Journal de Théorie des Nombres
de Bordeaux **11** (1999), 45–72

Class invariants by Shimura's reciprocity law

par Alice GEE

Résumé. On applique la loi de réciprocité de Shimura pour décider quand les valeurs des fonctions modulaires de haut niveau peuvent être utilisées pour engendrer le corps de classes de Hilbert d'un corps quadratique imaginaire. Lorsque c'est le cas, nous montrons aussi comment trouver le polynôme correspondant. Cela donne une preuve de certaines formules conjecturales de Morain et Zagier relatives à ces polynômes.

Abstract. We apply the Shimura reciprocity law to determine when values of modular functions of higher level can be used to generate the Hilbert class field of an imaginary quadratic field. In addition, we show how to find the corresponding polynomial in these cases. This yields a proof for conjectural formulas of Morain and Zagier concerning such polynomials.

1. Introduction

Let K be an imaginary quadratic number field of discriminant d with ring of integers $\mathcal{O} = \mathbb{Z}[\theta]$. The first main theorem of complex multiplication says that the modular invariant $j(\mathcal{O}) = j(\theta)$ generates the Hilbert class field over K.

Weber noticed that in many cases, the Hilbert class field can be generated by modular functions of higher level such as γ_2, γ_3, and the so-called Weber functions $\mathfrak{f}$, $\mathfrak{f}_1$, and $\mathfrak{f}_2$. We will also study Weber's resolvents ω_0 and ω_3 of level 5. These functions are defined in §4. When h is a modular function of level N, Weber calls the value $h(\theta)$ of a modular function h at θ a *class invariant* whenever $h(\theta)$ and $j(\theta)$ generate the same field over K.

Class invariants can be useful because $j(\mathcal{O})$ provides an ungainy description of the Hilbert class field from a computational point of view. Its minimum polynomial $H_d \in \mathbb{Z}[X]$ has zeroes at $j(\mathfrak{a})$, with $\mathfrak{a}$ ranging over the ideal classes of $\mathcal{O}$. As a function on the complex upper half plane, the value of $j(\theta)$ grows exponentially with the imaginary part of θ so that the coefficients of H_d grow exponentially with d. Even worse, the coefficients of H_d are unwieldy even when d is of modest size. For example, the class polynomial for $d = -71$ is

$$\begin{aligned} H_{-71} = X^7 &+ 313645809715\ X^6 - 3091990138604570\ X^5 \\ &+ 98394038810047812049302\ X^4 \\ &- 823534263439730779968091389\ X^3 \\ &+ 5138800366453976780323726329446\ X^2 \\ &- 425319473946139603274605151187659\ X \\ &+ 737707086760731113357714241006081263. \end{aligned}$$

However, taking $\theta = \frac{-1+\sqrt{-71}}{2}$, the function values $\zeta_3\gamma_2(\theta)$, $\zeta_{48}\mathfrak{f}(\theta)$ and $\omega_3(\theta)$ are all class invariants. These have minimum polynomials

$$\begin{aligned} f_{\mathbb{Q}}^{\zeta_3\gamma_2(\theta)} &= X^7 + 6745\ X^6 - 327467\ X^5 + 51857115\ X^4 + 2319299751\ X^3 \\ &\quad +41264582513\ X^2 - 307873876442\ X + 903568991567 \end{aligned}$$

$$\begin{aligned} f_{\mathbb{Q}}^{\omega_3(\theta)} &= X^7 + 221\ X^6 + 3999\ X^5 + 79447\ X^4 + 628970\ X^3 \\ &\quad +3746281\ X^2 + 12033163\ X + 19868711 \end{aligned}$$

$$f_{\mathbb{Q}}^{\zeta_{48}\mathfrak{f}_2(\theta)} = X^7 + X^6 - X^5 - X^4 - X^3 + X^2 + 2\ X - 1.$$

In this paper, we apply the Shimura reciprocity law, which describes the action of the idèle class group of K on the values of modular functions h taken at $\theta \in K$, to the problem of finding and computing class invariants.

The reciprocity law provides a method of systematically determining the instances when a given function yields a class invariant. By applying our method to Weber's functions γ_3, γ_2, $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$ we recover theorems of the type found in [7]. This treatment allows us dispense with the need for ad hoc arguments which appear even in the modern treatments [1] and [4], both of which pre–date Shimura's 1970 theorem.

Shimura's reciprocity law also describes the action of the class group $\mathrm{Cl}(\mathcal{O})$ on a class invariant $h(\theta)$. This provides an algorithm for computing the minimum polynomial of a class invariant numerically. We apply the algorithm to prove some conjectural formulas of Morain [3] and Zagier [8] regarding the conjugates of class invariants arising from γ_3 and $\mathfrak{f}_2$.

This paper is part of my thesis, which is being written at the University of Amsterdam. I have calculated the polynomials for the class invariants arising from the functions considered in this paper for the imaginary quadratic field discriminants d when $-1000 < d < 0$. The tables are not appended here.

2. The modular function field $\mathcal{F}$

Let $\mathbb{H}$ denote the complex upper half plane with completion $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. A matrix $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}^*$ as the fractional linear transformation $z \mapsto \frac{az+b}{cz+d}$.

When N is a positive integer, let $\Gamma_N \subset \mathrm{SL}_2(\mathbb{Z})$ denote the kernel of the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing coefficients modulo N. The quotient space $X(N) = \Gamma_N \backslash \mathbb{H}^*$ is a Galois cover of $\mathbb{P}^1(\mathbb{C})$ with group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. At the cusp corresponding to the point at infinity in $\mathbb{H}^*$, we have the local parameter $q^{1/N} = e^{2\pi i z/N}$. If h is a meromorphic function on $X(N)$, its the Laurent series expansion in the parameter $q^{1/N}$ is called the Fourier expansion of h.

We embed the algebraic closure $\bar{\mathbb{Q}}$ of the rational numbers in $\mathbb{C}$ and fix ζ_N to be the root of unity $e^{2\pi i/N}$. The algebraic curve $X(N)$ can be defined over $\mathbb{Q}(\zeta_N)$, and we let F_N be its function field over $\mathbb{Q}(\zeta_N)$. It is the field of meromorphic functions on $X(N)$ having Fourier coefficients in $\mathbb{Q}(\zeta_N)$. One has $F_1 = \mathbb{Q}(j)$, and defines the *automorphic function field* $\mathcal{F}$ as the union $\mathcal{F} = \cup_{N \geq 1} F_N$. We will describe the infinite Galois extension $F_1 \subset \mathcal{F}$ presently.

First consider the finite Galois extension $F_1 \subset F_N$. Let $\alpha_N \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ represent the Γ_N-equivalence class of a fractional linear transformation α on $\mathbb{H}^*$. For $h \in F_N$ the action $h^{\alpha_N} = h \circ \alpha$ is well-defined and induces an isomorphism

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} \simeq \mathrm{Gal}(F_N/F_1(\zeta_N)) = \mathrm{Gal}(\mathbb{C}\cdot F_N/\mathbb{C}\cdot F_1).$$

For $d \in (\mathbb{Z}/N\mathbb{Z})^*$, let σ_d denote the automorphism of $\mathbb{Q}(\zeta_N)$ given by $\zeta_N \mapsto \zeta_N^d$. The action of σ_d gives rise to a natural isomorphism

$$\mathrm{Gal}(F_1(\zeta_N)/F_1) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^*$$

which we can lift to F_N in the following way. If $h \in F_N$ has Fourier expansion $\sum_k c_k \cdot q^{\frac{k}{N}} \in \mathbb{Q}(\zeta_N)((q^{\frac{1}{N}}))$ then $\sum_k \sigma_d(c_k) \cdot q^{\frac{k}{N}}$ is again a Fourier expansion of some function in F_N which we denote by h^{σ_d}. Then $h \mapsto h^{\sigma_d}$ defines a group action of $(\mathbb{Z}/N\mathbb{Z})^*$ on F_N. The invariant field $F_{N,\mathbb{Q}}$ is the subfield of functions in F_N having Fourier coefficients in $\mathbb{Q}$, so we have $F_{N,\mathbb{Q}} \cap F_1(\zeta_N) = F_1$ in the following diagram

$$\begin{tikzcd}
 & F_N \arrow[dl, dash] \arrow[d, dash] \\
F_1(\zeta_N) \arrow[d, dash] & F_{N,\mathbb{Q}} \arrow[dl, dash] \\
F_1 &
\end{tikzcd}$$

of fields. Define the subgroup

$$G_N = \{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \mid d \in (\mathbb{Z}/N\mathbb{Z})^* \} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

The map $(\mathbb{Z}/N\mathbb{Z})^* \xrightarrow{\sim} G_N$ is a section of the determinant map on $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and the isomorphism $G_N \simeq \mathrm{Gal}\big(F_N/F_{N,\mathbb{Q}}\big)$ defines the action of G_N on F_N. We obtain the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccccc}
\{\pm 1\} & \rightarrow & \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) & \rightarrow & \mathrm{Gal}(F_N/F_1(\zeta_N)) & \rightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \\
\{\pm 1\} & \rightarrow & \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) & \rightarrow & \mathrm{Gal}(F_N/F_1) & \rightarrow & 1 \\
\downarrow & & \downarrow\mathrm{det} & & \downarrow & & \\
1 & \rightarrow & (\mathbb{Z}/N\mathbb{Z})^* & \rightarrow & \mathrm{Gal}(F_1(\zeta_N)/F_1) & \rightarrow & 1.
\end{array}$$

Passing to the projective limit yields the exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}}) \longrightarrow \mathrm{Gal}(\mathcal{F}/F_1) \longrightarrow 1. \tag{1}$$

3. Shimura reciprocity over the Hilbert class field

Let $\mathcal{O} = \mathbb{Z}[\theta]$ be the ring of integers of K, an imaginary quadratic number field. We assume K is embedded in the complex plane with $\theta \in \mathbb{H}$.

When $p \in \mathbb{Z}$ is a prime number we will use the notation $K_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} K$ and $\mathcal{O}_p = \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}$. For a prime ideal $\mathfrak{p} \subset \mathcal{O}$ lying over p, let $K_{\mathfrak{p}}$ denote the completion of K at $\mathfrak{p}$. Then K_p is canonically isomorphic to $\prod_{\mathfrak{p}|p} K_{\mathfrak{p}}$. We use the rational primes $p \in \mathbb{Z}$ to index the group of finite idèles

$$J_K^{\mathrm{f}} = {\prod_p}' K_p^*$$

of K. The restricted product is taken with respect to the subgroups $\mathcal{O}_p^* \subset K_p^*$.

Let $[\sim, K]$ denote the Artin map on J_K^{f}. We view K^* to be embedded along the diagonal of J_K^{f}. In the case that K is an imaginary quadratic number field, the exact sequence of class field theory takes on the following simple form:

$$1 \longrightarrow K^* \longrightarrow J_K^{\mathrm{f}} \xrightarrow{[\sim,K]} \mathrm{Gal}(K^{\mathrm{ab}}/K) \longrightarrow 1. \tag{2}$$

If $F \subset \mathcal{F}$ is a subfield of the automorphic function field, let $K(F(\theta))$ denote the field extension of K obtained by adjoining all of the function values $h(\theta)$ for which $h \in F$ is pole-free at θ.

Theorem 1 (First main theorem of complex multiplication). *Let $\mathcal{O} = \mathbb{Z}[\theta]$ be the ring of integers of an imaginary quadratic number field K. Then $j(\theta)$ generates the Hilbert class field over K. The maximal abelian extension K^{ab} is equal to $K(\mathcal{F}(\theta))$, and the sequence*

$$1 \longrightarrow \mathcal{O}^* \longrightarrow \prod_p \mathcal{O}_p^* \xrightarrow{[\sim,K]} \mathrm{Gal}(K^{\mathrm{ab}}/K(j(\theta))) \longrightarrow 1 \tag{3}$$

is exact. The ray class field of conductor N over K is $K(F_N(\theta))$. The subgroup of $\prod_p \mathcal{O}_p^*$ which acts trivially on $K(F_N(\theta))$ with respect to the Artin map is generated by $\mathcal{O}^*$ and $\prod_p \big((1+N\cdot\mathcal{O}_p)\cap\mathcal{O}_p^*\big)$.

Reference. Class field theory and [2; 10.1, Corollary to Theorem 2]. □

We now consider the map that relates the exact sequences (3) and (1). For every prime number $p \in \mathbb{Z}$, let

$$(g_\theta)_p : K_p^* \longrightarrow \mathrm{GL}_2(\mathbb{Q}_p)$$

be the injection that sends $x_p \in K_p^*$ to the matrix in $\mathrm{GL}_2(\mathbb{Q}_p)$ that represents multiplication by x_p with respect to the $\mathbb{Q}_p$-basis $[\theta, 1]$ for K_p. In other words, $(g_\theta)_p(x_p) \in \mathrm{GL}_2(\mathbb{Q}_p)$ is the matrix that satisfies the relation

$$(g_\theta)_p(x_p)\cdot\begin{pmatrix}\theta\\1\end{pmatrix} = x_p\begin{pmatrix}\theta\\1\end{pmatrix}.$$

If θ has minimum polynomial $f_{\mathbb{Q}}^\theta = X^2 + BX + C$, then for $s_p, t_p \in \mathbb{Q}_p$ we have

$$(g_\theta)_p : s_p\theta + t_p \mapsto \begin{pmatrix} t_p - B\cdot s_p & -C\cdot s_p \\ s_p & t_p\end{pmatrix}. \tag{4}$$

On $J_K^{\mathrm{f}} = \prod_p' K_p^*$ we obtain an injective product map

$$g_\theta = \prod_p (g_\theta)_p : J_K^{\mathrm{f}} \to \prod_p{}' \mathrm{GL}_2(\mathbb{Q}_p). \tag{5}$$

The restricted product is taken with respect to the subgroups $\mathrm{GL}_2(\mathbb{Z}_p) \subset \mathrm{GL}_2(\mathbb{Q}_p)$. We write $\prod_p \mathrm{GL}_2(\mathbb{Z}_p) = \mathrm{GL}_2(\hat{\mathbb{Z}})$ and consider the pre-image

$$g_\theta^{-1}\big(\mathrm{GL}_2(\hat{\mathbb{Z}})\big) = \{x \in J_K^{\mathrm{f}} \mid g_\theta(x) \in \mathrm{GL}_2(\hat{\mathbb{Z}})\}.$$

From (4) we note

$$g_\theta^{-1}\big(\mathrm{GL}_2(\hat{\mathbb{Z}})\big) = \prod_p \mathcal{O}_p^*,$$

because θ is an algebraic integer. Until section 10, we only need the restriction

$$g_\theta : \prod_p \mathcal{O}_p^* \to \mathrm{GL}_2(\hat{\mathbb{Z}})$$

of the map g_θ. In combination with (1) and (3), it yields the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & \prod_p \mathcal{O}_p^* & \xrightarrow{[\sim,K]} & \mathrm{Gal}(K^{\mathrm{ab}}/K(j(\theta))) & \longrightarrow & 1 \\
 & & & & \big\downarrow{\scriptstyle g_\theta} & & & & \\
1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathrm{GL}_2(\hat{\mathbb{Z}}) & \longrightarrow & \mathrm{Gal}(\mathcal{F}/F_1) & \longrightarrow & 1.
\end{array}$$

Theorem 2 (Shimura reciprocity law). *Let $\mathcal{O} = \mathbb{Z}[\theta]$ be the ring of integers of an imaginary quadratic number field K. For $h \in \mathcal{F}$ and $x \in \prod_p \mathcal{O}_p^*$ we have*

$$h(\theta)^{[x^{-1},K]} = h^{(g_\theta(x))}(\theta).$$

Suppose $G \subset \mathrm{GL}_2(\hat{\mathbb{Z}})$ is an open subgroup with fixed field $F \subset \mathcal{F}$. With respect to the Artin map, the subgroup of $\prod_p \mathcal{O}_p^*$ that acts trivially on $K(F(\theta))$ is generated by $\mathcal{O}^*$ and $g_\theta^{-1}(G) = \{x \in \prod_p \mathcal{O}_p^* \mid g_\theta(x) \in G\}$.

Reference. [5; Theorem 6.31, Proposition 6.33]. □

Corollary 3. *Let $\mathcal{O} = \mathbb{Z}[\theta]$ be the ring of integers of an imaginary quadratic number field K of discriminant $d < -4$. Suppose $h \in \mathcal{F}$ does not have a pole at θ and suppose that $\mathbb{Q}(j) \subset \mathbb{Q}(h)$. The function value $h(\theta)$ is a class invariant if and only if every element of the image $g_\theta[\prod_p \mathcal{O}_p^*] \subset \mathrm{GL}_2(\hat{\mathbb{Z}})$ acts trivially on h.*

Proof. The open subgroup $\mathrm{Stab}_{\mathbb{Q}(h)} = \{\alpha \in \mathrm{GL}_2(\hat{\mathbb{Z}}) \mid h^\alpha = h\}$ has fixed field $\mathbb{Q}(h) \subset \mathcal{F}$. The pre-image $g_\theta^{-1}(\mathrm{Stab}_{\mathbb{Q}(h)})$ contains $\mathcal{O}^* = \{\pm 1\}$, so $g_\theta^{-1}(\mathrm{Stab}_{\mathbb{Q}(h)}) \subset \prod_p \mathcal{O}_p^*$ is equal to the inverse image of $\mathrm{Gal}\big(K^{\mathrm{ab}}/K(h(\theta))\big)$ with respect to the Artin map. Thus $h(\theta)$ is a class invariant if and only if the equality $g_\theta^{-1}(\mathrm{Stab}_h) = \prod_p \mathcal{O}_p^*$ holds. This last equality is equivalent to the condition $g_\theta[\prod_p \mathcal{O}_p^*] \subset \mathrm{Stab}_h$ by the injectivity of g_θ. □

The infinite groups $\prod_p \mathcal{O}_p^*$ and $\mathrm{GL}_2(\hat{\mathbb{Z}})$ occuring in Corollary 3 are not directly suited for performing explicit computations. In practice, for $h \in F_N$ and θ an algebraic integer we can reduce modulo N and work with their finite quotient groups.

If N is a positive integer let $U_N \subset \mathrm{GL}_2(\hat{\mathbb{Z}})$ be the kernel of the natural map $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing coefficients modulo N.

We have $U_N = \mathrm{Stab}_{F_N}$ where Stab_{F_N} is the inverse image of $\mathrm{Gal}(\mathcal{F}/F_N)$ in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Also, we observe

$$g_\theta^{-1}(U_N) = \prod_p \big((1 + N\cdot \mathcal{O}_p) \cap \mathcal{O}_p^*\big).$$

Thus with respect to the Artin map, the subgroup of $\prod_p \mathcal{O}_p^*$ that acts trivially on $K(F_N(\theta))$ is generated by $\mathcal{O}^*$ and $g_\theta^{-1}(U_N)$. We write $\prod_p \mathcal{O}_p^* = g_\theta^{-1}(U_1)$. The sequence

$$\mathcal{O}^* \longrightarrow g_\theta^{-1}(U_1)/g_\theta^{-1}(U_N) \longrightarrow \mathrm{Gal}\big(K(F_N(\theta)/K(j(\theta))\big) \longrightarrow 1$$

is exact and g_θ induces a well-defined injection between the quotient groups

$$g_\theta^{-1}(U_1)/g_\theta^{-1}(U_N) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

We use the isomorphism $g_\theta^{-1}(U_1)/g_\theta^{-1}(U_N) \simeq (\mathcal{O}/N\mathcal{O})^*$ to define the map

$$g_{\theta,N} : (\mathcal{O}/N\mathcal{O})^* \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

which is the reduction of g_θ modulo N. One obtains the diagram

$$\begin{array}{ccccccc}
\mathcal{O}^* & \longrightarrow & (\mathcal{O}/N\mathcal{O})^* & \longrightarrow & \mathrm{Gal}\big(K(F_N(\theta))/K(j(\theta))\big) & \longrightarrow & 1 \\
 & & \Big\downarrow{\scriptstyle g_{\theta,N}} & & & & \\
\{\pm 1\} & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \mathrm{Gal}(F_N/F_1) & \longrightarrow & 1.
\end{array}$$

Define $W_{N,\theta}$ to be the image

$$W_{N,\theta} = g_{\theta,N}[(\mathcal{O}/N\mathcal{O})^*] \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

If θ has minimum polynomial $f_{\mathbb{Q}}^\theta = X^2 + BX + C \in \mathbb{Z}[X]$ we can list the elements of $W_{N,\theta}$ explicitly as a finite set

$$W_{N,\theta} = \Big\{ \begin{pmatrix} t-Bs & -Cs \\ s & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \;\Big|\; t, s \in \mathbb{Z}/N\mathbb{Z} \Big\}. \tag{6}$$

Corollary 4. *Let $\mathcal{O} = \mathbb{Z}[\theta]$ be the ring of integers of an imaginary number field K of discriminant $d < -4$. Let $h \in F_N$ and suppose $\mathbb{Q}(j) \subset \mathbb{Q}(h)$. Then*

$$h(\theta) \text{ is a class invariant} \Leftrightarrow W_{N,\theta} \text{ acts trivially on } h.$$

Proof. The image of $\mathrm{Stab}_{\mathbb{Q}(h)}$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing coeffients modulo N is given by

$$\mathrm{Stab}_{h,N} = \{\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \mid h^\alpha = h\}.$$

By Corollary 3, the inverse image of $\mathrm{Gal}\big(K(F_N(\theta))/K(h(\theta))\big)$ with respect to the Artin map on $(\mathcal{O}/N\mathcal{O})^*$ is $g_{\theta,N}^{-1}(\mathrm{Stab}_{h,N})$. As $g_{\theta,N}$ is injective, the equality $g_{\theta,N}^{-1}(\mathrm{Stab}_{h,N}) = (\mathcal{O}/N\mathcal{O})^*$ holds if and only if $W_{N,\theta}$ is contained in $\mathrm{Stab}_{h,N}$. ∎

4. Weber's modular functions

Weber constructs several functions which provide good candidates for producing class invariants for a large number of discriminants. These are modular functions h for which $\mathbb{Q}(h)$ is an extension of $\mathbb{Q}(j)$ having small degree.

We call f an *automorphic form of weight* k if it is meromorphic on $\mathbb{H}^*$ and satisfies the relation

$$f \circ \alpha(z) = (cz+d)^k f(z) \quad \text{for all } \alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}).$$

The normalized Eisenstein series

$$g_2(z) = 60 \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(m+nz)^4}$$

$$g_3(z) = 140 \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(m+nz)^6}$$

are automorphic functions of weights 4 and 6, respectively. The Dedekind-η function

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1-q^n)\ , \quad \text{with } q = e^{2\pi i z} \tag{7}$$

is holomorphic and non-zero for $z \in \mathbb{H}$. For the generating matrices $S, T \in \mathrm{SL}_2(\mathbb{Z})$ given by

$$S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \quad \text{and} \quad T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$$

the transformation rules

$$\eta \circ S\ (z) = \sqrt{-iz}\,\eta(z) \quad \text{and} \quad \eta \circ T\ (z) = \zeta_{24}\eta(z) \tag{8}$$

hold. Here, the branch of the square root on the half plane $\{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\}$ is chosen to be positive on the real axis. The Δ-function defined by

$$\Delta(z) = \eta^{24}(z)$$

is automorphic of weight 12 and without poles or zeros on $\mathbb{H}$.

Let $M_2^+(\mathbb{Z})$ denote the set of 2×2 matrices with integer coefficients and positive determinant. These matrices act as fractional linear transformations on the complex upper half plane. The next lemma provides a method for making Γ_N-invariant functions.

Lemma 5. *Let f and g be automorphic functions of the same weight, and let $\alpha \in M_2^+(\mathbb{Z})$ be an integral matrix such that $det(\alpha) = N$. Then the function*

$$h(z) = \frac{f \circ \alpha(z)}{g(z)}$$

is Γ_N-invariant.

Reference. [2; 11, §2 Theorem 3]. □

Applying lemma 5 in the case $\alpha = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, we can recover the well-known fact that the j-invariant

$$j(z) = 12^3 \frac{g_2^3(z)}{(2\pi)^{12}\Delta(z)} = 12^3 + 6^6 \frac{g_3^2(z)}{(2\pi)^{12}\Delta(z)}$$

is invariant under $\Gamma_1 = \mathrm{SL}_2(\mathbb{Z})$. As $\Delta = \eta^{24}$ is a 24th power, the above expressions for j show that one can extract holomorphic roots $\sqrt[3]{j}$ and $\sqrt{j - 12^3}$. The resulting Weber functions

$$\gamma_2(z) = \frac{12 g_2(z)}{(2\pi)^4\eta^8(z)}$$
$$\gamma_3(z) = \frac{6^3 g_3(z)}{(2\pi)^6\eta^{12}(z)}$$

are no longer $\mathrm{SL}_2(\mathbb{Z})$-invariant. Under S and T they transform as

$$\begin{array}{ll} \gamma_2 \circ S = \gamma_2 & \gamma_2 \circ T = \zeta_3^{-1}\gamma_2 \\ \gamma_3 \circ S = -\gamma_3 & \gamma_3 \circ T = -\gamma_3 \end{array} \tag{9}$$

from which one deduces that γ_2 is Γ_3-invariant and that γ_3 is Γ_2-invariant.

The function values of γ_2 and γ_3 are only moderately smaller than the j-function. Better results can be obtained by applying lemma 5 to quotients of Δ. One can then extract holomorphic roots of higher power.

The functions

$$\frac{\Delta \circ \left(\begin{smallmatrix}1&1\\0&2\end{smallmatrix}\right)}{\Delta}, \quad -\frac{\Delta \circ \left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)}{\Delta}, \quad -2^{12}\frac{\Delta \circ \left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)}{\Delta}$$

are of level 2 and have rational Fourier coefficients. They are the distinct roots of $(X - 16)^3 - jX$. As we have $\Delta = \eta^{24}$, we can extract holomorphic 24th roots to obtain the Weber-$\mathfrak{f}$ functions

$$\begin{aligned} \mathfrak{f}(z) &= \zeta_{48}^{-1} \cdot \frac{\eta(\frac{z+1}{2})}{\eta(z)} \\ \mathfrak{f}_1(z) &= \frac{\eta(\frac{z}{2})}{\eta(z)} \\ \mathfrak{f}_2(z) &= \sqrt{2} \cdot \frac{\eta(2z)}{\eta(z)}. \end{aligned} \tag{10}$$

These Weber functions have considerably smaller values than j, but they also have higher level and generate extensions of higher degree over $\mathbb{Q}(j)$. It follows from the product expansion (7) for $\eta(z)$ that each of the functions

$\mathfrak{f}$, $\mathfrak{f}_1$, and $\sqrt{2}\cdot\mathfrak{f}_2$ have rational Fourier expansions. From the transformation rules (8) for $\eta(z)$ we obtain

$$(11) \qquad \begin{array}{rcl} (\mathfrak{f},\ \mathfrak{f}_1,\ \mathfrak{f}_2)\circ S & = & (\mathfrak{f},\ \mathfrak{f}_2,\ \mathfrak{f}_1) \\ (\mathfrak{f},\ \mathfrak{f}_1,\ \mathfrak{f}_2)\circ T & = & (\zeta_{48}^{-1}\mathfrak{f}_1,\ \zeta_{48}^{-1}\mathfrak{f},\ \zeta_{48}^{2}\mathfrak{f}_2). \end{array}$$

One deduces that $\mathfrak{f}$, $\mathfrak{f}_1$ and $\mathfrak{f}_2$ are contained in F_{48}. Taking suitable powers of Weber's functions, one obtains various modular functions of level dividing 48. For example, the functions

$$(12) \qquad \begin{array}{l} \gamma_3 = \dfrac{(\mathfrak{f}^{24}+8)\cdot(\mathfrak{f}_1^8-\mathfrak{f}_2^8)}{\mathfrak{f}^8} \\ \gamma_2 = \dfrac{\mathfrak{f}^{24}-16}{\mathfrak{f}^8} = \dfrac{\mathfrak{f}_1^{24}+16}{\mathfrak{f}_1^8} = \dfrac{\mathfrak{f}_2^{24}+16}{\mathfrak{f}_2^8} \end{array}$$

are contained in $\mathbb{Q}(\mathfrak{f}^8,\mathfrak{f}_1^8,\mathfrak{f}_2^8)$. Thus we note that both γ_3 and γ_2 have Fourier coefficients in $\mathbb{Q}$, and in particular we have $\gamma_3 \in F_2$ and $\gamma_2 \in F_3$.

Let K be an imaginary quadratic number field and suppose $h \in \mathcal{F}$. The class invariants $h(\theta) \in \mathbb{R}$ which arise from real function values are particularly convenient because their minimum polynomials satisfy

$$f_K^{h(\theta)} = f_{\mathbb{Q}}^{h(\theta)} \in \mathbb{Q}[X].$$

Namely, when we embed the algebraic closure $\bar{\mathbb{Q}}$ in $\mathbb{C}$, the generator of $\mathrm{Gal}(K/\mathbb{Q})$ is obtained by restricting complex conjugation to K. Thus if $\sigma \in \mathrm{Aut}(\mathbb{C})$ denotes complex conjugation and $h(\theta) = \sigma(h(\theta))$ is real, then the polynomial

$$f_K^{h(\theta)} = f_K^{\sigma(h(\theta))} = (f_K^{h(\theta)})^{\sigma}$$

is invariant under $\mathrm{Gal}(K/\mathbb{Q})$.

The product expansion (7) and the expressions (10) and (12) imply that the functions $\mathfrak{f}$, $\mathfrak{f}_1$, $\mathfrak{f}_2$, γ_3 and γ_2 all take on real values along the imaginary axis in $\mathbb{H}$. As γ_2 has Fourier expansion in $\mathbb{Q}((q^{\frac{1}{3}}))$, we also note when $z \in \mathbb{H}$ has real part $\Re(z) \in \frac{3}{2}\cdot\mathbb{Z}$, then the function value $\gamma_2(z)$ is real.

It is difficult to produce modular functions of small degree over $\mathbb{Q}(j)$ when the level N is not divisible by 2 or 3. The reason for this is group theoretical. For $p \geq 5$ the group

$$\mathrm{Gal}(\mathbb{C}\cdot F_p/\mathbb{C}(j)) \simeq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\{\pm 1\}.$$

is simple. Weber shows that any subgroup of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\{\pm 1\}$ has index at least p, and that a subgroup of index exactly p can only occur in the cases $p = 5, 7, 11$.

For the smallest example $p = 5$, Weber constructs modular functions $\omega_i \in F_5$ with $i = 0, \ldots, 4$ such that $\mathbb{Q}(j) \subset \mathbb{Q}(\omega_i)$ is an extension of degree

5. These are known as Weber's resolvents of level and degree 5. For $i = 0, \ldots, 4$, let c_i be an integer such that

$$c_i \equiv 0 \pmod{12} \quad \text{and} \quad c_i \equiv i \pmod 5.$$

Define the functions

$$v_i(z) = \left(\frac{\eta(\frac{z+c_i}{5})}{\eta(z)}\right)^2 \quad \text{and} \quad v_\infty(z) = 5\cdot\left(\frac{\eta(5z)}{\eta(z)}\right)^2.$$

Then the functions

$$\omega_i(z) = \frac{1}{\sqrt{5}}\cdot(v_\infty - v_i)(v_{i+1} - v_{i-1})(v_{i-2} - v_{i+2})(z), \quad i = 0, \ldots, 4$$

are in F_5. They are the five distinct roots of $(X+3)^3(X^2+11X+64) - j \in F_1[X]$.

The action of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in G_5$ induced by $\sigma_d : \zeta_5 \mapsto \zeta_5^d$ on the Fourier coefficients of ω_i is given by

$$(\omega_0, \omega_1, \omega_2, \omega_3, \omega_4)^{\sigma_d} = (\omega_0, \omega_d, \omega_{2d}, \omega_{3d}, \omega_{4d}).$$

Observe that the function ω_0 is G_5-invariant and thus has Fourier expansion in $\mathbb{Q}((q^{\frac{1}{5}}))$. In particular, if $z \in \mathbb{H}$ satisfies $\Re(z) \in \frac{5}{2}\cdot\mathbb{Z}$, then the function value $\omega_0(z)$ is real. From (8), one derives the action of the generators S and T for $\mathrm{SL}_2(\mathbb{Z})$

$$\begin{aligned} (\omega_0, \omega_1, \omega_2, \omega_3, \omega_4) \circ S &= (\omega_0, \omega_2, \omega_1, \omega_4, \omega_3) \\ (\omega_0, \omega_1, \omega_2, \omega_3, \omega_4) \circ T &= (\omega_1, \omega_2, \omega_3, \omega_4, \omega_0). \end{aligned} \tag{13}$$

Reference. [7; §34, §54 and §83].

5. Computation of $W_{N,\theta}$ and its action on F_N

In this section we collect a few remarks of a practical nature with regard to computing $W_{N,\theta}$ and the explicit action of $W_{N,\theta}$ on F_N.

It is well known that every matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ can be written as an element of $\langle S, T\rangle$. For $u \in M_2^+(\mathbb{Z})$ let $u_N \in M_2(\mathbb{Z}/N\mathbb{Z})$ denote the matrix obtained by reducing coefficients modulo N. If in particular, $N = p^r$ is a prime power, we have the following formula for writing $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)_N \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ as an element of $< S_N, T_N >$.

Lemma 6. *Let $N = p^r$ be a prime power and let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)_N \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, so that either a or c is invertible modulo N. If $(c, N) = 1$ let $y \equiv (1+a)\cdot c^{-1} \bmod N$. Otherwise, if $(a, N) = 1$ let $z \equiv (c+1)\cdot a^{-1} \bmod N$. Then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)_N$ has the decomposition*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}_N = \begin{cases} (T^y S T^c S T^{dy-b})_N & \textit{if } (c, N) = 1 \\ (S T^{-z} S T^{-a} S T^{bz-d})_N & \textit{if } (a, N) = 1. \end{cases}$$

Proof. If $(c,N)=1$ note that

$$T_N^{-y}\begin{pmatrix} a & b \\ c & d \end{pmatrix}_N = \begin{pmatrix} 1 & b-yd \\ c & d \end{pmatrix}_N .$$

Left multiplication by appropriate powers of S_N and T_N quickly produces a triangular matrix, which is some power of T_N. In the other case of $(a,N)=1$, the same argument applies to $S\cdot\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} -c & -d \\ a & b \end{smallmatrix}\right)$. □

The factorization formula in Lemma 6 makes it convenient to calculate the action of $W_{N,\theta}$ on some function $h \in F_N$ in the case that N is a prime power. If N and M are relative prime integers then for $h \in F_{NM}$ we will use the Chinese remainder theorem to we lift the action of $W_{N,\theta}$ to F_{NM} so that $W_{N,\theta} \times W_{M,\theta} \simeq W_{NM,\theta}$ as groups of automorphisms of F_{NM}.

In sections 8, 9 and 10 we need to determine whether the entire matrix group $W_{N,\theta}$ acts trivially on some given function $h \in F_N$. One could ignore the group structure completely and calculate the action of every element of $W_{N,\theta}$ given by the list (6). However, it is often less cumbersome to first find generators for $W_{N,\theta}$.

For $\mathcal{O} = \mathbb{Z}[\theta]$, the groups $W_{N,\theta} \simeq (\mathcal{O}/N\mathcal{O})^*$ are isomorphic. Suppose θ and τ are imaginary quadratic algebraic integers. Then the description (6) of $W_{N,\theta}$ shows

$$f_{\mathbb{Q}}^{\theta} \equiv f_{\mathbb{Q}}^{\tau} \bmod N \Longrightarrow W_{N,\theta} = W_{N,\tau} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Even if the coefficients of $f_{\mathbb{Q}}^{\theta}$ and $f_{\mathbb{Q}}^{\tau}$ are not congruent modulo N we can often use the following lemma to determine generators for $W_{N,\tau}$ from given generators for $W_{N,\theta}$.

Lemma 7. *Suppose $u \in M_2^+(\mathbb{Z})$ such that $u_N \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. If both θ and $u(\theta)$ are imaginary quadratic algebraic integers then $W_{N,u(\theta)}$ is the conjugate group*

$$W_{N,u(\theta)} = u_N \cdot W_{N,\theta} \cdot u_N^{-1}.$$

Proof. Regarding g_θ as a function on $\prod_p \mathcal{O}_p^*$, observe that

$$u\cdot g_\theta(x)\cdot u^{-1} = g_{u(\theta)}(x)$$

for any $x \in \prod_p \mathcal{O}_p^*$. □

Example 8. *Take $N=16$ and suppose $m \in \mathbb{Z}$ and*

$$f_{\mathbb{Q}}^{\theta} = X^2 + X + m \quad \textit{and} \quad f_{\mathbb{Q}}^{\tau} = X^2 + X + (m+8).$$

The congruence

$$f_{\mathbb{Q}}^{\theta+8} = X^2 + 17X + (m+72) \equiv f_{\mathbb{Q}}^{\tau} \bmod 16$$

gives

$$W_{16,\tau} = W_{16,\theta+8} = T^8 W_{16,\theta} T^{-8}.$$

Example 9. *Again, take $N = 16$ and now suppose $m \in \mathbb{Z}$ is odd with*

$$f_{\mathbb{Q}}^{\theta} = X^2 + m \quad \text{and} \quad f_{\mathbb{Q}}^{\tau} = X^2 + (m+8).$$

The congruence

$$f_{\mathbb{Q}}^{3\theta} = X^2 + 9m \equiv f_{\mathbb{Q}}^{\tau} \bmod 16$$

gives

$$W_{16,\tau} = W_{16,3\theta} = \left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot W_{16,\theta} \cdot \left(\begin{smallmatrix} 11 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

6. Class invariants for γ_3 and γ_2

We illustrate our technique by recovering some classical results due to Weber.

Theorem 10. *Let K be an imaginary quadratic number field of discriminant d, with $d < -4$. Let $\theta = \frac{-B+\sqrt{d}}{2}$ generate the ring of integers $\mathcal{O}$ of K. We have*

$$2 \nmid d \Longrightarrow \gamma_3(\theta) \text{ is a class invariant}$$

$$3 \nmid d \Longrightarrow \zeta_3^B \gamma_2(\theta) \text{ is a class invariant with } f_K^{\zeta_3^B \gamma_2(\theta)} \in \mathbb{Q}[X].$$

If 2 divides d, then $\gamma_3(\theta)$ generates the ray class field of conductor 2 over K. If 3 divides d, then $\gamma_2(\theta)$ generates the ray class field of conductor 3 over K.

Proof. Consider the assertion for γ_3. If 2 splits in $\mathcal{O}$ then $(\mathcal{O}/2\mathcal{O})^*$ is trivial. If 2 is inert in $\mathcal{O}$ then $(\mathcal{O}/2\mathcal{O})^* \simeq \mathbb{Z}/3\mathbb{Z}$. It follows that the length of the $W_{2,\theta}$-orbit of γ_3 divides 3. Because $\gamma_3^2 = j - 12^3$ we know $[K(\gamma_3(\theta)) : K(j(\theta))] \leq 2$ and conclude that $\gamma_3(\theta)$ is a class invariant.

If d is divisible by 2 then $W_{2,\theta} \simeq \mathbb{Z}/2\mathbb{Z}$. If $f_{\mathbb{Q}}^{\theta} = X^2 + BX + C$ is the minimum polynomial for θ then $W_{2,\theta}$ is generated by

$$\begin{cases} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)_2 = S_2 & \text{if } C \equiv 1 \bmod 2, \\ \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)_2 = (TST)_2 & \text{if } C \equiv 0 \bmod 2. \end{cases}$$

Both of these matrices act on $\mathbb{Q}(\gamma_3)$ as $\gamma_3 \mapsto -\gamma_3$. As

$$\mathrm{Gal}\big(K(F_2(\theta))/K(j(\theta))\big) \simeq W_{2,\theta}/\{\pm 1\}$$

is a group of order 2, we have $K(\gamma_3(\theta)) = K(F_2(\theta))$. In other words, $\gamma_3(\theta)$ generates the ray class field of conductor 2.

Consider the assertion for γ_2. In the case $B \equiv 0 \bmod 3$ we find the generators for $W_{3,\theta}$ given in the table below.

$d \bmod 3$	Structure	$W_{3,\theta}$
1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$\left\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)_3, \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)_3 \right\rangle$
2	$\mathbb{Z}/8\mathbb{Z}$	$\left\langle \left(\begin{smallmatrix} 1 & 2 \\ 1 & 1 \end{smallmatrix}\right)_3 \right\rangle$
0	$\mathbb{Z}/6\mathbb{Z}$	$\left\langle \left(\begin{smallmatrix} 2 & 0 \\ 1 & 2 \end{smallmatrix}\right)_3 \right\rangle$

Using the factorization formula from Lemma 6 and the transformation rules (9), we calculate the action of each of these generators on ζ_3 and γ_2. In the following table, the second column indicates the discriminants d for which a matrix in the first column occurs as a generator for $W_{3,\theta}$.

Generator	$d \bmod 3$	ζ_3	γ_2
$\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$	1	ζ_3	γ_2
$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$	1	ζ_3^2	γ_2
$\left(\begin{smallmatrix} 1 & 2 \\ 1 & 1 \end{smallmatrix}\right)$	2	ζ_3^2	γ_2
$\left(\begin{smallmatrix} 2 & 0 \\ 1 & 2 \end{smallmatrix}\right)$	0	ζ_3	$\zeta_3^2\gamma_2$

Observe that if d is not divisible by 3 then $\gamma_2(\theta)$ is a class invariant. We have $f_K^{\gamma_2(\theta)} \in \mathbb{Q}[X]$ because the function value $\gamma_2(\theta)$ is real.

In the case that 3 divides d, we see that $W_{3,\theta}$ does not fix $\zeta_3^m\gamma_2(\theta)$ for any integer $m \in \mathbb{Z}$. The group $W_{3,\theta}/\{\pm 1\}$ has order 3 so we conclude that $\gamma_2(\theta)$ generates the ray class field $K(F_3(\theta))$ of conductor 3 over K. Thus the statement of the theorem holds in the case $B \equiv 0 \bmod 3$.

In the general case, if $\theta = \frac{-B+\sqrt{d}}{2}$, then $T^{-B}(\theta) = \frac{-3B+\sqrt{d}}{2}$ generates $\mathcal{O}$. The transformation rules (8) for γ_2 imply

$$\zeta_3^B\gamma_2 = \gamma_2 \circ T^{-B}.$$

In particular, $\zeta_3^B\gamma_2(\theta) = \gamma_2(\theta - B)$ is a class invariant if and only if 3 does not divide d, and the proposition holds for all integers $B \in \mathbb{Z}$. $\square$

7. Class invariants for the resolvents ω_0 and ω_3 of level 5

If 5 is inert or if 5 is ramified in $\mathcal{O} = \mathbb{Z}[\theta]$ then $W_{5,\theta}$ fails to stabilize any of the resolvents ω_i, $i = 0, \dots, r$ of level and degree 5. In the split case we have the following:

Proposition 11. *Let K be an imaginary quadratic number field of discriminant $d \equiv \pm 1 \bmod 5$ with $d < -4$. Let $\mathcal{O} = \mathbb{Z}[\theta]$ be the ring of integers of K with*

$$\theta = \begin{cases} \frac{\sqrt{d}}{4} & \text{if } d \equiv 0 \bmod 4 \\ \frac{-1+\sqrt{d}}{4} & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

The following statements hold:

$$d \equiv 1 \bmod 4 \Longrightarrow \omega_3(\theta) \text{ is a class invariant with } f_K^{\omega_3(\theta)} \in \mathbb{Q}[X]$$
$$d \equiv 0 \bmod 4 \Longrightarrow \omega_1(\theta) \text{ is a class invariant with } f_K^{\omega_0(\theta)} \in \mathbb{Q}[X].$$

Proof. If $d \equiv \pm 1 \bmod 5$, then $W_{5,\theta}$ has structure $(\mathcal{O}/5\mathcal{O})^* \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Let

$$f_{\mathbb{Q}}^{\theta} = X^2 + BX + C \in \mathbb{Z}[X]$$

be the minimum polynomial for θ. We find generators for $W_{5,\theta}$ as the coefficients (B, C) range over the possible values. We then determine the action of these matrices on $\mathbb{Q}(\omega_0, \omega_1, \omega_2, \omega_3, \omega_4)$. The second column (B, C) in the table below indicates the θ for which a matrix in the first column appears as a generator for $W_{5,\theta}$. The image of ω_i, for $i = 0, \ldots, 4$ with respect to the action of these matrices is given in the remaining columns.

Generator	(B,C) mod 5	ω_0	ω_1	ω_2	ω_3	ω_4
$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	$(0,1),(0,4),(1,0),(1,3)$	ω_0	ω_1	ω_2	ω_3	ω_4
$\begin{pmatrix} 1 & 4 \\ 1 & 1 \end{pmatrix}$	$(0,1)$	ω_0	ω_3	ω_4	ω_2	ω_1
$\begin{pmatrix} 2 & 0 \\ 4 & 1 \end{pmatrix}$	$(1,0)$	ω_2	ω_0	ω_4	ω_3	ω_1
$\begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$	$(0,4)$	ω_0	ω_4	ω_1	ω_2	ω_3
$\begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}$	$(1,3)$	ω_1	ω_2	ω_4	ω_3	ω_0

Observe that ω_0 is invariant under $W_{5,\theta}$ in the case that $d \equiv 0 \bmod 4$, and that ω_3 is $W_{5,\theta}$-invariant in the case that $d \equiv 1 \bmod 4$.

The function ω_0 takes on real values at $z \in \mathbb{H}$ with $\Re(z) \in \frac{5}{2} \cdot \mathbb{Z}$ and the transformation rules (13) give

$$\omega_3 = \omega_0 \circ T^3.$$

In particular, if $d \equiv 0 \bmod 4$ we have $\omega_0(\theta) \in \mathbb{R}$. In the case $d \equiv 1 \bmod 4$ we have $\omega_3(\theta) = \omega_0(\theta + 3) \in \mathbb{R}$. □

8. Class invariants for the Weber-$\mathfrak{f}$ functions

We now determine class invariants for powers of the Weber-$\mathfrak{f}$ functions by computing the explicit action of $W_{48,\theta} \simeq W_{3,\theta} \times W_{16,\theta}$ on $\mathbb{Q}(\zeta_{48}, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2)$ as the coefficients of the minimum polynomial $f_{\mathbb{Q}}^{\theta} \in \mathbb{Z}[X]$ range through $\mathbb{Z}/48\mathbb{Z}$. In doing so we recover several results from [1], [4], and [7].

We lift the action of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ to F_{48} by the Chinese remainder theorem. First we need to embed the generators $S_3, T_3 \in \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ in

$\mathrm{SL}_2(\mathbb{Z}/48\mathbb{Z})$ as

$$S_3 \mapsto \begin{pmatrix} 33 & 32 \\ 16 & 33 \end{pmatrix}_{48} = (T^2S^3T^{-16}ST^{14})_{48}$$

$$T_3 \mapsto \begin{pmatrix} 1 & 16 \\ 0 & 1 \end{pmatrix}_{48} = (T^{16})_{48}.$$

Define the action of S_3 and T_3 on functions $h \in F_{48}$ as

$$\begin{aligned} h \bullet S_3 &= h \circ T^2S^3T^{-16}ST^{14} \\ h \bullet T_3 &= h \circ T^{16}. \end{aligned}$$

For $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)_3 \in G_3$, let σ_d be the action on F_{48} obtained by lifting the automorphism of $\mathbb{Q}(\zeta_{48})$ determined by $\zeta_3 \mapsto \zeta_3^d$ and $\zeta_{16} \mapsto \zeta_{16}$. We define

$$h \bullet \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)_3 = h_d^{\sigma}.$$

The explicit action of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ on $\mathbb{Q}(\zeta_{48}, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2)$ is given by

$$\begin{aligned} (\zeta_3, \zeta_{16}, \mathfrak{f},\ \mathfrak{f}_1,\ \mathfrak{f}_2) \bullet S_3 &= (\zeta_3, \zeta_{16}, \mathfrak{f},\ \mathfrak{f}_1,\ \mathfrak{f}_2) \\ (\zeta_3, \zeta_{16}, \mathfrak{f},\ \mathfrak{f}_1,\ \mathfrak{f}_2) \bullet T_3 &= (\zeta_3, \zeta_{16}, \zeta_3^2\mathfrak{f},\ \zeta_3^2\mathfrak{f}_1,\ \zeta_3^2\mathfrak{f}_2) \\ (\zeta_3, \zeta_{16}, \mathfrak{f},\ \mathfrak{f}_1,\ \mathfrak{f}_2) \bullet \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)_3 &= (\zeta_3^d, \zeta_{16}, \mathfrak{f},\ \mathfrak{f}_1,\ \mathfrak{f}_2). \end{aligned} \tag{14}$$

Proposition 12. *Let* $\theta = \frac{-B+\sqrt{d}}{2}$ *generate the imaginary quadratic order of fundamental discriminant* $d < -4$. *The group* $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ *acts trivially on* $\mathbb{Q}(\mathfrak{f}^3, \mathfrak{f}_1^3, \mathfrak{f}_2^3)$. *Furthermore we have*

$$3 \nmid d \Longrightarrow W_{3,\theta} \textit{ acts trivially on } \mathbb{Q}(\zeta_3^B\mathfrak{f}, \zeta_3^B\mathfrak{f}_1, \zeta_3^B\mathfrak{f}_2).$$

Proof. By the transformation rules (14) every matrix in $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ acts trivially on $\mathbb{Q}(\mathfrak{f}^3, \mathfrak{f}_1^3, \mathfrak{f}_2^3)$.

Suppose that 3 divides B. We use the generators of $W_{3,\theta}$ found in section 8 to compute the action of $W_{3,\theta}$ on $\mathbb{Q}(\zeta_{48}, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2)$. The second column in the table below indicates the discriminants d for which a matrix in the first column appears as a generator for $W_{16,\theta}$. The images of ζ_3, $\mathfrak{f}$, $\mathfrak{f}_1$, and $\mathfrak{f}_2$ respectively are displayed in the remaining columns.

Generator	d mod 3	ζ_3	$\mathfrak{f}$	$\mathfrak{f}_1$	$\mathfrak{f}_2$
$\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$	1	ζ_3	$\mathfrak{f}$	$\mathfrak{f}_1$	$\mathfrak{f}_2$
$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$	1	ζ_3^2	$\mathfrak{f}$	$\mathfrak{f}_1$	$\mathfrak{f}_2$
$\left(\begin{smallmatrix} 1 & 2 \\ 1 & 1 \end{smallmatrix}\right)$	2	ζ_3^2	$\mathfrak{f}$	$\mathfrak{f}_1$	$\mathfrak{f}_2$
$\left(\begin{smallmatrix} 2 & 0 \\ 1 & 2 \end{smallmatrix}\right)$	0	ζ_3	$\zeta_3^2\mathfrak{f}$	$\zeta_3^2\mathfrak{f}_1$	$\zeta_3^2\mathfrak{f}_2$

From the table it is clear that if 3 does not divide d then $W_{3,\theta}$ acts trivially on $\mathbb{Q}(\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2)$. Therefore the statement of the proposition holds in the case that B is divisible by 3.

In the general case, if $\theta = \frac{-B+\sqrt{d}}{2}$ then the translate $T^{-16B}(\theta) = \frac{-33B+\sqrt{d}}{2}$ is again a generator of $\mathcal{O}$. The transformation rules (14) give

$$(\zeta_3^B \mathfrak{f}, \zeta_3^B \mathfrak{f}_1, \zeta_3^B \mathfrak{f}_2) = (\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2) \bullet T_3^{-B}$$

and we note

$$W_{3,\theta-16B} = T_3^{-B} W_{3,\theta} T_3^B.$$

Since

$$W_{3,\theta-16B} \text{ acts trivially on } h \Leftrightarrow W_{3,\theta} \text{ acts trivially on } h \bullet T_3^{-B}$$

holds for any function $h \in F_{48}$, the proposition holds for all integers $B \in \mathbb{Z}$. $\square$

We lift the action of $\mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z})$ to F_{48}. First we embed $S_{16}, T_{16} \in \mathrm{SL}_2(\mathbb{Z}/16\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{Z}/48\mathbb{Z})$ according to the Chinese remainder theorem

$$\begin{array}{lcl} S_{16} \mapsto \begin{pmatrix} 16 & 15 \\ 33 & 16 \end{pmatrix}_{48} & = & (S^3 T^{-2} S T^{16} S T^{14})_{48} \\ T_{16} \mapsto \begin{pmatrix} 1 & 33 \\ 0 & 1 \end{pmatrix}_{48} & = & (T^{33})_{48} \end{array}$$

and define the action of S_{16} and T_{16} on $h \in F_{48}$ as

$$\begin{array}{lcl} h \bullet S_{16} & = & h \circ S^3 T^{-2} S T^{16} S T^{14} \\ h \bullet T_{16} & = & h \circ T^{33}. \end{array}$$

For $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)_{16} \in G_{16}$ define

$$h \bullet \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)_{16} = h^{\sigma_d}$$

where σ_d is the action on F_{48} obtained by lifting the automorphism of $\mathbb{Q}(\zeta_{48})$ determined by as $\zeta_3 \mapsto \zeta_3$ and $\zeta_{16} \mapsto \zeta_{16}^d$. The $\mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z})$-action on $\mathbb{Q}(\zeta_{48}, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2)$ is given by

$$\begin{array}{lcl} (\zeta_3, \zeta_{16}, \mathfrak{f},\ \mathfrak{f}_1,\ \mathfrak{f}_2) \bullet S_{16} & = & (\zeta_3, \zeta_{16}, \mathfrak{f},\ \mathfrak{f}_2,\ \mathfrak{f}_1) \\ (\zeta_3, \zeta_{16}, \mathfrak{f},\ \mathfrak{f}_1,\ \mathfrak{f}_2) \bullet T_{16} & = & (\zeta_3, \zeta_{16}, \zeta_{16}^5 \mathfrak{f}_1,\ \zeta_{16}^5 \mathfrak{f},\ \zeta_{16}^6 \mathfrak{f}_2) \\ (\zeta_3, \zeta_{16}, \mathfrak{f},\ \mathfrak{f}_1,\ \mathfrak{f}_2) \bullet \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)_{16} & = & (\zeta_3, \zeta_{16}^d, \mathfrak{f},\ \mathfrak{f}_1,\ \frac{\sigma_d(\sqrt{2})}{\sqrt{2}} \mathfrak{f}_2). \end{array}$$

In the remainder of this section we calculate the action of $W_{16,\theta}$ on $\mathbb{Q}(\zeta_{48}, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2)$ as the discriminant of $\mathcal{O} = \mathbb{Z}[\theta]$ ranges through the fundamental imaginary quadratic discriminants d. The cases where 2 is split, inert, or ramified in $\mathbb{Z}[\theta]$ will be dealt with separately. In each instance our goal is to find $W_{16,\theta}$-invariant functions in $\mathbb{Q}(\zeta_{48}, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2)$ which fulfil the additional condition $\mathbb{Q}(j) \subset \mathbb{Q}(h)$.

We begin with the split case.

Proposition 13. *Let $\mathcal{O}$ be an imaginary quadratic order of fundamental discriminant $d < -4$ and let $\theta = \frac{-1+\sqrt{d}}{2}$. We have*

$$d \equiv 1 \bmod 8 \Longrightarrow W_{16,\theta} \textit{ acts trivially on } \zeta_{16}^{-5}\mathfrak{f}_2.$$

Proof. If $d \equiv 1 \bmod 8$ then $W_{16,\theta}$ has structure $(\mathcal{O}/16\mathcal{O})^* \simeq (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^2$. It turns out that the matrix group $W_{16,\theta}$ is determined by the coefficients of $f_{\mathbb{Q}}^{\theta}$ modulo 8.

We calculate the action of generators for $W_{16,\theta}$ as $\frac{1-d}{4}$ ranges over $\mathbb{Z}/8\mathbb{Z}$. The second column indicates the discriminants d for which a matrix in the first column appears as a generator for $W_{16,\theta}$.

Generator	$\frac{1-d}{4}$ mod 8	ζ_{16}	$\mathfrak{f}$	$\mathfrak{f}_1$	$\mathfrak{f}_2$
$\left(\begin{smallmatrix} 15 & 0 \\ 0 & 15 \end{smallmatrix}\right)$	0,2,4,6	ζ_{16}	$\mathfrak{f}$	$\mathfrak{f}_1$	$\mathfrak{f}_2$
$\left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right)$	0,2,4,6	ζ_{16}^9	$\mathfrak{f}$	$\zeta_{16}^8\mathfrak{f}_1$	$\zeta_{16}^8\mathfrak{f}_2$
$\left(\begin{smallmatrix} 13 & 0 \\ 4 & 1 \end{smallmatrix}\right)$	0,4	ζ_{16}^{13}	$\zeta_{16}^{12}\mathfrak{f}$	$\mathfrak{f}_1$	$\zeta_{16}^{12}\mathfrak{f}_2$
$\left(\begin{smallmatrix} 13 & 8 \\ 4 & 1 \end{smallmatrix}\right)$	2,6	ζ_{16}^{13}	$\zeta_{16}^{4}\mathfrak{f}$	$\zeta_{16}^8\mathfrak{f}_1$	$\zeta_{16}^{12}\mathfrak{f}_2$
$\left(\begin{smallmatrix} 15 & 0 \\ 2 & 1 \end{smallmatrix}\right)$	0	ζ_{16}^{15}	$\zeta_{16}^{6}\mathfrak{f}$	$\zeta_{16}^4\mathfrak{f}_1$	$\zeta_{16}^{6}\mathfrak{f}_2$
$\left(\begin{smallmatrix} 15 & 8 \\ 2 & 1 \end{smallmatrix}\right)$	4	ζ_{16}^{15}	$\zeta_{16}^{14}\mathfrak{f}$	$\zeta_{16}^{12}\mathfrak{f}_1$	$\zeta_{16}^{6}\mathfrak{f}_2$
$\left(\begin{smallmatrix} 13 & 4 \\ 6 & 3 \end{smallmatrix}\right)$	2	ζ_{16}^{15}	$\zeta_{16}^{10}\mathfrak{f}$	$\mathfrak{f}_1$	$\zeta_{16}^{6}\mathfrak{f}_2$
$\left(\begin{smallmatrix} 13 & 12 \\ 6 & 3 \end{smallmatrix}\right)$	6	ζ_{16}^{15}	$\zeta_{16}^{2}\mathfrak{f}$	$\zeta_{16}^8\mathfrak{f}_1$	$\zeta_{16}^{6}\mathfrak{f}_2$

Observe that each the automorphisms in the above table fixes $\zeta_{16}^{-5}\mathfrak{f}_2$. ☐

We continue with the inert case.

In the case that $\mathcal{O}$ is an imaginary quadratic order of discriminant $d \equiv 5 \bmod 8$, we have group structure $(\mathcal{O}/16\mathcal{O})^* \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. The matrix group $W_{16,\theta}$ does not fix any of the functions $\mathfrak{f}^{24}$, $\mathfrak{f}_1^{24}$, or $\mathfrak{f}_2^{24}$.

One can of course determine functions $h \in \mathbb{Q}(\zeta_{48}, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2)$ which are invariant under $W_{16,\theta}$ but which might not satsify the extra condition $\mathbb{Q}(j) \subset \mathbb{Q}(h)$. One could then use Lemma 18 of Section 11 to determine whether the function value $h(\theta)$ nonetheless generates the Hilbert class field over K. We will not do this in this paper.

For $d \equiv 5 \bmod 8$, we choose the generator $\theta = \frac{-1+\sqrt{d}}{2} \subset \mathcal{O}$. The following table provides the action of the generators for $W_{16,\theta}$ on $\mathbb{Q}(\zeta_{48}, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2)$.

Generator	$\frac{1-d}{4}$ mod 16	ζ_{16}	$\mathfrak{f}$	$\mathfrak{f}_1$	$\mathfrak{f}_2$
$\left(\begin{smallmatrix} 13 & 12 \\ 4 & 1 \end{smallmatrix}\right)$	1,5,9,13	ζ_{16}^{13}	$\zeta_{16}^{8}\mathfrak{f}$	$\zeta_{16}^{12}\mathfrak{f}_1$	$\zeta_{16}^{4}\mathfrak{f}_2$
$\left(\begin{smallmatrix} 13 & 4 \\ 4 & 1 \end{smallmatrix}\right)$	3,7,11,15	ζ_{16}^{13}	$\mathfrak{f}$	$\zeta_{16}^{4}\mathfrak{f}_1$	$\zeta_{16}^{4}\mathfrak{f}_2$
$\left(\begin{smallmatrix} 15 & 14 \\ 2 & 1 \end{smallmatrix}\right)$	1,9	ζ_{16}^{3}	$\zeta_{16}^{8}\mathfrak{f}$	$\zeta_{16}^{14}\mathfrak{f}_1$	$\zeta_{16}^{2}\mathfrak{f}_2$
$\left(\begin{smallmatrix} 15 & 10 \\ 2 & 1 \end{smallmatrix}\right)$	3,11	ζ_{16}^{11}	$\zeta_{16}^{12}\mathfrak{f}$	$\zeta_{16}^{2}\mathfrak{f}_1$	$\zeta_{16}^{10}\mathfrak{f}_2$
$\left(\begin{smallmatrix} 15 & 6 \\ 2 & 1 \end{smallmatrix}\right)$	5,13	ζ_{16}^{3}	$\mathfrak{f}$	$\zeta_{16}^{6}\mathfrak{f}_1$	$\zeta_{16}^{2}\mathfrak{f}_2$
$\left(\begin{smallmatrix} 15 & 2 \\ 2 & 1 \end{smallmatrix}\right)$	7,15	ζ_{16}^{11}	$\zeta_{16}^{4}\mathfrak{f}$	$\zeta_{16}^{10}\mathfrak{f}_1$	$\zeta_{16}^{10}\mathfrak{f}_2$
$\left(\begin{smallmatrix} 1 & 1 \\ 15 & 0 \end{smallmatrix}\right)$	1	ζ_{16}	$\zeta_{16}^{11}\mathfrak{f}_2$	$\zeta_{16}^{11}\mathfrak{f}$	$\zeta_{16}^{10}\mathfrak{f}_1$
$\left(\begin{smallmatrix} 7 & 7 \\ 3 & 10 \end{smallmatrix}\right)$	3	ζ_{16}	$\zeta_{16}^{13}\mathfrak{f}_2$	$\zeta_{16}^{7}\mathfrak{f}$	$\zeta_{16}^{12}\mathfrak{f}_1$
$\left(\begin{smallmatrix} 5 & 13 \\ 7 & 12 \end{smallmatrix}\right)$	5	ζ_{16}	$\zeta_{16}^{7}\mathfrak{f}_2$	$\zeta_{16}^{3}\mathfrak{f}$	$\zeta_{16}^{6}\mathfrak{f}_1$
$\left(\begin{smallmatrix} 11 & 3 \\ 11 & 6 \end{smallmatrix}\right)$	7	ζ_{16}	$\zeta_{16}^{9}\mathfrak{f}_2$	$\zeta_{16}^{15}\mathfrak{f}$	$\zeta_{16}^{8}\mathfrak{f}_1$
$\left(\begin{smallmatrix} 9 & 9 \\ 15 & 8 \end{smallmatrix}\right)$	9	ζ_{16}	$\zeta_{16}^{3}\mathfrak{f}_2$	$\zeta_{16}^{11}\mathfrak{f}$	$\zeta_{16}^{2}\mathfrak{f}_1$
$\left(\begin{smallmatrix} 15 & 15 \\ 3 & 2 \end{smallmatrix}\right)$	11	ζ_{16}	$\zeta_{16}^{5}\mathfrak{f}_2$	$\zeta_{16}^{7}\mathfrak{f}$	$\zeta_{16}^{4}\mathfrak{f}_1$
$\left(\begin{smallmatrix} 13 & 5 \\ 7 & 4 \end{smallmatrix}\right)$	13	ζ_{16}	$\zeta_{16}^{15}\mathfrak{f}_2$	$\zeta_{16}^{3}\mathfrak{f}$	$\zeta_{16}^{14}\mathfrak{f}_1$
$\left(\begin{smallmatrix} 11 & 11 \\ 11 & 6 \end{smallmatrix}\right)$	15	ζ_{16}	$\zeta_{16}\mathfrak{f}_2$	$\zeta_{16}^{15}\mathfrak{f}$	$\mathfrak{f}_1$

We now consider the case when 2 ramifies in $\mathcal{O} = \mathbb{Z}[\theta]$.

Proposition 14. *Let $\mathcal{O}$ be an imaginary quadratic order of fundamental discriminant $d = -4m < -4$ with generator $\theta = \sqrt{-m}$. The following functions are $W_{16,\theta}$-invariant.*

m mod 8	$W_{16,\theta}$-*Invariant*
1	$\sqrt{2} \cdot \mathfrak{f}^2$
2	$\sqrt{2} \cdot \mathfrak{f}_1^2$
5	$\mathfrak{f}^4$
6	$\mathfrak{f}_1^2$

Proof. When d is even, $(\mathcal{O}/16\mathcal{O})^*$ is a group of order 2^7. The group structures for $W_{16,\theta}$ which arise are

$$W_{16,\theta} \simeq \begin{cases} \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } m \equiv 0 \bmod 2 \\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{if } m \equiv 1 \bmod 8 \\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } m \equiv 5 \bmod 8 \end{cases}$$

We first determine generators for $W_{16,\theta}$ in the case that m is even and then compute the action on of these generators on $\mathbb{Q}(\zeta_{48}, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2)$. The second column of the table indicates the m for which a matrix occurs as a generator for $W_{16,\theta}$.

Generator	m mod 16	ζ_{16}	$\mathfrak{f}$	$\mathfrak{f}_1$	$\mathfrak{f}_2$
$\begin{pmatrix} 15 & 0 \\ 0 & 15 \end{pmatrix}$	2,6,10,14	ζ_{16}	$\mathfrak{f}$	$\mathfrak{f}_1$	$\mathfrak{f}_2$
$\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$	2,6,10,14	ζ_{16}^9	$\mathfrak{f}$	$\zeta_{16}^8\mathfrak{f}_1$	$\zeta_{16}^8\mathfrak{f}_2$
$\begin{pmatrix} 1 & 10 \\ 3 & 1 \end{pmatrix}$	2	ζ_{16}^3	$\zeta_{16}^7\mathfrak{f}_2$	$\zeta_{16}^{12}\mathfrak{f}_1$	$\zeta_{16}^5\mathfrak{f}$
$\begin{pmatrix} 1 & 14 \\ 3 & 1 \end{pmatrix}$	6	ζ_{16}^7	$\zeta_{16}^{11}\mathfrak{f}_2$	$\zeta_{16}^8\mathfrak{f}_1$	$\zeta_{16}^{13}\mathfrak{f}$
$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$	10	ζ_{16}^{11}	$\zeta_{16}^{15}\mathfrak{f}_2$	$\zeta_{16}^4\mathfrak{f}_1$	$\zeta_{16}^5\mathfrak{f}$
$\begin{pmatrix} 1 & 6 \\ 3 & 1 \end{pmatrix}$	14	ζ_{16}^{15}	$\zeta_{16}^3\mathfrak{f}_2$	$\mathfrak{f}_1$	$\zeta_{16}^{13}\mathfrak{f}$

We see that all of the matrices listed in the table above act trivially on $\mathfrak{f}_1^4$. It's easy to verify that we can do a little better and provide a $W_{16,\theta}$-invariant function by using some suitable element of $\mathbb{Q}(\zeta_{16})$ to normalize $\mathfrak{f}_1^2$. Since $\mathfrak{f}_1$ takes on real values along the imaginary axis of the complex upper half plane, we choose the normalizations

$$\begin{cases} \mathfrak{f}_1^2 & \text{if } m \equiv 6 \bmod 8 \\ \sqrt{2}\cdot \mathfrak{f}_1^2 & \text{if } m \equiv 2 \bmod 8\ . \end{cases}$$

These are both $W_{16,\theta}$-invariant and real-valued at θ.

We now perform a similar calculation when m is odd.

Generator	m mod 16	ζ_{16}	$\mathfrak{f}$	$\mathfrak{f}_1$	$\mathfrak{f}_2$
$\begin{pmatrix} 15 & 0 \\ 0 & 15 \end{pmatrix}$	5,13	ζ_{16}	$\mathfrak{f}$	$\mathfrak{f}_1$	$\mathfrak{f}_2$
$\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$	1,9	ζ_{16}^9	$\mathfrak{f}$	$\zeta_{16}^8\mathfrak{f}_1$	$\zeta_{16}^8\mathfrak{f}_2$
$\begin{pmatrix} 2 & 15 \\ 1 & 2 \end{pmatrix}$	1	ζ_{16}^5	$\zeta_{16}^{12}\mathfrak{f}$	$\zeta_{16}^6\mathfrak{f}_2$	$\zeta_{16}^6\mathfrak{f}_1$
$\begin{pmatrix} 0 & 15 \\ 1 & 0 \end{pmatrix}$	1	ζ_{16}	$\mathfrak{f}$	$\mathfrak{f}_2$	$\mathfrak{f}_1$
$\begin{pmatrix} 2 & 7 \\ 1 & 2 \end{pmatrix}$	9	ζ_{16}^{13}	$\zeta_{16}^{12}\mathfrak{f}$	$\zeta_{16}^6\mathfrak{f}_2$	$\zeta_{16}^6\mathfrak{f}_1$
$\begin{pmatrix} 0 & 7 \\ 1 & 0 \end{pmatrix}$	9	ζ_{16}^9	$\mathfrak{f}$	$\mathfrak{f}_2$	$\mathfrak{f}_1$
$\begin{pmatrix} 2 & 11 \\ 1 & 2 \end{pmatrix}$	5	ζ_{16}^9	$\zeta_{16}^4\mathfrak{f}$	$\zeta_{16}^6\mathfrak{f}_2$	$\zeta_{16}^6\mathfrak{f}_1$
$\begin{pmatrix} 0 & 11 \\ 1 & 0 \end{pmatrix}$	5	ζ_{16}^5	$\mathfrak{f}$	$\zeta_{16}^8\mathfrak{f}_2$	$\mathfrak{f}_1$
$\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$	13	ζ_{16}	$\zeta_{16}^4\mathfrak{f}$	$\zeta_{16}^6\mathfrak{f}_2$	$\zeta_{16}^6\mathfrak{f}_1$
$\begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$	13	ζ_{16}^{13}	$\mathfrak{f}$	$\zeta_{16}^8\mathfrak{f}_2$	$\mathfrak{f}_1$

Here we see that each of the automorphisms in the above table stabilizes $\mathfrak{f}^4$. In the case of $m \equiv 1 \bmod 8$ we can actually do a little better by normalizing $\mathfrak{f}^2$ using some suitable element of $\mathbb{Q}(\zeta_{16})$. The function $\sqrt{2}\cdot \mathfrak{f}^2$ is $W_{16,\theta}$-invariant and real-valued at θ. $\square$

Theorem 15. *Let K be an imaginary quadratic number field of discriminant $d < -4$ and let $\theta = \frac{-1+\sqrt{d}}{2}$. If $d \equiv 1 \bmod 8$ then we have*

$$\begin{array}{lcl} 3 \nmid d & \Rightarrow & \zeta_{48}\mathfrak{f}_2(\theta) \textit{ is a class invariant} \\ 3 \mid d & \Rightarrow & \zeta_{16}\mathfrak{f}_2^3(\theta) \textit{ is a class invariant} \end{array}$$

In either case, the given class invariant is also invariant under $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. Apply Propositions 12 and 13 to $\zeta_3\zeta_{16}^{-5}\mathfrak{f}_2 = \zeta_{48}\mathfrak{f}_2$. Note from definitions (7) and (10) that if $z \in \mathbb{H}$ with $\Re(z) = -\frac{1}{2}$, then we have $\zeta_{48}\mathfrak{f}_2(z) \in \mathbb{R}$. □

Theorem 16 (2 ramified)**.** *Let K be an imaginary quadratic number field of discriminant $d = -4m < -4$ and let $\theta = \sqrt{-m}$. The following is a table of class invariants.*

m mod 8	$d \not\equiv 0$ mod 3	$d \equiv 0$ mod 3
1	$\sqrt{2}\cdot\mathfrak{f}^2(\theta)$	$\sqrt{2}\cdot\mathfrak{f}^6(\theta)$
2	$\sqrt{2}\cdot\mathfrak{f}_1^2(\theta)$	$\sqrt{2}\cdot\mathfrak{f}_1^6(\theta)$
5	$\mathfrak{f}^4(\theta)$	$\mathfrak{f}^{12}(\theta)$
6	$\mathfrak{f}_1^2(\theta)$	$\mathfrak{f}_1^6(\theta)$

The modular function values given above are also invariant under $\mathrm{Gal}(K/\mathbb{Q})$*.*

Proof. Apply Proposition 12 and 14. □

9. Shimura's reciprocity law

In this section we discuss a modification of the exact sequence (1)

$$1 \longrightarrow \mathbb{Z}^* \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}}) \longrightarrow \mathrm{Gal}(\mathcal{F}/F_1) \longrightarrow 1,$$

so that one can describe all of $\mathrm{Aut}(\mathcal{F})$ instead of only $\mathrm{Gal}(\mathcal{F}/F_1)$. This allows the Shimura reciprocity law to be stated in its full generality, which we will need in Section 11.

Let $A_{\mathbb{Q}}^{\mathrm{f}} = \prod_p' \mathbb{Q}_p$ denote the ring of finite rational adèles. Here, the restricted product is taken with respect to $\mathbb{Z}_p \subset \mathbb{Q}_p$. We write $\mathrm{GL}_2(A_{\mathbb{Q}}^{\mathrm{f}}) = \prod_p' \mathrm{GL}_2(\mathbb{Q}_p)$, where the restricted product is taken with respect to $\mathrm{GL}_2(\mathbb{Z}_p) \subset \mathrm{GL}_2(\mathbb{Q}_p)$. We consider $\mathrm{GL}_2(\hat{\mathbb{Z}}) \subset \mathrm{GL}_2(A_{\mathbb{Q}}^{\mathrm{f}})$ to be a subgroup by means of the embedding

$$\mathrm{GL}_2(\hat{\mathbb{Z}}) \simeq \prod_p \mathrm{GL}_2(\mathbb{Z}_p) \hookrightarrow \prod_p{}' \mathrm{GL}_2(\mathbb{Q}_p) \simeq \mathrm{GL}_2(A_{\mathbb{Q}}^{\mathrm{f}}).$$

Let $\mathrm{GL}_2^+(\mathbb{Q})$ denote the group of rational 2×2 matrices with positive determinant. Embedding $\mathbb{Q}$ along the diagonal of $A_{\mathbb{Q}}^{\mathrm{f}}$ we view $\mathrm{GL}_2^+(\mathbb{Q}) \subset \mathrm{GL}_2(A_{\mathbb{Q}}^{\mathrm{f}})$ to be a subgroup. In particular, we identify $\mathbb{Q}^*$ with the scalar matrices $\mathbb{Q}^* \subset \mathrm{GL}_2^+(\mathbb{Q}) \subset \mathrm{GL}_2(A_{\mathbb{Q}}^{\mathrm{f}})$.

One can show that every $x \in \mathrm{GL}_2(A_{\mathbb{Q}}^{\mathrm{f}})$ can be written as

$$x = u\cdot\alpha \text{ with } u \in \mathrm{GL}_2(\hat{\mathbb{Z}}) \text{ and } \alpha \in \mathrm{GL}_2^+(\mathbb{Q}).$$

This decomposition is not unique since $\mathrm{SL}_2(\mathbb{Z}) = \mathrm{GL}_2(\hat{\mathbb{Z}}) \cap \mathrm{GL}_2^+(\mathbb{Q})$. Nonetheless, the decomposition $x = u\cdot\alpha$ determines a group action of $\mathrm{GL}_2(A_{\mathbb{Q}}^{\mathrm{f}})$

on $\mathcal{F}$ given by $h^x = h^u \circ \alpha$. Here, $u \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ acts via (1) and $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ acts as a transformation on the complex upper half plane.

Theorem 17 (Shimura exact sequence)**.** *The sequence*

$$1 \longrightarrow \mathbb{Q}^* \longrightarrow \mathrm{GL}_2(A_{\mathbb{Q}}^{\mathrm{f}}) \longrightarrow \mathrm{Aut}(\mathcal{F}) \longrightarrow 1 \tag{15}$$

is exact.

Reference. [5; Theorem 6.23]. □

Recall the from (5) the embedding

$$g_\theta : J_K^{\mathrm{f}} \longrightarrow {\prod_p}' \mathrm{GL}_2(\mathbb{Q}_p)$$

and consider the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & K^* & \longrightarrow & J_K^{\mathrm{f}} & \xrightarrow{[\sim,K]} & \mathrm{Gal}(K^{\mathrm{ab}}/K) & \longrightarrow & 1 \\
 & & & & \big\downarrow g_\theta & & & & \\
1 & \longrightarrow & \mathbb{Q}^* & \longrightarrow & \mathrm{GL}_2(A_{\mathbb{Q}}^{\mathrm{f}}) & \longrightarrow & \mathrm{Aut}(\mathcal{F}) & \longrightarrow & 1.
\end{array}$$

Theorem 18 (Shimura reciprocity law)**.** *Let $\mathbb{Z}[\theta]$ be the ring of integers of an imaginary quadratic number field K with θ in the complex upper half plane. For $h \in \mathcal{F}$ and $x \in J_K^{\mathrm{f}}$ we have*

$$h(\theta)^{[x^{-1},K]} = h^{(g_\theta(x))}(\theta).$$

If $G \subset \mathrm{GL}_2(A_{\mathbb{Q}}^{\mathrm{f}})$ is an open subgroup with fixed field $F \subset \mathcal{F}$, then the subgroup of J_K^{f} that acts trivially on $K(F(\theta))$ with respect to the Artin map is generated by K^* and $g_\theta^{-1}(G)$.

Reference. [5; Theorem 6.31, Proposition 6.33]. □

10. Action of the class group on class invariants

Let K be the imaginary quadratic number field of discriminant d with ring of integers $\mathcal{O} = \mathbb{Z}[\theta]$. For an ideal $\mathfrak{a} \subset \mathcal{O}$ the formula

$$\mathfrak{a} : j(\mathcal{O}) \mapsto j(\mathfrak{a}^{-1}).$$

gives the action of the Artin symbol for $\mathfrak{a}$ on the class group $\mathrm{Cl}(\mathcal{O})$.

Every primitive reduced quadratic form of discriminant d corresponds uniquely with an ideal class in $\mathrm{Cl}(\mathcal{O})$. If $[a,b,c]$ is a primitive form of discriminant d then for $\tau = \frac{-b+\sqrt{d}}{2a}$, the $\mathbb{Z}$-lattice $L = [a, a\tau]$ is an integral $\mathcal{O}$-ideal. The Galois action of the Artin symbol for $[a,-b,c]$ on $K(j(\theta))/K$ is given by

$$j(\theta)^{[a,-b,c]} = j(\tau).$$

Suppose $h \in \mathcal{F}$ is a modular function for which $h(\theta) \in K(j(\theta))$. In this section we give a formula

$$\begin{array}{rccc} u: & \mathrm{Cl}(\mathcal{O}) & \to & \mathrm{GL}_2(\hat{\mathbb{Z}}) \\ & [a,b,c] & \mapsto & u_\tau \end{array}$$

such that

$$h(\theta)^{[a,-b,c]} = h^{u_\tau}(\tau).$$

We begin by producing an idèle $z_\tau \in J_K^{\mathrm{f}}$ such that the Galois action of the Artin symbol $[z_\tau, K]$ satisfies

$$j(\theta)^{[a,b,c]} = j(\theta)^{[z_\tau,K]}.$$

If $p \in \mathbb{Z}$ is prime, let $L_p = L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ so that $L_p \subset \mathcal{O}_p$. We need to produce a finite idèle $(z_p)_p \in \prod_p' K_p$ such that

$$\prod_p z_p \mathcal{O}_p = \prod_p L_p$$

holds. It turns out that one can always choose z_p to be among $\{a, a\tau, a\tau - a\}$.

Lemma 19. *Let K be the imaginary quadratic number field of discriminant d with ring of integers $\mathcal{O} = \mathbb{Z}[\theta]$. If $[a,b,c]$ is a primitive quadratic form of discriminant d let $\tau = \frac{-b+\sqrt{d}}{2a}$ and $L = [a, a\tau]$. For every prime $p \in \mathbb{Z}$ define $z_p \in L$ as*

$$z_p := \begin{cases} a & \text{if } p \nmid a \\ a\tau & \text{if } p \mid a \wedge p \nmid c \\ a(\tau - 1) & \text{if } p \mid a \wedge p \mid c\ . \end{cases}$$

For $z_\tau = (z_p)_p \in J_K^{\mathrm{f}}$ the Galois action of the Artin symbol $[z_\tau, K]$ satisfies

$$j(\theta)^{[a,b,c]} = j(\theta)^{[z_\tau,K]}.$$

Proof. The inclusion $z_p\mathcal{O}_p \subset L_p$ follows from $z_p \in L$. Note that $L \subset \mathcal{O}$ has index $[\mathcal{O} : L] = a$. For every $p \in \mathbb{Z}$ we compute

$$\mathrm{N}_{K/\mathbb{Q}}(z_p) = \begin{cases} a^2 & \text{if } p \nmid a \\ ac & \text{if } p \mid a \wedge p \nmid c \\ a(a+b+c) & \text{if } p \mid a \wedge p \mid c, \end{cases}$$

and since $(a,b,c) = 1$, one obtains $\| \mathrm{N}_{K/\mathbb{Q}}(z_p) \|_p = \|a\|_p$. From

$$[\mathcal{O}_p : z_p\mathcal{O}_p] = \|a\|_p = [\mathcal{O}_p : L_p]$$

we conclude $z_p\mathcal{O}_p = L_p$. □

Given an imaginary quadratic discriminant d, fix

$$\theta = \begin{cases} \frac{-1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4 \\ \frac{\sqrt{d}}{2} & \text{if } d \equiv 0 \bmod 4\ , \end{cases}$$

and given $[a, b, c]$, let $z = z_\tau$ be as stated in Lemma 19. For a class invariant $h(\theta)$, the Shimura reciprocity law states

$$h(\theta)^{[a,-b,c]} = h(\theta)^{[z^{-1},K]} = h^{g_\theta(z)}(\theta).$$

Let $M \in \mathrm{GL}_2^+(\mathbb{Q})$ satisfy $M \cdot \binom{\theta}{1} = \binom{a\tau}{a}$. Explicitly, one computes

$$M = \begin{cases} \begin{pmatrix} 1 & \frac{1-b}{2} \\ 0 & a \end{pmatrix} & \text{if } d \equiv 1 \bmod 4 \\ \begin{pmatrix} 1 & \frac{-b}{2} \\ 0 & a \end{pmatrix} & \text{if } d \equiv 0 \bmod 4. \end{cases}$$

The action of $\mathrm{GL}_2(A_{\mathbb{Q}}^{\mathrm{f}})$ via (15) gives

$$h^{g_\theta(z)}(\theta) = h^{g_\theta(z) \cdot M^{-1}}(\tau).$$

Define $u_\tau = g_\theta(z) \cdot M^{-1} \in \prod_p' \mathrm{GL}_2(\mathbb{Q}_p)$. Let $u_p \in \mathrm{GL}_2(\mathbb{Q}_p)$ denote the component of u_τ at p. Then the determinant of

$$u_p = (g_\theta)_p(z_p) \cdot M^{-1} \in \mathrm{GL}_2(\mathbb{Q}_p)$$

is given by

$$\det(u_p) = \mathrm{N}_{K/\mathbb{Q}}(z_p) \cdot \frac{1}{a} \in \mathbb{Z}_p^*.$$

Writing out u_p for $d \equiv 0 \bmod 4$, one obtains

$$u_p = \begin{cases} \begin{pmatrix} a & \frac{b}{2} \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a \\ \begin{pmatrix} -\frac{b}{2} & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \wedge p \nmid c \\ \begin{pmatrix} -\frac{b}{2} - a & -\frac{b}{2} - c \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \wedge p \mid c\,. \end{cases} \tag{16}$$

On the other hand for $d \equiv 1 \bmod 4$, we get

$$u_p = \begin{cases} \begin{pmatrix} a & \frac{b-1}{2} \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a \\ \begin{pmatrix} \frac{-b-1}{2} & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \wedge p \nmid c \\ \begin{pmatrix} \frac{-b-1}{2} - a & \frac{1-b}{2} - c \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \wedge p \mid c\,. \end{cases} \tag{17}$$

We observe that in either case, $u_p \in \mathrm{GL}_2(\mathbb{Z}_p)$ and we conclude $u_\tau \in \mathrm{GL}_2(\hat{\mathbb{Z}})$. We have demonstrated the following statement:

Lemma 20. *Let $\mathbb{Z}[\theta]$ be the ring of integers of an imaginary quadratic number field K of discriminant d and let $[a,b,c]$ be a primitive quadratic form of discriminant d. Define*

$$\theta = \begin{cases} \frac{\sqrt{d}}{2} & \text{if } d \equiv 0 \bmod 4 \\ \frac{-1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

and $\tau = \frac{-b+\sqrt{d}}{2a}$. Let $u_\tau = (u_p)_p$ be defined according to the local formulas for $u_p \in \mathrm{GL}_2(\mathbb{Z}_p)$ given in (16) *if d is even or* (17) *if d is odd. It follows that*

$$h(\theta)^{[a,-b,c]} = h^{u_\tau}(\tau)$$

for any $h \in \mathcal{F}$ such that $h(\theta) \in K(j(\theta))$. □

11. Formulas of Morain and Zagier

We can use Theorem 20 to verify some conjectural formulas of Morain and Zagier regarding conjugates of class invariants arising from some classical functions. The following proposition is Morain's Conjecture 1 from [3].

Proposition 21. *Let $d \equiv 1 \bmod 4$ be an imaginary quadratic discriminant and let $\theta = \frac{-1+\sqrt{d}}{2}$. The action of the class group on $\gamma_3(\theta)$ is given by the formula*

$$\gamma_3^{[a,-b,c]}(\theta) = (-1)^{\frac{b+1}{2}+ac+a+c}\gamma_3(\tau)$$

where $[a,b,c]$ is a primtive quadratic form of discriminant d and $\tau = \frac{-b+\sqrt{d}}{2a}$.

Proof. By Theorem 20, the matrix $M \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ given by

$$M = \begin{cases} \begin{pmatrix} 1 & \frac{b-1}{2} \\ 0 & 1 \end{pmatrix} & \text{if } 2 \nmid a \\ \begin{pmatrix} \frac{-b-1}{2} & 1 \\ 1 & 0 \end{pmatrix} & \text{if } 2 \mid a \wedge 2 \nmid c \\ \begin{pmatrix} \frac{-b-1}{2} & \frac{1-b}{2} \\ 1 & 1 \end{pmatrix} & \text{if } 2 \mid a \wedge 2 \mid c\,. \end{cases}$$

satisfies

$$\gamma_3^{[a,-b,c]}(\theta) = \gamma_3^M(\tau).$$

We decompose M in terms of S and T modulo 2

$$M \equiv \begin{cases} T^{\frac{b-1}{2}} & \text{if } 2 \nmid a \\ T^{\frac{1-b}{2}}STST & \text{if } 2 \mid a \wedge 2 \nmid c \\ T^{\frac{1-b}{2}}STS & \text{if } 2 \mid a \wedge 2 \mid c\,. \end{cases}$$

Using (9), we calculate

$$\gamma_3^M(\theta) = \begin{cases} (-1)^{\frac{b-1}{2}}\gamma_3(\tau) & \text{if } 2 \nmid a \\ (-1)^{\frac{b-1}{2}}\gamma_3(\tau) & \text{if } 2 \mid a \wedge 2 \nmid c \\ (-1)^{\frac{b-1}{2}+1}\gamma_3(\tau) & \text{if } 2 \mid a \wedge 2 \mid c\,. \end{cases}$$

A routine check shows that in each case, the above formulas are equivalent to the formula given by the proposition. ☐

We prove Zagier and Yui's conjectural formula ($2_?$) regarding the conjugates of the class invariant $\zeta_{48}\mathfrak{f}_2(\theta)$ from [8].

Proposition 22. *Suppose $d \equiv 1 \bmod 8$ is an imaginary quadratic discriminant such that $d \not\equiv 0 \bmod 3$. We let $\theta = \frac{-1+\sqrt{d}}{2}$. Let $[a,b,c]$ be a primitive quadratic form of discriminant d and let $\tau = \frac{-b+\sqrt{d}}{2a}$. The action of the class group on $\zeta_{48}\mathfrak{f}_2(\theta)$ is given by the formula*

$$(18)\quad \left(\zeta_{48}\mathfrak{f}_2(\theta)\right)^{[a,-b,c]} = \begin{cases} \zeta_{48}^{b(a-c+a^2c)}\mathfrak{f}_2(\tau) & \text{if } 2 \nmid a \\ \zeta_{48}^{b(a-c-ac^2)}\mathfrak{f}_1(\tau) & \text{if } 2 \mid a \wedge 2 \nmid c \\ (-1)^{\frac{d-1}{8}}\zeta_{48}^{b(a-c+ac^2)}\mathfrak{f}(\tau) & \text{if } 2 \mid a \wedge 2 \mid c\,. \end{cases}$$

Proof. Theorem 20 gives a matrix $M \in \mathrm{GL}_2(\mathbb{Z}/48\mathbb{Z})$ that satisfies

$$\zeta_{48}\mathfrak{f}_2(\theta)^{[a,-b,c]} = (\zeta_{48}\mathfrak{f}_2)^M(\tau).$$

The residue classes $M_3 \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and $M_{16} \in \mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z})$ of M are respectively

$$M_3 \equiv \begin{cases} \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right) \cdot ST^{-a}ST^{-a}ST^{-ba} & \text{if } 3 \nmid a \\ \left(\begin{smallmatrix} 1 & 0 \\ 0 & c \end{smallmatrix}\right) \cdot T^{(b-1)c}ST^{c}ST^{c} & \text{if } 3 \mid a \wedge 3 \nmid c \\ \left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right) \cdot T^{1-b}ST^{b}ST^{b-1} & \text{if } 3 \mid a \wedge 3 \mid c \end{cases}$$

and

$$M_{16} \equiv \begin{cases} \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right) \cdot ST^{\frac{-1}{a}}ST^{\frac{-1}{a}}ST^{\frac{b-3}{2}\frac{1}{a}} & \text{if } 2 \nmid a \\ \left(\begin{smallmatrix} 1 & 0 \\ 0 & c \end{smallmatrix}\right) \cdot T^{(\frac{1-b}{2})c}ST^{\frac{1}{c}}ST^{c} & \text{if } 2 \mid a \wedge 2 \nmid c \\ \left(\begin{smallmatrix} 1 & 0 \\ 0 & a+b+c \end{smallmatrix}\right) \cdot T^{(\frac{1-b-2a}{2})(a+b+c)}ST^{\frac{1}{a+b+c}}ST^{a+b+c-1} & \text{if } 2 \mid a \wedge 2 \mid c\,. \end{cases}$$

We write $\zeta_{48} = \zeta_{16}^{-5} \cdot \zeta_3$. Then

$$(\zeta_{48}\mathfrak{f}_2)^M = (\zeta_{16}^{-5}(\zeta_3\mathfrak{f}_2) \bullet M_3) \bullet M_{16}$$

gives the action of M on on $\zeta_{48}\mathfrak{f}_2$. First we compute $\zeta_3\mathfrak{f}_2 \bullet M_3 = \mu_3\mathfrak{f}_2$ using (14). Here, μ_3 is the third root of unity

$$\mu_3 = \begin{cases} \zeta_3^{ab} & \text{if } 3 \nmid a \\ \zeta_3^{-bc} & \text{if } 3 \mid a \wedge 3 \nmid c \\ 1 & \text{if } 3 \mid a \wedge 3 \mid c. \end{cases}$$

In a similar fashion, we find

$$(\zeta_{16}^{-5}\mathfrak{f}_2) \bullet M_{16} = \begin{cases} \mu_{16}\mathfrak{f}_2 & \text{if } 2 \nmid a \\ \mu_{16}\mathfrak{f}_1 & \text{if } 2 \nmid c \\ \mu_{16}\mathfrak{f} & \text{if } 2 \mid a \wedge 2 \mid c\,, \end{cases}$$

where $\mu_{16} \in \mathbb{Q}(\zeta_{16})$ is

$$\mu_{16} = \begin{cases} \zeta_{16}^{-5ab} & \text{if } 2 \nmid a \\ \zeta_{16}^{5bc} & \text{if } 2 \mid a \wedge 2 \nmid c \\ \zeta_{16}^{5(a+b+c)(b+2a)-5} & \text{if } 2 \mid a \wedge 2 \mid c\,. \end{cases} \tag{19}$$

The expressions (19) for μ_{16} have been simplified using the condition $d \equiv 1 \bmod 8$. We conclude

$$(\zeta_{48}\mathfrak{f}_2)^M = \begin{cases} \mu_3 \cdot \mu_{16} \cdot \mathfrak{f}_2 & \text{if } 2 \nmid a \\ \mu_3 \cdot \mu_{16} \cdot \mathfrak{f}_1 & \text{if } 2 \mid a \wedge 2 \nmid c \\ \mu_3 \cdot \mu_{16} \cdot \mathfrak{f} & \text{if } 2 \mid a \wedge 2 \mid c\,. \end{cases} \tag{20}$$

We need to check that the formulas in (18) and (20) coincide in the case $3 \nmid d$ and $d \equiv 1 \bmod 8$. The condition $d \not\equiv 0 \bmod 3$ implies

$$\begin{aligned} b \equiv 0 \quad \text{or} \quad ac \not\equiv 1 \bmod 3 \\ \Rightarrow b(a - c + a^2c) \equiv b(a - c - ac^2) \bmod 3 \end{aligned} \tag{21}$$

and we easily check

$$\zeta_3^{b(a-c+a^2c)} = \begin{cases} \zeta_3^{ab} & \text{if } 3 \nmid a \\ \zeta_3^{-bc} & \text{if } 3 \mid a \wedge 3 \nmid c \\ 1 & \text{if } 3 \mid a \wedge 3 \mid c\,. \end{cases}$$

Similarly, under the restriction $d \equiv 1 \bmod 8$, one verifies that

$$\mu_{16} = \begin{cases} \zeta_{16}^{-5b(a-c+a^2c)} & \text{if } 2 \nmid a \\ \zeta_{16}^{-5b(a-c-ac^2)} & \text{if } 2 \mid a \wedge 2 \nmid c \\ \zeta_{16}^{d-1}\zeta_{16}^{-5b(a-c+ac^2)} & \text{if } 2 \mid a \wedge 2 \mid c \end{cases}$$

holds. □

References

[1] B. Birch, *Weber's class invariants*. Mathematika **16** (1969), pp. 283-294.

[2] S. Lang, *Elliptic functions*. 2nd edition, Springer GTM 112, 1987.

[3] F. Morain, *Primality Proving Using Elliptic Curves: An Update*. Algorithmic Number Theory, Springer LNCS 1423 (1998), pp. 111-130.

[4] R. Schertz, *Die singulären Werte der Weberschen Funktionen* $\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2, \gamma_2, \gamma_3$. J. Reine Angew. Math. **286/287** (1976), pp. 46-74.

[5] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Iwanami Shoten and Princeton University Press, 1971.

[6] G. Shimura, *Complex Multiplication*, Modular functions of One Variable I. Springer LNM 320 (1973), pp. 39-56.
[7] H. Weber, *Lehrbuch der Algebra. Band III: Elliptische Funktionen und algebraische Zahlen*. 2nd edition, Braunschweig, 1908. (Reprint by Chelsea, New York, 1961.)
[8] N. Yui and D. Zagier, *On the singular values of Weber modular functions*. Math. Comp. **66** (1997), no 220, pp. 1645-1662.

Alice Gee
Faculteit WINS,
Universiteit van Amsterdam,
Plantage Muidergracht 24,
1018 TV Amsterdam, The Netherlands
E-mail : gee@wins.uva.nl