \ldots, U_d)$ is equal in turn to the number of isotropic systems $\{U_1, \ldots, U_d\} \in V_p(1_m)$ for which $p^{-1}K \in V_p(U_1, \ldots, U_d)$ times $p^{dm-d(d+1)/2}$. Thus it remains to find the number of isotropic systems $\{U_1, \ldots, U_d\} \in V_p(1_m)$ for which $p^{-1}K \in V_p(U_1, \ldots, U_d)$. Since $K \not\equiv 0 \pmod{p^2}$ then $p^{-1}K$ is a nonzero isotropic vector of $V_p(1_m)$, and so if $p^{-1}K \in V_p(U_1, \ldots, U_d)$ then $p^{-1}K$ can be complemented to a basis of $V_p(U_1, \ldots, U_d)$. Therefore the number of different isotropic systems in $V_p(1_m)$ with the property in question is equal to the number of isotropic systems of d vectors in $V_p(1_m)$ containing the vector $p^{-1}K$ (which was computed in the proof of Lemma 2.6) divided by $dp^{d-1}\cdot|GL_{d-1}(\mathbb{F}_p)|$, i.e. by the number of such isotropic systems generating the same module, and multiplied by $|GL_d(\mathbb{F}_p)|$, i.e. by the number of different bases of a d-dimensional linear space over $\mathbb{F}_p$. This finishes the proof of the Lemma. □

Combining the results of Lemmas 2.4 and 2.6–2.8 along with formulas (2.3) and (2.10), we deduce the following Theorem:

THEOREM 2.9. *Let* $\mathbf{q}$ *be an arbitrary integral nonsingular quadratic form in an odd number of variables* $m = 2k+1 \geq 3$, *and let* p *be a rational prime not dividing the determinant* $\det \mathbf{q}$ *of the form* $\mathbf{q}$. *Then for each integral column* $K \in \mathbb{Z}^m$ *such that* $\mathbf{q}[K] \equiv 0 \pmod{p^2}$ *the value of the isotropic sum (2.3) is given by*

$$\mathcal{S}_{p^2}(\mathbf{q}, D_p(d), K) = \\ \alpha_p(d) \cdot \Big\{ 1 + \Big(\varepsilon_p \chi_{\mathbf{q}}(p) p^{k-1} + \kappa_p(d) \Big) \cdot \delta_{(p^{-1}K)} + p^{m-2} \cdot \delta_{(p^{-2}K)} \Big\} \quad , \qquad (2.16)$$

where $D_p(d)$, $1 \leq d \leq k$ *is a matrix of the form (2.2),* $\varepsilon_p = \varepsilon_p \left(\mathbf{q}(p^{-1}K) \right)$ *is given by the Legendre symbol (2.13), the character* $\chi_{\mathbf{q}}(p)$ *of the form* $\mathbf{q}$ *is defined via (3.4),* $\delta_{(X)}$ *is the generalized Kronecker symbol (3.7) and*

$$\alpha_p(d) = p^{1-d} \cdot \prod_{s=1}^{d-1} (p^{2(k-s)} - 1)/(1 - p^{-s}) \quad ,$$
$$\kappa_p(d) = \frac{p^{m-2} - p^{d-1}}{p^d - 1} - 1 \quad .$$

Proof. It is well-known that for $n \geq 1$

$$|GL_n(\mathbb{F}_p)| = \prod_{s=0}^{n-1} (p^n - p^s) = p^{n^2} \cdot \prod_{s=1}^{n} (1 - p^{-s}) \; .$$

We also put $|GL_0(\mathbb{F}_p)| = 1$ and note that $|GL_{n-1}(\mathbb{F}_p)|^{-1} \cdot |GL_n(\mathbb{F}_p)| = p^{n-1} \cdot (p^n - 1)$. Assume that $K \not\equiv 0 \pmod{p}$, then according to Lemma 2.6

$$\mathcal{S}_{p^2}(\mathbf{q}, D_p(d), K) = \frac{p^{(d-1)^2 - d^2}(p^d - 1)}{1 - p^{-d}} \cdot \prod_{s=1}^{d-1} \frac{p^{2(k-s)} - 1}{1 - p^{-s}} = \alpha_p(d) \; ,$$

which coincides with the right-hand side of (2.16) for such K since $\delta_{(p^{-1}K)}$ and $\delta_{(p^{-2}K)}$ are both equal to 0 in this case. Next, assume that $K \equiv 0 \pmod{p}$ but $K \not\equiv 0 \pmod{p^2}$. Combining results of Lemmas 2.7, 2.8 and employing a rather straightforward calculation one can see that $\mathcal{S}_{p^2}(\mathbf{q}, D_p(d), K)$ is equal to

$$(p^d-1)^{-1}(p^k-\varepsilon_p\chi_{\mathbf{q}}(p))(p^{k-d}+\varepsilon_p\chi_{\mathbf{q}}(p)) \cdot \prod_{s=1}^{d-1}(p^{2(k-s)}-1)/(1-p^{-s}) \ ,$$

if $\mathbf{q}(p^{-1}K) \not\equiv 0 \pmod{p}$ and

$$(p^d-1)^{-1}(p^{a+b-1}-1) \cdot \prod_{s=1}^{d-1}(p^{2(k-s)}-1)/(1-p^{-s}) \ ,$$

if $\mathbf{q}(p^{-1}K) \equiv 0 \pmod{p}$. Note that in the latter case the symbol $\varepsilon_p = \varepsilon_p\left(\mathbf{q}(p^{-1}K)\right)$ in (2.13) is equal to zero and that otherwise $\varepsilon_p = \pm 1$. Therefore

$$\begin{aligned} &\mathcal{S}_{p^2}(\mathbf{q}, D_p(d), K) = \\ &(p^d-1)^{-1} \cdot \left(p^{d+b-1}-1+\varepsilon_p\chi_{\mathbf{q}}(p)p^k(1-p^{-d})\right) \cdot \prod_{s=1}^{d-1}(p^{2(k-s)}-1)/(1-p^{-s}) = \\ &\qquad \alpha_p(d) \cdot \left\{1+\varepsilon_p\chi_{\mathbf{q}}(p)p^{k-1}+\kappa_p(d)\right\} \end{aligned}$$

which coincides with the right-hand side of (2.16) in the case when $K \equiv 0 \pmod{p}$, $K \not\equiv 0 \pmod{p^2}$. Finally, if $K \equiv 0 \pmod{p^2}$ then $\varepsilon_p = 0$ and, using (2.10) we have

$$\mathcal{S}_{p^2}(\mathbf{q}, D_p(d), K) = \alpha_p(d) \cdot p^{d-1} \cdot (p^{2k}-1)/(p^d-1) \ ,$$

which coincides with the right-hand side of (2.16) for such K. □

Summing up the equalities (2.16) over d ranging from 1 to $k = (m-1)/2$ we immediately deuce the following

Corollary 2.10. *Under the notations and assumptions of Theorem 2.8,*

$$\sum_{d=1}^{k} \mathcal{S}_{p^2}(\mathbf{q}, D_p(d), K) =$$

$$c_p \cdot \left\{ 1 + \left(\varepsilon_p \chi_{\mathbf{q}}(p) p^{k-1} + c_p^{-1} \beta_p \right) \cdot \delta_{(p^{-1}K)} + p^{m-2} \cdot \delta_{(p^{-2}K)} \right\} ,$$

where $c_p = c_p(\mathbf{q})$ and $\beta_p = \beta_p(\mathbf{q})$ are given by (3.3).

We have finished computation of the isotropic sums of type (2.3). In order to apply the results of Theorem 2.9 and Corollary 2.10 to investigation of multiplicative arithmetic of integral representations by quadratic form $\mathbf{q}$, we need to rewrite the isotropic sums in a slightly different terms. Recall that the Minkowski reduction theory of quadratic forms (see [3] for example) shows that the similarity class of a nonsingular integral quadratic form in m variables is a finite union of mutually disjoint classes of integrally equivalent quadratic forms. Let us fix a complete system

$$\{\mathbf{q}_1, \ldots, \mathbf{q}_h\}$$

of representatives of different equivalence classes contained in the similarity class of $\mathbf{q}$. Then the isotropic sum (2.3) can be rewritten as follows. The condition $\mathbf{q}[M] \equiv 0 \pmod{p^2}$ means that $\mathbf{q}[M] = p^2\mathbf{q}'$, where $\mathbf{q}'$ is an integral quadratic form in m variables. Since $\det M = \det D_p = p^m$ then $\det \mathbf{q}' = \det \mathbf{q}$ and thus quadratic form $\mathbf{q}'$ is similar to $\mathbf{q}$. Since M is defined only modulo right multiplication by Λ^m, we can replace $\mathbf{q}'$ by any (integrally) equivalent form $\mathbf{q}'[U]$, $U \in \Lambda^m$. In particular we can assume that $\mathbf{q}[M] = p^2\mathbf{q}_i$ for exactly one of $\mathbf{q}_i$'s, $1 \leq i \leq h$ and $M \in \left(R(\mathbf{q}, p^2\mathbf{q}_i) \cap \Lambda^m D_p(d) \Lambda^m\right)/\Lambda^m$ for some d. Furthermore, if $M, MU \in R(\mathbf{q}, p^2\mathbf{q}_i) \cap \Lambda^m D_p(d)\Lambda^m$ where $U \in \Lambda^m$ then $U \in R(\mathbf{q}_i, \mathbf{q}_i) = E(\mathbf{q}_i)$ and so $M \in R(\mathbf{q}, p^2\mathbf{q}_i)/E(\mathbf{q}_i) \cap \Lambda^m D_p(d)\Lambda^m$. Therefore

$$\mathcal{S}_{p^2}(\mathbf{q}, D_p(d), K) = \sum_{i=1}^{h} \sum_{\substack{M \in \left(R(\mathbf{q}, p^2\mathbf{q}_i) \cap \Lambda^m D_p(d)\Lambda^m\right)/E(\mathbf{q}_i) \\ M|K}} 1 . \tag{2.17}$$

Next we note that according to the Lemma 2.2 the set of primitive automorphs $R^*(\mathbf{q}, p^2\mathbf{q}_i)$ is a disjoint union

$$R^*(\mathbf{q}, p^2\mathbf{q}_i) = \bigcup_{1 \le d \le (m-1)/2} \Big(R(\mathbf{q}, p^2\mathbf{q}_i) \cap \lambda^m D_p(d) \Lambda^m \Big) \ .$$

Therefore summing both sides of (2.17) over d ranging from 1 to $(m-1)/2$ and applying Corollary 2.10 we deduce the following Theorem:

Theorem 2.11. *Let $\mathbf{q}$ be an arbitrary integral nonsingular quadratic form in an odd number of variables $m = 2k+1 \ge 3$, and let p be a rational prime not dividing the determinant $\det \mathbf{q}$ of the form $\mathbf{q}$. Let $\{\mathbf{q}_1, \dots, \mathbf{q}_h\}$ be a complete system of representatives of different equivalence classes contained in the similarity class of $\mathbf{q}$. Then for each integral column $K \in \mathbb{Z}^m$ such that $\mathbf{q}[K] \equiv 0 \pmod{p^2}$ we have*

$$\sum_{i=1}^{h} \sum_{\substack{M \in R^*(\mathbf{q}, p^2\mathbf{q}_i)/E(\mathbf{q}_i) \\ M|K}} 1 =$$

$$c_p \cdot \Big\{ 1 + \Big(\varepsilon_p \chi_{\mathbf{q}}(p) p^{k-1} + c_p^{-1}\beta_p \Big) \cdot \delta_{(p^{-1}K)} + p^{m-2} \cdot \delta_{(p^{-2}K)} \Big\} \ , \qquad (2.18)$$

where the symbol $\varepsilon_p = \varepsilon_p \Big(\mathbf{q}(p^{-1}K) \Big)$ is defined in (2.13), $\chi_{\mathbf{q}}(p)$ is the character (3.4), $\delta_{(X)}$ is the generalized Kronecker symbol (3.7) and $c_p = c_p(\mathbf{q}), \beta_p = \beta_p(\mathbf{q})$ are given by (3.3).

Chapter 3

Action of Hecke operators on theta-series

If $\mathbf{q}$ is positive definite, the numbers $r(\mathbf{q}, n)$ are finite, and we can consider the theta-series

$$\Theta(z, \mathbf{q}) = \sum_{X \in \mathbb{Z}^m} e^{2\pi i z \mathbf{q}(X)} = \sum_{n \geq 0} r(\mathbf{q}, n) e^{2\pi i n z} \ , \ z \in \mathbb{H} \ ,$$

and show that it is a (classical) modular form of weight $m/2$ and some character with respect to a certain congruence subgroup (see, for example [3, Theorem 2.2.2]). In general, theta-series are not eigenfunctions of Hecke operators, but the spaces spanned by theta-series that come from a fixed similitude class of quadratic forms are invariant under the action of Hecke operators. The fundamental discovery of M. Eichler [6] is that in this situation the corresponding eigenmatrices ("Anzahlmatrizen" in Eichler's terminology) are purely arithmetical and can be defined without any reference to modular forms. (The same phenomenon occurs in the case of Siegel modular forms of arbitrary degree, as was shown by E. Freitag [7] and A. Andrianov [3].)

More specifically, let $\{\mathbf{q}_1, \ldots, \mathbf{q}_h\}$ be a full system of representatives of different equivalence classes of the similarity class of $\mathbf{q}$ and let p be a prime number not dividing $\det \mathbf{q}$, then

$$\Theta(z, \mathbf{q}) \mid_{\frac{m}{2}} T(p) = c_p^{-1} \cdot \sum_{1 \leq j \leq h} \frac{r^*(\mathbf{q}, p\mathbf{q}_j)}{e(\mathbf{q}_j)} \Theta(z, \mathbf{q}_j) \ , \tag{3.1}$$

if m (the number of variables of $\mathbf{q}$) is even and

$$\Theta(z, \mathbf{q}) \mid_{\frac{m}{2}} T(p^2) = c_p^{-1} \cdot \Big(\sum_{1 \leq j \leq h} \frac{r^*(\mathbf{q}, p^2\mathbf{q}_j)}{e(\mathbf{q}_j)} \Theta(z, \mathbf{q}_j) - \beta_p \Theta(z, \mathbf{q}) \Big) \ , \tag{3.2}$$

if m is odd.

Here we set

$$c_p = c_p(\mathbf{q}) = \begin{cases} 1 & \text{if } m = 2\ , \\ \prod\limits_{i=0}^{k-2} (1 + \chi_{\mathbf{q}}(p)p^i) & \text{if } m = 2k > 2\ , \\ \sum\limits_{a=1}^{k} \prod\limits_{i=1}^{a-1} \frac{p^{2(k-i)}-1}{1-p^{-i}} \cdot p^{1-a} & \text{if } m = 2k+1 \geq 3\ , \end{cases} \tag{3.3}$$

$$\beta_p = \beta_p(\mathbf{q}) = \sum_{a=1}^{k} \Big(\prod_{i=1}^{a-1} \frac{p^{2(k-i)} - 1}{1 - p^{-i}} \cdot \frac{p^{m-2} - p^{a-1}(p+1) + 1}{p^{a-1}(p^a - 1)} \Big)\ ,$$

and the quadratic character $\chi_{\mathbf{q}}(p)$ is given by the Legendre symbol

$$\chi_{\mathbf{q}}(p) = \Big(\frac{(-1)^k \det \mathbf{q}}{p} \Big)\ . \tag{3.4}$$

A detailed proof of formula (3.1) for the action of Hecke operators $T(p)$ on theta-series of integral weight can be found in [3, Chapter 5] and specifically in Theorem 5.2.5 there. The second formula (3.2) for the action of Hecke operators $T(p^2)$ on theta-series of half-integral weight easily follows from combination of [12, Theorem 1.7] and Theorem 2.11 above:

Proof of Formula (3.2). Assume that $\mathbf{q}$ is a positive definite (integral) quadratic form in an odd number of variables $m = 2k+1 \geq 3$. Then using [12, Theorem 1.7] we have

$$\Theta(z, \mathbf{q}) \mid_{\frac{m}{2}} T(p^2) = \\ \sum_{n \geq 0} \left\{ r(\mathbf{q}, p^2 n) + \chi_q(p) \left(\frac{2n}{p} \right) p^{k-1} r(\mathbf{q}, n) + p^{m-2} r(\mathbf{q}, \frac{n}{p^2}) \right\} e^{2\pi i n z}\ ,$$

where we understand that $r(\mathbf{q}, n/p^2) = 0$ if $p^2 \not| \, n$. On the other hand, summing up both sides of (2.18) over $K \in R^*(\mathbf{q}, p^2 n)$ for some $n \in \mathbb{N} \cup \{0\}$, we conclude that the sum

$$\sum_{i=1}^{h} \sum_{K \in R(\mathbf{q}, p^2 n)} \sum_{\substack{M \in R^*(\mathbf{q}, p^2 \mathbf{q}_i)/E(\mathbf{q}_i) \\ M | K}} 1 = \sum_{i=1}^{h} \sum_{\substack{M \in R^*(\mathbf{q}, p^2 \mathbf{q}_i) \\ L \in R(\mathbf{q}_i, n)}} \frac{1}{e(\mathbf{q}_i)}$$

on the left-hand side of the resulting identity is equal to

$$\sum_{i=1}^{h} \frac{r^*(\mathbf{q}, p^2\mathbf{q}_i)}{e(\mathbf{q}_i)} \cdot r(\mathbf{q}_i, n)$$

and also coincides with the expression on the right-hand side:

$$\sum_{K\in R(\mathbf{q},p^2n)} c_p \cdot \left\{1 + \left(\varepsilon_p(n)\chi_{\mathbf{q}}(p)p^{k-1} + c_p^{-1}\beta_p\right) \cdot \delta_{(p^{-1}K)} + p^{m-2} \cdot \delta_{(p^{-2}K)}\right\} =$$
$$c_p \cdot \left\{r(\mathbf{q}, p^2n) + \left(\varepsilon_p(n)\chi_{\mathbf{q}}(p)p^{k-1} + c_p^{-1}\beta_p\right) r(\mathbf{q}, n) + p^{m-2} r(\mathbf{q}, n/p^2)\right\} \ .$$

Thus

$$c_p^{-1} \cdot \left(\sum_{i=1}^{h} \frac{r^*(\mathbf{q}, p^2\mathbf{q}_i)}{e(\mathbf{q}_i)} r(\mathbf{q}_i, n) - \beta_p r(\mathbf{q}, n)\right)$$

coincides with the n^{th} Fourier coefficient of $\Theta(z, \mathbf{q})|_{\frac{m}{2}} T(p^2)$, and on the other hand it is equal to the n^{th} Fourier coefficient of the series on the right-hand side of (3.2). This finishes the proof of (3.2) because of the uniqueness of Fourier decomposition. □

It can easily be seen that in the case of an odd number of variables the formulas are not as nice as when m is even. (Unfortunately, this feature is typical.) Since we can substitute for $\mathbf{q}$ any of $\mathbf{q}_i$, $1 \le i \le h$, the above formulas lead to the so-called Eichler commutation relation:

$$\begin{pmatrix} \vdots \\ \frac{\Theta(z,\mathbf{q}_i)}{e(\mathbf{q}_i)} \\ \vdots \end{pmatrix} \Big|_{\frac{m}{2}} T(p^\iota) = c_p^{-1} \cdot \left(\mathfrak{t}^*(p^\iota) - \beta_p \delta_{(\frac{m+1}{2})} 1_h\right) \cdot \begin{pmatrix} \vdots \\ \frac{\Theta(z,\mathbf{q}_j)}{e(\mathbf{q}_j)} \\ \vdots \end{pmatrix} \quad , \tag{3.5}$$

where

$$\iota = \begin{cases} 1 & \text{if } m = 2k \text{ is even,} \\ 2 & \text{if } m = 2k+1 \text{ is odd,} \end{cases}$$

the square matrix

$$\mathfrak{t}^*(p^\iota) = \mathfrak{t}^*_{\mathbf{q}}(p^\iota) = \Big(\frac{r^*(\mathbf{q}_i, p^\iota \mathbf{q}_j)}{e(\mathbf{q}_i)}\Big) \tag{3.6}$$

of oder h is the Eichler's “Anzahlmatrix” (with multiplier p^ι), and δ is the generalized

Kronecker symbol defined by

$$\delta_{(X)} = \begin{cases} 1 & \text{if } X \text{ is an integral matrix,} \\ 0 & \text{if } X \text{ is not an integral matrix.} \end{cases} \tag{3.7}$$

Finally, following C. L. Siegel, we can consider the *generic* theta-series

$$\Theta_{\{\mathbf{q}\}}(z) = \sum_{j=1}^{h} e^{-1}(\mathbf{q}_j)\Theta(z, \mathbf{q}_j)$$

and show that for $p \nmid \det \mathbf{q}$ it is an eigenfunction of the corresponding Hecke operators $T(p^\iota)$ with eigenvalues $c_p^{-1}(\sum_j \frac{r^*(\mathbf{q}, p^\iota \mathbf{q}_j)}{e(\mathbf{q}_j)} - (\iota - 1)\beta_p)$, ι is either 1 or 2 depending on the parity of m. In case m is even and $\det \mathbf{q} = 1$ the generic theta-series is proportional to the Eisenstein series of weight $\frac{m}{2}$. (This implies the famous Siegel theorem on mean numbers of integral representations in the case of quadratic forms of determinant 1 , see, for example [3, Exercise 5.1.18].)

The above formulas together with remarkable multiplicative properties of corresponding Hecke algebras (see [3]) reveal multiplicative relations between the Fourier coefficients of the theta-series, which are best expresses in terms of associated zeta-functions:

$$\sum_{(n, \det \mathbf{q})=1} \frac{\bar{\mathfrak{r}}(na)}{n^s} = \prod_{p \nmid \det \mathbf{q}} \Big(\frac{1}{1 - c_p^{-1}\bar{\mathfrak{t}}^*(p)p^{-s} + \chi_{\mathbf{q}}(p)p^{k-1-2s}}\Big) \cdot \bar{\mathfrak{r}}(a) \tag{3.8}$$

if $m = 2k$ is even and a is any nonzero integer, or

$$\sum_{(n, \det \mathbf{q})=1} \frac{\bar{\mathfrak{r}}(n^2 a)}{n^s} = \prod_{p \nmid \det \mathbf{q}} \Big(\frac{1 - \chi_{\mathbf{q}}(p)(\frac{2a}{p})p^{k-1-s}}{1 - c_p^{-1}(\bar{\mathfrak{t}}^*(p^2) - \beta_p)p^{-s} + p^{m-2-2s}}\Big) \cdot \bar{\mathfrak{r}}(a) \tag{3.9}$$

if $m = 2k + 1 \geq 3$ is odd and a is a square-free integer.

For $\bar{\mathfrak{r}}(n)$ we can substitute either the column-vector ${}^t(\ldots, \frac{r(\mathbf{q}_j, n)}{e(\mathbf{q}_j)}, \ldots)$ or the mean number $\sum_{j=1}^{h} \frac{r(\mathbf{q}_j, n)}{e(\mathbf{q}_j)}$. The first case corresponds to the Fourier coefficients of the vector-valued modular form ${}^t(\ldots, \frac{\Theta(z, \mathbf{q}_j)}{e(\mathbf{q}_j)}, \ldots)$, and the second to the Fourier coefficients of the generic theta-series $\Theta_{\{\mathbf{q}\}}(z)$. Then $\bar{\mathfrak{t}}^*(p^\iota)$ stands either for Eichler's matrix (3.6) or for the average $\sum_{j=1}^{h} \frac{r^*(\mathbf{q}_j,p^\iota \mathbf{q})}{e(\mathbf{q}_j)}$. In any case the formulas (3.8) and (3.9) give us explicit expressions of multiplicative relations among the numbers $r(\mathbf{q}, n)$ of integral representations of integers by quadratic forms. The well-known formula (3.8) easily follows from (3.5) and [3, Exercise 4.3.6], for example. A proof of the formula (3.9) follows below.

Proof of Formula (3.9). Let $\bar{\mathfrak{r}}(n) = {}^t(\ldots, \frac{r(\mathbf{q}_j,n)}{e(\mathbf{q}_j)}, \ldots)$ and let $\bar{\mathfrak{t}}^*(p^2)$ be Eichler's matrix (3.6). Substituting quadratic form $\mathbf{q}_j$, $1 \le j \le h$ (from the full system of representatives $\{\mathbf{q}_1, \ldots, \mathbf{q}_h\}$) in place of $\mathbf{q}$ in (2.18), dividing both sides by $e(\mathbf{q}_j)$ and summing up over $K \in R^*(\mathbf{q}_j, p^2 n)$ in the same way we did for the proof of (3.2), we conclude that

$$c_p^{-1} \cdot \sum_{i=1}^{h} \frac{r^*(\mathbf{q}_j, p^2\mathbf{q}_i)}{e(\mathbf{q}_j)} \cdot \frac{r(\mathbf{q}_i, n)}{e(\mathbf{q}_i)} =$$
$$\left\{ r(\mathbf{q}_j, p^2 n) + \left(\varepsilon_p(n)\chi_{\mathbf{q}}(p)p^{k-1} + c_p^{-1}\beta_p\right) r(\mathbf{q}_j, n) + p^{m-2} r(\mathbf{q}_j, n/p^2) \right\} ,$$

for any j, $1 \le j \le h$ and any $n \in \mathbb{N} \cup 0$. In matrix notations:

$$c_p^{-1} \cdot \bar{\mathfrak{t}}^*(p^2) \cdot \bar{\mathfrak{r}}(n) = \bar{\mathfrak{r}}(p^2 n) + \left(\varepsilon_p(n)\chi_{\mathbf{q}}(p)p^{k-1} + c_p^{-1}\beta_p\right) \cdot \mathfrak{r}(n) + p^{m-2} \cdot \mathfrak{r}(n/p^2) \ .$$

The last equality implies the following identities for the following formal power series in t with coefficients in $\mathbb{Q}^h$:

$$\left(1_h - c_p^{-1}(\bar{\mathfrak{t}}^*(p^2) - \beta_p)t + p^{m-2}t^2\right) \cdot \sum_{\delta \ge 0} \bar{\mathfrak{r}}(p^{2\delta}a)t^\delta =$$
$$\bar{\mathfrak{r}}(a) + \left(\bar{\mathfrak{r}}(p^2 a) - c_p^{-1}(\bar{\mathfrak{t}}^*(p^2) - \beta_p)\bar{\mathfrak{r}}(a)\right) +$$
$$\sum_{\delta \ge 2} \left\{ \bar{\mathfrak{r}}(p^{2\delta}a) - c_p^{-1}(\bar{\mathfrak{t}}^*(p^2) - \beta_p)\bar{\mathfrak{r}}(p^{2(\delta-1)}a) + p^{m-2}\bar{\mathfrak{r}}(p^{2(\delta-2)}a) \right\} t^\delta =$$
$$\left(1_h - \varepsilon_p(a)\chi_{\mathbf{q}}(p)p^{k-1}t\right) \cdot \bar{\mathfrak{r}}(a) ,$$

where a is an arbitrary integer not divisible by p^2 . Define formal power series in t

with coefficients in $\mathbb{Z}_h^h$ by

$$\sum_{\delta\geq 0} \hat{\mathfrak{t}}_a^*(p^{2\delta})t^\delta = \frac{1_h - \varepsilon_p(a)\chi_{\mathbf{q}}(p)p^{k-1}t}{1_h - c_p^{-1}(\bar{\mathfrak{t}}^*(p^2) - \beta_p)t + p^{m-2}t^2} \ ,$$

in other words

$$\begin{cases} \hat{\mathfrak{t}}_a^*(1) & = & 1_h \ , \\ \hat{\mathfrak{t}}_a^*(p^2) & = & \left(c_p^{-1}(\bar{\mathfrak{t}}^*(p^2)\beta_p) - \varepsilon_p(a)\chi_{\mathbf{q}}(p)p^{k-1}\right) \cdot 1_h \ , \\ \hat{\mathfrak{t}}_a^*(p^{2\delta}) & = & c_p^{-1}(\bar{\mathfrak{t}}^*(p^2) - \beta_p)\hat{\mathfrak{t}}_a^*(()p^{2(\delta-1)}) - p^{m-2}\hat{\mathfrak{t}}_a^*(p^{2(\delta-2)}) \, , \text{ for } \delta \geq 2 \ . \end{cases}$$

Then formally

$$\sum_{\delta\geq 0} \bar{\mathfrak{r}}(p^{2\delta}a)t^\delta = \sum_{\delta\geq 0} \hat{\mathfrak{t}}_a^*(p^{2\delta})t^\delta \cdot \bar{\mathfrak{r}}(a)$$

and so $\bar{\mathfrak{r}}(p^{2\delta}a) = \hat{\mathfrak{t}}_a^*(p^{2\delta}) \cdot \bar{\mathfrak{r}}(a)$ for $\delta \geq 0$ and a not divisible by p^2. Define

$$\hat{\mathfrak{t}}_a^*(n^2) = \prod_{s=1}^{l} \hat{\mathfrak{t}}_a^*(p_s^{2\delta_s}) \, , \text{ if } \ n = p_1^{\delta_1} \cdot \ldots \cdot p_l^{\delta_l} \ ,$$

here p_j's are distinct prime factors of n and δ_j's are the corresponding orders. The definition does not depend on the oder of the factors. (To see this it is enough to note that according to [4, Lemmas 3.3–3.6], Eichler matrices $\bar{\mathfrak{t}}^*(p^2)$, $\bar{\mathfrak{t}}^*(u^2)$ commute for different primes p, u not dividing $\det \mathbf{q}$.) We also claim that $\bar{\mathfrak{r}}(n^2a) = \hat{\mathfrak{t}}_a^*(n^2) \cdot \bar{\mathfrak{r}}(a)$ for any integer n coprime to $\det \mathbf{q}$, and any integer a not divisible by the square of any prime factor of n. Indeed, let $n = p_1^{\delta_1} \cdot \ldots \cdot p_l^{\delta_l}$ be coprime to $\det \mathbf{q}$. We will use induction on l to justify our claim. If $l = 1$ then the statement is obvious because of the definition of $\hat{\mathfrak{t}}_a^*(n^2) = \hat{\mathfrak{t}}_a^*(p_1^{2\delta_1})$. Assume now that if b is a product of powers of $p_1, \ldots, p_{l-1}$ then $\bar{\mathfrak{r}}(b^2a)\hat{\mathfrak{t}}_a^*(b^2) \cdot \bar{\mathfrak{r}}(a)$ for any a not divisible by p_i^2, i ranging from 1 to $l-1$. Fix an integer a not divisible by any of p_i^2, $1 \leq i \leq l$, then

$$\bar{\mathfrak{r}}(n^2a) = \bar{\mathfrak{r}}(\textstyle\prod_{i=1}^{l-1} p_i^{2\delta_i} \cdot p_l^{2\delta_l}a) = \hat{\mathfrak{t}}^*_{(p_l^{2\delta_l}a)}(\textstyle\prod_{i=1}^{l-1} p_i^{2\delta_i}) \cdot \bar{\mathfrak{r}}(p_l^{2\delta_l}a) =$$
$$\hat{\mathfrak{t}}_a^*(\textstyle\prod_{i=1}^{l-1} p_i^{2\delta_i}) \cdot \hat{\mathfrak{t}}_a^*(p_l^{2\delta_l}) \cdot \bar{\mathfrak{r}}(a) = \hat{\mathfrak{t}}_a^*(n^2) \cdot \bar{\mathfrak{r}}(a) \ ,$$

since $\hat{\mathfrak{t}}^*_{(u^2a)}(p^2) = \hat{\mathfrak{t}}^*_a(p^2)$ if u and p are coprime. By induction on l we conclude that $\bar{\mathfrak{r}}(n^2a)\hat{\mathfrak{t}}^*_a(n^2)\cdot\bar{\mathfrak{r}}(a)$ for any integer n coprime to $\det\mathbf{q}$ and any integer a not divisible by the square of a prime factor of n (in particular for any square-free integer a). Combining the above equalities we deduce the following identities for the formal zeta-functions:

$$\sum_{(n,\det\mathbf{q})=1}\frac{\bar{\mathfrak{r}}(n^2a)}{n^s} = \sum_{(n,\det\mathbf{q})=1}\frac{\hat{\mathfrak{t}}^*_a(n^2)}{n^s}\cdot\bar{\mathfrak{r}}(a) = \prod_{p\not|\det\mathbf{q}}\Big(\sum_{\delta\geq 0}\frac{\hat{\mathfrak{t}}^*_a(p^{2\delta})}{p^{s\delta}}\Big)\cdot\bar{\mathfrak{r}}(a) =$$

$$\prod_{p\not|\det\mathbf{q}}\Big(\frac{1-\chi_{\mathbf{q}}(p)(\frac{2a}{p})p^{k-1-s}}{1-c_p^{-1}(\mathfrak{t}^*(p^2)-\beta_p)p^{-s}+p^{m-2-2s}}\Big)\cdot\bar{\mathfrak{r}}(a)$$

for any square-free integer a which finishes the proof of (3.9) for the case of column-vectors $\bar{\mathfrak{r}}(n) = {}^t(\ldots,\frac{r(\mathbf{q}_j,n)}{e(\mathbf{q}_j)},\ldots)$. Proof of (3.9) for the case of the mean numbers $\sum_j r(\mathbf{q}_j,n)/e(\mathbf{q}_j)$ proceeds in a similar fashion. One just needs to multiply both sides of the matrix equalities above by the row $(1,\ldots,1)$ of length h and observe that

$$(1,\ldots,1)\cdot\left(\frac{r^*(\mathbf{q}_i,p^l\mathbf{q}_j)}{e(\mathbf{q}_i)}\right) = \Big(c_p(1+p^{m-2})+\beta_p\Big)\cdot(1,\ldots,1)$$

according to comparison of the 0th Fourier coefficients in (3.2). □

We also note that the zeta-functions on the right hand side of (3.8) are closely related to Epstein's zeta-functions

$$\zeta(s,\mathbf{q}_j) = \sum_{n\geq 1}\frac{r(\mathbf{q}_j,n)}{n^s}\ , \tag{3.10}$$

which are Mellin transforms of the corresponding theta-series $\Theta(z,\mathbf{q}_j)$ and, therefore, have good analytic properties (they admit meromorphic continuation on the entire s-plane and obey standard functional equation, for more details see [8], [12] or exercises in [3, Section 4.3.1]).

Chapter 4
Matrix Hecke rings of orthogonal groups

For a long time it was somewhat of a mystery that the numbers $r(\mathbf{q}, n)$ of integral solutions of certain quadratic equations have general multiplicative properties even though no similar relations between the solutions themselves were known. (The sole exception to this rule was the case of the so-called composition of quadratic forms. Then the integral representations can be interpreted as elements of certain arithmetical rings and the multiplicative structure of these rings is reflected in relations among these representations. A classical example of this phenomenon is the Gauss theory of binary quadratic forms. Unfortunately, by a theorem of Hurwitz, there is no composition unless the number of variables is equal to $1, 2, 4$ or 8.)

In [1] A. Andrianov developed Shimura's construction of abstract matrix Hecke algebras (see [11]) specifically for the case of orthogonal groups, and introduced *automorph class rings*. The latter play the role of Hecke operators acting directly on the sets of solutions of quadratic Diophantine equations. The basic idea behind this action is that

$$R(\mathbf{q}, a\mathbf{q}') \cdot R(\mathbf{q}', b\mathbf{q}'') \subset R(\mathbf{q}, ab\mathbf{q}'')$$

for any integral quadratic forms $\mathbf{q}\,, \mathbf{q}', \mathbf{q}''$ and for any integers a, b (the dot refers to usual matrix multiplication). This purely algebraic approach revealed existence of general multiplicative relations between automorphs $R(\mathbf{q}, n\mathbf{q}')$ and representations $R(\mathbf{q}, n)$ of integers by quadratic forms. Remarkably, these relations can be expressed in terms of associated zeta-functions in the form almost identical to (3.8) and (3.9). In fact, the latter formulas for numbers of representations turn out to be immediate consequences of the former relations between representations themselves! This suggests the existence of some correlation between rings of Hecke operators for symplectic and for orthogonal groups.

Let us examine the construction in some detail. For an integral nonsingular quadratic form $\mathbf{q}$ in m variables, we fix a complete system $\{\mathbf{q}_1, \dots, \mathbf{q}_h\}$ of representatives of equivalence classes that are included in the similarity class of $\mathbf{q}$. Consider free $\mathbb{Z}$-modules $\mathbb{A}_{ij}$, $1 \le i, j \le h$, generated by the double cosets

$$\{E(\mathbf{q}_i)AE(\mathbf{q}_j)\ ,\ \text{where } A \in E(\mathbf{q}_i)\backslash \bigcup_{a\in\mathbb{N}} R(\mathbf{q}_i, a\mathbf{q}_j)/E(\mathbf{q}_j)\}\ .$$

Since any double coset of the above type is a finite disjoint union of left cosets modulo $E(\mathbf{q}_i)$, we shall write elements of $\mathbb{A}_{ij}$ as finite linear combinations with integral coefficients of (formal) symbols $<A>$ that bijectively correspond to left cosets $E(\mathbf{q}_i)A\ ,\ A \in E(\mathbf{q}_i)\backslash \bigcup_{a\in\mathbb{N}} R(\mathbf{q}_i, a\mathbf{q}_j)$. Note that elements of $\mathbb{A}_{ij}$ are invariant under the right multiplication by matrices belonging to $E(\mathbf{q}_j)$. Together with obvious inclusion

$$R(\mathbf{q}_i, a\mathbf{q}_j) \cdot R(\mathbf{q}_j, b\mathbf{q}_k) \subset R(\mathbf{q}_i, ab\mathbf{q}_k)$$

this allows us to define natural multiplication

$$\mathbb{A}_{ij} \times \mathbb{A}_{jk} \longrightarrow \mathbb{A}_{ik}\ ,$$
$$\sum_\alpha a_\alpha <A_\alpha> \cdot \sum_\beta b_\beta <B_\beta> = \sum_{\alpha,\beta} a_\alpha b_\beta <A_\alpha B_\beta>\ .$$

Finally, we introduce the ring of $(h \times h)$ matrices

$$\mathbb{A} = \mathbb{A}_{\{\mathbf{q}\}} = \{(A_{ij})\ ;\ A_{ij} \in \mathbb{A}_{ij}\ ,\ 1 \le i, j \le h\}\ ,$$

which is the *automorph class ring* (over $\mathbb{Z}$) of the form $\mathbf{q}$. Sometimes it is more convenient to consider $\mathbb{A} \otimes \mathbb{Q}$, the automorph class ring over $\mathbb{Q}$.

The automorph counterparts of the classical Hecke operators $T(p^\iota)$ (ι is 1 or 2 depending on the parity of m) are elements of the form

$$\mathfrak{T}^*(p^\iota) = \mathfrak{T}^*_{\mathbf{q}}(p^\iota) = \left(\mathfrak{T}^*_{ij}(p^\iota)\right),\ \text{where } \mathfrak{T}^*_{ij}(p^\iota) = \sum_{D\in E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^\iota\mathbf{q}_j)} <D>\ . \qquad (4.1)$$

Note that these matrices are close relatives of Eichler's "Anzahlmatrizen" (3.6).

Next we should define an action of $\mathbb{A}$ on the integral representations by the forms $\mathbf{q}_1, \ldots, \mathbf{q}_h$. The idea is based on the natural inclusion: $R(\mathbf{q}_i, n\mathbf{q}_j) \cdot R(\mathbf{q}_j, a) \subset R(\mathbf{q}_i, na)$. In order to suite our formalism we introduce column-vectors of length h :

$$\mathfrak{R}(a) = \mathfrak{R}_{\mathbf{q}}(a) = \begin{pmatrix} \vdots \\ \mathfrak{R}_j(a) \\ \vdots \end{pmatrix}, \text{ where } \mathfrak{R}_j(a) = \sum_{L \in E(\mathbf{q}_j) \backslash R(\mathbf{q}_j, a)} \mu_{\mathbf{q}_j}^{-1}(L) \cdot <L> , \quad (4.2)$$

which encode all orbits modulo $E(\mathbf{q}_j)$ of integral representations of a by the forms $\mathbf{q}_j$. Here $\mu_{\mathbf{q}_j}(L)$ is a suitably normalized measure of the stabilizer $E_L(\mathbf{q}_j) = \{U \in E(\mathbf{q}_j) \ ; \ UL = L\}$. The vectors of type (4.2) can be thought of as elements of $\mathbb{Q}$-module $\mathbb{D} = \mathbb{D}_{\mathbf{q}} = \mathbb{D}_1 \times \ldots \times \mathbb{D}_h$ whose j^{th} component $\mathbb{D}_j$ is a free $\mathbb{Q}$-module generated by (formal) symbols $< L >$ that are in one-to-one correspondence with orbits $E(\mathbf{q}_j)L$ in $E(\mathbf{q}_j)\backslash\mathbb{Z}^m$.

In this notation an automorph analog of Eichler's commutation relation (3.5) take the form:

$$\mathfrak{R}(pa) + \chi_{\mathbf{q}}(p)p^{k-1}[p]\mathfrak{R}(a/p) \ = \ c_p^{-1}\mathfrak{T}^*(p)\mathfrak{R}(a) \quad (4.3)$$

if $m = 2k$, or

$$\mathfrak{R}(p^2a) + \chi_{\mathbf{q}}(p)p^{k-1}\Big(\frac{2a}{p}\Big)[p]\mathfrak{R}(a) + p^{m-2}[p^2]\mathfrak{R}(a/p^2) \ = \ c_p^{-1}\Big(\mathfrak{T}^*(p^2) - \beta_p 1_h\Big)\mathfrak{R}(a) \quad (4.4)$$

if $m = 2k+1 \geq 3$. Here p is a prime number coprime to $\det \mathbf{q}$, a is a positive integer, and $[p^\iota] = diag(<p^\iota 1_m>, \ldots, <p^\iota 1_m>) \in \mathbb{A}$ are simple elements of the automorph class ring that are responsible for nonprimitive automorphs. The automorph class theory formalism was initially developed in [1], where the original proof of the formula (4.3) can be found (see [1, section 1, formula (1.18)]. The formula (4.4) was proved in [4, Theorem 3.1] (for the case of positive-definite quadratic forms) and in [5, formula (2.8)] for the case of arbitrary nonsingular forms.

The above formulas relating sets of representations $R(\mathbf{q}, p^\iota a)$ and $R(\mathbf{q}, a)$ immediately imply similar relations between the numbers $r(\mathbf{q}, p^\iota a)$ and $r(\mathbf{q}, a)$ of representations. Namely, consider two " coefficient" homomorphisms π:

$$\mathbb{A} \longrightarrow \mathbb{M}_h(\mathbb{Z}) \quad \text{or} \quad \mathbb{D} \longrightarrow \mathbb{Z}^h$$

defined entry-wise by

$$\pi : \sum_\alpha a_\alpha < A_\alpha > \longmapsto \sum_\alpha a_\alpha$$

for a corresponding finite formal linear combination of "orbits" $<\cdot>$. For example,

$$\pi\Big(\mathfrak{T}^*_{\mathbf{q}}(p^\iota)\Big) = \mathfrak{t}^*_{\mathbf{q}}(p^\iota) = \Big(|E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^\iota \mathbf{q}_j)|\Big)$$

is Eichler's "Anzahlmatrix" (3.6). In case $\mathbf{q}$ is positive definite all sets of representations under consideration are finite, in particular

$$\pi\Big(\mathfrak{R}_{\mathbf{q}}(n)\Big) = \mathfrak{r}_{\mathbf{q}}(n) = \begin{pmatrix} \vdots \\ \frac{r(\mathbf{q}_j,n)}{e(\mathbf{q}_j)} \\ \vdots \end{pmatrix}$$

is the n^{th} Fourier coefficient of the vector modular form ${}^t(\ldots, \frac{\Theta(z,\mathbf{q}_j)}{e(\mathbf{q}_j)}, \ldots)$. Then application of the homomorphisms π to (4.3) and (4.4) leads directly to Eichler's identities (3.5) written in terms of the Fourier coefficients of the corresponding theta-series. Furthermore, the automorph class ring $\mathbb{A}$ itself has good multiplicative properties (as could be expected of an arbitrary Hecke algebra). Combining these properties with (4.3) or (4.4) we deduce Euler product expansions of (formal) zeta-functions

$$\sum_{(n,\det \mathbf{q})=1} \frac{\mathfrak{R}(n)}{n^s} \qquad \text{or} \qquad \sum_{(n,\det \mathbf{q})=1} \frac{\mathfrak{R}(n^2 a)}{n^s}$$

very similar to Euler products (3.8) or (3.9) respectively (for exact formulas and their detailed proofs see [1, formula (1.19)] and [5, formula (1.13) with Theorem 1.1]). This method also provides an alternative proof of identities (3.8), (3.9) themselves via appropriate application of the "coefficient" homomorphisms π. It should be emphasized here once again that all of the above considerations are purely algebraic and remain valid for any nondegenerate quadratic form over a Dedekind domain. (For an extensive account of multiplicative properties of general automorph class rings and of Euler products of associated formal zeta-functions the reader is referred to [1],[5] and especially to [2].)

Chapter 5

Shimura's lift for theta-series

In [12] G. Shimura showed that if a cusp form $f(z) = \sum_{n\geq 1} c(n)\exp(2\pi inz)$ of weight $m/2$ (where $m = 2k+1 \geq 3$) is a common eigenfunction for all Hecke operators $T(p^2)$, then the zeta-function $\sum_{n\geq 1} c(n^2a)/n^s$ has Euler product decomposition of type (3.9) for every square-free positive integer a (it suffices to replace $\bar{\mathfrak{r}}(\cdot)$ by $c(\cdot)$ and $c_p^{-1}(\bar{\mathfrak{t}}^*(p^2) - \beta_p)$ by the corresponding eigenvalues of Hecke operators). Comparing the denominators of the local factors in (3.8) and (3.9),we can observe their striking similarity. Indeed, Shimura used the Weil criterion to prove that the zeta-function

$$\Big(\sum_{n\geq 1} \frac{\chi_f(n)(\frac{a}{n})n^{k-1}}{n^s}\Big) \cdot \Big(\sum_{n\geq 1} \frac{c(n^2a)}{n^s}\Big) \tag{5.1}$$

defined by the Euler product of denominators of local factors of $\sum_{n\geq 1} c(n^2a)/n^s$ is the Mellin transform of a modular form $f^{(a)}(z)$ of integral weight $m-1 = 2k$ (see [12, Main theorem]). The form $c^{-1}(a)\cdot f^{(a)}(z)$ is independent of a and is called *Shimura's lift* of $f(z)$. In what follows we shall use this name for $f^{(a)}(z)$ as well.

P. Ponomarev in [10] investigated the lift for theta-series $\Theta(z, \mathbf{q})$ of certain ternary positive definite quadratic forms. In general, theta-series are neither cusp forms nor Hecke eigenforms but it is still possible to consider the lift $\Theta^{(a)}(z, \mathbf{q})$ defined for an integer a via product of type (5.1). As the reader already expects, in order to get a complete picture we should work not with an individual quadratic form $\mathbf{q}$ but rather with a complete system

$$\{\mathbf{q}_1, \ldots, \mathbf{q}_h\} \tag{5.2}$$

of representatives of different equivalence classes of the similarity class of $\mathbf{q}$. Employing particular case where $m = 3$ of Eichler's commutation relation (3.5) P. Ponomarev showed that

$$\Theta^{(a)}(z,\mathbf{q}_k) = \sum_{j=1}^{h}\Big(r(\mathbf{q}_j,a)\cdot\sum_{n\geq 0}\pi_{kj}(n^2)\,e^{2\pi inz}\Big)\ ,\ 1\leq k\leq h\ ,$$

where each $\sum_{n\geq 0}\pi_{kj}(n^2)\exp(2\pi inz)$ is a finite linear combination of theta-series of quaternary quadratic forms associated with certain lattices in a quaternion algebra (see [10, Theorem 1]). The quaternion algebra is chosen so that the reduced norm on its pure part is similar over $\mathbb{Q}$ to the form $\mathbf{q}$. In particular then $(\pi_{kj}(p^2)) = (r^*(\mathbf{q}_k,p^2\mathbf{q}_j)/e(\mathbf{q}_j))$ is none other than the transpose of Eichler's matrix (3.6) .

One of our goals in the present paper is to find an automorph analog of Shimura's lift for theta-series of ternary quadratic forms. Let us start with a brief reexamination of P. Ponomarev's main result from a somewhat different point of view. For simplicity assume that $\mathbf{q}$ is an integral ternary positive definite quadratic form of class number h. We fix the system (5.2) of representatives in the similitude class. Then the generic theta-series $\Theta_{\{\mathbf{q}\}}(z)$ is an eigenform of all Hecke operators $T(p^2)$ with $p\not|\det\mathbf{q}$ and identity (3.9) is true for the associated zeta-functions. From (3.3) it follows that for ternary quadratic forms the local constants in (3.9) are given by: $c_p^{-1} = 1\,,\ \beta_p = 0\,.$ Define coefficients b_n by

$$\sum_n\frac{b_n}{n^s} = \prod_p(1-\bar{\mathfrak{t}}^*(p^2)p^{-s}+p^{1-2s})^{-1}\ ,$$

where

$$\bar{\mathfrak{t}}^*(p^2) = \bar{\mathfrak{t}}^*_{\mathbf{q}}(p^2) = \sum_{j=1}^{h}\frac{r^*(\mathbf{q}_j,p^2\mathbf{q})}{e(\mathbf{q}_j)}\ ,$$

and put

$$B(z) = \sum_n b_n e^{2\pi inz}\ .$$

Observe that, in particular, $b_1 = 1\,,\ b_p = \bar{\mathfrak{t}}^*(p^2)\,.$ We expect $B(z)$ to be equal to a finite linear combination

$$B(z)\ =\ \sum_{j=1}^{H}x_j\Theta(z,\mathbf{n}_j)\ =\ \sum_n\Big(\sum_{j=1}^{H}x_jr(\mathbf{n}_j,n)\Big)e^{2\pi inz}$$

of theta-series associated with some quaternary (integral) quadratic forms $\mathbf{n}_j$. We also expect $B(z)$ to satisfy

$$B(z) \mid_2 T(p) \; = \; \bar{\mathfrak{t}}^*_{\mathbf{q}}(p^2)B(z)$$

for any prime p , $p \not| \det \mathbf{q}$. A plausible candidate would be

$$B(z) = \Big(\sum_{i=1}^{H} \frac{r(\mathbf{n}_i,1)}{e(\mathbf{n}_i)}\Big)^{-1} \cdot \sum_{j=1}^{H} e^{-1}(\mathbf{n}_j)\Theta(z,\mathbf{n}_j) \tag{5.3}$$

which is proportional to the generic theta-series $\Theta_{\{\mathbf{n}\}}(z)$ of a quaternary form $\mathbf{n}$ of class number H . In this case we would have

$$\bar{\mathfrak{t}}^*_{\mathbf{q}}(p^2) = b_p = \Big(\sum_{i=1}^{H} \frac{r(\mathbf{n}_i,1)}{e(\mathbf{n}_i)}\Big)^{-1} \cdot \sum_{j=1}^{H} \frac{r(\mathbf{n}_j,p)}{e(\mathbf{n}_j)} \ . \tag{5.4}$$

On the other hand from Eichler's commutation relations (4.3) or (3.5) we know that

$$\begin{pmatrix} \vdots \\ \frac{r(\mathbf{n}_i,p)}{e(\mathbf{n}_i)} \\ \vdots \end{pmatrix} \; = \; c_p^{-1}(\mathbf{n})\Big(\frac{r^*(\mathbf{n}_i,p\mathbf{n}_j)}{e(\mathbf{n}_i)}\Big) \begin{pmatrix} \vdots \\ \frac{r(\mathbf{n}_j,1)}{e(\mathbf{n}_j)} \\ \vdots \end{pmatrix} \ ,$$

which implies the identity

$$\sum_{i=1}^{H} \frac{r(\mathbf{n}_i,p)}{e(\mathbf{n}_i)} \; = \; c_p^{-1}(\mathbf{n}) \sum_{j=1}^{H} \Big(\sum_{i=1}^{H} \frac{r^*(\mathbf{n}_i,p\mathbf{n}_j)}{e(\mathbf{n}_i)}\Big) \frac{r(\mathbf{n}_j,1)}{e(\mathbf{n}_j)} \ .$$

But the sum $(\sum_i r(\mathbf{n}_i,p\mathbf{n}_j)/e(\mathbf{n}_i))$ does not depend on j . (In fact, the sum coincides with $c_p(\mathbf{n})$ times the zero Fourier coefficient of $\Theta(z,\mathbf{n}_j)|_2T(p)$; this coefficient is equal to $1+p$ for any j). Therefore, together with conjectural relation (5.4), the last identity would imply that

$$\sum_{i=1}^{h} \frac{r^*(\mathbf{q}_i,p^2\mathbf{q})}{e(\mathbf{q}_i)} = \bar{\mathfrak{t}}^*_{\mathbf{q}}(p^2) = c_p^{-1}(\mathbf{n}) \sum_{i=1}^{H} \frac{r^*(\mathbf{n}_i,p\mathbf{n})}{e(\mathbf{n}_i)} \ ,$$

where $c_p(\mathbf{n}) = (1+\chi_{\mathbf{n}}(p))$ by (3.3) . The above formula can be rewritten in a slightly more general form

$$\sum_{A \in \bigcup_{i=1}^{h} R^*(\mathbf{q}, p^2\mathbf{q}_i)/E(\mathbf{q}_i)} 1 \quad = \quad (1+\chi_{\mathbf{n}}(p))^{-1} \sum_{M \in \bigcup_{i=1}^{H} R(\mathbf{n}, p\mathbf{n}_i)/E(\mathbf{n}_i)} 1 \ , \tag{5.5}$$

which makes sense for any *nonsingular* (integral) ternary form $\mathbf{q}$. Thus, in accordance with our heuristic argument, we can expect that an automorph $A \in R(\mathbf{q}, p^2\mathbf{q}')$ of quadratic form $\mathbf{q}$ can be "lifted" to an automorph $M \in R(\mathbf{n}, p\mathbf{n}')$ of some quaternary form $\mathbf{n}$ associated to $\mathbf{q}$. Moreover, relation (5.5) should appear as a consequence of the expected lifting of automorphs. In the next sections we shall prove that this is so indeed, by providing an explicit construction for the "lift" (see (6.30), Theorems 7.3, 7.7, and Corollary 7.8).

Chapter 6

Clifford algebras and automorph class lift

Since our construction of the automorph lift is based on Clifford algebras, we start with a brief review of their properties. In the course we also introduce some convenient notation. Let

$$\mathbf{q}(X) = q_1 x_1^2 + b_{12} x_1 x_2 + b_{13} x_1 x_3 + q_2 x_2^2 + b_{23} x_2 x_3 + q_3 x_3^2 \tag{6.1}$$

be an integral nonsingular (ternary) quadratic form. We set

$$Q_0 = \begin{pmatrix} q_1 & b_{12} & b_{13} \\ 0 & q_2 & b_{23} \\ 0 & 0 & q_3 \end{pmatrix} \quad , \quad B = \begin{pmatrix} -b_{23} \\ b_{13} \\ -b_{12} \end{pmatrix} . \tag{6.2}$$

Then the matrix Q of the form $\mathbf{q}$ and its determinant $\det \mathbf{q}$ are given by

$$Q = {}^t Q_0 + Q_0 \quad , \quad 2\Delta = \det \mathbf{q} = 2 \cdot (4 \det Q_0 - Q_0[B]) \ , \tag{6.3}$$

where $\det Q_0 = q_1 q_2 q_3$ and $\Delta = \det \mathbf{q}/2$. The matrices adjoint to Q_0 and Q are

$$\tilde{Q_0} = \begin{pmatrix} q_2 q_3 & -q_3 b_{12} & b_{12} b_{23} - q_2 b_{13} \\ 0 & q_1 q_3 & -q_1 b_{23} \\ 0 & 0 & q_1 q_2 \end{pmatrix}$$

and

$$\tilde{Q} = 2({}^t\tilde{Q_0} + \tilde{Q_0}) - B \cdot {}^t B \ . \tag{6.4}$$

With $\mathbf{q}$, we associate the quadratic $\mathbb{Z}$-module $(E, \mathbf{q}) = (\mathbb{Z}^3, \mathbf{q})$ with the corresponding symmetric bilinear form

$$\mathbf{b}(x, y) = \mathbf{q}(x + y) - \mathbf{q}(x) - \mathbf{q}(y) \ , \qquad x, y \in E \ , \tag{6.5}$$

whose matrix $(\mathbf{b}(e_i, e_j))$ relative to the standard basis e_1, e_2, e_3 of $\mathbb{Z}^3$ is Q. The *Clifford algebra* $C(E) = C(E, \mathbf{q})$ of $(E, \mathbf{q})$ is a free $\mathbb{Z}$-algebra with monomorphism $\iota : E \hookrightarrow C(E)$ such that $\iota(x)^2 = \mathbf{q}(x) \cdot 1_{C(E)}$ for any $x \in E$. It is uniquely characterized by the following *universal* property: for any homomorphism $\eta : E \to D$ into an algebra D with $\eta(x)^2 = \mathbf{q}(x) \cdot 1_D$, there exists unique homomorphism of algebras $\tau : C(E) \to D$ such that the diagram

$$\begin{tikzcd} E \arrow[d, "\eta"'] & E \arrow[l, "id"'] \arrow[d, "\iota"] \\ D & C(E) \arrow[l, "\tau"'] \end{tikzcd} \tag{6.6}$$

commutes (i.e. $\eta = \tau \circ \iota$). The algebra $C(E)$ can be realized as a free $\mathbb{Z}$-module of rank 8 generated by products of e_1, e_2, e_3 (see [9] for details). We will denote the product $e_i e_j$ in $C(E)$ by e_{ij} and $e_i e_j e_k$ by e_{ijk}. The unit element of $C(E)$ is denoted by e_0 and we identify $\mathbb{Z}$ with $\mathbb{Z}e_0$. We also identify E with $\iota(E) \subset C(E)$. The *even subalgebra*

$$C_0(E) = \mathbb{Z}e_0 \oplus \mathbb{Z}e_{23} \oplus \mathbb{Z}(-e_{13}) \oplus \mathbb{Z}e_{12} \tag{6.7}$$

is a free $\mathbb{Z}$-module of rank 4 generated by products of even number of vectors of E. (Note the order of the elements of the basis in (6.7)! Strange at first glance, this oder is *natural.* This basis of $C_0(E)$ will be referred to as the *natural basis*). Next, putting $C_1(E) = \mathbb{Z}(-e_{123}) \oplus \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$ one has $C(E) = C_0(E) \oplus C_1(E)$. Sometimes it is also useful to consider $C(E) \otimes \mathbb{Q}$ or $C_0(E) \otimes \mathbb{Q}$ – the Clifford algebra of $(E, \mathbf{q})$ over $\mathbb{Q}$ and its even subalgebra, in which $C(E)$ and $C_0(E)$ are orders. The algebra $C(E)$ has an antiautomorphism $x \mapsto \bar{x}$ defined on the generators by

$$\bar{e_j} = -e_j\ , \qquad j = 1, 2, 3\ . \tag{6.8}$$

The restriction of the antiautomorphism $x \mapsto \bar{x}$ to $C_0(E)$ can be written in coordinates as

$$x_0e_0+x_1e_{23}-x_2e_{13}+x_3e_{12} \mapsto (x_0+x_3b_{12}-x_2b_{13}+x_1b_{23})e_0-x_1e_{23}+x_2e_{13}-x_3e_{12} \tag{6.9}$$

and gives us the *standard involution* on $C_0(E)$. That is to say,

$$\mathbf{s}(x)=x+\bar{x}\in\mathbb{Z} \quad , \quad \mathbf{n}(x)=x\cdot\bar{x}\in\mathbb{Z} \tag{6.10}$$

for any $x \in C_0(E)$. In particular, each element x of $C_0(E)$ satisfies the equation $(z-x)(z-\bar{x})=z^2-\mathbf{s}(x)z+\mathbf{n}(x)=0$ which is unique in case x and e_0 are linearly independent. The integers $\mathbf{s}(x)$ and $\mathbf{n}(x)$ are called respectively the *trace* and the *norm* of $x \in C_0(E)$. The norm $\mathbf{n}$ turns the even subalgebra C_0 into quadratic $\mathbb{Z}$-module $(C_0(E),\mathbf{n})$ of rank 4 with associated bilinear form

$$\mathbf{s}(x\bar{y})=\mathbf{n}(x+y)-\mathbf{n}(x)-\mathbf{n}(y)\ , \quad x,y\in C_0(E)\ . \tag{6.11}$$

The matrix N of the form $\mathbf{n}$ with respect to the natural basis (6.7) is

$$N=\begin{pmatrix} 2 & -{}^tB \\ & \\ -B & ({}^t\tilde{Q}_0+\tilde{Q}_0) \end{pmatrix} \tag{6.12}$$

We easily compute the determinant

$$\det\mathbf{n}=\Delta^2=((\det\mathbf{q})/2)^2 \tag{6.13}$$

and the inverse matrix

$$N^{-1}=\Delta^{-1}\cdot\begin{pmatrix} 2\cdot\det Q_0 & {}^t(Q_0B) \\ & \\ (Q_0B) & Q \end{pmatrix}\ , \tag{6.14}$$

where Q_0 and B are given by (6.2). From the above formulas it can be seen that the quadratic modules $(E, \mathbf{q})$ and $(C_0(E), \mathbf{n})$ are closely related. In fact $(C_0(E), \mathbf{n})$ contains a certain quadratic submodule of rank 3 which is "almost identical" $(E, \mathbf{q})$. We shall present the construction shortly, but first we need to introduce the special element

$$t = e_{123} + \overline{e_{123}} = e_{123} - e_{321} \in C(E) \tag{6.15}$$

used by M. Kneser in [9]. Straightforward (but rather tiresome) calculations show that t belongs to the center of $C(E)$, $t = \bar{t}$ and

$$t = (-e_{123}, e_1, e_2, e_3) \begin{pmatrix} -2 \\ B \end{pmatrix} \;, \quad t^2 = -\Delta \;. \tag{6.16}$$

Consider now $\mathbb{Z}$-submodule Et of $C_0(E)$. Using (6.16) we see that Et has rank 3 and

$$(e_1t, e_2t, e_3t) = (e_0, e_{23}, -e_{13}, e_{12}) \cdot T$$

form its $\mathbb{Z}$-basis, where

$$T = \begin{pmatrix} {}^t(Q_0B) \\ \\ Q \end{pmatrix} \in \mathbb{Z}_3^4 \;. \tag{6.17}$$

Let us compute the matrix of the restriction of the norm-form $\mathbf{n}$ to Et with respect to the basis e_1t, e_2t, e_3t. We have

$$N \cdot T = \begin{pmatrix} 2 \cdot {}^t(Q_0B) - {}^tB \cdot Q \\ \\ ({}^t\tilde{Q_0} + \tilde{Q_0})({}^tQ_0 + Q_0) - B \cdot {}^tB \cdot {}^tQ_0 \end{pmatrix} = \begin{pmatrix} 0\,0\,0 \\ \Delta \cdot 1_3 \end{pmatrix}$$

and so

$$N[T] = \Delta \cdot Q \;. \tag{6.18}$$

Recall that $\Delta = \det \mathbf{q}/2$ is an integer (see (6.3)), thus $T \in R(\mathbf{n}, \Delta\mathbf{q})$ and $(Et, \Delta\mathbf{q}) \hookrightarrow (C_0(E), \mathbf{n})$ as we claimed. Finally, we observe that

$$-e_{123} \cdot t = (e_0, e_{23}, -e_{13}, e_{12}) \begin{pmatrix} 2 \det Q_0 \\ \\ Q_0 B \end{pmatrix} \ , \tag{6.19}$$

which extends multiplication of E by t to an injection $C_1(E) \cdot t \hookrightarrow C_0(E)$, whose matrix with respect to our choice of bases is $\Delta \cdot N^{-1}$.

Let $\mathbf{q}''$ be another integral ternary quadratic form. With it, we associate a quadratic module $(E'', \mathbf{q}'')$ and Clifford algebra $C(E'')$ exactly as above. Let $A \in R(\mathbf{q}, \mathbf{q}'')$ be an integral automorph. From the geometric point of view, A determines an isometry $\alpha = \alpha_A$ from the quadratic module $(E'', \mathbf{q}'')$ into $(E, \mathbf{q})$:

$$(\alpha_A(e''_1), \alpha_A(e''_2), \alpha_A(e''_3)) = (e_1, e_2, e_3) \cdot A \ ,$$

where e''_1, e''_2, e''_3 is the standard basis of $E'' = \mathbb{Z}^3$. Let ι and ι'' be the natural inclusions of $(E, \mathbf{q})$ and $(E'', \mathbf{q}'')$ into corresponding Clifford algebras. Since $(\iota \circ \alpha(x''))^2 = \mathbf{q}(\alpha(x'')) \cdot e_0 = \mathbf{q}''(x'') \cdot e_0$ for any $x'' \in E''$, there exists a unique homomorphism of algebras $\varphi = \varphi_A$ which makes the diagram

$$\begin{tikzcd}
(E, \mathbf{q}) \arrow[d, "\iota"'] & (E'', \mathbf{q}'') \arrow[l, "\alpha_A"'] \arrow[d, "\iota''"] \\
C(E) & C(E'') \arrow[l, "\varphi_A"']
\end{tikzcd} \tag{6.20}$$

commutative. (This follows immediately from the universal property (6.6) of Clifford algebras.) Clearly, the homomorphism φ_A is compatible with the involutions (6.8) on $C(E)$ and $C(E'')$:

$$\varphi_A(\bar{x}'') = \overline{\varphi_A(x'')} \text{ for all } x'' \in C(E'') \ . \tag{6.21}$$

Therefore the restriction of φ_A to the even subalgebra $C_0(E'')$ is an isometry of quadratic modules $\varphi_A : (C_0(E''), \mathbf{n}'') \to (C_0(E), \mathbf{n})$ whose matrix with respect to our choice of bases (6.7) is

$$\Phi_A = \begin{pmatrix} 1 & {}^tA_3Q_0A_2 & -{}^tA_3Q_0A_1 & {}^tA_2Q_0A_1 \\ 0 & & & \\ 0 & & {}^t\tilde{A} & \\ 0 & & & \end{pmatrix}, \tag{6.22}$$

so that

$$(\varphi_A(e''_0), \varphi_A(e''_{23}), \varphi_A(-e''_{13}), \varphi_A(e''_{12})) = (e_0, e_{23}, -e_{13}, e_{12}) \cdot \Phi_A \ .$$

Here A_j denotes the j^{th} column of the original automorph $A \in R(\mathbf{q}, \mathbf{q}'')$ that gave rise to $\Phi_A \in R(\mathbf{n}, \mathbf{n}'')$. (By $\mathbf{n}, \mathbf{n}''$ we mean the integral quaternary quadratic forms which are specializations of the corresponding norm-forms in the natural bases (6.7) of $C_0(E)$ and $C_0(E'')$ respectively.) To complete the picture, we also need a description of the action of φ_A on the special element $t'' \in C(E'')$ of the form (6.15):

LEMMA 6.1. *Let* $A = (a_{ij}) \in R(\mathbf{q}, \mathbf{q}'')$ *be an integral automorph. Let* t *and* t'' *be elements of the form (6.15) of the algebras* $C(E)$ *and* $C(E'')$ *respectively. Then*

$$\varphi_A(t'') = (\det A) \cdot t$$

in the notation introduced above.

Proof. Note that the elements of E are multiplied in $C(E)$ by the following rule:

$$(\, e_1, e_2, e_3 \,) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \cdot (\, e_1, e_2, e_3 \,) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = (\, e_0, e_{23}, -e_{13}, e_{12} \,) \begin{pmatrix} {}^tYQ_0X \\ x_2y_3 - x_3y_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{pmatrix} .$$

Therefore

$$\varphi_A(-e''_{123}) = -\varphi_A(e''_1)\varphi_A(e''_2)\varphi_A(e''_3) = -\alpha_A(e''_1)\alpha_A(e''_2)\alpha_A(e''_3) =$$
$$-1\cdot (\, e_1, e_2, e_3\,)\, A_1 \cdot (\, e_1, e_2, e_3\,)\, A_2 \cdot (\, e_1, e_2, e_3\,)\, A_3 = (\, -e_{123}, e_1, e_2, e_3\,) \begin{pmatrix} \delta \\ Z \end{pmatrix} \ ,$$

where $A = (A_1A_2A_3)$, $\delta = \det A$, the components z_1, z_2, z_3 of the column Z are given by

$$z_1 = -({}^tA_2Q_0A_1)a_{13} + b_{13}a_{13}\hat{a}_{23} + b_{23}a_{23}\hat{a}_{23} - b_{12}a_{13}\hat{a}_{33} - q_2a_{23}\hat{a}_{33} + q_3a_{33}\hat{a}_{23} \ ,$$
$$z_2 = -({}^tA_2Q_0A_1)a_{23} - b_{13}a_{13}\hat{a}_{13} - b_{23}a_{23}\hat{a}_{13} + q_1a_{13}\hat{a}_{33} - q_3a_{33}\hat{a}_{13} \ ,$$
$$z_3 = -({}^tA_2Q_0A_1)a_{33} + b_{12}a_{13}\hat{a}_{13} + q_2a_{23}\hat{a}_{13} - q_1a_{13}\hat{a}_{23} \ ,$$

and $\hat{a}_{ij}$ is the cofactor of a_{ij} in A. Using (6.16) applied to t'', we have

$$\varphi_A(t'') = (\, -e_{123}, e_1, e_2, e_3\,) \begin{pmatrix} \delta & 0\,0\,0 \\ Z & A \end{pmatrix} \begin{pmatrix} -2 \\ B'' \end{pmatrix} \ .$$

On the other hand, from (6.16) we also know the coordinates of t in this basis. Therefore, in order to prove the lemma it remains to check the relation

$$A \cdot \begin{pmatrix} -b''_{23} \\ b''_{13} \\ -b''_{12} \end{pmatrix} - 2\cdot \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \delta \cdot \begin{pmatrix} -b_{23} \\ b_{13} \\ -b_{12} \end{pmatrix} \ . \tag{6.23}$$

Before entering into computations, we make several remarks. First, since ${}^tA_2Q_0A_1 + {}^tA_2{}^tQ_0A_1 = {}^tA_2QA_1 = b''_{12}$, then $2\cdot{}^tA_2Q_0A_1 - b''_{12} = {}^tA_2(Q_0 - {}^tQ_0)A_1 = -b_{12}\hat{a}_{33} + b_{13}\hat{a}_{23} - b_{23}\hat{a}_{13}$. Second, $Q[A] = Q''$ implies that $\delta^{-1}\cdot{}^t\tilde{A}Q'' = QA$. Third, $(a_{ij}) = A = (A^{-1})^{-1} = \delta^{-1}\cdot\breve{A} = \delta^{-1}\cdot(\breve{a}_{ij})$, where $\breve{A}$ is the double adjoint of A. Now we proceed to calculation of the entries of the column-vector on the left hand side of the identity (6.23).

First entry:

$$\begin{aligned}
&-a_{11}b''_{23} + a_{12}b''_{13} - a_{13}b''_{12} - 2z_1 = \\
&-b_{23}(a_{13}\hat{a}_{13} + a_{23}\hat{a}_{23}) - b_{13}a_{13}\hat{a}_{23} + b_{12}a_{13}\hat{a}_{33} - b_{23}a_{23}\hat{a}_{23} + 2q_2a_{23}\hat{a}_{33} \\
&\qquad -2q_3a_{33}\hat{a}_{23} - (a_{11}b''_{23} - a_{12}b''_{13}) = \\
&-\delta b_{23} + \hat{a}_{33}(b_{12}a_{13} + 2q_2a_{23} + b_{23}a_{33}) - (a_{11}b''_{23} - a_{12}b''_{13}) - \\
&\qquad \hat{a}_{23}(b_{13}a_{13} + b_{23}a_{23} + 2q_3a_{33}) = \\
&\delta^{-1}\hat{a}_{33}(\hat{a}_{21}b''_{13} + \hat{a}_{22}b''_{23} + \hat{a}_{23}2q''_3) - \delta^{-1}\hat{a}_{23}(\hat{a}_{31}b''_{13} + \hat{a}_{32}b''_{23} + \hat{a}_{33}2q''_3) - \delta b_{23} = \\
&\delta^{-1}b''_{13}(\hat{a}_{33}\hat{a}_{21} - \hat{a}_{23}a_{31}) + \delta^{-1}b''_{23}(\hat{a}_{33}\hat{a}_{22} - \hat{a}_{23}\hat{a}_{32}) - (a_{11}b''_{23} - a_{12}b''_{13}) - \delta b_{23} = \\
&\qquad \delta^{-1}b''_{13}(-\check{a}_{12}) + \delta^{-1}b''_{23}(\check{a}_{11}) - (a_{11}b''_{23} - a_{12}b''_{13}) - \delta b_{23} = -\det A \cdot b_{23} \ .
\end{aligned}$$

Second entry:

$$\begin{aligned}
&-a_{21}b''_{23} + a_{22}b''_{13} - a_{23}b''_{12} - 2z_2 = \\
&b_{13}(a_{13}\hat{a}_{13} + a_{23}\hat{a}_{23}) + \hat{a}_{13}(b_{13}a_{13} + b_{23}a_{23} + 2q_3a_{33}) - \hat{a}_{33}(2q_1a_{13} + b_{12}a_{23}) \\
&\qquad -(a_{21}b''_{23} - a_{22}b''_{13}) = \\
&\delta^{-1}\hat{a}_{13}(\hat{a}_{31}b''_{13} + \hat{a}_{32}b''_{23}) - \delta^{-1}\hat{a}_{33}(\hat{a}_{11}b''_{13} + \hat{a}_{12}b''_{23}) - (a_{21}b''_{23} - a_{22}b''_{13}) + \delta b_{13} = \\
&\qquad \det A \cdot b_{13} \ .
\end{aligned}$$

Third entry:

$$\begin{aligned}
&-a_{31}b''_{23} + a_{32}b''_{13} - a_{33}b''_{12} - 2z_3 = \\
&-b_{12}(a_{13}\hat{a}_{13} + a_{33}\hat{a}_{33}) + \hat{a}_{23}(2q_1a_{13} + b_{13}a_{33}) - \hat{a}_{11}(b_{12}a_{13} + 2q_2a_{23} + b_{23}a_{33}) \\
&\qquad -(a_{31}b''_{23} - a_{32}b''_{13}) = \\
&\delta^{-1}\hat{a}_{23}(\hat{a}_{11}b''_{13} + \hat{a}_{12}b''_{23}) - \delta^{-1}\hat{a}_{13}(\hat{a}_{21}b''_{13} + \hat{a}_{22}b''_{23}) - (a_{31}b''_{23} - a_{32}b''_{13}) - \delta b_{12} = \\
&\qquad -\det A \cdot b_{12} \ .
\end{aligned}$$

This finishes the proof of the Lemma. □

Along with (6.16), the above lemma leads us to the following criterion.

THEOREM 6.2. *Let $\varphi : C_0(E'') \to C_0(E)$ be a homomorphism of even subalgebras of Clifford algebras associated with ternary quadratic $\mathbb{Z}$-modules $(E'', \mathbf{q}'')$ and $(E, \mathbf{q})$. Let $\Delta = \det \mathbf{q}/2$, $\Delta'' = \det \mathbf{q}''/2$ and let $t \in C(E)$, $t'' \in C(E'')$ be special elements of the form (6.15). Then φ coincides with the lift (6.20) of an isometry $\alpha : (E'', \mathbf{q}'') \to (E, \mathbf{q})$ if and only if*

$$\varphi(E'' \cdot t'') \subset \sqrt{\Delta''/\Delta} \cdot (E \cdot t) \ . \tag{6.24}$$

In this case the isometry α is unique (up to sign) and is given by

$$\alpha(x'') = \frac{\pm\varphi(x''t'') \cdot t}{\sqrt{\Delta\Delta''}} \quad \text{for } \ x'' \in E'' \ , \tag{6.25}$$

where we can fix either "+" or "−".

Proof. Assuming (6.24),we consider the map α as defined in (6.25). For an $x'' \in E''$ we have:

$$\alpha(x'') \subset (\sqrt{\Delta\Delta''})^{-1} \cdot \varphi(E''t'') \cdot t \subset (\sqrt{\Delta\Delta''})^{-1} \sqrt{\Delta''/\Delta} \cdot E \cdot t^2 \subset -|\Delta|^{-1}\Delta \cdot E \subset E \ .$$

Furthermore,

$$\mathbf{q}(\alpha(x'')) = \alpha(x'') \cdot \alpha(x'') = (\Delta\Delta'')^{-1} \cdot \varphi(x''t'') \cdot t \cdot \varphi(x''t'') \cdot t =$$
$$(\Delta\Delta'')^{-1} \cdot \varphi(x''t''x''t'') \cdot t^2 = (\Delta\Delta'')^{-1} \cdot \varphi(-\Delta''(x'')^2) \cdot (-\Delta) = \varphi(\mathbf{q}''(x'')) = \mathbf{q}''(x'') \ ,$$

thus $\alpha : (E'', \mathbf{q}'') \to (E, \mathbf{q})$ is indeed an isometry. By (6.20) it can be lifted to an algebraic homomorphism $\varphi_\alpha : C(E'') \to C(E)$ the restriction of which to $C_0(E'')$ is a homomorphism into $C(E)$. Then

$$\varphi_\alpha(e''_{ij}) = \alpha(e''_i) \cdot \alpha(e''_j) = (\Delta\Delta'')^{-1} \cdot \varphi(e''_i t'' e''_j t'') \cdot t^2 =$$
$$(\Delta\Delta'')^{-1}(-\Delta) \cdot \varphi(-\Delta'' e''_i e''_j) = \varphi(e''_{ij}) \ ,$$

so φ_α and φ coincide on $C_0(E'')$.

Conversely, if $\varphi = \varphi_\alpha \,|_{C_0}$ for some lift φ_α of an isometry $\alpha : (E'', \mathbf{q}'') \to (E, \mathbf{q})$, then

$$\varphi(x''t'') = \varphi_\alpha(x''t'') = \varphi_\alpha(x'')\cdot\det\alpha\cdot t = \alpha(x'')\cdot\det\alpha\cdot t \subset \det\alpha\cdot E\cdot t \subset \sqrt{\Delta''/\Delta}\cdot(E\cdot t)\,,$$

so (6.24) is satisfied. Identity (6.25) is also true for some choice of sign. □

We summarize what we have established so far. The universal property (6.6) of Clifford algebras allows us to lift an integral automorph $A \in R(\mathbf{q}, \mathbf{q}'')$ of ternary forms to an integral automorph $\Phi_A \in R(\mathbf{n}, \mathbf{n}'')$ of quaternary forms associated with norms on the even subalgebras of Clifford algebras. Conversely, the original automorph $A \in R(\mathbf{q}, \mathbf{q}'')$ can be recovered by the lift $\Phi_A \in R(\mathbf{n}, \mathbf{n}'')$ with the help of Theorem 6.2 above. (We note again that quaternary quadratic forms $\mathbf{n}$, $\mathbf{n}''$ are specializations of norm-forms (6.10) in the natural bases (6.7).)

Recall that the quadratic forms we are working with are not necessarily positive definite and so the sets $R(\mathbf{q}, \mathbf{q}'')$, $R(\mathbf{n}, \mathbf{n}'')\ldots$ of automorphs or the sets $R(\mathbf{q}, a)$, $R(\mathbf{n}, a)\ldots$ of representations of a number a can be infinite in general. But the quotients modulo the corresponding groups of units ($E(\mathbf{q})$, $E(\mathbf{n})\ldots$) are always finite for nonsingular forms. Because of this, it is more convenient sometimes to consider the orbits modulo groups of units rather than individual automorphs or representations (compare to section 3). The following lemma shows that this transition is compatible with the lift (6.22).

Lemma 6.3. *Let* $A, D \in R(\mathbf{q}, \mathbf{q}'')$ *be integral automorphs. Then* $A \in E(\mathbf{q})D$ *if and only if* $\Phi_A \in E(\mathbf{n})\Phi_D$.

Proof. Let $E \in E(\mathbf{q})$ be such that $A = ED$. Consider the following commutative diagram:

$$\begin{tikzcd}
(E,\mathbf{q}) \arrow[d, "\iota"] & (E,\mathbf{q}) \arrow[l, "\alpha_E"'] \arrow[d, "\iota"] & (E'',\mathbf{q}'') \arrow[l, "\alpha_D"'] \arrow[d, "\iota''"] \\
C(E) & C(E) \arrow[l, "\varphi_E"'] & C(E'') \arrow[l, "\varphi_D"']
\end{tikzcd}$$

where the isometries α_E, α_D and algebraic homomorphisms φ_E, φ_D are defined as in (6.20). Since $\alpha_E \circ \alpha_D = \alpha_A$, we know that there exists unique algebraic homomorphism $\varphi_A = \varphi_{ED} : C(E'') \to C(E)$ such that $\iota \circ \alpha_A = \varphi_A \circ \iota''$ as in (6.20). But $\iota \circ \alpha_A = \iota \circ \alpha_E \circ \alpha_D = \varphi_E \circ \iota \circ \alpha_D = \varphi_E \circ \varphi_D \circ \iota''$, which implies that $\varphi_{ED} = \varphi_E \circ \varphi_D$ and thus $\Phi_A = \Phi_E \Phi_D$ (see (6.22)). Note that since $E \in E(\mathbf{q})$ then $\Phi_E \in E(\mathbf{n})$.

Conversely, assume that $\Phi_A \in E(\mathbf{n})\Phi_D$. Then $\Phi_A \Phi_D^{-1} \in E(\mathbf{n})$ and in particular

$$\begin{pmatrix} 1 & * & * & * \\ 0 & & & \\ 0 & & {}^t\tilde{A} & \\ 0 & & & \end{pmatrix} \begin{pmatrix} 1 & * & * & * \\ 0 & & & \\ 0 & & {}^t\tilde{D}^{-1} & \\ 0 & & & \end{pmatrix} = \begin{pmatrix} 1 & * \; * \; * \\ 0 & \\ 0 & \frac{1}{\det D}{}^t\tilde{A} \cdot {}^tD \\ 0 & \end{pmatrix}$$

is an integral matrix. But $\det D = \det A$, so ${}^tA^{-1} . {}^tD$ is also an integral matrix. Then $E = DA^{-1}$ is also integral and $Q[E] = Q[DA^{-1}] = Q''[A^{-1}] = Q$, i.e. $E \in E(\mathbf{q})$ and $A \in E(\mathbf{q})D$. □

Remark . *An obvious modification of the above proof shows that*

$$A \in D \cdot E(\mathbf{q}'') \iff \Phi_A \in \Phi_D \cdot E(\mathbf{n}'') .$$

We will also need the following technical result.

Lemma 6.4. *Assume that (ternary) quadratic forms* $\mathbf{q}$ *and* $\mathbf{q}''$ *belong to the same similarity class. Then* $\mathbf{q}$ *and* $\mathbf{q}''$ *are integrally equivalent if and only if the corresponding quadratic forms* $\mathbf{n}$ *and* $\mathbf{n}''$ *(see (6.12)) are integrally equivalent.*

Proof. Suppose $\mathbf{q}$ and $\mathbf{q}''$ belong to the same equivalence class, i.e. there exists a matrix $U \in R(\mathbf{q}, \mathbf{q}'') \cap \Lambda^3$. Then $\alpha_U : (E'', \mathbf{q}'') \to (E, \mathbf{q})$ is an isometric isomorphism of quadratic modules which gives rise to an isomorphism $\varphi_U : C(E'') \to C(E)$ of Clifford algebras exactly as in (6.20). The restriction of φ_U to $C_0(E'')$ is an isomorphism of even subalgebras whose matrix with respect to the natural bases (6.7) is $\Phi_U \in R(\mathbf{n}, \mathbf{n}'') \cap \Lambda^4$ (see (6.22)). Thus $\mathbf{n}$ and $\mathbf{n}''$ are integrally equivalent.

Conversely, suppose that there exists $\mathcal{U} \in R(\mathbf{n}, \mathbf{n}'') \cap \Lambda^4$. The matrix $\mathcal{U}$ defines a (linear) isometric isomorphism of quadratic modules:

$$\upsilon : (C_0(E''), \mathbf{n}'') \longrightarrow (C_0(E), \mathbf{n}) \ ,$$

$$(\upsilon(e_0''), \upsilon(e_{23}''), \upsilon(-e_{13}''), \upsilon(e_{12}'')) = (e_0, e_{23}, -e_{13}, e_{12}) \cdot \mathcal{U} \ .$$

Since $\mathbf{n}(\upsilon(e_0'')) = \mathbf{n}''(e_0'') = 1$, the element $\upsilon(e_0'')$ has an inverse $\upsilon(e_0'')^{-1} = \overline{\upsilon(e_0'')} \in C_0(E)$ whose norm is also 1. Then the right multiplication $x \mapsto x \cdot \overline{\upsilon(e_0'')}$ is a (linear) isometric automorphism of $C_0(E)$. The composition of these two isometries

$$\omega : x'' \mapsto \upsilon(x'') \cdot \overline{\upsilon(e_0'')} \qquad x'' \in C_0(E'')$$

gives an isometric isomorphism of quadratic modules $(C_0(E''), \mathbf{n}'') \to (C_0(E), \mathbf{n})$ which maps e_0'' to e_0. Therefore, its matrix with respect to natural bases (6.7) has the form

$$\mathcal{W} = \begin{pmatrix} 1 & & * * * & \\ 0 & & & \\ 0 & & W & \\ 0 & & & \end{pmatrix} \qquad \text{with } W \in \Lambda^3 \ .$$

Further, since $N[\mathcal{W}] = N''$, then $N^{-1}[{}^t\mathcal{W}^{-1}] = (N'')^{-1}$ with N^{-1}, $(N'')^{-1}$ given by (6.14). By our assumption the forms $\mathbf{q}$ and $\mathbf{q}''$ are similar, in particular $\Delta =$

$\det \mathbf{q}/2 = \Delta''$. Therefore (6.14) implies

$$\begin{pmatrix} 2\,\det Q_0 & {}^t(Q_0B) \\ & \\ (Q_0B) & Q \end{pmatrix} \left[\begin{pmatrix} 1 & 0\;0\;0 \\ * & \\ * & {}^tW^{-1} \\ * & \end{pmatrix} \right] = \begin{pmatrix} 2\,\det Q_0'' & {}^t(Q_0''B'') \\ & \\ (Q_0''B'') & Q'' \end{pmatrix} .$$

It follows that $Q[{}^tW^{-1}] = Q''$ with $W \in \Lambda^3$, i.e. the quadratic forms $\mathbf{q}$ and $\mathbf{q}''$ are (integrally) equivalent. □

Now we proceed directly to an automorph analog of Shimura's lift. Let $\mathbf{q}'$ be a quadratic form *similar* to $\mathbf{q}$ (see section 1) and let p be a prime number coprime to $\det \mathbf{q} = \det \mathbf{q}'$. Given an integral automorph $A \in R(\mathbf{q}, p^2\mathbf{q}')$ we can set $\mathbf{q}'' = p^2\mathbf{q}'$ and apply the construction (6.20) to get the homomorphism φ_A of Clifford algebras:

$$\begin{tikzcd} (E,\mathbf{q}) \arrow[d, "\iota"'] & (E'', p^2\mathbf{q}') \arrow[l, "\alpha_A"'] \arrow[d, "\iota''"] \\ C(E,\mathbf{q}) & C(E'', p^2\mathbf{q}') \arrow[l, "\varphi_A"'] \end{tikzcd} \tag{6.26}$$

The restriction of φ_A to the even subalgebra $C_0(E'', p^2\mathbf{q}')$ yields an automorph $\Phi_A \in R(\mathbf{n}, \mathbf{n}'') = R(N, N'')$ given by (6.22). Here N is the matrix (6.12) and

$$N'' = \begin{pmatrix} 2 & -p^2 \cdot {}^tB' \\ & \\ -p^2B' & p^4({}^t\tilde{Q}_0' + \tilde{Q}_0') \end{pmatrix} = N'\left[\begin{pmatrix} 1 & \\ & p^2 1_3 \end{pmatrix} \right] \tag{6.27}$$

is the matrix (6.12) of the norm-form (6.10) of the even subalgebra $C_0(E'', p^2\mathbf{q}')$ with respect to its natural basis (6.7). Note that $C_0(E'', p^2\mathbf{q}')$ can be identified with the subring of $C_0(E', \mathbf{q}')$ spanned by $e_0', p^2e_{23}', -p^2e_{13}', p^2e_{12}'$. (Indeed, the natural isometry of quadratic modules $E'' \cong pE'$ defined by $e_i'' \mapsto pe_i'$ gives rise to an algebraic monomorphism $C(E'', p^2\mathbf{q}') \hookrightarrow C(E', \mathbf{q}')$, the restriction of which to the even subalgebra is the desired ring homomorphism.) In particular, N' on the right hand side of (6.27) is exactly the matrix (6.12) of the norm-form $\mathbf{n}'$ on the subalgebra $C_0(E', \mathbf{q}')$. Combining (5.27) with the relation $N[\Phi_A] = N''$, we conclude that if $A \in R(\mathbf{q}, p^2\mathbf{q}')$, then $N[\Psi_A] = N'[(p \cdot 1_4)] = p^2N'$, where we set

$$\Psi_A = \Phi_A \cdot \begin{pmatrix} p & \\ & p^{-1}1_3 \end{pmatrix} = \begin{pmatrix} p & p^{-1}(\ {}^tA_3Q_0A_2 & -{}^tA_3Q_0A_1 & {}^tA_2Q_0A_1\ ) \\ 0 & & & \\ 0 & & p^2 \cdot {}^tA^{-1} & \\ 0 & & & \end{pmatrix}. \tag{6.28}$$

Lemma 6.5. *In the above notations $\Psi_A \in R(\mathbf{n}, p^2\mathbf{n}')$, in particular, the matrix Ψ_A is integral.*

Proof. We already know that $N[\Psi_A] = p^2N'$ therefore, to prove the lemma it remains to show that Ψ_A is integral. Since $A \in R(\mathbf{q}, p^2\mathbf{q}')$, we have $Q[A] = p^2Q'$ and so $p^2A^{-1} = (\det \mathbf{q})^{-1}\tilde{Q}'^tAQ$, which implies that $\det \mathbf{q} \cdot p^2A^{-1}$ is an integral matrix. But $\det A = p^3$ is coprime to $\det \mathbf{q}$, thus p^2A^{-1} is integral. Next we need to deal with the first row of Ψ_A in (6.28). Denote

$${}^tZ_A = \left({}^tA_3Q_0A_2, -{}^tA_3Q_0A_1, {}^tA_2Q_0A_1\right). \tag{6.29}$$

Then

$$N[\Phi_A] = \begin{pmatrix} 2 & 2 \cdot {}^tZ_A - p^3 \cdot {}^t(A^{-1}B) \\ * & \\ * & \frac{1}{2}(p^4\tilde{Q}' + (2Z_A - p^3A^{-1}B)^t(2Z_A - p^3A^{-1}B)) \end{pmatrix} = N'\left[\begin{pmatrix} 1 & \\ & p^21_3 \end{pmatrix}\right],$$

which implies that $2Z_A - p^3A^{-1}B = -p^2B' \equiv 0 \pmod{p^2}$. But p^2A^{-1} is integral, so $p^3A^{-1}B \equiv 0 \pmod{p}$ and therefore $Z_A \equiv 0 \pmod{p}$. Thus Ψ_A is indeed an integral matrix. □

We conclude that the correspondence $A \mapsto \Psi_A$ gives us an injection $R(\mathbf{q}, p^2\mathbf{q}') \hookrightarrow$

$R(\mathbf{n}, p^2\mathbf{n}')$. Because of Lemma 6.3, we can also view this map as injection

$$\Psi\ :\ E(\mathbf{q})\backslash R(\mathbf{q}, p^2\mathbf{q}') \hookrightarrow E(\mathbf{n})\backslash R(\mathbf{n}, p^2\mathbf{n}') \quad , \quad p \not| \det \mathbf{q}\,. \tag{6.30}$$

Remark 6.6. The above construction does not depend on primality of p and works equally well for any number a coprime to $\det \mathbf{q}$ resulting in injection $R(\mathbf{q}, a^2\mathbf{q}') \hookrightarrow R(\mathbf{n}, a^2\mathbf{n}')$. In particular, if $\mathbf{q}$ is similar to $\mathbf{q}'$ then $\mathbf{n}$ is similar to $\mathbf{n}'$.

Remark 6.7. The lift Ψ is also compatible with the bijection $R(\mathbf{q}, p^2\mathbf{q}') \longrightarrow R(\mathbf{q}', p^2\mathbf{q})$ given by $A \mapsto p^2A^{-1}$ in the sense that $\Psi_{p^2A^{-1}} = p^2\Psi_A^{-1} \in R(\mathbf{n}', p^2\mathbf{n})$. Indeed, the fact that $\Psi_{p^2A^{-1}}$ and $p^2\Psi_A^{-1}$ both belong to $R(\mathbf{n}', p^2\mathbf{n})$ follows directly from definition of Ψ. Then using the equality $N'[\Psi_{p^2A^{-1}}] = N'[p^2\Psi_A^{-1}]$ together with (6.12) and (6.28), we see that $\Psi_{p^2A^{-1}} = p^2\Psi_A^{-1}$.

Chapter 7

Factorization of automorph lifts

Thus, we can lift an automorph $A \in R(\mathbf{q}, p^2\mathbf{q}')$ of ternary quadratic forms to an automorph $\Psi_A \in R(\mathbf{n}, p^2\mathbf{n}')$ of quaternary forms (see 5.28). But with quaternary quadratic forms we are no longer limited to multipliers p^2 and can use automorphs with multipliers p (compare to the existence of Hecke operators $T(p)$ rather than $T(p^2)$ for corresponding theta-series). By [2, Theorem 1.3], each integral automorph $\mathcal{A} \in R(\mathbf{n}, p^2\mathbf{n}')$, $p \not| \det \mathbf{n}$ is a product $\mathcal{ML}$ of automorphs $\mathcal{M} \in R(\mathbf{n}, p\mathbf{f})$ and $\mathcal{L} \in R(\mathbf{f}, p\mathbf{n}')$ for some quadratic form $\mathbf{f}$ similar to $\mathbf{n}$. Our next goal is to describe explicitly such factorizations for the lift $\Psi_A \in R(\mathbf{n}, p^2\mathbf{n}')$ constructed above. Since the general strategy behind Clifford algebras is to replace questions about representations by quadratic forms with questions concerning multiplicative arithmetic of these algebras, we shall try to use certain properties of ideals of the algebras for our purposes. First, we are going to look more closely at the algebraic homomorphism φ_A in (6.26) the restriction of which to the even subalgebra $C_0(E'', p^2\mathbf{q}')$ defines the lift Ψ_A via (6.28). Recall that the restricted φ_A can be regarded as a ring homomorphism

$$\varphi_A : (e'_0, p^2e'_{23}, -p^2e'_{13}, p^2e'_{12})\mathbb{Z}^4 \longrightarrow C_0(E, \mathbf{q}) \ ,$$
$$(\varphi_A(e'_0), \varphi_A(p^2e'_{23}), \varphi_A(-p^2e'_{13}), \varphi_A(p^2e'_{12})) = (e_0, e_{23}, -e_{13}, e_{12}) \cdot \Phi_A \ ,$$

defined on the corresponding order of $C_0(E', \mathbf{q}')$. This homomorphism can easily be extend to an isomorphism of $\mathbb{Q}$-algebras:

$$\varphi_A : C_0(E', \mathbf{q}') \otimes \mathbb{Q} \longrightarrow C_0(E, \mathbf{q}) \otimes \mathbb{Q} \ ,$$

whose matrix with respect to the natural bases is $\Phi_A \cdot \operatorname{diag}(1, p^{-2}, p^{-2}, p^{-2}) = p^{-1}\Psi_A$. Using Lemma 6.5 one can see that the matrix $\Phi_A \cdot \operatorname{diag}(1, p^{-1}, p^{-1}, p^{-1})$ is integral, which implies that the image under φ_A of the order of $C_0(E')$ generated by $e_0, pe'_{23}, -pe'_{13}, pe'_{12}$ belongs to $C_0(E)$. Then from (6.28) it follows that the submodule $(e_0, e_{23}, -e_{13}, e_{12})\Psi_A \cdot \mathbb{Z}^4 \subset C_0(E)$ is none other than the image $\varphi_A(p\,C_0(E'))$ of the principle ideal $p\,C_0(E') \subset C_0(E')$ and therefore is itself an ideal of the of the order $\varphi_A(C_0(E')) \cap C_0(E)$. Consider the left $C_0(E)$-ideal

$$\mathfrak{I}_A = C_0(E) \cdot \varphi_A(p\,C_0(E')) \ , \tag{7.1}$$

which extends $\varphi_A(p\,C_0(E'))$.

Lemma 7.1. *In the above notation, $\mathfrak{I}_A$ is a proper (left) $C_0(E)$-ideal that properly includes $\varphi_A(p\,C_0(E'))$:*

$$\varphi_A(p\,C_0(E')) \subset \mathfrak{I}_A \subset C_0(E) \ .$$

Moreover, the norm of any element of $\mathfrak{I}_A$ is divisible by p.

Proof. The inclusions themselves are clear, and we only need to prove that both of them are proper. To show that $\varphi_A(p\,C_0(E')) \neq \mathfrak{I}_A$, suppose the contrary. Since $\mathfrak{I}_A$ is a left $C_0(E)$-ideal, we would then obtain the inclusion $c \cdot \varphi_A(p\,C_0(E')) \subset \varphi_A(p\,C_0(E'))$ for any $c \in C_0(E)$. Recall that, as an isomorphism of $\mathbb{Q}$-algebras φ_A is invertible, the matrix of φ_A^{-1} with respect to the natural bases is $p\Psi_A^{-1} = p^{-1}\Psi_{p^2A^{-1}}$, in particular $\varphi_A^{-1}(C_0(E)) \subset p^{-1}C_0(E')$. Thus, our assumption would imply that $\varphi_A(\varphi_A^{-1}(c) \cdot p\,C_0(E')) \subset \varphi_A(p\,C_0(E'))$ and so $\varphi_A^{-1}(c) \cdot p\,C_0(E') \subset p\,C_0(E')$ for any $c \in C_0(E)$. The latter inclusion would be possible only if $\varphi_A^{-1}(c) \in C_0(E')$ for any $c \in C_0(E)$, which is definitely not the case (for example for $c = e_{23}$). Therefore $\varphi_A(p\,C_0(E'))$ is a proper subset of $\mathfrak{I}_A$. Next, to prove that $\mathfrak{I}_A \neq C_0(E)$ we show that the norm of any element of $\mathfrak{I}_A$ is divisible by p. Indeed, any element of $\mathfrak{I}_A = C_0(E) \cdot \varphi_A(p\,C_0(E'))$ is a sum of elements of the form $c \cdot \varphi_A(pc')$ with $c \in C_0(E)$ and $c' \in C_0(E')$. Observe that $\mathbf{n}(\varphi_A(pc')) \equiv 0 \pmod{p^2}$ for any $c' \in C_0(E')$, by Lemma 6.5 . It remains to note that if $b, c \in C_0(E)$ and $b', c' \in C_0(E')$ then

$$\mathbf{n}(b\,\varphi_A(pb') + c\,\varphi_A(pc')) = \mathbf{n}(b\,\varphi_A(pb')) + \mathbf{n}(c\,\varphi_A(pc')) + \mathbf{s}(b\,\varphi_A(pb') \cdot \overline{c\,\varphi_A(pc')}) \ \equiv$$

$$\mathbf{s}(b\,\varphi_A(pb')\cdot\varphi_A(p\,\overline{c'})\,\bar{c}) \;\equiv\; \mathbf{s}(pb\,\varphi_A(pb'\,\overline{c'})\,\bar{c}) \;\equiv\; p\cdot\mathbf{s}(b\,\varphi_A(pb'\,\overline{c'})\,\bar{c}) \;\equiv\; 0 \pmod{p}\ ,$$

therefore $\mathbf{n}\,|_{\mathfrak{I}_A} \equiv 0 \pmod{p}$ as claimed and so $\mathfrak{I}_A$ is a proper subset of $C_0(E)$. □

The above lemma immediately leads to the following statement.

Lemma 7.2. *Let $\mathcal{I}_A$ be a generating matrix of the extension ideal $\mathfrak{I}_A$ (7.1) with respect to the natural basis, so that $\mathfrak{I}_A = (e_0, e_{23}, -e_{13}, e_{12})\cdot\mathcal{I}_A\mathbb{Z}^4$. Then $\Psi_A \in \mathcal{I}_A\mathbb{Z}^4_4$, $\mathcal{I}_A \in R(\mathbf{n}, p\mathbf{f})$ where the integral quadratic form*

$$\mathbf{f}_{\mathfrak{I}_A} = \frac{\mathbf{n}\,|_{\mathfrak{I}_A}}{\sqrt{|\mathfrak{I}_A|}}$$

is similar to $\mathbf{n}$. Here we have set $|\mathfrak{I}_A| = |\mathcal{I}_A| = |C_0(E)/\mathfrak{I}_A|$, the index of $\mathfrak{I}_A$ in $C_0(E)$.

Proof. Indeed, since $\mathfrak{I}_A$ is a proper (left) ideal of $C_0(E)$, we know that $|\mathcal{I}_A| \neq 1$. Moreover, for a fixed element $\mathfrak{i} \in \mathfrak{I}_A$ we have $C_0(E)\cdot\mathfrak{i} \subset \mathfrak{I}_A$ and thus $C_0(E)\cdot\mathfrak{i} = (e_0\mathfrak{i}, e_{23}\mathfrak{i}, -e_{13}\mathfrak{i}, e_{12}\mathfrak{i})\,\mathbb{Z}^4 = (e_0, e_{23}, -e_{13}, e_{12})\cdot\mathcal{I}_A\mathcal{Y}\,\mathbb{Z}^4$ with some $\mathcal{Y} \in \mathbb{Z}^4_4$. Then, looking at the matrix of the restriction of the norm-form $\mathbf{n}$ to the submodule $C_0(E)\cdot\mathfrak{i} \subset C_0(E)$ we see that $\mathbf{n}(\mathfrak{i})N = N[\mathcal{I}_A\mathcal{Y}]$ which implies that $|\mathfrak{I}_A|$ divides $\mathbf{n}^2(\mathfrak{i})$. Denote $|\mathcal{I}_A| = a^2b$ with a square-free positive integer b. Clearly, then ab divides $\mathbf{n}(\mathfrak{i})$, but $\mathfrak{i} \in \mathfrak{I}_A$ was arbitrary and therefore the form $\frac{1}{ab}\mathbf{n}|_{\mathfrak{I}_A}$ is integral as well as its matrix $(ab)^{-1}N[\mathcal{I}_A]$ with respect to the natural basis. In particular $\det\big((ab)^{-1}N[\mathcal{I}_A]\big) = (|\mathfrak{I}_A|^2\det\mathbf{n})/(ab)^4 = (\det\mathbf{n})/b^2 = (\Delta/b)^2$ is integral and so b divides $\Delta = \det\mathbf{q}/2$, see (6.13). On the other hand, using Lemma 7.1 we also see that $\varphi_A(p\,C_0(E'))$ is a proper subset of $\mathfrak{I}_A$ which in terms of corresponding matrices means that $\Psi_A = \mathcal{I}_A\mathcal{X}$ for some $\mathcal{X} \in \mathbb{Z}^4_4$, $|\mathcal{X}| \neq 1$ and in particular $|\mathfrak{I}_A|$ is a proper divisor of $|\Psi_A| = p^4$. Therefore $b \mid \gcd(\Delta, p^4)$, but in accordance with our assumption the prime p is coprime to $\det\mathbf{q} = 2\Delta$ thus $b = 1$ and $|\mathfrak{I}_A| = p^2$. We conclude that the quadratic form

$$\mathbf{f}_{\mathfrak{I}_A}(x) = \frac{\mathbf{n}\,|_{\mathfrak{I}_A}(x)}{\sqrt{|\mathfrak{I}_A|}} = p^{-1}\cdot\mathbf{n}\,|_{\mathfrak{I}_A}(x) \tag{7.2}$$

is integral. The matrix of $\mathbf{f}_{\mathfrak{J}_A}$ with respect to the natural basis $(e_0, e_{23}, -e_{13}, e_{12})\cdot\mathcal{I}_A$ is $F_{\mathfrak{J}_A} = p^{-1}N[\mathcal{I}_A] \in \mathbb{Z}_4^4$ and its determinant $\det \mathbf{f}_{\mathfrak{J}_A}$ is equal to $\det \mathbf{n}$. Summing up we see that $\mathbf{f}_{\mathfrak{J}_A}$ is *similar* to $\mathbf{n}$ and that $\mathcal{I}_A \in R(\mathbf{n}, p\,\mathbf{f}_{\mathfrak{J}_A})$. □

In essence, Lemmas 7.1 and 7.2 allow us to write a lift $\Psi_A \in R(\mathbf{n}, p^2\mathbf{n}')$ as a product of automorphs with multipliers p of *similar* quadratic forms $\mathbf{n}$, $\mathbf{n}'$ and $\mathbf{f}$. Note that the quadratic form $\mathbf{f} = \mathbf{f}_{\mathfrak{J}_A}$ in the above factorization is associated with a class of equivalent (left) ideals of $C_0(E, \mathbf{q})$ and is defined only up to integral equivalence, see (7.2). (Two left $C_0(E)$-ideals $\mathfrak{I}, \mathfrak{J} \subset C_0(E)$ are called *equivalent* if $\mathfrak{I}\alpha = \mathfrak{J}\beta$ for some $\alpha, \beta \in C_0(E)$.) A similar factorization of Ψ_A can be obtained if we consider the extension of $\varphi_A(p\,C_0(E'))$ to the right ideal $\varphi_A(p\,C_0(E'))\cdot C_0(E)$ instead of the left ideal as in (7.1). Now we seek to find the total number of such factorizations (different modulo corresponding groups of units) for a given Ψ_A. Following a general method developed in [1], we shall view a matrix $\mathcal{M} \in R(\mathbf{n}, p\,\mathbf{f})$ for a quadratic form $\mathbf{f}$ *similar* to $\mathbf{n}$ as a solution of the quadratic congruence

$$\mathbf{n}[\mathcal{M}] \equiv 0 \pmod{p} ,$$

whose matrix of *elementary divisors* is equal to $\mathcal{D}_p = \operatorname{diag}(1, 1, p, p)$. That is to say, $\mathcal{M}$ belongs to the double coset $\Lambda^4\mathcal{D}_p\Lambda^4$ which is a necessary condition for $\mathcal{M}$ to determine an automorph with multiplier p of similar quaternary quadratic forms. (Indeed, we should have $|\mathcal{M}| = p^2$ and $p\mathcal{M}^{-1} \in \mathbb{Z}_4^4$, which leaves us with $\mathcal{D}_p$ as the only possible matrix of elementary divisors.) Since at the moment we do not want to distinguish a particular form $\mathbf{f}$ in its equivalent class $\{\mathbf{f}[\mathcal{U}]\ ;\ \mathcal{U} \in \Lambda^4\}$, we will next be counting only different left cosets $\mathcal{M}\Lambda^4 \subset \Lambda^4\mathcal{D}_p\Lambda^4/\Lambda^4$. Finally, because of our interest in factorizations of automorphs with multipliers p^2, we restrict our search to only those automorphs $\mathcal{M}$, which divide (from the left) a particular $\mathcal{A} \in R(\mathbf{n}, p^2\mathbf{n}')$. Thus, following [1], in order to find the total number of factorizations of $\mathcal{A}$ one introduces *isotropic sums*

$$\mathcal{S}_p(\mathbf{n},\mathcal{D}_p,\mathcal{A}) = \sum_{\substack{\mathcal{M}\in\Lambda^4\mathcal{D}_p\Lambda^4/\Lambda^4\\ \mathbf{n}[\mathcal{M}]\equiv 0 \pmod{p}\,,\,\mathcal{M}|\mathcal{A}}} 1\ . \tag{7.3}$$

General isotropic sums of the above type were computed in [1, Theorem 5.1] (see also [2] and [4]). The idea behind the computation is to relate a matrix $\mathcal{L}\in\mathbb{Z}_*^4$ to the subspace $V_p(\mathcal{L})$ of the quadratic space $\Big((\mathbb{Z}/p\mathbb{Z})^4, \mathbf{n} \bmod p\Big)$ spanned by the columns of $\mathcal{L}$ modulo p. Then the summation conditions on $\mathcal{M}$ in (7.3) mean exactly that $V_p(\mathcal{M})$ is a 2-dimensional isotropic subspace of $\Big((\mathbb{Z}/p\mathbb{Z})^4, \mathbf{n}\Big)$ which contains fixed subspace $V_p(\mathcal{A})$. The number of such subspaces can be found with help of standard methods of Geometric Algebra over finite fields (see [9]). Specializing results of [1, Theorem 5.1] to our case we find that

$$\mathcal{S}_p(\mathbf{n},\mathcal{D}_p,\mathcal{A}) \quad = \quad \begin{cases} 1 & \text{if } \operatorname{rank}_{\mathbb{F}_p}\mathcal{A}=2,\\ 1+\chi_{\mathbf{n}}(p) & \text{if } \operatorname{rank}_{\mathbb{F}_p}\mathcal{A}=1,\\ (1+\chi_{\mathbf{n}}(p))(p+1) & \text{if } \operatorname{rank}_{\mathbb{F}_p}\mathcal{A}=0,\end{cases} \tag{7.4}$$

where $p\not|\det\mathbf{q}$ and $\chi_{\mathbf{n}}(p)$ is the character (3.4) of the form $\mathbf{n}$. (Note that $\chi_{\mathbf{n}}(p)=1$ for $p\not|\det\mathbf{q}$ because of (6.13).) The above sum can be rewritten as follows. The condition $N[\mathcal{M}] \equiv 0 \pmod{p}$ means that $N[\mathcal{M}] = p\,F$ for some even matrix F of oder 4. Since $\det\mathcal{M} = \det\mathcal{D}_p = p^2$, we have $\det F = \det N$ and thus the quadratic form $\mathbf{f}(X)=2^{-1}F[X]$ is *similar* to $\mathbf{n}$. Since $\mathcal{M}$ is determined only modulo right multiplication by Λ^4, we can replace F by any (integrally) equivalent form $F[\mathcal{U}]$, $\mathcal{U}\in\Lambda^4$. We fix a complete system $\{\mathbf{n}_1,\ldots,\mathbf{n}_H\}$ of representatives of different equivalence classes of the similarity class of $\mathbf{n}$ (as in (5.2)). Note that $h\le H$ because we can choose $\mathbf{n}_i$ with $1\le i\le h$ to be quadratic forms defined by the norms on the even Clifford subalgebras $C_0(\mathbb{Z}^3,\mathbf{q}_i)$, $1\le i\le h$. (Indeed, by Lemmas 6.4 and 6.5 these $\mathbf{n}_i$'s $1\le i\le h$ belong to the different equivalence classes of the same similarity class.) Then for each $\mathcal{M}\in\Lambda^4\mathcal{D}_p\Lambda^4/\Lambda^4$ with $N[\mathcal{M}] \equiv 0 \pmod{p}$ there exists a unique number i, $1\le i\le H$ such that $\mathbf{n}[\mathcal{M}\mathcal{U}]=p\,\mathbf{n}_i$ for some $\mathcal{U}\in\Lambda^4$. Next we note that by the theory of elementary divisors (see [3, Lemma 3.2.2]) $R(\mathbf{n},p\,\mathbf{n}_i)\subset\Lambda^4\mathcal{D}_p\Lambda^4$, therefore,

$$\mathcal{S}_p(\mathbf{n}, \mathcal{D}_p, \mathcal{A}) \;=\; \sum_{i=1}^{H} \sum_{\substack{\mathcal{M}\in R(\mathbf{n}, p\,\mathbf{n}_i)/E(\mathbf{n}_i) \\ \mathcal{M}|\mathcal{A}}} 1 \;, \tag{7.5}$$

which already resembles the right hand side of the conjectural relation (5.5) we seek to establish. Similar considerations of another isotropic sum allow us to compute also the left hand side of (5.5). Indeed, let $\{\mathbf{q}_1, \ldots, \mathbf{q}_h\}$ be a complete system (5.2). By the theory of elementary divisors the set of primitive automorphs $R^*(\mathbf{q}, p^2\mathbf{q}_i)$ coincides with $R(\mathbf{q}, p^2\mathbf{q}_i) \cap \Lambda^3 D_p \Lambda^3$, where $D_p = \mathrm{diag}(1, p, p^2)$, see [4 Lemma 3.1]. Conversely, any $A \in \Lambda^3 D_p \Lambda^3/\Lambda^3$ such that $Q[A] \equiv 0 \pmod{p^2}$ defines a quadratic form, namely, $p^{-2}\,\mathbf{q}[A]$, which is *similar* to $\mathbf{q}$ and therefore is integrally equivalent to exactly one of the forms $\mathbf{q}_i$ so that $\mathbf{q}[AU] = p^2\mathbf{q}_i$ for a unique number i , $1 \le i \le h$ and some $U \in \Lambda^3$. We conclude that

$$\sum_{i=1}^{h} \sum_{A\in R^*(\mathbf{q}, p^2\mathbf{q}_i)/E(\mathbf{q}_i)} 1 \;=\; \mathcal{S}_{p^2}(\mathbf{q}, D_p, O_3) \;=\; \sum_{\substack{A\in \Lambda^3 D_p \Lambda^3/\Lambda^3 \\ Q[A]\equiv 0 \pmod{p^2}}} 1 \;, \tag{7.6}$$

where O_3 is the zero matrix of order 3. Furthermore, using [4, Theorem 2.2] we can provide an explicit value of the isotropic sum (7.6):

$$\mathcal{S}_{p^2}(\mathbf{q}, D_p, O_3) \;=\; p+1 \;. \tag{7.7}$$

Combining formulas (7.3)–(7.7) we finally establish (5.5) and deduce the following Theorem, which expresses total number of ternary automorphs of $\mathbf{q}$ with multiplier p^2 in terms of quaternary automorphs with multiplier p and can be viewed as a generalization of Shimura's correspondence for theta-series of ternary positive definite quadratic forms to the case of indeterminate forms:

Theorem 7.3. *Let* $\mathbf{q}$ *be an integral nonsingular ternary quadratic form (6.1) with determinant* $\det \mathbf{q} = 2\Delta$ *, and let* p *be a prime not dividing* 2Δ *. Fix a complete system* $\{\mathbf{q}_1, \ldots, \mathbf{q}_h\}$ *of representatives of different equivalence classes of the similarity* *class of* $\mathbf{q}$. *Then*

$$\sum_{A\in\bigcup_{i=1}^{h} R^*(\mathbf{q},p^2\mathbf{q}_i)/E(\mathbf{q}_i)} 1 \quad = \quad (1+\chi_{\mathbf{n}}(p))^{-1} \sum_{M\in\bigcup_{i=1}^{H} R(\mathbf{n},p\mathbf{n}_i)/E(\mathbf{n}_i)} 1\,,$$

where $\mathbf{n}$ *is the integral quaternary quadratic form determined (in some basis) by the norm (6.10) on the even subalgebra* $C_0(E)$ *of the Clifford Algebra* $C(E,\mathbf{q})$, $\chi_{\mathbf{n}}(p) = \left(\frac{(-1)^2\Delta^2}{p}\right)$ *is the character (3.4) of* $\mathbf{n}$, *and* $\{\mathbf{n}_1,\dots,\mathbf{n}_H\}$ *is a complete system of representatives of equivalent classes in the similarity class of* $\mathbf{n}$.

Proof. Indeed, taking $\mathcal{A}$ to be the zero matrix of order 4 in (7.4) and using (7.7) we see that

$$\mathcal{S}_{p^2}(\mathbf{q},D_p,O_3) \;=\; (1+\chi_{\mathbf{n}}(p))^{-1}\,\mathcal{S}_p(\mathbf{n},\mathcal{D}_p,O_4)$$

Because of (7.5) and (7.6), this relation between the isotropic sums is equivalent to the above relation between numbers of automorphs, which also proves (5.5). □

Tracing back the considerations of section 4, we can see that the above theorem immediately implies the following statement.

Corollary 7.4. *With the notation and under the assumptions of Theorem 7.3, let in addition* $\mathbf{q}$ *be positive definite. Then Shimura's lift of the generic theta-series* $\Theta_{\{\mathbf{q}\}}(z)$ *and the generic theta-series* $\Theta_{\{\mathbf{n}\}}(z)$ *of the norm* $\mathbf{n}$ *on the even Clifford subalgebra* $C_0(E,\mathbf{q})$ *have the same eigenvalues* $p+1$ *for all Hecke operators* $T(p)$ *with* $p\not|\det\mathbf{q}$. □

Unfortunately, up to the present the isotropic sums of type (7.3) or (7.6) have not been computed in the case of prime p dividing the determinant of the corresponding quadratic form. This prevents us from comparing directly the eigenvalues of $\Theta_{\{\mathbf{n}\}}(z)$ and of Shimura's lift of $\Theta_{\{\mathbf{q}\}}(z)$ on singular Hecke operators $T(p)$, where p is a divisor of the level. Thus, the question as to whether Shimura's lift of $\Theta_{\{\mathbf{q}\}}(z)$ for an arbitrary ternary form $\mathbf{q}$ is always proportional to $\Theta_{\{\mathbf{n}\}}(z)$ remains open.

Nevertheless automorph class lifting $A\mapsto\Psi_A$ (6.30) constructed in section 5 allows us to make progress in another direction and exhibit algebraic origins of the relation (5.5) and, therefore, of Shimura's correspondence for generic theta-series. Indeed, because of Eichler's commutation relation (3.5), linear combinations of theta-series invariant under Hecke operators (such as generic theta-series, for example) are determined by corresponding sets of automorphs with multipliers p or p^2 (in accordance with the weight of the theta-series). Thus, algebraic relations between various sets of automorphs can in principle be responsible for correspondences between certain linear combinations of theta-series. (Moreover, they can provide a natural generalization of such correspondences to the case of indeterminate forms.) In particular, in the case of Shimura's lift of generic theta-series of ternary forms we seek relations between two sets of automorphs:

$$\bigcup_{i=1}^{h} E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q}) \qquad \text{and} \qquad \bigcup_{j=1}^{H} E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n}) \ ,$$

of ternary and quaternary quadratic forms respectively. Recall that by factoring Ψ_A in Lemmas 7.1 and 7.2, we extended our automorph lift $A \mapsto \Psi_A$ to an inclusion $A \mapsto \mathcal{I}_A$ of $\cup_i E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q})$ into $\cup_j E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n})$. Now we claim that this map is in fact an injection whose inverse can be extended in a natural way, which turns the set of quaternary automorphs with multiplier p into a 2-fold covering of the set of ternary automorphs with multipliers p^2. More precisely we have the following

Theorem 7.5. *Let* $\mathbf{q}$ *be an integral nonsingular ternary quadratic form with matrix* Q *given by (6.3), and let* N *be the matrix (6.12). If* p *is a prime number coprime to* $\det \mathbf{q}$, *then for any* $\mathcal{M} \in \Lambda^4 \mathcal{D}_p \Lambda^4/\Lambda^4$ *such that* $N[\mathcal{M}] \equiv 0 \pmod{p}$ *there exists (a unique)* $A \in \Lambda^3 D_p \Lambda^3/\Lambda^3$ *such that* $Q[A] \equiv 0 \pmod{p^2}$ *and* $\mathcal{M}|\Psi_A$ *(see (6.28)).*

Proof. First of all, if $\mathcal{M}|\Psi_A$, then $\mathcal{M}^{-1}\Psi_A$ is an integral automorph (of quaternary forms) with multiplier p, and thus $p\Psi_A^{-1}\mathcal{M}$ is an integral matrix. Therefore, using Remark 6.7 we see that

$$\mathcal{M}|\Psi_A \Longleftrightarrow \Psi_{p^2A^{-1}} \cdot \mathcal{M} \equiv 0 \pmod{p} \ . \tag{7.8}$$

Next, let $\mathcal{M} = \mathcal{U}\mathcal{D}_p\mathcal{W}$ with $\mathcal{U}, \mathcal{W} \in \Lambda^4$. Since $N[\mathcal{M}] \equiv 0 \pmod{p}$ if and only if

$N[\mathcal{M}\mathcal{W}^{-1}] \equiv 0 \pmod{p}$, $\Psi_{p^2A^{-1}}\mathcal{M} \equiv 0 \pmod{p}$ if and only if $\Psi_{p^2A^{-1}}\mathcal{M}\mathcal{W}^{-1} \equiv 0 \pmod{p}$ and $\mathcal{M}$ is defined only up to right multiplication by Λ^4, it is suffices to consider $\mathcal{W} = 1_4$ and $\mathcal{M} = \mathcal{U}\mathcal{D}_p$.

Similarly, let $A = VD_pW$ with $V, W \in \Lambda^3$. Clearly $Q[A] \equiv 0 \pmod{p^2}$ if and only if $Q[AW^{-1}] \equiv 0 \pmod{p^2}$. We also claim that $\Psi_{p^2A^{-1}}\mathcal{M} \equiv 0 \pmod{p}$ if and only if $\Psi_{p^2WA^{-1}}\mathcal{M} \equiv 0 \pmod{p}$. Indeed, consider the following commutative diagram:

$$\begin{tikzcd}
(\mathbb{Z}^3, \mathbf{q}[p^{-1}AW^{-1}]) \arrow[d, "\iota"] & (\mathbb{Z}^3, \mathbf{q}[p^{-1}A]) \arrow[l, "\alpha_W"'] \arrow[d, "\iota"] & (E, p^2\mathbf{q}) \arrow[l, "\alpha_{p^2A^{-1}}"'] \arrow[d, "\iota"] \\
C(\mathbb{Z}^3, \mathbf{q}[p^{-1}AW^{-1}]) & C(\mathbb{Z}^3, \mathbf{q}[p^{-1}A]) \arrow[l, "\varphi_W"'] & C(E, p^2\mathbf{q}) \arrow[l, "\varphi_{p^2A^{-1}}"']
\end{tikzcd}$$

Using (6.20),(6.22) and (6.28) we can see that $\Psi_{p^2WA^{-1}} = \Phi_W \cdot \Psi_{p^2A^{-1}} \in \Lambda^4\Psi_{p^2A^{-1}}$ because φ_W is an isomorphism of Clifford algebras. Thus we can take $W = 1_3$ and $A = VD_p$. Next we set $V = (V_1, V_2, V_3)$ and

$$\mathcal{U} = (\mathcal{U}_1, \mathcal{U}_2, \mathcal{U}_3, \mathcal{U}_4) = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 \\ \check{U}_1 & \check{U}_2 & \check{U}_3 & \check{U}_4 \end{pmatrix}.$$

Thus given $\mathcal{M} = \mathcal{U}\mathcal{D}_p = (\mathcal{U}_1, \mathcal{U}_2, p\mathcal{U}_3, p\mathcal{U}_4)$ with ${}^t\mathcal{U}_iN\mathcal{U}_j \equiv 0 \pmod{p}$ for $i = 1, 2$ we want to find $A = VD_p = (V_1, pV_2, p^2V_3)$ such that $V \in \Lambda^3$ with $Q[V_1] \equiv 0 \pmod{p^2}$, ${}^tV_2QV_1 \equiv 0 \pmod{p}$ and

$$\Psi_{p^2A^{-1}} \cdot \mathcal{M} = \begin{pmatrix} p & {}^tZ \\ 0 & {}^tV_1 \\ 0 & p\,{}^tV_2 \\ 0 & p^2\,{}^tV_3 \end{pmatrix} \cdot \begin{pmatrix} u_1 & u_2 & p\,u_3 & p\,u_4 \\ \check{U}_1 & \check{U}_2 & p\,\check{U}_3 & p\,\check{U}_4 \end{pmatrix} \equiv 0 \pmod{p},$$

where $Z = p^{-1}Z_{(p^2A^{-1})}$ depends on V, see (6.28). The latter condition is equivalent to the system of congruences ${}^tZ\check{U}_i \equiv 0 \pmod{p}$, ${}^tV_1\check{U}_i \equiv 0 \pmod{p}$ for $i = 1, 2$.

Note that all of the above conditions on the columns of a matrix $V \in \Lambda^3$ are modulo p (or p^2) and therefore the choice of particular representatives $\bmod p^2$ is irrelevant as long as $V \in \Lambda^3$. Recall that columns $V_1, V_2 \in \mathbb{Z}^3$ can be complemented to a matrix $(V_1, V_2, V_3) \in \Lambda^3$ if and only if the greatest common divisor of principal minors of $(V_1, V_2) \in \mathbb{Z}_2^3$ is 1. Using the above remarks and Lemma 2.3 above we can replace the condition $V \in \Lambda^3$ by linear independence of V_1 and V_2 modulo p. Thus, combining all the conditions, we need to find $V_1, V_2 \in \mathbb{Z}^3$ such that V_1, V_2 are linearly independent modulo p and

$$\begin{cases} Q[V_1] \equiv 0 \pmod{p^2} \\ {}^tV_2QV_1 \equiv 0 \pmod{p} \\ {}^tV_1 \cdot \check{U}_i \equiv 0 \pmod{p} \quad \text{for } i = 1, 2 \\ {}^tZ \cdot \check{U}_i \equiv 0 \pmod{p} \quad \text{for } i = 1, 2 \; . \end{cases}$$

Denote

$$\mathcal{W} = {}^t\mathcal{U}^{-1} = (\mathcal{W}_1, \mathcal{W}_2, \mathcal{W}_3, \mathcal{W}_4) = \begin{pmatrix} w_1 & w_2 & w_3 & w_4 \\ \check{W}_1 & \check{W}_2 & \check{W}_3 & \check{W}_4 \end{pmatrix} \in \Lambda^4 \; ,$$

then ${}^t\mathcal{W} \cdot \mathcal{U} = ({}^t\mathcal{W}_i \cdot \mathcal{U}_j) = 1_4$ which implies that $w_i \cdot u_j + {}^t\check{W}_i \cdot \check{U}_j \equiv 0 \pmod{p}$ if $i \neq j$. Next,since $N[\mathcal{U}\mathcal{D}_p] \equiv 0 \pmod{p}$, using (6.14) we obtain

$$\tilde{N}[{}^t\mathcal{U}^{-1}] = \Delta \cdot \begin{pmatrix} 2\det Q_0 & {}^t(Q_0B) \\ & \\ (Q_0B) & Q \end{pmatrix} \left[\begin{pmatrix} & w_i & \\ \cdots & & \cdots \\ & \check{W}_i & \end{pmatrix} \right] = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & p & p \\ * & * & p & p \end{pmatrix}$$

and therefore ${}^t\mathcal{W}_i\tilde{N}\mathcal{W}_j \equiv 0 \pmod{p}$ for $i, j = 3, 4$. Since $\mathcal{W} \in \Lambda^4$, the columns $\mathcal{W}_3, \mathcal{W}_4$ are linearly independent modulo p and thus their linear span (over $\mathbb{F}_p$) contains a column $\mathcal{X} \not\equiv 0 \pmod{p}$ whose first component is zero modulo p:

$$a\mathcal{W}_3 + b\mathcal{W}_4 = \mathcal{X} \equiv \begin{pmatrix} 0 \\ \check{X} \end{pmatrix} \pmod{p} \quad , \quad \check{X} \not\equiv 0 \pmod{p} \; .$$

Using the properties of $\mathcal{W}_3, \mathcal{W}_4$ exhibited above, we see that ${}^t\check{X}\check{U}_i \equiv {}^t\mathcal{X}\mathcal{U}_i \equiv 0 \pmod{p}$ for $i = 1, 2$ and $Q[\check{X}] \equiv \Delta^{-1}\tilde{N}[\mathcal{X}] \equiv 0 \pmod{p}$. By [4, Lemma 2.3] there exists p^2 distinct (modulo p^2) columns $X \in \mathbb{Z}^3$ such that $X \equiv \check{X} \pmod{p}$ and $Q[X] \equiv 0 \pmod{p^2}$. For any of these columns we can take $V_1 \equiv X \pmod{p^2}$.

Next, consider the congruence ${}^tV_1QY \equiv 0 \pmod{p}$ as a linear equation with 3 variables over $\mathbb{F}_p$. Since $Q \in GL_3(\mathbb{F}_p)$ and $V_1 \not\equiv 0 \pmod{p}$, we also have ${}^tV_1Q \not\equiv 0 \pmod{p}$ and therefore the space of solutions of the above equation is two dimensional. One nontrivial solution is V_1. Thus there exists $V_2 \in \mathbb{Z}^3$ such that ${}^tV_1QV_2 \equiv 0 \pmod{p}$ and V_1, V_2 are linearly independent modulo p. Using Lemma 2.3 we can change V_1 and V_2 modulo p^2 in such a way that the matrix (V_1, V_2) becomes primitive and therefore complementable to an invertible matrix $V = (V_1, V_2, V_3) \in \Lambda^3$. Thus given $\mathcal{U} \in \Lambda^4$ such that $N[\mathcal{U}\mathcal{D}_p] \equiv 0 \pmod{p}$ we can find $V \in \Lambda^3$ such that $Q[VD_p] \equiv 0 \pmod{p^2}$ and ${}^tV_1\check{U}_i \equiv 0 \pmod{p}$ for $i = 1, 2$. To prove the Theorem we still need to show that ${}^tZ\check{U}_i \equiv 0 \pmod{p}$ for $i = 1, 2$ (Z depends on V, see above). Luckily, this condition is met automatically with our choice of V. Indeed, set $A = VD_p$ and $\mathbf{q}' = p^{-2} \cdot \mathbf{q}[A]$, then $A \in R(\mathbf{q}, p^2\mathbf{q}')$ and so $p^2\Psi_A^{-1} = \Psi_{p^2A^{-1}} \in R(\mathbf{n}', p^2\mathbf{n})$, in other words $N'[\Psi_{p^2A^{-1}}] = p^2N$ (see (6.12),(6.27) and Remark 6.7). Then $N'[\Psi_{p^2A^{-1}} \cdot \mathcal{U}_i] = p^2N[\mathcal{U}_i] \equiv 0 \pmod{p^3}$ for $i = 1, 2$. But

$$\Psi_{p^2A^{-1}} \cdot \mathcal{U}_i = \begin{pmatrix} p & {}^tZ \\ 0 & {}^tV_1 \\ 0 & p\,{}^tV_2 \\ 0 & p^2\,{}^tV_3 \end{pmatrix} \cdot \begin{pmatrix} u_i \\ \\ \check{U}_i \end{pmatrix} \equiv \begin{pmatrix} {}^tZ\check{U}_i \\ 0 \\ 0 \\ 0 \end{pmatrix} \pmod{p} \qquad \text{for} \quad i = 1, 2$$

by the above choice of V, therefore using (6.12) we have $N'[\Psi_{p^2A^{-1}} \cdot \mathcal{U}_i] \equiv 2({}^tZ\check{U}_i)^2 \equiv 0 \pmod{p}$ and so ${}^tZ\check{U}_i \equiv 0 \pmod{p}$ for $i = 1, 2$ as claimed (recall that $p \neq 2$ since $2|\det \mathbf{q}$).

Summing up, there exists A such that $\Psi_{p^2A^{-1}} \cdot \mathcal{U}\mathcal{D}_p \equiv 0 \pmod{p}$, i.e. $\mathcal{M}|\Psi_A$. Finally, it is easy to see that for a given $\mathcal{M} \in \cup_i R(\mathbf{n}, p\mathbf{n}_i)/E(\mathbf{n}_i)$ such an $A \in \cup_j R(\mathbf{q}, p^2\mathbf{q}_j)/E(\mathbf{q}_j)$ is unique. Indeed, first note that since $A \in \Lambda^3 D_p \Lambda^3$ then the double coset $\Lambda^4\Psi_A\Lambda^4$ contains matrix of the form

$$\begin{pmatrix} p & * & * & * \\ 0 & & & \\ 0 & & D_p & \\ 0 & & & \end{pmatrix}$$

and so $\operatorname{rank}_{\mathbb{F}_p}\Psi_A$ is either 1 or 2. Then (7.4) implies that each $\Psi_A \in R(\mathbf{n}, p^2\mathbf{n}')$ is divisible from the left by at most $2 = 1 + \chi_{\mathbf{n}}(p)$ different cosets $\mathcal{M} \in \cup_{i=1}^{H} R(\mathbf{n}, p\mathbf{n}_i)/E(\mathbf{n}_i)$. (The same is true for any $A \in \cup_i R^*(\mathbf{q}, p^2\mathbf{q}_i)$). If the same $\mathcal{M}$ would divide Ψ_A for different classes of A's, then the union over A

$$\bigcup_{A\in \cup_{i=1}^{h} R^*(\mathbf{q},p^2\mathbf{q}_i)/E(\mathbf{q}_i)} \{ \ \mathcal{M} \in \cup_{j=1}^{H} R(\mathbf{n}, p\mathbf{n}_j)/E(\mathbf{n}_j) \ ; \ \mathcal{M}|\Psi_A \ \} \qquad (7.9)$$

would not be disjoint and, therefore, its cardinality would be less than

$$(1 + \chi_{\mathbf{n}}(p)) \cdot \sum_{i=1}^{h} r^*(\mathbf{q}, p^2\mathbf{q}_i)/e(\mathbf{q}_i) \qquad = \qquad (1 + \chi_{\mathbf{n}}(p)) \cdot (p + 1) \ .$$

On the other hand, we have proved that any $\mathcal{M} \in \cup_j R(\mathbf{n}, p\mathbf{n}_j)/E(\mathbf{n}_j)$ divides some Ψ_A from the left and, thus, belongs to the union (7.9), whose cardinality in view of this should be at least $(1 + \chi_{\mathbf{n}}(p)) \cdot (p + 1)$, see (7.4) and (7.5). We conclude that for any $\mathcal{M}$ there exists exactly one $A \in \Lambda^3 D_p \Lambda^3/\Lambda^3$ such that $Q[A] \equiv 0 \pmod{p^2}$ and $\mathcal{M}|\Psi_A$. Incidentally we have also proved that $\operatorname{rank}_{\mathbb{F}_p}\Psi_A = 1$ for any such A. □

Remark 7.6. The above result means that for any class $\mathcal{M}E(\mathbf{n}_i) \in R(\mathbf{n}, p\mathbf{n}_i)/E(\mathbf{n}_i)$ there exists a unique class $AE(\mathbf{q}_j) \in R^*(\mathbf{q}, p^2\mathbf{q}_j)/E(\mathbf{q}_j)$ such that any $\mathcal{M}' \in \mathcal{M}E(\mathbf{n}_i)$ divides from the left $\Psi_{A'}$ for any $A' \in AE(\mathbf{q}_j)$. Thus, the correspondence established above is indeed between classes modulo groups of units rather than between individual automorphs. (To see this, we let $A' = AE$ and $\mathcal{M}' = \mathcal{M}\mathcal{E}$ with $E \in E(\mathbf{q}_j)$, $\mathcal{E} \in E(\mathbf{n}_i)$. Then using (6.28), (7.8) and Lemma 6.3 we obtain $\mathcal{M}'|\Psi_{A'} \Leftrightarrow \Psi_{p^2A'^{-1}} \cdot \mathcal{M}\mathcal{E} \equiv 0 \pmod{p} \Leftrightarrow \Phi_{E^{-1}}\Psi_{p^2A^{-1}} \cdot \mathcal{M} \equiv 0 \pmod{p} \Leftrightarrow \mathcal{M}|\Psi_A$, because $\Phi_{E^{-1}} \in E(\mathbf{n}_j)$ and so it is invertible.)

In order to obtain a generalization of Shimura's lift in terms of the automorph class theory, we need to consider correspondences between left (rather than right) classes of automorphs. To this end we extend the automorph class lift Ψ (6.28) and define a map $\Upsilon : \cup_i E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q}) \to \cup_j E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n})$ via the following chain, the elements of which are already familiar (see Lemmas 6.5 and 7.2):

$$\Upsilon \,:\, A \mapsto \Psi_A \mapsto p^2(\Psi_A)^{-1} = \Psi_{p^2A^{-1}} \mapsto \mathcal{I}_{p^2A^{-1}} \mapsto p(\mathcal{I}_{p^2A^{-1}})^{-1} = \Upsilon_A \qquad (7.10)$$

Summing up our knowledge about the above maps, we arrive at the following statement.

Theorem 7.7. *Let $\mathbf{q}$ be an integral nonsingular ternary quadratic form and let $\mathbf{n}$ be the integral quadratic form determined (up to integral equivalence) by the norm on the even subalgebra of the Clifford algebra $C(\mathbf{q})$. Take $\{\mathbf{q}_1, \ldots, \mathbf{q}_h\}$ and $\{\mathbf{n}_1, \ldots, \mathbf{n}_H\}$ to be complete systems of representatives of different equivalence classes of the similarity classes of $\mathbf{q}$ and of $\mathbf{n}$ respectively. Let p be a prime number coprime to $\det \mathbf{q}$. Then the map of classes of automorphs $A \mapsto \Upsilon_A$ defined via (7.10), (6.28) and Theorem 7.5:*

$$\Upsilon \,:\, \bigcup_{i=1}^{h} E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q}) \hookrightarrow \bigcup_{j=1}^{H} E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n})$$

is an injection, such that for any class of automorphs $A \in \cup_i E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q})$, its image Υ_A divides from the right the lift Ψ_A.

Proof. Indeed, the map $\Psi : E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q}) \to E(\mathbf{n}_i)\backslash R^*(\mathbf{n}_i, p^2\mathbf{n})$ is an injection by (6.30) and Lemmas 6.3 , 6.5. The second element of our chain is the bijection $\mathcal{M} \mapsto p^2\mathcal{M}^{-1}$ of classes of primitive automorphs $E(\mathbf{n}_i)\backslash R^*(\mathbf{n}_i, p^2\mathbf{n}) \to R^*(\mathbf{n}, p^2\mathbf{n}_i)/E(\mathbf{n}_i)$ restricted to the image of Ψ. The identity $p^2(\Psi_A)^{-1} = \Psi_{p^2A^{-1}}$ was established in Remark 6.7. The map $\Psi_{p^2A^{-1}} \mapsto \mathcal{I}_{p^2A^{-1}}$, $R^*(\mathbf{n}, p^2\mathbf{n}_i)/E(\mathbf{n}_i) \to R(\mathbf{n}, p\mathbf{n}_j)/E(\mathbf{n}_j)$ for some j is defined via extension of ideals of the corresponding Clifford algebras in Lemmas 7.1 and 7.2. It provides us with $\mathcal{I}_{p^2A^{-1}} \in \Lambda^4\mathcal{D}_p\Lambda^4/\Lambda^4$ such that $\mathcal{I}_{p^2A^{-1}}$ divides $\Psi_{p^2A^{-1}}$ from the left and, therefore, is an injection by Theorem 7.5

and Remark 7.6. The last step in the chain (7.10) is the bijection $\mathcal{M} \mapsto p\mathcal{M}^{-1}$, $R(\mathbf{n}, p\mathbf{n}_j)/E(\mathbf{n}_j) \to E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n})$. As a composition of injections, Υ is certainly an injection itself. Moreover, since $\mathcal{I}_{p^2 A^{-1}}$ divides $p^2(\Psi_A)^{-1}$ from the left, then $\Upsilon_A = p(\mathcal{I}_{p^2 A^{-1}})^{-1}$ divides Ψ_A from the right. □

From the above theorem it easily follows that we can view the set of classes of quaternary automorphs of $\mathbf{n}$ as a 2-fold covering of the set of classes of ternary automorphs of $\mathbf{q}$:

Corollary 7.8. *With the notation and under the assumptions of Theorem 7.7,*

$$\bigcup_{j=1}^{H} E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n}) = \bigcup_{A \in \cup_{i=1}^{h} E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q})} \{ \mathcal{M} \in \cup_j E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n}) \ ; \ \Psi_A \mathcal{M}^{-1} \in \mathbb{Z}_4^4 \} \ , \tag{7.11}$$

where for a fixed A the set $\{\mathcal{M} \in \cup_j E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n}) \ ; \ \Psi_A \mathcal{M}^{-1} \in \mathbb{Z}_4^4\}$ consists of exactly 2 classes, and the union over A is disjoint.

Proof. By Remark 7.6, for each $\mathcal{M} \in \cup_j E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n})$ there exists a unique $A \in \cup_i E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q})$ such that $(p\mathcal{M})^{-1}$ divides $\Psi_{p^2 A^{-1}}$ from the left, which immediately implies that $\mathcal{M}$ divides $\Psi_A = p^2(\Psi_{p^2 A^{-1}})^{-1}$ from the right. This establishes our claim (7.11) and shows that the cardinality of the union over A on the right hand side of (7.11) is equal to $(1 + \chi_{\mathbf{n}}(p)) \cdot (p + 1)$, see formulas (7.3),(7.4) and (7.5). On the other hand, because of (7.6) and (7.7) we see that this cardinality can be attained only if the union over A in (7.11) is disjoint (recall that in the proof of Theorem 7.5 we already established that $\mathrm{rank}_{\mathbb{F}_p} \Psi_A = 1$ and so the number of elements in the set $\{\mathcal{M} \in \cup_j E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n}) \ ; \ \Psi_A \mathcal{M}^{-1} \in \mathbb{Z}_4^4\}$ is equal to $1 + \chi_{\mathbf{n}}(p) = 2$ by (7.4)). □

In other words, Corollary 7.8 states that each class in $\cup_j E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n})$ is a right divisor of a unique class in $\Psi\left(\cup_i E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q})\right)$. And conversely, each class in the image $\Psi\left(\cup_i E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q})\right)$ is divisible from the right by exactly $(1 + \chi_{\mathbf{n}}(p)) = 2$ classes of automorphs in $\cup_j E(\mathbf{n}_j)\backslash R(\mathbf{n}_j, p\mathbf{n})$.

Chapter 8
Concluding remarks

Automorph class lift and its factorizations studied in preceding sections shed a new light on the relationships between representations of integers by ternary and quaternary quadratic forms. In the particular case of positive definite ternary forms, from the construction we can deduce certain relations involving the corresponding theta-series similar to Shimura's lift as defined by P.Ponomarev in [10]. Still the theory is far from being complete, and I would like to discuss some open questions.

First of all it is necessary to address the issue of singular primes, i.e. those p that divide the determinant $\det \mathbf{q}$. As we already noted in Corollary 7.4, the isotropic sums of types (7.3) and (7.6) have not been computed in the case of such primes. This prevents us from stating a stronger versions of Theorem 7.3 and Corollary 7.4 which would satisfactorily resolve the question of whether or not Shimura's lift of $\Theta_{\{\mathbf{q}\}}(z)$ is always equal to a normalized $\Theta_{\{\mathbf{n}\}}(z)$. Exact formulas for singular isotropic sums would also have other important applications, such as a complete Euler product decomposition of general Eichler and Epstein zeta-functions as well as investigation of their analytical properties (see [2]).

Another unclear issue concerning singular primes is proper construction of the automorph class lift (6.28) $\Psi : \cup_i E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q}) \hookrightarrow \cup_j E(\mathbf{n}_j)\backslash R^*(\mathbf{n}_j, p^2\mathbf{n})$ for such p and its further factorization into a product of quaternary automorphs with prime multipliers (similar to Lemmas 7.1 and 7.2). All our proofs use the primality of p to $\det \mathbf{q}$ and it would be very interesting to see to what extent the same construction works in the singular case and what modifications (if any) should be made.

The next interesting possibility is related to investigation of effects of the automorph class lift on individual quadratic forms. (In the case of positive definite quadratic forms, this could lead to correspondences between certain spaces of modular forms spanned by theta-series of different weights and invariant under Hecke operators.) For this, we need to explicitly describe factorizations of an individual image $\Psi\left(E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q})\right)$ into products of quaternary automorphs with multiplier p. (Recall that we provided such a description only in the case of the entire image $\Psi\left(\cup_i E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q})\right)$ which corresponds to Shimura's lift of the generic theta-series $\Theta_{\{\mathbf{q}\}}(z)$). Inspired by results of P.Ponomarev [10], here is a sketch of what one might expect.

The subspace of modular forms of half-integral weight 3/2 spanned by h theta-series of ternary quadratic forms (5.2) is invariant under the Hecke operators $|_{\frac{3}{2}} T(p^2)$ and its eigenmatrix with respect to $\Theta(z, \mathbf{q}_i)/e(\mathbf{q}_i)$, $1 \leq i \leq h$ is the matrix $\mathbf{t}^*_{\mathbf{q}}(p^2)$ given by (3.6). Let $F_i(z)$ denote Shimura's lift $\Theta^{(a)}(z, \mathbf{q}_i)$ for some fixed a and let $F_{\mathbf{q}}(z) = {}^t(\ldots, F_i(z), \ldots)$ be the associated vector-valued modular form of integral weight 2. Then we expect the space spanned by $F_i(z)$, $1 \leq i \leq h$ to be invariant under Hecke operators $|_2 T(p)$, and its eigenmatrix with respect to F_i's to be given again by $\mathbf{t}^*_{\mathbf{q}}(p^2)$. Furthermore, let $\Theta_{\mathbf{n}}(z) = {}^t\left(\ldots, \Theta(z, \mathbf{n}_j)/e(\mathbf{n}_j), \ldots\right)$ be the the vector-valued theta-series of weight 2 associated with a complete system $\{\mathbf{n}_1, \ldots, \mathbf{n}_H\}$ of quaternary quadratic forms representing different equivalent classes of the similarity class of quadratic form determined by the norm on the even subalgebra of Clifford algebra $C(\mathbb{Z}^3, \mathbf{q}_i)$ for some i. (We note again that we can take $\mathbf{n}_i$ to be the norm on $C_0(\mathbb{Z}^3, \mathbf{q}_i)$, $1 \leq i \leq h$ and so $h \leq H$, see Lemmas 6.4 and 6.5). We expect the space spanned by Shimura's lifts of $\Theta(z, \mathbf{q}_i)$, $1 \leq i \leq h$ to be a subspace of the space spanned by the normalized theta-series $\Theta(z, \mathbf{n}_j)/e(\mathbf{n}_j)$, $1 \leq j \leq H$, which is invariant under Hecke operators $|_2 T(p)$. In other words, we hope that there exists a matrix $X \in \mathbb{Q}^h_H$ (of arithmetical nature) such that $F_{\mathbf{q}}(z) = X \cdot \Theta_{\mathbf{n}}(z)$. This would imply that

$$\mathbf{t}^*_{\mathbf{q}}(p^2) \cdot X\Theta_{\mathbf{n}}(z) = F_{\mathbf{q}}(z) \,|_2\, T(p) = X\Theta_{\mathbf{n}}(z) \,|_2\, T(p) = (1 + \chi_{\mathbf{n}}(p))^{-1} X \,\mathbf{t}^*_{\mathbf{n}}(p) \cdot \Theta_{\mathbf{n}}(z)$$

Building up expectations, we may hope that $\mathbf{t}^*_{\mathbf{q}}(p^2) \cdot X = (1 + \chi_{\mathbf{n}}(p))^{-1} X \cdot \mathbf{t}^*_{\mathbf{n}}(p)$ for some arithmetical matrix $X \in \mathbb{Q}^h_H$, in other words

$$\left(|E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q}_j)|\right)_{h\times h} \cdot X = (1+\chi_{\mathbf{n}}(p))^{-1} X \cdot \left(|E(\mathbf{n}_k)\backslash R^*(\mathbf{n}_k, p\mathbf{n}_l)|\right)_{H\times H} \quad (8.1)$$

The existence of such an X is not totally impossible: using Theorem 7.3, we may take, for instance, $h=1$ and $X=(\sum_j r(\mathbf{n}_j,1)/e(\mathbf{n}_j))^{-1}\cdot(1,\ldots,1)$, the particular scalar multiple is chosen in order to make the first Fourier coefficient of $X\cdot\Theta_{\mathbf{n}}(z)$ equal to 1. Another, rather trivial example of matrix X with property (8.1) is

$$X=\begin{pmatrix} e^{-1}(\mathbf{q}_1) & \ldots & e^{-1}(\mathbf{q}_1)\\ \vdots & & \vdots\\ e^{-1}(\mathbf{q}_h) & \ldots & e^{-1}(\mathbf{q}_h)\end{pmatrix}_{h\times H},$$

for which we have $\mathfrak{t}^*_{\mathbf{q}}(p^2)\cdot X=(p+1)\cdot X=(1+\chi_{\mathbf{n}}(p))^{-1}X\cdot\mathfrak{t}^*_{\mathbf{n}}(p)$ by Theorem 7.3. Both examples produce the generic theta-series $\Theta_{\{\mathbf{n}\}}(z)$ as a Hecke eigenform of weight 2 whose eigenvalue is equal to $\mathfrak{t}^*_{\mathbf{q}}(p^2)$. It would be extremely interesting to find nontrivial (of rank >1) examples of matrices with property (8.1), which could lead to construction of other subspaces invariant under Hecke operators in the space spanned by the theta-series $\Theta(z,\mathbf{n}_j)$, $1\le j\le H$ with eigenmatrix $\mathfrak{t}^*_{\mathbf{q}}(p^2)$. Furthermore, and perhaps more interesting, identity of type (8.1) would provide a direct link between various zeta-functions associated to ternary and quaternary quadratic forms, which could lead to insights concerning their analytic properties (such as meromorphic continuation and functional equations). We illustrate this with a simple example.

If we start with $\mathbf{q}(x)=x_1^2+x_2^2+x_3^2$ (the sum of 3 squares), then the corresponding quaternary form (6.12) on $C_0(E,\mathbf{q})$ is the the sum of 4 squares $\mathbf{n}(y)=y_1^2+y_2^2+y_3^2+y_4^2$. Both forms are positive definite and both have class number equal to 1 (i.e. $h=1$ and $H=1$), so their theta-series $\Theta(z,\mathbf{q})=e(\mathbf{q})\cdot\Theta_{\{\mathbf{q}\}}(z)$ and $\Theta(z,\mathbf{n})=e(\mathbf{n})\cdot\Theta_{\{\mathbf{n}\}}(z)$ are eigenforms of the Hecke operators $|_{\frac{3}{2}}T(p^2)$ or $|_2 T(p)$ with respective eigenvalues $\mathfrak{t}^*_3(p^2)=r^*(\mathbf{q},p^2\mathbf{q})/e(\mathbf{q})$ or $\mathfrak{t}^*_4(p)=r(\mathbf{n},p\mathbf{n})/e(\mathbf{n})$, see (3.6). The only singular prime dividing the determinants in our example is $p=2$. By Corollary 7.4, the odd-numbered Fourier coefficients of Shimura's lift of $\Theta(z,\mathbf{q})$ coincide with those of the series $\frac{1}{8}\Theta(z,\mathbf{n})$, which we normalize with r($\mathbf{n}$,1)=8. Note that, by Theorem 7.3, identity (8.1) is actually true in this situation with $X=1$: $\mathfrak{t}^*_3(p^2)=\frac{1}{2}\mathfrak{t}^*_4(p)$ for $p\neq 2$. Next we set

$$\mathfrak{r}_k(m)=\left|R\left(\sum_{i=1}^{k}x_i^2\,,\ m\right)\right|\Big/\left|E\left(\sum_{i=1}^{k}x_i^2\right)\right|,$$

then, using (3.8) and (3.9) we obtain the following chain of identities for any square-free positive integer a and any positive integer b:

$$\begin{aligned}
\sum_{m\,-\mathrm{odd}} \frac{\mathfrak{r}_4(mb)}{m^s} \;&=\; \prod_{p\,-\mathrm{odd}} \Big(1 - \tfrac{1}{2}\mathfrak{t}_4^*(p)p^{-s} + p^{1-2s}\Big)^{-1} \cdot \mathfrak{r}_4(b) \;= \\
&\prod_{p\,-\mathrm{odd}} \Big(1 - \mathfrak{t}_3^*(p^2)p^{-s} + p^{1-2s}\Big)^{-1} \cdot \mathfrak{r}_4(b) \;= \\
\sum_{m\,-\mathrm{odd}} \frac{\chi_{\mathbf{q}}(m)(\frac{2a}{m})}{m^s} \cdot &\prod_{p\,-\mathrm{odd}} \left(1 - \chi_{\mathbf{q}}(p)\Big(\frac{2a}{p}\Big)p^{-s}\right) \cdot \\
&\prod_{p\,-\mathrm{odd}} \Big(1 - \mathfrak{t}_3^*(p^2)p^{-s} + p^{1-2s}\Big)^{-1} \cdot \mathfrak{r}_4(b) \;= \\
&L\left(s\,, (\frac{-a}{\cdot})\right) \cdot \sum_{m\,-\mathrm{odd}} \frac{\mathfrak{r}_3(m^2a)}{m^s} \cdot \frac{\mathfrak{r}_4(b)}{\mathfrak{r}_3(a)}\;.
\end{aligned}$$

Taking $b = 1$ and setting $L\left(s, (\frac{-a}{\cdot})\right) = L_a(s)$, where $(\frac{-a}{\cdot})$ is the Legendre symbol, we conclude that

$$\sum_{m\,-\mathrm{odd}} \frac{\mathfrak{r}_3(m^2a)}{m^s} \;=\; L_a^{-1}(s) \cdot \sum_{m\,-\mathrm{odd}} \frac{\mathfrak{r}_4(m)}{m^s} \cdot \mathfrak{r}_3(a)\;. \tag{8.2}$$

The particular zeta-function on the left-hand side of (8.2) has Euler product (3.9) and is associated to the theta-series $\Theta(z,\, x_1^2+x_2^2+x_3^2)$ of half-integral weight. Now we can also deduce analytic properties (meromorphic continuation and functional equation) of this zeta-function from known properties of the Epstein zeta-function and of the L-series on the right-hand side of (8.2).

Finally, we can try to interpret (and generalize) of identity (8.1) in terms of the automorph class theory which would provide a direct link between $\mathfrak{T}_{\mathbf{q}}^*(p^2)$ and $\mathfrak{T}_{\mathbf{n}}^*(p)$, see (4.1), i.e., between individual classes of ternary automorphs $E(\mathbf{q}_i)\backslash R^*(\mathbf{q}_i, p^2\mathbf{q}_j)$ and quaternary automorphs $E(\mathbf{n}_k)\backslash R^*(\mathbf{n}_k, p\mathbf{n}_l)$ with fixed i, j, k, l, for an arbitrary integral nonsingular ternary quadratic form $\mathbf{q}$. Automatically, this would also furnish a natural proof for the above conjectures on relations between numbers of representations and, as a consequence, between corresponding Eichler or Epstein zeta-functions. Such an interpretation seems to require a better understanding of the arithmetic of even Clifford subalgebras $C_0(E, \mathbf{q})$ in order to characterize explicitly factorizations of individual lifts $\Psi_A \subset E(\mathbf{n}_i)\backslash R^*(\mathbf{n}_i, p^2\mathbf{n}_j)$ in terms of automorph classes in $E(\mathbf{n}_k)\backslash R^*(\mathbf{n}_k, p\mathbf{n}_l)$ for specific k and l. To this day attempts to find such an interpretation have been unsuccessful.

Finally, we mention the most intriguing mystery concerning Shimura's lift for theta-series – the question of theta-series of quadratic forms in more than 3 variables. The apparatus of Clifford algebras extensively used in the present paper seems to be of no use in that situation since on one hand dimensions of corresponding algebras do not match the expected weights of the lifting and on the other hand the standard norm on an even Clifford subalgebra of dimension greater than 4 does not define a quadratic form in general. To the author's knowledge there is no result describing effects of Shimura's lift on such theta-series. The mountain is still in clouds!

References

[1] A. Andrianov. *Automorphic factorizations of solutions of quadratic congruences and their applications.* St.Petersburg Math. J. **5** (1994), no. 5, 1–38.

[2] — . *Quadratic congruences and rationality of local zeta-series of ternary and quaternary quadratic forms.* St.Petersburg Math. J. **6** (1995), no 2, 199–240.

[3] — . *Quadratic Forms and Hecke Operators.* Grundlehren Math. Wiss. **286**, Springer-Verlag, Berlin–New York, 1987.

[4] F. Andrianov. *Multiplicative decompositions of integral representations by quadratic forms.* Zap. Nauchn. Sem. St.Petersburg. Otdel. Mat. Inst. Steklov (POMI) **212** (1994), 12–55.

[5] — . *Euler expansions of formal zeta-series of quadratic forms in an odd number of variables.* St.Petersburg Math. J. **7** (1996), no. 1, 1–16.

[6] M. Eichler. *Quadratishe Formen und orthogonale Gruppen.* Grundlehren Math. Wiss. **63**, Springer-Verlag, Berlin–New York, 1974.

[7] E. Freitag. *Siegelsche Modulfunktionen.* Grundlehren Math. Wiss. **254**, Springer-Verlag, Berlin–New York, 1983.

[8] H. Hida. *Elementary theory of L-functions and Eisenstein series.* London Math. Soc. Student Texts **26**, Cambridge University Press, Cambridge, 1993.

[9] M. Kneser. *Quadratishe Formen, Vorlesung.* Mathematisches Institut der Universität Götingen, Götingen, 1992.

[10] P. Ponomarev. *Ternary Quadratic Forms and Shimura's correspondence.* Nagoya Math. J. **81** (1981), 123–151.

[11] G. Shimura. *Introduction to the Arithmetical Theory of Automorphic Functions.* Iwanami Publishers and Princeton University Press, Tokyo–Princeton, N.J., 1971.

[12] — . *On modular forms of half integral weight.* Ann. of Math. **97** (1973), 440–481.