Arithmetic Relations Between Fourier Coefficients of Siegel Paramodular Forms

A Dissertation

Presented in Partial Fullfillment of the Requirements for the

Degree of Doctor of Philosophy

with a

Major in Mathematics

in the

College of Graduate Studies

University of Idaho

by

Daniel A. Reiss

Major Professor: Jennifer Johnson-Leung, Ph.D.

Committee Members: Brooks Roberts, Ph.D., Hirotachi Abo, Ph.D.,

Ruprecht Machleidt, Ph.D.

Department Chair: Christopher Williams, Ph.D.

August 2019

Authorization to Submit Dissertation

This dissertation of Daniel A. Reiss, submitted for the degree Doctor of Philosophy with a Major in Mathematics and titled "Arithmetic Relations Between Fourier Coefficients of Siegel Paramodular Forms," has been reviewed in final form. Permission, as indicated by the signatures and dates below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor: ______________________ Date: ________
Jennifer Johnson-Leung, Ph.D.

Committee Members: ______________________ Date: ________
Brooks Roberts, Ph.D.

______________________ Date: ________
Hirotachi Abo, Ph.D.

______________________ Date: ________
Ruprecht Machleidt, Ph.D.

Department Chair: ______________________ Date: ________
Christopher Williams, Ph.D.

Abstract

This dissertation presents fundamental relations satisfied by the Fourier coefficients of a Siegel paramodular form $F : \mathcal{H}_2 \to \mathbb{C}$ which is an eigenform for the paramodular Hecke operators at primes which do not divide the level of the Siegel paramodular form. We exhibit relations between coefficients indexed by positive-definite, primitive, integral binary quadratic forms of discriminant δf^2 where $\delta < 0$ is a fundamental discriminant and f is a positive integer.

Acknowledgments

I would first like to thank my advisor Jennifer Johnson-Leung for her guidance and support throughout this entire project. I would also like to thank Brooks Roberts for the many hours he spent going over this work with me. Without his feedback, this work would not have been possible. I would also like to thank Hirotachi Abo and Ruprecht Machleidt for their valuable feedback and for the time they put in to serve on my committee.

I would like to thank the faculty and staff of the mathematics department at the University of Idaho, especially Jana Joyce and Melissa Gottschalk, for everything that they have taught me and provided for me. My experiences here will never be forgotten.

On a more personal note, I would like to thank those who made my years spent in Moscow some of the best years of my life. In particular, I would like to thank John Pawlina, Jordan Hardy, Josh Parker, Dillon Tiedeman-Mueller, Savannah Tiedeman-Mueller, Tanya Tjoelker, Chelsea Embree, Kara Hutchison, Jedediah McProud, Michael Noel, Alex Woychek, Andrew Raub, Daniel Ferguson, and, of course, my beautiful wife Annelise Nielsen.

Dedication

For Annelise, with gratitude and love.

Table of Contents

1 Introduction

"Modular forms are functions on the complex plane that are inordinately symmetric. They satisfy so many internal symmetries that their mere existence seem like accidents. But they do exist"

-Barry Mazur, Nova's "The Proof", PBS

1.1 Background and Motivation

Elliptic modular forms are complex-valued holomorphic functions on the complex upper half-plane

$$\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\},$$

that are invariant under the action of $\mathrm{SL}(2, \mathbb{Z})$ and satisfy certain growth conditions [12] which, together with the identity

$$f(z) = f(z + 1),$$

ensure that they admit a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a(n)e^{2\pi i n z}.$$

To each elliptic modular form we associate a positive integer called the weight, and we denote the vector space of weight k elliptic modular forms by $\mathcal{M}_k(\mathrm{SL}(2, \mathbb{Z}))$. The term modular form is attributed to Hecke [14].

The theory of Hecke operators on the vector space of weight k elliptic modular forms establishes that Fourier coefficients of eigenforms enjoy arithmetic relations. For example, the Fourier coefficients of the discriminant function, often called the Ramanujan delta function,

$$\begin{aligned}\Delta(z) &= e^{2\pi i z} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z})^{24} \\ &= \sum_{n=1}^{\infty} \tau(n)e^{2\pi i n z}\end{aligned}$$

satisfy multiple arithmetic relations including the multiplicative relation

$$\tau(mn) = \tau(m)\tau(n)$$

for m and n relatively prime. This relation was conjectured by Ramanujan and proved by Mordell [28]. Furthermore, the Dirichlet series formed by the Fourier coefficients,

$$L(s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s},$$

expands as an Euler product over all primes p [8],

$$\sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \prod_p (1 - \tau(p)p^{-s} + p^{11}p^{-2s})^{-1}.$$

For a more thorough exposition on the theory of elliptic modular forms the reader should see [12], [21], and [38].

1.2 Siegel Modular Forms

Siegel modular forms of genus 2 are complex-valued holomorphic functions defined on the Siegel upper half-space

$$\mathcal{H}_2 = \{Z \in M(4, \mathbb{C}) : {}^tZ = Z \text{ and } \mathrm{Im}(Z) > 0\}$$

that are invariant under the action of $\mathrm{Sp}(4, \mathbb{Z})$. We note here that the Koecher principle [2, 5] implies that a Siegel modular form $F : \mathcal{H}_2 \to \mathbb{C}$ has a Fourier expansion

$$F(Z) = \sum_{S \in A(1)} a(S) e^{2\pi i \mathrm{tr}(SZ)},$$

without any assumed boundary conditions. Here, for $M \geq 1$ an integer,

$$A(M) = \left\{ \begin{bmatrix} Mr & t/2 \\ t/2 & s \end{bmatrix} \in M(4, \mathbb{Q}) : r, t, s \in \mathbb{Z} \text{ and } Mrs - \frac{t^2}{4} \geq 0 \right\}.$$

The work of Andrianov [1, 2, 3, 4] extended the theory of Hecke operators to Siegel modular forms. As Siegel modular forms are more complicated than elliptic modular forms, it is natural to expect that the Fourier coefficients exhibit more complex relations. Andrianov established the existence of an Euler product attached to Siegel modular eigenforms. We state the result pertaining to indices of fundamental discriminant [1] here.

Theorem 1.2.1 (Andrianov, 1971)**.** *Let*

$$F(Z) = \sum_{S \in A(1)} a(S) e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(\mathrm{Sp}(4, \mathbb{Z}))$$

with $k > 0$*. Suppose that* F *is an eigenform of the Hecke operators* $\{T(m)\}_{m \geq 1}$ *with eigenvalues* $\{\mu(m)\}_{m \geq 1}$*. Let* $\delta < 0$ *be a fundamental discriminant and let* $K = \mathbb{Q}(\sqrt{\delta})$*. Let* $S_1, \ldots, S_h$ *be a complete set of representatives from the classes of equivalent binary quadratic forms of discriminant* δ *which are positive-definite, integral, and primitive. For* $m \geq 1$*, set*

$$a(m) = \sum_{i=1}^{h} a(mS_i).$$

Then in some right half-plane

$$L_K(s-k+2)\sum_{m=1}^{\infty}\frac{a(m)}{m^s}=a(1)\prod_p L_p(p^{-s})^{-1}$$

where L_K *is the L-series of the field* K *and*

$$L_p(p^{-s})=1-\mu(p)p^{-s}+(\mu(p)^2-\mu(p^2)-p^{2k-4})p^{-2s}-\mu(p)p^{2k-3}p^{-3s}+p^{4k-6}p^{-4s}.$$

Theorem 1.2.1 was extended to indices of general discriminant in [3] and later was extended to the principal congruence subgroup of $\mathrm{Sp}(4,\mathbb{Z})$ by Evdokimov [13]. We define for an integer $M\geq 1$

$$A(M,\delta f^2)=\{S\in A(M): S \text{ is primitive of discriminant } \delta f^2\}.$$

Theorem 1.2.2 (Evdokimov, 1976)**.** *Let* $M\geq 1$ *be an integer. Let*

$$F(Z)=\sum_{S\in A(1)}a(S)e^{2\pi i\mathrm{tr}(SZ)/M}\in\mathcal{M}_k(\Gamma(M))$$

with $k>0$*. Suppose that* F *is an eigenform of the Hecke operators* $\{T(m)\}_{m\geq 1,\ \gcd(m,M)=1}$ *with eigenvalues* $\{\mu(m)\}_{m\geq 1,\ \gcd(m,M)=1}$*. Let* $\delta<0$ *be a fundamental discriminant and let* $K=\mathbb{Q}(\sqrt{\delta})$*. Fix an order* $\mathfrak{o}_f$ *of* K *for some* $f\in\mathbb{N}$*. Then for every* $S\in A(1,\delta f^2)$*, we have in some right half-plane*

$$L_{\delta f^2}(s-k+2)\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)}\sum_{\substack{m=1\\ \gcd(m,M)=1}}^{\infty}\frac{a(mS_{\mathfrak{u}})}{m^s}=\chi_{S,F}(s)\prod_{p\nmid M}Q_{p,F}(p^{-s})^{-1}$$

where $Q_{p,F}(t)$ *is the Euler factor at* p*,* $L_{\delta f^2}(s)$ *is the L-series of* $\mathfrak{o}_f$*, the matrix* $S_{\mathfrak{u}}$ *is determined by the action of* $H(\mathfrak{o}_f,M)$*, and* $\chi_{S,F}(s)$ *is a function depending on* S *and* F*.*

Theorems 1.2.1 and 1.2.2 provide an amazing connection between the Fourier coefficients of the Siegel modular eigenform and its eigenvalues. More recently, McCarthy [25] established from Andrianov's formulas that arithmetic relations exist for specific Fourier coefficients. We state this result here.

Theorem 1.2.3 (McCarthy, 2016)**.** *Let*

$$F(Z)=\sum_{S\in A(1)}a(S)e^{2\pi i\mathrm{tr}(SZ)}\in\mathcal{M}_k(\mathrm{Sp}(4,\mathbb{Z}))$$

with $k>0$*. Suppose that* F *is an eigenform. Let* $I_{1,0}$ *denote the* 2×2 *identity matrix.*

(i) If $a(I_{1,0})=0$*, then* $a(mI_{1,0})=0$ *for all* $m\in\mathbb{N}$*.*

(ii) If $m,n\in\mathbb{N}$ *with* $\gcd(m,n)=1$*, then*

$$a(mnI_{1,0})a(I_{1,0})=a(mI_{1,0})a(nI_{1,0}).$$

Theorem 1.2.3 has been generalized to Siegel modular forms with level by Walling [41] utilizing an alternative formula for the action of the Hecke operators on a Siegel modular form [15].

If the reader has more interest in the theory of Siegel modular forms we recommend they see [1] and [40].

1.3 Current Work and Summary of Results

The objects of study in this work are known as Siegel paramodular forms which are Siegel modular forms for the paramodular group $\mathrm{K}(M)$. We will define these objects more carefully in Chapter 2. The study of Siegel paramodular forms has gained a lot of traction recently due to a conjecture of Brumer and Kramer [6] which roughly states that there is a correspondence between the collection of isogeny classes of abelian surfaces over $\mathbb{Q}$ of conductor $M \in \mathbb{Z}$ with trivial endomorphism ring together with isogeny classes of abelian fourfolds over $\mathbb{Q}$ of conductor M^2 and certain weight 2 Siegel paramodular forms on $\mathrm{K}(M)$.

This work in particular presents extensions of Theorem 1.2.2 and Theorem 1.2.3. Our method of proof is similar to that used by Andrianov and Evdokimov, however proofs are built with invariance properties of Fourier coefficients of Siegel paramodular forms in mind.

The main results of Chapter 6 are extensions of Theorems 1.2.2 and 1.2.3. We start with multiplicative relations exhibited in another collection of Fourier coefficients.

Theorem 1.3.1 (R., 2019). *Let*

$$F(Z) = \sum_{S \in A(1)} a(S) e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(\mathrm{Sp}(4,\mathbb{Z}))$$

for $k > 0$. Suppose that F is an eigenform. Let $I_{1,1}$ denote the matrix

$$\begin{bmatrix} 1 & 1/2 \\ 1/2 & 1 \end{bmatrix}.$$

(i) If $a(I_{1,1}) = 0$, then $a(mI_{1,1}) = 0$ for all $m \in \mathbb{N}$.

(ii) For $m, n \in \mathbb{N}$ with $\gcd(m,n) = 1$ we have

$$a(mnI_{1,1})a(I_{1,1}) = a(mI_{1,1})a(nI_{1,1}).$$

In addition, we see that other arithmetic relations hold for any $S \in A(1)$ whose discriminant is a fundamental discriminant.

Theorem 1.3.2 (R., 2019)**.** *Let*

$$F(Z) = \sum_{S \in A(1)} a(S) e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(\mathrm{Sp}(4, \mathbb{Z}))$$

for $k > 0$. Suppose that F is an eigenform. Let $S_1, \ldots, S_h$ be a complete set of representatives of the classes of positive-definite, primitive, integral binary quadratic forms of discriminant δ with δ a fundamental discriminant.

(i) If $a(S_i) = 0$ for each $i \in \{1, \ldots, h\}$, then $a(mS_i) = 0$ for all $m \in \mathbb{N}$ and all $i \in \{1, \ldots, h\}$.

(ii) For $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$ we have

$$\sum_{i=1}^{h} \sum_{j=1}^{h} a(mnS_i) a(S_j) = \sum_{i=1}^{h} \sum_{j=1}^{h} a(mS_i) a(nS_j).$$

To prove these results we rely heavily on the theory of full modules in imaginary quadratic fields. We note here that McCarthy's result and Theorems 1.3.1 and 1.3.2 provide relations between Fourier coefficients seen for paramodular level $M = 1$ associated to binary quadratic forms of fixed discriminant given by a fundamental discriminant. To approach the general case where $M \geq 1$ we start by looking for relations between Fourier coefficients associated to binary quadratic forms whose discriminant corresponds to a class group of size 1. We note the following theorem which is due to Gauss.

Theorem 1.3.3 (Gauss)**.** *Suppose $\delta f^2 \equiv 0, 1 \pmod 4$ with $\delta < 0$ a fundamental discriminant. Then $h(\delta f^2) = 1$ if and only if $\delta f^2 = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67$, or -163.*

The previous theorm provides an analog to Theorems 1.2.3 and 1.3.1 for Siegel paramodular eigenforms of level $M = 2, 3, 4, 5, 7, 11, 17$, and 41 where we see strictly multiplicative relations in a specific collection of Fourier coefficients. More precisely, we have the following theorem.

Theorem 1.3.4 (R., 2019)**.** *Let $M \geq 1$ be an integer. Let*

$$F(Z) = \sum_{S \in A(M)} a(S) e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(K(M))$$

with $k > 0$. Suppose that F is an eigenform. Let $I_{M,0}$ and $I_{M,1}$ denote the matrices

$$\begin{bmatrix} M & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} M & 1/2 \\ 1/2 & 1 \end{bmatrix}$$

respectively. Let $h(D)$ denote the size of the class group of forms of discriminant $D < 0$.

(i) If $h(-4M) = 1$*, then for* $m, n \in \mathbb{N}$ *with* n *odd and* $\gcd(mM, n) = 1$ *we have*

$$a(mnI_{M,0})a(I_{M,0}) = a(mI_{M,0})a(nI_{M,0}).$$

(ii) If $h(-4M + 1) = 1$*, then for* $m, n \in \mathbb{N}$ *with* $n \not\equiv 0 \pmod 3$ *and* $\gcd(mM, n) = 1$ *we have*

$$a(mnI_{M,1})a(I_{M,1}) = a(mI_{M,1})a(nI_{M,1}).$$

We then move to the main results of Chapter 6. The first result characterizes the arithmetic relations seen between Fourier coefficients of Siegel paramodular forms associated to binary quadratic forms of fixed discriminant $D < 0$. This result captures McCarthy's result and much more.

Theorem 1.3.5 (R., 2019)**.** *Let* $M \geq 1$ *be an integer. Let*

$$F(Z) = \sum_{S \in A(M)} a(S)e^{2\pi i \operatorname{tr}(SZ)} \in \mathcal{M}_k(\mathrm{K}(M))$$

with $k > 0$*. Suppose that* F *is an eigenform. Let* $S_1, \ldots, S_d$ *be a complete set of representatives of the set* $\Gamma_0(M) \setminus A(M, \delta f^2)$ *where* $\delta < 0$ *is a fundamental discriminant and* $f \in \mathbb{N}$*.*

(i) If $a(S_i) = 0$ *for each* $i \in \{1, \ldots, d\}$*, then* $a(mS_i) = 0$ *for all* $m \in \mathbb{N}$ *with* $\gcd(m, f) = 1$ *and for all* $i \in \{1, \ldots, d\}$*.*

(ii) For $m, n \in \mathbb{N}$ *with* $\gcd(mM, n) = \gcd(mn, f) = 1$ *we have*

$$\sum_{i=1}^{d}\sum_{j=1}^{d} a(mnS_i)a(S_j) = \sum_{i=1}^{d}\sum_{j=1}^{d} a(mS_i)a(nS_j).$$

The next theorem presents a modest generalization of Theorems 1.2.1 and 1.2.2. In particular, we show that when viewing Theorems 1.2.1 and 1.2.2 in the context of Siegel paramodular forms, the quantities contained in the formula are in general non-zero.

Theorem 1.3.6 (R., 2019)**.** *Let* $M \geq 1$ *be an integer. Let*

$$F(Z) = \sum_{S \in A(M)} a(S)e^{2\pi i \operatorname{tr}(SZ)} \in \mathcal{M}_k(K(M))$$

with $k > 0$*. Suppose that* F *is an eigenform of the Hecke operators* $\{T(m)\}_{m \geq 1,\ \gcd(m,M)=1}$ *with eigenvalues* $\{\mu(m)\}_{m \geq 1,\ \gcd(m,M)=1}$*. Let* $\delta < 0$ *be a fundamental discriminant and let* $K = \mathbb{Q}(\sqrt{\delta})$*. Fix an order* $\mathfrak{o}_f$ *of* K *for some* $f \in \mathbb{N}$*. Then for every* $S \in A(M, \delta f^2)$*, we have in some right half-plane*

$$L_{\delta f^2}(s - k + 2) \sum_{[\mathfrak{u}] \in H(\mathfrak{o}_f, M)} \sum_{\substack{m=1 \\ \gcd(m,M)=1}}^{\infty} \frac{a(mS_{\mathfrak{u}})}{m^s} = \chi_{S,F}(s) \prod_{p \nmid M} Q_{p,F}(p^{-s})^{-1}$$

where $Q_{p,F}(t)$ *is the Euler factor at* p*,* $L_{\delta f^2}(s)$ *is the L-series of* $\mathfrak{o}_f$*, the matrix* $S_{\mathfrak{u}}$ *is determined by the action of* $H(\mathfrak{o}_f, M)$*, and* $\chi_S(s)$ *is a function depending on* S *and* F*.*

Chapters 2-5 build up the necessary machinery required to prove our main results in Chapter 6. In Chapter 2, we address the abstract Hecke theory that is prominent throughout this work. In Chapter 3, we present the definitions of the paramodular group and Siegel paramodular forms and present some basic structural theory on the matrix groups $\mathrm{GSp}(4,\mathbb{R})$ and $\mathrm{Sp}(4,\mathbb{Z})$ that will be utilized in later computations. In particular, we prove a theorem on the Smith normal form for matrices in $M(2,\mathbb{Z})$. In Chapter 4, we give a construction of the paramodular Hecke operators for $p \nmid M$ following the construction of Andrianov [1] and for $p|M$ with M squarefree following the work of Johnson-Leung and Roberts [20] and the work of Roberts and Schmidt [34]. In Chapter 5, we build the theory of full modules in imaginary quadratic fields following works such as [7] which we will exploit in the proofs of the main results in Chapter 6. It is a topic of further research to understand the action of the paramodular Hecke operators for $p|M$ on the Fourier coefficients of a Siegel paramodular form of squarefree level M.

1.4 Related Results

When discussing Siegel paramodular forms which are eigenforms of the paramodular Hecke operators we are often interested in determining how the eigenvalues relate to the Fourier coefficients of the form. McCarthy proves the following theorem [25].

Theorem 1.4.1. *Let*

$$F(Z) = \sum_{S \in A(1)} a(S) e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(\mathrm{Sp}(4,\mathbb{Z}))$$

with $k > 0$. Suppose that F is an eigenform normalized such that $a(I_{1,0}) = 1$. Let

$$\left(\frac{n}{p}\right)$$

denote the Legendre symbol where p is an odd prime. Set

$$h_1(p) = \begin{cases} 2 & \text{if } (\frac{-4}{p}) = 1, \\ 1 & \text{if } p = 2, \\ 0 & \text{if } (\frac{-4}{p}) = -1, \end{cases}$$

and

$$h_2(p) = \begin{cases} 2 & \text{if } (\frac{-4}{p}) = 1, \\ 0 & \text{if } p = 2 \textit{ or } (\frac{-4}{p}) = -1. \end{cases}$$

Then for any prime p, the eigenvalues of index p and p^2 associated to F satisfy

$$\mu(p) = a(pI_{1,0}) + h_1(p)p^{k-2}$$

and

$$\mu(p^2) = a(p^2 I_{1,0}) + h_1(p)p^{k-2}a(pI_{1,0}) + h_2(p)p^{2k-4}.$$

Determining such a relation between Fourier coefficients of Siegel paramodular eigenforms and its eigenvalues is still an open problem and is a topic of future research.

2 Abstract Hecke Rings

The structure of this chapter loosely follows [27]. For this chapter we let G be a topological group and X a topological space.

2.1 Function Space

Suppose that G acts on X on the left. We will denote this action by $g \cdot z$ for $g \in G$ and $z \in X$. Let $H(X)$ denote the set of all holomorphic functions from X to $\mathbb{C}$, and let Γ be a subgroup of G. Let $\{C_g\}_{g \in G}$ be a collection of constants such that $C_{g_1 g_2} = C_{g_1} C_{g_2}$ for $g_1, g_2 \in G$ and $C_g = 1$ for all $g \in \Gamma$.

Definition 2.1.1. *Let $j : G \times X \to \mathbb{C}$ be a non-zero holomophic function. We say j is a* ***factor of automorphy*** *if for all $g_1, g_2 \in G$ and for all $z \in X$,*

$$j(g_1 g_2, z) = j(g_1, g_2 \cdot z) j(g_2, z).$$

This relation is known as the ***cocycle relation****.*

Let j be a factor of automorphy. Note that the cocycle relation implies that $j(1_G, z) = 1$ for all $z \in X$ where 1_G denotes the identity in G. The left action of G on X induces a right action of G on $H(X)$. Let k be a nonnegative integer. For $g \in G$, define $f \star_k g : X \to \mathbb{C}$ to be

$$(f \star_k g)(z) = C_g^k j(g, z)^{-k} f(g \cdot z).$$

We call k the weight. We will show that this defines a right action. Let $f \in H(X)$. Then

$$\begin{aligned}(f \star_k 1_G)(z) &= C_{1_G}^k j(1_G, z)^{-k} f(1_G \cdot z) \\ &= f(z).\end{aligned}$$

and for $g_1, g_2 \in G$

$$\begin{aligned}(f \star_k g_1 g_2)(z) &= C_{g_1 g_2}^k j(g_1 g_2, z)^{-k} f(g_1 g_2 \cdot z) \\ &= C_{g_1}^k C_{g_2}^k j(g_1, g_2 \cdot z)^{-k} j(g_2, z)^{-k} f(g_1 \cdot (g_2 \cdot z)) \\ &= C_{g_2}^k j(g_2, z)(f \star_k g_1)(g_2 \cdot z) \\ &= ((f \star_k g_1) \star_k g_2)(z).\end{aligned}$$

Hence G acts via $\star_k$ on $H(X)$.

Definition 2.1.2. *Let $f \in H(X)$. We say f is an* ***automorphic form*** *for Γ if for some integer $k \geq 0$,*

$$(f \star_k g)(z) = f(z)$$

for all $g \in \Gamma$ and for all $z \in X$. If we want to emphasize the integer k then we call f a ***weight*** *k* ***automorphic form*** *for Γ.*

For fixed $k \in \mathbb{Z}_{\geq 0}$ we denote by $\mathcal{M}_k(\Gamma)$ the set of all weight k automorphic forms for Γ. It is clear that $\mathcal{M}_k(\Gamma)$ is a vector space over $\mathbb{C}$. We emphasize a few important properties of $\mathcal{M}_k(\Gamma)$.

1. If Γ' and Γ'' are subgroups of Γ such that $\Gamma' \subseteq \Gamma''$ then $\mathcal{M}_k(\Gamma'') \subseteq \mathcal{M}_k(\Gamma')$.

2. If $f \in \mathcal{M}_k(\Gamma)$ and $g \in G$ then $f \star_k g \in \mathcal{M}_k(g^{-1}\Gamma g)$.

3. If $f \in \mathcal{M}_k(\Gamma)$ and $f' \in \mathcal{M}_1(\Gamma)$ then $ff' \in \mathcal{M}_{k+1}(\Gamma)$.

Define $\mathcal{M}(\Gamma)$ to be the module generated by all of the $\mathcal{M}_k(\Gamma)$. That is

$$\mathcal{M}(\Gamma) = \sum_{k=0}^{\infty} \mathcal{M}_k(\Gamma).$$

We will assume that this has the structure of a graded ring,

$$\mathcal{M}(\Gamma) = \bigoplus_{k=0}^{\infty} \mathcal{M}_k(\Gamma).$$

2.2 Hecke Rings

Here we will describe briefly the necessary information on Hecke rings that we will need for the material ahead.

Definition 2.2.1. *Let Γ and Γ' be subgroups of G. We say that Γ and Γ' are* ***commensurable*** *if the indices $[\Gamma : \Gamma \cap \Gamma']$ and $[\Gamma' : \Gamma \cap \Gamma']$ are both finite.*

If Γ and Γ' are commensurable subgroups of G, we shall write $\Gamma \sim \Gamma'$. For a fixed subgroup, Γ, of G we let

$$\mathrm{Com}_G(\Gamma) = \{g \in G : g^{-1}\Gamma g \sim \Gamma\}.$$

We prove some properties of the relation $\sim$ and the set $\mathrm{Com}_G(\Gamma)$.

Proposition 2.2.2. *The relation $\sim$ is an equivalence relation.*

Proof. The reflexivity and symmetry of $\sim$ is obvious. We prove transitivity. Let Γ, Γ', and Γ'' be subgroups of G such that $\Gamma \sim \Gamma'$ and $\Gamma' \sim \Gamma''$. Then

$$\begin{aligned}[\Gamma : \Gamma \cap \Gamma' \cap \Gamma''] &= [\Gamma : \Gamma \cap \Gamma'][\Gamma \cap \Gamma' : \Gamma \cap \Gamma' \cap \Gamma''] \\ &\leq [\Gamma : \Gamma \cap \Gamma'][\Gamma' : \Gamma' \cap \Gamma''] \\ &< \infty.\end{aligned}$$

Similarly, $[\Gamma'' : \Gamma \cap \Gamma' \cap \Gamma''] < \infty$. Since $\Gamma \cap \Gamma' \cap \Gamma'' \subseteq \Gamma \cap \Gamma''$ it follows that $[\Gamma : \Gamma \cap \Gamma''] < \infty$ and $[\Gamma'' : \Gamma \cap \Gamma''] < \infty$. Hence $\Gamma \sim \Gamma''$ and transitivity is proved. □

Proposition 2.2.3. *Let Γ and Γ' be subgroups of G.*

(i) The set $\mathrm{Com}_G(\Gamma)$ is a subgroup of G.

(ii) If $\Gamma \sim \Gamma'$, then $\mathrm{Com}_G(\Gamma) = \mathrm{Com}_G(\Gamma')$.

(iii) Suppose $\Gamma \sim \Gamma'$. Then for any $g \in \mathrm{Com}_G(\Gamma)$ we have

$$\Gamma g \Gamma' = \bigsqcup_{i=1}^{c} \Gamma g \gamma_i = \bigsqcup_{j=1}^{d} \delta_j g \Gamma'$$

where $\{\gamma_i\}_{i=1}^{c}$ and $\{\delta_j\}_{j=1}^{d}$ are finite sets of representatives of $(\Gamma' \cap g^{-1}\Gamma g) \setminus \Gamma'$ and $\Gamma/(\Gamma \cap g\Gamma' g^{-1})$ respectively.

Proof. We start by proving (i). Let $g_1, g_2 \in \mathrm{Com}_G(\Gamma)$. We need to show that $g_1 g_2 \in \mathrm{Com}_G(\Gamma)$. Consider $\tau : G \to G$ given by $\tau(g) = g_1 g g_1^{-1}$. Then τ is an inner automorphism of G and hence preserves the index of subgroups. Let $\Gamma' = g_1 \Gamma g_1^{-1}$ and $\Gamma'' = g_2 \Gamma g_2^{-1}$. Since $\Gamma' \sim \Gamma''$ we have $[\tau(\Gamma) : \tau(\Gamma \cap \Gamma'')] < \infty$ and $[\tau(\Gamma'') : \tau(\Gamma \cap \Gamma'')] < \infty$. We have $\tau(\Gamma) = \Gamma'$, $\tau(\Gamma'') = g_1 \Gamma'' g_1^{-1}$, and $\tau(\Gamma \cap \Gamma'') = \Gamma' \cap g_1 \Gamma'' g_1^{-1}$. It follows that $\tau(\Gamma'') \sim \Gamma'$. By transitivity, $\tau(\Gamma'') \sim \Gamma$. Thus $g_1 g_2 \in \mathrm{Com}_G(\Gamma)$. Now let $h \in \mathrm{Com}_G(\Gamma)$. Then $\Gamma''' = h^{-1}\Gamma h \sim \Gamma$. We want to show $h\Gamma h^{-1} \sim \Gamma$. Let $\sigma : G \to G$ be the inner automorphism $\sigma(g) = hgh^{-1}$. Since $\Gamma''' \sim \Gamma$ we have $[\sigma(\Gamma) : \sigma(\Gamma \cap \Gamma''')] < \infty$ and $[\sigma(\Gamma''') : \sigma(\Gamma \cap \Gamma''')] < \infty$. It is clear that $\sigma(\Gamma) = h\Gamma h^{-1}$, $\sigma(\Gamma''') = \Gamma$, and $\sigma(\Gamma \cap \Gamma''') = h\Gamma h^{-1} \cap \Gamma$. Hence $h\Gamma h^{-1} \sim \Gamma$ and $h^{-1} \in \mathrm{Com}_G(\Gamma)$. Since 1_G is clearly in $\mathrm{Com}_G(\Gamma)$ this proves (i). We now prove (ii). Suppose that $\Gamma \sim \Gamma'$. Then, since $g^{-1}\Gamma' g \sim g^{-1}\Gamma g \sim \Gamma \sim \Gamma'$, we have that

$$\begin{aligned}\mathrm{Com}_G(\Gamma) &= \{g \in G : g^{-1}\Gamma g \sim \Gamma\} \\ &= \{g \in \Gamma : g^{-1}\Gamma' g \sim \Gamma'\} \\ &= \mathrm{Com}_G(\Gamma').\end{aligned}$$

Lastly, we prove (iii). Suppose again that $\Gamma \sim \Gamma'$. We prove only one decomposition as the other is follows mutatis mutandis. Every right coset in $\Gamma g \Gamma'$ is of the form $\Gamma g \gamma$ for some $\gamma \in \Gamma'$. It is easy to see that if $\Gamma g \gamma = \Gamma g \gamma'$ for $\gamma, \gamma' \in \Gamma'$ then $\gamma(\gamma')^{-1} \in \Gamma' \cap g^{-1}\Gamma g$. Since $g^{-1}\Gamma g$ is commensurable with Γ and hence with Γ' the desired decomposition follows. □

Let Γ be a subgroup of G and let $\mathfrak{s}(\Gamma)$ be a subgroup of G such that $\Gamma \subseteq \mathfrak{s}(\Gamma) \subseteq \mathrm{Com}_G(\Gamma)$. We then call the pair $(\Gamma, \mathfrak{s}(\Gamma))$ a **Hecke pair**. We define the **Hecke algebra**, $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$, as the free $\mathbb{Z}$-module generated by the double cosets $\Gamma g \Gamma$ with $g \in \mathfrak{s}(\Gamma)$,

$$\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma)) = \left\{ \sum_{g \in \mathfrak{s}(\Gamma)} m_g \Gamma g \Gamma : m_g \in \mathbb{Z},\ m_g = 0 \text{ for all but finitely many } g \right\}.$$

Suppose further that $\mathfrak{s}(\Gamma)$ acts on a $\mathbb{Z}$-module N on the right via $(n, g) \mapsto n^g$ and let N^Γ be the submodule consisting of Γ-invariant elements of N.

Proposition 2.2.4. *Let $n \in N^\Gamma$ and let $\Gamma g \Gamma \in \mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$. Suppose we have two disjoint decompositions*

$$\Gamma g \Gamma = \bigsqcup_{i=1}^{c} \Gamma g_i = \bigsqcup_{i=1}^{c} \Gamma g_i'.$$

Then

$$\sum_{i=1}^{c} n^{g_i} = \sum_{i=1}^{c} n^{g_i'}.$$

Furthermore,

$$\sum_{i=1}^{c} n^{g_i} \in N^\Gamma.$$

Proof. Let

$$\Gamma g \Gamma = \bigsqcup_{i} \Gamma g_i = \bigsqcup_{i} \Gamma g_i'$$

be disjoint decompositions of $\Gamma g \Gamma$. If $\Gamma g_i = \Gamma g_i'$ then there exists $\gamma \in \Gamma$ such that $g_i' = \gamma g_i$. Then for $n \in N^\Gamma$,

$$n^{g_i'} = n^{\gamma g_i} = n^{g_i}$$

which proves the first part of the proposition. To prove the second part of the proposition let $\gamma \in \Gamma$ and notice that

$$\Gamma g \Gamma = \bigsqcup_{i} \Gamma g_i = \bigsqcup_{i} \Gamma g_i \gamma.$$

Then for $n \in N^\Gamma$,

$$\begin{aligned} n[\Gamma g \Gamma]^\gamma &= \sum_i n^{g_i \gamma} \\ &= \sum_i n^{g_i} \\ &= n[\Gamma g \Gamma] \end{aligned}$$

establishing that $n[\Gamma g \Gamma] \in N^\Gamma$. □

The previous proposition shows that a fixed element $\Gamma g \Gamma \in \mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$ defines a map on $[\Gamma g \Gamma] : N^\Gamma \to N^\Gamma$ given by

$$n[\Gamma g \Gamma] = \sum_{i=1}^{c} n^{g_i}.$$

where

$$\Gamma g \Gamma = \bigsqcup_{i=1}^{c} \Gamma g_i$$

is a disjoint decomposition. Extending linearly, every element of $\mathscr{H}(\Gamma g \Gamma)$ defines a map from N^Γ to N^Γ. We call the elements of $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$ **Hecke operators**.

Proposition 2.2.5. *Let* $\Gamma g \Gamma, \Gamma h \Gamma \in \mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$. *Suppose we have disjoint decompositions*

$$\Gamma g \Gamma = \bigsqcup_i \Gamma g_i$$

and

$$\Gamma h \Gamma = \bigsqcup_j \Gamma h_j.$$

The multiplication

$$\Gamma g \Gamma \cdot \Gamma h \Gamma = \sum_{[\gamma] \in \Gamma \backslash \mathfrak{s}(\Gamma) / \Gamma} c_\gamma \Gamma \gamma \Gamma$$

where $c_\gamma = \#\{(i,j) : \Gamma g_i h_j = \Gamma \gamma\}$ *extends to a well-defined binary operation on* $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$.

Proof. Consider the free $\mathbb{Z}$-module $\mathbb{Z}[\Gamma \setminus \mathfrak{s}(\Gamma)]$ generated by the right cosets Γg for $g \in \mathfrak{s}(\Gamma)$. We then have a map from $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$ into $\mathbb{Z}[\Gamma \setminus \mathfrak{s}(\Gamma)]$ given by

$$\Gamma g \Gamma = \bigsqcup_i \Gamma g_i \mapsto \sum_i \Gamma g_i.$$

We then consider $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$ as a $\mathbb{Z}$-submodule of $\mathbb{Z}[\Gamma \setminus \mathfrak{s}(\Gamma)]$. It follows from the definitions that

$$\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma)) \cong \mathbb{Z}[\Gamma \setminus \mathfrak{s}(\Gamma)]^{\Gamma}.$$

Let

$$\Gamma g \Gamma = \bigsqcup_i \Gamma g_i \quad \text{and} \quad \Gamma h \Gamma = \bigsqcup_j \Gamma h_j$$

be disjoint decompositions. It is clear that $\mathfrak{s}(\Gamma)$ act on $\mathbb{Z}[\Gamma \setminus \mathfrak{s}(\Gamma)]$ via

$$\left(\sum_k \Gamma \gamma_k\right)^g = \sum_k (\Gamma \gamma_k)^g = \sum_k \Gamma \gamma_k g.$$

By the definition of the mapping $[\Gamma h \Gamma : \mathbb{Z}[\Gamma \setminus \mathfrak{s}(\Gamma)]^{\Gamma} \to \mathbb{Z}[\Gamma \setminus \mathfrak{s}(\Gamma)]^{\Gamma}]$ we have

$$\begin{aligned}\left(\sum_i \Gamma g_i\right)[\Gamma h \Gamma] &= \sum_j \left(\sum_i \Gamma g_i\right)^{h_j} \\ &= \sum_j \sum_i (\Gamma g_i)^{h_j} \\ &= \sum_i \sum_j \Gamma g_i h_j \\ &= \sum_{[\gamma] \in \Gamma \setminus \mathfrak{s}(\Gamma)/\Gamma} c_\gamma \Gamma \gamma \Gamma\end{aligned}$$

with $c_\gamma = \#\{(i,j) : \Gamma g_i h_j = \Gamma \gamma\}$. Thus the mapping for elements of $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$ on $\mathbb{Z}[\Gamma \setminus \mathfrak{s}(\Gamma)]^{\Gamma}$ is just the multiplication defined on $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$. The result now follows from the previous proposition. □

Proposition 2.2 endows $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$ with the structure of a ring. Moreover, we have the following corollary

Corollary 2.2.6. *Let $n \in N^{\Gamma}$. Then for $\Gamma g \Gamma, \Gamma h \Gamma \in \mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$ we have*

$$n[\Gamma g \Gamma][\Gamma h \Gamma] = n[\Gamma g \Gamma \cdot \Gamma h \Gamma].$$

In particular, $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$ acts on N^{Γ}.

Proof. The proposition follows easily from the definitions and the fact that the product $\Gamma g \Gamma \cdot \Gamma h \Gamma$ is well-defined. □

We end this chapter by giving a sufficient condition for the Hecke ring $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$ to be commutative.

Theorem 2.2.7. *Let $\sigma : \mathfrak{s}(\Gamma) \to \mathfrak{s}(\Gamma)$ be a map that satisfies*

(i) $\sigma(gh) = \sigma(h)\sigma(g)$ *and* $\sigma(\sigma(g)) = g$ *for all* $g, h \in \mathfrak{s}(\Gamma)$,

(ii) $\sigma(\Gamma) = \Gamma$,

(iii) $\Gamma g \Gamma = \Gamma \sigma(g) \Gamma$ *for all* $g \in \mathfrak{s}(\Gamma)$.

Then the product of elements in $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$ *is commutative.*

Proof. Let $g \in \mathfrak{s}(\Gamma)$ and let

$$\Gamma g \Gamma = \bigsqcup_{i=1}^{c} \Gamma g_i.$$

Then

$$\begin{aligned} \Gamma g \Gamma &= \Gamma \sigma(g) \Gamma \\ &= \sigma(\Gamma g \Gamma) \\ &= \bigsqcup_{i=1}^{c} \sigma(g_i) \Gamma. \end{aligned}$$

We prove that $\Gamma g_k \cap \sigma(g_l)\Gamma \neq \emptyset$ for all k and l. Assume that $\Gamma g_k \cap \sigma(g_l)\Gamma = \emptyset$. Then

$$\Gamma g_k \subseteq \bigsqcup_{i \neq l} \sigma(g_i)\Gamma$$

implying that

$$\Gamma g \Gamma = \Gamma g_k \Gamma \subseteq \bigsqcup_{i \neq l} \sigma(g_i)\Gamma \subset \Gamma g \Gamma$$

which is, of course, a contradiction. Thus $\Gamma g_k \cap \sigma(g_l)\Gamma \neq \emptyset$. In particular, $\Gamma g_i \cap \sigma(g_i)\Gamma \neq \emptyset$ for all i. For each i, let $g_i' \in \Gamma g_i \cap \sigma(g_i)\Gamma$. Then

$$\Gamma g \Gamma = \bigsqcup_i \Gamma g_i' = \bigsqcup_i g_i' \Gamma.$$

Now let $\Gamma g \Gamma, \Gamma h \Gamma \in \mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$. By the above argument we have sets of representatives $\{g_i\}$ and $\{h_j\}$ such that

$$\Gamma g \Gamma = \bigsqcup_i \Gamma g_i = \bigsqcup_i g_i \Gamma$$

and

$$\Gamma h \Gamma = \bigsqcup_j \Gamma h_j = \bigsqcup_j h_j \Gamma.$$

Moreover, we have

$$\Gamma g\Gamma = \bigsqcup_i \Gamma\sigma(g_i) = \bigsqcup_i \sigma(g_i)\Gamma$$

and

$$\Gamma h\Gamma = \bigsqcup_j \Gamma\sigma(h_j) = \bigsqcup_j \sigma(h_j)\Gamma.$$

Now we compute the products $\Gamma g\Gamma \cdot \Gamma h\Gamma$ and $\Gamma h\Gamma \cdot \Gamma g\Gamma$. By definition,

$$\Gamma g\Gamma \cdot \Gamma h\Gamma = \sum_{[\gamma]\in\Gamma\backslash\mathfrak{s}(\Gamma)/\Gamma} c_\gamma \Gamma\gamma\Gamma$$

and

$$\Gamma h\Gamma \cdot \Gamma g\Gamma = \sum_{[\gamma]\in\Gamma\backslash\mathfrak{s}(\Gamma)/\Gamma} c'_\gamma \Gamma\gamma\Gamma.$$

We need to prove that $c_\gamma = c'_\gamma$ for all $\gamma \in \mathfrak{s}(\Gamma)$. To this end, we have that

$$\begin{aligned} c_\gamma &= \#\{(i,j) : \Gamma g_i h_j = \Gamma\gamma\} \\ &= \frac{\#\{(i,j) : \Gamma g_i h_j \Gamma = \Gamma\gamma\Gamma\}}{|\Gamma \setminus \Gamma\gamma\Gamma|} \\ &= \frac{\#\{(i,j) : \Gamma\sigma(h_j)\sigma(g_i)\Gamma = \Gamma\sigma(\gamma)\Gamma\}}{|\Gamma \setminus \Gamma\sigma(\gamma)\Gamma|} \\ &= c'_\gamma. \end{aligned}$$

The claim is proved. □

2.3 Hecke Operators on the Space of Automorphic Forms

Recall that we showed previously that if the group G acts on X on the right then G acts on the $\mathbb{Z}$-module $H(X)$ on the left via $\star_k$. Let Γ be a subgroup of G and let $\mathfrak{s}(\Gamma)$ be a subgroup of G such that $\Gamma \subseteq \mathfrak{s}(\Gamma) \subseteq \mathrm{Com}_G(\Gamma)$. By definition, $H(X)^\Gamma = \mathcal{M}_k(\Gamma)$ and hence $\mathscr{H}(\Gamma, \mathfrak{s}(\Gamma))$ acts on $\mathcal{M}_k(\Gamma)$ by

$$f[\Gamma g\Gamma]_k = \sum_i f \star_k g_i$$

for $f \in \mathcal{M}_k(\Gamma)$, $g \in \mathfrak{s}(\Gamma)$, and with

$$\Gamma g\Gamma = \bigsqcup_i \Gamma g_i$$

a disjoint decomposition into right cosets. By Proposition 2.2.4 we know that $f[\Gamma g\Gamma]_k \in \mathcal{M}_k(\Gamma)$. It is often common to include a normalization factor in the definition of $f[\Gamma g\Gamma]_k$, however we will be sure to specify when this is included in our later definitions.

3 The General Symplectic Group, the Paramodular Group and Siegel Paramodular Forms

3.1 The General Symplectic Group and the Paramodular Group

The goal of this section is to define the key groups and objects that will play a big role in this work. In addition, we will identify important elements and relations that these groups and objects exhibit.

Let E_n denote the $n \times n$ identity matrix, and let 0_n denote the $n \times n$ zero matrix. We put

$$J_n = \begin{bmatrix} 0_n & E_n \\ -E_n & 0_n \end{bmatrix}.$$

We call J_n a **symplectic form**.

Definition 3.1.1. *The **general symplectic group** is defined as*

$$\mathrm{GSp}(2n, \mathbb{R}) = \{g \in \mathrm{GL}(2n, \mathbb{R}) : {}^t g J_n g = \lambda(g) J_n\}$$

*where $\lambda : \mathrm{GSp}(2n, \mathbb{R}) \to \mathbb{R} \setminus \{0\}$ is a group homomorphism called the **multiplier homomorphism**.*

We denote by $\mathrm{GSp}^+(2n, \mathbb{R})$ the subgroup of the general symplectic group consisting of elements g with $\lambda(g) > 0$. Let

$$g = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathrm{GSp}(2n, \mathbb{R})$$

with $A, B, C, D \in M(2n, \mathbb{R})$. Then a computation establishes that ${}^t AC = {}^t CA$, ${}^t BD = {}^t DB$, and ${}^t AD - {}^t CB = \lambda(g) E_n$. We further note here that if ${}^t g J_n g = \lambda(g) J_n$ then

$${}^t g = \lambda(g) J_n g^{-1} J_n^{-1} = -\lambda(g) J_n g^{-1} J_n$$

and

$$\begin{aligned} {}^t({}^t g) J_n {}^t g &= {}^t(-\lambda(g) J_n g^{-1} J_n) J_n (-\lambda(g) J_n g^{-1} J_n) \\ &= (\lambda(g)^2) {}^t J_n ({}^t g^{-1}) {}^t J_n J_n J_n g^{-1} J_n \\ &= (\lambda(g)^2) {}^t J_n ({}^t g^{-1}) J_n g^{-1} J_n \\ &= (\lambda(g)^2) \lambda(g^{-1}) {}^t J_n J_n J_n \\ &= \lambda(g) J_n \end{aligned}$$

which implies that ${}^tg \in \mathrm{GSp}(2n,\mathbb{R})$. It is clear that if $g \in \mathrm{GSp}^+(2n,\mathbb{R})$ then ${}^tg \in \mathrm{GSp}(2n,\mathbb{R})$. This closure under transposition property implies that if

$$g = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathrm{GSp}(2n,\mathbb{R})$$

with $A, B, C, D \in M(2n,\mathbb{R})$ we have the additional relations $A^tB = B^tA$, $C^tD = D^tC$, and $A^tD - B^tC = \lambda(g)E_n$.

Definition 3.1.2. *The* ***symplectic group*** *is defined to be*

$$\mathrm{Sp}(2n,\mathbb{R}) = \{g \in \mathrm{GSp}(2n,\mathbb{R}) : \lambda(g) = 1\}.$$

From an arithmetic point of view we will be interested in some specific subgroups of $\mathrm{Sp}(2n,\mathbb{R})$.

Definition 3.1.3. *The* ***modular group*** *is defined to be*

$$\mathrm{Sp}(2n,\mathbb{Z}) = \mathrm{Sp}(2n,\mathbb{R}) \cap M(2n,\mathbb{Z}).$$

Definition 3.1.4. *Let $M \geq 1$ be an integer. The* ***principal congruence subgroup of level*** *M is defined to be*

$$\Gamma(M) = \{g \in \mathrm{Sp}(2n,\mathbb{Z}) : g \equiv E_{2n} \pmod{M}\}.$$

We call $\Gamma \subseteq \mathrm{Sp}(2n,\mathbb{Z})$ a ***congruence subgroup of level*** *M if $\Gamma(M) \subseteq \Gamma$ and $\Gamma(M') \not\subseteq \Gamma$ for all $M' < M$.*

From this point on we fix $n = 2$ and we set $J_2 = J$. We mention some important congruence subgroups. For an integer $M \geq 1$, the Siegel congruence subgroup is

$$\mathrm{Si}(4,M) = \mathrm{Sp}(4,\mathbb{Z}) \cap \begin{bmatrix} \mathbb{Z} & \mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ M\mathbb{Z} & M\mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ M\mathbb{Z} & M\mathbb{Z} & \mathbb{Z} & \mathbb{Z} \end{bmatrix},$$

i.e., those matrices in the modular group whose lower left 2×2 block is congruent to 0 modulo M. The Klingen congruence subgroup is

$$\mathrm{Kl}(4,M) = \mathrm{Sp}(4,\mathbb{Z}) \cap \begin{bmatrix} \mathbb{Z} & \mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ M\mathbb{Z} & \mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ M\mathbb{Z} & M\mathbb{Z} & \mathbb{Z} & M\mathbb{Z} \\ M\mathbb{Z} & \mathbb{Z} & \mathbb{Z} & \mathbb{Z} \end{bmatrix}.$$

The Klingen congruence subgroup will play an important role in this work. We also define the subgroup of $\mathrm{GSp}(4,\mathbb{R})$ that will be of the most importance to us.

Definition 3.1.5. *Let $M \geq 1$ be an integer. We define the* ***paramodular group of level*** M *to be*

$$\mathrm{K}(M) = \mathrm{Sp}(4,\mathbb{R}) \cap M(4,\mathbb{Q}) \cap \begin{bmatrix} \mathbb{Z} & \mathbb{Z} & M^{-1}\mathbb{Z} & \mathbb{Z} \\ M\mathbb{Z} & \mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ M\mathbb{Z} & M\mathbb{Z} & \mathbb{Z} & M\mathbb{Z} \\ M\mathbb{Z} & \mathbb{Z} & \mathbb{Z} & \mathbb{Z} \end{bmatrix}.$$

We note that $\mathrm{Kl}(M) = \mathrm{Kl}(4,M) \subseteq \mathrm{K}(M)$ and $K(1) = \mathrm{Sp}(4,\mathbb{Z})$. The paramodular group also contains some important symmetry elements that we will abuse frequently.

Proposition 3.1.6. *Let $M \geq 1$ be an integer. Let*

$$V \in \Gamma_0(M) \cup \left\{ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\},$$

and let

$$T \in \begin{bmatrix} M^{-1}\mathbb{Z} & \mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}.$$

with ${}^tT = T$. Then

$$\begin{bmatrix} V & 0_2 \\ 0_2 & {}^tV^{-1} \end{bmatrix}, \begin{bmatrix} E_2 & T \\ 0_2 & E_2 \end{bmatrix} \in \mathrm{K}(M).$$

Proof. It is clear that the elements are of the appropriate form. We need only show that they are in $\mathrm{GSp}^+(4,\mathbb{R})$. We have

$$\begin{aligned} \begin{bmatrix} {}^tV & 0_2 \\ 0_2 & V^{-1} \end{bmatrix} \begin{bmatrix} 0_2 & E_2 \\ -E_2 & 0_2 \end{bmatrix} \begin{bmatrix} V & 0_2 \\ 0_2 & {}^tV^{-1} \end{bmatrix} &= \begin{bmatrix} {}^tV & 0_2 \\ 0_2 & V^{-1} \end{bmatrix} \begin{bmatrix} 0_2 & {}^tV^{-1} \\ -V & 0_2 \end{bmatrix} \\ &= \begin{bmatrix} 0_2 & E_2 \\ -E_2 & 0_2 \end{bmatrix} \end{aligned}$$

and

$$\begin{aligned} \begin{bmatrix} E_2 & 0_2 \\ {}^tT & E_2 \end{bmatrix} \begin{bmatrix} 0_2 & E_2 \\ -E_2 & 0_2 \end{bmatrix} \begin{bmatrix} E_2 & T \\ 0_2 & E_2 \end{bmatrix} &= \begin{bmatrix} E_2 & 0_2 \\ T & E_2 \end{bmatrix} \begin{bmatrix} 0_2 & E_2 \\ -E_2 & -T \end{bmatrix} \\ &= \begin{bmatrix} 0_2 & E_2 \\ -E_2 & 0_2 \end{bmatrix}. \end{aligned}$$

The claim is proved. □

The paramodular group also contains the following four symmetry elements which will be invaluable in many computations

$$t_M = \begin{bmatrix} 0 & 0 & -M^{-1} & 0 \\ 0 & 1 & 0 & 0 \\ M & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad p_1 = \begin{bmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \text{and} \quad p_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & a' & 0 & b' \\ 0 & 0 & 1 & 0 \\ 0 & c' & 0 & d' \end{bmatrix},$$

where

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(M) \quad \text{and} \quad \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z}).$$

For much of the matrix theory ahead, it is convenient to prove some claims for $M = 1$ and then extend to general $M > 1$.

3.2 Some Results on $\mathbf{K}(1) = \mathbf{Sp}(4, \mathbb{Z})$

Our goal of this section is to prove some structural theorems involving $K(1) = \mathrm{Sp}(4, \mathbb{Z})$. We start with a few technical lemmas.

Lemma 3.2.1. *Let*

$$u = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \quad \text{and} \quad v = \begin{bmatrix} v_1 & v_2 \end{bmatrix}$$

with $u_1, u_2, v_1, v_2 \in \mathbb{Z}$. *Then there exists matrices* $g, h \in \mathrm{SL}(2,\mathbb{Z})$ *such that*

$$gu = \begin{bmatrix} \delta_1 \\ 0 \end{bmatrix} \quad \text{and} \quad vh = \begin{bmatrix} \delta_2 & 0 \end{bmatrix}$$

where $\delta_1 = \gcd(u_1, u_2)$ *and* $\delta_2 = \gcd(v_1, v_2)$.

Proof. Let $\delta_1 = \gcd(u_1, u_2)$ and write $\delta_1 = au_1 + bu_2$. Then

$$1 = a\frac{u_1}{\delta_1} + b\frac{u_2}{\delta_1}$$

and hence

$$\begin{bmatrix} a & b \\ -\frac{u_2}{\delta_1} & \frac{u_1}{\delta_1} \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

and

$$\begin{bmatrix} a & b \\ -\frac{u_2}{\delta_1} & \frac{u_1}{\delta_1} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} \delta_1 \\ 0 \end{bmatrix}.$$

The other case is proved similarly. □

Lemma 3.2.2 (Smith normal form over $\mathrm{SL}(2,\mathbb{Z})$)**.** *Let A be a 2×2 integer matrix. There exists $g, h \in \mathrm{SL}(2,\mathbb{Z})$ such that*

$$gAh = \begin{bmatrix} m_1 & 0 \\ 0 & m_2 \end{bmatrix}$$

with $m_1, m_2 \in \mathbb{Z}$ and $m_1 | m_2$.

Proof. Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(2,\mathbb{Z}).$$

and let $\delta_1 = \gcd(a,c)$. By Lemma 3.2.1, there exists $\alpha_1 \in \mathrm{SL}(2,\mathbb{Z})$ such that

$$\alpha_1 A = \begin{bmatrix} \delta_1 & b_2 \\ 0 & d_2 \end{bmatrix}.$$

Now let $\delta_2 = \gcd(\delta_1, b_2)$. Again by Lemma 3.2.1, there exists $\alpha_2 \in \mathrm{SL}(2,\mathbb{Z})$ such that

$$\alpha_1 A \alpha_2 = \begin{bmatrix} \delta_2 & 0 \\ c_3 & d_3 \end{bmatrix}.$$

We repeat this process and thus build a sequence $\{\delta_n\}_{n=1}^{\infty}$. It is clear that for all $n \in \mathbb{N}$, $\delta_{n+1} \leq \delta_n$. Let r be the minimal such r such that $\delta_{r+1} = \delta_r$. We suppose for now that r is odd. Then, by nature of the construction in Lemma 3.2.1, we end up at

$$\alpha_r \alpha_{r-2} \cdots \alpha_1 A \alpha_2 \alpha_4 \cdots \alpha_{r+1} = \begin{bmatrix} \delta_{r+1} & 0 \\ 0 & d_{r+2} \end{bmatrix}.$$

If $\delta_{r+1} | d_{r+2}$ then we are done. If this is not the case then we add a few more steps. First multiply on the right by

$$\alpha = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

to obtain

$$\alpha_r\alpha_{r-2}\cdots\alpha_1 A\alpha_2\alpha_4\cdots\alpha_{r+1}\alpha = \begin{bmatrix} \delta_{r+1} & 0 \\ d_{r+2} & d_{r+2} \end{bmatrix}.$$

Let $\delta = \gcd(\delta_{r+1}, d_{r+2})$ and let $x, y \in \mathbb{Z}$ be such that $\delta = x\delta_{r+1} + yd_{r+2}$. Then

$$\beta = \begin{bmatrix} x & y \\ -\frac{d_{r+2}}{\delta} & \frac{\delta_{r+1}}{\delta} \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z})$$

and

$$\beta\alpha_r\alpha_{r-1}\cdots\alpha_1 A\alpha_2\alpha_4\cdots\alpha_{r+1}\alpha = \begin{bmatrix} \delta & yd_{r+2} \\ 0 & \frac{\delta_{r+1}}{\delta}d_{r+2} \end{bmatrix}.$$

Lastly, we multiply on the right by

$$\gamma = \begin{bmatrix} 1 & -\frac{yd_{r+2}}{\delta} \\ 0 & 1 \end{bmatrix}$$

to obtain

$$\beta\alpha_r\alpha_{r-1}\cdots\alpha_1 A\alpha_2\alpha_4\cdots\alpha_{r+1}\alpha\gamma = \begin{bmatrix} \delta & 0 \\ 0 & \frac{\delta_{r+1}}{\delta}d_{r+2} \end{bmatrix}$$

completing the proof in the case r is odd. The proof is similar in the case r is even □

Lemma 3.2.3. *Let*

$$u = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix}$$

with $u_1, u_2, u_3, u_4 \in \mathbb{Z}$. *Then there exists* $g \in \mathrm{Sp}(4, \mathbb{Z})$ *such that*

$$gu = \begin{bmatrix} \delta \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

where $\delta = \gcd(u_1, u_2, u_3, u_4)$

Proof. Note that $\mathrm{Sp}(4,\mathbb{Z})$ contains the elements

$$\begin{bmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & c & 0 & d \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & d & -c \\ 0 & 0 & -b & a \end{bmatrix}$$

where

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z}).$$

The result now follows from three applications of Lemma 3.2.1. □

The previous lemmas are pivotal in proving some extremely valuable results.

Proposition 3.2.4. *Let $g \in M(4,\mathbb{Q})$ be such that ${}^t gJg = qJ$ for some $q \in \mathbb{Q} \setminus \{0\}$. Then there exists $\alpha \in \mathrm{Sp}(4,\mathbb{Z})$ such that αg has the form*

$$\begin{bmatrix} a_1 & a_2 & b_1 & b_2 \\ 0 & a_4 & b_3 & b_4 \\ 0 & 0 & d_1 & 0 \\ 0 & 0 & d_3 & d_4 \end{bmatrix} \in M(4,\mathbb{Q}).$$

Proof. Start by writing g in the form

$$g = \begin{bmatrix} u_1 & u_2 & u_3 & u_4 \\ u_5 & u_6 & u_7 & u_8 \\ u_9 & u_{10} & u_{11} & u_{12} \\ u_{13} & u_{14} & u_{15} & u_{16} \end{bmatrix}$$

with $u_i \in \mathbb{Q}$ for $1 \le i \le 16$. Without loss of generality we may assume that $u_i \in \mathbb{Z}$ for $1 \le i \le 16$. We then apply the Lemma 3.2.3 to the first column of g. So for some $\gamma_1 \in \mathrm{Sp}(4,\mathbb{Z})$ we obtain

$$\gamma_1 g = \begin{bmatrix} u'_1 & u'_2 & u'_3 & u'_4 \\ 0 & u'_6 & u'_7 & u'_8 \\ 0 & u'_{10} & u'_{11} & u'_{12} \\ 0 & u'_{14} & u'_{15} & u'_{16} \end{bmatrix}$$

with $u'_1 = \gcd(u_1, u_2, u_3, u_4)$. Since

$$\begin{bmatrix} u'_1 & 0 \\ u'_2 & u'_6 \end{bmatrix} \begin{bmatrix} 0 & u'_{10} \\ 0 & u'_{14} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ u'_{10} & u'_{14} \end{bmatrix} \begin{bmatrix} u'_1 & u'_2 \\ 0 & u'_6 \end{bmatrix}$$

we see that $u'_1 u'_{10} = 0$ and hence $u'_{10} = 0$. Moreover, since

$$\begin{bmatrix} 0 & 0 \\ 0 & u'_{14} \end{bmatrix} \begin{bmatrix} u'_{11} & u'_{15} \\ u'_{12} & u'_{16} \end{bmatrix} = \begin{bmatrix} u'_{11} & u'_{12} \\ u'_{15} & u'_{16} \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & u'_{14} \end{bmatrix}$$

we see that $u'_{12} u'_{14} = 0$ and hence $u'_{14} = 0$ or $u'_{12} = 0$. If $u'_{14} = 0$ then the fact that

$$\begin{bmatrix} u'_1 & 0 \\ u'_2 & u'_4 \end{bmatrix} \begin{bmatrix} u'_{11} & u'_{12} \\ u'_{15} & u'_{16} \end{bmatrix} = \begin{bmatrix} \lambda(g) & 0 \\ 0 & \lambda(g) \end{bmatrix}$$

yields $u'_1 u'_{12} = 0$. Hence $u'_{12} = 0$. If $u'_{12} = 0$ then we have a matrix of the form

$$\gamma_1 g = \begin{bmatrix} u'_1 & u'_2 & u'_3 & u'_4 \\ 0 & u'_6 & u'_7 & u'_8 \\ 0 & 0 & u'_{11} & 0 \\ 0 & u'_{14} & u'_{15} & u'_{16} \end{bmatrix}.$$

Considering the submatrix

$$\begin{bmatrix} u'_6 & u'_8 \\ u'_{14} & u'_{16} \end{bmatrix}$$

we apply Lemma 3.2.1 to obtain a matrix $\beta \in \mathrm{SL}(2, \mathbb{Z})$ such that

$$\beta \begin{bmatrix} u'_6 & u'_8 \\ u'_{14} & u'_{16} \end{bmatrix} = \begin{bmatrix} u''_6 & u''_8 \\ 0 & u''_{16} \end{bmatrix}$$

where $u''_6 = \gcd(u'_6, u'_{14})$. But then the previous lemma allows us to construct a matrix $\gamma_2 \in \mathrm{Sp}(4, \mathbb{Z})$ using β to obtain a matrix of the form

$$\gamma_2 \gamma_1 g = \begin{bmatrix} u'_1 & u'_2 & u'_3 & u'_4 \\ 0 & u''_6 & u''_7 & u''_8 \\ 0 & 0 & u'_{11} & 0 \\ 0 & 0 & u''_{15} & u''_{16} \end{bmatrix}.$$

This completes the proof. □

Putting everything together we obtain the following theorem.

Theorem 3.2.5. *Every double coset* $\mathrm{Sp}(4, \mathbb{Z}) g \mathrm{Sp}(4, \mathbb{Z})$ *with* $g \in \mathrm{GSp}^+(4, \mathbb{Q})$ *contains an element of the form*

$$\mathrm{diag}(d_1, d_2, e_1, e_2)$$

with $d_1, d_2, e_1, e_2 > 0$*,* $d_1 | d_2 | e_2 | e_1$*, and* $d_1 e_1 = d_2 e_2 = \lambda(g)$*.*

Proof. We follow the proof given in [2] and [5]. Without loss of generality, we may assume that g is an integer matrix. Furthermore, we may assume that g has relatively prime entries. Let δ_i denote the greates common divisor of the ith column of g, and let $\delta = \min\{\delta_i : 1 \le i \le 4\}$. We proceed by induction on δ and prove that the double coset $\mathrm{Sp}(4, \mathbb{Z})$ contains a representative of the form

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & u_6 & 0 & u_8 \\ 0 & 0 & \lambda(g) & 0 \\ 0 & u_{14} & 0 & u_{16} \end{bmatrix}.$$

First suppose that $\delta = 1$. Let i be the index of the first column whose entries are relatively prime. By replacing g by gJ we assume $i = 1$ or $i = 2$. If $i = 2$, we replace g by

$$g \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

allowing us to assume that $i = 1$. We now apply Lemma 3.2.3 to the first column of g obtaining a matrix of the form

$$\begin{bmatrix} 1 & u_2 & u_3 & u_4 \\ 0 & u_6 & u_7 & u_8 \\ 0 & u_{10} & u_{11} & u_{12} \\ 0 & u_{14} & u_{15} & u_{16} \end{bmatrix}.$$

We now multiply on the right by the matrix

$$\begin{bmatrix} 1 & u_2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -u_2 & 0 \end{bmatrix}$$

to obtain a matrix of the form

$$\begin{bmatrix} 1 & 0 & u_3' & u_4 \\ 0 & u_6 & u_7' & u_8 \\ 0 & u_{10} & u_{11}' & u_{12} \\ 0 & u_{14} & u_{15}' & u_{16} \end{bmatrix}.$$

We then multiply on the right by

$$\begin{bmatrix} 1 & 0 & -u_3' & -u_4 \\ 0 & 1 & -u_4 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

to arrive at a matrix of the form

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & u_6 & u_7'' & u_8 \\ 0 & u_{10} & u_{11}'' & u_{12} \\ 0 & u_{14} & u_{15}'' & u_{16} \end{bmatrix}.$$

It now follows from relations on $\mathrm{GSp}(4,\mathbb{R})$ that $u_7'' = u_{10} = u_{12} = u_{15}'' = 0$. We have thus arrived at a matrix of the form

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & u_6 & 0 & u_8 \\ 0 & 0 & \lambda(g) & 0 \\ 0 & u_{14} & 0 & u_{16} \end{bmatrix}.$$

This proves the claim for $\delta = 1$. We now assume the claim has been proven for all matrices with relatively prime entries with $\delta < \delta'$. We prove the claim for matrices with relatively prime entries and with $\delta = \delta'$. As before, we modify until we obtain a matrix of the form

$$\begin{bmatrix} \delta' & u_2 & u_3 & u_4 \\ 0 & u_6 & u_7 & u_8 \\ 0 & u_{10} & u_{11} & u_{12} \\ 0 & u_{14} & u_{15} & u_{16} \end{bmatrix}$$

with the property that u_2, u_3, and u_4 lie between 1 and δ' (with 1 and δ' allowed). We then have a matrix with $\delta \leq \delta'$. If $\delta = \delta'$ then all entries of the matrix would be divisible by δ', a contradiction. Thus $\delta < \delta'$. By the induction hypothesis, we obtain a matrix of the desired form. Returning now to the general case we have the ability to modify g to obtain a matrix of the form

$$\begin{bmatrix} d_1 & 0 & 0 & 0 \\ 0 & u_6 & 0 & u_8 \\ 0 & 0 & e_1 & 0 \\ 0 & u_{14} & 0 & u_{16} \end{bmatrix}$$

with $d_1, e_1 > 0$, $d_1 | e_1$, and $d_1 e_1 = \lambda(g)$. Now we apply Lemma 3.2.2 to the block

$$\begin{bmatrix} u_6 & u_8 \\ u_{14} & u_{16} \end{bmatrix}$$

to obtain a matrix of the form

$$\begin{bmatrix} d_1 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 \\ 0 & 0 & e_1 & 0 \\ 0 & 0 & 0 & e_2 \end{bmatrix}$$

with $d_2, e_2 > 0$, $d_2 | e_2$, and $d_2 e_2 = \lambda(g)$. If necessary, we apply Lemma 3.2.2 to the block

$$\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$$

to ensure that $d_1 | d_2$. We thus can guarantee a matrix of the form

$$\begin{bmatrix} d_1 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 \\ 0 & 0 & e_1 & 0 \\ 0 & 0 & 0 & e_2 \end{bmatrix}$$

with $d_1, d_2, e_1, e_2 > 0$, $d_1 | d_2 | e_2 | e_1$, and $d_1 e_1 = d_2 e_2 = \lambda(g)$. The proof is complete. □

3.3 Siegel Paramodular Forms

The Siegel upper half-space is the set

$$\mathcal{H}_2 = \{Z \in M(2, \mathbb{C}) : {}^t Z = Z, \ \mathrm{Im}(Z) > 0\}.$$

The group $\mathrm{GSp}^+(4, \mathbb{R})$ acts on $\mathcal{H}_2$ by

$$g \cdot Z = (AZ + B)(CZ + D)^{-1}$$

for

$$g = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathrm{GSp}^+(4, \mathbb{R})$$

with $A, B, C, D \in M(2, R)$ and $Z \in \mathcal{H}_2$. We saw in Section 2.1 that this left action on $\mathcal{H}_2$ induces a right action on $H(\mathcal{H}_2)$. We have for $k \geq 0$

$$(F \star_k g)(Z) = \lambda(g)^k \det(CZ + D)^{-k} F(g \cdot Z)$$

for $g \in \mathrm{GSp}^+(4, \mathbb{R})$ as above and $Z \in \mathcal{H}_2$.

Definition 3.3.1. *Let $M \geq 1$ and $k \geq 0$ be fixed integers. Let $F : \mathcal{H}_2 \to \mathbb{C}$ be a holomorphic function. We say F is a **Siegel paramodular form of level M and weight k** if for all $g \in \mathrm{K}(M)$ we have*

$$F \star_k g = F.$$

By Proposition 3.1.6 we have

$$\begin{bmatrix} E_2 & E_2 \\ 0_2 & E_2 \end{bmatrix} \in \mathrm{K}(M)$$

and hence for a Siegel paramodular form of level M and weight k we have

$$F \star_k \begin{bmatrix} E_2 & E_2 \\ 0_2 & E_2 \end{bmatrix} = F.$$

This is to say

$$F(Z + E_2) = F(Z),$$

i.e., F is periodic. The Koecher principle (see [5], pg. 62) implies that F has a Fourier expansion

$$F(Z) = \sum_{S \in A(1)} a(S) e^{2\pi i \mathrm{tr}(SZ)}$$

where

$$A(1) = \left\{ \begin{bmatrix} r & t/2 \\ t/2 & s \end{bmatrix} \in M(2, \mathbb{Q}) : r, t, s \in \mathbb{Z} \text{ and } rs - \frac{t^2}{4} \geq 0 \right\}.$$

Proposition 3.3.2. *Let $M \geq 1$ and $k \geq 0$ be integers. Let $F : \mathcal{H}_2 \to \mathbb{C}$ be a Siegel paramodular form of level M and weight k with Fourier expansion*

$$F(Z) = \sum_{S \in A(1)} a(S) e^{2\pi i \mathrm{tr}(SZ)}.$$

If $M \nmid r$, then $a(S) = 0$ and for all

$$U \in \Gamma_0(M) \cup \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \Gamma_0(M)$$

we have

$$a(S) = a({}^tUSU).$$

Proof. Both of these claims follow easily by observing that $\mathrm{K}(M)$ contains the elements

$$\begin{bmatrix} 1 & 0 & M^{-1}n & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} U & 0_2 \\ 0_2 & {}^tU^{-1} \end{bmatrix}$$

where $n \in \mathbb{Z}$ and

$$U \in \Gamma_0(M) \cup \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \Gamma_0(M)$$

by Proposition 3.1.6. $\square$

The previous proposition establishes that a Siegel paramodular form of level M and weight k has a Fourier expansion of the form

$$F(Z) = \sum_{S \in A(M)} a(S) e^{2\pi i \mathrm{tr}(SZ)}$$

where

$$A(M) = \left\{ \begin{bmatrix} Mr & t/2 \\ t/2 & s \end{bmatrix} \in M(2, \mathbb{Q}) : r, t, s \in \mathbb{Z} \text{ and } Mrs - \frac{t^2}{4} \geq 0 \right\}.$$

For more information on Siegel paramodular forms one should see [33] and [35]. If one is interested in the Siegel paramodular forms in accordance with the paramodular conjecture of Brumer and Kramer [6] then one should see [31] and [32].

4 Construction of Paramodular Hecke Operators

In this chapter we will be developing the definition of the paramodular Hecke operators that are used in the literature. We will be doing this by first looking at the Hecke operators of a specific congruence subgroup of $\mathrm{Sp}(4,\mathbb{Z})$ and then extending in a natural way to the paramodular group $\mathrm{K}(M)$.

4.1 Hecke Operators of a Certain Congruence Subgroup

In this section we will construct the Hecke operators of a certain congruence subgroup of $\mathrm{Sp}(4,\mathbb{Z})$ following the construction appearing in [2]. Let

$$\mathfrak{s}(M) = \left\{ g = \begin{bmatrix} * & * & * & * \\ M* & * & * & * \\ M* & M* & * & M* \\ M* & * & * & * \end{bmatrix} \in \mathrm{GSp}^+(4,\mathbb{Q}) \cap \mathrm{GL}(4,\mathbb{Z}_{(M)}) : * \in \mathbb{Z}_{(M)} \right\}$$

where $\mathbb{Z}_{(M)}$ is the ring of rational numbers whose denominator is prime to $M \in \mathbb{Z}$. It is clear that $\mathfrak{s}(M)$ is a subgroup of $\mathrm{GSp}^+(4,\mathbb{Q})$. Define also the group

$$\mathfrak{s}^*(M) = \left\{ g \in \mathrm{GSp}^+(4,\mathbb{Q}) \cap \mathrm{GL}(4,\mathbb{Z}_{(M)}) : g \equiv \begin{bmatrix} E_2 & 0_2 \\ 0_2 & \lambda(g)E_2 \end{bmatrix} \pmod{M} \right\}.$$

where

$$E_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Each of these groups play an important role in building the operators we are interested in studying. To build the Hecke operators of the paramodular group we begin with a study of a certain congruence subgroup whose associated Hecke operators are related to those of the paramodular group.

Definition 4.1.1. *Let* Γ *be a congruence subgroup of* $\mathrm{Sp}(4,\mathbb{Z})$*. We say that* Γ *is* ***M-symmetric*** *if*

$$\Gamma\mathfrak{s}^*(M) = \mathfrak{s}^*(M)\Gamma.$$

In this case, we associate to Γ *the set*

$$\mathfrak{s}^{\Gamma}(M) = \Gamma\mathfrak{s}^*(M)\Gamma = \Gamma\mathfrak{s}^*(M) = \mathfrak{s}^*(M)\Gamma$$

which is a subgroup of $\mathrm{GSp}^+(4,\mathbb{Q})$*. We call* $s^{\Gamma}(M)$ *the* ***symmetrizer*** *of* Γ*.*

Recall now the definition of the Klingen parabolic subgroup, $\mathrm{Kl}(M)$, given in § 5. This congruence subgroup will be the group that will help us bridge the gap to the definition of the paramodular Hecke operators.

Lemma 4.1.2. *Each of the right cosets* $\mathrm{Kl}(M)g$ *with* $g \in \mathfrak{s}(M)$ *contains a representative of the form*

$$\begin{bmatrix} a_1 & a_2 & b_1 & b_2 \\ 0 & a_4 & b_3 & b_4 \\ 0 & 0 & d_1 & 0 \\ 0 & 0 & d_3 & d_4 \end{bmatrix}.$$

Proof. By Theorem 3.2.4, there exists $\alpha \in \mathrm{Sp}(4,\mathbb{Z})$ such that $\alpha g = g'$ is of the desired form. But

$$\alpha = g' g^{-1} \in \mathfrak{s}(M) \cap \mathrm{Sp}(4,\mathbb{Z}) = \mathrm{Kl}(M).$$

This completes the proof. □

Lemma 4.1.3. *The congruence subgroup* $\mathrm{Kl}(M)$ *is an* M*-symmetric group. Moreover,*

$$\mathfrak{s}(M) = \mathfrak{s}^{Kl(M)}(M).$$

Proof. Let $g \in \mathfrak{s}(M)$. By Lemma 4.1.2, we may assume that g is of the form

$$\begin{bmatrix} a_1 & a_2 & b_1 & b_2 \\ 0 & a_4 & b_3 & b_4 \\ 0 & 0 & d_1 & 0 \\ 0 & 0 & d_3 & d_4 \end{bmatrix}.$$

Consider the matrix

$$g' = \begin{bmatrix} -\frac{1}{a_1} & \frac{a_2}{a_1 a_4} & \frac{1}{d_1}\left(\frac{b_1}{a_1} - \frac{a_2 b_3}{a_1 a_4}\right) - \frac{d_3}{d_1 d_4}\left(\frac{b_2}{a_1} - \frac{a_2 b_4}{a_1 a_4}\right) & \frac{1}{d_4}\left(\frac{b_2}{a_1} - \frac{a_2 b_4}{a_1 a_4}\right) \\ 0 & -\frac{1}{a_4} & \frac{1}{d_1}\left(\frac{b_3}{a_4} - \frac{b_4 d_3}{a_4 d_4}\right) & \frac{b_4}{a_4 d_4} \\ 0 & 0 & a_1 & 0 \\ 0 & 0 & a_2 & a_4 \end{bmatrix} \in \mathfrak{s}(M).$$

Then g' is an M-integral matrix and, modulo M, belongs to $\mathrm{Sp}(4, \mathbb{Z}/M\mathbb{Z})$. Let $\alpha \in \mathrm{Sp}(4, \mathbb{Z})$ such that $\alpha \equiv g' \pmod{M}$. Then clearly $\alpha \in \mathrm{Kl}(M)$ and

$$\begin{aligned}
\alpha g &\equiv g'g \pmod{M} \\
&= \begin{bmatrix} -\frac{1}{a_1} & \frac{a_2}{a_1a_4} & \frac{1}{d_1}\left(\frac{b_1}{a_1} - \frac{a_2b_3}{a_1a_4}\right) - \frac{d_3}{d_1d_4}\left(\frac{b_2}{a_1} - \frac{a_2b_4}{a_1a_4}\right) & \frac{1}{d_4}\left(\frac{b_2}{a_1} - \frac{a_2b_4}{a_1a_4}\right) \\ 0 & -\frac{1}{a_4} & \frac{1}{d_1}\left(\frac{b_3}{a_4} - \frac{b_4d_3}{a_4d_4}\right) & \frac{b_4}{a_4d_4} \\ 0 & 0 & a_1 & 0 \\ 0 & 0 & a_2 & a_4 \end{bmatrix} \begin{bmatrix} a_1 & a_2 & b_1 & b_2 \\ 0 & a_4 & b_3 & b_4 \\ 0 & 0 & d_1 & 0 \\ 0 & 0 & d_3 & d_4 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a_1d_1 & 0 \\ 0 & 0 & a_2d_1 + a_4d_3 & a_4d_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \lambda(g) & 0 \\ 0 & 0 & 0 & \lambda(g) \end{bmatrix},
\end{aligned}$$

where the last equality follows from the definitions of $\mathrm{GSp}^+(4, \mathbb{R})$. Thus $\alpha g \in \mathfrak{s}^*(M)$ and therefore $g \in \mathrm{Kl}(M)\mathfrak{s}^*(M)$. Consider now g^{-1}. Since $\mathfrak{s}(M)$ is a subgroup of $\mathrm{GSp}^+(4, \mathbb{Q})$, $g^{-1} \in \mathfrak{s}(M)$. By a similar argument as above we have $\beta \in \mathrm{Kl}(M)$ such that

$$\beta g^{-1} \equiv \begin{bmatrix} I_1 & 0_2 \\ 0_2 & \lambda(g^{-1})I_1 \end{bmatrix} \pmod{M}.$$

Hence it follows that

$$g^{-1} \in \mathrm{Kl}(M)\mathfrak{s}^*(M).$$

We then deduce that $g \in \mathfrak{s}^*(M)\mathrm{Kl}(M)$. This proves that $\mathfrak{s}(M) \subseteq \mathrm{Kl}(M)\mathfrak{s}^*(M)$ and $\mathfrak{s}(M) \subseteq \mathfrak{s}^*(M)\mathrm{Kl}(M)$. Since it is obvious that each of the reverse inclusions hold, we have that

$$\mathrm{Kl}(M)\mathfrak{s}^*(M) = \mathfrak{s}^*(M)\mathrm{Kl}(M).$$

Hence $\mathrm{Kl}(M)$ is M-symmetric. It follows immediately that

$$\mathfrak{s}(M) = \mathfrak{s}^{\mathrm{Kl}(M)}(M).$$

The lemma is proved. □

The main purpose of Lemma 4.1.3 will be apparent in a moment, but in the meantime let's state the following theorem from [2] which will also be of some significance.

Theorem 4.1.4. *Let Γ and Γ' be two congruence subgroups of $\mathrm{Sp}(4, \mathbb{Z})$ and suppose that both Γ and Γ' are both M-symmetric with $\Gamma \subset \Gamma'$. Then* *(i)* $\mathfrak{s}^{\Gamma}(M) = \Gamma\mathfrak{s}^{\Gamma'}(M) = \mathfrak{s}^{\Gamma'}(M)\Gamma$,

(ii) $\mathrm{Sp}(4,\mathbb{Z}) \cap \mathfrak{s}^{\Gamma}(M) = \Gamma$,

(iii) if $g, g' \in \mathfrak{s}^{\Gamma}(M)$ *and* $g' \in \Gamma' g \Gamma'$, *then* $g' \in \Gamma(M) g \Gamma$, *where* $\Gamma(M)$ *is the principal congruence subgroup of level* M.

Proof. As mentioned prior to the statement of the theorem, see [2], Theorem 3.3.3, for the proof of these statements. □

These results now come together to establish a very fundamental result about the diagonalizability of the double cosets of the form

$$\mathrm{Kl}(M) g \mathrm{Kl}(M),$$

where $g \in \mathfrak{s}(M)$.

Theorem 4.1.5. *Let* $g \in \mathfrak{s}(M)$ *where* $M \geq 1$. *There exists* $d_1, d_2, e_1, e_2 \in \mathbb{Q}$ *with* $d_i, e_i > 0$ *for* $i \in \{1, 2\}$, $d_1 | d_2 | e_2 | e_1$, *and* $d_i e_i = \lambda(g)$ *for* $i \in \{1, 2\}$ *such that*

$$\mathrm{Kl}(M) g \mathrm{Kl}(M) = \mathrm{Kl}(M) \mathrm{diag}(d_1, d_2, e_1, e_2) \mathrm{Kl}(M).$$

Moreover, the numbers $d_1, d_2, e_1, e_2 \in \mathbb{Q}$ *are unique.*

Proof. The statement for $M = 1$ was proven in Theorem 3.2.5. For arbitrary $M > 1$ let $\gamma_1, \gamma_2 \in \mathrm{Sp}(4,\mathbb{Z})$ be such that $\gamma_1 g \gamma_2$ is of the form $\mathrm{diag}(d_1, d_2, e_1, e_2)$ with d_1, d_2, e_1, e_2 satisfying the desired conditions. Since $\mathrm{diag}(d_1, d_2, e_1, e_2) \in \mathfrak{s}(M)$, by Theorem 4.1.4(iii) we have

$$\begin{aligned}\mathrm{diag}(d_1, d_2, e_1, e_2) &\in \Gamma(M) g \mathrm{Kl}(M)\\ &\subset \mathrm{Kl}(M) g \mathrm{Kl}(M).\end{aligned}$$

We now prove uniqueness. Let $\mathrm{diag}(d_1, d_2, e_1, e_2)$ and $\mathrm{diag}(d_1', d_2', e_1', e_2')$ be two matrices that satisfy the conclusions of the theorem. Then there exists matrices $\gamma_1, \gamma_2 \in \mathrm{Kl}(M)$ such that

$$\gamma_1 \mathrm{diag}(d_1, d_2, e_1, e_2) \gamma_2 = \mathrm{diag}(d_1', d_2', e_1', e_2').$$

One can deduce from this relation that $d_1 | d_1'$. Similarly we have $d_1' | d_1$. Hence $d_1 = d_1'$ and it follows that

$$d_1 e_1 = d_1' e_1' = d_1 e_1'$$

and thus $e_1 = e_1'$. Next we compute the 2×2 principal minors and compare. It is apparent from the computation that we must have $d_2 | d_2'$. Similarly we have $d_2' | d_2$. Hence $d_2 = d_2'$ and it follows that $e_2 = e_2'$. Thus uniqueness is proved. □

Fix $k \in \mathbb{N}$. Let us now consider the subsets of $\mathfrak{s}(M)$

$$\mathfrak{s}_n(M) = \{g \in \mathfrak{s}(M) \cap M(4, \mathbb{Z}) : \lambda(g) = n\}$$

for $n \in \mathbb{N}$ and $\gcd(n, M) = 1$. We define the Hecke operators $T(n)$ for $n \in \mathbb{N}$ with $\gcd(n, M) = 1$ for the Klingen parabolic subgroup by

$$\begin{aligned} T(n) &= n^{k-3} \sum_{[g] \in \mathrm{Kl}(M) \backslash \mathfrak{s}_n(M) / \mathrm{Kl}(M)} [\mathrm{Kl}(M) g \mathrm{Kl}(M)]_k \\ &= n^{k-3} \sum_{\substack{d_1, d_2, e_1, e_2 \in \mathbb{N} \\ d_1 | d_2 | e_2 | e_1 \\ d_1 e_1 = d_2 e_2 = n}} [\mathrm{Kl}(M) \mathrm{diag}(d_1, d_2, e_1, e_2) \mathrm{Kl}(M)]_k, \end{aligned}$$

where $[\mathrm{Kl}(M) g \mathrm{Kl}(M)]_k$ is defined as in Section 2.3 and the last equality follows from Theorem 4.1.5.

Theorem 4.1.6. *Let* $n, n' \in \mathbb{N}$ *with* $\gcd(n, n') = \gcd(nn', M) = 1$. *Then*

$$T(n)T(n') = T(nn') = T(n')T(n).$$

Proof. We prove the commutativity relation first. Consider the map $\sigma : \mathfrak{s}(M) \to \mathfrak{s}(M)$ defined by

$$\sigma\left(\begin{bmatrix} a_1 & a_2 & b_1 & b_2 \\ Ma_3 & a_4 & b_3 & b_4 \\ Mc_1 & Mc_2 & d_1 & Md_2 \\ Mc_3 & c_4 & d_3 & d_4 \end{bmatrix}\right) = \begin{bmatrix} a_1 & a_3 & c_1 & c_3 \\ Ma_2 & a_4 & c_2 & c_4 \\ Mb_1 & Mb_3 & d_1 & Md_3 \\ Mb_2 & b_4 & d_2 & d_4 \end{bmatrix}.$$

A tedious yet straightforward computation establishes that $\sigma(gh) = \sigma(h)\sigma(g)$, $\sigma(\sigma(g)) = g$, $\sigma(\mathrm{Kl}(M) = \mathrm{Kl}(M))$, and $\Gamma\sigma(g)\Gamma = \Gamma g \Gamma$ for all $g, h \in \mathfrak{s}(M)$. The result now follows by Theorem 2.2.7. The multiplicativity of the Hecke operators follows from the fact that

$$\mathfrak{s}_n(M)\mathfrak{s}_{n'}(M) = \mathfrak{s}_{nn'}(M)$$

whenever $\gcd(n, n') = 1$. □

We have that each double coset $\mathrm{Kl}(M) g \mathrm{Kl}(M)$ for $g \in \mathfrak{s}(M)$ is a finite union of right cosets, i.e.,

$$\mathrm{Kl}(M) g \mathrm{Kl}(M) = \bigcup_{i=1}^{m} \mathrm{Kl}(M) g_i.$$

Therefore, since $|\mathrm{Kl}(M)\setminus\mathfrak{s}_n(M)/\mathrm{Kl}(M)|$ is finite, we have that $T(n)$ is defined in terms of a finite collection of matrices. Ultimately, in lieu of the commutativity and multiplicativity relation in Theorem 4.1.6, we are able consider just the operators $T(p^{r_0})$ for p prime with $\gcd(p,M)=1$ and $r_0\geq 0$,

$$T(p^{r_0}) = p^{r_0(k-3)} \sum_{r_1\leq r_2\leq \lfloor \frac{r_0}{2}\rfloor} \left[\mathrm{Kl}(M) \begin{bmatrix} p^{r_1} & 0 & 0 & 0 \\ 0 & p^{r_2} & 0 & 0 \\ 0 & 0 & p^{r_0-r_1} & 0 \\ 0 & 0 & 0 & p^{r_0-r_2} \end{bmatrix} \mathrm{Kl}(M) \right]_k .$$

4.2 Hecke Operators over K(M), $p\nmid M$

In this section we will look at the paramodular Hecke operators over $\mathrm{K}(M)$. We will be using the results from the previous section and so we will only be constructing operators for $p\nmid M$ at this point in time. We'll start by considering the group

$$\mathfrak{s}^{\circ}(M) = \left\{ g = \begin{bmatrix} * & * & M^{-1}* & * \\ M* & * & * & * \\ M* & M* & * & M* \\ M* & * & * & * \end{bmatrix} \in \mathrm{GSp}^{+}(4,\mathbb{Q})\cap \mathrm{GL}(4, M^{-1}\mathbb{Z}_{(M)}) : * \in \mathbb{Z}_{(M)} \right\}$$

which is a subgroup of $\mathrm{GSp}^+(4,\mathbb{Q})$. We will again be considering double cosets of the form

$$\mathrm{K}(M)g\mathrm{K}(M),\;\; g\in\mathfrak{s}^{\circ}(M).$$

It turns out that we actually won't need to use the entirety of $\mathfrak{s}^{\circ}(M)$.

Lemma 4.2.1. *Let $g\in\mathfrak{s}^{\circ}(M)$. Then there exists $\gamma\in\mathrm{K}(M)$ such that $g\gamma\in\mathfrak{s}(M)$.*

Proof. Let $g\in\mathfrak{s}^{\circ}(M)$. Then g has the form

$$\begin{bmatrix} a_1 & a_2 & M^{-1}b_1 & b_2 \\ Ma_3 & a_4 & b_3 & b_4 \\ Mc_1 & Mc_2 & d_1 & Md_2 \\ Mc_3 & c_4 & d_3 & d_4 \end{bmatrix}.$$

As the denominators of the entries a_i, b_i, c_i, d_i for $i\in\{1,2,3,4\}$ are relatively prime to M, we may clear the denominators to obtain a matrix which is still in $\mathrm{GL}(4, M^{-1}\mathbb{Z})$. Upon clearing denominators we may assume that $a_i, b_i, c_i, d_i \in \mathbb{Z}$ for $i \in \{1,2,3,4\}$. Now we note that the matrix

$$\gamma = \begin{bmatrix} 1 & 0 & M^{-1}y & 0 \\ 0 & 1 & 0 & 0 \\ Mx & 0 & xy+1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is an element of $\mathrm{K}(M)$ for all $x, y \in \mathbb{Z}$. Let $d = \gcd(a_1, b_1)$ and let $d_0 = \gcd(a_1, b_1, M)$. Write $a_1 = md$ and $b_1 = nd$ and note that $\gcd(m, n) = 1$. By Dirichlet's theorem on primes in arithmetic progression we may choose x such that $\gcd(m+nx, M) = 1$. It then follows that $\gcd(a_1+b_1x, M) = d_0$. Pick $y, z \in \mathbb{Z}$ such that $-(a_1 + b_1x)y + zM = b_1$. Then

$$\begin{bmatrix} a_1 & a_2 & M^{-1}b_1 & b_2 \\ Ma_3 & a_4 & b_3 & b_4 \\ Mc_1 & Mc_2 & d_1 & Md_2 \\ Mc_3 & c_4 & d_3 & d_4 \end{bmatrix} \begin{bmatrix} 1 & 0 & M^{-1}y & 0 \\ 0 & 1 & 0 & 0 \\ Mx & 0 & xy+1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is an integral matrix. □

Since $\mathrm{Kl}(M) \subset \mathrm{K}(M)$, by Theorem 4.1.5, we know that every double coset $\mathrm{K}(M)g\mathrm{K}(M)$ with $g \in \mathfrak{s}(M)$ contains an element of the form $\mathrm{diag}(d_1, d_2, e_1, e_2)$ with $d_1|d_2|e_2|e_1$. Moreover, this element is unique by a similar argument for the case of double cosets of the form $\mathrm{Kl}(M)g\mathrm{Kl}(M)$. Let $k \in \mathbb{N}$. We can now define the weight k paramodular Hecke operators in the same way as for the case of the Klingen parabolic subgroup. The paramodular Hecke operators are given by

$$\begin{aligned} T(n) &= n^{k-3} \sum_{g \in \mathrm{K}(M)\backslash \mathfrak{s}_n(M)/\mathrm{K}(M)} [\mathrm{K}(M)g\mathrm{K}(M)]_k \\ &= n^{k-3} \sum_{\substack{d_1,d_2,e_1,e_2 \in \mathbb{N} \\ d_1|d_2|e_2|e_1 \\ d_1e_1 = d_2e_2 = n}} [\mathrm{K}(M)\mathrm{diag}(d_1, d_2, e_1, e_2)\mathrm{K}(M)]_k, \ \ (n, M) = 1, \ \ n \in \mathbb{N}. \end{aligned}$$

The commutativity of these operators follows via a similar argument to that used with the Hecke operators for the Klingen subgroup. This allows us to again restrict our attention to the operators

$$T(p^{r_0}) = p^{r_0(k-3)} \sum_{r_1 \le r_2 \le \lfloor \frac{r_0}{2} \rfloor} \left[\mathrm{K}(M) \begin{bmatrix} p^{r_1} & 0 & 0 & 0 \\ 0 & p^{r_2} & 0 & 0 \\ 0 & 0 & p^{r_0-r_1} & 0 \\ 0 & 0 & 0 & p^{r_0-r_2} \end{bmatrix} \mathrm{K}(M) \right]_k . \qquad (4.1)$$

where p is a prime with $\gcd(p, M) = 1$ and $r_0 \geq 0$.

Like with the Klingen subgroup, the double cosets appearing above can be decomposed into a finite number of right cosets. With such a decomposition we would be able to compute the explicit action of these operators on a Siegel paramodular form. In order to do this we need a complete system of representatives for the double cosets appearing in the formula for $T(p^{r_0})$. The following proposition provides this system of representatives.

Definition 4.2.2. *We let*

$$D_{\alpha,\beta} = \begin{bmatrix} p^\alpha & 0 \\ 0 & p^{\alpha+\beta} \end{bmatrix}$$

where p is a prime, $\alpha, \beta \geq 0$ and $\alpha + \beta \leq r_0$.

Definition 4.2.3. *Let $B, B' \in M(2,\mathbb{Z})$ and $D \in \mathrm{GL}(2,\mathbb{Q}) \cap M(2,\mathbb{Z})$. We say that B and B' are* ***equivalent modulo D*** *if*

$$(B - B')D^{-1} \in M(2,\mathbb{Z}).$$

We also define a special set of matrices.

Definition 4.2.4. *Let $M \geq 1$ be an integer and let p be a prime with $p \nmid M$. For integers $\beta \geq 0$ define the set $R(p^\beta)$ to be a complete system of representatives of the set $\Gamma_0(M)/\Gamma_0(Mp^\beta)$.*

Note that $R(p^\beta)$ has size

$$[\Gamma_0(M) : \Gamma_0(Mp^\beta)] = \frac{[\mathrm{SL}(2,\mathbb{Z}) : \Gamma_0(Mp^\beta)]}{[\mathrm{SL}(2,\mathbb{Z}) : \Gamma_0(M)]} = \frac{Mp^\beta \displaystyle\prod_{q \mid Mp^\beta} \left(1 + \frac{1}{q}\right)}{M \displaystyle\prod_{q \mid M} \left(1 + \frac{1}{q}\right)} = \begin{cases} p^\beta \left(1 + \frac{1}{p}\right) & \text{if } \beta \geq 1, \\ 1 & \text{if } \beta = 0. \end{cases}$$

We will construct an explicit representation of $R(p^\beta)$ shortly. However we first prove a proposition that is critical to computing the action of the Hecke operators on a Siegel paramodular form.

Proposition 4.2.5. *Let $M \geq 1$ and $r_0 \geq 0$ be integers and let p be a prime not dividing M. The set*

$$V(p^{r_0}) = \bigsqcup_{\substack{\alpha,\beta \geq 0 \\ \alpha+\beta \leq r_0}} \left\{ \begin{bmatrix} A & B \\ 0_2 & D \end{bmatrix} \in \mathfrak{s}_{p^{r_0}}(M) : D = D_{\alpha,\beta}({}^tU), U \in R(p^\beta), A = p^{r_0} \cdot {}^tD^{-1}, B \bmod D \right\}$$

is a complete set of representatives of the right cosets contained in the double cosets appearing in equation (4.1).

Proof. Let $g_1, g_2 \in V(p^{r_0})$ such that $\mathrm{K}(M)g_1 = \mathrm{K}(M)g_2$. We will prove that $g_1 = g_2$. According to Lemma 4.1.2 we assume that g_1 and g_2 are of the form

$$g_1 = \begin{bmatrix} A_1 & B_1 \\ 0_2 & D_1 \end{bmatrix} \text{ and } g_2 = \begin{bmatrix} A_2 & B_2 \\ 0_2 & D_2 \end{bmatrix},$$

with

$$D_1 = D_{\alpha_1,\beta_1}{}^t U_1 \text{ and } D_2 = D_{\alpha_2,\beta_2}{}^t U_2.$$

where $U_1, U_2 \in R(p^\beta)$. By definition of the set $V(p^{r_0})$ we have $\alpha_i, \beta_i \geq 0$ and $\alpha_i + \beta_i \leq r_0$ for $i \in \{1, 2\}$. Further we have

$$A_1 = p^{r_0} \cdot {}^t D_1^{-1} \text{ and } A_2 = p^{r_0} \cdot {}^t D_2^{-1}$$

and $B_1, B_2 \in \mathrm{M}(2, \mathbb{Z})$. From the equality $\mathrm{K}(M)g_1 = \mathrm{K}(M)g_2$ we have $g_1 g_2^{-1} \in \mathrm{K}(M)$. Therefore

$$g_1 g_2^{-1} = \begin{bmatrix} A_1 A_2^{-1} & -A_1 A_2^{-1} B_2 D_2^{-1} + B_1 D_2^{-1} \\ 0_2 & D_1 D_2^{-1} \end{bmatrix} \in \mathrm{K}(M).$$

Let $V = A_1 A_2^{-1}$ and $T = -A_1 A_2^{-1} B_2 D_2^{-1} + B_1 D_2^{-1}$. Note that $V \in \mathrm{GL}(2, \mathbb{Z})$ and thus $D_1 D_2^{-1} \in \mathrm{GL}(2, \mathbb{Z})$. However,

$$\begin{aligned} D_1 D_2^{-1} &= D_{\alpha_1,\beta_1}{}^t U_1 {}^t U_2^{-1} D_{\alpha_2,\beta_2}^{-1} \\ &= p^{\alpha_1 - \alpha_2} \begin{bmatrix} a & p^{-\beta_2} b \\ p^{\beta_1} c & p^{\beta_1 - \beta_2} d \end{bmatrix} \end{aligned}$$

where

$${}^t U_1 {}^t U_2^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in {}^t\Gamma_0(M).$$

It follows that $\mathrm{GL}(2, \mathbb{Z}) D_{\alpha_1,\beta_1} \mathrm{GL}(2, \mathbb{Z}) = \mathrm{GL}(2, \mathbb{Z}) D_{\alpha_2,\beta_2} \mathrm{GL}(2, \mathbb{Z})$. By the uniqueness of the Smith normal form (see Theorem 3.2.2) we must have $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$. We write $\alpha = \alpha_1 = \alpha_2$ and $\beta = \beta_1 = \beta_2$. We now have

$$D_1 D_2^{-1} = \begin{bmatrix} a & p^{-\beta} b \\ p^\beta c & d \end{bmatrix}.$$

Since this matrix is in $\mathrm{GL}(2, \mathbb{Z})$ we must have $p^\beta | b$. Since $p \nmid M$ we have that

$$U_2^{-1} U_1 \in \Gamma_0(p^\beta M).$$

This implies that $U_1 = U_2$, $D_1 = D_2$, and $A_1 = A_2$. We write $U = U_1 = U_2$, $A = A_1 = A_2$, and $D = D_1 = D_2$. We thus have

$$T = -B_2D^{-1} + B_1D^{-1} = (B_1 - B_2)D^{-1}.$$

We know that

$$T \in \begin{bmatrix} M^{-1}\mathbb{Z} & \mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{bmatrix}.$$

Furthermore,

$$\begin{aligned} T &= (B_1 - B_2)D^{-1} \\ &= (B_1 - B_2){}^tU^{-1}D_{\alpha,\beta}^{-1} \\ &= \begin{bmatrix} p^{-\alpha}n & * \\ * & * \end{bmatrix} \end{aligned}$$

where $n \in \mathbb{Z}$. Since $p^{-\alpha}n = M^{-1}m$ for some $m \in \mathbb{Z}$ we have $Mn = p^{\alpha}m$ and thus $p^{\alpha}|n$. Thus $T \in \mathrm{M}(2, \mathbb{Z})$ and $B_1 \equiv B_2 \pmod{D}$. This implies that $B_1 = B_2$. Hence $g_1 = g_2$.

We now show that if $\mathrm{K}(M)g$ for $g \in \mathfrak{s}_{p^{r_0}}(M)$ is a left coset contained in one of the double cosets appearing in equation (4.1) then there exists $g' \in V(p^{r_0})$ such that $\mathrm{K}(M)g = \mathrm{K}(M)g'$. By Lemma 4.1.2 there exists a matrix in $\mathrm{K}(M)g$ of the form

$$\begin{bmatrix} a_1 & a_2 & b_1 & b_2 \\ 0 & a_4 & b_3 & b_4 \\ 0 & 0 & d_1 & 0 \\ 0 & 0 & d_3 & d_4 \end{bmatrix}.$$

We may assume that the determinant of

$$D = \begin{bmatrix} d_1 & 0 \\ d_3 & d_4 \end{bmatrix}$$

is positive since $\mathrm{K}(M)$ contains the element

$$\begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Moreover, we have that the determinant of D is a power of p. We put D into Smith normal form and we see that by Lemma 3.2.2

$$D \in \mathrm{SL}(2,\mathbb{Z}) D_{\alpha,\beta} \mathrm{SL}(2,\mathbb{Z})$$

for some $\alpha, \beta \geq 0$ with $\alpha + \beta \leq r_0$. We can actually say something more. In fact,

$$D \in {}^t\Gamma_0(M) D_{\alpha,\beta} {}^t\Gamma_0(M).$$

Since $g \in \mathfrak{s}_{p^{r_0}}(M)$ it follows that $\alpha + \beta \leq r_0$. The double coset

$$ {}^t\Gamma_0(M) D_{\alpha,\beta} {}^t\Gamma_0(M)$$

can be decomposed into a disjoint union of right cosets

$$ {}^t\Gamma_0(M) D_{\alpha,\beta} {}^t\Gamma_0(M) = \bigsqcup_{i=1}^{m} {}^t\Gamma_0(M)\gamma_i.$$

We have that $m = [{}^t\Gamma_0(M) : D_{\alpha,\beta} {}^t\Gamma_0(M) D_{\alpha,\beta}^{-1}] = [{}^t\Gamma_0(M) : {}^t\Gamma_0(Mp^\beta)]$. It is clear that for $U \in R(p^\beta)$ we have

$$ {}^t\Gamma_0(M) D_{\alpha,\beta} {}^tU \subseteq {}^t\Gamma_0(M) D_{\alpha,\beta} {}^t\Gamma_0(M).$$

We proved above that if ${}^t\Gamma_0(M) D_{\alpha,\beta} {}^tU_1 = {}^t\Gamma_0(M) D_{\alpha,\beta} {}^tU_2$ for $U_1, U_2 \in R(p^\beta)$ then $U_1 = U_2$. Therefore $D_{\alpha,\beta} {}^tR(p^\beta)$ can be taken as a complete set of representatives of

$$ {}^t\Gamma_0(M) \backslash {}^t\Gamma_0(M) D_{\alpha,\beta} {}^t\Gamma_0(M).$$

Now we have $D = D_{\alpha,\beta} {}^tU$ for some $U \in R(p^\beta)$. It follows from properties of $\mathrm{GSp}(4,\mathbb{R})$ that $A = p^{r_0} \cdot {}^tD^{-1}$. Lastly we multiply on the left by a matrix of the form

$$\begin{bmatrix} E_2 & T \\ 0_2 & E_2 \end{bmatrix} \in \mathrm{K}(M)$$

with $T \in \mathrm{M}(2,\mathbb{Z})$ to get

$$\begin{bmatrix} E_2 & T \\ 0_2 & E_2 \end{bmatrix} \begin{bmatrix} A & B \\ 0_2 & D \end{bmatrix} = \begin{bmatrix} A & B + TD \\ 0_2 & D \end{bmatrix}$$

thereby allowing us to reduce $B \pmod{D}$. This completes the proof. □

The next result describes $R(p^\beta)$ explicitly. Note first that $R(p^0)$ consists of just I_1, the 2×2 identity matrix.

Lemma 4.2.6. *Let $M \geq 1$ be an integer and let p be a prime not dividing M. For each $\beta \geq 1$ fix a matrix*

$$\begin{bmatrix} p^\beta & -a_\beta \\ M & b_\beta \end{bmatrix}$$

where $a_\beta, b_\beta \in \mathbb{Z}$ are such that $a_\beta M + b_\beta p^\beta = 1$. For $\beta \geq 1$, the following form a complete set of representatives of $\Gamma_0(M)/\Gamma_0(Mp^\beta)$

$$\begin{bmatrix} 1 & \\ Mu & 1 \end{bmatrix}, \quad u \in \mathbb{Z}/p^\beta\mathbb{Z},$$

$$\begin{bmatrix} Mup + p^\beta & upb_\beta - a_\beta \\ M & b_\beta \end{bmatrix}, \quad u \in \mathbb{Z}/p^{\beta-1}\mathbb{Z}.$$

Proof. Let R be the set including the elements defined above. As $\#R = \#R(p^\beta)$, it suffices to show that each element defines a distinct left coset. First we note that two matrices

$$\begin{bmatrix} v_1 & v_2 \\ v_3 & v_4 \end{bmatrix}, \begin{bmatrix} v_1' & v_2' \\ v_3' & v_4' \end{bmatrix}$$

define the same left coset if and only if there exists

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(Mp^\beta)$$

such that

$$\begin{bmatrix} v_1 & v_2 \\ v_3 & v_4 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} v_1' & v_2' \\ v_3' & v_4' \end{bmatrix}.$$

Note that this last equality says

$$av_1 + cv_2 = v_1',$$

$$av_3 + cv_4 = v_3'.$$

Hence there exists $a \in (\mathbb{Z}/p^\beta\mathbb{Z})^\times$ such that

$$av_1 \equiv v_1' \pmod{p^\beta},$$

$$av_3 \equiv v_3' \pmod{p^\beta}.$$

The existence of such an a is also a sufficient condition so we can conclude that the matrices

$$\begin{bmatrix} v_1 & v_2 \\ v_3 & v_4 \end{bmatrix}, \begin{bmatrix} v_1' & v_2' \\ v_3' & v_4' \end{bmatrix}$$

define the same left coset if and only if there exists $a \in (\mathbb{Z}/p^\beta\mathbb{Z})^\times$ such that

$$av_1 \equiv v_1' \pmod{p^\beta},$$
$$av_3 \equiv v_3' \pmod{p^\beta}.$$

We prove the claim bearing this in mind. If $(1, u_1M)$ and $(1, u_2M)$ are equivalent modulo p^β then there exists $a \in (\mathbb{Z}/p^\beta\mathbb{Z})^\times$ such that

$$a \equiv 1 \pmod{p^\beta} \text{ and } au_1M \equiv u_2M \pmod{p^\beta}.$$

This implies that $u_1M \equiv u_2M \pmod{p^\beta}$ and therefore $u_1 \equiv u_2 \pmod{p^\beta}$. If $(Mu_1p + p^\beta, M)$ and $(Mu_2p + p^\beta, M)$ are equivalent modulo p^β then there exists $a' \in (\mathbb{Z}/p^\beta\mathbb{Z})^\times$ such that

$$a'(Mu_1p + p^\beta) \equiv Mu_2p + p^\beta \pmod{p^\beta} \text{ and } a'M \equiv M \pmod{p^\beta}.$$

This implies that $a' \equiv 1 \pmod{p^\beta}$ and therefore $u_1p \equiv u_2p \pmod{p^\beta}$. Hence it follows that $u_1 \equiv u_2 \pmod{p^{\beta-1}}$. If $(1, u_1M)$ and $(Mu_2p + p^\beta, M)$ are equivalent modulo p^β then there exists $a'' \in (\mathbb{Z}/p^\beta\mathbb{Z})^\times$ such that

$$a'' \equiv Mu_2p + p^\beta \pmod{p^\beta} \text{ and } a''u_1M \equiv M \pmod{p^\beta}.$$

This implies that $Mu_1u_2p \equiv 1 \pmod{p^\beta}$. This is of course a contradiction and thus $(1, u_1M)$ and $(Mu_2p + p^\beta, M)$ are not equivalent modulo p^β. The proof is complete. □

By Proposition 4.2.5, we can now easily apply the operator $T(p^{r_0})$, $r_0 \geq 0$, to a Siegel paramodular form. We will not use the explicit representation of $R(p^\beta)$ here but we will be returning to that description later when we start our analysis of Fourier coefficients of paramodular forms.

4.3 Hecke Operators over $\mathrm{K}(M)$, $p|M$

For this section we assume that $M \geq 1$ is a squarefree integer. In order to build the Hecke operators for primes $p|M$ we will utilize the constructions in [34] and modify them as in [39].

Definition 4.3.1. *The* ***local paramodular group of level*** $\mathbf{p^{r_0}}$*, denoted by* $\mathrm{K}^{\mathrm{loc}}(p^{r_0})$*, consists of elements*

$$g \in \mathrm{GSp}(4, \mathbb{Q}_p) \cap \begin{bmatrix} \mathbb{Z}_p & \mathbb{Z}_p & p^{-r_0}\mathbb{Z}_p & \mathbb{Z}_p \\ p^{r_0}\mathbb{Z}_p & \mathbb{Z}_p & \mathbb{Z}_p & \mathbb{Z}_p \\ p^{r_0}\mathbb{Z}_p & p^{r_0}\mathbb{Z}_p & \mathbb{Z}_p & p^{r_0}\mathbb{Z}_p \\ p^{r_0}\mathbb{Z}_p & \mathbb{Z}_p & \mathbb{Z}_p & \mathbb{Z}_p \end{bmatrix}$$

with $\lambda(g) \in \mathbb{Z}_p^\times$*.*

We will only be studying the Hecke operators $T(p)$ and

$$T_1(p^2) = \mathrm{K}(M) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{bmatrix} \mathrm{K}(M)$$

in the case $p|M$.

Proposition 4.3.2. *We have the following double coset decompositions for $r_0 \geq 1$,*

$$\mathrm{K}^{\mathrm{loc}}(p^{r_0}) \begin{bmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p^{r_0}) = \bigsqcup_{x,y,z \in \mathbb{Z}/p\mathbb{Z}} \begin{bmatrix} 1 & 0 & zp^{-r_0} & y \\ 0 & 1 & y & x \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p^{r_0})$$

$$\sqcup \bigsqcup_{x,z \in \mathbb{Z}/p\mathbb{Z}} \begin{bmatrix} 1 & x & zp^{-r_0} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -x & 0 \end{bmatrix} \begin{bmatrix} p & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & p \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p^{r_0})$$

$$\sqcup \bigsqcup_{x,y \in \mathbb{Z}/p\mathbb{Z}} t_{p^{r_0}} \begin{bmatrix} 1 & 0 & 0 & y \\ 0 & 1 & y & x \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p^{r_0})$$

$$\sqcup \bigsqcup_{x \in \mathbb{Z}/p\mathbb{Z}} t_{p^{r_0}} \begin{bmatrix} 1 & x & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -x & 1 \end{bmatrix} \begin{bmatrix} p & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & p \end{bmatrix},$$

$$\mathrm{K}^{\mathrm{loc}}(p^{r_0}) \begin{bmatrix} p^2 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & p \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p^{r_0}) = \bigsqcup_{\substack{x,y \in \mathbb{Z}/p\mathbb{Z} \\ z \in \mathbb{Z}/p^2\mathbb{Z}}} \begin{bmatrix} 1 & x & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -x & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & zp^{-r_0} & y \\ 0 & 1 & y & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} p^2 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & p \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p^{r_0})$$

$$\sqcup \bigsqcup_{x,y,z \in \mathbb{Z}/p\mathbb{Z}} t_{p^{r_0}} \begin{bmatrix} 1 & x & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -x & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & zp^{-r_0+1} & y \\ 0 & 1 & y & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} p^2 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & p \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p^{r_0}).$$

Proof. The proof can be found in Chapter 6 of [34]. One just needs to apply the appropriate involution on the paramodular group used therein to obtain appropriate decompositions. □

The major difficulty in utilizing these double coset decompositions is the fact that the lower left block of some of the representatives contain non-zero elements. The rest of this section is to rectify this issue. We note that since M is assumed to be squarefree we have $r_0 = 1$ and can appeal to the following theorem.

Theorem 4.3.3 (Iwasawa Decomposition)**.** *Let p be a prime. For any $g \in \mathrm{GSp}(4, \mathbb{Q}_p)$ there exists $h \in \mathrm{K}^{\mathrm{loc}}(p)$ such that gh is of the form*

$$\begin{bmatrix} A & B \\ 0_2 & D \end{bmatrix}$$

where $A, B, D \in M(2, \mathbb{Q}_p)$.

Proof. This is Proposition 5.1.2 in [34]. □

With the previous theorem in mind we can put all the representatives appearing in Proposition 4.3.2 into block upper triangular form which will make them very easy to compute with later. In addition, we will use the following theorem from [19] to globalize the coset representatives in the case $r_0 = 1$.

Theorem 4.3.4. *Let $M \geq 1$ be an integer, let p be a prime, and let $p^{r_0} || M$. There exists finite disjoint decompositions*

$$\mathrm{K}^{\mathrm{loc}}(p^{r_0}) \begin{bmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p^{r_0}) = \bigsqcup_{i=1}^{N_1} g_i \mathrm{K}^{\mathrm{loc}}(p^{r_0})$$

and

$$\mathrm{K}^{\mathrm{loc}}(p^{r_0}) \begin{bmatrix} p^2 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & p \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p^{r_0}) = \bigsqcup_{j=1}^{N_2} h_j \mathrm{K}^{\mathrm{loc}}(p^{r_0})$$

such that

$$\mathrm{K}(M)\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&p&0\\0&0&0&p\end{bmatrix}\mathrm{K}(M)=\bigsqcup_{i=1}^{N_1}\mathrm{K}(M)pg_i^{-1}$$

and

$$\mathrm{K}(M)\begin{bmatrix}1&0&0&0\\0&p&0&0\\0&0&p^2&0\\0&0&0&p\end{bmatrix}\mathrm{K}(M)=\bigsqcup_{j=1}^{N_2}\mathrm{K}(M)p^2h_j^{-1}.$$

The representatives $\{g_i\}_{i=1}^{N_1}$ *and* $\{h_j\}_{j=1}^{N_2}$ *are constructed from Proposition 4.3.2.*

The rest of this section is to prove the previous theorem in the case $r_0 = 1$ while simultaneously providing a set of coset representatives with a lower left block of zeroes. We provide a set of lemmas which will give us a desirable set of representatives. Ultimately we need only fix those coset representatives which have a t_p appearing in them. We fix those by shifting the element t_p to the right and absorbing it into the local paramodular group. We have

$$t_p\begin{bmatrix}1&0&0&y\\0&1&y&x\\0&0&1&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}p&0&0&0\\0&p&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\mathrm{K}^{\mathrm{loc}}(p)=\begin{bmatrix}1&0&0&0\\-yp&1&0&x\\0&0&1&yp\\0&0&0&1\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&p&0&0\\0&0&p&0\\0&0&0&1\end{bmatrix}\mathrm{K}^{\mathrm{loc}}(p),$$

$$t_p\begin{bmatrix}1&x&0&0\\0&1&0&0\\0&0&1&0\\0&0&-x&1\end{bmatrix}\begin{bmatrix}p&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&p\end{bmatrix}\mathrm{K}^{\mathrm{loc}}(p)=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&xp&1&0\\xp&0&0&1\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&p&0\\0&0&0&p\end{bmatrix}\mathrm{K}^{\mathrm{loc}}(p),$$

and

$$t_p\begin{bmatrix}1&x&0&0\\0&1&0&0\\0&0&1&0\\0&0&-x&1\end{bmatrix}\begin{bmatrix}1&0&z&y\\0&1&y&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}p^2&0&0&0\\0&p&0&0\\0&0&1&0\\0&0&0&p\end{bmatrix}\mathrm{K}^{\mathrm{loc}}(p)=A\mathrm{K}^{\mathrm{loc}}(p)$$

with

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & xp & 1 & 0 \\ xp & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ -yp & 1 & 0 & 0 \\ -zp^2 & 0 & 1 & yp \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{bmatrix}.$$

We further note that if $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ we have

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & xp & 1 & 0 \\ xp & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & x^{-1}p^{-1} \\ 0 & 1 & x^{-1}p^{-1} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ p & 0 & 0 & 0 \\ 0 & 0 & 0 & p \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & -x^{-1}p^{-1} & 0 \\ 0 & 0 & 0 & -x^{-1} \\ xp & 0 & 0 & p \\ 0 & x & 1 & 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & xp & 1 & 0 \\ xp & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & x^{-1}p^{-1} \\ 0 & 1 & x^{-1}p^{-1} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ p^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & p^2 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & -x^{-1}p^{-1} & 0 \\ 0 & 0 & 0 & -x^{-1} \\ xp & 0 & 0 & p \\ 0 & x & 1 & 0 \end{bmatrix}$$

where the last matrix on the right of each formula is an element of $\mathrm{K}^{\mathrm{loc}}(p)$. The proofs of the following lemmas are all straightforward computations.

Lemma 4.3.5. *Let $n \geq 1$ and $M \geq 1$ be integers. Let N be such that*

$$\frac{MN}{p} \equiv 1 \pmod{p}.$$

Then

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ p^n & 0 & 0 & 0 \\ 0 & 0 & 0 & p^n \\ 0 & 0 & 1 & 0 \end{bmatrix} \in \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & p^n & 0 & 0 \\ 0 & 0 & -p^n & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ MNp^{-1} & 1 & 0 & 0 \\ 0 & 0 & 1 & -MNp^{-1} \\ 0 & 0 & 0 & 1 \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p).$$

Lemma 4.3.6. *Let $n \geq 1$ be an integer. Then*

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ wp^{n+1} & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{bmatrix} = p \begin{bmatrix} 1 & 0 & w^{-1}z^{-n+1} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} t_{p^n} \begin{bmatrix} 1 & 0 & wp^{-n+1} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} w & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & w^{-1} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Lemma 4.3.7. *Let p be a prime dividing $M \geq 1$. Let $x, y \in \mathbb{Z}/p\mathbb{Z}$ and let N be such that*

$$\frac{MN}{p} \equiv 1 \pmod{p}.$$

Then we have the following equivalence of cosets,

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -yp & 1 & 0 & x \\ 0 & 0 & 1 & yp \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p) = A_1 \mathrm{K}^{\mathrm{loc}}(p).$$

with

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -yMN & 1 & 0 & x \\ 0 & 0 & 1 & yMN \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Lemma 4.3.8. *Let p be a prime dividing $M \geq 1$. Let $x, y \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ be such that*

$$xy \equiv 1 \pmod{p}.$$

Let N be such that

$$\frac{MN}{p} \equiv 1 \ (mod\ p).$$

Then we have the following equivalence of cosets,

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & xp & 1 & 0 \\ xp & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p) = A_2 \mathrm{K}^{\mathrm{loc}}(p).$$

with

$$A_2 = \begin{bmatrix} 1 & 0 & 0 & yp^{-1} \\ 0 & 1 & yp^{-1} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} (MN-p)p^{-1} & 1 & 0 & 0 \\ MN & p & 0 & 0 \\ 0 & 0 & -p & MN \\ 0 & 0 & 1 & (-MN+p)p^{-1} \end{bmatrix}$$

Lemma 4.3.9. *Let p be a prime dividing $M \geq 1$. Let $x, y, z \in \mathbb{Z}/p\mathbb{Z}$ and let $w \in \mathbb{Z}/p\mathbb{Z}$ be such that*

$$w \equiv -(z + 2xy) \ (mod\ \ell).$$

Then we have the following equivalence of cosets,

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & xp & 1 & \\ xp & & & 1 \end{bmatrix}\begin{bmatrix} 1 & & & \\ -yp & 1 & & \\ -zp^2 & & 1 & yp \\ & & & 1 \end{bmatrix}\begin{bmatrix} 1 & & & \\ & p & & \\ & & p^2 & \\ & & & p \end{bmatrix}\mathrm{K}^{\mathrm{loc}}(p) = A_3\mathrm{K}^{\mathrm{loc}}(p).$$

with

$$A_3 = \begin{bmatrix} 1 & & & \\ -yp & 1 & & \\ & & 1 & yp \\ & & & 1 \end{bmatrix}\begin{bmatrix} 1 & & & \\ & 1 & & \\ wp^2 & xp & 1 & \\ xp & & & 1 \end{bmatrix}\begin{bmatrix} 1 & & & \\ & p & & \\ & & p^2 & \\ & & & p \end{bmatrix}$$

Lemma 4.3.10. *Let p be a prime dividing $M \geq 1$. Let $y \in \mathbb{Z}/p\mathbb{Z}$ and let N be such that*

$$\frac{MN}{p} \equiv 1 \pmod{p}.$$

Then we have the following equivalence of cosets,

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -yp & 1 & 0 & 0 \\ 0 & 0 & 1 & yp \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{bmatrix}\mathrm{K}^{\mathrm{loc}}(p) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -yMN & 1 & 0 & 0 \\ 0 & 0 & 1 & yMN \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{bmatrix}\mathrm{K}^{\mathrm{loc}}(p).$$

Lemma 4.3.11. *Let p be a prime dividing $M \geq 1$. Let $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, $y \in \mathbb{Z}/p\mathbb{Z}$, and let $w \in (\mathbb{Z}/p\mathbb{Z})^\times$ be such that*

$$xw \equiv 1 \pmod{p},$$

and let N be such that

$$\frac{MN}{p} \equiv 1 \pmod{p}.$$

Then we have the following equivalence of cosets,

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -yp & 1 & 0 & 0 \\ 0 & 0 & 1 & yp \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & xp & 1 & 0 \\ xp & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{bmatrix}\mathrm{K}^{\mathrm{loc}}(p) = A_4\mathrm{K}^{\mathrm{loc}}(p)$$

where A_4 is the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -yMN & 1 & 0 & 0 \\ 0 & 0 & 1 & yMN \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & wp^{-1} \\ 0 & 1 & wp^{-1} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} (MN-p)p^{-1} & 1 & 0 & 0 \\ MNp & p^2 & 0 & 0 \\ 0 & 0 & -p^2 & MNp \\ 0 & 0 & 1 & (-MN+p)p^{-1} \end{bmatrix}.$$

Lemma 4.3.12. *Let p be a prime dividing $M \geq 1$. Let $x, y \in \mathbb{Z}/p\mathbb{Z}$, let $w \in (\mathbb{Z}/p\mathbb{Z})^\times$, and let N be such that*

$$\frac{MN}{p} \equiv 1 \pmod{p}.$$

In addition, let $s \in (\mathbb{Z}/p\mathbb{Z})^\times$ be such that

$$ws \equiv 1 \pmod{p},$$

and let $t \in \mathbb{Z}/p\mathbb{Z}$ be such that

$$t \equiv xs \pmod{p}.$$

Then we have the following equivalence of cosets,

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -yp & 1 & 0 & 0 \\ 0 & 0 & 1 & yp \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ wp^2 & xp & 1 & 0 \\ xp & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{bmatrix} \mathrm{K}^{\mathrm{loc}}(p) = A_5 \mathrm{K}^{\mathrm{loc}}(p)$$

where

$$A_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -yMN & 1 & 0 & 0 \\ 0 & 0 & 1 & yMN \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -tp^{-1} & sp^{-2} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & tp^{-1} & 1 \end{bmatrix} \begin{bmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{bmatrix}.$$

Putting all the lemmas together we obtain the following theorem.

Theorem 4.3.13. *Let p be a prime dividing $M \geq 1$ exactly once, i.e., $p||M$. Let N be an inverse* *of M/p modulo p. We have the following double coset decompositions,*

$$\mathrm{K}(M)\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&p&0\\0&0&0&p\end{bmatrix}\mathrm{K}(M)=\bigsqcup_{x,y,z\in\mathbb{Z}/p\mathbb{Z}}\mathrm{K}(M)\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&p&0\\0&0&0&p\end{bmatrix}\begin{bmatrix}1&0&-zp^{-1}&-y\\0&1&-y&-x\\0&0&1&0\\0&0&0&1\end{bmatrix}$$

$$\sqcup\bigsqcup_{x,z\in\mathbb{Z}/p\mathbb{Z}}\mathrm{K}(M)\begin{bmatrix}1&0&0&0\\0&p&0&0\\0&0&p&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}1&-x&-zp^{-1}&0\\0&1&0&0\\0&0&1&0\\0&0&x&1\end{bmatrix}$$

$$\sqcup\bigsqcup_{x,y\in\mathbb{Z}/p\mathbb{Z}}\mathrm{K}(M)\begin{bmatrix}p&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&p\end{bmatrix}\begin{bmatrix}1&0&0&0\\yMN&1&0&x\\0&0&1&-yMN\\0&0&0&1\end{bmatrix}$$

$$\sqcup\bigsqcup_{x\in(\mathbb{Z}/p\mathbb{Z})^\times}\mathrm{K}(M)\begin{bmatrix}-p&1&0&0\\MN&(-MN+p)p^{-1}&0&0\\0&0&(MN-p)p^{-1}&MN\\0&0&1&p\end{bmatrix}\begin{bmatrix}1&0&0&-xp^{-1}\\0&1&-xp^{-1}&0\\0&0&1&0\\0&0&0&1\end{bmatrix}$$

$$\sqcup\,\mathrm{K}(M)\begin{bmatrix}p&0&0&0\\0&p&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}$$

$$\mathrm{K}(M)\begin{bmatrix}1&0&0&0\\0&p&0&0\\0&0&p^2&0\\0&0&0&p\end{bmatrix}\mathrm{K}(M)=\bigsqcup_{\substack{x,y\in\mathbb{Z}/p\mathbb{Z}\\z\in\mathbb{Z}/p^2\mathbb{Z}}}\mathrm{K}(M)\begin{bmatrix}1&0&0&0\\0&p&0&0\\0&0&p^2&0\\0&0&0&p\end{bmatrix}\begin{bmatrix}1&0&-zp^{-1}&-y\\0&1&-y&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}1&-x&0&0\\0&1&0&0\\0&0&1&0\\0&0&x&1\end{bmatrix}$$

$$\sqcup\bigsqcup_{y\in\mathbb{Z}/p\mathbb{Z}}\mathrm{K}(M)\begin{bmatrix}p^2&0&0&0\\0&p&0&0\\0&0&1&0\\0&0&0&p\end{bmatrix}\begin{bmatrix}1&0&0&0\\yMN&1&0&0\\0&0&1&-yMN\\0&0&0&1\end{bmatrix}$$

$$\sqcup\bigsqcup_{\substack{y\in\mathbb{Z}/p\mathbb{Z}\\x\in(\mathbb{Z}/p\mathbb{Z})^\times}}\mathrm{K}(M)\begin{bmatrix}-p^2&1&-xp^{-1}&xp\\MNp&(-MN+p)p^{-1}&x(MN-p)p^{-2}&-xMN\\0&0&(MN-p)p^{-1}&MNp\\0&0&1&p^2\end{bmatrix}\begin{bmatrix}1&0&0&0\\yMN&1&0&0\\0&0&1&-yMN\\0&0&0&1\end{bmatrix}$$

$$\sqcup\bigsqcup_{\substack{x,y\in\mathbb{Z}/p\mathbb{Z}\\z\in(\mathbb{Z}/p\mathbb{Z})^\times}}\mathrm{K}(M)\begin{bmatrix}p&0&0&0\\0&p&0&0\\0&0&p&0\\0&0&0&p\end{bmatrix}\begin{bmatrix}1&xp^{-1}&-zp^{-2}&0\\0&1&0&0\\0&0&1&0\\0&0&-xp^{-1}&1\end{bmatrix}\begin{bmatrix}1&0&0&0\\yMN&1&0&0\\0&0&1&-yMN\\0&0&0&1\end{bmatrix}$$

Proof. Starting with the decompositions in Proposition 4.3.2 and taking $r_0 = 1$ we implement the previous lemmas to obtain a new set of representatives of the double cosets

$$\mathrm{K}^{\mathrm{loc}}(p)\begin{bmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\mathrm{K}^{\mathrm{loc}}(p)$$

and

$$\mathrm{K}^{\mathrm{loc}}(p)\begin{bmatrix} p^2 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & p \end{bmatrix}\mathrm{K}^{\mathrm{loc}}(p).$$

The theorem now follows from Theorem 4.3.4. $\square$

5 Full Modules in Quadratic Fields

In this section we discuss the theory of full modules in quadratic fields and their correspondence with binary quadratic forms.

5.1 Full Modules

Let $\delta_0 \neq 0, 1$ be a squarefree integer and let $K = \mathbb{Q}(\sqrt{\delta_0})$. The discriminant of the field K coincides with the discriminant of the ring of integers of K which we will denote by $\mathfrak{o}_K$. This discriminant is equal to δ_0 if $\delta_0 \equiv 1 \pmod 4$ and is equal to $4\delta_0$ if $\delta_0 \equiv 2, 3 \pmod 4$.

Definition 5.1.1. *Let δ be an integer. We say δ is a* ***fundamental discriminant*** *if $\delta \equiv 1 \pmod 4$ and δ squarefree or $\delta = 4\delta_0$ with $\delta_0 \equiv 2, 3 \pmod 4$ and δ_0 squarefree.*

Let $K = \mathbb{Q}(\sqrt{\delta})$ be a quadratic field with fundamental discriminant δ. By a module G in K we mean a $\mathbb{Z}$-submodule of K of rank 0, 1, or 2. We say a module of K is **full** if $K = \mathbb{Q}G$. Note that this implies that G has rank 2. For the remainder of this work we will work strictly with full modules.

Definition 5.1.2. *A set of generators $\{\omega_1, \omega_2\}$ of the module G is called a* ***basis*** *of G if*

$$a_1\omega_1 + a_2\omega_2 = 0, \ a_1, a_2 \in \mathbb{Z}$$

implies that $a_1 = a_2 = 0$.

Proposition 5.1.3. *Let G be a full module in K and let $\{\omega_1, \omega_2\}$ be a basis for G. Let $\{\omega_1', \omega_2'\}$ be such that*

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \gamma \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

for some $\gamma \in \mathrm{GL}(2, \mathbb{Z})$. Then $\{\omega_1', \omega_2'\}$ is also a basis for G.

Proof. Consider the equality

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \gamma \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

with $\gamma \in \mathrm{GL}(2, \mathbb{Z})$ and write

$$\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Then

$$\omega_1' = a\omega_1 + b\omega_2$$
$$\omega_2' = c\omega_1 + d\omega_2$$

Now assume that

$$a_1\omega_1' + a_2\omega_2' = 0.$$

for some $a_1, a_2 \in \mathbb{Z}$. Then

$$a_1(a\omega_1 + b\omega) + a_2(c\omega_1 + d\omega_2) = 0$$

and therefore

$$(a_1a + a_2c)\omega_1 + (a_1b + a_2d)\omega_2 = 0.$$

Since $\{\omega_1, \omega_2\}$ is a basis for G we must have

$$a_1a + a_2c = 0,$$
$$a_1b + a_2d = 0.$$

Solving this system yields $a_1 = a_2 = 0$. As $\gamma \in \mathrm{GL}(2, \mathbb{Z})$, the elements ω_1' and ω_2' is a set of generators of G. Thus $\{\omega_1', \omega_2'\}$ is a basis for G. □

Any full module in K has a basis $\{\omega_1, \omega_2\}$. It is immediate that any element $\alpha \in G$ can be written uniquely in the form

$$\alpha = c_1\omega_1 + c_2\omega_2,\ \ c_1, c_2 \in \mathbb{Z}.$$

Definition 5.1.4. *Let G be a full module in K and let $\{\omega_1, \omega_2\}$ be a basis of G. If we have*

$$\frac{1}{i^{(1-sgn(\delta))/2}}\det\begin{bmatrix} \omega_1 & \omega_2 \\ \overline{\omega_1} & \overline{\omega_2} \end{bmatrix} > 0 \tag{5.1}$$

where $\overline{\omega_i}$ represents the Galois conjugate of ω_i then we say that the basis is ***ordered****.*

It is clear that if $\{\omega_1, \omega_2\}$ is basis of a full module G in K which is not ordered then exchanging ω_1 and ω_2 creates an ordered basis. Note that Proposition 5.1.3 implies that if two ordered bases differ by a matrix in $\mathrm{GL}(2, \mathbb{Z})$ then they actually differ by a matrix in $\mathrm{SL}(2, \mathbb{Z})$.

Definition 5.1.5. *A full module G in K which contains 1 and is a subring of $\mathfrak{o}_K$ is called an* ***order*** *of K. The* ***discriminant*** *of an order, denoted by $\mathrm{disc}(G)$, is defined to be*

$$\mathrm{disc}(G) = \mathrm{disc}(\mathfrak{o}_K)[\mathfrak{o}_K : G]^2.$$

Proposition 5.1.6. *Let G be an order of $K = \mathbb{Q}(\sqrt{\delta})$ where δ is a fundamental discriminant. Let $\mathfrak{o}_f \subset K$ be the full module with basis $\{1, f\omega\}$ where $f \in \mathbb{N}$ and*

$$\omega = \begin{cases} \frac{1+\sqrt{\delta_0}}{2} & \text{if } \delta \equiv 1 \pmod 4, \\ \sqrt{\delta_0} & \text{if } \delta \equiv 0 \pmod 4. \end{cases}$$

Note that $\mathfrak{o}_K = \mathfrak{o}_1$. Then

(i) $G = \mathfrak{o}_{[\mathfrak{o}_K:G]}$,

(ii) and the discriminant of G is δf^2.

Proof. Since $G \subset \mathfrak{o}_K$ we have for $\alpha \in G$ that there exists $a, b \in \mathbb{Z}$ such that

$$\alpha = a + b\omega.$$

Since $1 \in G$ we have that $-a \in G$ and hence $b\omega \in G$. Let f be the smallest positive integer such that $f\omega \in G$. Write

$$b = fq + r$$

for $q, r \in \mathbb{N}$ with $0 \leq r < f$. Then $\alpha - a - fq\omega = r\omega \in G$. By the minimality of f we must have $r = 0$. Hence $f|b$ and therefore $\alpha \in \mathfrak{o}_f$. Hence $G \subseteq \mathfrak{o}_f$. The other inclusion is obvious and so we can conclude that $G = \mathfrak{o}_f$. This proves (i) since $f = [\mathfrak{o}_K : G]$. We now prove (ii). We have

$$\begin{aligned} \mathrm{disc}(G) &= \mathrm{disc}(\mathfrak{o}_K)[\mathfrak{o}_K : G]^2 \\ &= \delta f^2 \end{aligned}$$

This completes the proof. ∎

For $f \in \mathbb{N}$, we are going to need an ordered basis for $\mathfrak{o}_f$. We'll take

$$\begin{cases} \left\{1, \dfrac{f - f\sqrt{\delta}}{2}\right\} & \text{if } \delta \equiv 1 \pmod 4 \\ \left\{1, -\dfrac{f\sqrt{\delta}}{2}\right\} & \text{if } \delta \equiv 0 \pmod 4 \end{cases}$$

to be our desired ordered basis.

Definition 5.1.7. *Let G be a full module in K. The ring*

$$\mathfrak{o}_G = \{\alpha \in K : \alpha G \subseteq G\}$$

is called the ***ring of coefficients*** *of the module G.*

Proposition 5.1.8. *For a full module G in K, the ring $\mathfrak{o}_G$ is an order of K.*

Proof. Let G be a full module in K and let $\mathfrak{o}_G$ be the ring of coefficients of G. For $\beta \in G$ we have $\beta\mathfrak{o}_G \subseteq G$. As $\beta\mathfrak{o}_G$ is a group under addition we have that $\beta\mathfrak{o}_G$ is a module in K. It then follows that $\mathfrak{o}_G$ is a module in K. We show that $\mathfrak{o}_G$ is a full module. To prove this we need to show that $\mathfrak{o}_G$ is of rank 2. Let γ be an arbitrary element of K and let $\{\omega_1, \omega_2\}$ be a basis of G. Write

$$\gamma\omega_1 = a_1\omega_1 + a_2\omega_2,$$

$$\gamma\omega_2 = b_1\omega_1 + b_2\omega_2,$$

where $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. Multiply each equation by the least common multiple l of the denominators of a_1, a_2, b_1,and b_2. Then it follows that $l\gamma \in \mathfrak{o}_G$. This is true for any element in K. Thus taking any two linearly independent elements of K we obtain linearly independent elements in $\mathfrak{o}_G$. Thus $\mathfrak{o}_G$ must be of rank 2. This completes the proof of the claim. □

Definition 5.1.9. *Let G be a full module in K and let $\mathfrak{o}_G$ be the ring of coefficients of G. Let*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

be the matrix which transforms a basis of $\mathfrak{o}_G$ to a basis of G. The ***norm of G*** *is defined to be $|ad - bc|$ and will be denoted by $N(G)$. For an element $\alpha \in G$, we define the* ***norm of $\boldsymbol{\alpha}$*** *to be $\alpha\overline{\alpha}$.*

Definition 5.1.10. *Let G be a full module in K with ring of coefficients $\mathfrak{o}_G$. Then the* ***discriminant of G*** *is given as the discriminant of $\mathfrak{o}_G$.*

The following proposition allows us to express the norm of a full module in K in terms of the basis of G.

Proposition 5.1.11. *Let G be a full module in K with ring of coefficients $\mathfrak{o}_f$ and ordered basis $\{\omega_1, \omega_2\}$. Let $a, b, c, d \in \mathbb{Q}$ be such that*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ \omega \end{bmatrix} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}.$$

where ω is given as in Proposition 5.1.6. Then

$$N(G)f = bc - ad,$$

Proof. Write $\omega_1 = a + b\omega$ and $\omega_2 = c + d\omega$. The transition matrix from $\mathfrak{o}_f$ to G is

$$\begin{bmatrix} a & b/f \\ c & d/f \end{bmatrix}.$$

Then, by definition,

$$N(G) = \left| \det \begin{bmatrix} a & b/f \\ c & d/f \end{bmatrix} \right| = \frac{|ad - bc|}{f} = \frac{bc - ad}{f}$$

since $bc - ad > 0$ by equation (5.1). This completes the proof. □

As a result of the previous proposition we now have a test to determine if two elements of G actually form a basis of G.

Corollary 5.1.12. *Let $\omega_1, \omega_2 \in G$ satisfy (5.1). Then $\{\omega_1, \omega_2\}$ forms an ordered basis for G if and only if*

$$\frac{1}{f\sqrt{\delta}N(G)} \det \begin{bmatrix} \omega_1 & \omega_2 \\ \overline{\omega_1} & \overline{\omega_2} \end{bmatrix} = 1.$$

Proof. Assume that $\{\omega_1, \omega_2\}$ forms an ordered basis of G and write $\omega_1 = a + b\omega$ and $\omega_2 = c + d\omega$. Thus, by proposition 6.3.3,

$$\begin{aligned} \frac{1}{f\sqrt{\delta}N(G)} \det \begin{bmatrix} \omega_1 & \omega_2 \\ \overline{\omega_1} & \overline{\omega_2} \end{bmatrix} &= \frac{1}{(bc - ad)\sqrt{\delta}} \det \begin{bmatrix} a + b\omega & c + d\omega \\ a + b\overline{\omega} & c + d\overline{\omega} \end{bmatrix} \\ &= \frac{1}{(bc - ad)\sqrt{\delta}}((a + b\omega)(c + d\overline{\omega}) - (a + b\overline{\omega})(c + d\omega)) \\ &= \frac{1}{(bc - ad)\sqrt{\delta}}((ad - bc)(\overline{\omega} - \omega)) \\ &= 1, \end{aligned}$$

since $\overline{\omega} - \omega = -2^{1-\epsilon}\sqrt{\delta_0} = -\sqrt{\delta}$ where $\delta \equiv \epsilon \pmod 4$. Now assume that

$$\frac{1}{f\sqrt{\delta}N(G)} \det \begin{bmatrix} \omega_1 & \omega_2 \\ \overline{\omega_1} & \overline{\omega_2} \end{bmatrix} = 1.$$

Fix an ordered basis $\{\zeta_1, \zeta_2\}$ of G and expand ω_1 and ω_2 in terms of this basis,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \zeta_1 \\ \zeta_2 \end{bmatrix} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

Thus

$$\begin{aligned} 1 &= \frac{1}{f\sqrt{\delta}N(G)} \det \begin{bmatrix} a\zeta_1 + b\zeta_2 & c\zeta_1 + d\zeta_2 \\ a\overline{\zeta_1} + b\overline{\zeta_2} & c\overline{\zeta_1} + d\overline{\zeta_2} \end{bmatrix} \\ &= \frac{1}{f\sqrt{\delta}N(G)} \det \begin{bmatrix} \zeta_1 & \zeta_2 \\ \overline{\zeta_1} & \overline{\zeta_2} \end{bmatrix} \det \begin{bmatrix} a & c \\ b & d \end{bmatrix} \\ &= \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \end{aligned}$$

Where the last equality follows from the necessity of the condition proved above. Thus we have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

It now follows that $\{\omega_1, \omega_2\}$ is an ordered basis for G by Proposition 5.1.3. □

We note here that if we drop the ordered basis condition in the previous corollary then a necessary and sufficient condition for $\{\omega_1, \omega_2\}$ to be a basis of the full module G is

$$\frac{1}{f\sqrt{\delta}N(G)} \det \begin{bmatrix} \omega_1 & \omega_2 \\ \overline{\omega_1} & \overline{\omega_2} \end{bmatrix} = \pm 1.$$

We will often identify a full module with a basis. We will write $(G, \boldsymbol{\xi})$ when we would like to emphasize the choice of basis of the module where

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}.$$

Definition 5.1.13. *Let G and G' be full modules in K. We say that G and G' are* ***similar*** *if there exists $\eta \in K \setminus \{0\}$ such that $G' = \eta G$.*

From the corollary above, if two full modules G and G' are similar and $\boldsymbol{\xi}$ is a basis of G, then $\eta\boldsymbol{\xi}$ is a basis of G' where $G' = \eta G$. Note that if the basis $\boldsymbol{\xi}$ is ordered we do not necessarily have that the basis $\eta\boldsymbol{\xi}$ is ordered. However, if the quadratic field K is imaginary then the ordering is preserved. The following proposition indicates that the rings of coefficients of similar modules are related.

Proposition 5.1.14. *Let G and G' be similar full modules in K. Then $\mathfrak{o}_G = \mathfrak{o}_{G'}$. In particular, similar full modules have the same discriminant.*

Proof. Since G and G' are similar, there exists $\eta \in K$ such that $G' = \eta G$. Thus we have that

$$\begin{aligned}\mathfrak{o}_{G'} &= \{\alpha \in K : \alpha G' \subseteq G'\}\\ &= \{\alpha \in K : \alpha\eta G \subseteq \eta G\}\\ &= \{\alpha \in K : \alpha G \subseteq G\}\\ &= \mathfrak{o}_G.\end{aligned}$$

This completes the proof. □

Definition 5.1.15. *Let $\gamma \in K$. The minimal polynomial for γ is the irreducible polynomial*

$$\varphi(z) = rz^2 + tz + s, \;\; r, t, s \in \mathbb{Z}, \;\; r > 0$$

such that $\varphi(\gamma) = 0$.

Calculating the ring of coefficients for a given full module in K is rather simple.

Proposition 5.1.16. *Let $(G, \boldsymbol{\xi})$ be a full module in K with ordered basis*

$$\boldsymbol{\xi} = \begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}$$

and let

$$\varphi(z) = rz^2 + tz + s, \;\; r > 0$$

be the minimal polynomial of $\gamma = \omega_2/\omega_1$. Then $\{1, r\gamma\}$ is a basis for $\mathfrak{o}_G$ and

$$N(G) = \frac{|N(\omega_1)|}{r}.$$

Proof. Consider instead the full module G_0 with basis $\{1, \gamma\}$. Let $\alpha = x + y\gamma$ with $x, y \in \mathbb{Q}$. Note that the condition $\alpha G_0 \subseteq G_0$ is equivalent to the conditions $\alpha \in G_0$ and $\alpha\gamma \in G_0$. We have

$$\alpha\gamma = (x + y\gamma)\gamma = x\gamma + y\frac{-t\gamma - s}{r} = -\frac{sy}{r} + \left(x - \frac{ty}{r}\right)\gamma.$$

Thus α and $\alpha\gamma$ belong to G_0 and hence $\mathfrak{o}_{G_0}$ if and only if $x, y, \frac{ty}{r}$, and $\frac{sy}{r}$ are all integers. Since the greatest common divisor of r, t, and s is 1, this occurs if and only if x and y are integers and y

is divisible by r. Thus $\{1, r\gamma\}$ spans $\mathfrak{o}_{G_0}$. It follows that $\{1, r\gamma\}$ is a basis for $\mathfrak{o}_{G_0}$. Now the first claim now follows from Proposition 5.1.14. By the definition for the norm of a full module we have

$$N(G_0) = \left|\det \begin{bmatrix} 1 & 0 \\ 0 & 1/r \end{bmatrix}\right| = \frac{1}{r}.$$

Thus,

$$N(G) = N(\omega_1 G_0) = \frac{|N(\omega_1)|}{r}.$$

□

We present an example to illustrate the last proposition.

Example 5.1.17. Consider the full module

$$\left(G, \begin{bmatrix} 3+3\sqrt{-23} \\ 5+3\sqrt{-23} \end{bmatrix}\right)$$

in $K = \mathbb{Q}(\sqrt{-23})$. We can compute the norm of G by considering the similar module

$$\left(G_0, \begin{bmatrix} 1 \\ \dfrac{37-\sqrt{-23}}{36} \end{bmatrix}\right) = \left(G_0, \begin{bmatrix} 1 \\ \gamma \end{bmatrix}\right)$$

The minimal polynomial for γ is $\varphi(t) = 54t^2 - 111t + 58$. By Proposition 5.1.16,

$$N(G_0) = \frac{1}{54}.$$

This implies that $N(G) = N(3+3\sqrt{-23})N(G_0) = 4$. Note that this in turn implies that

$$\mathfrak{o}_G = \mathfrak{o}_3.$$

This is due to the fact that $\delta = -23$ implies $\omega = (1+\sqrt{\delta})/2$ and

$$3+3\sqrt{-23} = 0+6\omega$$
$$5+3\sqrt{-23} = 2+6\omega.$$

Hence we have

$$f = \frac{12}{4} = 3.$$

■

We would now like to define the product of two full modules in K. Given two full modules G and G', the product GG' is defined to be the full module

$$GG' = \left\{ \sum_{n=1}^{m} g_n g_n' : g_n \in G \text{ and } g_n' \in G' \right\}.$$

It is clear from the definition of the ring of coefficients that $G\mathfrak{o}_G = G$ for any full module G in K.

Proposition 5.1.18. *Let G and G' be full modules in K such that $\mathfrak{o}_G = \mathfrak{o}_{G'}$. Then the ring of coefficients, $\mathfrak{o}_{GG'}$, for the product GG' coincides with the ring of coefficients of G and G'. Moreover, we have $N(GG') = N(G)N(G')$.*

Proof. We prove that $\mathfrak{o}_G = \mathfrak{o}_{GG'}$. Let $\alpha \in \mathfrak{o}_G$. Then $\alpha G \subseteq G$. Hence it follows that $\alpha GG' \subseteq GG'$. Thus $\mathfrak{o}_G \subseteq \mathfrak{o}_{GG'}$. To complete the proof of the proposition we will need the following lemma.

Lemma 5.1.19. *Let G be a full module of K and let $\overline{G}$ denote the radical conjugate module of G. Then $G\overline{G} = N(G)\mathfrak{o}_G$.*

Proof. We may assume that G has a basis of the form

$$\xi = \begin{bmatrix} 1 \\ \gamma \end{bmatrix}$$

and let $a\gamma^2 + b\gamma + c = 0$ with a, b, and c relatively prime integers. Then

$$\begin{aligned} G\overline{G} &= \text{span}_{\mathbb{Z}}\{1, \gamma, \overline{\gamma}, \gamma\overline{\gamma}\} \\ &= \text{span}_{\mathbb{Z}}\left\{1, \gamma, -\gamma - \frac{b}{a}, \frac{c}{a}\right\} \\ &= \frac{1}{a}\text{span}_{\mathbb{Z}}\{a, b, c, a\gamma\} \\ &= \frac{1}{a}\text{span}_{\mathbb{Z}}\{1, a\gamma\} \\ &= N(G)\mathfrak{o}_G, \end{aligned}$$

where the last equality follows from Proposition 5.1.16. □

We now continue with the proof of Proposition 5.1.18. Let $\alpha \in \mathfrak{o}_{GG'}$. Then $\alpha GG' \subseteq GG'$. Multiplying on the right by $\overline{G'}$ we have $\alpha N(G')G \subseteq N(G')G$ which implies that $\alpha \in \mathfrak{o}_{G'} = \mathfrak{o}_G$. We now prove the last part of the proposition. We have $G\overline{G} = N(G)\mathfrak{o}_G$, $G'\overline{G'} = N(G')\mathfrak{o}_{G'}$, and $GG'\overline{GG'} = N(GG')\mathfrak{o}_{GG'}$. Since $\mathfrak{o}_G = \mathfrak{o}_{G'} = \mathfrak{o}_{GG'}$ we immediately obtain $N(GG') = N(G)N(G')$.

□

In general, it can be rather difficult to calculate the product of two full modules. However, the product of two full modules of a certain form can be easy to calculate. Before we look at this however, we will look at a small lemma.

Lemma 5.1.20. *Let* $(G, \boldsymbol{\xi})$ *be a full module in* K *with ring of coefficients* $\mathfrak{o}_f$. *Then there exists a unique* $\alpha \in K \setminus \{0\}$ *such that for* $(\alpha G, \alpha \boldsymbol{\xi})$ *is of the form*

$$\left(G', \begin{bmatrix} r \\ \frac{t - f\sqrt{\delta}}{2} \end{bmatrix}\right)$$

with $r, t \in \mathbb{Z}$ *and* $\gcd\left(r, t, \frac{t^2 - \delta f^2}{4r}\right) = 1$.

Proof. We note first that by Proposition 5.1.14 we have that G and αG have the same ring of coefficients for any choice of $\alpha \in K$. We first prove the existence of such an α. Let

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}.$$

We first choose $\alpha = \dfrac{\overline{\omega_1}}{N(G)}$. With this choice we have

$$r = \frac{\omega_1 \overline{\omega_1}}{N(G)} = \frac{N(\omega_1)}{N(G)} \in \mathbb{Z}$$

and

$$\frac{\omega_2 \overline{\omega_1}}{N(G)} \in \mathfrak{o}_f.$$

This implies that

$$\frac{\omega_2 \overline{\omega_1}}{N(G)} = a + b\frac{f\epsilon - f\sqrt{\delta}}{2} = \frac{c - bf\sqrt{\delta}}{2}$$

where $\delta \equiv \epsilon \pmod 4$ with $\epsilon = 0$ or 1 and $c = 2a + bf\epsilon$. As

$$\begin{bmatrix} r \\ \frac{c - bf\sqrt{\delta}}{2} \end{bmatrix}$$

is a basis for the full module $(\overline{\omega_1}/N(G))G$ we must have that

$$\pm 1 = \frac{1}{f\sqrt{\delta}\frac{|N(\omega_1)|}{N(G)^2} N(G)} \det \begin{bmatrix} r & \frac{c - bf\sqrt{\delta}}{2} \\ r & \frac{c + bf\sqrt{\delta}}{2} \end{bmatrix}$$

by the comment following Corollary 5.1.12 from which it follows that

$$\pm 1 = \frac{1}{f\sqrt{\delta}\frac{|N(\omega_1)|}{N(G)^2}N(G)} rbf\sqrt{\delta} = \frac{bN(\omega_1)}{|N(\omega_1)|}.$$

Hence $b = \pm 1$. If $b = -1$ then we just try $\alpha = -\frac{\overline{\omega_1}}{N(G)}$ to obtain a full module of the desired form. One should note that the element

$$\frac{\omega_2}{\omega_1} = \frac{t - f\sqrt{\delta}}{2r}$$

is a root of the polynomial $\varphi(z) = rz^2 - tz + s$ where

$$s = \frac{t^2 - \delta f^2}{4r}.$$

Since $|r|$ is the leading coefficient of the minimal polynomial for ω_2/ω_1 it follows that the coefficients of φ must be relatively prime.

We now prove uniqueness. Let α and α' be two elements of $K \setminus \{0\}$ that satisfy the claim of the lemma. Then it follows that there exists a nonzero rational number q such that

$$q\alpha = \alpha'.$$

It follows that

$$\frac{t' - f\sqrt{\delta}}{2} = \alpha'\omega_2 = q\alpha\omega_2 = q\frac{t - f\sqrt{\delta}}{2}$$

Hence

$$q = 1$$

and thus $\alpha = \alpha'$. The proof is complete. □

Proposition 5.1.21. *Let $\varphi(z) = rz^2 + tz + s$ and $\varphi'(z) = r'z^2 + t'z + s'$ be irreducible polynomials in $\mathbb{Z}[z]$ such that*

$$t^2 - 4rs = (t')^2 - 4r's' = \delta f^2$$

where δ is a fundamental discriminant and $f \in \mathbb{N}$. Assume that

$$\gcd(r, t, s) = \gcd(r', t', s') = 1.$$

Consider the full modules

$$\left(G, \begin{bmatrix} r \\ \frac{t - f\sqrt{\delta}}{2} \end{bmatrix}\right) \text{ and } \left(G', \begin{bmatrix} r' \\ \frac{t' - f\sqrt{\delta}}{2} \end{bmatrix}\right)$$

in $K = \mathbb{Q}(\sqrt{\delta})$. *Assume that*

$$\gcd\left(r, r', \frac{t+t'}{2}\right) = m.$$

Then a basis of the product GG' *is*

$$m\begin{bmatrix} r_0 \\ \dfrac{t_0 - f\sqrt{\delta}}{2} \end{bmatrix}$$

where

$$r_0 = \frac{rr'}{m^2}$$

and $t_0 \in \mathbb{Z}$ *with* $0 \leq t_0 < 2r_0$. *Moreover,* t_0 *is unique modulo* $2r_0$.

Proof. The proof is fairly straightforward. First note that since G and G' have the same ring of coefficients $\mathfrak{o}_f$ we have by Proposition 5.1.18 that GG' has the ring of coefficients $\mathfrak{o}_f$. It is clear that the generators of GG' are

$$\begin{aligned} &rr', \\ &\frac{r(t' - f\sqrt{\delta})}{2}, \\ &\frac{r'(t - f\sqrt{\delta})}{2}, \\ &\frac{(tt' + \delta f^2)/2 - (t+t')f\sqrt{\delta}/2}{2}. \end{aligned}$$

Thus every element $\alpha \in G$ is of the form

$$\alpha = arr' + b\frac{r(t' - f\sqrt{\delta})}{2} + c\frac{r'(t - f\sqrt{\delta})}{2} + d\left(\frac{(tt' + \delta f^2)/2 - (t+t')f\sqrt{\delta}/2}{2}\right)$$

which, after rearranging, becomes

$$\alpha = \frac{2arr' + brt' + cr't + d(tt' + \delta f^2)/2}{2} - \frac{br + cr' + d(t+t')/2}{2} f\sqrt{\delta}.$$

Since the greatest common divisor of r, r', and $(t+t')/2$ is equal to m, the coefficient on $f\sqrt{\delta}$ is of the form

$$\frac{mn}{2}$$

for some $n \in \mathbb{Z}$. Let $H = GG'$ and take any basis

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

of H. We have that

$$\omega_1 = \frac{y_1}{2} - \frac{mn_1}{2} f\sqrt{\delta},$$
$$\omega_2 = \frac{y_2}{2} - \frac{mn_2}{2} f\sqrt{\delta}.$$

Again, since the greatest common divisor of r, r', and $(t+t')/2$ is equal to m, it follows that n_1 and n_2 must be relatively prime. By Lemma 5.1.20 there exists a unique $\alpha \in K \setminus \{0\}$ such that

$$\alpha\omega_1 = r'' \in \mathbb{Z}$$

and

$$\alpha\omega_2 = \frac{t'' - f\sqrt{\delta}}{2}$$

with $t'' \in \mathbb{Z}$. In particular, we have that α is one of the elements in the set

$$\left\{ \frac{\overline{\omega_1}}{N(H)}, -\frac{\overline{\omega_1}}{N(H)} \right\}.$$

As the two cases are similar, we assume that

$$\alpha = \frac{\overline{\omega_1}}{N(H)}.$$

This implies that

$$\begin{aligned} \frac{1}{N(H)} \left(\frac{y_1}{2} + \frac{mn_1}{2} f\sqrt{\delta}\right)\left(\frac{y_2}{2} - \frac{mn_2}{2} f\sqrt{\delta}\right) &= \frac{1}{N(H)}\left(\frac{y_1y_2}{4} - \frac{m^2n_1n_2\delta f^2}{4} + \left(\frac{mn_1y_2 - mn_2y_1}{4}\right) f\sqrt{\delta}\right) \\ &= \frac{t'' - f\sqrt{\delta}}{2} \end{aligned}$$

and hence

$$\frac{mn_2y_1 - mn_1y_2}{2N(H)} = 1.$$

Upon multiplying $\boldsymbol{\xi}$ by the matrix

$$\begin{bmatrix} n_2 & -n_1 \\ k_1 & k_2 \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z})$$

we obtain as a basis for H

$$\begin{aligned} \begin{bmatrix} n_2 & -n_1 \\ k_1 & k_2 \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} &= \begin{bmatrix} \dfrac{N(H)}{m} \\ \dfrac{(k_1y_1 + k_2y_2) - mf\sqrt{\delta}}{2} \end{bmatrix} \\ &= \begin{bmatrix} \dfrac{rr'}{m} \\ \dfrac{(k_1y_1 + k_2y_2) - mf\sqrt{\delta}}{2} \end{bmatrix} \end{aligned}$$

By Lemma 5.1.20 we know that $k_1y_1 + k_2y_2$ is divisible by m and thus we know that

$$m\begin{bmatrix} \dfrac{rr'}{m^2} \\ \dfrac{(k_1y_1+k_2y_2)/m - f\sqrt{\delta}}{2} \end{bmatrix}$$

is a basis for H. We now set

$$r_0 = \frac{rr'}{m^2}$$

and obtain a basis

$$\boldsymbol{\xi} = m\begin{bmatrix} r_0 \\ \dfrac{(k_1y_1+k_2y_2)/m - f\sqrt{\delta}}{2} \end{bmatrix}.$$

We now multiply on the left by a matrix of the form

$$\begin{bmatrix} 1 & 0 \\ \ell & 1 \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

with $\ell \in \mathbb{Z}$ to obtain a basis of the form

$$\boldsymbol{\xi} = m\begin{bmatrix} r_0 \\ \dfrac{t_0 - f\sqrt{\delta}}{2} \end{bmatrix}$$

with $0 \le t_0 < 2r_0$. The uniqueness of t_0 follows from the construction. □

Note that by Lemma 5.1.20 and Proposition 5.1.21 we can define the product of two full modules in more generality.

Definition 5.1.22. *Let $(G_1, \boldsymbol{\xi}_1)$ and $(G_2, \boldsymbol{\xi}_2)$ be two full modules with the same ring of coefficients $\mathfrak{o}_f$. Let $\alpha_1, \alpha_2 \in K \setminus \{0\}$ be the quantities coming from Lemma 5.1.20 corresponding to $(G_1, \boldsymbol{\xi}_1)$ and $(G_2, \boldsymbol{\xi}_2)$ respectively. We define the product of these two full modules to be*

$$(G_1, \boldsymbol{\xi}_1) \cdot (G_2, \boldsymbol{\xi}_2) = (G_1G_2, \boldsymbol{\xi}_3)$$

where

$$\boldsymbol{\xi}_3 = (\alpha_1\alpha_2)^{-1}\boldsymbol{\xi}_0$$

and $\boldsymbol{\xi}_0$ is the basis of the module $\alpha_1\alpha_2G_1G_2$ obtained from Proposition 5.1.21.

Example 5.1.23. Consider the full modules

$$\left(G, \begin{bmatrix} 3+3\sqrt{-23} \\ 5+3\sqrt{-23} \end{bmatrix}\right) \text{ and } \left(G', \begin{bmatrix} -33+3\sqrt{-23} \\ 1+\sqrt{-23} \end{bmatrix}\right).$$

Note that $\mathfrak{o}_G = \mathfrak{o}_{G'} = \mathfrak{o}_3$. Then it follows that

$$\left(G, \begin{bmatrix} 3+3\sqrt{-23} \\ 5+3\sqrt{-23} \end{bmatrix}\right) \cdot \left(G', \begin{bmatrix} -33+3\sqrt{-23} \\ 1+\sqrt{-23} \end{bmatrix}\right) = \left(GG', \frac{(1+\sqrt{-23})(-11+\sqrt{-23})}{324} \begin{bmatrix} 972 \\ \frac{1845-9\sqrt{-23}}{2} \end{bmatrix}\right)$$
$$= \left(GG', \begin{bmatrix} -102-30\sqrt{-23} \\ -100-28\sqrt{-23} \end{bmatrix}\right).$$

So we conclude that the product of the above full modules is

$$\left(GG', \begin{bmatrix} -102-30\sqrt{-23} \\ -100-28\sqrt{-23} \end{bmatrix}\right).$$

■

It follows that the collection of full modules in K which have ring of coefficients $\mathfrak{o}_f$ forms an abelian group under multiplication of modules with identity element $\mathfrak{o}_f$ and inverses determined by Lemma 5.1.19.

The quotient of the group of modules by the subgroup of full modules similar to $\mathfrak{o}_f$ is called the ring class group of modules and will be denoted by $H(\mathfrak{o}_f)$.

Lemma 5.1.24. *The elements of $H(\mathfrak{o}_f)$ consist of similarity classes of full modules with ring of coefficients $\mathfrak{o}_f$.*

Proof. Let B denote the subgroup of full modules that are similar to $\mathfrak{o}_f$. Let G and G' be full modules in K with ring of coefficients $\mathfrak{o}_f$ and suppose $GB = G'B$. Then $\eta G \mathfrak{o}_f = G'$ for some $\eta \in K \setminus \{0\}$. Hence $\eta G = G'$ and thus G and G' are similar. □

Evidently, the group $H(\mathfrak{o}_f)$ is finite. This is a non-trivial result and one can see [36] for a proof of this claim.

Definition 5.1.25. *Let $\mathfrak{o}_f$ be a fixed order in K. We say that a full module $\mathfrak{a}$ in K*

1. *is an **ideal** of the order $\mathfrak{o}_f$ if $\mathfrak{o}_\mathfrak{a} \subset \mathfrak{o}_f$.*

2. *is **regular** if $\mathfrak{o}_\mathfrak{a} = \mathfrak{o}_f$.*

3. *is **integral** if $\mathfrak{a} \subset \mathfrak{o}_f$.*

*4. is **principal** if* $\mathfrak{a} = \gamma \mathfrak{o}_f$ *for some* $\gamma \in K$.

Two regular, integral ideals $\mathfrak{a}, \mathfrak{b}$ *of the order* $\mathfrak{o}_f$ *are said to be **relatively prime** if*

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{o}_f.$$

Fix a regular, integral ideal $\mathfrak{o}$ of $\mathfrak{o}_f$ and consider the following group, a particular subset of the collection of fractional ideals of $\mathfrak{o}_f$,

$$A(\mathfrak{o}_f, \mathfrak{o}) = \left\{ \mathfrak{u} = \frac{\mathfrak{a}}{\mathfrak{b}} : \mathfrak{a}, \mathfrak{b} \text{ are regular, integral ideals of the order } \mathfrak{o}_f \text{ and are relatively prime to } \mathfrak{o} \right\}.$$

The quotient of the group $A(\mathfrak{o}_f, \mathfrak{o})$ by the subgroup of principal ideals of the form $\mathfrak{c} = \gamma \mathfrak{o}_f$, where $\gamma \in K$ and $\gamma = a_1/a_2$ with $a_1, a_2 \equiv 1 \pmod{\mathfrak{o}}$, is called the ray class group of modules modulo $\mathfrak{o}$ in the order $\mathfrak{o}_f$ (cf. [16], [26], and [36]). We denote this quotient by $H(\mathfrak{o}_f, \mathfrak{o})$. The group $H(\mathfrak{o}_f, \mathfrak{o})$, like $H(\mathfrak{o}_f)$, is finite for any regular, integral ideal $\mathfrak{o}$ of the order $\mathfrak{o}_f$. In fact, we have a bigger connection between these two groups.

Proposition 5.1.26. *Let* $\mathfrak{o}_f$ *be an order of* K*. Then*

$$H(\mathfrak{o}_f, \mathfrak{o}_f) \cong H(\mathfrak{o}_f).$$

Proof. This follows immediately from the definition of the ray class group modulo $\mathfrak{o}$ with $\mathfrak{o} = \mathfrak{o}_f$. □

For $M \geq 1$ we will denote $A(\mathfrak{o}_f, M\mathfrak{o}_f)$ by $A(\mathfrak{o}_f, M)$. Before we think about this group any further we move into the connection between full modules and binary quadratic forms.

5.2 Full Modules and Binary Quadratic Forms

In this section we will discuss the connection between full modules and binary quadratic forms. From this point on we will assume that $K = \mathbb{Q}(\sqrt{\delta})$ is an imaginary quadratic field of fundamental discriminant δ. We will start with presenting some basic definitions about binary quadratic forms.

Definition 5.2.1. *A binary quadratic form* $S(x, y)$ *is a homogeneous polynomial of degree 2 in two variables* x *and* y.

Definition 5.2.2. *Consider a binary quadratic form*

$$S(x, y) = rx^2 + txy + sy^2.$$

(i) We say S *is **integral** if the coefficients* r, s, t *are elements of* $\mathbb{Z}$.

(ii) We say S *is **primitive** if* S *is integral and* $\gcd(r, s, t) = 1$.

(iii) We say S *is **positive definite** if* $S(x, y) > 0$ *for all* $(x, y) \neq (0, 0)$.

Let $(G, \boldsymbol{\xi})$ be a full module in K with ordered basis $\boldsymbol{\xi}$. Suppose further that $\mathfrak{o}_G = \mathfrak{o}_f$ for some $f \in \mathbb{N}$. Write

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}.$$

We then build a binary quadratic form corresponding to this full module

$$S_{(G,\boldsymbol{\xi})}(x, y) = \frac{(\omega_1 x + \omega_2 y)(\overline{\omega_1} x + \overline{\omega_2} y)}{N(G)}.$$

Proposition 5.2.3. *Given a full module $(G, \boldsymbol{\xi})$ with ordered basis $\boldsymbol{\xi}$ and $f \in \mathbb{N}$ such that $\mathfrak{o}_G = \mathfrak{o}_f$, the binary quadratic form $S_{(G,\boldsymbol{\xi})}$ is integral, primitive, and positive definite with discriminant δf^2.*

Proof. The integrality of $S_{(G,\boldsymbol{\xi})}$ follows from Lemma 5.1.19. We now show that $S_{(G,\boldsymbol{\xi})}$ is primitive. Let $\varphi(z) = rz^2 + tz + s$ with $r > 0$ be the minimal polynomial for $\gamma = -\omega_2/\omega_1$. Then $\gcd(r, s, t) = 1$ and

$$\varphi(z) = r\left(z + \frac{\omega_2}{\omega_1}\right)\left(z + \frac{\overline{\omega_2}}{\overline{\omega_1}}\right).$$

Letting $z = x/y$ we have

$$\begin{aligned} \varphi(x/y) &= r\left(\frac{x}{y} + \frac{\omega_2}{\omega_1}\right)\left(\frac{x}{y} + \frac{\overline{\omega_2}}{\overline{\omega_1}}\right) \\ &= \frac{r}{y^2 N(\omega_1)}(\omega_1 x + \omega_2 y)(\overline{\omega_1} x + \overline{\omega_2} y) \\ &= \frac{1}{y^2 N(G)}(\omega_1 x + \omega_2 y)(\overline{\omega_1} x + \overline{\omega_2} y) \\ &= \frac{1}{y^2} S_{(G,\boldsymbol{\xi})}(x, y), \end{aligned}$$

where the third equality uses Proposition 5.1.16. Hence

$$S_{(G,\boldsymbol{\xi})}(x, y) = y^2 \varphi(x/y) = rx^2 + txy + sy^2.$$

Thus $S_{(G,\boldsymbol{\xi})}(x, y)$ is primitive. We then deduce that $S_{(G,\boldsymbol{\xi})}(x, y)$ is positive definite since the basis $\boldsymbol{\xi}$ is ordered. Lastly, we show that the discriminant of $S_{(G,\boldsymbol{\xi})}(x, y)$ is δf^2. The discriminant of $S_{(G,\boldsymbol{\xi})}(x, y)$ is given by

$$\begin{aligned} t^2 - 4rs &= \frac{1}{(N(G))^2}((\omega_1 \overline{\omega_2} + \overline{\omega_1} \omega_2)^2 - 4\omega_1 \overline{\omega_1} \omega_2 \overline{\omega_2}) \\ &= \frac{1}{(N(G))^2}(\omega_1 \overline{\omega_2} - \overline{\omega_1} \omega_2)^2 \\ &= \delta f^2, \end{aligned}$$

by Corollary 5.1.12. This completes the proof. □

Conversely, given an integral, primitive, positive definite binary quadratic form

$$S(x,y) = rx^2 + txy + sy^2$$

with discriminant δf^2 with $f \in \mathbb{N}$ we associate the full module $(G_S, \boldsymbol{\xi}_{G_S})$ where

$$\boldsymbol{\xi}_{G_S} = \begin{bmatrix} r \\ \dfrac{t - f\sqrt{\delta}}{2} \end{bmatrix}.$$

Proposition 5.2.4. *Let $S(x,y) = rx^2 + txy + sy^2$ be an integral, primitive, positive definite binary quadratic form with discriminant δf^2 with $f \in \mathbb{N}$. Then the full module $(G_S, \boldsymbol{\xi}_{G_S})$ has discriminant δf^2 and the basis $\boldsymbol{\xi}_{G_S}$ satisfies equation (5.1), i.e., the basis $\boldsymbol{\xi}$ is ordered.*

Proof. First note that $\mathfrak{o}_{G_S} = \mathfrak{o}_f$ and hence the discriminant of G_S is equal to δf^2. Furthermore, we have $r > 0$ since $S(x,y)$ is positive definite and hence

$$\frac{1}{i}\det \begin{bmatrix} r & \dfrac{t - f\sqrt{\delta}}{2} \\ r & \dfrac{t + f\sqrt{\delta}}{2} \end{bmatrix} = \frac{1}{i} r f \sqrt{\delta} > 0.$$

This completes the proof. □

One can now check that for an integral, primitive, positive definite binary quadratic form $S(x,y)$ with discriminant δf^2 with $f \in \mathbb{N}$ we have

$$S_{(G_S, \boldsymbol{\xi}_{G_S})} = S$$

and for a full module $(G, \boldsymbol{\xi})$ with ordered basis

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

satisfying equation (5.1) we have

$$(G_{S_{(G,\boldsymbol{\xi})}}, \boldsymbol{\xi}_{S_{(G,\boldsymbol{\xi})}}) = \left(\frac{\overline{\omega_1}}{N(G)} G, \frac{\overline{\omega_1}}{N(G)} \boldsymbol{\xi} \right).$$

In the next section we will use this to establish a one-to-one correspondence between classes of full modules and classes of binary quadratic forms modulo congruence subgroups of $\mathrm{SL}(2,\mathbb{Z})$.

5.3 Correspondence between Full Modules and Binary Quadratic Forms

Again let $K = \mathbb{Q}(\sqrt{\delta})$ be an imaginary quadratic field of fundamental discriminant δ. Let Γ be a congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$ of level $M \geq 1$. We will say that two full modules $(G_1, \boldsymbol{\xi}_1)$ and

$(G_2, \boldsymbol{\xi}_2)$ in K are **equivalent modulo** Γ if

$$G_1 = \eta G_2 \text{ and } {}^tU\xi_1 = \eta\xi_2$$

for some $\eta \in K \setminus \{0\}$ and $U \in \Gamma$. We will say that two binary quadratic forms $S_1(x, y)$ and $S_2(x, y)$ are **equivalent modulo** Γ if

$$S_1(ax + by, cx + dy) = S_2(x, y)$$

for some

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma.$$

We can always associate a binary quadratic form $S(x, y) = rx^2 + txy + sy^2$ to a symmetric matrix

$$S = \begin{bmatrix} r & t/2 \\ t/2 & s \end{bmatrix}.$$

Thus the equivalence between binary quadratic forms $S_1(x, y)$ and $S_2(x, y)$ is equivalent to the existence of a $U \in \Gamma$ such that

$${}^tUS_1U = S_2.$$

It is clear that equivalent forms have the same discriminant.

Proposition 5.3.1. *Let $(G_1, \boldsymbol{\xi}_1)$ and $(G_2, \boldsymbol{\xi}_2)$ be equivalent full modules in K modulo Γ with $\boldsymbol{\xi}_1$ and $\boldsymbol{\xi}_2$ satisfying inequality (5.1). Then $S_{(G_1,\boldsymbol{\xi}_1)}(x, y)$ and $S_{(G_2,\boldsymbol{\xi}_2)}(x, y)$ are equivalent binary quadratic forms modulo Γ.*

Proof. Assume that $(G_1, \boldsymbol{\xi}_1)$ and $(G_2, \boldsymbol{\xi}_2)$ are equivalent full modules in K modulo Γ with $\boldsymbol{\xi}_1$ and $\boldsymbol{\xi}_2$ satisfying equation (5.1). Then there exists $\eta \in K \setminus \{0\}$ and $U \in \Gamma$ such that

$$G_1 = \eta G_2 \text{ and } {}^tU\boldsymbol{\xi}_1 = \eta\boldsymbol{\xi}_2.$$

For simplicity of notation we'll write $S_1(x, y) = S_{(G_1,\boldsymbol{\xi}_1)}(x, y)$ and $S_2(x, y) = S_{(G_2,\boldsymbol{\xi}_2)}(x, y)$. Write

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \ \boldsymbol{\xi}_1 = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}, \ \boldsymbol{\xi}_2 = \begin{bmatrix} \Omega_1 \\ \Omega_2 \end{bmatrix}$$

and note that

$$a\omega_1 + c\omega_2 = \eta\Omega_1,$$

$$b\omega_1 + d\omega_2 = \eta\Omega_2.$$

We then have

$$\begin{aligned}
S_2(x,y) &= \frac{1}{N(G_2)}(\Omega_1 x + \Omega_2 y)(\overline{\Omega_1}x + \overline{\Omega_2}y) \\
&= \frac{\eta\overline{\eta}}{N(G_1)}\left(\left(\frac{a}{\eta}\omega_1 + \frac{c}{\eta}\omega_2\right)x + \left(\frac{b}{\eta}\omega_1 + \frac{d}{\eta}\omega_2\right)y\right)\left(\left(\frac{a}{\overline{\eta}}\overline{\omega_1} + \frac{c}{\overline{\eta}}\overline{\omega_2}\right)x + \left(\frac{b}{\overline{\eta}}\overline{\omega_1} + \frac{d}{\overline{\eta}}\overline{\omega_2}\right)y\right) \\
&= \frac{1}{N(G_1)}(\omega_1(ax+by) + \omega_2(cx+dy))(\overline{\omega_1}(ax+by) + \overline{\omega_2}(cx+dy)) \\
&= S_1(ax+by, cx+dy).
\end{aligned}$$

Thus $S_1(x,y)$ and $S_2(x,y)$ are equivalent. □

Proposition 5.3.2. *Let $S_1(x,y)$ and $S_2(x,y)$ be binary quadratic forms. Assume that S_1 and S_2 are integral, primitive, and positive definite of discriminant δf^2 with $f \in \mathbb{N}$. Further assume that S_1 and S_2 are equivalent modulo Γ. Then $(G_{S_1}, \boldsymbol{\xi}_{S_1})$ and $(G_{S_2}, \boldsymbol{\xi}_{S_2})$ are equivalent full modules modulo Γ.*

Proof. Write $S_1(x,y) = r_1x^2 + t_1xy + s_1y^2$ and $S_2(x,y) = r_2x^2 + t_2xy + s_2y^2$. Since $S_1(x,y)$ and $S_2(x,y)$ are equivalent modulo Γ there exists

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$$

such that $S_1(ax+by, cx+dy) = S_2(x,y)$. Thus we have that

$$\begin{aligned}
r_2 &= r_1a^2 + t_1ac + s_1c^2, \\
t_2 &= 2r_1ab + t_1(ad+bc) + 2s_1cd, \\
s_2 &= r_1b^2 + t_1bd + s_1d^2.
\end{aligned}$$

Let

$$\eta = \frac{2r_1a + t_1c - cf\sqrt{\delta}}{2r_1a^2 + 2t_1ac + 2s_1c^2}.$$

Then $\eta \in K \setminus \{0\}$ and one can show

$${}^tU \begin{bmatrix} r_1 \\ \dfrac{t_1 - f\sqrt{\delta}}{2} \end{bmatrix} = \eta \begin{bmatrix} r_2 \\ \dfrac{t_2 - f\sqrt{\delta}}{2} \end{bmatrix}.$$

using the fact that $ad - bc = 1$ and $t_1^2 - 4r_1s_1 = \delta f^2$. Thus $(G_{S_1}, \boldsymbol{\xi}_{S_1})$ and $(G_{S_2}, \boldsymbol{\xi}_{S_2})$ are equivalent full modules modulo Γ. □

Definition 5.3.3. *Let Γ be a congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$. Let $\mathscr{M}(\delta f^2)$ denote the set of full modules $(G,\boldsymbol{\xi})$ in K with discriminant δf^2. Also define $\overline{\mathscr{M}}_\Gamma(\delta f^2)$ to be the set of of pairs $[(G,\boldsymbol{\xi})]$ where $[(G,\boldsymbol{\xi})] = [(G',\boldsymbol{\xi}')]$ if and only if the full modules $(G,\boldsymbol{\xi})$ and $(G',\boldsymbol{\xi}')$ are equivalent modulo Γ.*

The previous two propositions prove the following important fact.

Theorem 5.3.4. *Let*

$$A(1,\delta f^2) = \{S \in A(1) : S \text{ is primitive and has discriminant } \delta f^2 < 0\}.$$

Then

$$\Gamma \setminus A(1,\delta f^2) \cong \overline{\mathscr{M}}_\Gamma(\delta f^2)$$

where $\Gamma \setminus A(1,\delta f^2)$ denotes the set of equivalence classes of $A(1,\delta f^2)$ modulo Γ.

Recall that we defined multiplication of full modules. We would like to utilize this multiplication in conjunction with the set $\overline{\mathscr{M}}_\Gamma(\delta f^2)$. We show that this multiplication is well-defined.

Proposition 5.3.5. *Let $\Gamma = \mathrm{SL}(2,\mathbb{Z})$. The multiplication given by*

$$[(G_1,\boldsymbol{\xi}_1)]\cdot[(G_2,\boldsymbol{\xi}_2)] = [(G_1,\boldsymbol{\xi}_1)\cdot(G_2,\boldsymbol{\xi}_2)]$$

is a well-defined binary operation on $\overline{\mathscr{M}}_\Gamma(\delta f^2)$.

Proof. Consider the full modules $(G_1,\boldsymbol{\xi}_1)$, $(G_1',\boldsymbol{\xi}_1')$, $(G_2,\boldsymbol{\xi}_2)$, and $(G_2',\boldsymbol{\xi}_2')$ and assume that

$$[(G_1,\boldsymbol{\xi}_1)] = [(G_1',\boldsymbol{\xi}_1')] \text{ and } [(G_2,\boldsymbol{\xi}_2)] = [(G_2',\boldsymbol{\xi}_2')]$$

We now consider now the full modules G_1G_2 and $G_1'G_2'$ with basis determined by Definition 5.1.22. We'll label these bases $\boldsymbol{\xi}$ and $\boldsymbol{\xi}'$. It is clear that these two full modules are similar, i.e., there exists $\eta \in K\setminus\{0\}$ such that $G_1G_2 = \eta G_1'G_2'$. Therefore, multiplying the full module $(G_1'G_2',\boldsymbol{\xi}')$ by η takes us to the full module $(G_1G_2,\eta\boldsymbol{\xi}')$. Now $\boldsymbol{\xi}$ and $\eta\boldsymbol{\xi}'$ are bases of the same full module G_1G_2 and thus differ by a matrix in $\mathrm{SL}(2,\mathbb{Z})$. This proves the claim. □

The previous proposition implies that we have a group structure on $\overline{\mathscr{M}}_{\mathrm{SL}(2,\mathbb{Z})}(\delta f^2)$ and hence a group structure on $\mathrm{SL}(2,\mathbb{Z})\setminus A(1,\delta f^2)$. We call $\mathrm{SL}(2,\mathbb{Z})\setminus A(1,\delta f^2)$ the class group and we refer to the group operation on $\mathrm{SL}(2,\mathbb{Z})\setminus A(1,\delta f^2)$ as composition. We will denote the operation of composition by $\circ$. The composition of two forms can be obtained using Proposition 5.1.21.

Lemma 5.3.6. *Let $\Gamma = \mathrm{SL}(2,\mathbb{Z})$. The map $i : H(\mathfrak{o}_f) \to \overline{\mathscr{M}}_\Gamma(\delta f^2)$ given by*

$$i([G]) = [(G, \boldsymbol{\xi})]$$

where $\boldsymbol{\xi}$ is any ordered basis of G is a well-defined bijection such that

$$i([G] \cdot [G']) = i([G]) \cdot i([G'])$$

Proof. This is clear from the previous proposition. $\square$

Let $M \geq 1$ be an integer. We define $A(M, \delta f^2)$ to be the set of primitive, integral, positive definite binary quadratic forms of discriminant δf^2

$$S(x, y) = rx^2 + txy + sy^2$$

such that r is divisible by M.

We remark here that the set $\Gamma_0(M)$ acts on $A(M, \delta f^2)$. We also define $\mathscr{A}(M, \delta f^2)$ to be the subset of $\mathscr{M}(\delta f^2)$ that consists of full modules (G, ξ) that satisfy $S_{(G,\xi)} \in A(M, \delta f^2)$. We define $\overline{\mathscr{A}}(M, \delta f^2)$ accordingly, i.e.,

$$\Gamma_0(M) \setminus \mathscr{A}(M, \delta f^2) = \overline{\mathscr{A}}(M, \delta f^2).$$

This leads us to the following specialization of Theorem 5.3.4.

Theorem 5.3.7. *Let $M \geq 1$ be an integer. Then*

$$\Gamma_0(M) \setminus A(M, \delta f^2) \cong \overline{\mathscr{A}}(M, \delta f^2).$$

An important feature to note here is that there is not a group structure on $\overline{\mathscr{A}}(M, \delta f^2)$. Hence there is not a group structure on $\Gamma_0(M) \setminus A(M, \delta f^2)$. For a discussion of this feature, see [10].

5.4 Action on $\overline{\mathscr{M}}_{\Gamma_0(M)}(\delta f^2)$

We return now to our discussion about the group $A(\mathfrak{o}_f, M)$ where for the entirety of this section $M \geq 1$ and $f \geq 1$ are integers. Recall that $A(\mathfrak{o}_f, M)$ is the collection of fractional ideals consisting of quotients of regular, integral ideals of $\mathfrak{o}_f$ which are prime to $M\mathfrak{o}_f$. It is thus also convenient here to also consider the set

$$A_{\text{int}}(\mathfrak{o}_f, M) = \{\mathfrak{a} : \mathfrak{a} \text{ is a regular, integral ideal of the order } \mathfrak{o}_f \text{ and is relatively prime to } M\mathfrak{o}_f\}.$$

Our ultimate goal in this section is to prove that the group $H(\mathfrak{o}_f, M)$, the ray class group of modules modulo $M\mathfrak{o}_f$, acts on $\overline{\mathscr{A}}(M, \delta f^2)$ as a group of automorphisms. Before we get there however, we need to establish a couple preliminary results that will be especially useful.

Lemma 5.4.1. *Let $\mathfrak{u} \in A(\mathfrak{o}_f, M)$ an let $\mathfrak{a}, \mathfrak{b} \in A_{\text{int}}(\mathfrak{o}_f, M)$ be such that $\mathfrak{u} = \mathfrak{a}\mathfrak{b}^{-1}$. Then there exists $x_{\mathfrak{a},\mathfrak{b}} \in \mathfrak{u}$ such that $N(\mathfrak{b})x_{\mathfrak{a},\mathfrak{b}} \equiv 1 \pmod{M\mathfrak{o}_f}$.*

Proof. By definition of $A(\mathfrak{o}_f, M)$ we have that $\mathfrak{a} + M\mathfrak{o}_f = \mathfrak{o}_f$ and $\mathfrak{b} + M\mathfrak{o}_f = \mathfrak{o}_f$. It follows that $\overline{b} + M\mathfrak{o}_f = \mathfrak{o}_f$. Recall now that $\mathfrak{b}^{-1} = N(\mathfrak{b})^{-1}\overline{\mathfrak{b}}$ from which we compute that

$$\begin{aligned}
\mathfrak{o}_f &= (\mathfrak{a} + M\mathfrak{o}_f)(\overline{\mathfrak{b}} + M\mathfrak{o}_f) \\
&= (\mathfrak{a} + M\mathfrak{o}_f)(N(\mathfrak{b})\mathfrak{b}^{-1} + M\mathfrak{o}_f) \\
&= N(\mathfrak{b})\mathfrak{a}\mathfrak{b}^{-1} + M\mathfrak{a} + MN(\mathfrak{b})\mathfrak{b}^{-1} + M^2\mathfrak{o}_f \\
&= N(\mathfrak{b})\mathfrak{u} + M(\mathfrak{a} + M\mathfrak{o}_f) + MN(\mathfrak{b})\mathfrak{b}^{-1} \\
&= N(\mathfrak{b})\mathfrak{u} + M\mathfrak{o}_f + MN(\mathfrak{b})\mathfrak{b}^{-1} \\
&= N(\mathfrak{b})\mathfrak{u} + M(N(\mathfrak{b})\mathfrak{b}^{-1} + \mathfrak{o}_f) \\
&= N(\mathfrak{b})\mathfrak{u} + M(\overline{\mathfrak{b}} + \mathfrak{o}_f) \\
&= N(\mathfrak{b})\mathfrak{u} + M\mathfrak{o}_f.
\end{aligned}$$

It immediately follows that there exists $x \in \mathfrak{u}$ and $y \in M\mathfrak{o}_f$ such that $N(\mathfrak{b})x + My = 1$. The claim is proved. □

Lemma 5.4.2. *Let G be a full module in K with ring of coefficients $\mathfrak{o}_f$ and let $\alpha, \beta \in G$. There exists an ordered basis*

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

of G such that $\omega_1 \equiv \alpha \pmod{MG}$ and $\omega_2 \equiv \beta \pmod{MG}$ if and only if

$$\frac{1}{f\sqrt{\delta}N(G)} \det \begin{bmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{bmatrix} \equiv 1 \pmod{M}.$$

Proof. First note that for $\alpha, \beta \in G$, it follows from the relations $\overline{\alpha\overline{\beta} - \overline{\alpha}\beta} = -(\alpha\overline{\beta} - \overline{\alpha}\beta)$ and $\alpha\overline{\beta} - \overline{\alpha}\beta \in N(G)\mathfrak{o}_f$ that $\alpha\overline{\beta} - \overline{\alpha}\beta \in f\sqrt{\delta}N(G)\mathbb{Z}$. Hence

$$\frac{1}{f\sqrt{\delta}N(G)} \det \begin{bmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{bmatrix} \in \mathbb{Z}.$$

We now proceed with the proof of the statement. Assume that G has an ordered basis

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

such that $\omega_1 \equiv \alpha \pmod{MG}$ and $\omega_2 \equiv \beta \pmod{MG}$. Then by Corollary 5.1.12, for some $\alpha', \beta' \in G$,

$$\begin{aligned}
\frac{1}{f\sqrt{\delta}N(G)}\det\begin{bmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{bmatrix} &= \frac{1}{f\sqrt{\delta}N(G)}\det\begin{bmatrix} \omega_1 + M\alpha' & \omega_2 + M\beta' \\ \overline{\omega_1} + M\overline{\alpha'} & \overline{\omega_2} + M\overline{\beta'} \end{bmatrix} \\
&= \frac{1}{f\sqrt{\delta}N(G)}((\omega_1 + M\alpha')(\overline{\omega_2} + M\overline{\beta'}) - (\overline{\omega_1} + M\overline{\alpha'})(\omega_2 + M\beta')) \\
&= \frac{1}{f\sqrt{\delta}N(G)}(\omega_1\overline{\omega_2} - \overline{\omega_1}\omega_2 + M\omega_1\overline{\beta'} + M\overline{\omega_2}\alpha' + M^2\alpha'\overline{\beta'} - M\overline{\omega_1}\beta' - M\omega_2\overline{\alpha'} - M^2\overline{\alpha'}\beta) \\
&= \frac{1}{f\sqrt{\delta}N(G)}\left(\det\begin{bmatrix} \omega_1 & \omega_2 \\ \overline{\omega_1} & \overline{\omega_2} \end{bmatrix} + M\det\begin{bmatrix} \omega_1 & \beta' \\ \overline{\omega_1} & \overline{\beta'} \end{bmatrix} - M\det\begin{bmatrix} \omega_2 & \alpha' \\ \overline{\omega_2} & \overline{\alpha'} \end{bmatrix} + M\det\begin{bmatrix} M\alpha' & \beta' \\ M\overline{\alpha'} & \overline{\beta'} \end{bmatrix}\right) \\
&\equiv 1 \pmod{M}.
\end{aligned}$$

Now assume that

$$\frac{1}{f\sqrt{\delta}N(G)}\det\begin{bmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{bmatrix} \equiv 1 \pmod{M}.$$

Fix an ordered basis

$$\boldsymbol{\xi}_0 = \begin{bmatrix} \alpha_0 \\ \beta_0 \end{bmatrix}$$

of G and expand α and β in terms of this basis,

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix}\begin{bmatrix} \alpha_0 \\ \beta_0 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

Thus

$$\begin{aligned}
\frac{1}{f\sqrt{\delta}N(G)}\det\begin{bmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{bmatrix} &= \frac{1}{f\sqrt{\delta}N(G)}\det\begin{bmatrix} p\alpha_0 + q\beta_0 & r\alpha_0 + s\beta_0 \\ p\overline{\alpha_0} + q\overline{\beta_0} & r\overline{\alpha_0} + s\overline{\beta_0} \end{bmatrix} \\
&= \frac{1}{f\sqrt{\delta}N(G)}\det\begin{bmatrix} \alpha_0 & \beta_0 \\ \overline{\alpha_0} & \overline{\beta_0} \end{bmatrix}\det\begin{bmatrix} p & r \\ q & s \end{bmatrix} \\
&= \det\begin{bmatrix} p & q \\ r & s \end{bmatrix}.
\end{aligned}$$

Hence

$$\det \begin{bmatrix} p & q \\ r & s \end{bmatrix} \equiv 1 \pmod{M}.$$

Thus there exists $U \in \mathrm{SL}(2,\mathbb{Z})$ such that

$$U \equiv \begin{bmatrix} p & q \\ r & s \end{bmatrix} \pmod{M}.$$

Now let

$$\begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = U \begin{bmatrix} p & q \\ r & s \end{bmatrix}^{-1} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

It then follows that we have that $\omega_1 \equiv \alpha \pmod{MG}$ and $\omega_2 \equiv \beta \pmod{MG}$. This completes the proof. □

One should note that if two distinct bases are found using Lemma 5.4.2 then they necessarily differ by a matrix in $\Gamma_0(M)$. Let $a, b \in \mathbb{Z}$ with $\gcd(b, M) = 1$. Let

$$\widetilde{\left(\frac{a}{b}\right)}$$

denote the least non-negative residue of ab^* (mod M) where $0 < b^* < M$ and $bb^* \equiv 1 \pmod{M}$. We observe here that this definition is independent of how the fraction is written. For $\mathfrak{u} = \mathfrak{a}\mathfrak{b}^{-1} \in A(\mathfrak{o}_f, M)$ we interpret $\widetilde{N(\mathfrak{u})}$ as the integer $\widetilde{(\frac{N(\mathfrak{a})}{N(\mathfrak{b})})}$. We will first define a map ϕ from $\mathscr{A}(M, \delta f^2) \times A_{\mathrm{int}}(\mathfrak{o}_f, M) \times A_{\mathrm{int}}(\mathfrak{o}_f, M)$ to $\overline{\mathscr{A}}(M, \delta f^2)$. Let $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$ with

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix},$$

let $\mathfrak{a}, \mathfrak{b} \in A_{\mathrm{int}}(\mathfrak{o}_f, M)$, and let $\mathfrak{u} = \mathfrak{a}\mathfrak{b}^{-1}$. We set

$$\phi((G, \boldsymbol{\xi}), \mathfrak{a}, \mathfrak{b}) = [(G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}})]$$

where $\boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}}$ is any ordered basis of $G\mathfrak{u}$ such that

$$\boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}} \equiv \begin{bmatrix} \widetilde{N(\mathfrak{u})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(\mathfrak{b})\omega_1 x_{\mathfrak{a},\mathfrak{b}} \\ N(\mathfrak{b})\omega_2 x_{\mathfrak{a},\mathfrak{b}} \end{bmatrix} \pmod{MG\mathfrak{u}}$$

where $x_{\mathfrak{a},\mathfrak{b}} \in \mathfrak{u}$ is such that $N(\mathfrak{b})x_{\mathfrak{a},\mathfrak{b}} \equiv 1 \pmod{M\mathfrak{o}_f}$. Notice that

$$\frac{1}{f\sqrt{\delta}N(G\mathfrak{u})}(\widetilde{N(\mathfrak{u})}\omega_1\overline{\omega_2}N(\mathfrak{b})^2|x_{\mathfrak{a},\mathfrak{b}}|^2 - \widetilde{N(\mathfrak{u})}\overline{\omega_1}\omega_2 N(\mathfrak{b})^2|x_{\mathfrak{a},\mathfrak{b}}|^2) \equiv 1 \pmod{M}$$

and thus the existence of such a basis follows from the Lemma 5.4.2. The well-definedness of the map ϕ also follows based on the remark immediately following the proof of Lemma 5.4.2.

Proposition 5.4.3. *Let* $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$*, let* $\mathfrak{a}, \mathfrak{b} \in A_{\mathrm{int}}(\mathfrak{o}_f, M)$*, and let* $\mathfrak{u} = \mathfrak{a}\mathfrak{b}^{-1}$*. Then* $[(G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}})]$ *is an element of* $\overline{\mathscr{A}}(M, \delta f^2)$ *for any choice of* $\boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}}$*.*

Proof. Let

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

be an ordered basis of G. By the definition, we can write any $\boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}}$ as

$$\boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}} = \begin{bmatrix} \widetilde{N(\mathfrak{u})} N(\mathfrak{b}) \omega_1 x_{\mathfrak{a},\mathfrak{b}} + M z_1 \\ N(\mathfrak{b}) \omega_2 x_{\mathfrak{a},\mathfrak{b}} + M z_2 \end{bmatrix}$$

for some $z_1, z_2 \in G\mathfrak{u}$. All we need to check is that

$$\frac{1}{N(G\mathfrak{u})} (\widetilde{N(\mathfrak{u})} N(\mathfrak{b}) \omega_1 x_{\mathfrak{a},\mathfrak{b}} + M z_1)(\widetilde{N(\mathfrak{u})} N(\mathfrak{b}) \overline{\omega_1 x_{\mathfrak{a},\mathfrak{b}}} + M \overline{z_1}) \in M\mathbb{Z}.$$

Expanding we get

$$\frac{1}{N(G\mathfrak{u})} (\widetilde{N(\mathfrak{u})}^2 N(\mathfrak{b})^2 |\omega_1|^2 |x_{\mathfrak{a},\mathfrak{b}}|^2 + M \widetilde{N(\mathfrak{u})} N(\mathfrak{b}) (\omega_1 x_{\mathfrak{a},\mathfrak{b}} \overline{z_1} + \overline{\omega_1 x_{\mathfrak{a},\mathfrak{b}}} z_1) + M^2 |z_1|^2).$$

Since

$$\frac{1}{N(G)} |\omega_1|^2 \in M\mathbb{Z}, \;\; \frac{1}{N(\mathfrak{u})} |x_{\mathfrak{a},\mathfrak{b}}|^2 \in \mathbb{Z}, \;\text{ and } G\mathfrak{u}\overline{G\mathfrak{u}} = N(G\mathfrak{u})\mathfrak{o}_f$$

it follows that the above is an element of $M\mathbb{Z}$. □

The previous proposition establishes that we have a map

$$\phi : \mathscr{A}(M, \delta f^2) \times A_{\mathrm{int}}(\mathfrak{o}_f, M) \times A_{\mathrm{int}}(\mathfrak{o}_f, M) \to \overline{\mathscr{A}}(M, \delta f^2).$$

There is one important property of this map that we will need to address.

Proposition 5.4.4. *Let* $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$ *and let* $\mathfrak{u} \in A(\mathfrak{o}_f, M)$*. Suppose* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d} \in A_{\mathrm{int}}(\mathfrak{o}_f, M)$ *are such that* $\mathfrak{u} = \mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{c}\mathfrak{d}^{-1}$*. Then*

$$\phi((G, \boldsymbol{\xi}), \mathfrak{a}, \mathfrak{b}) = \phi((G, \boldsymbol{\xi}), \mathfrak{c}, \mathfrak{d}).$$

Proof. Let $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$ with

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

and let $\mathfrak{u} \in A(\mathfrak{o}_f, M)$. Let $x_{\mathfrak{a},\mathfrak{b}}$ and $x_{\mathfrak{c},\mathfrak{d}}$ be such that

$$N(\mathfrak{b})x_{\mathfrak{a},\mathfrak{b}} \equiv 1 \pmod{M\mathfrak{o}_f} \quad \text{and} \quad N(\mathfrak{d})x_{\mathfrak{c},\mathfrak{d}} \equiv 1 \pmod{M\mathfrak{o}_f}.$$

Hence $N(\mathfrak{b})x_{\mathfrak{a},\mathfrak{b}} \equiv N(\mathfrak{d})x_{\mathfrak{c},\mathfrak{d}} \pmod{M\mathfrak{o}_f}$ and thus $N(\mathfrak{b})x_{\mathfrak{a},\mathfrak{b}} - N(\mathfrak{d})x_{\mathfrak{c},\mathfrak{d}} \in \mathfrak{u} \cap M\mathfrak{o}_f \subseteq M\mathfrak{u}$. Now construct $\boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}}$ and $\boldsymbol{\xi}_{\mathfrak{c},\mathfrak{d}}$ such that

$$\boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}} \equiv \begin{bmatrix} \widetilde{N(\mathfrak{u})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(\mathfrak{b})\omega_1 x_{\mathfrak{a},\mathfrak{b}} \\ N(\mathfrak{b})\omega_2 x_{\mathfrak{a},\mathfrak{b}} \end{bmatrix} \pmod{MG\mathfrak{u}}$$

and

$$\boldsymbol{\xi}_{\mathfrak{c},\mathfrak{d}} \equiv \begin{bmatrix} \widetilde{N(\mathfrak{u})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(\mathfrak{d})\omega_1 x_{\mathfrak{c},\mathfrak{d}} \\ N(\mathfrak{d})\omega_2 x_{\mathfrak{c},\mathfrak{d}} \end{bmatrix} \pmod{MG\mathfrak{u}}$$

It follows that $\boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}} \equiv \boldsymbol{\xi}_{\mathfrak{c},\mathfrak{d}} \pmod{MG\mathfrak{u}}$. Since $\boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}}$ and $\boldsymbol{\xi}_{\mathfrak{c},\mathfrak{d}}$ are ordered bases of $G\mathfrak{u}$ there exists a matrix $U \in \mathrm{SL}(2,\mathbb{Z})$ such that $\boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}} = {}^tU\boldsymbol{\xi}_{\mathfrak{c},\mathfrak{d}}$. We write

$$\boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad \text{and} \quad \boldsymbol{\xi}_{\mathfrak{c},\mathfrak{d}} = \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} \quad \text{and} \quad U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

We then have

$$\begin{aligned} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} &= {}^tU \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} \\ &= \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} \\ &= \begin{bmatrix} a\alpha' + c\beta' \\ b\alpha' + d\beta' \end{bmatrix}. \end{aligned}$$

Thus we have that $\alpha = \alpha' + Mz = a\alpha' + c\beta'$ where $z \in G\mathfrak{u}$. Since $\boldsymbol{\xi}_{\mathfrak{c},\mathfrak{d}}$ is an ordered basis of $G\mathfrak{u}$ we can write

$$z = a'\alpha' + c'\beta'$$

where $a', c' \in \mathbb{Z}$. Hence $\alpha' + a'M\alpha' + c'M\beta' = a\alpha' + c\beta'$. It follows that c must be divisible by M. Hence $U \in \Gamma_0(M)$. It follows that

$$[(G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{a},\mathfrak{b}})] = [(G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{c},\mathfrak{d}})].$$

□

The previous proposition allows us to unambiguously construct a pairing $\phi_1 : \mathscr{A}(M, \delta f^2) \times A(\mathfrak{o}_f, M) \to \overline{\mathscr{A}}(M, \delta f^2)$ given by

$$\phi_1((G, \boldsymbol{\xi}), \mathfrak{u}) = [(G\mathfrak{u}, \boldsymbol{\xi}_\mathfrak{u})]$$

where $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$ with

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix},$$

$\mathfrak{u} \in A(\mathfrak{o}_f, M)$ with $\mathfrak{u} = \mathfrak{a}\mathfrak{b}^{-1}$ for $\mathfrak{a}, \mathfrak{b} \in A_{\text{int}}(\mathfrak{o}_f, M)$, and $\boldsymbol{\xi}_\mathfrak{u}$ is any ordered basis of $G\mathfrak{u}$ such that

$$\boldsymbol{\xi}_\mathfrak{u} \equiv \begin{bmatrix} \widetilde{N(\mathfrak{u})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(\mathfrak{b})\omega_1 x_{\mathfrak{a},\mathfrak{b}} \\ N(\mathfrak{b})\omega_2 x_{\mathfrak{a},\mathfrak{b}} \end{bmatrix} \pmod{MG\mathfrak{u}} \tag{5.2}$$

where $x_{\mathfrak{a},\mathfrak{b}} \in \mathfrak{u}$ is such that $N(\mathfrak{b})x_{\mathfrak{a},\mathfrak{b}} \equiv 1 \pmod{M\mathfrak{o}_f}$.

Proposition 5.4.5. *Let* $(G, \boldsymbol{\xi}), (G', \boldsymbol{\xi}') \in \mathscr{A}(M, \delta f^2)$ *with* $[(G, \boldsymbol{\xi})] = [(G', \boldsymbol{\xi}')]$ *(this is* $\Gamma_0(M)$*-equivalence) and let* $\mathfrak{u} \in A(\mathfrak{o}_f, M)$*. Then*

$$[(G\mathfrak{u}, \boldsymbol{\xi}_\mathfrak{u})] = [(G'\mathfrak{u}, \boldsymbol{\xi}'_\mathfrak{u})]$$

Proof. Let $(G, \boldsymbol{\xi}), (G', \boldsymbol{\xi}') \in \mathscr{A}(M, \delta f^2)$ with

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} \quad \text{and} \quad \boldsymbol{\xi}' = \begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix}$$

and such that $[(G, \boldsymbol{\xi})] = [(G', \boldsymbol{\xi}')]$. Let $\mathfrak{u} \in A(\mathfrak{o}_f, M)$ and write $\mathfrak{u} = \mathfrak{a}\mathfrak{b}^{-1}$ for some $\mathfrak{a}, \mathfrak{b} \in A_{\text{int}}(\mathfrak{o}_f, M)$. Let $\eta \in K \setminus \{0\}$ and $U \in \Gamma_0(M)$ be such that $G' = \eta G$ and ${}^t U \boldsymbol{\xi}' = \eta \boldsymbol{\xi}$. Write

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Let

$$\boldsymbol{\xi}_\mathfrak{u} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad \text{and} \quad \boldsymbol{\xi}'_\mathfrak{u} = \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix}$$

Then

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \widetilde{N(\mathfrak{u})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(\mathfrak{b})\omega_1 x_{\mathfrak{a},\mathfrak{b}} \\ N(\mathfrak{b})\omega_2 x_{\mathfrak{a},\mathfrak{b}} \end{bmatrix} + \begin{bmatrix} Mz_1 \\ Mz_2 \end{bmatrix}$$

where $z_1, z_2 \in G\mathfrak{u}$. Hence,

$$\begin{aligned}\eta\begin{bmatrix}\alpha\\ \beta\end{bmatrix} &= \begin{bmatrix}\widetilde{N(\mathfrak{u})} & \\ & 1\end{bmatrix}\begin{bmatrix}N(\mathfrak{b})\eta\omega_1 x_{\mathfrak{a},\mathfrak{b}}\\ N(\mathfrak{b})\eta\omega_2 x_{\mathfrak{a},\mathfrak{b}}\end{bmatrix} + \begin{bmatrix}M\eta z_1\\ M\eta z_2\end{bmatrix}\\ &= \begin{bmatrix}\widetilde{N(\mathfrak{u})} & \\ & 1\end{bmatrix}\begin{bmatrix}N(\mathfrak{b})(a\omega_1' + c\omega_2')x_{\mathfrak{a},\mathfrak{b}}\\ N(\mathfrak{b})(b\omega_1' + d\omega_2')x_{\mathfrak{a},\mathfrak{b}}\end{bmatrix} + \begin{bmatrix}M\eta z_1\\ M\eta z_2\end{bmatrix}\\ &= \begin{bmatrix}\widetilde{N(\mathfrak{u})} & \\ & 1\end{bmatrix}\begin{bmatrix}a & c\\ b & d\end{bmatrix}\begin{bmatrix}N(\mathfrak{b})\omega_1' x_{\mathfrak{a},\mathfrak{b}}\\ N(\mathfrak{b})\omega_2' x_{\mathfrak{a},\mathfrak{b}}\end{bmatrix} + \begin{bmatrix}M\eta z_1\\ M\eta z_2\end{bmatrix}.\end{aligned}$$

It then follows that

$$\begin{aligned}\eta\begin{bmatrix}\alpha\\ \beta\end{bmatrix} &\equiv \begin{bmatrix}a & \widetilde{N(\mathfrak{u})}c\\ \widetilde{N(\mathfrak{u})^{-1}}b & d\end{bmatrix}\begin{bmatrix}\widetilde{N(\mathfrak{u})} & \\ & 1\end{bmatrix}\begin{bmatrix}N(\mathfrak{b})\omega_1' x_{\mathfrak{a},\mathfrak{b}}\\ N(\mathfrak{b})\omega_2' x_{\mathfrak{a},\mathfrak{b}}\end{bmatrix} \pmod{MG'\mathfrak{u}}\\ &\equiv \begin{bmatrix}p & r\\ q & s\end{bmatrix}\begin{bmatrix}\widetilde{N(\mathfrak{u})} & \\ & 1\end{bmatrix}\begin{bmatrix}N(\mathfrak{b})\omega_1' x_{\mathfrak{a},\mathfrak{b}}\\ N(\mathfrak{b})\omega_2' x_{\mathfrak{a},\mathfrak{b}}\end{bmatrix} \pmod{MG'\mathfrak{u}}\\ &\equiv \begin{bmatrix}p & r\\ q & s\end{bmatrix}\begin{bmatrix}\alpha'\\ \beta'\end{bmatrix} \pmod{MG'\mathfrak{u}}\end{aligned}$$

where

$$\begin{bmatrix}p & r\\ q & s\end{bmatrix} \equiv \begin{bmatrix}a & \widetilde{N(\mathfrak{u})}c\\ \widetilde{N(\mathfrak{u})^{-1}}b & d\end{bmatrix} \ (\mathrm{mod} M)$$

is a lift to $\mathrm{SL}(2,\mathbb{Z})$. Since c is divisible by M we can thus conclude that r is divisible by M and hence

$$\begin{bmatrix}p & q\\ r & s\end{bmatrix} \in \Gamma_0(M).$$

Now we notice that

$$\begin{aligned}\frac{1}{f\sqrt{\delta}N(G'\mathfrak{u})}\det\begin{bmatrix}\eta\alpha & \eta\beta\\ \overline{\eta\alpha} & \overline{\eta\beta}\end{bmatrix} &= \frac{1}{f\sqrt{\delta}N(\eta G\mathfrak{u})}\det\begin{bmatrix}\eta\alpha & \eta\beta\\ \overline{\eta\alpha} & \overline{\eta\beta}\end{bmatrix}\\ &= \frac{1}{f\sqrt{\delta}|\eta|^2 N(G\mathfrak{u})}|\eta|^2\det\begin{bmatrix}\alpha & \beta\\ \overline{\alpha} & \overline{\beta}\end{bmatrix}\\ &= 1\end{aligned}$$

where the last line uses Corollary 5.1.12. Invoking Corollary 5.1.12 one more time we conclude that

$\eta\boldsymbol{\xi}_{\mathfrak{u}}$ is an ordered basis for $G'\mathfrak{u}$. Hence there exists $V \in \mathrm{SL}(2,\mathbb{Z})$ such that

$$ {}^{t}V \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = \eta \begin{bmatrix} \alpha \\ \beta \end{bmatrix}. $$

We need to show that $V \in \Gamma_0(M)$. We know

$$ \eta \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \equiv \begin{bmatrix} p & r \\ q & s \end{bmatrix} \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} \pmod{MG'\mathfrak{u}} $$

which implies that

$$ {}^{t}V \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} \equiv \begin{bmatrix} p & r \\ q & s \end{bmatrix} \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} \pmod{MG'\mathfrak{u}}. $$

Let

$$ V = \begin{bmatrix} w & x \\ y & z \end{bmatrix}. $$

Then

$$ \begin{aligned} w\alpha' + y\beta' &\equiv p\alpha' + r\beta' \pmod{MG'\mathfrak{u}} \\ &\equiv p\alpha' \pmod{MG'\mathfrak{u}}. \end{aligned} $$

It is immediate that y is divisible by M and hence $V \in \Gamma_0(M)$. The proposition is proved. □

The previous proposition implies that we have a well-defined pairing

$$ \phi_2 : \overline{\mathscr{A}}(M, \delta f^2) \times A(\mathfrak{o}_f, M) \to \overline{\mathscr{A}}(M, \delta f^2). $$

This pairing then induces a pairing $\Phi : \overline{\mathscr{A}}(M, \delta f^2) \times H(\mathfrak{o}_f, M) \to \overline{\mathscr{A}}(M, \delta f^2)$. Notice that for $[(G, \boldsymbol{\xi})] \in \overline{\mathscr{A}}(M, \delta f^2)$ with

$$ \boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}, $$

for $\mathfrak{u} \in A(\mathfrak{o}_f, M)$, and for regular, integral ideals of the form $\gamma\mathfrak{o}_f$ where $\gamma = a_1/a_2$ with $a_1, a_2 \equiv 1 \pmod{M\mathfrak{o}_f}$ we have that

$$ \begin{aligned} [(G\gamma\mathfrak{o}_f\mathfrak{u}, \boldsymbol{\xi}_{\gamma\mathfrak{o}_f\mathfrak{u}})] &= [(\gamma G\mathfrak{u}, \boldsymbol{\xi}_{\gamma\mathfrak{u}})] \\ &= [(\gamma G\mathfrak{u}, \gamma\boldsymbol{\xi}_{\mathfrak{u}})] \\ &= [(G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{u}})] \end{aligned} $$

as

$$\begin{aligned}
\boldsymbol{\xi}_{\gamma\mathfrak{u}} &\equiv \begin{bmatrix} \widetilde{N(\gamma\mathfrak{u})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(a_2\mathfrak{b})\omega_1 x_{a_1\mathfrak{a},a_2\mathfrak{b}} \\ N(a_2\mathfrak{b})\omega_2 x_{a_1\mathfrak{a},a_2\mathfrak{b}} \end{bmatrix} \pmod{M\gamma G\mathfrak{u}} \\
&\equiv \begin{bmatrix} \widetilde{N(\gamma)}\widetilde{N(\mathfrak{u})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(a_2)N(\mathfrak{b})\omega_1 \dfrac{a_1}{a_2} x_{\mathfrak{a},\mathfrak{b}} \\ N(a_2)N(\mathfrak{b})\omega_2 \dfrac{a_1}{a_2} x_{\mathfrak{a},\mathfrak{b}} \end{bmatrix} \pmod{M\gamma G\mathfrak{u}} \\
&\equiv \gamma \begin{bmatrix} \widetilde{N(\mathfrak{u})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(\mathfrak{b})\omega_1 x_{\mathfrak{a},\mathfrak{b}} \\ N(\mathfrak{b})\omega_2 x_{\mathfrak{a},\mathfrak{b}} \end{bmatrix} \pmod{M\gamma G\mathfrak{u}} \\
&\equiv \gamma\boldsymbol{\xi}_{\mathfrak{u}} \pmod{M\gamma G\mathfrak{u}}.
\end{aligned}$$

This easily establishes the well-definedness of Φ.

Proposition 5.4.6. *Let* $[(G,\boldsymbol{\xi})] \in \overline{\mathscr{A}}(M,\delta f^2)$ *and let* $[\mathfrak{u}],[\mathfrak{v}] \in H(\mathfrak{o}_f, M)$*. Then*

$$\Phi([(G,\boldsymbol{\xi})],[\mathfrak{o}_f]) = [(G,\boldsymbol{\xi})]$$

and

$$\Phi([(G,\boldsymbol{\xi})],[\mathfrak{u}\mathfrak{v}]) = \Phi(\Phi([(G,\boldsymbol{\xi})],[\mathfrak{u}]),[\mathfrak{v}]).$$

Proof. It is easy to see that the first equality is true. We will prove the second equality. Let $\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{d} \in A_{\text{int}}(\mathfrak{o}_f, M)$ be such that $\mathfrak{u} = \mathfrak{a}\mathfrak{b}^{-1}$ and $\mathfrak{v} = \mathfrak{c}\mathfrak{d}^{-1}$. Let $[(G,\boldsymbol{\xi})] \in \overline{\mathscr{A}}(M,\delta f^2)$ with

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}.$$

Then

$$\begin{aligned}
\Phi(\Phi([(G,\boldsymbol{\xi})],[\mathfrak{u}]),[\mathfrak{v}]) &= \Phi([(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}})],[\mathfrak{v}]) \\
&= [(G\mathfrak{u}\mathfrak{v},(\boldsymbol{\xi}_{\mathfrak{u}})_{\mathfrak{v}})].
\end{aligned}$$

Let

$$\boldsymbol{\xi}_{\mathfrak{u}} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

By definition, we have

$$
\begin{aligned}
(\boldsymbol{\xi}_{\mathfrak{u}})_{\mathfrak{v}} &\equiv \begin{bmatrix} \widetilde{N(\mathfrak{v})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(\mathfrak{d})\alpha x_{\mathfrak{c},\mathfrak{d}} \\ N(\mathfrak{d})\beta x_{\mathfrak{c},\mathfrak{d}} \end{bmatrix} \pmod{MG\mathfrak{u}\mathfrak{v}} \\
&\equiv \begin{bmatrix} \widetilde{N(\mathfrak{v})} & \\ & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} N(\mathfrak{d}) x_{\mathfrak{c},\mathfrak{d}} \pmod{MG\mathfrak{u}\mathfrak{v}} \\
&\equiv \begin{bmatrix} \widetilde{N(\mathfrak{v})} & \\ & 1 \end{bmatrix} \begin{bmatrix} \widetilde{N(\mathfrak{u})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(\mathfrak{b})\omega_1 x_{\mathfrak{a},\mathfrak{b}} \\ N(\mathfrak{b})\omega_2 x_{\mathfrak{a},\mathfrak{b}} \end{bmatrix} N(\mathfrak{d}) x_{\mathfrak{c},\mathfrak{d}} \pmod{MG\mathfrak{u}\mathfrak{v}} \\
&\equiv \begin{bmatrix} \widetilde{N(\mathfrak{u}\mathfrak{v})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(\mathfrak{b}\mathfrak{d})\omega_1 x_{\mathfrak{a},\mathfrak{b}} x_{\mathfrak{c},\mathfrak{d}} \\ N(\mathfrak{b}\mathfrak{d})\omega_2 x_{\mathfrak{a},\mathfrak{b}} x_{\mathfrak{c},\mathfrak{d}} \end{bmatrix} \pmod{MG\mathfrak{u}\mathfrak{v}} \\
&\equiv \begin{bmatrix} \widetilde{N(\mathfrak{u}\mathfrak{v})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(\mathfrak{b}\mathfrak{d})\omega_1 x_{\mathfrak{a}\mathfrak{c},\mathfrak{b}\mathfrak{d}} \\ N(\mathfrak{b}\mathfrak{d})\omega_2 x_{\mathfrak{a}\mathfrak{c},\mathfrak{b}\mathfrak{d}} \end{bmatrix} \pmod{MG\mathfrak{u}\mathfrak{v}} \\
&\equiv \boldsymbol{\xi}_{\mathfrak{u}\mathfrak{v}} \pmod{MG\mathfrak{u}\mathfrak{v}}.
\end{aligned}
$$

Thus

$$\Phi(\Phi([(G,\boldsymbol{\xi})],[\mathfrak{u}]),[\mathfrak{v}]) = \Phi([(G,\boldsymbol{\xi})],[\mathfrak{u}\mathfrak{v}])$$

and the proof is complete. □

The previous theorem shows that Φ defines a right action of $H(\mathfrak{o}_f, M)$ on $\overline{\mathscr{A}}(M,\delta f^2)$. This is an extremely valuable feature that we will exploit in results to come.

We will now extend the previous construction slightly. Let f_0 be a divisor of f such that $\gcd(f_0, M) = 1$. Then for $[(G,\boldsymbol{\xi})] \in \overline{\mathscr{A}}(M,\delta f^2)$ with

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

and $\mathfrak{u} = \mathfrak{a}\mathfrak{b}^{-1} \in A(\mathfrak{o}_{f/f_0}, M)$ we define $\phi_{f_0}([(G,\boldsymbol{\xi})],\mathfrak{u}) = [(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}})]$ where $\boldsymbol{\xi}_{\mathfrak{u}}$ is any basis of $G\mathfrak{u}$ such that

$$\boldsymbol{\xi}_{\mathfrak{u}} = \begin{bmatrix} f_0^{-1}\widetilde{N(\mathfrak{u})} & \\ & 1 \end{bmatrix} \begin{bmatrix} N(\mathfrak{b})\omega_1 x_{\mathfrak{a},\mathfrak{b}} \\ N(\mathfrak{b})\omega_2 x_{\mathfrak{a},\mathfrak{b}} \end{bmatrix} \pmod{MG\mathfrak{u}}$$

where, again, $x_{\mathfrak{a},\mathfrak{b}} \in \mathfrak{u}$ is such that $N(\mathfrak{b})x_{\mathfrak{a},\mathfrak{b}} \equiv 1 \pmod{M\mathfrak{o}_{f/f_0}}$. Notice, again, that

$$\frac{1}{(f/f_0)\sqrt{\delta}N(G\mathfrak{u})}(f_0^{-1}\widetilde{N(\mathfrak{u})}\omega_1\overline{\omega_2}|x_{\mathfrak{a},\mathfrak{b}}|^2 - f_0^{-1}\widetilde{N(\mathfrak{u})}\overline{\omega_1}\omega_2|x_{\mathfrak{a},\mathfrak{b}}|^2) \equiv 1 \pmod{M}$$

Hence $[(G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{u}})] \in \overline{\mathscr{A}}(M, \delta(f/f_0)^2)$. Slight modifications to the previous propositions allow one to show that $\phi^*_{f_0}$ is a well-defined map, thus inducing a well-defined pairing

$$\Phi^*_{f_0} : \overline{\mathscr{A}}(M, \delta f^2) \times H(\mathfrak{o}_{f/f_0}, M) \to \overline{\mathscr{A}}(M, \delta(f/f_0)^2).$$

Proposition 5.4.6 also generalizes here and the proof is essentially identical.

Proposition 5.4.7. *Let* $[(G, \boldsymbol{\xi})] \in \overline{\mathscr{A}}(M, \delta f^2)$*, let* f_0 *be a divisor of* f *such that* $\gcd(f_0, M)$*, and let* f_1 *be a divisor of* f/f_0 *such that* $\gcd(f_1, M) = 1$*. For* $[\mathfrak{u}] \in H(\mathfrak{o}_{f/f_0}, M)$ *and* $[\mathfrak{v}] \in H(\mathfrak{o}_{f/(f_0 f_1)}, M)$ *we have*

$$\Phi_{f_1}(\Phi_{f_0}([(G, \boldsymbol{\xi})], [\mathfrak{u}]), [\mathfrak{v}]) = \Phi_{f_0 f_1}([(G, \boldsymbol{\xi})], [\mathfrak{u}\mathfrak{v}]).$$

Proof. The argument is similar to that appearing in the proof of Proposition 5.4.6. □

Putting everything together we obtain the following theorem.

Theorem 5.4.8. *Let* f_0 *be a divisor of* f *such that* $\gcd(f_0, M) = 1$*. The map* $\Phi_{f_0} : \overline{\mathscr{A}}(M, \delta f^2) \times H(\mathfrak{o}_{f/f_0}, M) \to \overline{\mathscr{A}}(M, \delta(f/f_0)^2)$ *establishes a well-defined pairing between the group* $H(\mathfrak{o}_{f/f_0}, M)$ *and the set* $\overline{\mathscr{A}}(M, \delta f^2)$*. Moreover, for fixed* $[\mathfrak{u}] \in H(\mathfrak{o}_{f/f_0}, M)$ *the map*

$$\Phi_{f_0}(\cdot, [\mathfrak{u}]) : \overline{\mathscr{A}}(M, \delta f^2) \to \overline{\mathscr{A}}(M, \delta(f/f_0)^2)$$

is a surjection. Finally, all of the pairings are compatible in the sense that the diagram

$$\begin{array}{ccc} \overline{\mathscr{A}}(M, \delta f^2) \times H(\mathfrak{o}_{f/f_0}, M) \times H(\mathfrak{o}_{f/f_1}, M) & \longrightarrow & \overline{\mathscr{A}}(M, \delta(f/f_1)^2) \times H(\mathfrak{o}_{f/f_0}, M) \\ \downarrow & & \downarrow \\ \overline{\mathscr{A}}(M, \delta(f/f_0)^2) \times H(\mathfrak{o}_{f/f_1}, M) & \longrightarrow & \overline{\mathscr{A}}(M, \delta(f/(f_0 f_1))^2). \end{array}$$

commutes for divisors f_0 *of* f *and* f_1 *of* f/f_0 *such that and* $\gcd(f_0 f_1, M) = 1$*. In particular, the group* $H(\mathfrak{o}_f, M)$ *acts on* $\overline{\mathscr{A}}(M, \delta f^2)$ *as a group of automorphisms.*

Proof. The first and third parts of the theorem have already been proved. We prove that for fixed $[\mathfrak{u}] \in H(\mathfrak{o}_{f/f_0}, M)$ the map $\Phi_{f_0}(\cdot, [\mathfrak{u}])$ is a surjection. First we will prove the claim with $[\mathfrak{u}] = [\mathfrak{o}_{f/f_0}]$. Note that the map $[\mathfrak{v}] \mapsto [\mathfrak{o}_{f/f_0}\mathfrak{v}]$ is a surjective map from $H(\mathfrak{o}_f, M)$ to $H(\mathfrak{o}_{f/f_0}, M)$ (see [13]). Let $[(G', \boldsymbol{\xi}')] \in \overline{\mathscr{A}}(M, \delta(f/f_0)^2)$ and write

$$\boldsymbol{\xi}' = \begin{bmatrix} \omega'_1 \\ \omega'_2 \end{bmatrix}.$$

It is clear that

$$\boldsymbol{\xi}' \equiv \begin{bmatrix} \widetilde{f_0^{-1}}(f_0\omega_1') \\ \omega_2' \end{bmatrix} \pmod{MG'}.$$

Consider the full module $[(G, \boldsymbol{\xi})]$ with

$$\boldsymbol{\xi} = \begin{bmatrix} f_0\omega_1' \\ \omega_2' \end{bmatrix}.$$

Then $[(G, \boldsymbol{\xi})] \in \overline{\mathscr{A}}(M, \delta f^2)$ by Proposition 5.1.12 as $N(G) = N(G')$ and

$$\frac{1}{f\sqrt{\delta}N(G)}\det\begin{bmatrix} f_0\omega_1' & \omega_2' \\ f_0\overline{\omega_1'} & \overline{\omega_2'} \end{bmatrix} = \frac{1}{(f/f_0)\sqrt{\delta}N(G')}\det\begin{bmatrix} \omega_1' & \omega_2' \\ \overline{\omega_1'} & \overline{\omega_2'} \end{bmatrix} = 1$$

Thus

$$\begin{aligned} \Phi_{f_0}([(G, \boldsymbol{\xi})], [\mathfrak{o}_{f/f_0}]) &= [(G\mathfrak{o}_{f/f_0}, \boldsymbol{\xi}_{\mathfrak{o}_{f/f_0}})] \\ &= [(G', \boldsymbol{\xi}')] \end{aligned}$$

proving the surjectivity of $\Phi_{f_0}(\cdot, [\mathfrak{o}_{f/f_0}])$. To prove the general statement we let $[\mathfrak{u}_0] \in H(\mathfrak{o}_f, M)$ such that $[\mathfrak{u}^{-1}] = [\mathfrak{o}_{f/f_0}\mathfrak{u}_0]$. Then for some $\gamma = a_1/a_2 \in K$ with $a_1, a_2 \equiv 1 \pmod{M\mathfrak{o}_{f/f_0}}$ we have $\mathfrak{o}_{f/f_0}\mathfrak{u}_0 = \gamma\mathfrak{u}^{-1}$. Hence

$$\begin{aligned} \Phi_{f_0}([(G\mathfrak{u}_0, \boldsymbol{\xi}_{\mathfrak{u}_0})], [\mathfrak{u}]) &= [(G\mathfrak{u}_0\mathfrak{u}, (\boldsymbol{\xi}_{\mathfrak{u}_0})_{\mathfrak{u}})] \\ &= [(G\mathfrak{o}_{f/f_0}\mathfrak{u}_0\mathfrak{u}, (\boldsymbol{\xi}_{\mathfrak{u}_0})_{\mathfrak{o}_{f/f_0}\mathfrak{u}})] \\ &= [(G\gamma\mathfrak{u}^{-1}\mathfrak{u}, (\boldsymbol{\xi}_{\gamma\mathfrak{u}^{-1}})_{\mathfrak{u}})] \\ &= [(\gamma G\mathfrak{o}_{f/f_0}, \gamma\boldsymbol{\xi}_{\mathfrak{o}_{f/f_0}})] \\ &= [(\gamma G', \gamma\boldsymbol{\xi}')] \\ &= [(G', \boldsymbol{\xi}')] \end{aligned}$$

proving the surjectivity of $\Phi_{f_0}(\cdot, [\mathfrak{u}])$ and completing the proof. □

Corollary 5.4.9. *The group $H(\mathfrak{o}_f, M)$ acts on the set $\Gamma_0(M) \setminus A(M, \delta f^2)$ as a group of automorphisms.*

5.5 Some Useful Operators

Here we will introduce some operators that will become very involved in our analysis later of the Fourier coefficients of Siegel paramodular forms. Let $M \geq 1$ be an integer and let $\mathcal{B}(M)$ denote the vector space of complex-valued functions defined on the set $A(M)$ which are constant on equivalence classes modulo $\Gamma_0(M)$. For

$$S = \begin{bmatrix} Mr & t/2 \\ t/2 & s \end{bmatrix} \in A(M)$$

we let $e(S) = \gcd(Mr, t, s)$. We consider also the subset

$$P(M) = \{S \in A(M) : S > 0 \text{ and } e(S)^{-1}S \in A(M)\}.$$

It is simple to check that $P(M)$ is invariant under the action of $\Gamma_0(M)$. Let

$$g = \begin{bmatrix} a & b \\ cM & d \end{bmatrix} \in M(2, \mathbb{Z})$$

be such that $\gcd(\det(g), M) = 1$. Let

$$\Gamma_0(M)g\Gamma_0(M) = \bigsqcup_{i=1}^{N} g_i\Gamma_0(M),$$

and define for $\rho \in \mathcal{B}(M)$

$$(T(\Gamma_0(M)g\Gamma_0(M))\rho)(S) = \sum_{i=1}^{N} \rho({}^tg_iSg_i).$$

The following proposition is immediately apparent.

Proposition 5.5.1. *The operator $T(\Gamma_0(M)g\Gamma_0(M))$ does not depend on the choice of the representatives in the double coset decomposition for $\Gamma_0(M)g\Gamma_0(M)$. Furthermore, the operator maps $\mathcal{B}(M)$ to itself.*

Definition 5.5.2. *Let $m \in \mathbb{N}$ with $\gcd(m, M) = 1$ and let $\rho \in \mathcal{B}(M)$. We define the* ***diagonal down operator*** *$\Delta^-(m) : \mathcal{B}(M) \to \mathcal{B}(M)$ by*

$$(\Delta^-(m)\rho)(S) = \begin{cases} \rho(m^{-1}S) & \text{if } m^{-1}S \in A(M), \\ 0 & \text{if } m^{-1}S \notin A(M). \end{cases}$$

We define the ***diagonal up operator*** *$\Delta^+(m) : \mathcal{B}(M) \to \mathcal{B}(M)$ by*

$$(\Delta^+(m)\rho)(S) = \rho(mS).$$

Lastly, we define the ***diagonal operator*** *$\Delta(m) : \mathcal{B}(M) \to \mathcal{B}(M)$ by*

$$(\Delta(m)\rho)(S) = \left(T\left(\Gamma_0(M)\begin{bmatrix} 1 & 0 \\ 0 & m \end{bmatrix}\Gamma_0(M)\right)(\Delta^-(m)\rho)\right)(S).$$

We note that for a prime p not dividing M and for $\beta \geq 0$, the set of matrices

$$R(p^\beta) \begin{bmatrix} 1 & 0 \\ 0 & p^\beta \end{bmatrix}$$

form a complete set of representatives of the right cosets contained in the double coset

$$\Gamma_0(M) \begin{bmatrix} 1 & 0 \\ 0 & p^\beta \end{bmatrix} \Gamma_0(M).$$

It then follows that for $\rho \in \mathcal{B}(M)$,

$$(\Delta(p^\beta)\rho)(S) = \sum_{U \in R(p^\beta)} (\Delta^-(p^\beta)\rho) \left(\begin{bmatrix} 1 & 0 \\ 0 & p^\beta \end{bmatrix} {}^t U S U \begin{bmatrix} 1 & 0 \\ 0 & p^\beta \end{bmatrix} \right).$$

Let $\mathcal{B}'(M)$ denote the space of complex-valued functions defined on

$$\mathbb{N} \times \bigcup_{\substack{\delta<0, f \in \mathbb{N} \\ \delta \text{ fund. disc.}}} \mathscr{A}(M, \delta f^2)$$

satisfying the condition

$$\rho'(m, (G_1, \boldsymbol{\xi}_1)) = \rho'(m, (G_2, \boldsymbol{\xi}_2))$$

if $[(G_1, \boldsymbol{\xi}_1)] = [(G_2, \boldsymbol{\xi}_2)]$ and G_1 and G_2 are contained in the same field K. In light of the correspondence between equivalence classes of positive-definite, primitive, integral binary quadratic forms of discriminant δf^2 modulo $\Gamma_0(M)$ and equivalence classes of full modules with ring of coefficients $\mathfrak{o}_f$ modulo $\Gamma_0(M)$, we can interpret functions in $\mathcal{B}'(M)$ as being obtained from functions in $\mathcal{B}(M)$. We associate to $\rho \in \mathcal{B}(M)$ the function $\rho' \in \mathcal{B}'(M)$ given by

$$\rho'(m_0, (G, \boldsymbol{\xi})) = \rho(m_0 S_{(G,\boldsymbol{\xi})}). \tag{5.3}$$

It follows from Propositions 5.3.1 and 5.3.2 that this association is well-defined.

Proposition 5.5.3. *Consider the map $\mathcal{B}(M) \to \mathcal{B}'(M)$ given by $\rho \mapsto \rho'$ if*

$$\rho'(m_0, (G, \boldsymbol{\xi})) = \rho(m_0 S_{(G,\boldsymbol{\xi})})$$

for all $m_0 \in \mathbb{N}$ and $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$. Then θ defines a surjection from $\mathcal{B}(M)$ to $\mathcal{B}'(M)$.

Proof. Let $\rho' \in \mathcal{B}'(M)$. We want to construct $\rho \in \mathcal{B}(M)$ such that ρ' is the image of ρ under the map from $\mathcal{B}(M) \to \mathcal{B}'(M)$. For $m_0 \in \mathbb{N}$ and $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$ we have

$$m_0 S_{(G,\boldsymbol{\xi})} \in P(M).$$

Furthermore, for $S \in P(M)$,

$$S = e(S)S', \ \ S' \in A(M, \delta f^2),$$

we have $(G_{S'}, \boldsymbol{\xi}_{S'}) \in \mathscr{A}(M, \delta f^2)$. By Lemma 5.1.20 every full module in $\mathscr{A}(M, \delta f^2)$ can be obtained in this way. We thus define $\rho : A(M) \to \mathbb{C}$ by

$$\rho(S) = \begin{cases} \rho'(e(S), (G_{S'}, \boldsymbol{\xi}_{S'})) & \text{if } S \in P(M), \\ 0 & \text{if } S \notin P(M). \end{cases}$$

It is clear that $\rho \in \mathcal{B}(M)$ and it follows the ρ maps to ρ'. □

We can now define how the diagonal down, diagonal up, and diagonal operators act on functions in $\mathcal{B}'(M)$. We start with $m, m_0 \in \mathbb{N}$ with $\gcd(m, M) = 1$ and $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$. The diagonal up and diagonal down operators are defined for $\rho' \in \mathcal{B}'(M)$ as

$$(\Delta^-(m)\rho')(m_0, (G, \boldsymbol{\xi})) = \begin{cases} \rho'(m_0/m, (G, \boldsymbol{\xi})) & \text{if } m | m_0, \\ 0 & \text{if } m \nmid m_0, \end{cases}$$

and

$$(\Delta^+(m)\rho')(m_0, (G, \boldsymbol{\xi})) = \rho'(m_0 m, (G, \boldsymbol{\xi})).$$

We define for

$$\Gamma_0(M) g \Gamma_0(M) = \bigsqcup_{i=1}^{N} g_i \Gamma_0(M), \ \ g = \begin{bmatrix} a & b \\ cM & d \end{bmatrix} \in M(2, \mathbb{Z})$$

with $\gcd(\det(g), M) = 1$ and $\rho' \in \mathcal{B}'(M)$,

$$(T(\Gamma_0(M) g \Gamma_0(M))\rho')(m_0, (G, \boldsymbol{\xi})) = \sum_{i=1}^{N} \rho'(m_0 e({}^t g_i S_{(G,\boldsymbol{\xi})} g_i), (G_{S_i}, \boldsymbol{\xi}_{S_i}))$$

where S_i is the positive-definite, primitive, integral binary quadratic form

$$\frac{1}{e({}^t g_i S_{(G,\boldsymbol{\xi})} g_i)} {}^t g_i S_{(G,\boldsymbol{\xi})} g_i.$$

A computation shows that the above form is an element of $A(M)$.

The next theorem establishes that the definitions of the above operators on $\rho' \in \mathcal{B}'(M)$ are compatible with the surjection from $\mathcal{B}(M)$ to $\mathcal{B}'(M)$.

Theorem 5.5.4. *Let $M \geq 1$ be an integer. Let $m, m_0 \in \mathbb{N}$ with $\gcd(m, M) = 1$. Let*

$$g = \begin{bmatrix} a & b \\ cM & d \end{bmatrix} \in M(2, \mathbb{Z})$$

with $\gcd(\det(g), M) = 1$. Let $S = e(S)S' \in P(M)$ and let $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$ be the full module associated to S'. Then we have the following equalities for $\rho \in \mathcal{B}(M)$:

$$(\Delta^-(m)\rho)' = \Delta^-(m)\rho',$$
$$(\Delta^+(m)\rho)' = \Delta^+(m)\rho',$$
$$(T(\Gamma_0(M)g\Gamma_0(M))\rho)' = T(\Gamma_0(M)g\Gamma_0(M))\rho'$$

where

$$g = \begin{bmatrix} a & b \\ cM & d \end{bmatrix} \in M(2, \mathbb{Z})$$

with $\gcd(\det(g), M) = 1$.

Proof. We prove the first formula. We have for $m_0 \in \mathbb{N}$ and $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$

$$\begin{aligned}
(\Delta^-(m)\rho)'(m_0, (G, \boldsymbol{\xi})) &= (\Delta^-(m)\rho)(m_0 S_{(G,\boldsymbol{\xi})}) \\
&= \begin{cases} \rho((m_0/m)S_{(G,\boldsymbol{\xi})}) & \text{if } m | m_0, \\ 0 & \text{if } m \nmid m_0, \end{cases} \\
&= \begin{cases} \rho'(m_0/m, (G, \boldsymbol{\xi})) & \text{if } m | m_0, \\ 0 & \text{if } m \nmid m_0, \end{cases} \\
&= (\Delta^-(m)\rho')(m_0, (G, \boldsymbol{\xi})).
\end{aligned}$$

The second formula is proved similarly. We now prove the third formula. Let

$$\Gamma_0(M)g\Gamma_0(M) = \bigsqcup_{i=1}^{N} g_i \Gamma_0(M)$$

We have for $m_0 \in \mathbb{N}$ and $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$

$$\begin{aligned}
(T(\Gamma_0(M)g\Gamma_0(M))\rho)'(m_0, (G, \boldsymbol{\xi})) &= (T(\Gamma_0(M)g\Gamma_0(M))\rho)(m_0 S_{(G,\boldsymbol{\xi})}) \\
&= \sum_{i=1}^{N} \rho(m_0 {}^t g_i S_{(G,\boldsymbol{\xi})} g_i) \\
&= \sum_{i=1}^{N} \rho'(m_0 e({}^t g_i S_{(G,\boldsymbol{\xi})} g_i), (G_{S_i}, \boldsymbol{\xi}_{S_i})) \\
&= (T(\Gamma_0(M)g\Gamma_0(M))\rho')(m_0, (G, \boldsymbol{\xi})).
\end{aligned}$$

This completes the proof of the theorem. $\square$

We can then define the diagonal operator on elements $\rho' \in \mathcal{B}'(M)$. We have for $m \in \mathbb{N}$ with $\gcd(m, M) = 1$, $m_0 \in \mathbb{N}$, and $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$

$$(\Delta(m)\rho')(m_0, (G, \boldsymbol{\xi})) = \left(T \left(\Gamma_0(M) \begin{bmatrix} 1 & 0 \\ 0 & m \end{bmatrix} \Gamma_0(M) \right) (\Delta^-(m)\rho') \right) (m_0, (G, \boldsymbol{\xi})).$$

In particular, for a prime p not dividing M and for $\beta \geq 0$,

$$(\Delta(p^\beta)\rho')(m_0, (G, \boldsymbol{\xi})) = \sum_{U \in R(p^\beta)} (\Delta^-(p^\beta)\rho') \left(m_0 e \left(\begin{bmatrix} 1 & 0 \\ 0 & p^\beta \end{bmatrix} {}^t U S_{(G,\boldsymbol{\xi})} U \begin{bmatrix} 1 & 0 \\ 0 & p^\beta \end{bmatrix} \right), (G_{S(U)}, \boldsymbol{\xi}_{S(U)}) \right)$$

where $S(U)$ is the positive-definite, primitive, integral binary quadratic form

$$\frac{1}{e\left(\begin{bmatrix} 1 & 0 \\ 0 & p^\beta \end{bmatrix} {}^t U S_{(G,\boldsymbol{\xi})} U \begin{bmatrix} 1 & 0 \\ 0 & p^\beta \end{bmatrix} \right)} \begin{bmatrix} 1 & 0 \\ 0 & p^\beta \end{bmatrix} {}^t U S_{(G,\boldsymbol{\xi})} U \begin{bmatrix} 1 & 0 \\ 0 & p^\beta \end{bmatrix}.$$

Theorem 5.5.5. *Let $M \geq 1$ be an integer. Let $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$ with*

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

and let p be a prime not dividing Mf. Then for all $\beta \geq 1$, for all $m_0 \in \mathbb{N}$ with $\gcd(m_0, p) = 1$, and for all $\rho' \in \mathcal{B}'(M)$ we have

(i) if $p\mathfrak{o}_f = \mathfrak{p}\overline{\mathfrak{p}}$ where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are the two distinct prime ideals of $\mathfrak{o}_f$ of norm p, then

$$(\Delta(p^\beta)\rho')(m_0, (G, \boldsymbol{\xi})) = \rho'(m_0, (G\mathfrak{p}^\beta, \boldsymbol{\xi}_{\mathfrak{p}^\beta})) + \rho'(m_0, (G\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{\overline{\mathfrak{p}}^\beta})),$$

(ii) if $p\mathfrak{o}_f = \mathfrak{p}^2$ where $\mathfrak{p}$ is the unique prime ideal of $\mathfrak{o}_f$ of norm p, then

$$(\Delta(p^\beta)\rho')(m_0, (G, \boldsymbol{\xi})) = \begin{cases} \rho'(m_0, (G\mathfrak{p}, \boldsymbol{\xi}_{\mathfrak{p}})) & \text{if } \beta = 1, \\ 0 & \text{if } \beta > 1, \end{cases}$$

(iii) if $p\mathfrak{o}_f = \mathfrak{p}$ is a prime ideal of $\mathfrak{o}_f$, then

$$(\Delta(p^\beta)\rho')(m_0, (G, \boldsymbol{\xi})) = 0,$$

where $\boldsymbol{\xi}_{\mathfrak{p}^\beta}$ is given by equation 5.2.

Proof. Let $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$. Without loss of generality, we may assume that $\boldsymbol{\xi}$ is of the form

$$\begin{bmatrix} Mr \\ \dfrac{t - f\sqrt{\delta}}{2} \end{bmatrix}.$$

Let

$$S = S_{(G,\boldsymbol{\xi})} = \begin{bmatrix} Mr & t/2 \\ t/2 & s \end{bmatrix}.$$

For $U \in \Gamma_0(M)$ we set

$${}^tUSU = \begin{bmatrix} Mr_U & t_U/2 \\ t_U/2 & s_U \end{bmatrix} = S_U.$$

Before we prove the three statements we show that, for fixed β, there is a bijection between the sets

$$T_1(p^\beta) = \{U \in R(p^\beta) : r_U \equiv 0 \pmod{p^\beta}\}$$

and

$$T_2(p^\beta) = \{\mathfrak{u} \in A(\mathfrak{o}_f, M) : \mathfrak{u} \subset \mathfrak{o}_f \text{ and } N(\mathfrak{u}) = p^\beta\}.$$

Since regular, integral ideals of $\mathfrak{o}_f$ with norm prime to f can be factored uniquely into a product of prime ideals of $\mathfrak{o}_f$, $T_2(p^\beta)$ consists of elements of the form $\mathfrak{p}^i\overline{\mathfrak{p}}^j$, $i + j = \beta$, where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are prime ideals in $\mathfrak{o}_f$ of norm p (it is possible $\mathfrak{p} = \overline{\mathfrak{p}}$). Let's assume that $T_1(p^\beta)$ is non-empty. Let $U \in T_1(p^\beta)$ and consider the full module $\mathfrak{u}(U)$ with basis

$$\begin{bmatrix} p^\beta \\ \dfrac{t_U - f\sqrt{\delta}}{2} \end{bmatrix}.$$

We show that the norm of $\mathfrak{u}(U)$ is $N(\mathfrak{u}(U)) = p^\beta$ and, more importantly, that $\mathfrak{u}(U) \in T_2(p^\beta)$. The element

$$\frac{t_U - f\sqrt{\delta}}{2p^\beta}$$

is a root of the polynomial

$$\varphi(z) = p^\beta z^2 - t_U z + Mp^{-\beta} r_U s_U.$$

We then split into two cases, $p|\delta$ and $p \nmid \delta$. Assume that $p \nmid \delta$. Then $p \nmid t_U$, and it follows that the coefficients of φ are relatively prime. Hence, by Proposition 5.1.16, we have that $N(\mathfrak{u}(U)) = p^\beta$.

It follows that $\mathfrak{u}(U)$ is an element of $T_2(p^\beta)$. Now assume that $p|\delta$. Then $p|t_U$. We prove that $p \nmid Mp^{-\beta}r_U s_U$. Suppose $p = 2$. Then $\delta = 4\delta_0$ with $\delta_0 \equiv 2, 3 \pmod 4$. Let $t_U = 2t'_U$. Then

$$\delta f^2 = 4\delta_0 f^2 = 4((t'_U)^2 - Mr_U s_U)$$

and hence

$$Mr_U s_U = (t'_U)^2 - \delta_0 f^2 \equiv (t'_U)^2 - \delta_0 \pmod 4.$$

Since $(t'_U)^2 \equiv 0, 1 \pmod 4$ and $\delta_0 \equiv 2, 3 \pmod 4$ it follows that $Mr_U s_U$ is not divisible by 4. This implies that $\beta = 1$ and $M2^{-1}r_U s_U$ is odd. It then follows that the coefficients of φ are relatively prime and the norm of $\mathfrak{u}(U)$ is $N(\mathfrak{u}(U)) = 2$, implying that $\mathfrak{u}(U)$ is an element of $T_2(2)$. Now suppose $p \neq 2$. We have the congruence

$$\delta f^2 \equiv 4Mr_U s_U \pmod{p^2}.$$

Since δ is not divisible by p^2, we conclude that $Mr_U s_U$ is not divisible by p^2. This implies that $\beta = 1$ and $Mp^{-1}r_U s_U$ is not divisible by p. Hence, by Proposition 5.1.16, the norm of $\mathfrak{u}(U)$ is $N(\mathfrak{u}(U)) = p$ and thus $\mathfrak{u} \in T_2(p)$. From what we have shown above, there is a map $\mathfrak{u} : T_1(p^\beta) \to T_2(p^\beta)$.

We show that this map is an injection. Given $U, V \in T_1(p^\beta)$ with $\mathfrak{u}(U) = \mathfrak{u}(V)$, we have

$$r_U \equiv r_V \equiv \frac{t_U - t_V}{2} \equiv 0 \pmod{p^\beta}.$$

We prove that $U = V$. Since ${}^tUSU = S_U$ and ${}^tVSV = S_V$ we have

$$\begin{aligned} S_V &= {}^tVSV \\ &= {}^tV({}^tU^{-1}S_U U^{-1})V \\ &= {}^t(U^{-1}V)S_U(U^{-1}V). \end{aligned}$$

Write

$$U^{-1}V = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Then

$$Mr_V = Mr_U a^2 + t_U ac + s_U c^2 \equiv t_U ac + s_U c^2 \equiv 0 \pmod{p^\beta}.$$

Moreover, we have that

$$\frac{t_U - t_V}{2} = \frac{t_U - 2Mr_U ab - 2s_U cd - 2t_U bc - t_U}{2} = -Mr_U ab - s_U cd - t_U bc \equiv s_U cd + t_U bc \equiv 0 \pmod{p^\beta}.$$

Manipulating the above system of congruences we can show that

$$ct_U \equiv 0 \pmod{p^\beta} \text{ and } cs_U \equiv 0 \pmod{p^\beta}.$$

Hence c is divisible by p^β. It follows that $U^{-1}V \in \Gamma_0(Mp^\beta)$ and thus $U = V$.

We now compute the image of $\mathfrak{u} : T_1(p^\beta) \to T_2(p^\beta)$. Assume that U and V are distinct elements of $T_1(p^\beta)$. We show that

$$\mathfrak{u}(U) + \mathfrak{u}(V) = \mathfrak{o}_f.$$

It suffices to prove that

$$\gcd\left(\frac{t_U - t_V}{2}, p\right) = 1.$$

Assume that the greatest common divisor is p. We then have that the bases

$$\begin{bmatrix} p \\ \frac{t_U - f\sqrt{\delta}}{2} \end{bmatrix} \text{ and } \begin{bmatrix} p \\ \frac{t_V - f\sqrt{\delta}}{2} \end{bmatrix}$$

define the same module $\mathfrak{v}$. Since $t_U^2 \equiv \delta f^2 \pmod{4p^\beta}$ and $t_V^2 \equiv \delta f^2 \pmod{4p^\beta}$ we have that

$$\left(\frac{t_U + t_V}{2}\right)\left(\frac{t_U - t_V}{2}\right) \equiv 0 \pmod{p^\beta}.$$

Assume that p divides the first factor on the left in the above congruence. It follows that $p|t_U$. If $\beta > 1$, then this would imply $p|f$ which is false. So $\beta = 1$. But this is a contradiction since, in this case, we would have $\mathfrak{u}(U) = \mathfrak{u}(V)$ with $U \neq V$.

We then conclude that $p^\beta|[(t_U - t_V)/2]$. But then $\mathfrak{u}(U) = \mathfrak{u}(V)$ with $U \neq V$. This is also a contradiction and thus the greatest common divisor of $(t_U - t_V)/2$ and p is 1. Our claim then follows.

We now proceed with the proof of the theorem. We start by proving (i). In this case $\mathfrak{u}(T_1(p^\beta)) = \{\mathfrak{p}^\beta, \overline{\mathfrak{p}}^\beta\}$. Suppose that $U, V \in T_1(p^\beta)$ correspond to $\mathfrak{p}^\beta$ and $\overline{\mathfrak{p}}^\beta$ respectively. Then, upon applying $\Delta(p^\beta)$ to ρ', we obtain

$$(\Delta(p^\beta)\rho')(m_0, (G, \boldsymbol{\xi})) = \rho'\left(m_0, \left(G_{S(U)}, \begin{bmatrix} Mr_U p^{-\beta} \\ \frac{t_U - f\sqrt{\delta}}{2} \end{bmatrix}\right)\right) + \rho'\left(m_0, \left(G_{S(V)}, \begin{bmatrix} Mr_V p^{-\beta} \\ \frac{t_V - f\sqrt{\delta}}{2} \end{bmatrix}\right)\right)$$

where $\mathfrak{u}(U) = \mathfrak{p}^\beta$ and $\mathfrak{u}(V) = \overline{\mathfrak{p}}^\beta$. We note that by what we have shown $r_U p^{-\beta}$ and $r_V p^{-\beta}$ are not divisible p. It is now simple to check that

$$\left[\left(G_{S(U)}, \begin{bmatrix} Mr_U p^{-\beta} \\ \frac{t_U - f\sqrt{\delta}}{2} \end{bmatrix}\right)\right] = [(G\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{\overline{\mathfrak{p}}^\beta})]$$

and

$$\left[\left(G_{S(V)}, \begin{bmatrix} Mr_V p^{-\beta} \\ \dfrac{t_V - f\sqrt{\delta}}{2} \end{bmatrix}\right)\right] = [(G\mathfrak{p}^{\beta}, \boldsymbol{\xi}_{\mathfrak{p}^{\beta}})]$$

thereby proving (i).

Case (ii) is dealt with similarly. In this case however $\mathfrak{u}(T_1(p)) = \{\mathfrak{p}\}$ and $T_1(p^{\beta}) = \emptyset$ for $\beta > 1$. In case (iii) we have $T_1(p^{\beta}) = \emptyset$ for all $\beta \geq 1$. The claim is proved. □

Theorem 5.5.6. *Let $M \geq 1$ be an integer. Let $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$ with*

$$\boldsymbol{\xi} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

and let p be a prime not dividing M and dividing f. Then for all $m_0 \in \mathbb{N}$ with $\gcd(m_0, p) = 1$ and for all $\rho' \in \mathcal{B}'(M)$ we have

$$(\Delta(p)\rho')(m_0, (G, \boldsymbol{\xi})) = \rho'(m_0 p, (G\mathfrak{o}_{f/p}, \boldsymbol{\xi}_{\mathfrak{o}_{f/p}}))$$

and

$$((\Delta(p)^2 - \Delta(p^2) - 1)\rho')(m_0, (G, \boldsymbol{\xi})) = 0.$$

Proof. As in the proof of the previous theorem we start with $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$ with $\boldsymbol{\xi}$ of the form

$$\begin{bmatrix} Mr \\ \dfrac{t - f\sqrt{\delta}}{2} \end{bmatrix}$$

and let

$$S = S_{(G,\boldsymbol{\xi})} = \begin{bmatrix} Mr & t/2 \\ t/2 & s \end{bmatrix}.$$

Since $p|f$ the congruence

$$z^2 \equiv \delta f^2 \pmod{4p}$$

has a solution. According to a theorem in [7] (see Theorem 7, pg. 145), there exists $U \in R(p)$ such that $r_U \equiv 0 \pmod{p}$. In fact, such a U is unique. We prove this claim. Let $V \in R(p)$ such that $r_V \equiv 0 \pmod{p}$. We will prove $U = V$. Since $p|f$ we have that $p|t_U$ and hence $p \nmid s_U$. With ${}^tUSU = S_U$ and ${}^tVSV = S_V$ we have

$$S_V = {}^t(U^{-}V)S_U(U^{-1}V).$$

We write

$$U^{-1}V = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

We then have the congruence

$$Mr_V = Mr_U a^2 + t_U ac + s_U c^2 \equiv t_U ac + s_U c^2 \equiv s_U c^2 \equiv 0 \pmod{p}.$$

Thus $p|c$ and hence $U = V$.

We now prove that $p|Mp^{-1}r_U s_U$. Suppose $p = 2$. Then the congruence $\delta \equiv 0, 1 \pmod 4$ implies that

$$\delta f^2 = t_U^2 - 4Mr_U s_U \equiv 0, 4 \pmod{16}.$$

Thus $(t_U/2)^2 - Mr_U s_U \equiv 0, 1 \pmod 4$. Since $Mr_U s_U$ is even, it follows that $Mr_U s_U \equiv 0 \pmod 4$. Hence $M2^{-1}r_U s_U \equiv 0 \pmod 2$. Now suppose that $p \neq 2$. We have the congruence

$$\delta f^2 \equiv -4Mr_U s_U \pmod{p^2}$$

and it follows fairly readily that $p|Mp^{-1}r_U s_U$.

We now consider the element

$$\frac{t_U - f\sqrt{\delta}}{2p}.$$

This number is a root of the polynomial

$$\varphi(z) = z^2 - (t_U/p)z + Mp^{-2}r_U s_U$$

and thus the full module generated by the basis

$$\begin{bmatrix} p \\ \dfrac{t_U - f\sqrt{\delta}}{2} \end{bmatrix}$$

has ring of coefficients $\mathfrak{o}_{f/p}$ by Proposition 5.1.16. Write

$$\frac{1}{p}\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} S_U \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} = pS(U)'$$

where $S(U)'$ is a primitive and integral binary quadratic form. Then

$$(\Delta(p)\rho')(m_0, (G, \boldsymbol{\xi})) = \rho'\left(m_0 p, \left(G_{S(U)'}, \begin{bmatrix} Mr_U p^{-2} \\ \dfrac{t_U - f\sqrt{\delta}}{2p} \end{bmatrix}\right)\right).$$

It is then simple to check that

$$\left[\left(G_{S(U)'}, \begin{bmatrix} Mr_U p^{-2} \\ \dfrac{t_U - f\sqrt{\delta}}{2p} \end{bmatrix}\right)\right] = [(G_{\mathfrak{o}_{f/p}}, \boldsymbol{\xi}_{\mathfrak{o}_{f/p}})].$$

We now prove the second formula. We consider $S(U)'$ as computed above and use the explicit representation of $R(p^\beta)$ as given in Lemma 4.2.6. First we assume that U is of the form

$$\begin{bmatrix} 1 & 0 \\ Mu & 1 \end{bmatrix}$$

for some $u \in \mathbb{Z}/p\mathbb{Z}$. We then have that

$$Mr_U = Mr + Mtu + M^2su^2 \equiv 0 \pmod{p}.$$

As we also have

$$Mr_U = Mr + Mtu + M^2su^2 \equiv 0 \pmod{p^2}$$

we further have that $p|(t - 2Msu)$. By Hensel's Lemma, we obtain p solutions modulo p^2 to the congruence

$$Mr + Mtv + M^2sv^2 \equiv 0 \pmod{p^2}$$

where $v = u + lp$ for $l = 0, 1, \ldots, p-1$. A direct computation now yields the desired result. A similar argument is made in the case where U is of the form

$$\begin{bmatrix} p & -a_1 \\ M & b_1 \end{bmatrix}$$

where $a_1M + b_1p = 1$. This completes the proof. □

5.6 The Structure of $\Gamma_0(M) \setminus A(M, \delta f^2)$

In this section we break down some of the structures of $\Gamma_0(M) \setminus A(M, \delta f^2)$. To this end, we look briefly at the case $M = 1$ in which case we are considering the class group $\mathrm{SL}(2,\mathbb{Z}) \setminus A(1, \delta f^2)$. Note that we will use the matrix representation of binary quadratic forms in our discussion here. The following definition is from [11].

Definition 5.6.1. *The identity element of the class group* $\mathrm{SL}(2,\mathbb{Z})\backslash A(1, \delta f^2)$ *is called the* ***principal form****.*

If $\delta f^2 = -4D$ with $D > 0$ then the principal form is

$$I^*_{D,0} = \begin{bmatrix} 1 & 0 \\ 0 & D \end{bmatrix}$$

and if $\delta f^2 = -4D + 1$ with $D > 0$ then the principal form is

$$I^*_{D,1} = \begin{bmatrix} 1 & 1/2 \\ 1/2 & D \end{bmatrix}.$$

Fix $M \geq 1$ an integer. We have a decomposition

$$\mathrm{SL}(2,\mathbb{Z}) = \bigsqcup_{i=1}^{m} g_i \Gamma_0(M)$$

where

$$\begin{aligned} m &= [\mathrm{SL}(2,\mathbb{Z}) : \Gamma_0(M)] \\ &= M \prod_{p|M} \left(1 + \frac{1}{p}\right). \end{aligned}$$

It then follows that each class in $\mathrm{SL}(2,\mathbb{Z}) \setminus A(1, \delta f^2)$ partitions into m orbits when considered modulo $\Gamma_0(M)$. In particular, we are interested in those orbits that are contained in $A(M, \delta f^2)$.

Proposition 5.6.2. *Let $S \in A(1, \delta f^2)$ and fix a decomposition*

$$\mathrm{SL}(2,\mathbb{Z}) = \bigsqcup_{i=1}^{m} g_i \Gamma_0(M).$$

Suppose that there exists $g \in \mathrm{SL}(2,\mathbb{Z})$ such that ${}^t g S g \in A(M, \delta f^2)$. Then there exists i with $1 \leq i \leq m$ such that ${}^t g_i S g_i \in A(M, \delta f^2)$.

Proof. Suppose $g \in \mathrm{SL}(2,\mathbb{Z})$ is such that ${}^t g S g \in A(M, \delta f^2)$. For some i with $1 \leq i \leq m$ we have

$$g \in g_i \Gamma_0(M).$$

Hence $g = g_i g_0$ for some $g_0 \in \Gamma_0(M)$. It follows that

$$({}^t g_0^{-1}) {}^t g_0 {}^t g_i S g_i g_0 (g_0)^{-1} = {}^t g_i S g_i \in A(M, \delta f^2).$$

This completes the proof. □

We now ask the question as to when we can ensure there exists a matrix g in $\mathrm{SL}(2,\mathbb{Z})$ such that ${}^t g S g \in A(M, \delta f^2)$ for some fixed $S \in A(1, \delta f^2)$. In general, it is not always the case. However, for certain discriminants, we can indeed identify when every class in $\mathrm{SL}(2,\mathbb{Z}) \setminus A(1, \delta f^2)$ does contain an element in $A(M, \delta f^2)$. The following proposition addresses two such discriminants.

Proposition 5.6.3. *Let $M \geq 1$ be a fixed positive integer and let $f \in \mathbb{N}$ be such that $\delta f^2 = -4M$ or $\delta f^2 = -4M+1$. Then for every $S \in A(1, \delta f^2)$, there exists $S' \in A(M, \delta f^2)$ such that $S' = {}^t gSg$ for some $g \in \mathrm{SL}(2, \mathbb{Z})$.*

Proof. We only prove the claim when $\delta f^2 = -4M$ as the other case is similar. Consider the matrix

$$I_{M,0} = \begin{bmatrix} M & 0 \\ 0 & 1 \end{bmatrix} \in A(M, \delta f^2).$$

If S is equivalent modulo $\mathrm{SL}(2, \mathbb{Z})$ to $I_{M,0}$ then we are done. Assume that this is not the case. Write

$$S = \begin{bmatrix} r & t/2 \\ t/2 & s \end{bmatrix}.$$

We may assume that $\gcd(r, M) = 1$ (see Lemma 2.25, [11]). Now consider the matrix $I^*_{M,0}$. The binary quadratic forms $I_{M,0}$ and $I^*_{M,0}$ are clearly equivalent modulo $\mathrm{SL}(2, \mathbb{Z})$. As $I^*_{M,0}$ is the principal form we have

$$[S][I^*_{M,0}] = [S].$$

Since $[I^*_{M,0}] = [I_{M,0}]$, it follows that the product of the class of S and the class of $I_{M,0}$ is equal to the class of S. A direct computation of $[S][I_{M,0}]$ establishes that $[S]$ contains an element S' with $S' \in A(M, \delta f^2)$. This completes the proof. $\square$

It is possible to by more general here and not restrict to such a narrow set of discriminants. Fix an integer $M \geq 1$. We say a congruence

$$rx^2 + txy + sy^2 \equiv 0 \pmod{M}$$

with $r, t, z \in \mathbb{Z}$ and $\gcd(r, t, s) = 1$ is solvable when there exists a pair (x, y) which satisfies the congruence with x and y relatively prime. We say that two pairs (x_1, y_1), and (x_2, y_2) are equivalent solutions if there exists $a \in (\mathbb{Z}/M\mathbb{Z})^\times$ such that

$$ax_1 \equiv x_2 \pmod{M} \quad \text{and} \quad ay_1 \equiv y_2 \pmod{M}.$$

Proposition 5.6.4. *Let $M \geq 1$ be a positive integer and write*

$$M = \prod_{k=1}^{l} p_k^{e_k}.$$

Let $S(x,y) = rx^2 + txy + sy^2$ *be a positive definite, integral, primitive binary quadratic form of discriminant* δf^2 *with the congruence*

$$rx^2 + txy + sy^2 \equiv 0 \pmod{p_k^{e_k}}$$

solvable for each k *with* $1 \leq k \leq l$. *Then there exists* $g \in \mathrm{SL}(2,\mathbb{Z})$ *such that* ${}^t gSg \in A(M, \delta f^2)$.

Proof. By the Chinese remainder theorem, a solution to the system of congruences

$$rx^2 + txy + sy^2 \equiv 0 \pmod{p_k^{e_k}}, \ 1 \leq k \leq l,$$

lifts to a solution of

$$rx^2 + txy + sy^2 \equiv 0 \pmod{M}.$$

Let (a,c) be such a solution. We can then construct a matrix

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z}).$$

A simple computation shows that ${}^t gSg \in A(M, \delta f^2)$. □

Let $M \geq 1$ be an integer, and fix a decomposition

$$\mathrm{SL}(2,\mathbb{Z}) = \bigsqcup_{i=1}^{m} g_i \Gamma_0(M).$$

Let $S \in A(1, \delta f^2)$ and define the set $J_S = \{i \in \{1,\ldots,m\} : {}^t g_i S g_i \in A(M, \delta f^2)\}$. The last result of this section concerns the size of this set.

Theorem 5.6.5. *Let* $M \geq 1$ *be an integer, let* $S, S' \in A(1, \delta f^2)$, *and fix a decomposition*

$$\mathrm{SL}(2,\mathbb{Z}) = \bigsqcup_{i=1}^{m} g_i \Gamma_0(M).$$

Then $|J_S| = |J_{S'}|$.

Proof. If $M = 1$ then the claim is obvious so we suppose $M > 1$. If S and S' are equivalent modulo $\mathrm{SL}(2,\mathbb{Z})$ then the claim follows trivially. We then suppose that S and S' define distinct classes modulo $\mathrm{SL}(2,\mathbb{Z})$. Write

$$S = \begin{bmatrix} r & t/2 \\ t/2 & s \end{bmatrix} \quad \text{and} \quad S' = \begin{bmatrix} r' & t'/2 \\ t'/2 & s' \end{bmatrix}$$

with $\gcd(r, M) = \gcd(r', M) = 1$. We have that $|J_S|$ is the number of pairs $(x, y) \in \mathbb{P}^1(\mathbb{Z}/M\mathbb{Z})$ that satisfy

$$rx^2 + txy + sy^2 \equiv 0 \pmod{M}.$$

Furthermore, we have that $|J_{S'}|$ is the number of pairs $(x, y) \in \mathbb{P}^1(\mathbb{Z}/M\mathbb{Z})$ that satisfy

$$r'x^2 + t'xy + s'y^2 \equiv 0 \pmod{M}.$$

If $J_S = \emptyset$, then for some prime p dividing M we have

$$rx^2 + txy + sy^2 \equiv 0 \pmod{p^n}$$

is not solvable (here n is the power of p which divides M). Thus $z^2 \equiv \delta f^2 \pmod{4p^n}$ has no solution and hence

$$r'x^2 + t'xy + s'y^2 \equiv 0 \pmod{p^n}$$

is not solvable. Thus $J_{S'} = \emptyset$. This proves that $J_S \neq \emptyset$ if and only if $J_{S'} \neq \emptyset$.

Assume that $J_S \neq \emptyset$. We show that $|J_S| = |J_{S'}|$. Let $[T] \in \mathrm{SL}(2, \mathbb{Z}) \setminus A(1, \delta f^2)$ be such that

$$[S'] = [S][T].$$

Pick a prime p which does not divide M and is represented by the binary quadratic form T. Then $[p\mathfrak{o}_f]$ is an element of both $H(\mathfrak{o}_f, 1)$ and $H(\mathfrak{o}_f, M)$. By Corollary 5.4.9, it follows that $|J_S| = |J_{S'}|$. This completes the proof. $\square$

6 Properties of Fourier Coefficients of Siegel Paramodular Forms

In this chapter we will bring all the previous content together to establish relations on Fourier coefficients for Siegel modular forms for the paramodular group. We will see that in some contexts these relations are purely multiplicative and in other contexts these relations are simply arithmetic.

6.1 Action of Hecke Operators on Fourier Coefficients, $p \nmid M$

Throughout this section we assume that p is a prime not dividing $M \geq 1$. We start by computing the action of the Hecke operators $T(p^{r_0})$ on a Siegel paramodular form of level M. The contructions appearing in chapter 4 allows us to do this without too much difficulty.

Let $F : \mathcal{H}_2 \to \mathbb{C}$ be a Siegel paramodular form of fixed level $M \geq 1$ with weight $k > 0$ and suppose that F has a Fourier expansion given by

$$F(Z) = \sum_{S \in A(M)} a(S) e^{2\pi i \mathrm{tr}(SZ)}.$$

For an integer $r_0 \geq 0$, let $\Lambda_{r_0} = \{(\alpha, \beta, \gamma) \in \mathbb{Z}^3 : \alpha, \beta, \gamma \geq 0, \alpha + \beta + \gamma = r_0\}$. We use equation (4.1) in conjunction with Proposition 4.2.5 and we obtain

$$\begin{aligned}
(T(p^{r_0})(F))(Z) &= p^{r_0(k-3)} \sum_{g \in V(p^{r_0})} F \star_k g \\
&= p^{r_0(k-3)} \sum_{\left[\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right] \in V(p^{r_0})} \left(\sum_{S \in A(M)} a(S) p^{r_0 k} (\det(D))^{-k} e^{2\pi i \mathrm{tr}(S(AZ+B)D^{-1})} \right) \\
&= p^{r_0(2k-3)} \sum_{S \in A(M)} \sum_{\left[\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right] \in V(p^{r_0})} a(S) (\det(D))^{-k} e^{2\pi i \mathrm{tr}(SAZD^{-1})} e^{2\pi i \mathrm{tr}(SBD^{-1})} \\
&= p^{r_0(2k-3)} \sum_{S \in A(M)} \sum_{(\alpha,\beta,\gamma) \in \Lambda_{r_0}} \sum_{\substack{D \in D_{\alpha,\beta} {}^t R(p^\beta) \\ A = p^{r_0} {}^t D^{-1}}} a(S) (\det(D))^{-k} e^{2\pi i \mathrm{tr}(SAZD^{-1})} l_D(S)
\end{aligned}$$

where

$$l_D(S) = \sum_{\substack{B \bmod D \\ {}^t BD = {}^t DB}} e^{2\pi i \mathrm{tr}(SBD^{-1})}$$

This sum for fixed D is called a Gauss sum and can be analyzed separately. The following lemma addresses this sum.

Lemma 6.1.1. *Let*

$$l_D(S) = \sum_{\substack{B \bmod D \\ {}^tBD = {}^tDB}} e^{2\pi i \operatorname{tr}(SBD^{-1})}$$

where $D \in \mathrm{GL}(2, \mathbb{Q}) \cap M(2, \mathbb{Z})$*,* $S \in A(M)$*, and* B *mod* D *is defined as in 4.2.3.*
(i) For any $V \in \mathrm{SL}(2, \mathbb{Z})$*,*

$$l_{DV}(S) = l_D(S).$$

(ii) For $\alpha, \beta \in \mathbb{N}$ *such that* $D = D_{\alpha,\beta}{}^tU$ *with* $U \in R(p^\beta)$*,*

$$l_D(S) = \begin{cases} p^{3\alpha+\beta} & \textit{if } r \equiv t \equiv 0 \pmod{p^\alpha},\ s \equiv 0 \pmod{p^{\alpha+\beta}}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. For $V \in \mathrm{SL}(2, \mathbb{Z})$ we have

$$\begin{aligned} l_{DV}(S) &= \sum_{\substack{B \bmod DV \\ {}^tBDV = {}^tV{}^tDB}} e^{2\pi i \operatorname{tr}(SB(DV)^{-1})} \\ &= \sum_{\substack{BV^{-1} \bmod D \\ {}^t(BV^{-1})D = {}^tD(BV^{-1})}} e^{2\pi i \operatorname{tr}(SBV^{-1}D^{-1})} \\ &= \sum_{\substack{B' \bmod D \\ {}^tB'D = {}^tDB'}} e^{2\pi i \operatorname{tr}(SB'D^{-1})} \\ &= l_D(S). \end{aligned}$$

This completes the proof of (i). Next we prove (ii). By (i) we need only prove the claim in the case $D = D_{\alpha,\beta}$. We need to construct a complete set of representatives modulo $D_{\alpha,\beta}$. We have as a complete set of representatives modulo $D_{\alpha,\beta}$

$$\left\{ \begin{bmatrix} b_1 & p^\beta b_2 \\ b_2 & b_3 \end{bmatrix} : 0 \le b_1, b_2 < p^\alpha,\ 0 \le b_3 < p^{\alpha+\beta} \right\}.$$

Write

$$S = \begin{bmatrix} Mr & t/2 \\ t/2 & s \end{bmatrix}.$$

We then have

$$
\begin{aligned}
l_{D_{\alpha,\beta}}(S) &= \sum_{B \bmod D_{\alpha,\beta}} e^{2\pi i \mathrm{tr}(SBD_{\alpha,\beta}^{-1})} \\
&= \sum_{\substack{0\le b_1,b_2<p^\alpha \\ 0\le b_3<p^{\alpha+\beta}}} e^{2\pi i \mathrm{tr}\left(\begin{bmatrix} Mr & t/2 \\ t/2 & s \end{bmatrix}\begin{bmatrix} b_1 & p^\beta b_2 \\ b_2 & b_3 \end{bmatrix}\begin{bmatrix} p^\alpha & 0 \\ 0 & p^{\alpha+\beta} \end{bmatrix}^{-1}\right)} \\
&= \sum_{\substack{0\le b_1,b_2<p^\alpha \\ 0\le b_3<p^{\alpha+\beta}}} e^{2\pi i\left(\frac{b_1 Mr}{p^\alpha}+\frac{b_2 t}{p^\alpha}+\frac{b_3 s}{p^{\alpha+\beta}}\right)} \\
&= \sum_{b_1=0}^{p^\alpha-1} e^{2\pi i b_1 Mr/p^\alpha} \sum_{b_2=0}^{p^\alpha-1} e^{2\pi i b_2 t/p^\alpha} \sum_{b_3=0}^{p^{\alpha+\beta}-1} e^{2\pi i b_3 s/p^{\alpha+\beta}}.
\end{aligned}
$$

Therefore

$$
l_D(S) = l_{D_{\alpha,\beta}}(S) = \begin{cases} p^{3\alpha+\beta} & \text{if } r \equiv t \equiv 0 \pmod{p^\alpha},\ s \equiv 0 \pmod{p^{\alpha+\beta}}, \\ 0 & \text{otherwise.} \end{cases}
$$

This completes the proof of (ii). □

Define for arbitrary $n \in \mathbb{Z}$ the map $d_m : \mathbb{Z}^n \to \{0,1\}$ by

$$
d_m(x_1, x_2, \ldots, x_n) = \begin{cases} 0 & \text{if } m \nmid x_i \text{ for some } i \\ 1 & \text{if } m | x_i \text{ for all } i \end{cases}.
$$

Going back to our computation we then have

$$
\begin{aligned}
(T(p^{r_0})(F))(Z) &= \sum_{S\in A(M)} a(S) \sum_{(\alpha,\beta,\gamma)\in\Lambda_{r_0}} \sum_{D\in D_{\alpha,\beta}{}^tR(p^\beta)} p^{\beta(k-2)+\gamma(2k-3)} d_{p^\alpha}(r,t) d_{p^{\alpha+\beta}}(s) e^{2\pi i \mathrm{tr}(p^{r_0} S^tD^{-1} Z D^{-1})} \\
&= \sum_{S\in A(M)} a(S) \sum_{(\alpha,\beta,\gamma)\in\Lambda_{r_0}} d_{p^\alpha}(r,t) d_{p^{\alpha+\beta}}(s) p^{\beta(k-2)+\gamma(2k-3)} \sum_{D\in D_{\alpha,\beta}{}^tR(p^\beta)} e^{2\pi i \mathrm{tr}(p^{r_0} D^{-1} S^tD^{-1} Z)} \\
&= \sum_{S\in A(M)} \sum_{(\alpha,\beta,\gamma)\in\Lambda_{r_0}} \sum_{U\in R(p^\beta)} a(S) d_{p^\alpha}(r,t) d_{p^{\alpha+\beta}}(s) p^{\beta(k-2)+\gamma(2k-3)} e^{2\pi i \mathrm{tr}(f_U^{(\alpha,\beta,\gamma)}(S) Z)}
\end{aligned}
$$

where $f_U^{(\alpha,\beta,\gamma)}(S) = p^{r_0} D^{-1} S({}^tD^{-1})$ and $D = D_{\alpha,\beta}{}^tU$. Suppose $S \in A(M)$ such that $r \equiv t \equiv 0 \pmod{p^\alpha}$ and $s \equiv 0 \pmod{p^{\alpha+\beta}}$ and write

$$
r = p^\alpha r',\ t = p^\alpha t',\ \text{and } s = p^{\alpha+\beta} s'.
$$

Then we have

$$\begin{aligned} f_U^{(\alpha,\beta,\gamma)}(S) &= p^{r_0} D^{-1} S({}^tD^{-1}) \\ &= p^{r_0} \cdot {}^tU^{-1} D_{\alpha,\beta}^{-1} S D_{\alpha,\beta}^{-1} U^{-1} \\ &= {}^tU^{-1} \left(p^{\gamma} \begin{bmatrix} Mr'p^{\beta} & t'/2 \\ t'/2 & s' \end{bmatrix} \right) U^{-1} \in A(M). \end{aligned}$$

It is clear that $f_U^{(\alpha,\beta,\gamma)}$ is an injective map. For notational simplicity, we denote for $S \in A(M)$ and $U \in R(p^{\beta})$

$${}^tUSU = \begin{bmatrix} Mr_U & t_U/2 \\ t_U/2 & s_U \end{bmatrix} = S_U.$$

It now follows that

$$(T(p^{r_0})(F))(Z) = \sum_{S \in A(M)} a(p^{r_0}; S) e^{2\pi i \mathrm{tr}(SZ)}.$$

where

$$a(p^{r_0}; S) = \sum_{(\alpha,\beta,\gamma) \in \Lambda_{r_0}} \sum_{U \in R(p^{\beta})} d_{p^{\beta+\gamma}}(r_U) d_{p^{\gamma}}(t_U, s_U) p^{\beta(k-2)+\gamma(2k-3)} a((f_U^{(\alpha,\beta,\gamma)})^{-1}(S)).$$

We also can make note here that

$$\begin{aligned} \sum_{U \in R(p^{\beta})} d_{p^{\beta+\gamma}}(r_U) d_{p^{\gamma}}(t_U, s_U) a((f_U^{(\alpha,\beta,\gamma)})^{-1}(S)) &= \sum_{U \in R(p^{\beta})} d_{p^{\beta+\gamma}}(r_U) d_{p^{\gamma}}(t_U, s_U) a\left(p^{\alpha-\beta-\gamma} \begin{bmatrix} 1 & 0 \\ 0 & p^{\beta} \end{bmatrix} S_U \begin{bmatrix} 1 & 0 \\ 0 & p^{\beta} \end{bmatrix} \right) \\ &= (\Delta^{-}(p^{\gamma})(\Delta(p^{\beta})(\Delta^{+}(p^{\alpha})a)))(S) \end{aligned}$$

and thus

$$a(p^{r_0}; S) = \sum_{(\alpha,\beta,\gamma) \in \Lambda_{r_0}} p^{\beta(k-2)+\gamma(2k-3)} (\Delta^{-}(p^{\gamma})(\Delta(p^{\beta})(\Delta^{+}(p^{\alpha})a)))(S).$$

We further note here that if S is primitive and $m_0 \in \mathbb{N}$ with $\gcd(m_0, p) = 1$, then

$$a(p^{r_0}; m_0 S) = \sum_{(\alpha,\beta,0) \in \Lambda_{r_0}} p^{(k-2)\beta} (\Delta(p^{\beta})(\Delta^{+}(p^{\alpha})a))(m_0 S).$$

Theorem 6.1.2. *Let $\delta < 0$ be a fundamental discriminant. Let*

$$F(Z) = \sum_{S \in A(M)} a(S) e^{2\pi i \mathrm{tr} SZ} \in \mathcal{M}_k(\mathrm{K}(M))$$

for $k > 0$. Let $S \in A(M, \delta f^2)$ and let $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$ be associated to S. Let p be a prime not dividing Mf.

(i) If $p\mathfrak{o}_f = \mathfrak{p}\overline{\mathfrak{p}}$ *in* $\mathbb{Q}(\sqrt{\delta})$ *then for* $m_0 \in \mathbb{N}$ *with* $\gcd(m_0, p) = 1$

$$a(p^{r_0}; m_0 S) = a(p^{r_0} m_0 S) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(p^{r_0-\beta} m_0 S_{(G\mathfrak{p}^\beta, \boldsymbol{\xi}_{\mathfrak{p}^\beta})}) + a(p^{r_0-\beta} m_0 S_{(G\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{\overline{\mathfrak{p}}^\beta})})].$$

(ii) If $p\mathfrak{o}_f = \mathfrak{p}^2$ *in* $\mathbb{Q}(\sqrt{\delta})$ *then for* $m_0 \in \mathbb{N}$ *with* $\gcd(m_0, p) = 1$

$$a(p^{r_0}; m_0 S) = a(p^{r_0} m_0 S) + p^{k-2} a(p^{r_0-1} m_0 S_{(G\mathfrak{p}, \boldsymbol{\xi}_{\mathfrak{p}})}).$$

(iii) If $p\mathfrak{o}_f = \mathfrak{p}$ *in* $\mathbb{Q}(\sqrt{\delta})$ *then for* $m_0 \in \mathbb{N}$ *with* $\gcd(m_0, p) = 1$

$$a(p^{r_0}, m_0 S) = a(p^{r_0} m_0 S).$$

Proof. The Fourier coefficients of a Siegel paramodular form can be viewed as the outputs of a function in $\mathcal{B}(M)$, i.e., $a \in \mathcal{B}(M)$. We then consider $a' \in \mathcal{B}'(M)$ (see equation 5.3). We first prove (i). We have

$$\begin{aligned} a'(p^{r_0}; m_0, (G, \boldsymbol{\xi})) &= \sum_{(\alpha,\beta,0)\in\Lambda_{r_0}} p^{(k-2)\beta} (\Delta(p^\beta)(\Delta^+(p^\alpha) a'))(m_0, (G, \boldsymbol{\xi})) \\ &= a'(p^{r_0} m_0, (G, \boldsymbol{\xi})) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a'(p^{r_0-\beta} m_0, (G\mathfrak{p}^\beta, \boldsymbol{\xi}_{\mathfrak{p}^\beta})) + a'(p^{r_0-\beta} m_0, (G\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{\overline{\mathfrak{p}}^\beta}))] \end{aligned}$$

where we have used Theorem 5.5.5. The result now follows upon lifting a' back to a. The proof of (ii) and (iii) are similar. □

Definition 6.1.3. *Let* $F : \mathcal{H}_2 \to \mathbb{C}$ *be a Siegel paramodular form. If for each prime* p *not dividing* M *there exists constants* $\{\mu(p^{r_0})\}_{r_0=0}^{\infty}$ *such that*

$$T(p^{r_0})F = \mu(p^{r_0})F$$

then we say that F *is a Siegel paramodular eigenform.*

From this point onward, eigenforms will be the key objects we will focus on.

Definition 6.1.4. *Let* $M \geq 1$ *be an integer and let* $F : \mathcal{H}_2 \to \mathbb{C}$ *be a Siegel paramodular eigenform. Let* p *be a prime number that does not divide* M. *We define the* ***Euler factor at*** p *to be the polynomial*

$$Q_{p,F}(t) = 1 - \mu(p)t + (\mu(p)^2 - \mu(p^2) - p^{2k-4})t^2 - \mu(p)p^{2k-3}t^3 + p^{4k-6}t^4.$$

One can compare the above Euler factor to that appearing in [18]. The authors there use the Hecke operator $T_1(p^2)$ instead of $T(p^2)$. Another interesting feature to note is that the eigenvalues $\mu(p)$ and $\mu(p^2)$ appearing in the definition are, in general, not integral (see [17]). The following theorem is a result due to Shimura [37]. For a proof of the claim, which requires quite a bit of theory which we do not cover here, see [4].

Theorem 6.1.5. *Let $M \geq 1$ be an integer and let $F : \mathcal{H}_2 \to \mathbb{C}$ be a Siegel paramodular eigenform. Let p be a prime number that does not divide M and let $\{\mu(p^{r_0})\}_{r_0=0}^{\infty}$ be the corresponding eigenvalues at p. Then*

$$\sum_{r_0=0}^{\infty} \mu(p^{r_0})t^{r_0} = (1 - p^{2k-4}t^2)Q_{p,F}(t)^{-1}.$$

Theorem 6.1.6. *Let $M \geq 1$ be an integer and let*

$$F(Z) = \sum_{S \in A(M)} a(S)e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(\mathrm{K}(M))$$

of weight $k > 0$. Let p be a prime number that does not divide M. Then for any $S \in A(M)$ such that $\gcd(p, e(S)) = 1$ *we have*

$$\left(\sum_{r_0=0}^{\infty} a(p^{r_0}S)t^{r_0}\right) Q_{p,F}(t) = a(S) - p^{k-2}(\Delta(p)a)(S)t + (p^{2k-4}(\Delta^*(p)a)(S) + p^{3k-5}(\Delta(p)(\Delta^-(p)a))(S))t^2$$

where

$$\Delta^*(p) = \Delta(p)^2 - \Delta(p^2) - 1.$$

Proof. We provide additional details to the proof found in [2]. Write

$$\left(\sum_{r_0=1}^{\infty} a(p^{r_0}S)t^{r_0}\right) Q_{p,F}(t) = \sum_{n=0}^{\infty} c_n t^n.$$

We will compute expressions for c_n, $n \geq 0$. Let $\{\mu(p^{r_0})\}_{r_0=0}^{\infty}$ be the eigenvalues of F at p. Using the definition of $Q_{p,F}(t)$ we have on the left side after expanding,

$$\sum_{r_0=0}^{\infty} a(p^{r_0}S)t^{r_0} - \sum_{r_0=0}^{\infty} a(p^{r_0}S)\mu(p)t^{r_0+1} + \sum_{r_0=0}^{\infty} a(p^{r_0}S)(\mu(p)^2 - \mu(p^2) - p^{2k-4})t^{r_0+2}$$
$$- \sum_{r_0=0}^{\infty} a(p^{r_0}S)\mu(p)p^{2k-3}t^{r_0+3} + \sum_{r_0=0}^{\infty} a(p^{r_0}S)p^{4k-6}t^{r_0+4}$$

We now identify the c_n for $n \geq 0$. We have

$$c_n = \begin{cases} a(S) & \text{if } n = 0, \\ a(pS) - \mu(p)a(S) & \text{if } n = 1, \\ a(p^2S) - \mu(p)a(pS) + (\mu(p)^2 - \mu(p^2) - p^{2k-4})a(S) & \text{if } n = 2, \\ a(p^3S) - \mu(p)a(p^2S) + (\mu(p)^2 - \mu(p^2) - p^{2k-4})a(pS) - \mu(p)p^{2k-3}a(S) & \text{if } n = 3, \\ a(p^nS) - \mu(p)a(p^{n-1}S) + (\mu(p)^2 - \mu(p^2) - p^{2k-4})a(p^{n-2}S) & \\ -\mu(p)p^{2k-3}a(p^{n-3}S) + p^{4k-6}a(p^{n-4}S) & \text{if } n \geq 4. \end{cases}$$

We also have for $l \geq 0$,

$$\mu(p)a(p^lS) = \sum_{(\alpha,\beta,\gamma)\in\Lambda_1} p^{(k-2)\beta+(2k-3)\gamma}(\Delta^-(p^\gamma)(\Delta(p^\beta)(\Delta^+(p^\alpha)a)))(p^lS)$$
$$= (\Delta^+(p)a)(p^lS) + p^{k-2}(\Delta(p)a)(p^lS) + p^{2k-3}(\Delta^-(p)a)(p^lS)$$

and

$$
\begin{aligned}
(\mu(p)^2 - \mu(p^2) - p^{2k-4})a(p^l S) &= \mu(p)^2 a(p^l S) - \mu(p^2)a(p^l S) - p^{2k-4}a(p^l S) \\
&= p^{2k-4}((\Delta(p)^2 - \Delta(p^2) + p - 1)a)(p^l S) + p^{k-2}(\Delta(p)(\Delta^+(p)a))(p^l S) \\
&\quad + p^{3k-5}(\Delta(p)(\Delta^-(p)a))(p^l S).
\end{aligned}
$$

It now follows that

$$
c_n = \begin{cases} a(S) & \text{if } n = 0, \\ -p^{k-2}(\Delta(p)a)(S) & \text{if } n = 1, \\ p^{2k-4}((\Delta(p)^2 - \Delta(p^2) - 1)a)(S) + p^{3k-5}(\Delta(p)(\Delta^-(p)a))(S) & \text{if } n = 2, \\ p^{2k-4}(\Delta^+(p)(\Delta(p)^2 - \Delta(p^2) - (p+1))a)(S) & \text{if } n = 3, \\ p^{2k-4}(\Delta^+(p^{n-2})(\Delta(p)^2 - \Delta(p^2) - (p+1))a)(S) & \text{if } n \geq 4. \end{cases}
$$

□

We now prove a lemma.

Lemma 6.1.7. *Let $M \geq 1$ be an integer. For every prime p not dividing M we have*

$$
\Delta^+(p) \circ (\Delta(p)^2 - \Delta(p^2) - (p+1)) = 0.
$$

Proof. We have

$$
\begin{aligned}
\Delta^+(p) \circ \Delta(p)^2 &= \Delta^+(p) \circ T\left(\Gamma_0(M)\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}\Gamma_0(M)\right) \circ \Delta^-(p) \circ T\left(\Gamma_0(M)\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}\Gamma_0(M)\right) \circ \Delta^-(p) \\
&= \left[T\left(\Gamma_0(M)\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}\Gamma_0(M)\right)\right]^2 \circ \Delta^-(p).
\end{aligned}
$$

By the identity

$$
\left[T\left(\Gamma_0(M)\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}\Gamma_0(M)\right)\right]^2 = T\left(\Gamma_0(M)\begin{bmatrix} 1 & 0 \\ 0 & p^2 \end{bmatrix}\Gamma_0(M)\right) + (p+1)T\left(\Gamma_0(M)\begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix}\Gamma_0(M)\right),
$$

we have

$$
\begin{aligned}
\Delta^+(p) \circ \Delta(p)^2 &= T\left(\Gamma_0(M)\begin{bmatrix} 1 & 0 \\ 0 & p^2 \end{bmatrix}\Gamma_0(M)\right) \circ \Delta^-(p) + (p+1)T\left(\Gamma_0(M)\begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix}\Gamma_0(M)\right) \circ \Delta^-(p) \\
&= \Delta^+(p) \circ \Delta(p^2) + (p+1)\Delta^+(p).
\end{aligned}
$$

The lemma is proved. □

Going back to the proof of the theorem we have

$$c_n = \begin{cases} a(S) & \text{if } n=0, \\ -p^{k-2}(\Delta(p)a)(S) & \text{if } n=1, \\ p^{2k-4}((\Delta(p)^2-\Delta(p^2)-1)a)(S)+p^{3k-5}(\Delta(p)(\Delta^-(p)a))(S) & \text{if } n=2, \\ 0 & \text{if } n\geq 3. \end{cases}$$

The desired formula not follows which completes the proof of the theorem.

6.2 An Euler Product for Siegel Paramodular Forms

This section will be focused on proving one of our main theorems. Let $M \geq 1$ be an integer and for a fixed integer $\delta < 0$ where δ is a fundamental discriminant, we denote by

$$L_{\delta f^2}(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{(N(\mathfrak{p}))^s}\right)^{-1} \quad (Re(s) > 1),$$

the L-series of the order $\mathfrak{o}_f$ in $K = \mathbb{Q}(\sqrt{\delta})$, where the product ranges over all prime ideals of $\mathfrak{o}_f$ whose ring of coefficients is $\mathfrak{o}_\mathfrak{p} = \mathfrak{o}_f$ and whose norms are relatively prime to Mf (see [22]).

Theorem 6.2.1. *Let $M \geq 1$ be an integer. Let*

$$F(Z) = \sum_{S\in A(M)} a(S)e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(K(M))$$

with $k > 0$. Suppose that F is an eigenform of the Hecke operators $\{T(m)\}_{m\geq 1,\ \gcd(m,M)=1}$ with eigenvalues $\{\mu(m)\}_{m\geq 1,\ \gcd(m,M)=1}$. Let $\delta < 0$ be a fundamental discriminant and let $K = \mathbb{Q}(\sqrt{\delta})$. Fix an order $\mathfrak{o}_f$ of K for some $f \in \mathbb{N}$. Then for every $S \in A(M, \delta f^2)$, we have in some right half-plane

$$L_{\delta f^2}(s-k+2) \sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \sum_{\substack{m=1\\ \gcd(m,M)=1}}^{\infty} \frac{a(mS_\mathfrak{u})}{m^s} = \chi_{S,F}(s) \prod_{p\nmid M} Q_{p,F}(p^{-s})^{-1}$$

where $L_{\delta f^2}(s)$ is the L-series of $\mathfrak{o}_f$, the matrix $S_\mathfrak{u}$ is determined by the action of $H(\mathfrak{o}_f, M)$, and

$$\chi_{S,F}(s) = \sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \left(\prod_{\substack{p\nmid M\\ p\mid f}} \left[\left(1 - \frac{\Delta(p)}{p^{s-k+2}}\right)\left(1 - \frac{\Delta^-(p)}{p^{s-2k+3}}\right) a \right] (S_\mathfrak{u}) \right).$$

Proof. Let $S \in A(M, \delta f^2)$ and let $(G, \boldsymbol{\xi}) \in \mathscr{A}(M, \delta f^2)$ be the full module associated to S. For every prime p not dividing M and for every $m_0 \in \mathbb{N}$ with $\gcd(m_0, p) = 1$ we compute the series

$$\left(\sum_{r_0=1}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} a'(m_0p^{r_0}, (G\mathfrak{u}, \boldsymbol{\xi}_\mathfrak{u})) \right) p^{-sr_0} \right) Q_{p,F}(p^{-s}).$$

where $a' \in \mathcal{B}'(M)$ is associated to $a \in \mathcal{B}(M)$.

We first suppose that p splits in K. Then by Theorem 5.5.5 we have

$$(\Delta(p)a')(m_0, (G, \boldsymbol{\xi})) = a'(m_0, (G\mathfrak{p}, \boldsymbol{\xi}_{\mathfrak{p}})) + a'(m_0, (G\overline{\mathfrak{p}}, \boldsymbol{\xi}_{\overline{\mathfrak{p}}}))$$

and

$$((\Delta(p)^2 - \Delta(p^2) - 1)a')(m_0, (G, \boldsymbol{\xi})) = a'(m_0, (G, \boldsymbol{\xi})).$$

Furthermore, we have

$$(\Delta(p)\Delta^-(p)a')(m_0, (G, \boldsymbol{\xi})) = (\Delta^-(p)a')(m_0, (G\mathfrak{p}, \boldsymbol{\xi}_{\mathfrak{p}})) + (\Delta^-(p)a')(m_0, (G\overline{\mathfrak{p}}, \boldsymbol{\xi}_{\overline{\mathfrak{p}}})) = 0.$$

Thus, by Theorem 6.1.6, we have that

$$\left(\sum_{r_0=1}^{\infty} \left(\sum_{[\mathfrak{u}] \in H(\mathfrak{o}_f, M)} a'(m_0 p^{r_0}, (G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{u}})) \right) p^{-sr_0} \right) Q_{p,F}(p^{-s})$$

is equal to

$$\sum_{[\mathfrak{u}] \in H(\mathfrak{o}_f, M)} [a'(m_0, (G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{u}})) + p^{k-2}(a'(m_0, (G\mathfrak{u}\mathfrak{p}, \boldsymbol{\xi}_{\mathfrak{u}\mathfrak{p}})) + a'(m_0, (G\mathfrak{u}\overline{\mathfrak{p}}, \boldsymbol{\xi}_{\mathfrak{u}\overline{\mathfrak{p}}})))p^{-s}$$
$$+ p^{2k-4} a'(m_0, (G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{u}}))p^{-2s}].$$

Observing that $H(\mathfrak{o}_f, M)[\mathfrak{p}] = H(\mathfrak{o}_f, M)$ we find that the above expression is equal to

$$\sum_{[\mathfrak{u}] \in H(\mathfrak{o}_f, M)} a'(m_0, (G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{u}})) \left(1 - \frac{1}{N(\mathfrak{p})^{s-k+2}}\right) \left(1 - \frac{1}{N(\overline{\mathfrak{p}})^{s-k+2}}\right).$$

We repeat the same analysis in the cases where p is ramified or inert in K and $p \nmid f$ and in the case where $p|f$. In each case respectively we obtain the expressions

$$\sum_{[\mathfrak{u}] \in H(\mathfrak{o}_f, M)} a'(m_0, (G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{u}})) \left(1 - \frac{1}{N(\mathfrak{p})^{s-k+2}}\right),$$

$$\sum_{[\mathfrak{u}] \in H(\mathfrak{o}_f, M)} a'(m_0, (G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{u}})) \left(1 - \frac{1}{N(\mathfrak{p})^{s-k+2}}\right),$$

and

$$\sum_{[\mathfrak{u}] \in H(\mathfrak{o}_f, M)} \left[\left(1 - \frac{\Delta(p)}{p^{s-k+2}}\right) \left(1 - \frac{\Delta^-(p)}{p^{s-2k+3}}\right) a' \right] (m_0, (G\mathfrak{u}, \boldsymbol{\xi}_{\mathfrak{u}})).$$

We proceed with the proof of the claim. We note that we will prove the formula at first only formally. Let p_0 be a prime not dividing Mf which ramifies in $\mathbb{Q}(\sqrt{\delta})$. Then

$$\begin{aligned}
&\prod_{p\nmid M} Q_{p,F}(p^{-s}) \sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \sum_{\substack{m=1\\ \gcd(m,M)=1}}^{\infty} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s}\\
&= \prod_{\substack{p\nmid M\\ p|f}} Q_{p,F}(p^{-s}) \prod_{p\nmid Mf} Q_{p,F}(p^{-s}) \sum_{\substack{m=1\\ \gcd(m,M)=1}}^{\infty} \sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s}\\
&= \prod_{\substack{p\nmid M\\ p|f}} Q_{p,F}(p^{-s}) Q_{p_0,F}(p_0^{-s}) \prod_{\substack{p\nmid Mf\\ p\neq p_0}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1\\ \gcd(m,Mp_0)=1}}^{\infty} \frac{1}{m^s} \sum_{r_0=0}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(mp_0^{r_0},(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{p_0^{sr_0}} \right)\\
&= \prod_{\substack{p\nmid M\\ p|f}} Q_{p,F}(p^{-s}) \prod_{\substack{p\nmid Mf\\ p\neq p_0}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1\\ \gcd(m,Mp_0)=1}}^{\infty} \frac{1}{m^s} \sum_{r_0=0}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(mp_0^{r_0},(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{p_0^{sr_0}} \right) Q_{p_0,F}(p_0^{-s})\\
&= \prod_{\substack{p\nmid M\\ p|f}} Q_{p,F}(p^{-s}) \prod_{\substack{p\nmid Mf\\ p\neq p_0}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1\\ \gcd(m,Mp_0)=1}}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s} \left(1-\frac{1}{N(\mathfrak{p}_0)^{s-k+2}}\right) \right)\\
&= \left(1-\frac{1}{N(\mathfrak{p}_0)^{s-k+2}}\right) \prod_{\substack{p\nmid M\\ p|f}} Q_{p,F}(p^{-s}) \prod_{\substack{p\nmid Mf\\ p\neq p_0}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1\\ \gcd(m,Mp_0)=1}}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s} \right)
\end{aligned}$$

where $\mathfrak{p}_0$ is the unique prime ideal of norm p_0^2.

Let $p_1,\dots,p_d$ be the remaining ramified primes in $\mathbb{Q}(\sqrt{\delta})$ and let $\mathfrak{p}_1,\dots,\mathfrak{p}_d$ be the corresponding prime ideals of norm $p_1^2,\dots,p_d^2$ respectively. Then repeating the above argument for this finite set of primes we obtain

$$\begin{aligned}
&\prod_{p\nmid M} Q_{p,F}(p^{-s}) \sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \sum_{\substack{m=1\\ \gcd(m,M)=1}}^{\infty} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s}\\
&= \prod_{i=0}^{d} \left(1-\frac{1}{N(\mathfrak{p}_i)^{s-k+2}}\right) \prod_{\substack{p\nmid M\\ p|f}} Q_{p,F}(p^{-s}) \prod_{\substack{p\nmid Mf\\ p\,\text{unramified}}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1\\ \gcd(m,MP_r)=1}}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s} \right)
\end{aligned}$$

where P_r is the product of all the ramified primes.

We consider now the remaining expression

$$\prod_{\substack{p\nmid M\\ p|f}} Q_{p,F}(p^{-s}) \prod_{\substack{p\nmid Mf\\ p\,\text{unramified}}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1\\ \gcd(m,MP_r)=1}}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s} \right).$$

Let q_0 be a prime not dividing Mf which splits in $\mathbb{Q}(\sqrt{\delta})$ and let

$$C = \prod_{\substack{p\nmid M\\ p|f}} Q_{p,F}(p^{-s}).$$

Then

$$
\begin{aligned}
& C \prod_{\substack{p\nmid Mf \\ p\,\text{unramified}}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1 \\ \gcd(m,MP_r)=1}}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s} \right) \\
&= CQ_{q_0,F}(q_0^{-s}) \prod_{\substack{p\nmid Mf \\ p\neq q_0\,\text{unramified}}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1 \\ \gcd(m,MP_r)=1}}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s} \right) \\
&= C \prod_{\substack{p\nmid Mf \\ p\neq q_0\,\text{unramified}}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1 \\ \gcd(m,MP_rq_0)=1}}^{\infty} \frac{1}{m^s} \sum_{r_0=0}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(mq_0^{r_0},(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{q_0^{sr_0}} \right) Q_{q_0,F}(q_0^{-s}) \\
&= \left(1-\frac{1}{N(\mathfrak{q}_0)^{s-k+2}}\right)\left(1-\frac{1}{N(\overline{\mathfrak{q}}_0)^{s-k+2}}\right) C \prod_{\substack{p\nmid Mf \\ p\neq q_0\,\text{unramified}}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1 \\ \gcd(m,MP_rq_0)=1}}^{\infty} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s}.
\end{aligned}
$$

Let $\{q_i\}_{i=1}^{\infty}$ be the remaining split primes in $\mathbb{Q}(\sqrt{\delta})$. We know that there are infinitely many by the Čebotarev Density Theorem (see [11]). We prove that

$$
\begin{aligned}
& C \prod_{\substack{p\nmid Mf \\ p\,\text{unramified}}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1 \\ \gcd(m,MP_r)=1}}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s} \right) \\
&= \prod_{i=0}^{\infty} \left(1-\frac{1}{N(\mathfrak{q}_i)^{s-k+2}}\right)\left(1-\frac{1}{N(\overline{\mathfrak{q}}_i)^{s-k+2}}\right) C \prod_{\substack{p\nmid Mf \\ p\,\text{unramified} \\ p\,\text{non-split}}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1 \\ \gcd(m,MP_r)=1 \\ \gcd(m,q_i)=1\,\text{for all}\,i}}^{\infty} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s}.
\end{aligned}
$$

Indeed, based on the argument for q_0 above, we have for $d' \in \mathbb{N}$

$$
\begin{aligned}
& \prod_{\substack{p\nmid M \\ p\mid f}} Q_{p,F}(p^{-s}) \prod_{\substack{p\nmid Mf \\ p\,\text{unramified}}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1 \\ \gcd(m,MP_r)=1}}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s} \right) \\
&= \prod_{i=0}^{d'} \left(1-\frac{1}{N(\mathfrak{q}_i)}\right)\left(1-\frac{1}{N(\overline{\mathfrak{q}}_i)}\right) \prod_{\substack{p\nmid M \\ p\mid f}} Q_{p,F}(p^{-s}) \prod_{\substack{p\nmid Mf \\ p\,\text{unramified} \\ p\neq q_i\,\text{for}\,i\leq d'}} Q_{p,F}(p^{-s}) \\
& * \sum_{\substack{m=1 \\ \gcd(m,MP_r)=1 \\ \gcd(m,q_i)=1\,\text{for all}\,i\leq d'}}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s} \right).
\end{aligned}
$$

Taking the limit as d' goes to infinity yields the desired result.

We then repeat the same argument for the inert primes. We then obtain

$$
\begin{aligned}
& \prod_{p\nmid M} Q_{p,F}(p^{-s}) \sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \sum_{\substack{m=1 \\ \gcd(m,M)=1}}^{\infty} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s} \\
&= L_{\delta f^2}(s-k+2)^{-1} \prod_{\substack{p\nmid M \\ p\mid f}} Q_{p,F}(p^{-s}) \sum_{\substack{m=1 \\ \gcd(m,Mq)=1 \\ \text{for all}\,q\,\text{prime},\,q\nmid Mf}}^{\infty} \left(\sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s} \right).
\end{aligned}
$$

We lastly apply the appropriate identity for the remaining set of primes which divide f but do not divide M. We then obtain

$$\prod_{p\nmid M} Q_{p,F}(p^{-s}) \sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \sum_{\substack{m=1\\ \gcd(m,M)=1}}^{\infty} \frac{a'(m,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}}))}{m^s}$$
$$= L_{\delta f^2}(s-k+2)^{-1} \sum_{[\mathfrak{u}]\in H(\mathfrak{o}_f,M)} \left(\prod_{\substack{p\nmid M\\ p\mid f}} \left[\left(1-\frac{\Delta(p)}{p^{s-k+2}}\right)\left(1-\frac{\Delta^{-}(p)}{p^{s-2k+3}}\right) a' \right] (1,(G\mathfrak{u},\boldsymbol{\xi}_{\mathfrak{u}})) \right).$$

The desired formula now follows. The convergence of the series follows from bounds on the Fourier coefficients of F. In particular, the Fourier coefficients of F satisfy

$$|a(S)| \le C(\det(S))^k$$

for some constant $C > 0$ (see [13]). The theorem is proved.

□

6.3 Multiplicative Properties of Fourier Coefficients for Class Number One

We begin with the case of class number one as it is the simpler case. A case for $M = 1$ was proved by McCarthy and we state the results again here for the reader's convenience.

Theorem 6.3.1 (McCarthy, 2016)**.** *Let*

$$F(Z) = \sum_{S\in A(1)} a(S)e^{2\pi i \operatorname{tr}(SZ)} \in \mathcal{M}_k(\mathrm{Sp}(4,\mathbb{Z}))$$

with $k > 0$. Suppose that F is an eigenform.

(i) If $a(I_{1,0}) = 0$, then $a(mI_{1,0}) = 0$ for all $m \in \mathbb{N}$.

(ii) For $m, n \in \mathbb{N}$ with $\gcd(m,n) = 1$ we have

$$a(I_{1,0})a(mnI_{1,0}) = a(mI_{1,0})a(nI_{1,0}).$$

The proof of Theorem 6.3.1 uses primarily an exercise from [29] (see Exercise 5, pg. 77 of this reference). The proofs of our generalizations, however, take advantage of the theory developed in Chapter 5. We note further that Theorem 6.3.1 uses the quadratic form

$$I_{1,0} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

which has discriminant -4. This discriminant corresponds to a case where the class number is one. We prove another case of this theorem using the quadratic form

$$I_{1,1} = \begin{bmatrix} 1 & 1/2 \\ 1/2 & 1 \end{bmatrix}$$

which has discriminant -3. This is also a discriminant which corresponds to a case where the class number happens to be one.

Theorem 6.3.2. *Let*

$$F(Z) = \sum_{S \in A(1)} a(S) e^{2\pi i \operatorname{tr}(SZ)} \in \mathcal{M}_k(\mathrm{Sp}(4, \mathbb{Z}))$$

with $k > 0$. Suppose that F is an eigenform.

(i) If $a(I_{1,1}) = 0$, then $a(mI_{1,1}) = 0$ for all $m \in \mathbb{N}$.

(ii) For $m, n \in \mathbb{N}$ with $\gcd(m,n) = 1$ and we have

$$a(I_{1,1})a(mnI_{1,1}) = a(mI_{1,1})a(nI_{1,1}).$$

Proof. Let $K = \mathbb{Q}(\sqrt{-3})$. The full module associated to $I_{1,1}$ is $\mathfrak{o}_1 \subseteq K$ with basis

$$\boldsymbol{\xi} = \begin{bmatrix} 1 \\ \dfrac{1 - \sqrt{-3}}{2} \end{bmatrix}.$$

We start by proving (i). We note that we are working in the case $M = 1$ here. We consider for $m \in \mathbb{N}$

$$a(p^{r_0}; mI_{1,1}) = \mu(p^{r_0})a(mI_{1,1})$$

for various primes p with $\gcd(m, p) = 1$. We assume that $a(mI_{1,1}) = 0$.

We break the proof down based on the splitting behavior of p in K. Suppose first that p splits in K. By Theorem 6.1.2 we have

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}S_{(\mathfrak{o}_1\mathfrak{p}^\beta, \boldsymbol{\xi}_{\mathfrak{p}^\beta})}) + a(mp^{r_0-\beta}S_{(\mathfrak{o}_1\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{\overline{\mathfrak{p}}^\beta})})].$$

The binary quadratic forms $S_{(\mathfrak{o}_1\mathfrak{p}^\beta, \boldsymbol{\xi}_{\mathfrak{p}^\beta})}$ and $S_{(\mathfrak{o}_1\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{\overline{\mathfrak{p}}^\beta})}$ each have discriminant -3 and thus belong to the same class as $I_{1,1}$ modulo $\Gamma_0(1) = \mathrm{SL}(2, \mathbb{Z})$. Thus we arrive at the formula

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}I_{1,1}) + a(mp^{r_0-\beta}I_{1,1})].$$

In particular, if $r_0 = 1$, we have

$$\mu(p)a(mI_{1,1}) = a(mpI_{1,1}) + p^{k-2}[a(mI_{1,1}) + a(mI_{1,1})].$$

Hence, if $a(mI_{1,1}) = 0$ we then have $a(mpI_{1,1}) = 0$. We now prove by induction that $a(mp^{r_0}I_{1,1}) = 0$ for $r_0 \geq 1$. We just proved the case $r_0 = 1$. Assume that the claim has been proven for all positive integers less than r_0. Since

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}I_{1,1}) + a(mp^{r_0-\beta}I_{1,1})]$$

the induction hypothesis implies that $a(mp^{r_0-\beta}I_{1,1}) = 0$ for all β with $1 \leq \beta < r_0$. Therefore we can conclude that $a(mp^{r_0}I_{1,1}) = 0$. To prove the claim in the case that p splits we apply the above argument to the specific case $m = 1$.

Suppose now that p is ramified in K. By Theorem 6.1.2 we have

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}) + p^{k-2}a(mp^{r_0-1}S_{(G_{\mathfrak{p}},\boldsymbol{\xi}_{\mathfrak{p}})}).$$

The binary quadratic form $S_{(G_{\mathfrak{p}},\boldsymbol{\xi}_{\mathfrak{p}})}$ has discriminant -3 and thus belongs to the same class as $I_{1,1}$ modulo $\mathrm{SL}(2,\mathbb{Z})$. Thus we have the formula

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}) + p^{k-2}a(mp^{r_0-1}I_{1,1}).$$

In particular, if $r_0 = 1$, we have

$$\mu(p)a(mI_{1,1}) = a(mpI_{1,1}) + p^{k-2}a(mI_{1,1}).$$

Hence, if $a(mI_{1,1}) = 0$ we then have $a(mpI_{1,1}) = 0$. We now prove by a simple induction that if $a(mI_{1,1}) = 0$ then $a(mp^{r_0}I_{1,1}) = 0$ for $r_0 \geq 1$. We just proved the case $r_0 = 1$. Assume that the claim has been proven for $r_0 - 1$. Since

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}) + p^{k-2}a(mp^{r_0-1}I_{1,1})$$

the induction hypothesis implies that $a(mp^{r_0-1}I_{1,1}) = 0$. Therefore we can make the conclusion that $a(mp^{r_0}I_{1,1}) = 0$. To prove the claim for the case that p is ramified we apply the argument in the case $m = 1$.

Now suppose that p is inert in K. By Theorem 6.1.2 we have

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}).$$

Thus if $a(mI_{1,1}) = 0$ we have $a(mp^{r_0}I_{1,1}) = 0$ for all $r_0 \geq 1$. To prove the claim for the case that p is inert we just take $m = 1$. To prove the general claim we assume that $a(I_{1,1}) = 0$ and let

$$m = p_1^{\ell_1} p_2^{\ell_2} \cdots p_d^{\ell_d}.$$

Then using what we have proven, we have $a(mI_{1,1}) = 0$. This proves (i).

We now prove (ii). Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Let p be a prime with $\gcd(m, p) = \gcd(n, p) = 1$. We prove that

$$a(mp^{r_0}I_{1,1})a(nI_{1,1}) = a(mI_{1,1})a(np^{r_0}I_{1,1}).$$

We first suppose that p splits in K. We use the formula appearing before in the split case

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}I_{1,1}) + a(mp^{r_0-\beta}I_{1,1})].$$

We again proceed by induction on r_0. First suppose that $r_0 = 1$. Then we have

$$\mu(p)a(mI_{1,1}) = a(mpI_{1,1}) + p^{k-2}[a(mI_{1,1}) + a(mI_{1,1})]$$

and

$$\mu(p)a(nI_{1,1}) = a(npI_{1,1}) + p^{k-2}[a(nI_{1,1}) + a(nI_{1,1})].$$

We multiply the first of these equations by $a(nI_{1,1})$ and the second by $a(mI_{1,1})$. This yields

$$\mu(p)a(mI_{1,1})a(nI_{1,1}) = a(mpI_{1,1})a(nI_{1,1}) + p^{k-2}[a(mI_{1,1})a(nI_{1,1}) + a(mI_{1,1})a(nI_{1,1})]$$

and

$$\mu(p)a(nI_{1,1})a(mI_{1,1}) = a(npI_{1,1})a(mI_{1,1}) + p^{k-2}[a(nI_{1,1})a(mI_{1,1}) + a(nI_{1,1})a(mI_{1,1})].$$

Subtracting the two equations from one another we obtain

$$0 = a(mpI_{1,1})a(nI_{1,1}) - a(npI_{1,1})a(mI_{1,1})$$

which is the desired result. We now assume that the claim has been proved for all positive integers less than r_0. That is

$$a(mp^{\ell}I_{1,1})a(nI_{1,1}) = a(mI_{1,1})a(np^{\ell}I_{1,1})$$

for $1 \leq \ell < r_0$. We then consider

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}I_{1,1}) + a(mp^{r_0-\beta}I_{1,1})]$$

and

$$\mu(p^{r_0})a(nI_{1,1}) = a(np^{r_0}I_{1,1}) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(np^{r_0-\beta}I_{1,1}) + a(np^{r_0-\beta}I_{1,1})].$$

Multiplying the first equation by $a(nI_{1,1})$ and the second equation by $a(mI_{1,1})$ yields

$$\mu(p^{r_0})a(mI_{1,1})a(nI_{1,1}) = a(mp^{r_0}I_{1,1})a(nI_{1,1}) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}I_{1,1})a(nI_{1,1}) + a(mp^{r_0-\beta}I_{1,1})a(nI_{1,1})]$$

and

$$\mu(p^{r_0})a(nI_{1,1})a(mI_{1,1}) = a(np^{r_0}I_{1,1})a(mI_{1,1}) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(np^{r_0-\beta}I_{1,1})a(mI_{1,1}) + a(np^{r_0-\beta}I_{1,1})a(mI_{1,1})].$$

Subtracting the two equations from one another and implementing the induction hypothesis yields

$$0 = a(mp^{r_0}I_{1,1})a(nI_{1,1}) - a(np^{r_0}I_{1,1})a(mI_{1,1})$$

which is the desired result.

We now prove the claim in the case where p ramifies in K. We use the formula appearing before in the ramified case

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}) + p^{k-2}a(mp^{r_0-1}I_{1,1}).$$

We proceed by induction on r_0. First suppose $r_0 = 1$. Then we have

$$\mu(p)a(mI_{1,1}) = a(mpI_{1,1}) + p^{k-2}a(mI_{1,1})$$

and

$$\mu(p)a(nI_{1,1}) = a(npI_{1,1}) + p^{k-2}a(nI_{1,1}).$$

We multiply the first equation by $a(nI_{1,1})$ and the second equation by $a(mI_{1,1})$ which yields

$$\mu(p)a(mI_{1,1})a(nI_{1,1}) = a(mpI_{1,1})a(nI_{1,1}) + p^{k-2}a(mI_{1,1})a(nI_{1,1})$$

and

$$\mu(p)a(nI_{1,1})a(mI_{1,1}) = a(npI_{1,1})a(mI_{1,1}) + p^{k-2}a(nI_{1,1})a(mI_{1,1}).$$

Subtracting the two equations from each other gives

$$0 = a(mpI_{1,1})a(nI_{1,1}) - a(npI_{1,1})a(mI_{1,1})$$

which is the desired result. Now assume the claim has been proven for $r_0 - 1$, that is

$$a(mp^{r_0-1}I_{1,1})a(nI_{1,1}) = a(mI_{1,1})a(np^{r_0-1}I_{1,1}).$$

We have

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}) + p^{k-2}a(mp^{r_0-1}I_{1,1})$$

and

$$\mu(p^{r_0})a(nI_{1,1}) = a(np^{r_0}I_{1,1}) + p^{k-2}a(np^{r_0-1}I_{1,1}).$$

We multiply the first equation by $a(nI_{1,1})$ and the second equation by $a(mI_{1,1})$ yielding

$$\mu(p^{r_0})a(mI_{1,1})a(nI_{1,1}) = a(mp^{r_0}I_{1,1})a(nI_{1,1}) + p^{k-2}a(mp^{r_0-1}I_{1,1})a(nI_{1,1})$$

and

$$\mu(p^{r_0})a(nI_{1,1})a(mI_{1,1}) = a(np^{r_0}I_{1,1})a(mI_{1,1}) + p^{k-2}a(np^{r_0-1}I_{1,1})a(mI_{1,1}).$$

Subtracting the two equations from one another and implementing the induction hypothesis yields

$$0 = a(mp^{r_0}I_{1,1})a(nI_{1,1}) - a(np^{r_0}I_{1,1})a(mI_{1,1})$$

which is the desired result.

We now prove the claim in the case where p is inert in K. We use the formula appearing before in the inert case

$$\mu(p^{r_0})a(mI_{1,1}) = a(mp^{r_0}I_{1,1}).$$

We also consider

$$\mu(p^{r_0})a(nI_{1,1}) = a(np^{r_0}I_{1,1}).$$

Multiplying the first equation by $a(nI_{1,1})$ and the second by $a(mI_{1,1})$ gives

$$0 = a(mp^{r_0}I_{1,1})a(nI_{1,1}) - a(np^{r_0}I_{1,1})a(mI_{1,1})$$

which is the desired result.

To prove the general claim we let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$ and write

$$n = p_1^{\ell_1} p_2^{\ell_2} \cdots p_d^{\ell_d}.$$

Then by what we have proved above

$$\begin{aligned} a(I_{1,1})a(mnI_{1,1}) &= a(I_{1,1})a(mp_1^{\ell_1} p_2^{\ell_2} \cdots p_d^{\ell_d} I_{1,1}) \\ &= a(p_1^{\ell_1} I_{1,1})a(mp_2^{\ell_2} \cdots p_d^{\ell_d} I_{1,1}) \\ &= \cdots = a(nI_{1,1})a(mI_{1,1}). \end{aligned}$$

□

The proof of the previous theorem extends naturally to cover other cases where the class number is one. For fundamental discriminant $\delta < 0$ and for $f \in \mathbb{N}$ we will denote by $h(\delta f^2)$ the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{\delta})$. We note that the class number is equal to the size of the set $\mathrm{SL}(2,\mathbb{Z}) \setminus A(1,\delta f^2)$. We will denote by $h_M(\delta f^2)$ the size of the set $\Gamma_0(M) \setminus A(M,\delta f^2)$.

Theorem 6.3.3. *Let $M \geq 1$ be an integer. Let*

$$F(Z) = \sum_{S \in A(M)} a(S) e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(K(M))$$

with $k > 0$. Suppose that F is an eigenform. Let $I_{M,0}$ and $I_{M,1}$ denote the matrices

$$\begin{bmatrix} M & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} M & 1/2 \\ 1/2 & 1 \end{bmatrix}$$

respectively.

(i) If $h(-4M) = 1$, then for $m, n \in \mathbb{N}$ with n odd and $\gcd(mM, n) = 1$ we have

$$a(mnI_{M,0})a(I_{M,0}) = a(mI_{M,0})a(nI_{M,0}).$$

(ii) If $h(-4M+1) = 1$, then for $m, n \in \mathbb{N}$ with $n \not\equiv 0 \pmod 3$ and $\gcd(mM, n) = 1$ we have

$$a(mnI_{M,1})a(I_{M,1}) = a(mI_{M,1})a(nI_{M,1}).$$

More generally, suppose $\delta < 0$ is a fundamental discriminant and let $f \in \mathbb{N}$. If $h_M(\delta f^2) = 1$ then for $m, n \in \mathbb{N}$ with $\gcd(mMf, n) = 1$ we have

$$a(mnS)a(S) = a(mS)a(nS)$$

where $S \in A(M, \delta f^2)$.

Proof. The structure of the proof is similar to the proof of the previous theorem. □

We note here that $h(-4M) = 1$ for the values $M = 1, 2, 3, 4$, and 7 and $h(-4M+1) = 1$ for the values $M = 1, 2, 3, 5, 7, 11, 17$, and 41.

6.4 Arithmetic Properties of Fourier Coefficients for Arbitrary Class Number

We now prove the main results of this particular work. Let's start with a considerable extension of the results for Siegel modular forms, i.e., Siegel paramodular forms of level 1.

Theorem 6.4.1. *Let*

$$F(Z)=\sum_{S\in A(1)} a(S)e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(\mathrm{Sp}(4,\mathbb{Z}))$$

for $k>0$. Suppose that F is an eigenform. Let $S_1,\dots,S_h$ be a complete set of representatives of the classes of positive-definite, primitive, integral binary quadratic forms of discriminant δ with $\delta<0$ a fundamental discriminant.

(i) If $a(S_i)=0$ for all $i\in\{1,\dots,h\}$, then $a(mS_i)=0$ for all $m\in\mathbb{N}$ and all $i\in\{1,\dots,h\}$.

(ii) For $m,n\in\mathbb{N}$ with $\gcd(m,n)=1$ we have

$$\sum_{i=1}^{h}\sum_{j=1}^{h} a(mnS_i)a(S_j)=\sum_{i=1}^{h}\sum_{j=1}^{h} a(mS_i)a(nS_j).$$

Proof. We start by proving (i). For each S_i with $1\le i\le h$ we associate the full module G_i with ordered basis $\boldsymbol{\xi}_i$. Suppose first that p splits in $K=\mathbb{Q}(\sqrt{\delta})$. By Theorem 6.1.2 we have

$$\begin{aligned}
\mu(p)a(mS_1)&=a(mpS_1)+p^{k-2}[a(mS_{(G_1\mathfrak{p},\boldsymbol{\xi}_{1\mathfrak{p}})})+a(mS_{(G_1\overline{\mathfrak{p}},\boldsymbol{\xi}_{1\overline{\mathfrak{p}}})})]\\
\mu(p)a(mS_2)&=a(mpS_2)+p^{k-2}[a(mS_{(G_2\mathfrak{p},\boldsymbol{\xi}_{2\mathfrak{p}})})+a(mS_{(G_2\overline{\mathfrak{p}},\boldsymbol{\xi}_{2\overline{\mathfrak{p}}})})]\\
&\vdots\\
\mu(p)a(mS_h)&=a(mpS_h)+p^{k-2}[a(mS_{(G_h\mathfrak{p},\boldsymbol{\xi}_{h\mathfrak{p}})})+a(mS_{(G_h\overline{\mathfrak{p}},\boldsymbol{\xi}_{h\overline{\mathfrak{p}}})})]
\end{aligned}$$

Since $S_1,\dots,S_h$ is a complete set of representatives of the classes of positive-definite, primitive, integral binary quadratic forms of discriminant δ we have that $(G_1,\boldsymbol{\xi}_1),(G_2,\boldsymbol{\xi}_2),\dots,(G_h,\boldsymbol{\xi}_h)$ is a complete set of representatives of the classes in $\overline{\mathscr{M}}_{\mathrm{SL}(2,\mathbb{Z})}(\delta)$. Since the maps $\Phi(\cdot,[\mathfrak{p}]):\overline{\mathscr{M}}_{\mathrm{SL}(2,\mathbb{Z})}(\delta)\to\overline{\mathscr{M}}_{\mathrm{SL}(2,\mathbb{Z})}(\delta)$ and $\Phi(\cdot,[\overline{\mathfrak{p}}]):\overline{\mathscr{M}}_{\mathrm{SL}(2,\mathbb{Z})}(\delta)\to\overline{\mathscr{M}}_{\mathrm{SL}(2,\mathbb{Z})}(\delta)$ are surjections (hence bijections), we have that $S_{(G_1\mathfrak{p},\boldsymbol{\xi}_{1\mathfrak{p}})},S_{(G_2\mathfrak{p},\boldsymbol{\xi}_{2\mathfrak{p}})},\dots,S_{(G_h\mathfrak{p},\boldsymbol{\xi}_{h\mathfrak{p}})}$ and $S_{(G_1\overline{\mathfrak{p}},\boldsymbol{\xi}_{1\overline{\mathfrak{p}}})},S_{(G_2\overline{\mathfrak{p}},\boldsymbol{\xi}_{2\overline{\mathfrak{p}}})},\dots,S_{(G_h\overline{\mathfrak{p}},\boldsymbol{\xi}_{h\overline{\mathfrak{p}}})}$ are both complete sets of representatives of the classes of positive-definite, primitive, integral binary quadratic forms of discriminant δ. Thus if $a(mS_i)=0$ for each i we have

$$a(mS_{(G_i\mathfrak{p},\boldsymbol{\xi}_{i\mathfrak{p}})})=a(mS_{(G_i\overline{\mathfrak{p}},\boldsymbol{\xi}_{i\overline{\mathfrak{p}}})})=0$$

for each i. Thus $a(mpS_i)=0$ for all i.

We now prove by induction that if $a(mS_i)=0$ for all i, then $a(mp^{r_0}S_i)=0$ for all i and all $r_0\ge 1$. We proved the case $r_0=1$ above. Assume now that the claim has been proven for all positive integers less than r_0. Since

$$\mu(p^{r_0})a(mS_1) = a(mp^{r_0}S_1) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}S_{(G_1\mathfrak{p}^\beta,\boldsymbol{\xi}_{1\mathfrak{p}^\beta})}) + a(mp^{r_0-\beta}S_{(G_1\overline{\mathfrak{p}}^\beta,\boldsymbol{\xi}_{1\overline{\mathfrak{p}}^\beta})})]$$

$$\mu(p^{r_0})a(mS_2) = a(mp^{r_0}S_2) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}S_{(G_2\mathfrak{p}^\beta,\boldsymbol{\xi}_{2\mathfrak{p}^\beta})}) + a(mp^{r_0-\beta}S_{(G_2\overline{\mathfrak{p}}^\beta,\boldsymbol{\xi}_{2\overline{\mathfrak{p}}^\beta})})]$$

$$\vdots$$

$$\mu(p^{r_0})a(mS_h) = a(mp^{r_0}S_h) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}S_{(G_h\mathfrak{p}^\beta,\boldsymbol{\xi}_{h\mathfrak{p}^\beta})}) + a(mp^{r_0-\beta}S_{(G_h\overline{\mathfrak{p}}^\beta,\boldsymbol{\xi}_{h\overline{\mathfrak{p}}^\beta})})]$$

By the induction hypothesis we have that $a(mp^{r_0}S_i) = 0$ for each i. The proof is similar when p is ramified or inert in K.

To prove the general claim we assume that $a(S_i) = 0$ for each i and let

$$m = p_1^{\ell_1} p_2^{\ell_2} \cdots p_d^{\ell_d}.$$

Then using what we have proven, we have that $a(mS_i) = 0$ for each i. This proves (i).

We now prove (ii). We prove only the case where p is split in K as the proof is similar in the other cases. We consider

$$\mu(p)a(mS_1) = a(mpS_1) + p^{k-2}[a(mS_{(G_1\mathfrak{p},\boldsymbol{\xi}_{1\mathfrak{p}})}) + a(mS_{(G_1\overline{\mathfrak{p}},\boldsymbol{\xi}_{1\overline{\mathfrak{p}}})})]$$

$$\mu(p)a(mS_2) = a(mpS_2) + p^{k-2}[a(mS_{(G_2\mathfrak{p},\boldsymbol{\xi}_{2\mathfrak{p}})}) + a(mS_{(G_2\overline{\mathfrak{p}},\boldsymbol{\xi}_{2\overline{\mathfrak{p}}})})]$$

$$\vdots$$

$$\mu(p)a(mS_h) = a(mpS_h) + p^{k-2}[a(mS_{(G_h\mathfrak{p},\boldsymbol{\xi}_{h\mathfrak{p}})}) + a(mS_{(G_h\overline{\mathfrak{p}},\boldsymbol{\xi}_{h\overline{\mathfrak{p}}})})]$$

Applying a similar argument as before we have that $S_{(G_1\mathfrak{p}^\beta,\boldsymbol{\xi}_{1\mathfrak{p}^\beta})}, S_{(G_2\mathfrak{p}^\beta,\boldsymbol{\xi}_{2\mathfrak{p}^\beta})}, \ldots, S_{(G_h\mathfrak{p}^\beta,\boldsymbol{\xi}_{h\mathfrak{p}^\beta})}$ and $S_{(G_1\overline{\mathfrak{p}}^\beta,\boldsymbol{\xi}_{1\overline{\mathfrak{p}}^\beta})}, S_{(G_2\overline{\mathfrak{p}}^\beta,\boldsymbol{\xi}_{2\overline{\mathfrak{p}}^\beta})}, \ldots, S_{(G_h\overline{\mathfrak{p}}^\beta,\boldsymbol{\xi}_{h\overline{\mathfrak{p}}^\beta})}$ both form a complete set of representatives of the classes of positive-definite, primitive, integral binary quadratic forms of discriminant δ. We also consider the equations

$$\mu(p)a(nS_1) = a(npS_1) + p^{k-2}[a(nS_{(G_1\mathfrak{p},\boldsymbol{\xi}_{1\mathfrak{p}})}) + a(nS_{(G_1\overline{\mathfrak{p}},\boldsymbol{\xi}_{1\overline{\mathfrak{p}}})})]$$

$$\mu(p)a(nS_2) = a(npS_2) + p^{k-2}[a(nS_{(G_2\mathfrak{p},\boldsymbol{\xi}_{2\mathfrak{p}})}) + a(nS_{(G_2\overline{\mathfrak{p}},\boldsymbol{\xi}_{2\overline{\mathfrak{p}}})})]$$

$$\vdots$$

$$\mu(p)a(nS_h) = a(npS_h) + p^{k-2}[a(nS_{(G_h\mathfrak{p},\boldsymbol{\xi}_{h\mathfrak{p}})}) + a(nS_{(G_h\overline{\mathfrak{p}},\boldsymbol{\xi}_{h\overline{\mathfrak{p}}})})]$$

For some fixed j with $1 \leq j \leq h$ we multiply to the first set of equations by

$$\sum_{j=1}^{h} a(nS_j)$$

and the second set of equations by

$$\sum_{j=1}^{h} a(mS_j)$$

which gives

$$\mu(p)a(mS_1)\sum_{j=1}^{h} a(nS_j) = a(mpS_1)\sum_{j=1}^{h} a(nS_j) + p^{k-2}[a(mS_{(G_1\mathfrak{p},\boldsymbol{\xi}_{1\mathfrak{p}})})\sum_{j=1}^{h} a(nS_j) + a(mS_{(G_1\overline{\mathfrak{p}},\boldsymbol{\xi}_{1\overline{\mathfrak{p}}})})\sum_{j=1}^{h} a(nS_j)]$$

$$\mu(p)a(mS_2)\sum_{j=1}^{h} a(nS_j) = a(mpS_2)\sum_{j=1}^{h} a(nS_j) + p^{k-2}[a(mS_{(G_2\mathfrak{p},\boldsymbol{\xi}_{2\mathfrak{p}})})\sum_{j=1}^{h} a(nS_j) + a(mS_{(G_2\overline{\mathfrak{p}},\boldsymbol{\xi}_{2\overline{\mathfrak{p}}})})\sum_{j=1}^{h} a(nS_j)]$$

$$\vdots$$

$$\mu(p)a(mS_h)\sum_{j=1}^{h} a(nS_j) = a(mpS_h)\sum_{j=1}^{h} a(nS_j) + p^{k-2}[a(mS_{(G_h\mathfrak{p},\boldsymbol{\xi}_{h\mathfrak{p}})})\sum_{j=1}^{h} a(nS_j) + a(mS_{(G_h\overline{\mathfrak{p}},\boldsymbol{\xi}_{h\overline{\mathfrak{p}}})})\sum_{j=1}^{h} a(nS_j)]$$

and

$$\mu(p)a(nS_1)\sum_{j=1}^{h} a(mS_j) = a(npS_1)\sum_{j=1}^{h} a(mS_j) + p^{k-2}[a(nS_{(G_1\mathfrak{p},\boldsymbol{\xi}_{1\mathfrak{p}})})\sum_{j=1}^{h} a(mS_j) + a(nS_{(G_1\overline{\mathfrak{p}},\boldsymbol{\xi}_{1\overline{\mathfrak{p}}})})\sum_{j=1}^{h} a(mS_j)]$$

$$\mu(p)a(nS_2)\sum_{j=1}^{h} a(mS_j) = a(npS_2)\sum_{j=1}^{h} a(mS_j) + p^{k-2}[a(nS_{(G_2\mathfrak{p},\boldsymbol{\xi}_{2\mathfrak{p}})})\sum_{j=1}^{h} a(mS_j) + a(nS_{(G_2\overline{\mathfrak{p}},\boldsymbol{\xi}_{2\overline{\mathfrak{p}}})})\sum_{j=1}^{h} a(mS_j)]$$

$$\vdots$$

$$\mu(p)a(nS_h)\sum_{j=1}^{h} a(mS_j) = a(npS_h)\sum_{j=1}^{h} a(mS_j) + p^{k-2}[a(nS_{(G_h\mathfrak{p},\boldsymbol{\xi}_{h\mathfrak{p}})})\sum_{j=1}^{h} a(mS_j) + a(nS_{(G_h\overline{\mathfrak{p}},\boldsymbol{\xi}_{h\overline{\mathfrak{p}}})})\sum_{j=1}^{h} a(mS_j)]$$

Adding each system separately and then taking their cumulative difference we obtain

$$0 = \sum_{i=1}^{h} a(mpS_i)\sum_{j=1}^{h} a(nS_j) - \sum_{i=1}^{h} a(npS_i)\sum_{j=1}^{h} a(mS_j).$$

This proves that

$$\sum_{i=1}^{h}\sum_{j=1}^{h} a(mpS_i)a(nS_j) = \sum_{i=1}^{h}\sum_{j=1}^{h} a(mS_i)a(npS_j)$$

We proceed by induction. We assume that the claim has been proved for all positive integers less than r_0. That is

$$\sum_{i=1}^{h}\sum_{j=1}^{h} a(mp^{\ell}S_i)a(nS_j) = \sum_{i=1}^{h}\sum_{j=1}^{h} a(mS_i)a(np^{\ell}S_j)$$

We then consider

$$\mu(p^{r_0})a(mS_1) = a(mp^{r_0}S_1) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}S_{(G_1\mathfrak{p}^\beta, \boldsymbol{\xi}_{1\mathfrak{p}^\beta})}) + a(mp^{r_0-\beta}S_{(G_1\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{1\overline{\mathfrak{p}}^\beta})})]$$

$$\mu(p^{r_0})a(mS_2) = a(mp^{r_0}S_2) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}S_{(G_2\mathfrak{p}^\beta, \boldsymbol{\xi}_{2\mathfrak{p}^\beta})}) + a(mp^{r_0-\beta}S_{(G_2\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{2\overline{\mathfrak{p}}^\beta})})]$$

$$\vdots$$

$$\mu(p^{r_0})a(mS_h) = a(mp^{r_0}S_h) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(mp^{r_0-\beta}S_{(G_h\mathfrak{p}^\beta, \boldsymbol{\xi}_{h\mathfrak{p}^\beta})}) + a(mp^{r_0-\beta}S_{(G_h\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{h\overline{\mathfrak{p}}^\beta})})]$$

and

$$\mu(p^{r_0})a(nS_1) = a(np^{r_0}S_1) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(np^{r_0-\beta}S_{(G_1\mathfrak{p}^\beta, \boldsymbol{\xi}_{1\mathfrak{p}^\beta})}) + a(np^{r_0-\beta}S_{(G_1\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{1\overline{\mathfrak{p}}^\beta})})]$$

$$\mu(p^{r_0})a(nS_2) = a(np^{r_0}S_2) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(np^{r_0-\beta}S_{(G_2\mathfrak{p}^\beta, \boldsymbol{\xi}_{2\mathfrak{p}^\beta})}) + a(np^{r_0-\beta}S_{(G_2\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{2\overline{\mathfrak{p}}^\beta})})]$$

$$\vdots$$

$$\mu(p^{r_0})a(nS_h) = a(np^{r_0}S_h) + \sum_{\beta=1}^{r_0} p^{(k-2)\beta}[a(np^{r_0-\beta}S_{(G_h\mathfrak{p}^\beta, \boldsymbol{\xi}_{h\mathfrak{p}^\beta})}) + a(np^{r_0-\beta}S_{(G_h\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{h\overline{\mathfrak{p}}^\beta})})]$$

As before, we multiply the first set of equations by

$$\sum_{j=1}^{h} a(nS_j)$$

and the second set of equations by

$$\sum_{j=1}^{h} a(mS_j).$$

We then obtain

$$\begin{aligned}\mu(p^{r_0})a(mS_1)\sum_{j=1}^{h} a(nS_j) &= a(mp^{r_0}S_1)\sum_{j=1}^{h} a(nS_j)\\ &+ \sum_{\beta=1}^{r_0} p^{(k-2)\beta}\left[a(mp^{r_0-\beta}S_{(G_1\mathfrak{p}^\beta, \boldsymbol{\xi}_{1\mathfrak{p}^\beta})})\sum_{j=1}^{h} a(nS_j) + a(mp^{r_0-\beta}S_{(G_1\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{1\overline{\mathfrak{p}}^\beta})})\sum_{j=1}^{h} a(nS_j)\right]\end{aligned}$$

$$\begin{aligned}\mu(p^{r_0})a(mS_2)\sum_{j=1}^{h} a(nS_j) &= a(mp^{r_0}S_2)\sum_{j=1}^{h} a(nS_j)\\ &+ \sum_{\beta=1}^{r_0} p^{(k-2)\beta}\left[a(mp^{r_0-\beta}S_{(G_2\mathfrak{p}^\beta, \boldsymbol{\xi}_{2\mathfrak{p}^\beta})})\sum_{j=1}^{h} a(nS_j) + a(mp^{r_0-\beta}S_{(G_2\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{2\overline{\mathfrak{p}}^\beta})})\sum_{j=1}^{h} a(nS_j)\right]\end{aligned}$$

$$\vdots$$

$$\begin{aligned}\mu(p^{r_0})a(mS_h)\sum_{j=1}^{h} a(nS_j) &= a(mp^{r_0}S_h)\sum_{j=1}^{h} a(nS_j)\\ &+ \sum_{\beta=1}^{r_0} p^{(k-2)\beta}\left[a(mp^{r_0-\beta}S_{(G_h\mathfrak{p}^\beta, \boldsymbol{\xi}_{h\mathfrak{p}^\beta})})\sum_{j=1}^{h} a(nS_j) + a(mp^{r_0-\beta}S_{(G_h\overline{\mathfrak{p}}^\beta, \boldsymbol{\xi}_{h\overline{\mathfrak{p}}^\beta})})\sum_{j=1}^{h} a(nS_j)\right]\end{aligned}$$

and

$$\begin{aligned}
\mu(p^{r_0})a(nS_1)\sum_{j=1}^{h}a(mS_j) &= a(np^{r_0}S_1)\sum_{j=1}^{h}a(mS_j)\\
&\quad+\sum_{\beta=1}^{r_0}p^{(k-2)\beta}\left[a(np^{r_0-\beta}S_{(G_1\mathfrak{p}^\beta,\boldsymbol{\xi}_{1\mathfrak{p}^\beta})})\sum_{j=1}^{h}a(mS_j)+a(np^{r_0-\beta}S_{(G_1\overline{\mathfrak{p}}^\beta,\boldsymbol{\xi}_{1\overline{\mathfrak{p}}^\beta})})\sum_{j=1}^{h}a(mS_j)\right]\\
\mu(p^{r_0})a(nS_2)\sum_{j=1}^{h}a(mS_j) &= a(np^{r_0}S_2)\sum_{j=1}^{h}a(mS_j)\\
&\quad+\sum_{\beta=1}^{r_0}p^{(k-2)\beta}\left[a(np^{r_0-\beta}S_{(G_2\mathfrak{p}^\beta,\boldsymbol{\xi}_{2\mathfrak{p}^\beta})})\sum_{j=1}^{h}a(mS_j)+a(np^{r_0-\beta}S_{(G_2\overline{\mathfrak{p}}^\beta,\boldsymbol{\xi}_{2\overline{\mathfrak{p}}^\beta})})\sum_{j=1}^{h}a(mS_j)\right]\\
&\;\;\vdots\\
\mu(p^{r_0})a(nS_h)\sum_{j=1}^{h}a(mS_j) &= a(np^{r_0}S_h)\sum_{j=1}^{h}a(mS_j)\\
&\quad+\sum_{\beta=1}^{r_0}p^{(k-2)\beta}\left[a(np^{r_0-\beta}S_{(G_h\mathfrak{p}^\beta,\boldsymbol{\xi}_{h\mathfrak{p}^\beta})})\sum_{j=1}^{h}a(mS_j)+a(np^{r_0-\beta}S_{(G_h\overline{\mathfrak{p}}^\beta,\boldsymbol{\xi}_{h\overline{\mathfrak{p}}^\beta})})\sum_{j=1}^{h}a(mS_j)\right]
\end{aligned}$$

Adding each set of equations together and taking their cumulative difference, keeping in mind the induction hypothesis, we obtain

$$0=\sum_{i=1}^{h}a(mp^{r_0}S_i)\sum_{j=1}^{h}a(nS_j)-\sum_{i=1}^{h}a(np^{r_0}S_i)\sum_{j=1}^{h}a(mS_j).$$

It then follows that

$$\sum_{i=1}^{h}\sum_{j=1}^{h}a(mp^{r_0}S_i)a(nS_j)=\sum_{i=1}^{h}\sum_{j=1}^{h}a(mS_i)a(np^{r_0}S_j).$$

This completes the proof of the claim. □

We obtain the following theorem essentially as a corollary to the previous result.

Theorem 6.4.2. *Let*

$$F(Z)=\sum_{S\in A(1)}a(S)e^{2\pi i\operatorname{tr}(SZ)}\in\mathcal{M}_k(\mathrm{Sp}(4,\mathbb{Z}))$$

for $k>0$. Suppose that F is an eigenform. Let $S_1,\ldots,S_h$ be a complete set of representatives of the classes of positive-definite, primitive, integral binary quadratic forms of discriminant δf^2 with $\delta<0$ a fundamental discriminant and $f\in\mathbb{N}$.

(i) If $a(S_i)=0$ for all $i\in\{1,\ldots,h\}$, then $a(mS_i)=0$ for all $m\in\mathbb{N}$ with $\gcd(m,f)=1$ and all $i\in\{1,\ldots,h\}$.

(ii) For $m,n\in\mathbb{N}$ with $\gcd(m,n)=1$ and $\gcd(n,f)=1$ we have

$$\sum_{i=1}^{h}\sum_{j=1}^{h}a(mnS_i)a(S_j)=\sum_{i=1}^{h}\sum_{j=1}^{h}a(mS_i)a(nS_j).$$

We have another modest extension of these theorems.

Theorem 6.4.3. *Let*

$$F(Z) = \sum_{S \in A(1)} a(S) e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(\mathrm{Sp}(4,\mathbb{Z}))$$

for $k > 0$. Suppose that F is an eigenform. Let $S_1, \ldots, S_h$ be a complete set of representatives of the classes of positive-definite, primitive, integral binary quadratic forms of discriminant δf^2 with $\delta < 0$ a fundamental discriminant and $f \in \mathbb{N}$.

(i) If

$$\sum_{i=1}^{h} a(S_i) = 0$$

then

$$\sum_{i=1}^{h} a(mS_i) = 0$$

for all $m \in \mathbb{N}$ with $\gcd(m, f) = 1$.

(ii) For $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$ and $\gcd(n, f) = 1$ we have

$$\sum_{i=1}^{h} a(mnS_i) a(S_i) = \sum_{i=1}^{h} a(mS_i) a(nS_i).$$

We present here also the general result for Siegel paramodular forms.

Theorem 6.4.4. *Let $M \geq 1$ be an integer and let*

$$F(Z) = \sum_{S \in A(M)} a(S) e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(\mathrm{K}(M))$$

for $k > 0$. Suppose that F is an eigenform. Let $\delta < 0$ be a fundamental discriminant and let $f \in \mathbb{N}$. Let $S_1, \ldots, S_d$ be a complete set of representatives of the set $\Gamma_0(M) \setminus A(M, \delta f^2)$.

(i) If $a(S_i) = 0$ for all $i \in \{1, \ldots, d\}$, then $a(mS_i) = 0$ for all $m \in \mathbb{N}$ with $\gcd(m, Mf) = 1$ and all $i \in \{1, \ldots, h\}$. Moreover, if

$$\sum_{i=1}^{d} a(S_i) = 0$$

then

$$\sum_{i=1}^{d} a(mS_i) = 0$$

for all $m \in \mathbb{N}$ *with* $\gcd(m, Mf) = 1$.

(ii) For $m, n \in \mathbb{N}$ *with* $\gcd(mM, n) = 1$ *and* $\gcd(n, f) = 1$ *we have*

$$\sum_{i=1}^{d}\sum_{j=1}^{d} a(mnS_i)a(S_j) = \sum_{i=1}^{d}\sum_{j=1}^{d} a(mS_i)a(nS_j).$$

For paramodular level $M > 1$, we saw in section 5.6 that for a fixed discriminant δf^2 with $\delta < 0$ a fundamental discriminant and $f \in \mathbb{N}$ it is possible for $A(M, \delta f^2)$ to be empty. We saw however that the sets $A(M, -4M)$ and $A(M, -4M + 1)$ are always nonempty. Fourier coefficients indexed by elements in these sets exhibit relations involving all primes p not dividing M. In particular, we have the following corollary.

Corollary 6.4.5. *Let* $M \geq 1$ *be an integer and let*

$$F(Z) = \sum_{S \in A(M)} a(S)e^{2\pi i \operatorname{tr}(SZ)} \in \mathcal{M}_k(\mathrm{K}(M))$$

for $k > 0$. *Suppose that* F *is an eigenform. Let* $-4M = \delta_1 f_1^2$ *and* $-4M + 1 = \delta_2 f_2^2$ *with* $f_1, f_2 \in \mathbb{N}$ *and where* $\delta_1, \delta_2 < 0$ *are fundamental discriminants. Let* $S_1, \ldots, S_{d_1}$ *and* $T_1, \ldots, T_{d_2}$ *be a complete set of representatives of* $\Gamma_0(M) \setminus A(M, -4M)$ *and* $\Gamma_0(M) \setminus A(M, -4M + 1)$ *respectively. Let* Ω_{f_i} *be the set of primes* p *with* $\gcd(p, Mf_i) = 1$ *for* $i = 1, 2$.

(i) If $a(S_i) = 0$ *for all* $i \in \{1, \ldots, d_1\}$, *then* $a(mS_i) = 0$ *for all* $m \in \mathbb{N}$ *with* $\gcd(m, Mf) = 1$ *and all* $i \in \{1, \ldots, d_1\}$. *Moreover, if*

$$\sum_{i=1}^{d_1} a(S_i) = 0$$

then

$$\sum_{i=1}^{d_1} a(mS_i) = 0$$

for all $m \in \mathbb{N}$ *with* $\gcd(m, Mf) = 1$.

(ii) For $m, n \in \mathbb{N}$ *and* $p \in \Omega_{f_1}$ *a prime with* $\gcd(mn, p) = 1$ *we have for all* $\ell \geq 1$

$$\sum_{i=1}^{d_1}\sum_{j=1}^{d_1} a(mp^\ell S_i)a(nS_j) = \sum_{i=1}^{d_1}\sum_{j=1}^{d_1} a(mS_i)a(np^\ell S_j).$$

(iii) For $m, n \in \mathbb{N}$ *with* $p \in \Omega_{f_2}$ *a prime with* $\gcd(mn, p) = 1$ *we have for all* $\ell \geq 1$

$$\sum_{i=1}^{d_2}\sum_{j=1}^{d_2} a(mp^\ell T_i)a(nT_j) = \sum_{i=1}^{d_2}\sum_{j=1}^{d_2} a(mT_i)a(np^\ell T_j).$$

We also have the following general result which will conclude this section.

Theorem 6.4.6. *Let $M \geq 1$ be an integer and let*

$$F(Z) = \sum_{S \in A(M)} a(S) e^{2\pi i \operatorname{tr}(SZ)} \in \mathcal{M}_k(\mathrm{K}(M))$$

for $k > 0$. Suppose that F is an eigenform. Let $\delta < 0$ be a fundamental discriminant and let $f \in \mathbb{N}$. Let $S_1, \ldots, S_d$ be a complete set of representatives of the set $\Gamma_0(M) \setminus A(M, \delta f^2)$. For $[\mathfrak{u}] \in H(\mathfrak{o}_f, M)$, the matrix $S_{\mathfrak{u}}$ is determined by the action of $H(\mathfrak{o}_f, M)$ on $\overline{\mathscr{A}}(M, \delta f^2)$.

(i) If $a(S_{\mathfrak{u}}) = 0$ for all $[\mathfrak{u}] \in H(\mathfrak{o}_f, M)$, then $a(mS_{\mathfrak{u}}) = 0$ for all $m \in \mathbb{N}$ with $\gcd(m, Mf) = 1$ and all $i \in \{1, \ldots, h\}$. Moreover, if

$$\sum_{[\mathfrak{u}] \in H(\mathfrak{o}_f, M)} a(S_{\mathfrak{u}}) = 0$$

then

$$\sum_{[\mathfrak{u}] \in H(\mathfrak{o}_f, M)} a(mS_{\mathfrak{u}}) = 0$$

for all $m \in \mathbb{N}$ with $\gcd(m, Mf) = 1$.

(ii) For $m, n \in \mathbb{N}$ with $\gcd(mM, n) = 1$ and $\gcd(n, f) = 1$ we have

$$\sum_{[\mathfrak{u}] \in H(\mathfrak{o}_f, M)} \sum_{[\mathfrak{v}] \in H(\mathfrak{o}_f, M)} a(mnS_{\mathfrak{u}}) a(S_{\mathfrak{v}}) = \sum_{[\mathfrak{u}] \in H(\mathfrak{o}_f, M)} \sum_{[\mathfrak{v}] \in H(\mathfrak{o}_f, M)} a(mS_{\mathfrak{u}}) a(nS_{\mathfrak{v}}).$$

Proof. The proof is very similar to the proof of the other results. We only note here that we utilize the fact that $H(\mathfrak{o}_f, M)[\mathfrak{p}^\beta] = H(\mathfrak{o}_f, M)$ for all $\beta \geq 1$ where $\mathfrak{p}$ is a given prime ideal in $\mathfrak{o}_f$ of norm p or p^2 depending on whether p is split, ramified, or inert in $K = \mathbb{Q}(\sqrt{\delta})$. $\square$

One could check the validity of these results by accessing the L-functions and Modular Forms Database [23] and utilize the calculated Fourier coefficients of the small number of Siegel paramodular forms that are present there. For example, the Siegel paramodular form of weight 2 and level 277 has non-zero Fourier coefficients indexed by primitive binary quadratic forms in $A(277)$ of discriminant -4. In fact, there is exactly one coefficient attached the form

$$\begin{bmatrix} 3601 & 60 \\ 60 & 1 \end{bmatrix}$$

with value

$$a\left(\begin{bmatrix} 3601 & 60 \\ 60 & 1 \end{bmatrix}\right) = -2.$$

We then check the following Fourier coefficients and find that

$$a\left(2\begin{bmatrix}3601 & 60\\ 60 & 1\end{bmatrix}\right) = 6,$$

$$a\left(3\begin{bmatrix}3601 & 60\\ 60 & 1\end{bmatrix}\right) = 2,$$

$$a\left(6\begin{bmatrix}3601 & 60\\ 60 & 1\end{bmatrix}\right) = -6,$$

from which it is easy to see that

$$a\left(\begin{bmatrix}3601 & 60\\ 60 & 1\end{bmatrix}\right) a\left(6\begin{bmatrix}3601 & 60\\ 60 & 1\end{bmatrix}\right) = a\left(2\begin{bmatrix}3601 & 60\\ 60 & 1\end{bmatrix}\right) a\left(3\begin{bmatrix}3601 & 60\\ 60 & 1\end{bmatrix}\right).$$

6.5 Action of Hecke Operators on Fourier Coefficients, $p|M$

We conclude this manuscript with a formula for the action of the paramodular Hecke operator $T(p)$ on a Siegel paramodular form of weight $k > 0$ and squarefree level M for bad primes p, i.e., those primes p dividing M. In particular we provide a formula for

$$T(p) = p^{k-3}\left[K(M)\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & p & 0\\ 0 & 0 & 0 & p\end{bmatrix}K(M)\right]_k.$$

The reader should see [24] for a version of the formula pertaining to this operator. One needs to be especially careful regarding any change of index utilized in applying these operators to a Siegel paramodular form.

Theorem 6.5.1. *Let $M \geq 1$ be an integer and let*

$$F(Z) = \sum_{S\in A(M)} a(S)e^{2\pi i \mathrm{tr}(SZ)} \in \mathcal{M}_k(K(M))$$

with $k > 0$. Let

$$S = \begin{bmatrix}Mr & t/2\\ t/2 & s\end{bmatrix}$$

Let $M' = M/p$ and let N be an inverse of M' modulo p. Then

$$(T(p))(F(Z)) = \sum_{S\in A(M)} b(S)e^{2\pi i tr(SZ)}$$

and

$$
\begin{aligned}
b(S) =& a(pS) + p^{k-2} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} d_p(s+tx) a\left(p^{-1} \begin{bmatrix} p & 0 \\ x & 1 \end{bmatrix} S \begin{bmatrix} p & x \\ 0 & 1 \end{bmatrix}\right) \\
&+ p^{k-2} \sum_{y \in \mathbb{Z}/p\mathbb{Z}} d_p(r - Nty) a\left(p^{-1} \begin{bmatrix} 1 & -yMN \\ 0 & p \end{bmatrix} S \begin{bmatrix} 1 & 0 \\ -yMN & p \end{bmatrix}\right) \\
&+ (-1)^k p^{k-3} (d_p(t)p - 1) a\left(p^{-1} \begin{bmatrix} (MN-p)p^{-1} & MN \\ 1 & p \end{bmatrix} S \begin{bmatrix} (MN-p)p^{-1} & 1 \\ MN & p \end{bmatrix}\right) \\
&+ p^{2k-3} d_p(r,t,s) a(p^{-1}S)
\end{aligned}
$$

Proof. This is a direct computation utilizing the decomposition appearing in Theorem 4.3.13. □

One can carry out a similar computation for the second operator

$$
T_1(p^2) = p^{2(k-3)} \left[K(M) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{bmatrix} K(M) \right]_k
$$

using the double coset decompostion appearing in Theorem 4.3.13. However, in order to extend our results from Chapter 6 in the case $p|M$ one should really consider the operators $T(p^{r_0})$ for $r_0 \geq 2$.

References

[1] Andrianov, A.N. *Dirichlet series with Euler product in the theory of Siegel modular forms of genus two.* (Russian) Collection of articles dedicated to Academician Ivan Matveevič Vinogradov on his eightieth birthday, I. Trudy Mat. Inst. Steklov. **112** (1971), 73-94, 386.

[2] Andrianov A.N. *Quadratic forms and Hecke operators.* Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 286. Springer-Verlag, Berlin, 1987. xii+374 pp.

[3] Andrianov A.N. *Euler products that correspond to Siegel's modular forms of genus 2.* (Russian) Uspehi Mat. Nauk **29** (1974), no. 3 (177), 43-110.

[4] Andrianov, A.N. *Rationality theorems for Hecke series and zeta functions of the groups* GL_n *and* Sp_n *over local fields.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 466-505.

[5] Andrianov, A.N.; Zhuravlëv, V.G. *Modular forms and Hecke operators.* Translated from the 1990 Russian original by Neal Koblitz. Translations of Mathematical Monographs, 145. American Mathematical Society, Providence, RI, 1995. viii+334 pp.

[6] Brumer, Armand; Kramer, Kenneth *Paramodular abelian varieties of odd conductor.* Trans. Amer. Math. Soc. 366 (2014), no. 5, 2463-2516.

[7] Borevich, A.I.; Shafarevich, I.R. *Number theory.* Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20 Academic Press, New York-London, 1966. x+435 pp.

[8] Bump, Daniel *Automorphic forms and representations.* Cambridge Studies in Advanced Mathematics, 55. Cambridge University Press, Cambridge, 1997. xiv+574 pp.

[9] Buchmann, Johannes; Vollmer, Ulrich *Binary quadratic forms, an algorithmic approach.* Algorithms and Computation in Mathematics, 20. Springer, Berlin, 2007. xiv+318 pp.

[10] Cho, Bumkyu *On the* Γ*-equivalence of binary quadratic forms.* arXiv: 1711.00230 [math.NT], 2017, 1-22, URL: https://arxiv.org/abs/1711.00230.

[11] Cox, David A. *Primes of the form* $x^2 + ny^2$*. Fermat, class field theory, and complex multiplication.* Second edition. Pure and Applied Mathematics (Hoboken). John Wiley and Sons, Inc., Hoboken, NJ, 2013. xviii+356 pp.

[12] Diamond, Fred; Shurman, Jerry *A first course in modular forms.* Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005. xvi+436 pp.

[13] Evdokimov, S.A. *Euler products for congruences subgroups of the Siegel group of genus 2.* (Russian) Mat. Sb. (N.S.) **99(141)** (1976), no. 4, 483-513.

[14] Edixhoven, Bas; van der Geer, Gerard; Moonen, Ben *Modular forms.* Modular Forms on Schiermonnikoog, Cambridge University Press, Cambridge, 2008, 1-11.

[15] Hafner, James Lee; Walling, Lynne H. *Explicit action of Hecke operators on Siegel modular forms.* J. Number Theory 93 (2012), no. 1, 34-57.

[16] Heilbronn, H. *Zeta functions and L-functions.* Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 204-230, Thompson, Washington, D.C., 1967.

[17] Ibukiyama, Tomoyoshi *On symplectic Euler factors of genus two.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. 30 (1984), no. 3, 587-614.

[18] Johnson-Leung, Jennifer; Roberts, Brooks *Siegel modular forms of degree two attached to Hilbert modular forms.* J. Number Theory 132 (2012), no. 4, 543-564.

[19] Johnson-Leung, Jennifer; Roberts, Brooks *Twisting of Siegel paramodular forms.* Int. J. Number Theory 13 (2017), no. 7, 1755-1854.

[20] Johnson-Leung, Jennifer; Roberts, Brooks *Fourier coefficients for twists of Siegel paramodular forms.* J. Ramanujan Math. Soc. 32 (2017), no. 2, 101-119.

[21] Kilford, L.J.P. *Modular forms, a classical and computational introduction.* Second edition. Imperial College Press, London, 2015. xii+239 pp.

[22] Lang, Serge *Algebraic number theory.* Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994. xiv+357 pp.

[23] The LMFDB Collaboration, The L-functions and Modular Forms Database. URL:http://www.lmfdb.org, 2019.

[24] Marzec, Jolanta *Non-vanishing of fundamental Fourier coefficients of paramodular forms.* J. Number Theory 182 (2018), 311-324.

[25] McCarthy, Dermot *Multiplicative relations for Fourier coefficients of degree 2 Siegel eigenforms.* J. Number Theory 170 (2017), 263-281.

[26] Milne, J.S. *Class field theory (v4.02).* Course notes in class field theory (2013), viii+281 pp. URL:www.jmilne.org/math/CourseNotes/CFT.pdf.

[27] Miyake, Toshitsune *Modular forms* Translated from the 1976 Japanese original by Yoshitaka Maeda. Reprint of the first 1989 English edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006. x+335 pp.

[28] Mordell, Louis J. *On Mr. Ramanujan's empirical expansions of modular functions.* Proceedings of the Cambridge Philosphical Society. **19** (1917), 117-124.

[29] Newman, Morris *Integral matrices.* Pure and Applied Mathematics, Vol. 45. Academic Press, New York-London, 1972. xvii+224 pp.

[30] Pizer, Arnold *Hecke operators for* $\Gamma_0(N)$. J. Algebra 83 (1983), no. 1, 39-64.

[31] Poor, Cris; Shurman, Jerry; Yuen, David S. *Siegel paramodular forms of weight 2 and squarefree level.* Int. J. Number Theory 13 (2017), no. 10, 2627-2652.

[32] Poor, Cris; Schmidt, Ralf; Yuen, David S. *Paramodular forms of level 8 and weights 10 and 12.* Int. J. Number Theory 14 (2018), no. 2, 417-467.

[33] Poor, Cris; Yuen, David S. *Paramodular cusp forms.* Math. Comp. 84 (2015), no. 293, 1401-1438.

[34] Roberts, Brooks; Schmidt, Ralf *Local newforms for* GSp(4). Lecture Notes in Mathematics, 1918. Springer-Berlin, 2007, viii+307 pp.

[35] Roberts, Brooks; Schmidt, Ralf *On modular forms for the paramodular group.* Automorphic Forms and Zeta Functions, 334-364, World Sci. Publ., Hackensack, NJ, 2006.

[36] Schertz, Reinhard *Complex multiplication.* New Mathematical Monographs, 15. Cambridge University Press, Cambridge, 2010. xiv+361 pp.

[37] Shimura, Goro *On modular correspondences for* $\mathrm{Sp}(n,\mathbb{Z})$ *and their congruence relations.* Proc. Nat. Acad. Sci. U.S.A. **49** (1963), 824-828.

[38] Shimura, Goro *Modular forms: basics and beyond.* Springer Monographs in Mathematics. Springer, New York, 2012. x+175 pp.

[39] Schmidt, Ralf *Packet structure and paramodular forms.* Trans. Amer. Math. Soc. 370 (2018), no. 5, 3085-3112.

[40] Skoruppa, Nils-Peter *Computations of Siegel modular forms of genus two.* Math. Comp. 58 (1992), no. 197, 381-398.

[41] Walling, Lynne H. *Some relations on Fourier coefficients of degree 2 Siegel forms of arbitrary level.* J. Number Theory 180 (2017), 349-359.