Class fields by Shimura reciprocity
Gee, A.C.P.

Citation for published version (APA):
ter verkrijging van de graad van doctor aan de Universiteit van Amsterdam, op gezag van de Rector Magnificus prof. dr. J. J. M. Franse ten overstaan van een door het college voor promoties ingestelde commissie in het openbaar te verdedigen in de Aula der Universiteit op donderdag 11 januari 2001 te 10:00 uur

door

Alice Chia Ping Gee

geboren te Taipei, Taiwan
Promotor: Prof. dr. P. Stevenhagen

Deze promotie vindt plaats aan de Faculteit Natuurwetenschappen, Wiskunde en Informatica
PREFACE

This thesis consists of four papers. Each is concerned with the problem of finding explicit generators for some given class field of an imaginary quadratic number field. The first chapter was written in 1997 and appeared in print as


In it, generators for the Hilbert class field are found using singular values of the classical functions $\gamma_2$ and $\gamma_3$, Weber’s classical $f$-functions of level 48, and his $\omega$-functions of level 5. The method devised for computing the minimum polynomial of these generators proves some conjectural formulas appearing in recent literature.

Chapter two consists of joint work with my promotor P. Stevenhagen. This paper was published as


Here, the technical core of chapter one is given a simpler, more natural treatment. Examples of class invariants are calculated using a number of modular functions of higher level.

The third paper, “*Singular values of the Rogers-Ramanujan continued fraction*”, written with Mascha Honsbeek, was submitted for publication in June 1999. We determine the class fields generated by singular values of the famous Rogers-Ramanujan continued fraction and give a method for writing these values as nested radicals.

In the fourth and final chapter, we consider a certain generalization of the Weber $f$-functions. Using these functions, one obtains a range of class invariants for any imaginary quadratic number field.

Several changes of a typographical nature have been made to the published articles in order to allow for a uniform appearance of this thesis. In particular, page numbers and internal references have been altered.
# TABLE OF CONTENTS

1 Class invariants by Shimura’s reciprocity law 7
   1 Introduction ........................................ 7
   2 The modular function field $\mathcal{F}$ ............... 9
   3 Shimura reciprocity over the Hilbert class field .... 10
   4 Weber’s modular functions .......................... 14
   5 Computation of $W_{N, \theta}$ and its action on $F_N$ . 18
   6 Class invariants for $\gamma_3$ and $\gamma_2$ ........... 20
   7 Class invariants for the resolvents $\omega_0$ and $\omega_3$ of level 5 21
   8 Class invariants for the Weber $f$-functions .......... 22
   9 Shimura’s reciprocity law .......................... 28
  10 Action of the class group on class invariants ......... 30
  11 Formulas of Morain and Yui-Zagier .................. 33
      References ....................................... 35

2 Generating class fields using Shimura reciprocity 37
   1 Introduction ........................................ 37
   2 Modular functions ................................... 40
   3 Finding class invariants ............................ 43
   4 Computing class polynomials ........................ 45
   5 Numerical examples ................................ 46
      References ....................................... 50

3 Singular values of the Rogers-Ramanujan continued fraction 53
   1 Introduction ........................................ 53
   2 The modular function field of level 5 ................ 54
   3 Galois theory for singular values of modular functions 59
   4 The ray class field $H_5$ ............................ 62
   5 Nested radicals .................................... 66
      References ....................................... 69

4 Class invariants from Dedekind’s eta-function 71
   1 Introduction ........................................ 71
   2 Modularity of $\eta$-quotients ........................ 76
   3 Shimura reciprocity law ............................ 80
   4 The case $N = 3$ .................................. 81
   5 The case $N$ prime to 6 ............................. 83
   6 Examples and observations .......................... 89
      References ....................................... 92

Samenvatting 93
Acknowledgements 95
Curriculum Vitae 96
CLASS INVARIANTS BY SHIMURA'S RECIPROCITY LAW

ALICE GEE

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

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.

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 $\gamma_2$, $\gamma_3$, and the so-called Weber functions $f$, $f_1$, and $f_2$. We will also study Weber's resolvents $\omega_0$ and $\omega_3$ 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 $\theta$ 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 $j(\alpha)$, with $\alpha$ 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 $\theta$ 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

\[
H_{-71} = X^7 + 313645809715 X^6 - 3091990138604570 X^5 \\
+ 9839403881004781204930 X^4 \\
- 823534263439730779968091389 X^3 \\
+ 513880036645397678032372632946 X^2 \\
- 425319473946139603274605151187659 X \\
+ 737707086760731113357714241006081263.
\]

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

\[
f_Q^{\zeta_3 \gamma_2(\theta)} = X^7 + 6745 X^6 - 327467 X^5 + 51857115 X^4 + 2319299751 X^3 \\
+ 41264582513 X^2 - 307873876442 X + 903568991567
\]

\[
f_Q^{\omega_3(\theta)} = X^7 + 221 X^6 + 3999 X^5 + 79447 X^4 + 628970 X^3 \\
+ 3746281 X^2 + 12033163 X + 19868711
\]

\[
f_Q^{\zeta_{48} f(\theta)} = X^7 + X^6 - X^5 - X^4 - X^3 + X^2 + 2 X - 1.
\]

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 the Weber's functions \( \gamma_3, \gamma_2, f, f_1, f_2 \) we recover theorems of the type found in [7]. This treatment allows us to dispense with the need for ad hoc arguments which appear even in the more 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 \( \text{Cl}(O) \) 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 \( \gamma_3 \) and \( f_2 \).

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 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}^*$ as the fractional linear transformation $z \mapsto \frac{az + b}{cz + d}$.

When $N$ is a positive integer, let $\Gamma_N \subset \text{SL}_2(\mathbb{Z})$ denote the kernel of the map $\text{SL}_2(\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing coefficients modulo $N$. The quotient space $X(N) = \Gamma_N \backslash \mathbb{H}^*$ is a Galois cover of the projective line $\mathbb{P}^1(\mathbb{C})$ with group $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$. 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 Laurent series expansion in the parameter $q^{1/N}$ is called the Fourier expansion of $h$.

We embed the algebraic closure $\overline{\mathbb{Q}}$ of the rational numbers in $\mathbb{C}$ and fix $\zeta_N$ 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 $\mathcal{F} = \bigcup_{N \geq 1} F_N$. 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 $\alpha_N \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ represent the $\Gamma_N$-equivalence class of a fractional linear transformation $\alpha$ on $\mathbb{H}^*$. For $h \in F_N$ the action $h^{\alpha_N} = h \circ \alpha$ is well-defined and induces an isomorphism

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

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

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

which we can lift to $F_N$ in the following way. If $h \in F_N$ has Fourier expansion $\sum_k c_k q^{kN} \in \mathbb{Q}(\zeta_N)((q^{1/N}))$ then $\sum_k \sigma_d(c_k) q^{kN}$ is again a Fourier expansion of a function in $F_N$ which we denote by $h^{\sigma_d}$. 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

$$\begin{array}{c}
F_N \\
\downarrow \\
F_{N,\mathbb{Q}} \\
\downarrow \\
F_1 \\
\end{array}\quad \begin{array}{c}
F_1(\zeta_N) \\
\downarrow \\
F_1 \\
\end{array}$$
of fields. Define the subgroup
\[ G_N = \{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \mid d \in (\mathbb{Z}/NZ)^* \} \subset \text{GL}_2(\mathbb{Z}/NZ). \]

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

\[
\begin{array}{cccccc}
\{\pm 1\} & \rightarrow & \text{SL}_2(\mathbb{Z}/NZ) & \rightarrow & \text{Gal}(F_N/F_1(\zeta_N)) & \rightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \\
\{\pm 1\} & \rightarrow & \text{GL}_2(\mathbb{Z}/NZ) & \rightarrow & \text{Gal}(F_N/F_1) & \rightarrow & 1 \\
\downarrow & & \downarrow_{\text{det}} & & \downarrow & & \\
1 & \rightarrow & (\mathbb{Z}/NZ)^* & \rightarrow & \text{Gal}(F_1(\zeta_N)/F_1) & \rightarrow & 1.
\end{array}
\]

Passing to the projective limit yields the exact sequence
\[
1 \rightarrow \{\pm 1\} \rightarrow \text{GL}_2(\hat{\mathbb{Z}}) \rightarrow \text{Gal}(\mathcal{F}/F_1) \rightarrow 1.
\]

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 \(p \subset \mathcal{O}\) lying over \(p\), let \(K_p\) denote the completion of \(K\) at \(p\). Then \(K_p\) is canonically isomorphic to \(\prod_{p \mid p} K_p\). We use the rational primes \(p \in \mathbb{Z}\) to index the group of finite idèles

\[ J'_K = \prod_p K_p^* \]

of \(K\). The restricted product is taken with respect to the subgroups \(O_p^* \subset K_p^*\).

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

\[
1 \rightarrow K^* \rightarrow J'_K \xrightarrow{[\sim, K]} \text{Gal}(K^{ab}/K) \rightarrow 1.
\]

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 \(\theta\).
Theorem 1. (First main theorem of complex multiplication). Let \( O = \mathbb{Z}[\theta] \) 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

\[
1 \to O^* \to \prod_p \mathcal{O}_p^{*,[-1]} \to \text{Gal}(K^{ab}/K(j(\theta))) \to 1
\]

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 \( O^* \) and \( \prod_p ((1 + N \cdot \mathcal{O}_p) \cap \mathcal{O}_p^*) \).

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

\[
(g\theta)_p : K_p^* \to \text{GL}_2(\mathbb{Q}_p)
\]

be the injection that sends \( x_p \in K_p^* \) to the matrix in \( \text{GL}_2(\mathbb{Q}_p) \) that represents multiplication by \( x_p \) with respect to the \( \mathbb{Q}_p \)-basis \([\theta, 1]\) for \( K_p \). In other words, \( (g\theta)_p(x_p) \in \text{GL}_2(\mathbb{Q}_p) \) 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 \( \theta \) has minimum polynomial \( f_\theta^Q = X^2 + BX + C \), then for \( s_p, t_p \in \mathbb{Q}_p \) we have

\[
(g\theta)_p : s_p\theta + t_p \mapsto \begin{pmatrix}
t_p - B \cdot s_p & -C \cdot s_p \\
\frac{s_p}{t_p}
\end{pmatrix}.
\]

On \( J'_{K} = \prod'_p K_p^* \) we obtain an injective product map

\[
g_\theta = \prod_p (g\theta)_p : J'_{K} \to \prod_p' \text{GL}_2(\mathbb{Q}_p).
\]

Here, the restricted product is taken with respect to the subgroups \( \text{GL}_2(\mathbb{Z}_p) \) of \( \text{GL}_2(\mathbb{Q}_p) \). We write \( \prod_p \text{GL}_2(\mathbb{Z}_p) = \text{GL}_2(\hat{\mathbb{Z}}) \) and consider the pre-image

\[
g_\theta^{-1}(\text{GL}_2(\hat{\mathbb{Z}})) = \{ x \in J'_{K} \mid g_\theta(x) \in \text{GL}_2(\hat{\mathbb{Z}}) \}.
\]
From (4) we note

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

because \(\theta\) is an algebraic integer. Until section 10, we only need the restriction

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

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

$$
\begin{align*}
1 \to \mathcal{O}^* &\to \prod_p \mathcal{O}_p^* \xrightarrow{[\sim, K]} \text{Gal}(K^{ab}/K(j(\theta))) \to 1 \\
1 \to \{\pm 1\} &\to \text{GL}_2(\hat{\mathbb{Z}}) \to \text{Gal}(\mathcal{F}/F_1) \to 1.
\end{align*}
$$

**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 \(G \subset \text{GL}_2(\hat{\mathbb{Z}})\) 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 \(\theta\) 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 \(g_\theta[\prod_p \mathcal{O}_p^*] \subset \text{GL}_2(\hat{\mathbb{Z}})\) acts trivially on \(h\).

**Proof.** The open subgroup

$$\text{Stab}_{\mathcal{Q}(h)} = \{\alpha \in \text{GL}_2(\hat{\mathbb{Z}}) \mid h^\alpha = h\}$$

has fixed field \(\mathbb{Q}(h) \subset \mathcal{F}\). The pre-image \(g_\theta^{-1}(\text{Stab}_{\mathcal{Q}(h)})\) contains \(\mathcal{O}^* = \{\pm 1\}\), so \(g_\theta^{-1}(\text{Stab}_{\mathcal{Q}(h)}) \subset \prod_p \mathcal{O}_p^*\) is equal to the inverse image of \(\text{Gal}(K^{ab}/K(h(\theta)))\) with respect to the Artin map. Thus \(h(\theta)\) is a class invariant if and only if the equality \(g_\theta^{-1}(\text{Stab}_h) = \prod_p \mathcal{O}_p^*\) holds. This last equality is equivalent to the condition \(g_\theta[\prod_p \mathcal{O}_p^*] \subset \text{Stab}_h\) by the injectivity of \(g_\theta\). □
The infinite groups $\prod_p \mathcal{O}_p^*$ and $\text{GL}_2(\hat{\mathbb{Z}})$ occurring in Corollary 3 are not directly suited for performing explicit computations. In practice, for $h \in F_N$ and $\theta$ an algebraic integer we can reduce modulo $N$ and work with their finite quotient groups.

If $N$ is a positive integer let $U_N \subset \text{GL}_2(\hat{\mathbb{Z}})$ be the kernel of the natural map $\text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing coefficients modulo $N$. We have $U_N = \text{Stab}_{F_N}$ where $\text{Stab}_{F_N}$ is the inverse image of $\text{Gal}(\mathcal{F}/F_N)$ in $\text{GL}_2(\hat{\mathbb{Z}})$. Also, we observe

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

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

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

is exact and $g_\theta$ induces a well-defined injection between the quotient groups

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

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

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

which is the reduction of $g_\theta$ modulo $N$. One obtains the diagram

$$\begin{array}{ccc}
\mathcal{O}^* & \to & (\mathcal{O}/N\mathcal{O})^* \\
\downarrow{g_{\theta,N}} & & \downarrow{g_{\theta,N}} \\
\{\pm 1\} & \to & \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \\
& & \to \text{Gal}(F_N/F_1) \\
& & \to 1.
\end{array}$$

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

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

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

$$(6) \quad W_{N,\theta} = \left\{ \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \mid t, s \in \mathbb{Z}/N\mathbb{Z} \right\}.$$
Corollary 4. Let $O = \mathbb{Z}[\theta]$ 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 $\text{Stab}_{\mathbb{Q}(h)}$ in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing coefficients modulo $N$ is given by

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

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

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

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

The normalized Eisenstein series

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

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

are automorphic functions of weights 4 and 6, respectively. The Dedekind $\eta$-function

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

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

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$$
the transformation rules

\begin{equation}
\eta \circ S(z) = \sqrt{-iz} \eta(z) \quad \text{and} \quad \eta \circ T(z) = \zeta_{24}\eta(z)
\end{equation}

hold. Here, the branch of square root on the half plane \( \{ z \in \mathbb{C} \mid \text{Re}(z) > 0 \} \) is chosen to be positive on the real axis. The \( \Delta \)-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 \( 2 \times 2 \) 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 \( \Gamma_N \)-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 \( \Gamma_N \)-invariant.

**Reference.** [2; 11, §2 Theorem 3].

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

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

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

\[ \gamma_2(z) = 12 \frac{g_2(z)}{(2\pi)^{4}\eta^8(z)} \]

\[ \gamma_3(z) = 6^3 \frac{g_3(z)}{(2\pi)^{6}\eta^{12}(z)} \]

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

\begin{align*}
\gamma_2 \circ S &= \gamma_2 \\
\gamma_3 \circ S &= -\gamma_3 \\
\gamma_2 \circ T &= \zeta_3^{-1}\gamma_2 \\
\gamma_3 \circ T &= -\gamma_3
\end{align*}
from which one deduces that $\gamma_2$ is $\Gamma_3$-invariant and that $\gamma_3$ is $\Gamma_2$-invariant.

The function values of $\gamma_2$ and $\gamma_3$ are only moderately smaller than the $j$-function. Better results can be obtained by applying lemma 5 to quotients of $\Delta$. 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 $j$-functions.

\[
\begin{align*}
\eta(z) &= \zeta_{48}^{-1} \cdot \eta\left( \frac{z+1}{2} \right), \\
\eta_1(z) &= \frac{\eta\left( \frac{z}{2} \right)}{\eta(z)}, \\
\eta_2(z) &= \sqrt{2} \cdot \frac{\eta(2z)}{\eta(z)}.
\end{align*}
\]

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 $\eta_1, \eta_2,$ and $\sqrt{2} \cdot \eta_2$ have rational Fourier expansions. From the transformation rules (8) for $\eta(z)$ we obtain

\[
(f, f_1, f_2) \circ S = (f, f_2, f_1),
\]
\[
(f, f_1, f_2) \circ T = (\zeta_{48}^{-1} f_1, \zeta_{48}^{-1} f_2, \zeta_{48}^{-1} f_2).
\]

One deduces that $f, f_1$ and $f_2$ 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

\[
\gamma_3 = \frac{(j^{24} + 8) \cdot (f_1^{8} - f_2^{8})}{f_1^{8}}
\]
\[
\gamma_2 = \frac{j^{24} - 16}{f_1^{8}} = \frac{f_1^{24} + 16}{f_1^{8}} = \frac{f_2^{24} + 16}{f_2^{8}}
\]

are contained in $\mathbb{Q}(f_1^{8}, f_1^{8}, f_2^{8})$. Thus we note that both $\gamma_3$ and $\gamma_2$ 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

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

Namely, when we embed the algebraic closure $\overline{Q}$ in $\mathbb{C}$, the generator of $\text{Gal}(K/Q)$ is obtained by restricting complex conjugation to $K$. Thus if $\sigma \in \text{Aut}(\mathbb{C})$ 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 $\text{Gal}(K/Q)$.

The product expansion (7) and the expressions (10) and (12) imply that the functions $f, f_1, f_2, \gamma_3$ and $\gamma_2$ all take on real values along the imaginary axis in $\mathbb{H}$. As $\gamma_2$ has Fourier expansion in $\mathbb{Q}((q^{1/2}))$, we also note when $z \in \mathbb{H}$ has real part $\Re(z) \in \frac{1}{2} \cdot \mathbb{Z}$, 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

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

is simple. Weber shows that any subgroup of $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})/\{\pm 1\}$ 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

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

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 $\omega_i$ 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 $\omega_0$ is $G_5$-invariant and thus has Fourier expansion in \( \mathbb{Q}((q^{1/5})) \). In particular, if $z \in H$ 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 $\text{SL}_2(\mathbb{Z})$

$$
(\omega_0, \omega_1, \omega_2, \omega_3, \omega_4) \circ S = (\omega_0, \omega_2, \omega_1, \omega_4, \omega_3)
$$

$$
(\omega_0, \omega_1, \omega_2, \omega_3, \omega_4) \circ T = (\omega_1, \omega_2, \omega_3, \omega_4, \omega_0).
$$

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 $\left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \text{SL}_2(\mathbb{Z})$ 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 $\left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ as an element of $\langle S_N, T_N \rangle$.

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

$$
\left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)_N = \begin{cases}
(\text{T}^yS\text{T}^c\text{ST}^dy-b)_N & \text{if } (c, N) = 1 \\
(\text{ST}^{-y}\text{ST}^{-a}\text{ST}^{by-d})_N & \text{if } (a, N) = 1.
\end{cases}
$$

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

$$
\text{ST}^{-y}\left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)_N = \left( \begin{smallmatrix} 1 & b+yd \\ c & d \end{smallmatrix} \right)_N.
$$

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 $S \cdot \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)_N = \left( \begin{smallmatrix} -c & -d \\ a & b \end{smallmatrix} \right)_N$. \( \square \)
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 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 $W_{N,\theta} \simeq (\mathcal{O}/\mathcal{O}^\star)$ are isomorphic. Suppose $\theta$ and $\tau$ are imaginary quadratic algebraic integers. Then the description (6) of $W_{N,\theta}$ shows

$$f_\theta^T \equiv f_\theta^\tau \mod N \implies W_{N,\theta} = W_{N,\tau} \subset \text{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

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

**Lemma 7.** Suppose $u \in M_2^+(\mathbb{Z})$ such that $u_N \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. If both $\theta$ 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 $g_\theta$ as a function on $\prod_p \mathcal{O}_p^\star$, observe that

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

for any $x \in \prod_p \mathcal{O}_p^\star$. \qed

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

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

The congruence

$$f_\theta^{\theta + 8} = X^2 + 17X + (m + 72) \equiv f_\theta^T \mod 16$$

which 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
\[
f_Q^6 = X^2 + m \quad \text{and} \quad f_Q^6 = X^2 + (m + 8).
\]
The congruence
\[
f_Q^{3\theta} = X^2 + 9m \equiv f_Q^6 \mod 16
\]
gives
\[
W_{16, r} = W_{16, 3\theta} = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \cdot W_{16, \theta} \cdot \begin{pmatrix} 11 & 0 \\ 0 & 1 \end{pmatrix}.
\]

6. Class invariants for \( \gamma_3 \) and \( \gamma_2 \)
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
\[
2 \nmid d \implies \gamma_3(\theta) \text{ is a class invariant}
\]
\[
3 \nmid d \implies \zeta_3^7 \gamma_2(\theta) \text{ is a class invariant with } f_K^{3\theta} \gamma_2(\theta) \in \mathbb{Q}[X].
\]

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 \( \gamma_3 \). If \( 2 \) splits in \( \mathcal{O} \) then \( (\mathcal{O}/2\mathcal{O})^* \) is trivial. If \( 2 \) is inert in \( \mathcal{O} \) then \( (\mathcal{O}/2\mathcal{O})^* \simeq \mathbb{Z}/2\mathbb{Z} \). It follows that the length of the \( W_{2, \theta} \)-orbit of \( \gamma_3 \) divides 3. Because \( \gamma_3^2 = j - 12^2 \) 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 \( f_Q^6 = X^2 + BX + C \) is the minimum polynomial for \( \theta \) then \( W_{2, \theta} \) is generated by
\[
\begin{cases}
(0 \ 1) \ 2 = S_2 & \text{if } C \equiv 1 \mod 2 \\
(1 \ 0) \ 2 = (TST)_2 & \text{if } C \equiv 0 \mod 2.
\end{cases}
\]

Both of these matrices act on \( \mathbb{Q}(\gamma_3) \) as \( \gamma_3 \mapsto -\gamma_3 \). As
\[
\text{Gal}(K(F_2(\theta))/K(j(\theta))) \simeq W_{2, \theta}/\{\pm 1\}
\]
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 \( \gamma_2 \). In the case \( B \equiv 0 \mod 3 \) we find the generators for \( W_{3, \theta} \) given in the table below.
Using the factorization formula from Lemma 6 and the transformation rules (9), we calculate the action of each of these generators on $\zeta_3$ and $\gamma_2$. In the following table, the second column indicates the discriminants $d$ for which a matrix in the first column occurs as a generator for $W_{3,\theta}$.

<table>
<thead>
<tr>
<th>Generator</th>
<th>$d \mod 3$</th>
<th>Structure</th>
<th>$W_{3,\theta}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\begin{pmatrix} 2 &amp; 0 \ 0 &amp; 2 \end{pmatrix}$</td>
<td>1</td>
<td>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$</td>
<td>$\langle (1 \ 0 \ 3) \rangle$</td>
</tr>
<tr>
<td>$\begin{pmatrix} 0 &amp; 1 \ 1 &amp; 0 \end{pmatrix}$</td>
<td>1</td>
<td>$\mathbb{Z}/8\mathbb{Z}$</td>
<td>$\langle (1 \ 2 \ 1) \rangle$</td>
</tr>
<tr>
<td>$\begin{pmatrix} 1 &amp; 0 \ 0 &amp; 1 \end{pmatrix}$</td>
<td>2</td>
<td>$\mathbb{Z}/6\mathbb{Z}$</td>
<td>$\langle (1 \ 0 \ 3) \rangle$</td>
</tr>
<tr>
<td>$\begin{pmatrix} 0 &amp; 2 \ 1 &amp; 0 \end{pmatrix}$</td>
<td>0</td>
<td>$\mathbb{Z}/12\mathbb{Z}$</td>
<td>$\langle (1 \ 1 \ 3) \rangle$</td>
</tr>
</tbody>
</table>

Observe that if $d$ is not divisible by 3 then $\gamma_2(\theta)$ is a class invariant. We have $f_{K}(\theta) \in \mathbb{Q}[X]$ 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 for $B \equiv 0 \mod 3$.

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 $\gamma_2$ 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 $B \in \mathbb{Z}$. \qed

7. Class Invariants for the Resolvents $\omega_0$ and $\omega_3$ 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 $\omega_i$, $i = 0, \ldots, r$ 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 $d \equiv \pm 1 \mod 5$ with $d < -4$. Let $\mathcal{O} = \mathbb{Z}[\theta]$ be the ring of integers of $K$ with

$$\theta = \begin{cases} \frac{-1+\sqrt{d}}{4} & \text{if } d \equiv 0 \mod 4 \\ \frac{-1-\sqrt{d}}{4} & \text{if } d \equiv 1 \mod 4. \end{cases}$$
The following statements hold:

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

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

\[ f_\theta^0 = X^2 + BX + C \in \mathbb{Z}[X] \]

be the minimum polynomial for \( \theta \). 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 \( \theta \) for which a matrix in the first column appears as a generator for \( W_{5,\theta} \). The image of \( \omega_i \), for \( i = 0, \ldots, 4 \) with respect to the action of these matrices is given in the remaining columns.

<table>
<thead>
<tr>
<th>Generator</th>
<th>((B, C) \mod 5)</th>
<th>(\omega_0)</th>
<th>(\omega_1)</th>
<th>(\omega_2)</th>
<th>(\omega_3)</th>
<th>(\omega_4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\begin{pmatrix} 2 &amp; 0 \ 0 &amp; 2 \end{pmatrix})</td>
<td>((0, 1), (0, 4), (1, 0), (1, 3))</td>
<td>(\omega_0)</td>
<td>(\omega_1)</td>
<td>(\omega_2)</td>
<td>(\omega_3)</td>
<td>(\omega_4)</td>
</tr>
<tr>
<td>(\begin{pmatrix} 1 &amp; 4 \ 4 &amp; 1 \end{pmatrix})</td>
<td>((0, 1))</td>
<td>(\omega_0)</td>
<td>(\omega_3)</td>
<td>(\omega_4)</td>
<td>(\omega_2)</td>
<td>(\omega_1)</td>
</tr>
<tr>
<td>(\begin{pmatrix} 2 &amp; 0 \ 4 &amp; 1 \end{pmatrix})</td>
<td>((1, 0))</td>
<td>(\omega_2)</td>
<td>(\omega_0)</td>
<td>(\omega_4)</td>
<td>(\omega_3)</td>
<td>(\omega_1)</td>
</tr>
<tr>
<td>(\begin{pmatrix} 3 &amp; 1 \ 1 &amp; 3 \end{pmatrix})</td>
<td>((0, 4))</td>
<td>(\omega_0)</td>
<td>(\omega_4)</td>
<td>(\omega_1)</td>
<td>(\omega_2)</td>
<td>(\omega_3)</td>
</tr>
<tr>
<td>(\begin{pmatrix} 0 &amp; 2 \ 1 &amp; 3 \end{pmatrix})</td>
<td>((1, 3))</td>
<td>(\omega_1)</td>
<td>(\omega_2)</td>
<td>(\omega_4)</td>
<td>(\omega_3)</td>
<td>(\omega_0)</td>
</tr>
</tbody>
</table>

Observe that \(\omega_0\) is invariant under \(W_{5,\theta}\) in the case that \(d \equiv 0 \mod 4\), and \(\omega_3\) is \(W_{5,\theta}\)-invariant in the case that \(d \equiv 1 \mod 4\).

The function \(\omega_0\) takes on real values at \(z \in \mathbb{H}\) with \(R(z) \in \frac{5}{2} \cdot \mathbb{Z}\) and the transformation rules (13) give

\[ \omega_3 = \omega_0 \circ T^{\frac{3}{2}}. \]

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

8. Class invariants for the Weber f-functions

We now determine class invariants for powers of the Weber f-functions by computing the explicit action of \(W_{48,\theta} \cong W_{5,\theta} \times W_{16,\theta}\) on \(\mathbb{Q}(\zeta_{48}, f_1, f_2)\) as the coefficients of the minimum polynomial \(f_\theta^0 \in \mathbb{Z}[X]\) range through \(\mathbb{Z}/48\mathbb{Z}\). In doing so we recover several results from [1], [4], and [7].
We lift the action of $\GL_2(\mathbb{Z}/3\mathbb{Z})$ to $F_{48}$ by the Chinese remainder theorem. First we need to embed the generators $S_3, T_3 \in \SL_2(\mathbb{Z}/3\mathbb{Z})$ in $\SL_2(\mathbb{Z}/48\mathbb{Z})$ as

$$
S_3 \mapsto \left(\begin{array}{cc} 33 & 32 \\ 16 & 33 \end{array}\right)_{48} = (T^2S^3T^{-16}ST^{14})_{48} \\
T_3 \mapsto \left(\begin{array}{cc} 1 & 16 \\ 0 & 1 \end{array}\right)_{48} = (T^{16})_{48}.
$$

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

$$
h \cdot S_3 = h \circ T^2S^3T^{-16}ST^{14} \\
h \cdot T_3 = h \circ T^{16}.
$$

For $\left(\begin{array}{c} 1 \\ 0 \end{array}\right)_{3} \in G_3$, let $\sigma_d$ 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

$$h \cdot \left(\begin{array}{c} 1 \\ 0 \end{array}\right)_{3} = h^d_{\sigma}.
$$

The explicit action of $\GL_2(\mathbb{Z}/3\mathbb{Z})$ on $\mathbb{Q}(\zeta_{48}, f, f_1, f_2)$ is given by

$$
(\zeta_3, \zeta_{16}, f, f_1, f_2) \cdot S_3 = (\zeta_3, \zeta_{16}, f, f_1, f_2) \\
(\zeta_3, \zeta_{16}, f, f_1, f_2) \cdot T_3 = (\zeta_3, \zeta_{16}, \zeta_3^d f, \zeta_3^d f_1, \zeta_3^d f_2) \\
(\zeta_3, \zeta_{16}, f, f_1, f_2) \cdot \left(\begin{array}{c} 1 \\ 0 \end{array}\right)_{3} = (\zeta_3^d, \zeta_{16}, f, f_1, f_2).
$$

**Proposition 12.** Let $\theta = -B + \sqrt{3}$ generate the imaginary quadratic order of fundamental discriminant $d < -4$. The group $\GL_2(\mathbb{Z}/3\mathbb{Z})$ acts trivially on $\mathbb{Q}(f^3, f_1, f_2)$. Furthermore we have

$$3 \mid d \implies W_{3, \theta} \text{ acts trivially on } \mathbb{Q}(\zeta_3^B f, \zeta_3^B f_1, \zeta_3^B f_2).
$$

**Proof.** By the transformation rules (14) every matrix in $\GL_2(\mathbb{Z}/3\mathbb{Z})$ acts trivially on $\mathbb{Q}(f^3, f_1, f_2)$.

Suppose that 3 divides $B$. We use the generators of $W_{3, \theta}$ found section 8 to compute the action of $W_{3, \theta}$ on $\mathbb{Q}(\zeta_{48}, f, f_1, f_2)$. 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 image of $\zeta_3$, $f$, $f_1$, and $f_2$ respectively are displayed in the remaining columns.

<table>
<thead>
<tr>
<th>Generator</th>
<th>$d \mod 3$</th>
<th>$\zeta_3$</th>
<th>$f$</th>
<th>$f_1$</th>
<th>$f_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\left(\begin{array}{c} 2 \ 0 \end{array}\right)_{3}$</td>
<td>1</td>
<td>$\zeta_3$</td>
<td>$f$</td>
<td>$f_1$</td>
<td>$f_2$</td>
</tr>
<tr>
<td>$\left(\begin{array}{c} 1 \ 1 \end{array}\right)_{3}$</td>
<td>2</td>
<td>$\zeta_3^2$</td>
<td>$f$</td>
<td>$f_1$</td>
<td>$f_2$</td>
</tr>
<tr>
<td>$\left(\begin{array}{c} 2 \ 0 \end{array}\right)_{3}$</td>
<td>0</td>
<td>$\zeta_3$</td>
<td>$\zeta_3^2 f$</td>
<td>$\zeta_3^2 f_1$</td>
<td>$\zeta_3^2 f_2$</td>
</tr>
</tbody>
</table>
From the table it is clear that if 3 does not divide \(d\) then \(W_{3,\theta}\) acts trivially on \(\mathbb{Q}(f_1, f_2)\). 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

\[
(\zeta_3^B f, \zeta_3^B f_1, \zeta_3^B f_2) = (f, f_1, f_2) \cdot T_3^{-B}
\]

and we note

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

Since

\[
W_{3,\theta - 16B}
\]

acts trivially on \(h \Leftrightarrow W_{3,\theta}\) acts trivially on \(h \cdot T_3^{-B}\)

holds any function \(h \in \mathbb{F}_{48}\), the proposition holds for all integers \(B \in \mathbb{Z}\). \(\square\)

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

\[
S_{16} \mapsto \begin{pmatrix} 16 & 15 \\ 33 & 16 \end{pmatrix}_{48} = (S^3 T^{-2} S T^{16} S T^{14})_{48},
\]

\[
T_{16} \mapsto \begin{pmatrix} 1 & 33 \\ 0 & 1 \end{pmatrix}_{48} = (T^{33})_{48}.
\]

and define the action of \(S_{16}\) and \(T_{16}\) on \(h \in \mathbb{F}_{48}\) as

\[
h \cdot S_{16} = h \circ S^3 T^{-2} S T^{16} S T^{14},
\]

\[
h \cdot T_{16} = h \circ T^{33}.
\]

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

\[
h \cdot (\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix})_{16} = h^{\sigma_d}
\]

where \(\sigma_d\) is the action on \(\mathbb{F}_{48}\) obtained by lifting the automorphism of \(\mathbb{Q}(\zeta_{48})\) determined by \(\zeta_3 \mapsto \zeta_3\) and \(\zeta_{16} \mapsto \zeta_{16}^d\). The \(\text{GL}_2(\mathbb{Z}/16\mathbb{Z})\)-action on \(\mathbb{Q}(\zeta_{48}, f, f_1, f_2)\) is given by

\[
(\zeta_3, \zeta_{16}, f, f_1, f_2) \cdot S_{16} = (\zeta_3, \zeta_{16}, f, f_1, f_2)
\]

\[
(\zeta_3, \zeta_{16}, f, f_1, f_2) \cdot T_{16} = (\zeta_3, \zeta_{16}, \zeta_{16}^5 f_1, \zeta_{16}^5 f_2, \zeta_{16}^5 f_2)
\]

\[
(\zeta_3, \zeta_{16}, f, f_1, f_2) \cdot (\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix})_{16} = (\zeta_3, \zeta_{16}, f, f_1, f_2, \frac{\sigma_d(\sqrt{2})}{2} f_2).
\]

In the remainder of this section we calculate the action of \(W_{16,\theta}\) on \(\mathbb{Q}(\zeta_{48}, f, f_1, f_2)\) 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 \(\mathbb{Q}(\zeta_{48}, f, f_1, f_2)\) 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

\[
d \equiv 1 \mod 8 \implies W_{16, \theta} \text{ acts trivially on } \zeta_{16}^{-5}f_2.
\]

Proof. If \( d \equiv 1 \mod 8 \) 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 \( f_\mathbb{Q}^8 \) 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 \( W_{16, \theta} \).

<table>
<thead>
<tr>
<th>Generator</th>
<th>( \frac{1-d}{4} \mod 8 )</th>
<th>( \zeta_{16} )</th>
<th>( f_1 )</th>
<th>( f_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>\begin{pmatrix} 15 &amp; 0 \ 0 &amp; 15 \end{pmatrix}</td>
<td>0, 2, 4, 6</td>
<td>\zeta_{16}</td>
<td>f_1</td>
<td>f_2</td>
</tr>
<tr>
<td>\begin{pmatrix} 3 &amp; 0 \ 0 &amp; 3 \end{pmatrix}</td>
<td>0, 2, 4, 6</td>
<td>\zeta_8</td>
<td>f_1</td>
<td>\zeta_8f_1</td>
</tr>
<tr>
<td>\begin{pmatrix} 13 &amp; 0 \ 4 &amp; 1 \end{pmatrix}</td>
<td>0, 4</td>
<td>\zeta_{16}</td>
<td>\zeta_8f_1</td>
<td>f_1</td>
</tr>
<tr>
<td>\begin{pmatrix} 13 &amp; 8 \ 4 &amp; 1 \end{pmatrix}</td>
<td>2, 6</td>
<td>\zeta_{16}</td>
<td>\zeta_8f_1</td>
<td>\zeta_8f_1</td>
</tr>
<tr>
<td>\begin{pmatrix} 15 &amp; 0 \ 2 &amp; 1 \end{pmatrix}</td>
<td>0</td>
<td>\zeta_{16}</td>
<td>\zeta_8f_1</td>
<td>f_1</td>
</tr>
<tr>
<td>\begin{pmatrix} 15 &amp; 8 \ 2 &amp; 1 \end{pmatrix}</td>
<td>4</td>
<td>\zeta_{16}</td>
<td>\zeta_8f_1</td>
<td>\zeta_{16}f_1</td>
</tr>
<tr>
<td>\begin{pmatrix} 13 &amp; 4 \ 6 &amp; 3 \end{pmatrix}</td>
<td>2</td>
<td>\zeta_{16}</td>
<td>\zeta_8f_1</td>
<td>f_1</td>
</tr>
<tr>
<td>\begin{pmatrix} 13 &amp; 12 \ 6 &amp; 3 \end{pmatrix}</td>
<td>6</td>
<td>\zeta_{16}</td>
<td>\zeta_8f_1</td>
<td>\zeta_{16}f_1</td>
</tr>
</tbody>
</table>

Observe that each the automorphisms in the above table fixes \( \zeta_{16}^{-5}f_2 \). 

We continue with the inert case.

In the case that \( \mathcal{O} \) is an imaginary quadratic order of discriminant \( d \equiv 5 \mod 8 \), 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 \( f^4, f_1^4, \) or \( f_2^4 \).

One can of course determine functions \( h \in \mathbb{Q}(\zeta_{48}, f_1, f_2) \) which are invariant under \( W_{16, \theta} \) but which might not satisfy the extra condition \( \mathbb{Q}(h) \subset \mathbb{Q}(\mathcal{O}) \). 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 \( d \equiv 5 \mod 8 \), 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 \( \mathbb{Q}(\zeta_{48}, f_1, f_2) \).
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.

<table>
<thead>
<tr>
<th>Generator</th>
<th>( \frac{1-d}{4} \mod 16 )</th>
<th>( \zeta_{16} )</th>
<th>( f )</th>
<th>( f_1 )</th>
<th>( f_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \begin{pmatrix} 13 &amp; 12 \ 4 &amp; 1 \end{pmatrix} )</td>
<td>1, 5, 9, 13</td>
<td>( \zeta_{16}^{13} )</td>
<td>( \zeta_{16}^8 f )</td>
<td>( \zeta_{16}^{12} f_1 )</td>
<td>( \zeta_{16}^{15} f_2 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 13 &amp; 4 \ 4 &amp; 1 \end{pmatrix} )</td>
<td>3, 7, 11, 15</td>
<td>( \zeta_{16}^{13} )</td>
<td>( f )</td>
<td>( \zeta_{16}^{12} f_1 )</td>
<td>( \zeta_{16}^{15} f_2 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 15 &amp; 14 \ 2 &amp; 1 \end{pmatrix} )</td>
<td>1, 9</td>
<td>( \zeta_{16}^{3} )</td>
<td>( \zeta_{16}^8 f )</td>
<td>( \zeta_{16}^{14} f_1 )</td>
<td>( \zeta_{16}^2 f_2 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 15 &amp; 10 \ 2 &amp; 1 \end{pmatrix} )</td>
<td>3, 11</td>
<td>( \zeta_{16}^{11} )</td>
<td>( \zeta_{16}^8 f )</td>
<td>( \zeta_{16}^8 f_1 )</td>
<td>( \zeta_{16}^{15} f_2 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 15 &amp; 8 \ 2 &amp; 1 \end{pmatrix} )</td>
<td>5, 13</td>
<td>( \zeta_{16}^{3} )</td>
<td>( f )</td>
<td>( \zeta_{16}^{12} f_1 )</td>
<td>( \zeta_{16}^2 f_2 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 15 &amp; 2 \ 2 &amp; 1 \end{pmatrix} )</td>
<td>7, 15</td>
<td>( \zeta_{16}^{11} )</td>
<td>( \zeta_{16}^4 f )</td>
<td>( \zeta_{16}^{10} f_1 )</td>
<td>( \zeta_{16}^{15} f_2 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 1 &amp; 1 \ 2 &amp; 1 \end{pmatrix} )</td>
<td>1</td>
<td>( \zeta_{16} )</td>
<td>( \zeta_{16}^{11} f_2 )</td>
<td>( \zeta_{16}^{15} f_1 )</td>
<td>( \zeta_{16}^2 f_2 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 7 &amp; 7 \ 3 &amp; 10 \end{pmatrix} )</td>
<td>3</td>
<td>( \zeta_{16} )</td>
<td>( \zeta_{16}^{13} f_2 )</td>
<td>( \zeta_{16}^{15} f_1 )</td>
<td>( \zeta_{16}^3 f_2 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 5 &amp; 13 \ 7 &amp; 12 \end{pmatrix} )</td>
<td>5</td>
<td>( \zeta_{16} )</td>
<td>( \zeta_{16}^7 f_2 )</td>
<td>( \zeta_{16}^3 f_1 )</td>
<td>( \zeta_{16}^2 f_1 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 11 &amp; 8 \ 11 &amp; 6 \end{pmatrix} )</td>
<td>7</td>
<td>( \zeta_{16} )</td>
<td>( \zeta_{16}^{15} f_2 )</td>
<td>( \zeta_{16}^3 f_1 )</td>
<td>( \zeta_{16}^3 f_1 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 9 &amp; 9 \ 15 &amp; 8 \end{pmatrix} )</td>
<td>9</td>
<td>( \zeta_{16} )</td>
<td>( \zeta_{16}^3 f_2 )</td>
<td>( \zeta_{16}^{11} f_1 )</td>
<td>( \zeta_{16}^3 f_1 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 13 &amp; 15 \ 3 &amp; 2 \end{pmatrix} )</td>
<td>11</td>
<td>( \zeta_{16} )</td>
<td>( \zeta_{16}^{15} f_2 )</td>
<td>( \zeta_{16}^3 f_1 )</td>
<td>( \zeta_{16}^3 f_1 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 13 &amp; 5 \ 7 &amp; 4 \end{pmatrix} )</td>
<td>13</td>
<td>( \zeta_{16} )</td>
<td>( \zeta_{16}^{15} f_2 )</td>
<td>( \zeta_{16}^3 f_1 )</td>
<td>( \zeta_{16}^{15} f_1 )</td>
</tr>
<tr>
<td>( \begin{pmatrix} 11 &amp; 11 \ 15 &amp; 11 \end{pmatrix} )</td>
<td>15</td>
<td>( \zeta_{16} )</td>
<td>( \zeta_{16}^{15} f_2 )</td>
<td>( \zeta_{16}^{15} f_1 )</td>
<td>( f_1 )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( m \mod 8 )</th>
<th>( W_{16,\theta} ) Invariant</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( \sqrt{2} \cdot f^2 )</td>
</tr>
<tr>
<td>2</td>
<td>( \sqrt{2} \cdot f_1 )</td>
</tr>
<tr>
<td>5</td>
<td>( f^4 )</td>
</tr>
<tr>
<td>6</td>
<td>( f_1^2 )</td>
</tr>
</tbody>
</table>

**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

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

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 \( Q(\zeta_{48}, f_1, f_2) \). The second column of the table indicates the \( m \) for which a matrix occurs as a generator for \( W_{16,\theta} \).
We see that all of the matrices listed in the table above act trivially on $f_1$. 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 $f_1^2$. Since $f_1$ takes on real values along the imaginary axis of the complex upper half plane, we choose the normalizations

$$\begin{cases} f_1^2 & \text{if } m \equiv 6 \mod 8 \\ \sqrt{2} \cdot f_1^2 & \text{if } m \equiv 2 \mod 8. \end{cases}$$

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

We now perform a similar calculation when $m$ is odd.

<table>
<thead>
<tr>
<th>Generator</th>
<th>$m \mod 16$</th>
<th>$\zeta_{16}$</th>
<th>$f$</th>
<th>$f_1$</th>
<th>$f_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(1_{15}^5 0_{15}^5)$</td>
<td>5, 13</td>
<td>$\zeta_{16}$</td>
<td>$f$</td>
<td>$f_1$</td>
<td>$f_2$</td>
</tr>
<tr>
<td>$(1_{15}^5 0_{15}^5)$</td>
<td>1, 9</td>
<td>$\zeta_{16}^5$</td>
<td>$f$</td>
<td>$\zeta_{16}^8 f_1$</td>
<td>$\zeta_{16}^8 f_2$</td>
</tr>
<tr>
<td>$(0_{15}^5 1_{15}^5)$</td>
<td>1</td>
<td>$\zeta_{16}$</td>
<td>$f$</td>
<td>$f_2$</td>
<td>$f_1$</td>
</tr>
<tr>
<td>$(3_{12}^2 1_{12}^2)$</td>
<td>9</td>
<td>$\zeta_{16}^3$</td>
<td>$\zeta_{16}^8 f$</td>
<td>$\zeta_{16}^8 f_2$</td>
<td>$\zeta_{16}^8 f_1$</td>
</tr>
<tr>
<td>$(0_{12}^5 1_{12}^5)$</td>
<td>9</td>
<td>$\zeta_{16}$</td>
<td>$f$</td>
<td>$f_2$</td>
<td>$f_1$</td>
</tr>
<tr>
<td>$(3_{12}^2 1_{12}^2)$</td>
<td>5</td>
<td>$\zeta_{16}^3$</td>
<td>$\zeta_{16}^8 f$</td>
<td>$\zeta_{16}^8 f_2$</td>
<td>$\zeta_{16}^8 f_1$</td>
</tr>
<tr>
<td>$(0_{12}^5 1_{12}^5)$</td>
<td>5</td>
<td>$\zeta_{16}$</td>
<td>$f$</td>
<td>$\zeta_{16}^8 f_2$</td>
<td>$f_1$</td>
</tr>
<tr>
<td>$(2_{1}^3 1_{1}^3)$</td>
<td>13</td>
<td>$\zeta_{16}^3$</td>
<td>$\zeta_{16}^8 f$</td>
<td>$\zeta_{16}^8 f_2$</td>
<td>$\zeta_{16}^8 f_1$</td>
</tr>
<tr>
<td>$(0_{1}^3 1_{1}^3)$</td>
<td>13</td>
<td>$\zeta_{16}^3$</td>
<td>$f$</td>
<td>$\zeta_{16}^8 f_2$</td>
<td>$f_1$</td>
</tr>
</tbody>
</table>

Here we see that each of the automorphisms in the above table stabilizes $f^4$. In the case of $m \equiv 1 \mod 8$ we can actually do a little better by normalizing $f^2$ using some suitable element of $\mathbb{Q}(\zeta_{16})$. The function $\sqrt{2} \cdot f^2$ is $W_{16,\theta}$-invariant and real-valued at $\theta$. □
Theorem 15 (2 split). Let $K$ be an imaginary quadratic number field of discriminant $d < -4$ and let $\theta = \frac{-1 + \sqrt{-d}}{2}$. If $d \equiv 1 \mod 8$ then we have

$$3 \mid d \Rightarrow \zeta_{48}f_2(\theta) \text{ is a class invariant}$$
$$3 \mid d \Rightarrow \zeta_{16}f_3(\theta) \text{ is a class invariant}$$

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

Proof. Apply Propositions 12 and 13 to $\zeta_3 \zeta_2^{-5}f_2 = \zeta_{48}f_2$. Note from definitions (7) and (10) that if $z \in \mathbb{H}$ with $\Re(z) = -\frac{1}{2}$, then we have $\zeta_{48}f_2(z) \in \mathbb{R}$.

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.

<table>
<thead>
<tr>
<th>$m \mod 8$</th>
<th>$d \not\equiv 0 \mod 3$</th>
<th>$d \equiv 0 \mod 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\sqrt{2}f^8(\theta)$</td>
<td>$\sqrt{2}f^8(\theta)$</td>
</tr>
<tr>
<td>2</td>
<td>$\sqrt{2}f^3_1(\theta)$</td>
<td>$\sqrt{2}f^3_1(\theta)$</td>
</tr>
<tr>
<td>5</td>
<td>$f^4(\theta)$</td>
<td>$f^{12}(\theta)$</td>
</tr>
<tr>
<td>6</td>
<td>$f^3_1(\theta)$</td>
<td>$f^6(\theta)$</td>
</tr>
</tbody>
</table>

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

Proof. Apply Proposition 12 and 14.

9. Shimura's reciprocity law

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

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

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

Let $A'_Q = \prod'_p \mathbb{Q}_p$ 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 $\text{GL}_2(A'_Q) = \prod'_p \text{GL}_2(\mathbb{Q}_p)$, where the restricted product is taken with respect to $\text{GL}_2(\mathbb{Z}_p) \subset \text{GL}_2(\mathbb{Q}_p)$. We consider $\text{GL}_2(\hat{\mathbb{Z}}) \subset \text{GL}_2(A'_Q)$ to be a subgroup by means of the embedding

$$\text{GL}_2(\hat{\mathbb{Z}}) \cong \prod_p \text{GL}_2(\mathbb{Z}_p) \hookrightarrow \prod'_p \text{GL}_2(\mathbb{Q}_p) \cong \text{GL}_2(A'_Q).$$
Let $GL^+_2(\mathbb{Q})$ denote the group of rational $2 \times 2$ matrices with positive determinant. Embedding $\mathbb{Q}$ along the diagonal of $A^f_\mathbb{Q}$ we view $GL^+_2(\mathbb{Q}) \subset GL_2(A^f_\mathbb{Q})$ to be a subgroup. In particular, we identify $\mathbb{Q}^*$ with the scalar matrices $\mathbb{Q}^* \subset GL^+_2(\mathbb{Q}) \subset GL_2(A^f_\mathbb{Q})$.

One can show that every $x \in GL_2(A^f_\mathbb{Q})$ can be written as

$$x = u \cdot \alpha$$

with $u \in GL_2(\hat{\mathbb{Z}})$ and $\alpha \in GL^+_2(\mathbb{Q})$.

This decomposition is not unique since $SL_2(\mathbb{Z}) = GL_2(\hat{\mathbb{Z}}) \cap GL^+_2(\mathbb{Q})$. Nonetheless, the decomposition $x = u \cdot \alpha$ determines a group action of $GL_2(A^f_\mathbb{Q})$ on $\mathcal{F}$ given by $h^x = h^u \circ \alpha$. Here, $u \in GL_2(\hat{\mathbb{Z}})$ acts via (1) and $\alpha \in GL^+_2(\mathbb{Q})$ acts as a transformation on the complex upper half plane.

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

$$1 \rightarrow \mathbb{Q}^* \rightarrow GL_2(A^f_\mathbb{Q}) \rightarrow \text{Aut}(\mathcal{F}) \rightarrow 1$$

is exact.

Reference. [5; Theorem 6.23] \hfill \Box

Recall the from (5) the embedding

$$g_\theta : J^f_K \rightarrow \prod_p GL_2(\mathbb{Q}_p)$$

and consider the diagram

$$\begin{align*}
1 & \rightarrow K^* \rightarrow J^f_K \xrightarrow{[\cdot, K]} \text{Gal}(K^{ab}/K) \rightarrow 1 \\
1 & \rightarrow \mathbb{Q}^* \rightarrow GL_2(A^f_\mathbb{Q}) \rightarrow \text{Aut}(\mathcal{F}) \rightarrow 1.
\end{align*}$$

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

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

If $G \subset GL_2(A^f_\mathbb{Q})$ is an open subgroup with fixed field $F \subset \mathcal{F}$, then the subgroup of $J^f_K$ 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] \hfill \Box
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 $a \subset \mathcal{O}$ the formula

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

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

Every primitive reduced quadratic form of discriminant $d$ corresponds uniquely with an ideal class in $\text{Cl}(\mathcal{O})$. 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

$$u : \text{Cl}(\mathcal{O}) \to \text{GL}_2(\mathbb{Z})$$

$$[a, b, c] \mapsto u_\tau$$

such that

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

We begin by producing an idèle $z_\tau \in J_K^\ast$ 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 $(z_p)_p \in \prod' K_p$ 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 $z_r = (z_p)_p \in J^f_K$ the Galois action of the Artin symbol $[z_r, K]$ satisfies
\[ j(\theta)[a, b, c] = j(\theta)[z_r, K]. \]

**Proof.** The inclusion $z_p O_p \subset L_p$ follows from $z_p \notin L$. Note that $L \subset O$ has index $[O : L] = a$. For every $p \in \mathbb{Z}$ we compute
\[ N_{K/Q}(z_p) = \begin{cases} 
    a^2 & \text{if } p \nmid a \\
    ac & \text{if } p \mid a \land p \nmid c \\
    a(a + b + c) & \text{if } p \mid a \land p \mid c,
\end{cases} \]
and since $(a, b, c) = 1$, one obtains $\| N_{K/Q}(z_p) \|_p = \|a\|_p$. From
\[ [O_p : z_p O_p] = \|a\|_p = [O_p : L_p] \]
we conclude $z_p O_p = L_p$. \hfill \Box

Given an imaginary quadratic discriminant $d$, fix
\[ \theta = \begin{cases} 
    \frac{-1 + \sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4 \\
    \frac{\sqrt{d}}{2} & \text{if } d \equiv 0 \mod 4.
\end{cases} \]
and let $[a, b, c]$, and $z = z_r$ be as stated in Lemma 19. For a class invariant $h(\theta)$, the Shimura reciprocity law states
\[ h(\theta)[a, -, b, c] = h(\theta)[z^{-1}, K] = h^{g_0(z)}(\theta). \]

Let $M \in \text{GL}_2^+(\mathbb{Q})$ satisfy $M \cdot \left( \begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \right) = \left( \begin{smallmatrix} a^T \\ a \end{smallmatrix} \right)$. Explicitly, one computes
\[ M = \begin{cases} 
    \left( \begin{array}{cc} 1 & \frac{1-b}{2} \\
    0 & a \end{array} \right) & \text{if } d \equiv 1 \mod 4 \\
    \left( \begin{array}{cc} 1 & \frac{-b}{2} \\
    0 & a \end{array} \right) & \text{if } d \equiv 0 \mod 4.
\end{cases} \]

The action of $\text{GL}_2(A^f_Q)$ via (15) gives
\[ h^{g_0(z)}(\theta) = h^{g_0(z) \cdot M^{-1}}(\tau). \]

Define $u_r = g_0(z) \cdot M^{-1} \in \prod_p' \text{GL}_2(\mathbb{Q}_p)$. Let $u_p \in \text{GL}_2(\mathbb{Q}_p)$ denote the component of $u_r$ at $p$. Then the determinant of
\[ u_p = (g_0)_p(z_p) \cdot M^{-1} \in \text{GL}_2(\mathbb{Q}_p). \]
is given by
\[ \det(u_p) = N_{K/Q}(z_p) \cdot \frac{1}{a} \in \mathbb{Z}_p^*. \]

Writing out \( u_p \) for \( d \equiv 0 \mod 4 \), one obtains

\[
(16) \quad u_p = \begin{cases} 
\left( \begin{array}{cc} a & b \\ 0 & 1 \end{array} \right) & \text{if } p \nmid a \\
\left( \begin{array}{cc} -\frac{b}{2} & -c \\ 1 & 0 \end{array} \right) & \text{if } p \mid a \wedge p \nmid c \\
\left( \begin{array}{cc} -\frac{b}{2} - a & -\frac{b}{2} - c \\ 1 & -1 \end{array} \right) & \text{if } p \mid a \wedge p \mid c.
\end{cases}
\]

On the other hand for \( d \equiv 1 \mod 4 \), we get

\[
(17) \quad u_p = \begin{cases} 
\left( \begin{array}{cc} a & -\frac{b-1}{2} \\ 0 & 1 \end{array} \right) & \text{if } p \nmid a \\
\left( \begin{array}{cc} -\frac{b-1}{2} & -c \\ 1 & 0 \end{array} \right) & \text{if } p \mid a \wedge p \nmid c \\
\left( \begin{array}{cc} -\frac{b-1}{2} - a & 1 -\frac{b}{2} - c \\ 1 & -1 \end{array} \right) & \text{if } p \mid a \wedge p \mid c.
\end{cases}
\]

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

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

\[
\theta = \begin{cases} 
\frac{\sqrt{d}}{2} & \text{if } d \equiv 0 \mod 4 \\
-\frac{1+\sqrt{d}}{2a} & \text{if } d \equiv 1 \mod 4
\end{cases}
\]

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

\[ h(\theta)[a,-b,c] = h^u_r(\tau) \]

for any \( h \in \mathcal{F} \) such that \( h(\theta) \in K(j(\theta)) \). \(\square\)
11. Formulas of Morain and Yui-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 $d \equiv 1 \mod 4$ be an imaginary quadratic discriminant and let $\theta = -1 + \sqrt{d}$. 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 primitive quadratic form of discriminant $d$ and $\tau = -\frac{b + \sqrt{d}}{2a}$.

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

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

satisfies

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

We decompose $M$ in terms of $S$ and $T$ modulo 2

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

Using (9), we calculate

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

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 $(2\tau)$ regarding the conjugates of the class invariant $\zeta_{48}f_2(\theta)$ from [8].
Proposition 22. Suppose $d \equiv 1 \mod 8$ is an imaginary quadratic discriminant such that $d \neq 0 \mod 3$ and 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 $\zeta_{48}f_2(\theta)$ is given by the formula

\begin{equation}
(\zeta_{48}f_2(\theta))^{[a,-b,c]} = \begin{cases}
\zeta_{48}^{b(a-c+ac^2)}f_2(\tau) & \text{if } 2 \nmid a \\
\zeta_{48}^{b(a-c-ac^2)}f_1(\tau) & \text{if } 2 \mid a \wedge 2 \nmid c \\
(-1)^{\frac{a-1}{2}}\zeta_{48}^{b(a-c-ac^2)}f(\tau) & \text{if } 2 \mid a \wedge 2 \mid c.
\end{cases}
\end{equation}

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

\[ \zeta_{48}f_2(\theta)^{[a,-b,c]} = (\zeta_{48}f_2)^M(\tau). \]

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

\[ M_3 \equiv \begin{cases}
(1 \ 0) \cdot ST^{-a}ST^{-a}ST^{-b}a & \text{if } 3 \nmid a \\
(0 \ 1) \cdot T^{(b-1)c}ST^cST^c & \text{if } 3 \mid a \wedge 3 \nmid c \\
(1 \ 0) \cdot T^{-1-b}ST^bST^{-1} & \text{if } 3 \mid a \wedge 3 \mid c
\end{cases} \]

and

\[ M_{16} \equiv \begin{cases}
(1 \ 0) \cdot ST^{-\frac{a}{2}}ST^{-\frac{a}{2}}ST^{\frac{b-c}{2}} & \text{if } 2 \nmid a \\
(0 \ 1) \cdot T^{(\frac{a+b}{2})c}ST^cST^c & \text{if } 2 \mid a \wedge 2 \nmid c \\
(1 \ a+b+c) \cdot T^{(\frac{1-b-2a}{2})c(a+b+c)}ST^{-a+b+c}ST^{a+b+c} & \text{if } 2 \mid a \wedge 2 \mid c
\end{cases} \]

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

\[ (\zeta_{48}f_2)^M = (\zeta_{16}^{-5}(\zeta_3f_2) \cdot M_3) \cdot M_{16} \]

gives the action of $M$ on on $\zeta_{48}f_2$. First we compute $\zeta_3f_2 \cdot M_3 = \mu_3f_2$ using (14). Here, $\mu_3$ is the third root of unity

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

In a similar fashion, we find

\[ (\zeta_{16}^{-5}f_2) \cdot M_{16} = \begin{cases}
\mu_1f_2 & \text{if } 2 \nmid a \\
\mu_1f_1 & \text{if } 2 \mid c \\
\mu_1f & \text{if } 2 \mid a \wedge 2 \mid c.
\end{cases} \]
where \( \mu_{16} \in \mathbb{Q}(\zeta_{16}) \) is

\[
\mu_{16} = \begin{cases} 
\zeta_{16}^{-5ab} & \text{if } 2 \nmid a \\
\zeta_{16}^{5bc} & \text{if } 2 \mid a \land 2 \nmid c \\
\zeta_{16}^{5(a+b+c)(b+2a)-5} & \text{if } 2 \mid a \land 2 \mid c .
\end{cases}
\]

The expressions (20) for \( \mu_{16} \) have been simplified using the condition \( d \equiv 1 \mod 8 \).

We conclude

\[
(\zeta_{48}^3)^M = \begin{cases} 
\mu_3 \cdot \mu_{16} \cdot f_2 & \text{if } 2 \mid a \\
\mu_3 \cdot \mu_{16} \cdot f_1 & \text{if } 2 \mid a \land 2 \nmid c \\
\mu_3 \cdot \mu_{16} \cdot f & \text{if } 2 \mid a \land 2 \mid c .
\end{cases}
\]

We need to check that the formulas in (19) and (21) coincide in the case \( 3 \mid d \) and \( d \equiv 1 \mod 8 \). The condition \( d \not\equiv 0 \mod 3 \) implies

\[
b \equiv 0 \text{ or } ac \not\equiv 1 \mod 3
\]

\[
\Rightarrow b(a - c + a^2 c) \equiv b(a - c - ac^2) \mod 3
\]

and we easily check

\[
\zeta_3^{b(a-c+a^2 c)} = \begin{cases} 
\zeta_3^a & \text{if } 3 \nmid a \\
\zeta_3^{-bc} & \text{if } 3 \mid a \land 3 \nmid c \\
1 & \text{if } 3 \mid a \land 3 \mid c .
\end{cases}
\]

Similarly, under the restriction \( d \equiv 1 \mod 8 \), one verifies that

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

holds.

\[\square\]

REFERENCES

4. R. Schertz, *Die singulären Werte der Weberschen Funktionen \( f, f_1, f_2, \gamma_2, \gamma_3 \)*, J. Reine Angew. Math. 286/287 (1976), 46–74.

Reçu le 1 novembre, 1997
GENERATING CLASS FIELDS
USING SHIMURA RECIPROCITY

ALICE GEE AND PETER STEVENHAGEN

ABSTRACT. The abelian extensions of an imaginary quadratic field can theoretically be generated by the values of the modular j-function, but these values are too large to be useful in practice. We show how Shimura's reciprocity law can be applied to find small generators for these extensions, and to compute the corresponding irreducible polynomials.

1. INTRODUCTION

Among the finite extensions of a number field, the abelian extensions play a special role. Over the rational number field \( \mathbb{Q} \), the Kronecker-Weber theorem states that the abelian fields are the subfields of the cyclotomic fields \( \mathbb{Q}(\zeta) \) obtained by adjoining a root of unity \( \zeta \in \mathbb{C} \) to \( \mathbb{Q} \). If \( \zeta \) is of order \( N \), the corresponding irreducible polynomial is the \( N \)-th cyclotomic polynomial \( \Phi_N \). It is easy to compute \( \Phi_N \) for small \( N \), and for such \( N \) the coefficients of \( \Phi_N \) are very small. By Galois theory, essentially the theory of cyclotomic periods developed by Gauss, we can descend and find explicit generators for subfields of \( \mathbb{Q}(\zeta) \).

The arithmetic theory of abelian fields is much nicer than that of arbitrary number fields. They come with explicit groups of cyclotomic units, which can be exploited to find their class groups in situations where general class group algorithms currently have no hope of succeeding [10].

Over an arbitrary number field \( K \), the abelian extensions \( K \subset L \) are described by class field theory. For such \( L \), the Galois group \( \text{Gal}(L/K) \) is canonically isomorphic to a quotient \( J_K/(K^*N_{L/K}J_L) \) of the idèle group \( J_K \) of \( K \) by the open subgroup generated by \( K^* \) and the norm image \( N_{L/K}J_L \) of the idèle group of \( L \). Conversely, every open subgroup \( B \subset J_K \) containing \( K^* \) corresponds in this way to a unique abelian extension of \( K \), the class field of \( B \). The explicit determination of class fields is one of the main tasks of computational class field theory, an algorithmic area that has only recently come to enjoy popularity.

1991 Mathematics Subject Classification. Primary 11G15; Secondary 11R37, 11Y40.

Key words and phrases. Hilbert class field, complex multiplication, Shimura reciprocity law.

Typeset by \textsc{AMS-TeX}
The idèle group $J_K$ is a large object that is not always convenient for explicit computations. It is however possible to describe the finite quotients of $J_K/K^*$ corresponding to abelian extensions of $K$ in a different way, as quotients of the ray class groups $C_n$ of $K$. These are finite abelian groups depending on a conductor $n$, and they play a role that is analogous to that of the Galois groups $(\mathbb{Z}/n\mathbb{Z})^*$ in the case of the cyclotomic extensions $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$. A special role is played by the ray class field corresponding to the trivial conductor $n = 1$: this is the Hilbert class field $H$ of $K$. The Galois group $\text{Gal}(H/K)$ is canonically isomorphic to the class group $C$ of $K$, and for this reason it is one of the most important extension fields of $K$.

Just as in the case $K = \mathbb{Q}$, the explicit determination of abelian extensions of $K$ reduces to the problem of generating the ray class fields $H_n$ corresponding to the ray class group $C_n$, at least if we measure the size of an abelian extension by its conductor. By generating $H_n$ we mean computing a polynomial $h \in K[X]$ for which we have $H_n \cong K[X]/(h)$.

Even though class field theory proves the existence of class fields in a constructive way, it does not readily provide an algorithm to compute generators for class fields, not even for the Hilbert class field. The theory indicates that these extensions can in principle be generated over large extensions of $K$. Algorithmically it is often not feasible to do computations over these large number fields, and this is a serious obstruction.

The only class of fields $K$ different from $\mathbb{Q}$ for which there exists a theory that yields generators of class fields is the class of imaginary quadratic fields, and it is this class that we will address in the current paper.

The theory of complex multiplication asserts that the ray class fields over an imaginary quadratic field $K$ can be generated by the values of suitable modular functions. These modular functions can be viewed as elliptic analogues of the exponential function $q(z) = \exp(2\pi i z)$, whose values $\zeta^m_n$ at the rational points $z = m/n \in \mathbb{Q}$ generate the class fields of $\mathbb{Q}$. A basic example of the theorems from complex multiplication is the following.

**Theorem 1.** Let $K$ be imaginary quadratic with ring of integers $\mathcal{O} = \mathbb{Z}[\theta]$. Then the Hilbert class field $H$ of $K$ is generated by the value $j(\theta)$ of the modular function $j$.

The modular function $j : \mathbb{H} \to \mathbb{C}$ is a complex valued function on the complex upper half plane $\mathbb{H}$ that occurs in many contexts. As a function on lattices $\Lambda = [\omega_1, \omega_2] \in \mathbb{C}$, the value $j(\Lambda) = j(\omega_1/\omega_2)$ is the $j$-invariant of the complex elliptic curve $E = \mathbb{C}/\Lambda$.

The conjugates of $j(\theta) = j(\mathcal{O})$ over either $K$ or $\mathbb{Q}$ are the values $j(a)$ for $[a]$
ranging over the ideal classes in $\mathcal{C}(\mathcal{O})$. These values are algebraic integers, so the class polynomial $F_\mathcal{O} = \prod_{[\mathfrak{a}] \in \mathcal{C}(\mathcal{O})} (X - j(\mathfrak{a})) \in \mathbb{Z}[X]$ can be computed using complex approximations of the values $j(\mathfrak{a})$. As it is relatively easy to approximate these values, this method is to be preferred over the computationally unfeasible algebraic computation of $F_\mathcal{O}$ as a factor of some modular polynomial $\Phi_m(X, X)$ that is explained in [2].

Numerical examples show that the polynomial $F_\mathcal{O}$ is already huge for small values of the discriminant of $K$. For the field of discriminant $-71$, which has class number 7, the class polynomial equals

$$F_\mathcal{O} = X^7 + 313645809715 X^6 - 3091990138604570 X^5$$
$$+ 98394038810047812049302 X^4 - 823534263439730779968091389 X^3$$
$$+ 5138800366453976780323726329446 X^2$$
$$- 425319473946139603274605151187659 X$$
$$+ 737707086760731113357714241006081263,$$

and the situation rapidly gets worse. Weber discovered that in many cases, one can generate $H$ using functions that are considerably smaller than the $j$-function. For the example above, there exists a modular function $f$ of level 48 that gives rise to a class invariant $f(\theta)$ with irreducible polynomial

$$X^7 + X^6 - X^5 - X^4 - X^3 + X^2 + 2X + 1.$$

The observations on such ‘lucky occurrences’ in [11] range from theorems and numerical observations to open questions, and the distinction between them is not always clear. Following the confusion around Heegner’s purported proof of the class number one problem for imaginary quadratic orders, some of the obscure points were clarified by Birch [1] and Stark [9] in 1969. The revival of interest in modular forms in the seventies, and more in particular the contributions to the subject by Shimura [7, 8] have resulted in the development of abstract tools that are ideally suited to deal with the questions raised by Heegner.

The aim of this paper is to show that Shimura’s techniques can be applied to answer the following basic questions:

1. given a modular function $f$, determine for which $K$ the value $f(\theta)$ at a generator $\theta$ of $\mathcal{O}_K$ generates the Hilbert class field $H$ of $K$;
2. if $f(\theta)$ generates $H$, compute its irreducible polynomial.

In fact the techniques can be used to identify the field $K(f(\theta))$ in all cases, or to generate other class fields than the Hilbert class field. Even if $f(\theta)$ is not a class
invariant, the information obtained is usually sufficient to produce a generator of $H$ from $f(\theta)$. As we will see (theorem 3), a modular function $f$ that yields a class invariant for some imaginary quadratic field $K$ does so for a positive proportion of all imaginary quadratic fields.

From a complexity point of view, the improvement in using ‘small’ modular functions is not dramatic: as we are still working with exponential functions, the size of the coefficients of the generating polynomials for the Hilbert class field grows exponentially with the discriminant of $K$. This seems to be an unavoidable consequence of the theory of complex multiplication. On the other hand, the improvement by a constant factor (like 72 or 48) in the size of the coefficients enables us to produce decent generating polynomials when the discriminant of $K$ is of moderate size. The modular function $j$ does not have this property and is therefore never useful in computational practice.

2. MODULAR FUNCTIONS

Before we can start our investigations on class invariants, we provide concise definitions of the modular functions that we use and indicate some ‘small’ modular functions of not too high level that can be used to produce class invariants. Proofs of all statements in this section can be found in [4].

The basic example of a modular function is the $j$-function encountered in the introduction. This is a holomorphic function on $H$ that respects the action of the elements of the modular group $\Gamma = \text{SL}_2(\mathbb{Z})$ on $H$. By this we mean that we have $j\left(\frac{a\tau + b}{d\tau + c}\right) = j(\tau)$ for $\tau \in H$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Note that the action of $\Gamma$ on $H$ factors via the quotient $\Gamma/\pm 1$. The $j$-function has simple pole at infinity and extends to an isomorphism of Riemann surfaces $j : (\Gamma \setminus H)^- \rightarrow \mathbb{P}^1(\mathbb{C})$ between the compactified orbit space and the complex projective line. The elements of the corresponding function field $\mathbb{C}(j)$ of rational functions in $j$ are called modular functions of level 1.

One obtains modular functions of arbitrary level $N \geq 1$ by replacing the modular group $\Gamma$ in the setting above by the congruence subgroup $\Gamma(N) = \ker[\text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/N\mathbb{Z})]$. The compactified Riemann surface $(\Gamma(N) \setminus H)^-$ is then isomorphic to the modular curve $X(N)$ of level $N$ over $\mathbb{C}$. The natural map $X(N) \rightarrow X(1)$ is a Galois covering with group $\Gamma/(\pm 1 \cdot \Gamma(N)) = \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$. This implies that the function field $F_{N,C}$ of $X(N)$, whose elements are the modular functions of level $N$, is a Galois extension of $F_{1,C} = \mathbb{C}(j)$ with group $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$. Thus the modular functions of level $N$ are simply the $\Gamma(N)$-invariant meromorphic functions on $H$ that are also ‘meromorphic at infinity’. Note that such functions are invariant under $z \mapsto z + N$, hence periodic.
As we want our modular functions to have algebraic values, we need to define our function field $F_{N,C}$ over a smaller base field than $\mathbb{C}$. For $N = 1$, the modular curve $X(1) = \mathbb{P}^1(\mathbb{C})$ can clearly be defined over $\mathbb{Q}$, with function field $F_1 = \mathbb{Q}(j)$. In the general case one needs to pass to the cyclotomic base field $\mathbb{Q}(\zeta_N)$. This means that there exists a Galois extension $F_N$ of $\mathbb{Q}(\zeta_N,j)$ with group $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$ that yields $F_{N,C}$ after base change from $\mathbb{Q}(\zeta_N)$ to $\mathbb{C}$. More precisely, we can write the elements of $F_{N,C}$ as Laurent series in $q^{1/n}$ with $q = \exp(2\pi i z)$, and then $F_N$ is the subfield of $F_{N,C} \subset \mathbb{C}((q^{1/N}))$ consisting of the functions with Fourier coefficients in $\mathbb{Q}(\zeta_N)$. The action of the cyclotomic Galois group $(\mathbb{Z}/N\mathbb{Z})^* = \text{Gal}(\mathbb{Q}(\zeta_N,j)/\mathbb{Q}(j))$ has a natural extension to $F_N \subset \mathbb{Q}(\zeta_N)((q^{1/N}))$, and this leads to a description of $\text{Gal}(F_N/F_1) = \text{Gal}(F_N/\mathbb{Q}(j))$ as a semidirect product

$$(\text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1) \rtimes (\mathbb{Z}/N\mathbb{Z})^* \cong \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1.$$ 

Here $(\mathbb{Z}/N\mathbb{Z})^*$ is embedded in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$ as the subgroup of elements of the form $\left( \begin{array}{cc} 1 & 0 \\ 0 & \alpha \end{array} \right) \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. For the full modular function field $F_\infty = \bigcup_{N \geq 1} F_N$ one obtains the Galois group over $\mathbb{Q}(j)$ by passing to the projective limit:

$$\text{Gal}(F_\infty/\mathbb{Q}(j)) = \lim_{\leftarrow N} (\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1) = \text{GL}_2(\mathbb{Z})/\pm 1.$$ 

The main theorem of complex multiplication is the following generalization of the theorem stated in the introduction.

**Theorem 2.** Let $K$ be imaginary quadratic with ring of integers $\mathcal{O} = \mathbb{Z}[\theta]$ and $N \geq 1$ an integer. Then the ray class field $H_N$ of conductor $N$ of $K$ is generated over $K$ by the values $f(\theta)$ of the functions $f \in F_N$ that do not have a pole at $\theta$.

It follows that the maximal abelian extension $K^{ab}$ of $K$ is generated by the finite function values $f(\theta)$ for $f \in F_\infty$.

Our example for discriminant $-71$ in the introduction illustrates the fact that the $j$-function is already large for values of $\theta$ with small imaginary part. There are however modular functions of higher level that are ‘smaller’ than the $j$-function. As we are working with functions that are integral over $\mathbb{Z}[j]$, this simply means that the coefficients occurring in the $q$-expansion of $f$ are smaller than those we encounter for $j$. We mention a couple of possibilities for $f$, leaving a fuller treatment to chapter 4.

The oldest examples of modular functions yielding class invariants are obtained by modification of the $j$-function itself. One has representations

$$j = \frac{(12g_2)^3}{\Delta} = 1728 + \frac{(216g_3)^2}{\Delta}$$

where $g_2$ and $g_3$ are discriminants.
of \( j \) in terms of the normalized Eisenstein series \( g_2 \) and \( g_3 \) and the discriminant function \( \Delta \). It follows that there exist holomorphic branches \( \gamma_2 \) of the cube root of \( j \) and \( \gamma_3 \) of the square root of \( j - 1728 \) on \( \mathbb{H} \), both with rational \( q \) expansions. The modular group \( \Gamma \) acts on these functions via characters of order 3 and 2, respectively. In terms of the standard generators \( S = (0 \ 1) \) and \( T = (1 \ -1) \) of \( \Gamma/\pm 1 \) we have

\[
(\gamma_2, \gamma_3) \xrightarrow{S} (\gamma_2, -\gamma_3) \quad \text{and} \quad (\gamma_2, \gamma_3) \xrightarrow{T} (\zeta_3^{-1}\gamma_2, -\gamma_3).
\]

One deduces that we have \( \gamma_2 \in F_3 \) and \( \gamma_3 \in F_2 \).

Much smaller functions can be obtained form the fact that the discriminant function \( \Delta \) equals \((2\pi)^{12}\eta^{24}\), with \( \eta \) the Dedekind \( \eta \)-function. This is a holomorphic function on \( \mathbb{H} \) with rational \( q \)-expansion \( \eta(q) = q^{1/24}\prod_{n>0}(1-q^n) \), and its transformation behavior under \( \Gamma \) is given by a simple formula [4, 18, §5].

The discriminant function is a modular form of weight 12, not a modular function. One can obtain modular functions by forming suitable quotients of modular forms of the same weight, see [4, 11, §2]. A good example is the modular function \( \Delta(2z)/\Delta(z) \) of level 2, which has a holomorphic 24-th root \( \eta(2z)/\eta(z) \) on \( \mathbb{H} \). The function \( f_2 = \sqrt{2} \cdot \eta(2z)/\eta(z) \), which is integral over \( \mathbb{Z}[j] \), has been studied by Weber, who introduced related modular functions \( f \) and \( f_1 \) with rational \( q \)-expansions satisfying

\[
(X + f^6)(X - f_1^6)(X - f_2^6) = X^3 - \gamma_2X + 16.
\]

These functions \( f, f_1 \) and \( f_2 \) are in \( F_{48} \), and they are much smaller than \( j \). Each of them generates an extension of degree 72 of the field \( F_1 = \mathbb{Q}(j) \), and the action of \( S \) and \( T \) is given by

\[
(f, f_1, f_2) \xrightarrow{S} (f, f_2, f_1) \quad \text{and} \quad (f, f_1, f_2) \xrightarrow{T} (\zeta_{48}^{-1}f_1, \zeta_{48}^{-1}f, \zeta_{48}^2f_2).
\]

The miraculous fact that \( \zeta_{48}f_2(1+\sqrt{-71}) \) lies in the Hilbert class field of \( \mathbb{Q}(\sqrt{-71}) \) accounts for the existence of the small polynomial given in the introduction. There are other modular functions than those introduced by Weber that yield small generators as well. Schertz constructs small generators from quotients of \( \eta \)-functions in [6]. In a similar vein, one can generalize Weber's classical functions of level 48 by considering the holomorphic 24-th root \( \sqrt{n} \cdot \eta(nx)/\eta(z) \) of \( n^{12}\Delta(bz)/\Delta(z) \) for any integer \( n > 1 \). For \( n = 2 \) this is Weber's function \( f_2 \), for \( n = 3 \) we obtain a function \( g_3 = \sqrt{3} \cdot \eta(3z)/\eta(z) \in F_{72} \) of degree 48 over \( \mathbb{Q}(j) \) that satisfies an analogue

\[
(X + g_6^6)(X - g_1^6)(X - g_2^6)(X - g_3^6) = X^4 + 18X^2 + \gamma_3X - 27.
\]
GENERATING CLASS FIELDS USING SHIMURA RECIPROCITY

of the identity for $f_2$ above. The relation $gg_1g_2g_3 = \sqrt{3}$ is analogous to Weber's identity $ff_1f_2 = \sqrt{2}$. It shows that, unlike the case of the modular function $j$, the values of these functions at singular moduli are 'almost' algebraic units.

3. FINDING CLASS INVARIANTS

As in the previous sections, we let $K$ be an imaginary quadratic field with ring of integers $O = \mathbb{Z}[\theta]$. For uniqueness' sake, we normalize $\theta$ such that we have $\text{Tr}_{K/\mathbb{Q}}(\theta) \in \{-1, 0\}$.

We formulate the problem of finding class invariants as follows: given some modular function $f \in F_N$, determine for which $K$ the value $f(\theta)$ lies in the Hilbert class field $H$ of $K$.

By the complex multiplication theorem from section 2, we know that $f(\theta)$ is an element of $K^{ab}$, and even of the ray class field of conductor $N$ of $K$. In order to prove that $f(\theta)$ actually lies in $H$, it suffices to show that all automorphisms in $\text{Gal}(K^{ab}/H)$ act trivially on $f(\theta)$. The group $\text{Gal}(K^{ab}/H)$ can be described by class field theory. The main theorem of class field theory for imaginary quadratic fields can be phrased as a single exact sequence

$$1 \rightarrow K^* \rightarrow \hat{K}^* \xrightarrow{A} \text{Gal}(K^{ab}/K) \rightarrow 1.$$

Here $A$ denotes the Artin map on the finite idèle group $\hat{K}^* = (K \otimes \mathbb{Z})^*$ of $K$. Note that $\hat{K} = \prod_p (K \otimes \mathbb{Q} \mathbb{Q}_p)$ is the ring of finite adèles of $K$, and that $\hat{K}^*$ is the factor group of $J_K$ obtained by dividing out the component group corresponding to the infinite prime of $K$, which is also the connected component of the identity in $J_K$. Inside $\hat{K}$ we have the profinite completion $\hat{O} = O \otimes \mathbb{Z} \hat{\mathbb{Z}} = \lim_{\leftarrow \infty} (O/nO)$ of the ring of integers $O$ of $K$. The subgroup $\hat{O}^* = \prod_p (O \otimes \mathbb{Z} \mathbb{Q}_p)^*$ of $\hat{K}^*$ is the inverse image under the Artin map of $\text{Gal}(K^{ab}/H)$, and we need to check whether the natural action of $\hat{O}^*$ on $f(\theta)$ induced by $A$ is trivial. The Shimura reciprocity law says that the image of $f(\theta)$ under $x \in \hat{O}^*$ can be obtained as the value in $\theta$ of a modular function that is conjugate to $f$ over $\mathbb{Q}(j)$. More precisely, there is a map $g = g_{\theta}$ connecting the exact rows

$$1 \rightarrow O^* \rightarrow \hat{O}^* \xrightarrow{A} \text{Gal}(K^{ab}/H) \rightarrow 1$$

(1)

$$1 \rightarrow \{\pm 1\} \rightarrow \text{GL}_2(\hat{\mathbb{Z}}) \rightarrow \text{Gal}(F_\infty/F_1) \rightarrow 1.$$

such that we have Shimura's reciprocity relation

$$ (f(\theta))^x = (f^{(x^{-1})})(\theta)$$

(2)
and the fundamental equivalence

$$(f(\theta))^z = f(\theta) \iff f^{g(x)} = f$$

provided that $\mathbb{Q}(f) \subset F_\infty$ is Galois. Note that only the implication $\leftarrow$ is immediate from the reciprocity relation, the implication $\Rightarrow$ requires the hypothesis and an additional argument [7, prop. 6.33].

With the exponent $-1$ in the reciprocity relation (2), the definition of the connecting homomorphism $g$ is the following: $g(\theta) \in \text{GL}_2(\hat{\mathbb{Z}})$ is the transpose of the matrix describing the multiplication by $x \in \hat{\mathcal{O}}^*$ on the free $\hat{\mathbb{Z}}$-module $\hat{\mathcal{O}} = \hat{\mathbb{Z}} \cdot \theta + \hat{\mathbb{Z}}$ with respect to the basis $[\theta, 1]$. Explicitly, if $\theta$ has irreducible polynomial $X^2 + BX + C$, then we have

$$g_\theta : x = s\theta + t \mapsto \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix}$$

If $f \in F_N$ is a modular function of level $N$, the value $f(\theta)$ lies in the ray class field and the action of $\hat{\mathcal{O}}^*$ can be computed via the finite quotient $(\mathcal{O}/N\mathcal{O})^*$. Diagram (1) may then be reduced to a diagram of finite abelian groups

$$\begin{align*}
\mathcal{O}^* &\rightarrow (\mathcal{O}/N\mathcal{O})^* &\rightarrow &\text{Gal}(H_N/H) &\rightarrow &1 \\
\{\pm 1\} &\rightarrow &\text{GL}_2(\mathbb{Z}/N\mathbb{Z}) &\rightarrow &\text{Gal}(F_N/F_1) &\rightarrow &1.
\end{align*}$$

In order to prove that $f(\theta)$ lies in $H$, we compute generators $x_1, x_2, \ldots, x_k$ of the group $(\mathcal{O}/N\mathcal{O})^*$, map them to $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ using the reduction $\bar{g}$ of $g$ modulo $N$ and check that each of the matrices $g(x_i) \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts trivially on $f$. This is relatively straightforward if we know the action of the standard generators $S, T \in \Gamma$ and of the Galois group $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^*$ on $f$. We refer to section 1.5 for some explicit examples.

If we replace the base field $K$ in diagram (4) by another quadratic field whose discriminant is in the same residue class modulo $4N$, the integers $B$ and $C$ occurring in (3) coincide modulo $N$ and the image of $\bar{g} : (\mathcal{O}/N\mathcal{O})^* \rightarrow \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is the same for both fields. We get the following result.

**Theorem 3.** Let $K$ be imaginary quadratic with ring of integers $\mathbb{Z}[\theta]$, and $f \in F_N$ a modular function with the property that $f(\theta)$ lies in the Hilbert class field of $K$. Then the same statement holds for all for all imaginary quadratic fields whose discriminant is congruent to $\text{disc}(K)$ modulo $4N$. 
4. Computing class polynomials

Suppose that we have found a modular function \( f \) for which \( f(\theta) \) lies in the Hilbert class field \( H \) of \( K \). In order to find its irreducible polynomial over \( K \), we need to determine the conjugates of \( f(\theta) \) over \( K \). This means that we have to compute the action of the class group \( C(\mathcal{O}) = \text{Gal}(H/K) \) on \( f(\theta) \).

For any imaginary quadratic order \( \mathcal{O} \) of discriminant \( D \), we can list the elements of \( C(\mathcal{O}) \) as reduced primitive binary quadratic forms \([a, b, c]\) of discriminant \( D \). For our purposes, it suffices to know that these are triples \([a, b, c]\) of integers satisfying \( \gcd(a, b, c) = 1 \) and \( b^2 - 4ac = D \). They are reduced if they satisfy \( |b| \leq a \leq c \) and, in case we have \( |b| = a \) or \( a = c \), also \( b \geq 0 \). For given discriminant \( D < 0 \), there are only finitely many such triples, and they are easily enumerated if \( D \) is not too large. The correspondence between reduced forms and elements of the class group is obtained by associating to \([a, b, c]\) the class of the ideal with \( \mathbb{Z}\)-basis \([-b+\sqrt{D}/2a, a] \). Note that \([a, b, c]\) and \([a, -b, c]\) correspond to inverse ideal classes. In terms of quadratic forms, the action of the class group of \( \mathcal{O} = \mathbb{Z}[\theta] \) on the value \( j(\theta) \) of the \( j \)-function is given by

\[
j(\theta)[a, -b, c] = j(-b+\sqrt{D}/2a).
\]

For a general modular function \( f \) with \( f(\theta) \in H \), Shimura reciprocity enables us to determine the conjugate \( \tilde{f} \) of \( f \) over \( \mathbb{Q}(j) \) for which we have

\[
(5) \quad f(\theta)[a, -b, c] = \tilde{f}(-b+\sqrt{D}/2a).
\]

For this one needs a more general form of the law, which gives us the analogue of (1) for the action of the full group \( \tilde{K}^* = (\tilde{\mathcal{O}} \otimes \mathbb{Z} \mathbb{Q})^* \) on the values \( f(\theta) \). For this we need to replace \( \text{Gal}(F_{\infty}/F_1) \) in (1) by the full automorphism group \( \text{Aut}(F_{\infty}) \), which is generated by the automorphisms coming from \( \text{GL}_2(\hat{\mathbb{Z}}) \) and those coming from the group \( \text{GL}_2(\mathbb{Q})^+ \) of rational \( 2 \times 2 \)-matrices of positive determinant. The right action of \( \text{GL}_2(\mathbb{Q})^+ \) on \( F_{\infty} \) comes, just like in the case of \( \Gamma = \text{SL}_2(\mathbb{Z}) \), from the natural action of \( \text{GL}_2(\mathbb{Q})^+ \) on \( \mathbb{H} \) via fractional linear transformations:

\[
f^\alpha = f \circ \alpha.
\]

The groups \( \text{GL}_2(\hat{\mathbb{Z}}) = \prod_p \text{GL}_2(\mathbb{Z}_p) \) and \( \text{GL}_2(\mathbb{Q})^+ \) are subgroups of the group \( \text{GL}_2(\hat{\mathbb{Q}}) = \prod' \text{GL}_2(\mathbb{Q}_p) \) of invertible \( 2 \times 2 \)-matrices over the finite adèl e ring \( \hat{\mathbb{Q}} = \mathbb{Q} \otimes \mathbb{Z} \hat{\mathbb{Z}} \) of \( \mathbb{Q} \). They have intersection \( \Gamma = \text{SL}_2(\mathbb{Z}) \), and every element of \( \text{GL}_2(\hat{\mathbb{Q}}) \) can be written in a non-unique way as \( u \cdot \alpha \) with \( u \in \text{GL}_2(\hat{\mathbb{Z}}) \) and \( \alpha \in \text{GL}_2(\mathbb{Q})^+ \). One proves that this induces an action of \( \text{GL}_2(\hat{\mathbb{Q}}) \) on \( F_{\infty} \) given by \( f^{u\alpha} (f^u)^\alpha \). We can now enlarge diagram (1) to

\[
\begin{array}{cccccc}
1 & \rightarrow & K^* & \rightarrow & \tilde{K}^* & \rightarrow \text{Gal}(K^{ab}/K) & \rightarrow & 1 \\
& & \downarrow g_\theta & & & & \\
1 & \rightarrow & \mathbb{Q}^* & \rightarrow & \text{GL}(\hat{\mathbb{Q}}) & \rightarrow & \text{Aut}(F_{\infty}) & \rightarrow & 1.
\end{array}
\]
and with this diagram the reciprocity relation (2) holds unchanged. Here \( g = g_\theta \) is the natural \( \mathbb{Q} \)-linear extension of the map defined in (3).

For every ideal \( \mathfrak{a} \) of \( \mathcal{O} \), we can find an idèle \( x = (x_p)_p \in \hat{K}^* \) that locally generates \( \mathfrak{a} \) at \( p \) for all rational primes \( p \). This means that we have

\[
a \otimes_{\mathbb{Z}} \mathbb{Z}_p = x_p(\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)
\]

for all \( p \). For the ideal with \( \mathbb{Z} \)-basis \( \left[ \frac{-b+\sqrt{D}}{2}, a \right] \) corresponding to \( [a, b, c] \), we can take \( x = (x_p)_p \) with

\[
x_p = \begin{cases} 
a & \text{if } p \nmid a \\
\frac{-b+\sqrt{D}}{2} & \text{if } p \mid a \text{ and } p \nmid c \\
\frac{-b+\sqrt{D}}{2} - a & \text{if } p \mid a \text{ and } p \mid c.
\end{cases}
\]

This idèle maps to \( [a] \in \mathcal{C}(\mathcal{O}) \) under the Artin map, so we have \( f(\theta)^{[a, b, c]} = f \) for this \( x \). Applying the reciprocity relation (3) for \( x^{-1} \), we find \( f(\theta)^{[a, -b, c]} = (f^g(x))(\theta) \). Let \( M \in \text{GL}_2(\mathbb{Q})^+ \) describe with respect to the basis \([\theta, 1]\) the \( \mathbb{Q} \)-linear map \( K \to K \) that maps \([\theta, 1]\) to \([\frac{-b+\sqrt{D}}{2}, a]\). Then \( M \) acts on \( \mathbb{H} \) by \( M(\theta) = \frac{-b+\sqrt{D}}{2a} \), and we obtain

\[
f(\theta)^{[a, -b, c]} = f^g(x) \cdot M^{-1} \left( \frac{-b+\sqrt{D}}{2a} \right).
\]

A straightforward check shows that \( u_x = g(x) \cdot M^{-1} \) is in \( \text{GL}_2(\hat{\mathbb{Z}}) \), so \( \tilde{f} = f^g(x) \cdot M^{-1} \) is a conjugate of \( f \) over \( \mathbb{Q}(j) \), and (7) is the explicit form of (5). Computing the function \( \tilde{f} \) from \( f \) is another instance of the problem solved in the previous section. Clearly, we only need to compute \( u_x \) modulo the level \( N \) of \( f \). If \( p^k \) is the largest power the prime \( p \) dividing \( N \), we find that we have

\[
u_x \equiv \begin{cases} 
\left( \begin{array}{cc} a & \frac{b}{2} \\
1 & 0 \end{array} \right) \mod p^k & \text{if } p \nmid a \\
\left( \begin{array}{cc} -b/2 & -1 \\
1 & 0 \end{array} \right) \mod p^k & \text{if } p \mid a \text{ and } p \nmid c \\
\left( \begin{array}{cc} -b/2-a & -b/2-c \\
1 & -1 \end{array} \right) \mod p^k & \text{if } p \mid a \text{ and } p \mid c.
\end{cases}
\]

in the case that \( D \) is even. For odd discriminants there is a similar formula.

5. NUMERICAL EXAMPLES

We apply the methods explained in this paper to find small generators for a few imaginary quadratic fields \( K \). For each of these fields, the class polynomial obtained by a straightforward application of theorem 1 is huge.
Example 1. Let $D = -71$ be the prime discriminant occurring in the introduction. Then 2 and 3 do not divide $D$, and it was already known to Weber that in this situation, the functions $\gamma_2$ and $\gamma_3$ yield class invariants when evaluated at appropriate values in $\mathcal{O} = \mathbb{Z}[\theta]$, where $\theta = \frac{-1 + \sqrt{-71}}{2}$ has irreducible polynomial $X^2 + X + 18$.

In order to check this for $\gamma_2$, which has level 3, one notes first that 3 splits in $K$, so $(\mathcal{O}/3\mathcal{O})^*/\mathcal{O}^*$ is a cyclic group of order 2 generated by $\theta - 1$. The action of the matrix $g_3(\theta - 1) = (1 \ 0)
\in \text{GL}(\mathbb{Z}/3\mathbb{Z})$ is given by $\zeta_3 \mapsto \zeta_3^2$ and $\gamma_2 \mapsto \zeta_3^2 \gamma_2$, so it leaves $\alpha = \zeta_3 \gamma_2(\theta)$ invariant. In order to find the irreducible polynomial of $\alpha$, we list the 7 reduced quadratic forms of discriminant $-71$ and for each form the matrix $u \in \text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ corresponding to it by (8). From the complex approximations of the conjugates of $\alpha$ we find a polynomial

$$f_K^\theta = X^7 + 6745 \ X^6 - 327467 \ X^5 + 51857115 \ X^4 + 2319299751 \ X^3 + 41264582513 \ X^2 - 307873876442 \ X + 903568991567$$

that is somewhat smaller than the class polynomial listed in the introduction.

In order to discover the small class invariant arising from the Weber function $f_2 \in F_{48}$, we need to compute the action of the generators of $(\mathcal{O}/48\mathcal{O})^*/\mathcal{O}^*$ on $f_2(\theta)$. As 2 is also split in $K$, this is an abelian 2-group of type $(2) \times (2) \times (2) \times (4) \times (4)$. One can take $\{17, 16\theta + 17, 6\theta + 19, 19, 36\theta + 1\}$ as a set of generators. Applying $g_\theta$, one sees that the first generator acts trivially on $\mathbb{Q}(\zeta_{48}, f_2)$.

Table 1. Action of $(\mathcal{O}/48\mathcal{O})^*$ on $\mathbb{Q}(\zeta_{48}, f_2)$ for $\theta = \frac{-1 + \sqrt{-71}}{2}$

<table>
<thead>
<tr>
<th>$\sigma$</th>
<th>$\zeta_{48}^2$-1</th>
<th>$f_2^\theta$-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$16\theta + 17$</td>
<td>$\zeta_3^2$</td>
<td></td>
</tr>
<tr>
<td>$6\theta + 19$</td>
<td>$\zeta_8^5$</td>
<td>$\zeta_8^3$</td>
</tr>
<tr>
<td>19</td>
<td>$-1$</td>
<td>$-1$</td>
</tr>
<tr>
<td>$36\theta + 1$</td>
<td>$\zeta_4$</td>
<td>$\zeta_4$</td>
</tr>
</tbody>
</table>

Table 1 gives the action of the $g_\theta$-image, $\sigma$, for the remaining generators of $(\mathcal{O}/48\mathcal{O})^*$. It follows that $\zeta_{48}f_2(\theta)$ is left invariant. Its conjugates over $K$ are computed as before, and we find the small polynomial from the introduction

$$f_{K\zeta_{48}f_2}(\theta) = X^7 + X^6 - X^5 - X^4 - X^3 + X^2 + 2X + 1.$$  

In fact, one can show in this way that $\zeta_{48}f_2$ yields a class invariant for all fields $K$ in which 2 splits and 3 is unramified.
One can also construct class invariants for \( D = -71 \) using the generalized Weber function \( g(z) = \eta(z/3)/\eta(z) \in F_{72} \). The group \((\mathcal{O}/720)^*/\mathcal{O}^*\) is of type \( (2) \times (2) \times (2) \times (6) \times (6) \) with a set of generators \( \{19, 36\theta + 1, 18\theta + 1, 65, 64\theta + 65\} \) that act according to table 2.

Table 2. Action of \((\mathcal{O}/720)^*\) on \(Q(\zeta_3, g)\) for \( \theta = \frac{-1 + \sqrt{-71}}{2} \)

<table>
<thead>
<tr>
<th>( \sigma )</th>
<th>( \zeta_3^{\sigma-1} )</th>
<th>( g^{\sigma-1} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>36\theta + 1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>18\theta + 1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>65</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>64\theta + 65</td>
<td>( \zeta_3 )</td>
<td>( \zeta_3 )</td>
</tr>
</tbody>
</table>

One finds that \( \beta = \zeta_3 g^2(\theta) \) is a class invariant, with irreducible polynomial
\[
f_{K}^\beta = X^7 + (2 + 2\theta)X^5 - (30 + 3\theta)X^4 + (51 - 3\theta)X^3 - (8 - 10\theta)X^2 - (47 + 2\theta).\]

A normalization of the function \( g^2 \) always works when 3 splits and 2 is unramified in \( K \).

Example 2. For \( K \) of discriminant \( D = -580 = -4 \cdot 5 \cdot 29 \) the prime 2 is ramified and the prime 3 inert. In this case one can construct a class invariant from the Weber function \( f(z) = \eta(z/2)/\eta(z) \in F_{48} \) evaluated at \( \theta = \sqrt{-145} \). To see this, one computes the action of the group \((\mathcal{O}/480)^*\) of type \( (8) \times (8) \times (4) \times (4) \) generated by \( \{16\theta + 1, 33\theta + 34, 19, 33\theta + 16\} \).

Table 3. Action of \((\mathcal{O}/480)^*\) on \(Q(\zeta_{48}, f)\) for \( \theta = \sqrt{-145} \)

<table>
<thead>
<tr>
<th>( \sigma )</th>
<th>( \zeta_{48}^{\sigma-1} )</th>
<th>( f^{\sigma-1} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>16\theta + 1</td>
<td>( \zeta_3 )</td>
<td>1</td>
</tr>
<tr>
<td>33\theta + 34</td>
<td>( \zeta_3^3 )</td>
<td>( \zeta_3^3 )</td>
</tr>
<tr>
<td>19</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>33\theta + 16</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Clearly \( f^4 \) yields a class invariant. However, the action on \( \zeta_{48} \) shows that \( \zeta_3 \) is left invariant by all generators except the second, which maps \( \zeta_3 \) to \(-\zeta_3 \). It follows that \( \alpha = f^2(\theta)/\sqrt{2} \) is also a class invariant. In this case \( K \) has class number 8 and \( \mathcal{C}(\mathcal{O}) \) is of type \( (2) \times (4) \). We find
\[
f_{K}^{\alpha} = X^8 - 17X^7 + 7X^6 + 12X^5 - 42X^4 + 12X^3 + 7X^2 - 17X + 1.\]
Example 3. For $K$ of discriminant $D = -471 = -3 \cdot 157$ the primes 2 and 3 are respectively split and ramified in $K$, and $C(O)$ is cyclic of order 16. This case resembles that in Example 1, but the ramification at 3 yields a different action of $(O/48O)^*/O^*$, which is a group of type $(6) \times (4) \times (4) \times (2)$ having generating set $\{32\theta + 33, 19, 36\theta + 1, 6\theta + 19\}$.

Table 4. Action of $(O/48O)^*$ on $Q(\zeta_{48}, f)$ for $\theta = \frac{-1 + \sqrt{-145}}{2}$

<table>
<thead>
<tr>
<th>$\sigma$</th>
<th>$\zeta_{48}^{\sigma-1}$</th>
<th>$f^{\sigma-1}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$32\theta + 33$</td>
<td>1</td>
<td>$\zeta_3$</td>
</tr>
<tr>
<td>19</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>$36\theta + 1$</td>
<td>$\zeta_4$</td>
<td>$\zeta_4^2$</td>
</tr>
<tr>
<td>$6\theta + 9$</td>
<td>$\zeta_5$</td>
<td>$\zeta_5^3$</td>
</tr>
</tbody>
</table>

From the Galois action in table 4 one deduces that $\zeta_1 f^3$ yields a class invariant $\alpha$ when evaluated at $\theta = \frac{1 + \sqrt{-145}}{2}$. Its irreducible polynomial is

$$f_K^\alpha = X^{16} + 6X^{15} + 62X^{14} - 106X^{13} + 382X^{12} - 942X^{11} + 4756X^{10} - 9629X^9 + 18987X^8 - 22281X^7 + 36601X^6 - 44222X^5 + 60470X^4 - 29217X^3 + 4085X^2 + 1775X - 1.$$  

This is not as good as in Example 1, and we can do better by using the 'generalized Weber functions' of level 72. More precisely, we can use the function $g_2(z) = \eta\left(\frac{z+2}{3}\right)/\eta(z) \in F_{72}$, which yields a class invariant $\beta = \zeta_3^2 g_2^2(\theta)/\sqrt{-3}$ with irreducible polynomial

$$f_K^\beta = X^{16} + 20X^{15} - 127X^{14} + 342X^{13} + 183X^{12} - 427X^{11} - 1088X^{10} + 794X^9 + 1333X^8 + 794X^7 - 1088X^6 - 427X^5 + 183X^4 + 342X^3 - 127X^2 + 20X + 1.$$  

As in the previous example, we see that our class invariant is a unit — quite a contrast with the modular value $j(\theta)$.

Example 4. We finally take $K$ of discriminant $D = -803 = -11 \cdot 73$. Then 2 is inert and 3 is split in $K$, and $(O/48O)^*/O^*$ is a group of type $(2) \times (4) \times (8) \times (6)$ with generating set $\{16\theta + 17, 36\theta + 1, 18\theta + 1, 15\theta + 40\}$. This time the Galois action is more complicated, involving more than just multiplication by roots of unity.
The action of $15\theta - 8$ in the bottom row shows that none of the Weber functions can be normalized such as to yield a class invariant. A close approximation is however given by $\alpha = \sqrt{2}\zeta_{48}^{10}\bar{f}(\theta)$, an element invariant under the first 3 generators. It generates a cubic extension of the Hilbert class field $H$ of $K$, with conjugates $\beta = \sqrt{2}\zeta_{48}^{21}f_1(\theta)$ and $\gamma = \sqrt{2}\zeta_{48}^{25}f_2(\theta)$ over $H$. As we have $\alpha\beta\gamma = -4$, it follows that $H$ is generated over $K$ by the symmetric expressions $\alpha + \beta + \gamma$ and

$$\alpha\beta + \alpha\gamma + \beta\gamma = -4(\alpha^{-1} + \beta^{-1} + \gamma^{-1}).$$

One finds that the single expression $\delta = \frac{1}{2}(\alpha + \beta + \gamma)$ is sufficient by checking that $C(\mathcal{O})$, which has order 10, acts transitively on $\delta$. We obtain

$$f_\delta^K = X^{10} + 8X^9 + 19X^8 + 35X^7 + 101X^6 + 179X^5 + 220X^4$$
$$+ 263X^3 + 230X^2 + 100X + 16.$$

In this case, the symmetric expression $\epsilon = \alpha^{-1} + \beta^{-1} + \gamma^{-1}$ also yields a class invariant, with irreducible polynomial

$$f_\epsilon^K = X^{10} + 22X^9 + 32X^8 + 45X^7 + 109X^6 + 92X^5 + 266X^4$$
$$+ 161X^3 - 104X^2 + 48X + 128.$$

REFERENCES

3. A. C. P. Gee, This thesis.
5. R. Schertz, Die singulären Werte der Weberschen Funktionen $f, f_1, f_2$ (1976), 46–74.

Received Jan 12, 1998
SINGULAR VALUES OF THE
ROGERS-RAMANUJAN CONTINUED FRACTION

ALICE GEE AND MASCHA HONSBEEK

ABSTRACT. Let \( z \in \mathbb{C} \) be imaginary quadratic in the upper half plane. Then the Rogers-Ramanujan continued fraction evaluated at \( q = e^{2\pi iz} \) is contained in a class field of \( \mathbb{Q}(z) \). Ramanujan showed that for certain values of \( z \), one can write these continued fractions as nested radicals. We use the Shimura reciprocity law to obtain such nested radicals whenever \( z \) is imaginary quadratic.

1. INTRODUCTION

The Rogers-Ramanujan continued fraction is a holomorphic function on the complex upper half plane \( \mathbb{H} \), given by

\[
R(z) = q^{\frac{1}{2}} \prod_{n=1}^{\infty} (1 - q^n)^{\left(\frac{q}{n}\right)}, \quad \text{with } q = e^{2\pi iz} \text{ and } z \in \mathbb{H}.
\]

Here \((\frac{q}{n})\) denotes the Legendre symbol. The function \( R \) owes part of its name to the expansion

\[
R(z) = \frac{q^{\frac{1}{2}}}{1 + \frac{q}{1 + \frac{q^2}{1 + \frac{q^3}{\ldots}}}}
\]

as a continued fraction. In their first correspondence of 1913, Ramanujan astonished Hardy with the assertion

\[
e^{\frac{-2\pi}{q}} = \sqrt{\frac{5 + \sqrt{5}}{2}} - \frac{\sqrt{5 + 1}}{2}.
\]

1991 Mathematics Subject Classification. Primary 11Y65; Secondary 11Y40.
Key words and phrases. Rogers-Ramanujan continued fraction, Shimura reciprocity.

The first author thanks Heng Huat Chan for providing the opportunity to enjoy his kind hospitality in Singapore. She is indebted to the lively discussions that initiated this work. This research was funded in part by the Academic Research Fund of the National University of Singapore, project number RP3981645.
Hardy was unaware of the product expansion (1) that Ramanujan had used to compute identity (3), which is none other than the evaluation of $R$ at $i$. In the same correspondence, Ramanujan expressed the equality

$$-R\left(\frac{5+i}{2}\right) = \sqrt{\frac{5-\sqrt{5}}{2}} - \frac{\sqrt{5}-1}{2}$$

with a similar dramatic flair. The radical symbol in (3) and (4) should be interpreted as the real positive root on $\mathbb{R}$. Ramanujan communicated radical expressions for $R(\sqrt{-5})$ and $-R\left(\frac{5+i\sqrt{-5}}{2}\right)$ in his second letter to Hardy, and several other values of $R$ at imaginary quadratic arguments are recorded in his notebooks. The other name connected to the function $R$ is that of L.J. Rogers, who proved the equality of (1) and (2) in 1894. This was discovered by Ramanujan after his arrival in England.

In this paper, we evaluate singular values of the Rogers-Ramanujan continued fraction. These are the function values of $R$ taken at imaginary quadratic $\tau \in \mathbb{H}$. As $R$ is a modular function of level 5—a classical fact for which we furnish a proof—these values generate abelian extensions of $\mathbb{Q}(\tau)$. Exploiting the Galois action given by the Shimura reciprocity law, we give a method for constructing a nested radical for $R(\tau)$ that works whenever $\tau$ is imaginary quadratic. Our systematic approach extends the results of [1], [10] and [6], which only apply to individual examples.

By way of example, we provide nested radicals for $R(\sqrt{-n})$ for $n = 1, 2, \ldots, 16$ when $n \not\equiv 3 \bmod 4$. Writing down nested radicals for $R(\tau)$ becomes increasingly unwieldy as the discriminant of $\tau$ grows, so in the case $n \equiv 3 \bmod 4$, where $\mathbb{Q}$ and $R\left(\frac{5+i\sqrt{-n}}{2}\right)$ generate a subfield of $\mathbb{Q}(R(\sqrt{-n}))$, we evaluate $R\left(\frac{5+i\sqrt{-n}}{2}\right)$ instead of $R(\sqrt{-n})$. In the classical literature, the notation $S(z) = -R\left(\frac{5+i\sqrt{-n}}{2}\right)$ is frequently used.

The authors thank Heng Huat Chan and Peter Stevenhagen for several helpful discussions.

2. The Modular Function Field of Level 5

A modular function of level $N$ is a meromorphic function on the extended complex upper half plane $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ that is invariant under the natural action of the modular group $\Gamma(N) = \ker[\text{SL}_2(\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}/N\mathbb{Z})]$ of level $N$. As such functions are invariant under $z \mapsto z + N$, they admit a Fourier expansion in the variable $q = e^{2\pi i z}$. The modular functions of level $N$ with Fourier expansion in $\mathbb{Q}(\zeta_N)((q^{N}))$ form a field $F_N$, the function field of the modular curve $X(N)$ over $\mathbb{Q}(\zeta_N)$. 

The extension $F_N$ is Galois over $F_1$ with group $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. For a proof, see [5, p. 66, Thm 3]. One can describe the action of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $F_N$ explicitly. The group $(\mathbb{Z}/N\mathbb{Z})^*$ acts as a group of automorphisms of $F_N$ over $F_1$, by restricting its natural cyclotomic action on $\mathbb{Q}(\zeta_N)((q^{\frac{1}{N}}))$. The natural action of $\Gamma(1) = \text{SL}_2(\mathbb{Z})$ on $F$ induces a right action of $\Gamma(1)/\Gamma(N) = \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on $F_N$ which leaves $F_1$ invariant. The homomorphisms

\[(\mathbb{Z}/N\mathbb{Z})^* \to \text{Gal}(F_N/F_1) \quad \text{and} \quad \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to \text{Gal}(F_N/F_1)\]

can be combined into an action of the semi-direct product

\[(\mathbb{Z}/N\mathbb{Z})^* \ltimes \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) \simeq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})\]

on $F_N$. For the isomorphism (5), we identify $d \in (\mathbb{Z}/N\mathbb{Z})^*$ with the element $(1, 0) \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The resulting sequence

\[1 \to \{\pm 1\} \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \text{Gal}(F_N/F_1) \to 1\]

is exact.

The modular invariant $j$ generates $F_1$ over $\mathbb{Q}$, and induces the isomorphism $X(1) \simeq \mathbb{P}^1(\mathbb{Q})$. In a similar fashion, the curve $X(5)$ has genus 0, thus its function field $F_5$ can be generated by a single function over $\mathbb{Q}(\zeta_5)$. The Rogers-Ramanujan continued fraction $R$ is such a generator. There are several ways to prove this classical fact. Our proof is based upon Watson’s formulas [13]

\[\frac{1}{R(z)} - R(z) - 1 = \frac{\eta(z/5)}{\eta(5z)}, \tag{7'}\]

\[\frac{1}{R^5(z)} - R^5(z) - 11 = \left(\frac{\eta(z)}{\eta(5z)}\right)^6, \tag{8'}\]

which relate $R$ to Dedekind’s $\eta$-function

\[\eta(z) = q^{1/24} \prod_{m=1}^{\infty} (1 - q^m), \quad q^{1/24} = e^{2\pi iz/24}.\]

Watson’s formulas will prove useful in section 4, where we evaluate singular values of $R$. We define functions

\[\eta_0 = \frac{\eta \circ \left(\frac{1}{5} \frac{0}{1}\right)}{\eta} \quad \text{and} \quad \eta_5 = \sqrt{5} \cdot \frac{\eta \circ \left(\frac{5}{0} \frac{0}{1}\right)}{\eta},\]
so that equations (7') and (8') become

\[
(7) \quad \frac{1}{R} - R - 1 = \sqrt{5} \cdot \frac{b_0}{b_5},
\]

\[
(8) \quad \frac{1}{R^5} - R^5 - 11 = \frac{5^3}{b_5}.
\]

Before we show that \( R \) is modular, we first prove that the functions appearing on the right hand side of (7) and (8) are modular of level 5. This is well known for \( b_5^6 \) [9, p. 619], but for lack of a reference in the case of (7), we provide a proof that works in both cases.

In order to compute the action of \( SL_2(\mathbb{Z}) \) on \( b_0 \) and \( b_5 \), we begin by observing that the generating matrices \( S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \) and \( T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) of \( SL_2(\mathbb{Z}) \) act on the Dedekind \( \eta \)-function as

\[
(9) \quad \eta \circ S(z) = \sqrt{-iz} \eta(z) \quad \text{and} \quad \eta \circ T(z) = \zeta_4 \eta(z).
\]

The radical sign in (9) stands for the holomorphic branch of the square root on \(-i\mathbb{H}\) that is positive on the real axis. The observation \( \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \cdot S = S \cdot \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} \) gives \( b_0 \circ S = b_5 \) with the help of (9). Let \( \Delta_5 \) denote the set of \( 2 \times 2 \) matrices with coefficients in \( \mathbb{Z} \) that have determinant 5. The matrices

\[
M_i = \begin{pmatrix} 1 & i \\ 0 & 5 \end{pmatrix}, \quad i = 0,1,\ldots,4 \quad \text{and} \quad M_5 = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}
\]

form a set of representatives for \( \Gamma \backslash \Delta_5 \). For any \( A \in SL_2(\mathbb{Z}) \) and \( i = 0,1,\ldots,5 \), we can find \( B \in SL_2(\mathbb{Z}) \) and \( j \in \{0,1,\ldots,5\} \) such that \( M_i \cdot A = B \cdot M_j \) holds. We put

\[
(10) \quad b_5 = \sqrt{5} \cdot \frac{\eta \circ M_i}{\eta} \quad \text{and} \quad b_i = \frac{\eta \circ M_i}{\eta} \quad \text{for} \ i = 0,1,\ldots,4.
\]

Using (9) one computes

\[
(11) \quad \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix} \circ S = \begin{pmatrix} b_5 \\ \zeta_4^3 b_4 \\ b_3 \\ b_2 \\ \zeta_4^3 b_1 \\ b_0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix} \circ T = \begin{pmatrix} \zeta_4^{-1} b_1 \\ \zeta_4 b_2 \\ \zeta_4^{-1} b_3 \\ \zeta_4^3 b_4 \\ \zeta_4 b_0 \\ b_5 \end{pmatrix}.
\]
Lemma 1. The functions $h_i^6$ and $h_i/h_j$ with $i, j \in \{0, 1, \ldots, 5\}$, are modular of level 5.

Proof. From [7] we know that $\Gamma(5)$ is the normal closure of $(T^5)$ in $SL_2(\mathbb{Z})$. This means that $\Gamma(5)$ is generated by matrices of the form $AT^6A^{-1}$ with $A \in SL_2(\mathbb{Z})$. From (9) we observe

$$h_i \circ T^5 = \zeta_5^{-1} \cdot h_i \quad \text{for } i = 0, 1, \ldots, 5.$$ 

For $A \in SL_2(\mathbb{Z})$ and $j \in \{0, 1, \ldots, 5\}$, the equations (11) show that all $h_j \circ A$ are of the form $h_j \circ A = \zeta \cdot h_i$ for some $i \in \{0, 1, \ldots, 5\}$ and some root of unity $\zeta$. Similarly

$$h_j \circ AT^5 = \zeta_5^{-1} \cdot h_j \circ A$$

holds for every $A \in SL_2(\mathbb{Z})$. Thus $h_i^6$ is invariant under $AT^5A^{-1}$ for all $A \in SL_2(\mathbb{Z})$, as well as every quotient $h_i/h_j$. \hfill \Box

Lemma 2. The Rogers-Ramanujan continued fraction $R$ is modular of level 5.

Proof. As we know from (1) that $R$ is holomorphic on $H$, it suffices to show that $R \circ AT^5A^{-1} = R$ for all $A \in SL_2(\mathbb{Z})$. From Watson’s formula (7) one derives

$$(12) \quad (X - R)(X + \frac{1}{R}) = X^2 + \left(\sqrt{5} \cdot \frac{h_0}{h_5} + 1\right)X - 1.$$ 

As $AT^5A^{-1}$ acts trivially on $\sqrt{5}h_0/h_5$, it maps $R$ to either $R$ or $-1/R$. Suppose the latter to be true. Then $R \circ AT^5 = -1/(R \circ A)$ holds. As the translation $T^5$ fixes the cusp $i\infty$, we have

$$R \circ A(i\infty) = R \circ AT^5(i\infty) = \frac{-1}{R \circ A(i\infty)},$$

which implies $R \circ A(i\infty) = \pm i$. Then Watson’s formula (8) yields

$$(13) \quad \frac{5^3}{(h_5 \circ A(i\infty))^6} = \frac{1}{(\pm i)^6} - (\pm i)^6 - 11 = \pm 2i - 11.$$ 

On the other hand, we can evaluate $h_5 \circ A(i\infty)$ by considering the product expansion for $h_5 \circ A$ at $q = 0$. By (11), one has $h_5 \circ A = \zeta \cdot h_j$ for some root of unity $\zeta$ and some $j \in \{0, 1, \ldots, 5\}$. For $j = 0, 1, \ldots, 4$, we compute

$\lim_{N \to \infty} \frac{e^{2\pi i (1/N \pm i)}}{e^{2\pi i (iN)}} = 0.$

A similar calculation shows that $h_5$ has a pole at $i\infty$. Contradiction with (13). \hfill \Box
Proposition 3. The minimum polynomial of $R^5$ over $F_1 = \mathbb{Q}(j)$ is


The minimum polynomial of $R$ over $\mathbb{Q}(j)$ is $P(X^5)$, with $P$ as above.

Proof. Weber shows [14, p. 256] that $h_5^3$ is a zero of $X^6 + 10X^3 - \gamma_2 X + 5$, with $\gamma_2$ a cube root of $j$. Another zero is $h_5^2 = (h_0 \circ S)^2$ because $S$ fixes $\gamma_2$. We obtain

$$j = \left(\frac{h_5^{12} + 10h_5^6 + 5}{h_5^6}\right)^3.\tag{15}$$

Rewriting (8) gives the identity

$$h_5^6 = \frac{5^3 \cdot R^5}{-R^{10} - 11R^5 + 1}.$$

Substituting the above relation for $h_5^6$ into (15), we have

$$j = \left(\frac{1 + 228R^5 + 494R^{10} - 228R^{15} + R^{20}}{(-R + 11R^6 + R^{11})^5}\right)^3,$$

which readily yields $P(R^5) = 0$, with $P$ as in (14). To see that $P$ is irreducible in $\mathbb{Z}[X,j]$, compose the evaluation map $\mathbb{Z}[X,j] \rightarrow \mathbb{Z}[X]$ defined by $j \mapsto 1$ with reduction modulo 2. We obtain a homomorphism $\mathbb{Z}[X,j] \rightarrow \mathbb{F}_2[X]$ that sends $P$ to the cyclotomic polynomial $\Phi_{13} \in \mathbb{F}_2[X]$, which is irreducible because 2 is a primitive root modulo 13. As $P$ is a monic polynomial in $X$, we conclude that it is the minimum polynomial of $R^5$ over $\mathbb{Q}(j)$.

In order to see that $\mathbb{Q}(R)$ has degree $5 \cdot [\mathbb{Q}(R^5) : \mathbb{Q}(j)] = 60$ over $\mathbb{Q}(j)$, it suffices to observe that $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \text{SL}_2(\mathbb{Z})$, which acts as $R(z) \mapsto R(z + 1) = \zeta_5 R(z)$ induces an automorphism of order five of $\mathbb{Q}(R)$ over $\mathbb{Q}(R^5)$. Thus $P(X^5)$ is the minimum polynomial of $R$ over $\mathbb{Q}(j)$.

Theorem 4. The Rogers-Ramanujan continued fraction $R$ generates $F_5$ over $\mathbb{Q}(\zeta_5)$.

Proof. As $R$ has rational Fourier coefficients, the subfields $\mathbb{Q}(R) = F_1(R)$ and $F_1(\zeta_5)$ of $F_5$ are linearly disjoint extensions of $F_1$ having degree 60 and 4, respectively. Their composite, which has degree 240 = $\#(\text{GL}_2(\mathbb{Z}/5\mathbb{Z})/\{+1\})$ over $F_1$ is therefore equal to $F_5$. $\square$
The rational function on the right hand side of (16) appears in Klein's study of the finite subgroups of Aut($\mathbf{P}^1(C)$). His icosahedral group $A_5$ is isomorphic to $\text{SL}_2(\mathbb{Z}/5\mathbb{Z})/\{\pm 1\}$, and the natural map from $\mathbf{P}^1(C)$ to the orbit space of the icosahedral group ramifies above 3 points. The relation (16) defines a generator [4, p. 61, 65] for the field of functions invariant under the icosahedral group. In our situation the natural map $X(5) \to X(1)$ ramifies over 3 points and the Galois group of $\mathbb{C}(R)$ over $\mathbb{C}(j)$ is $\text{SL}_2(\mathbb{Z}/5\mathbb{Z})/\{\pm 1\}$.

The subgroups of $\text{GL}_2(\mathbb{Z}/5\mathbb{Z})/\{\pm 1\}$ that stabilize the functions appearing in the equations (7) and (8) are given in the diagram below. The stabilizers of $h_5^g$ and $\sqrt{5} \cdot h_0/h_5$ in $\text{SL}_2(\mathbb{Z}/5\mathbb{Z})/\{\pm 1\}$ can be determined using (11).

\[ F_5 = \mathbb{Q}(R, \zeta_5) \]

\[ \mathbb{Q}(R) \]

\[
\begin{bmatrix}
1 & 1 \\
0 & 5
\end{bmatrix}
\]

\[ \mathbb{Q}(\sqrt{5} \cdot h_0/h_5) \]

\[ \mathbb{Q}(h_5^g) \]

\[ \mathbb{Q}(j, \zeta_5) \]

\[ \mathbb{Q}(j) \]

\[ \mathbb{Q}(\varphi) \]

\[ \mathbb{Q}((\frac{1}{0} \, \frac{0}{1})) \]

\[ \text{SL}_2(\mathbb{Z}/5\mathbb{Z})/\{\pm 1\} \]

3. **Galois Theory for Singular Values of Modular Functions**

Let $O$ be an imaginary quadratic order having $\mathbb{Z}$-basis $[\tau, 1]$. Define $H_N = H_{N,O}$ to be the field generated over $K = \mathbb{Q}(\tau)$ by the function values $h(\tau)$, where $h$ ranges over the modular functions in $F_N$ that are pole-free at $\tau$. The first main theorem of complex multiplication [5] states that $H_N$ is an abelian extension of $K$. For $N = 1$, the field $H_1$ is the ring class field for $O$. If $O$ is a maximal quadratic order with field of fractions $K$, then $H_N$ is the ray class field of conductor $N$ over $K$, and $H_1$ is the Hilbert class field of $K$. For ray class fields of non-maximal orders, see for example [12].
Before we can describe the explicit action of \( \text{Gal}(H_N/K) \) on elements of \( H_N \), we first look at \( \text{Gal}(H_N/H_1) \), which fits in a short exact sequence

\[
1 \rightarrow \mathcal{O}^* \rightarrow (\mathcal{O}/\mathcal{O})^* \xrightarrow{\Delta} \text{Gal}(H_N/H_1) \rightarrow 1.
\]

In order to describe the Artin map \( A \) in (18), we write the elements of \( \mathcal{O}/\mathcal{O} \) as row vectors with respect to the \( \mathbb{Z}/\mathbb{N}\mathbb{Z} \)-basis \([\tau, 1] \). If \( \tau \) has minimum polynomial \( X^2 + BX + C \in \mathbb{Z}[X] \), define the homomorphism

\[
g_{\tau} : (\mathcal{O}/\mathcal{O})^* \rightarrow \text{GL}_2(\mathbb{Z}/\mathbb{N}\mathbb{Z})
\]

\[
s\tau + t \mapsto \begin{pmatrix} t & -B \\ -C & t \end{pmatrix}.
\]

The matrix \( g_{\tau}(x) \) represents multiplication by \( x \) on \( \mathcal{O}/\mathcal{O} \) with respect to the \( \mathbb{Z}/\mathbb{N}\mathbb{Z} \)-basis \([\tau, 1] \). For \( h \in F_N \), the Shimura reciprocity law [11] gives the action of \( x \in (\mathcal{O}/\mathcal{O})^* \) on \( h(\tau) \) as

\[
(h(\tau))^x = h^{g_{\tau}(x)}(\tau).
\]

Here \( g_{\tau}(x) \in \text{GL}_2(\mathbb{Z}/\mathbb{N}\mathbb{Z}) \) acts on \( h \in F_N \) as described in (6). Moreover, if \( h \in F_N \) is a function for which \( \mathbb{Q}(h) \subset F_N \) is Galois, then \( K(h(\tau)) \) is the fixed field of

\[
\{ x \in (\mathcal{O}/\mathcal{O})^* \mid h^{g_{\tau}(x)} = h \} \subset (\mathcal{O}/\mathcal{O})^*.
\]

For any \( h \in F_N \), we aim to compute the conjugates of \( h(\tau) \) with respect to the full group \( \text{Gal}(H_N/K) \). In the case \( N = 1 \), the Galois group of \( H_1 = K(j(\tau)) \) over \( K \) is isomorphic to the ideal class group \( C(\mathcal{O}) \) of \( \mathcal{O} \). The elements of \( C(\mathcal{O}) \) can be represented as primitive quadratic forms \([a, b, c] \) of discriminant \( D = b^2 - 4ac \), where \( D \) is the discriminant of \( \mathcal{O} \). The \( \mathbb{Z} \)-module having basis \([a, -\frac{b}{2} + \frac{\sqrt{D}}{2a}] \) is an \( \mathcal{O} \)-ideal in the class of \([a, b, c] \), and the class of \([a, -b, c] \) acts on \( j(\tau) \) as

\[
j(\tau)^{[a, -b, c]} = j\left(\frac{-b + \sqrt{D}}{2a}\right).
\]

In the general case for \( N > 1 \), we need the elements of \( \text{Gal}(H_N/K) \) that lift (22) for each representative \([a, b, c] \) in \( C(\mathcal{O}) \). The formula [3, p. 32, Thm. 20] produces one element \( \sigma \in \text{Gal}(H_N/K) \) along with a matrix \( M_N = M_N(a, b, c) \) in \( \text{GL}_2(\mathbb{Z}/\mathbb{N}\mathbb{Z}) \) such that for all \( h \in F_N \), the relation

\[
h(\tau)^\sigma = h^{M_N}\left(\frac{-b + \sqrt{D}}{2a}\right)
\]
holds. The automorphism $\sigma$ clearly lifts the action in (22) to $\text{Gal}(H_N/K)$ because $M_N \in \text{GL}_2(\mathbb{Z}/\mathbb{N}\mathbb{Z})$ acts trivially on $j \in F_1$. As every automorphism in $\text{Gal}(H_N/K)$ is obtained by composing elements of $\text{Gal}(H_N/H_1)$ with one of the coset representatives for $\text{Gal}(H_1/K)$ in (23), we can determine the conjugates of $h(\tau)$ under $\text{Gal}(H_N/K)$ for any $h \in F_N$.

Given this explicit action on $H_N$ over $K$ we can compute representations for singular values of modular functions by minimal polynomials as well as radical expressions over $\mathbb{Q}$.

The natural way to describe an algebraic number is its minimum polynomial over $\mathbb{Q}$. Let $h \in F_N$ be a function for which $h(\tau)$ is an algebraic integer. The conjugates of $h(\tau)$ over $K$ can be approximated numerically when the Fourier expansion for $h$ is known. One expresses each conjugate in the form $h^M(\theta)$, with $M \in \text{GL}_2(\mathbb{Z}/\mathbb{N}\mathbb{Z})$ and $\theta \in K$, and then writes $M = \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \cdot A$ with $x = \text{det}(M)$ and $A \in \text{SL}_2(\mathbb{Z}/\mathbb{N}\mathbb{Z})$. After modifying the Fourier coefficients of $h$ with respect to $\zeta_N \mapsto \zeta_N^x$, one evaluates the new expansion at $\tilde{A}(z)$, where $\tilde{A} \in \text{SL}_2(\mathbb{Z})$ is a lift of $A$. We calculate the minimum polynomial $f$ of $h(\tau)$ over $\mathbb{Q}$ by approximating the conjugates of $h(\tau)$ over $K$. Adjoining complex conjugates gives a full set of conjugates over $\mathbb{Q}$. In order to determine the polynomial $f \in \mathbb{Z}[X]$, we need only to approximate its coefficients accurate to the nearest integer.

Because $H_5$ is abelian over $K$, one can also express $h(\tau)$ as a nested radical over $\mathbb{Q}$ in the spirit of Ramanujan's evaluations (3) and (4). Unlike the minimum polynomial $f$, which is unique, many different nested radicals over $\mathbb{Q}$ exist that all represent $h(\tau)$. Given any abelian extension $H/K$ of degree greater than 1 and any $w \in H$, the following standard procedure expresses $w$ as a radical expression over a field $H'$ with the property $[H' : K] < [H : K]$. Applying the procedure recursively produces a nested radical for $w$ over $K$.

We choose an automorphism $\sigma \in \text{Gal}(H/K)$ of order $m > 1$ and set $H' = H^\sigma(\zeta_m)$, where $H^\sigma$ denotes the fixed field of $\langle \sigma \rangle$. Then $H'/K$ is an abelian extension of degree

$$[H' : K] \leq \varphi(m) \cdot [H^\sigma : K] < m \cdot [H^\sigma : K] = [H : H^\sigma][H^\sigma : K] = [H : K].$$

We write

$$w = \frac{1}{m} (h_0 + h_1 + h_2 + \cdots + h_{m-1}),$$

where

$$h_i = \sum_{k=1}^{m} \zeta_m^{ik} \cdot w(\zeta_m^k), \quad i = 0, 1, \ldots, m - 1.$$
are the Lagrange resolvents for \( w \) with respect to \( \sigma \). Note that \( h_0 = \text{Tr}_{H/H^\sigma}(w) \) is an element of \( H^\sigma \). Every \( \rho \in \text{Gal}(H(\zeta_m)/H^\sigma) \) acts trivially on \( \zeta_m \) and as some \( \sigma^a \in \langle \sigma \rangle \) on \( H \). For \( i = 1, 2, \ldots, m - 1 \), we have

\[
h_i^\rho = \sum_{k=1}^{n} \zeta_{im}^k \cdot w^{(\sigma^k + \sigma^a)} = \zeta_{im}^{-ia} \cdot h_i,
\]

which means \( h_1^m, h_2^m, \ldots, h_{m-1}^m \in H^\sigma \). As \( h_i = \sqrt[m]{h_i^m} \) for the appropriate choice of the \( m \)-th root, equation (24) represents \( w \) as a radical expression over \( H^\sigma \). The recursion step is applied to \( h_0, h_1^m, h_2^m, \ldots, h_{m-1}^m \in H^\sigma \).

Suppose \( h \in F_N \) such that \( h(\tau) \) is an algebraic integer. In order to apply the recursive procedure, above to \( h(\tau) \), one needs not only the action of \( \text{Gal}(H_N/K) \), but also that of \( \text{Gal}(H_N(\zeta_d)/K) \) for various numbers \( d > 1 \). This is obtained by restricting the action of \( \text{Gal}(H_dN/K) \) to \( H_N(\zeta_d) \). The elements computed in the final recursion step are in \( \mathcal{O}_K \), which is a discrete subgroup of \( \mathbb{C} \). An approximation of their coordinates with respect to a \( \mathbb{Z} \)-basis for \( \mathcal{O}_K \), that is accurate to the nearest integer, produces a nested radical for \( h(\tau) \) over \( \mathbb{Q} \).

The methods above can be extended to arbitrary imaginary quadratic numbers \( \theta \in \mathbb{H} \) that are not necessarily algebraic integers. In order to compute the conjugates of \( h(\theta) \) over \( K = \mathbb{Q}(\theta) \) we take an integral basis \([\tau, 1]\) for \( K \) and write \( \theta = \frac{a}{d} \tau + \frac{b}{d} \) with \( a, b, d \in \mathbb{Z} \). One evaluates \( h \circ \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in F_{adN} \) at \( \tau \), which is contained in \( H_{adN} \). Again, (20) and (23) allow us to calculate the conjugates of \( h(\theta) \) over \( K \).

4. THE RAY CLASS FIELD \( H_5 \)

We turn our attention back to the functions of level 5 from section 2. In this section, we compute some singular values \( R(\tau) \) of the Rogers-Ramanujan continued fraction. As the singular values of \( j \) are known to be algebraic integers, the same holds true for \( R \) because the polynomial (14) has coefficients in \( \mathbb{Z}[j] \). We fix \( \mathcal{O} = [\tau, 1] \) to be an order in some imaginary quadratic number field \( K \). We state a few properties of \( R(\tau) \) before computing some examples.

**Theorem 5.** The class field \( H_5 = H_{5,\mathcal{O}} \) is generated by \( R(\tau) \) over \( K \).

**Proof.** As we have \( F_5 = \mathbb{Q}(R, \zeta_5) \) by Theorem 4, the extension \( F_5/\mathbb{Q}(R) \) is Galois and we are in the situation for which (21) applies. As \( \mathbb{Q}(R) \) is the subfield of \( F_5 \) fixed by

\[
\{ \left( \begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix} \right) \mid d \in (\mathbb{Z}/5\mathbb{Z})^* \} \subset \text{GL}_2(\mathbb{Z}/5\mathbb{Z}),
\]

the class field \( K(R(\tau)) \) is the subfield of \( H_5 \) fixed by

\[
G = \{ x \in (\mathcal{O}/5\mathcal{O})^* \mid g_r(x) = \pm \left( \begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix} \right) \text{ for some } d \in (\mathbb{Z}/5\mathbb{Z})^* \} \subset (\mathcal{O}/5\mathcal{O})^*.
\]
From formula (19) we see that the only diagonal matrices appearing in the image $g_r[(O/5O)^*]$ are scalar. We conclude $G = \{ \pm 1 \}$ and $K(R(r)) = H_5$.

Let $w(z) = \eta(\frac{z}{5})/\eta(5z)$ denote the function that appears on the right hand side of equation (7'). Thus we have

$$\frac{1}{R(z)} - R(z) - 1 = w(z).$$

**Proposition 6.** The values $R(\tau)$ and $-1/R(\tau)$ are conjugate over $K(w(\tau))$. Furthermore, $H_5$ is generated over $K$ by $\zeta_5$ together with $w(\tau)$.

**Proof.** The polynomial

$$X^2 + (w(\tau) + 1)X - 1 \in K(w(\tau))[X]$$

derived from (25) has zeroes $R(\tau)$ and $-1/R(\tau)$. To show that (26) is irreducible in $K(w(\tau))[X]$ we consider the homomorphism $g_r : (O/5O)^* \rightarrow \text{GL}_2(\mathbb{Z}/5\mathbb{Z})$ in (19). By (20), the group $\text{Gal}(H_5/H_1)$ contains the automorphism $R(\tau) \mapsto R^{g_r-2}(\tau)$. In order to determine the action action of

$$g_r(2) = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/5\mathbb{Z})$$
on $F_5$, we recall that $R$ and $w$ have rational Fourier coefficients and thus are fixed by $\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$. Using (11) one checks that $w$ is stabilized by $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \in \text{SL}_2(\mathbb{Z}/5\mathbb{Z})$. Theorem 2.4 together with equation (25) tells us that this matrix $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ sends $R$ to $-1/R$, so $R(\tau)$ and $-1/R(\tau)$ are conjugates over $K$. As $K(R(\tau)) = H_5$ contains $\zeta_5$, the situation $R(\tau) = -1/R(\tau) = \pm i$ is impossible. We conclude that (26) is irreducible in $K(w(\tau))[X]$.

We have $[H_5 : K(w(\tau))] = 2$. In fact, $K(w(\tau))$ is the subfield of $H_5$ fixed by the subgroup of $(O/5O)^*$ generated by 2 and the image of $O^*$. By (26) the action of $2 \in (O/5O)^*$ on $\zeta_5 \in H_5$ is $\zeta_5 \mapsto \zeta_5^{-1}$. We conclude $\zeta_5 \notin K(w(\tau))$ and $H_5 = K(w(\tau),\zeta_5)$.

To determine the minimum polynomial of $R(\tau)$ over $\mathbb{Q}$, it is convenient to first compute the polynomial for $w(\tau)$ and then recover $R(\tau)$ with (25). As both values $R(\tau)$ and $1/R(\tau)$ are algebraic integers, it follows that $w(\tau)$ is an algebraic integer too. In particular, the method of section 4 for computing $\mathcal{I}_{\mathbb{Q}}w(\tau)$ works here.

Working with values of $w$ is easier than working with $R$ directly as there are only half as many conjugates over $K$ to compute. More importantly, the
Dedekind $\eta$-function is implemented in several software packages that quickly compute $\eta(x)$ to a high degree of accuracy. These routines make use of $\text{SL}_2(\mathbb{Z})$-transformations to ensure that the imaginary part of $z$ is sufficiently large to guarantee rapid convergence of the Fourier expansion of $\eta(z)$. One obtains the minimal polynomial of $R(\tau)$ over $\mathbb{Q}$ from $f^{w(\tau)}_\mathbb{Q}$ by writing

$$w = \frac{1 - R - R^2}{R}$$

using ($7'$). Then $R(\tau)$ is a zero of the monic polynomial

$$X^{\deg} f^{w(\tau)}_\mathbb{Q}\left(\frac{1 - X - X^2}{X}\right) \in \mathbb{Q}[X]$$

with $\deg = \deg(f^{w(\tau)}_\mathbb{Q})$. According to proposition 6, the resulting polynomial is irreducible because its degree is $2 \cdot \deg$.

An inspection of product expansion (1) shows $R(z) \in \mathbb{R}$ whenever the real part of $z \in \mathbb{H}$ is an integer multiple of $\frac{1}{2}$. For the singular arguments

$$\tau_n = \begin{cases} \sqrt{-n} & \text{if } n \not\equiv 3 \mod 4 \\ \frac{5 + \sqrt{-n}}{2} & \text{if } n \equiv 3 \mod 4 \end{cases}$$

the value $R(\tau_n)$ is a real, and its minimum polynomial over $K$ is contained in $\mathbb{Z}[X]$ because complex conjugation acts as

$$f^{R(\tau_n)}_K = f^{R(\tau_n)}_K = f^{R(\tau_n)}_K.$$

Proposition 6 implies that $f^{R(\tau)}_\mathbb{Q} = \sum_{i=0}^{2d} c_i X^i$ is the minimum polynomial for both $R(\tau)$ and $-1/R(\tau)$, thus the coefficients satisfy $c_i = (-1)^i c_{2d-i}$. For this reason we only list the first half of the coefficients $c_{2d}, c_{2d-1}, \ldots, c_d$ in table 1, where we give the minimum polynomials for $R(\tau_n)$ with $1 \leq n \leq 16$.

A nice way of generating $H_5 = K(w(\tau_n), \zeta_5)$ comes from proposition 6. The subfield $K(w(\tau_n))$ of $H_5$ is the fixed field for the subgroup generated by 2 and $O^*$ in $(O/5O)^*$. Because $\sqrt{5}$ is invariant under $g_{\tau_n}(2) = \left( \begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix} \right)$, we conclude $\sqrt{5} \in K(w(\tau_n))$. Thus for the function

$$\tilde{w} = \frac{w}{\sqrt{5}} = \frac{b_0}{b_5}$$

we have $\tilde{w}(\tau_n) \subset K(w(\tau_n))$ and $H_5 = K(\tilde{w}(\tau_n), \zeta_5)$. 
Table 1. The minimum polynomials of $R(\tau_n)$ over $\mathbb{Q}$

<table>
<thead>
<tr>
<th>$n$</th>
<th>degree</th>
<th>first half of coefficients $c_{2d}, c_{2d-1} \ldots c_d$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>1, 2, -6</td>
</tr>
<tr>
<td>2</td>
<td>12</td>
<td>1, 6, -1, 0, 50, -14, 16</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>1, -3, -1</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>1, 24, 22, 22, 30</td>
</tr>
<tr>
<td>5</td>
<td>20</td>
<td>1, 10, -90, 280, -730, 1022, -2410, 2540, -3330, 1730, -2006</td>
</tr>
<tr>
<td>6</td>
<td>16</td>
<td>1, 28, 140, 60, -365, 264, 482, 340, 2035</td>
</tr>
<tr>
<td>7</td>
<td>12</td>
<td>1, -4, -1, -25, -25, -14, 31</td>
</tr>
<tr>
<td>8</td>
<td>24</td>
<td>1, 32, -96, 268, 31, -328, -1446, -5112, 996, 3972, 10594, 4208, -6924</td>
</tr>
<tr>
<td>9</td>
<td>16</td>
<td>1, 38, -240, -300, -235, -726, 92, -1840, -675</td>
</tr>
<tr>
<td>10</td>
<td>20</td>
<td>1, 60, 360, -120, 120, -1728, 3540, 840, 4320, -7620, -1006</td>
</tr>
<tr>
<td>11</td>
<td>8</td>
<td>1, -6, -13, -28, 5</td>
</tr>
<tr>
<td>12</td>
<td>24</td>
<td>1, 82, 329, -282, -74, 3672, -3846, 4238, 13521, -9028, 7844, 2408, 43651</td>
</tr>
<tr>
<td>13</td>
<td>24</td>
<td>1, 82, -996, 968, 1051, 1422, -96, -24912, 7896, 16722, 28844, 13658, -114024</td>
</tr>
<tr>
<td>14</td>
<td>32</td>
<td>1, 116, 614, -3040, 25230, 17988, -103372, 184292, 207725, -409400, -323390, -129140, 2879690, 3515800, -5057000, -4838560, 7624315</td>
</tr>
<tr>
<td>15</td>
<td>20</td>
<td>1, -15, 60, -270, 720, -1353, 2115, -2610, 2970, -1095, 3119</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>1, 148, -670, 240, 1570, -2616, 302, 1180, -1610</td>
</tr>
</tbody>
</table>

Proposition 7. The value $\tilde{w}(\tau_n)$ is an algebraic integer. If $5 \nmid n$ then $\tilde{w}(\tau_n)$ is a unit in $H_5$, the ray class field of conductor 5 over $\mathcal{O} = [\tau_n, 1]$.

Proof. Hasse and Deuring [2, p. 43] determine exactly the ideals generated by singular values of the lattice functions

$$\varphi_M(z) = \frac{\Delta(M(z))}{\Delta(z)} ,$$

with $M$ a $2 \times 2$ matrix having coefficients in $\mathbb{Z}$. Our functions $h_0$ and $h_5$ were defined in (10) as

$$h_0 = \frac{\eta \circ M_0}{\eta} , \quad h_5 = \sqrt{5} \cdot \frac{\eta \circ M_5}{\eta} \quad \text{with} \quad M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} , \quad M_5 = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} .$$

Thus we have

$$\varphi_{M_0} \left( \begin{pmatrix} z \\ 1 \end{pmatrix} \right) = h_0(z)^{24} \quad \text{and} \quad \varphi_{M_5} \left( \begin{pmatrix} z \\ 1 \end{pmatrix} \right) = h_5(z)^{24} ,$$

and

$$\tilde{w}(\tau_n)^{24} = \frac{\varphi_{M_0} \left( \begin{pmatrix} \tau_n \\ 1 \end{pmatrix} \right)}{\varphi_{M_5} \left( \begin{pmatrix} \tau_n \\ 1 \end{pmatrix} \right)} .$$
If \( n \) is not divisible by 5, then

\[
M_0\left(\frac{\tau_n}{1}\right) = [\tau_n, 5] \quad \text{and} \quad M_5\left(\frac{\tau_n}{1}\right) = [5\tau_n, 1]
\]

are both proper ideals of \( \mathcal{O} = [\tau_n, 1] \). Deuring's theorem [2, p. 42] shows that \( \varphi_{M_0}(\frac{\tau_n}{1}) \) and \( \varphi_{M_5}(\frac{\tau_n}{1}) \) are associate elements in the ring of integral algebraic numbers; one writes

\[
\varphi_{M_0}\left(\frac{\tau_n}{1}\right) \approx \varphi_{M_5}\left(\frac{\tau_n}{1}\right).
\]

It follows that the quotient \( \tilde{w}(\tau_n)^{24} \) is a unit.

If \( 5 \mid n \) but \( 25 \nmid n \), then \( \varphi_{M_0}(\frac{\tau_n}{1}) \) is again a proper \( \mathcal{O} \)-ideal. However, the multiplicator ring for \( M_5(\frac{\tau_n}{1}) \) is not \( \mathcal{O} \), but \([5\tau_n, 1]\). Deuring's formulas [2, p. 43] yield

\[
\varphi_{M_0}(\frac{\tau_n}{1}) \approx 5^6 \text{ in } \mathcal{O} \quad \text{and} \quad \varphi_{M_1}(\frac{\tau_n}{1}) \approx 5^{6/5} \text{ in } [5\tau_n, 1].
\]

We find \( \tilde{w}(\tau_n) \approx 5^{1/5} \).

When \( n \) is divisible by 25, the multiplicator rings for \( M_0(\frac{\tau_n}{1}) \) and \( M_5(\frac{\tau_n}{1}) \) are \( \mathcal{O} \) and \([1, \tau_n/5]\) respectively. In this case, the formulas [2, p. 43] show that \( \tilde{w}(\tau_n) \) is again associated to a positive rational power of 5.

When \( n \in \mathbb{Z} \) is not divisible by 5, the Galois action \( (6) \) for the matrix \( g_{\tau_n}(\tau_n) \) of (19) sends \( \tilde{w} \) to \( (\frac{n}{5}) \cdot \tilde{w}^{-1} \). We define

\[
(28) \quad v(\tau_n) = \tilde{w}(\tau_n) + \left(\frac{n}{5}\right) \tilde{w}(\tau_n)^{-1}.
\]

Clearly we have \( \tilde{w}(\tau_n) = v(\tau_n) \) when \( n \) is divisible by 5. However, if \( n > 1 \) with \( 5 \nmid n \) then \( \tilde{w}(\tau_n) \) has degree 2 over \( v(\tau_n) \). In these cases the minimum polynomial for \( \tilde{w}(\tau_n) \) satisfies

\[
(29) \quad f_Q^{\tilde{w}(\tau_n)} = X^{\deg} f_Q^{v(\tau_n)} \left( \frac{X^2 + \left(\frac{n}{5}\right)}{X} \right)
\]

with \( \deg = \deg(f_Q^{v(\tau_n)}) \). Table 2 lists the minimum polynomials over \( \mathbb{Q} \) for \( v(\tau_n) \) for \( 1 \leq n \leq 16 \).

5. Nested Radicals

In order to obtain nested radicals for \( R(\tau_n) \) over \( \mathbb{Q} \) it is sufficient to have a radical for \( \tilde{w}(\tau_n) \). On the imaginary axis, \( R(\tau) \) and \( w(\tau) \) and \( \tilde{w}(\tau) \) take positive real values, and when \( \text{Re}(\tau) = \frac{5}{2} \), each of the values \( R(\tau) \) and \( w(\tau) \) and \( \tilde{w}(\tau) \) are real.
negative numbers. As the conjugate of \( R(\tau) \) over \( K(w) \) is \(-1/R(\tau)\), equation (12) gives

\[
R(\tau) = \begin{cases} 
\frac{-1+w(\tau)}{2} + \sqrt{\left(\frac{1+w(\tau)}{2}\right)^2 + 1} & \text{if } n \not\equiv 3 \pmod{4} \\
\frac{-1+w(\tau)}{2} - \sqrt{\left(\frac{1+w(\tau)}{2}\right)^2 + 1} & \text{if } n \equiv 3 \pmod{4}
\end{cases}
\]

where \( \sqrt{.} \) is always the positive square root of a positive real number.

When \( n > 1 \) and \( 5 \nmid n \), the algebraic number \( \bar{w}(\tau_n) \) has degree 2 over \( \mathbb{Q}(v(\tau_n)) \). As the absolute value of \( \bar{w}(\tau_n) \) satisfies \( |\bar{w}(\tau_n)| > 2 \) when \( n > 1 \), one recovers \( \bar{w}(\tau_n) \) from \( v(\tau_n) \) as

\[
2\bar{w}(\tau_n) = \begin{cases} 
v(\tau_n) + \sqrt{v(\tau_n)^2 - 4\left(\frac{\tau}{5}\right)} & \text{if } n \not\equiv 3 \pmod{4} \\
v(\tau_n) - \sqrt{v(\tau_n)^2 - 4\left(\frac{\tau}{5}\right)} & \text{if } n \equiv 3 \pmod{4}
\end{cases}
\]

Note that the radicands in (30) are positive real numbers. This is obvious for \( \left(\frac{\tau}{5}\right) = -1 \). When \( \left(\frac{\tau}{5}\right) = 1 \), we have \( |v(\tau_n)| = |\bar{w}(\tau_n) + 1/\bar{w}(\tau_n)| > 2 \). One easily recovers \( R(\tau_n) \) from \( \sqrt{5}\cdot \bar{w}(\tau_n) = w(\tau_n) \). In the case \( n \) is divisible by 5, one simply has \( v(\tau_n) = \bar{w}(\tau_n) \).

Below, we give nested radicals for \( v(\tau_n) \) with \( 1 \leq n \leq 16 \). In many cases the radicals below have undergone some cosmetic modifications made by factorizing elements in real quadratic orders of class number one. Every root appearing in

<table>
<thead>
<tr>
<th>( n )</th>
<th>degree</th>
<th>coefficients</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1, 2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1, -2, 3, -4</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1, 1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>1, -6, 4</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>1, -10, 25, -30, 25, -10, 25, 0, 25, 0, 25</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>1, -8, -16, 28, 31</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>1, 2, 3, 9</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>1, -16, 20, -100, 25, -156, -124</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>1, -22, 54, 62, -59</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>1, -20, -75, -60, -75, -20, -25, 0, -25, 0, -25</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>1, 4, -1</td>
</tr>
<tr>
<td>12</td>
<td>6</td>
<td>1, -34, -5, -150, -75, -144, -99</td>
</tr>
<tr>
<td>13</td>
<td>6</td>
<td>1, -46, 210, -290, 905, -456, 576</td>
</tr>
<tr>
<td>14</td>
<td>8</td>
<td>1, -44, -238, 88, 520, -2508, -4978, -176, 2711</td>
</tr>
<tr>
<td>15</td>
<td>10</td>
<td>1, 5, 0, 15, 0, 5, -25, 0, -25, 0, -25</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>1, -68, 14, 328, -284</td>
</tr>
</tbody>
</table>
(30) and in our examples should be interpreted as the real positive root of its real positive argument. Our computation $v(\tau_1) = 2$ for example, leads to $w(\sqrt{-1}) = 1$ and $w(\sqrt{-5}) = \sqrt{-5}$, which gives Ramanujan’s formula (3). The value $v(\tau_3)$ also gives a trivial extension of $Q$.

$$v(\tau_1) = 2$$
$$v(\tau_3) = -1$$

For $n = 4, 6, 9, 11, 14, 16$ the degree $[Q(v(\tau_n)) : Q]$ is a power of 2. In these cases we opt for a tower of quadratic extensions in solving for $v(\tau_n)$.

$$v(\tau_4) = 3 + \sqrt{5}$$
$$v(\tau_6) = \frac{1}{2}(4 + \sqrt{10} + \sqrt{20} + \sqrt{50})$$
$$v(\tau_9) = \frac{1}{2}(11 + 5\sqrt{3} + 3\sqrt{5} + 3\sqrt{15})$$
$$v(\tau_{11}) = -2 - \sqrt{5}$$
$$v(\tau_{14}) = (1 + \frac{\sqrt{2}}{2})\left(6 + \sqrt{2} + 5\sqrt{-2} + 4\sqrt{2} + 2\sqrt{5\left(21 - 10\sqrt{2} + (15 - 2\sqrt{2})\sqrt{-11 + 8\sqrt{2}}\right)}\right)$$
$$v(\tau_{16}) = \frac{1}{2}(34 + 25\sqrt{2} + 11\sqrt{10} + 14\sqrt{5}).$$

For $n \equiv \pm 2 \pmod{5}$, the group $(\mathcal{O}/5\mathcal{O})^*$ is cyclic of order 24. If the discriminant $D$ of $\mathcal{O} = [\tau_n, 1]$ satisfies $D < -4$, then $v(\tau_n)$ generates a degree 3 extension over the ring class field $H_\mathcal{O}$. In the examples below, we choose the field tower $H_\mathcal{O}(v(\tau_n)) \supset H_\mathcal{O} \supset Q(\sqrt{-n})$ to solve for $v(\tau_n)$.

$$v(\tau_2) = \frac{1}{3}(2 + \sqrt{35 + 15\sqrt{6}} - \sqrt{35 + 15\sqrt{6}})$$
$$v(\tau_7) = \frac{1}{3}\left(-4 + \sqrt{20(-41 + 9\sqrt{21})} - \sqrt{20(41 + 9\sqrt{21})}\right)$$
$$v(\tau_9) = \frac{1}{3}\left(8 + 5\sqrt{2} + \sqrt{\frac{1}{8}(782 + 565\sqrt{2} + 3\sqrt{6(7771 + 5490\sqrt{2})}}\right)$$
$$+ \sqrt{\frac{1}{8}(782 + 565\sqrt{2} - 3\sqrt{6(7771 + 5490\sqrt{2})}})\right)$$
$$v(\tau_{12}) = \frac{1}{3}(17 + 10\sqrt{3} + 4\sqrt{260 + 150\sqrt{3}} + \sqrt{23975 + 13875\sqrt{3}})$$
$$v(\tau_{13}) = \frac{1}{3}\left(23 + 5\sqrt{13} + \sqrt{\frac{1}{8}(14123 + 3905\sqrt{13} + 9\sqrt{274434 + 76110\sqrt{13}})}\right)$$
$$+ \sqrt{\frac{1}{8}(14123 + 3905\sqrt{13} - 9\sqrt{274434 + 76110\sqrt{13}})}\right)$$

When $n$ is divisible by 5, the value of $v$ at $\tau_n$ generates a field extension of degree 5 over the ring class field for $\mathcal{O} = [\tau_n, 1]$. In applying the algorithm of section 3, our first step solves for $v(\tau_n)$ over $H_\mathcal{O}$.

$$v(\tau_5) = 1 + \frac{1}{\sqrt{5}}(\sqrt[3]{a_1} + \sqrt[3]{a_2} + \sqrt[3]{a_3} + \sqrt[3]{a_4}),$$
where
SINGULAR VALUES OF THE ROGERS-RAMANUJAN CONTINUED FRACTION

\[ a_1, a_2 = 10 \left( 55 + 25\sqrt{5} \pm \sqrt{5050 + 2258\sqrt{5}} \right) \]
\[ a_3, a_4 = \frac{5}{2} \left( 55 + 25\sqrt{5} \pm \sqrt{50 + 22\sqrt{5}} \right) \]

\[ v(\tau_{10}) = \frac{1}{5} \left( 5 + 2\sqrt{5} + \sqrt[4]{a_1} + \sqrt[4]{a_2} + \sqrt[4]{a_3} + \sqrt[4]{a_4} \right), \text{ where} \]
\[ a_1, a_2 = 20 \left( 5(3 + \sqrt{5})(16 + \sqrt{5})(9 + 4\sqrt{5}) \pm 51 \left( \frac{1 + \sqrt{5}}{2} \right)^6 \sqrt{2(5 + 2\sqrt{5})} \right) \]
\[ a_3, a_4 = 5 \left( \frac{1 + \sqrt{5}}{2} \right)^{12} (22 - 3\sqrt{5}) \pm 3 \left( \frac{1 + \sqrt{5}}{2} \right)^6 \sqrt{2(5 + 2\sqrt{5})} \]

\[ v(\tau_{15}) = -\frac{1}{5} \left( \frac{1}{3} (5 + 5\sqrt{5}) + \sqrt[4]{a_1} + \sqrt[4]{a_2} + \sqrt[4]{a_3} + \sqrt[4]{a_4} \right), \text{ where} \]
\[ a_1, a_2 = \frac{125}{4} \left( 5(25 + 13\sqrt{5}) \pm 14 \sqrt[4]{\frac{15}{2} (25 + 11\sqrt{5})} \right) \]
\[ a_3, a_4 = \frac{125}{4} \left( 5(15 + 7\sqrt{5}) \pm 2 \sqrt[4]{\frac{15}{2} (25 + 11\sqrt{5})} \right) \]

REFERENCES

2. M. Deuring, Die Klassenkörper der komplexen Multiplikation, Enzyklopädie der Math. Wiss., Band 1,2, Teil, Heft 10, Teil II.
3. A.C.P. Gee, This thesis.
8. D.S. Kubert and S. Lang, Modular Units, Springer Grundlehren 244, 1981.

Submitted June 13, 1999
CLASS INvariants FROM DEDEKIND'S ETA-FUNCTION

Alice Gee

Abstract. We study the Galois theoretic properties of the singular values of modular functions derived from Dedekind's eta function. This is a classical topic going back to Weber. It has regained interest in view of recent algorithmic applications.

1. Introduction

Modular functions used in complex multiplication often arise as quotients of two modular forms of equal weight. The $j$-function

$$j = \frac{E_4^3}{\Delta}$$

is a characteristic example. Here, $E_4$ is the Eisenstein series of weight 4 and the discriminant function

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}, \quad q = e^{2\pi iz}$$

has weight 12. Quotients of $\Delta$-functions are another source of examples. The values of

$$\frac{\Delta}{\Delta^o \begin{pmatrix} 1 & k \\ 0 & N \end{pmatrix}} \quad k \in \mathbb{Z}, N \in \mathbb{Z}_{>0}$$

have been studied extensively. Here, the matrix $\begin{pmatrix} 1 & k \\ 0 & N \end{pmatrix}$ acts on the complex upper half plane as $z \mapsto \frac{z+k}{N}$.

Like the $j$-function, singular values of (1) are known to generate ring class fields of imaginary quadratic fields. For an imaginary quadratic order $\mathcal{O} = [\theta, 1]$ in the number field $K = \mathbb{Q}(\theta)$, we use $H_\mathcal{O}$ to denote the ring class field for $\mathcal{O}$. If $f = X^2 + BX + C \in \mathbb{Z}[X]$ is the minimum polynomial of $\theta$, and $k \in \mathbb{Z}$ satisfies $f(-k) \equiv 0 \mod N$, then $\frac{k+k}{N}$ is a zero of

$$g = NX^2 + (B - 2k)X + f(-k)/N \in \mathbb{Z}[X].$$

1991 Mathematics Subject Classification. Primary 11Y40; Secondary 11G16.

Key words and phrases. class invariants, Dedekind eta-function.

Typeset by A\LaTeX
The number

\[ \phi = \frac{\Delta(\frac{\theta + k}{N})}{\Delta(\theta)} \]

is known to be an algebraic integer in \( H_\mathcal{O} \) which divides \( N^{12} \) [6, p. 159, 164]. Moreover, the prime factorization of \( \phi \) can be determined explicitly [2, p. 42]. By normalizing \( \phi \) with the appropriate power of \( N \), one obtains what is known as a Siegel unit in \( H_\mathcal{O} \). When \( \mathcal{O} = \mathcal{O}_K \) is a maximal order, \( g \) is the irreducible polynomial in \( \mathbb{Z}[X] \) for \( \frac{\theta + k}{N} \), and \([\theta + k, N] \) is a \( \mathbb{Z} \)-basis for a proper primitive ideal of norm \( N \) in \( \mathcal{O}_K \). If \([\theta + k, N] \) is not a principal ideal then \( \phi \) generates the Hilbert class field \( H_\mathcal{O} \) over \( K \) [11, Cor. 1].

In the case that \( \mathcal{O} \) is not the maximal order, one can obtain a generator for the ring class field \( H_\mathcal{O} \). For non-maximal orders \( \mathcal{O} \), let \( r \) denote the greatest common divisor of the coefficients of \( g \). The \( \mathbb{Z} \)-lattice \([\theta + k, N] \) is a proper ideal of the order \( \mathcal{O}' \) of discriminant \( D/r^2 \). If this ideal is non-principal and prime to \([\mathcal{O}_K : \mathcal{O}'] \), then \( \phi \) generates \( H_{\mathcal{O}'} \) over \( K \) [11, Cor. 1]. In particular, when the coefficients of \( g \) are relatively prime we get a generator for \( H_\mathcal{O} \).

The 24th root

\[ \eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n), \quad q = e^{2\pi i z}, \]

of \( \Delta \) is a holomorphic function on the complex upper half plane. The singular values of the \( \eta \)-quotients that are 24th roots of (2) are again algebraic integers. Weber discovered that the degree of these algebraic integers over \( \mathbb{Q} \) is sometimes not much larger than the degrees of the corresponding \( \Delta \)-quotients. He used the so-called Weber functions

\[ f(z) = \zeta_{48} \frac{\eta(\frac{z+1}{2})}{\eta(z)}, \quad f_1(z) = \frac{\eta(\frac{z}{2})}{\eta(z)}, \quad f_2(z) = \sqrt{2} \frac{\eta(2z)}{\eta(z)} \]

to provide "small" generators of certain class fields. As shown in the first chapter of this thesis, a small power of a suitably normalized Weber function can be used to generate the ring class field \( H_\mathcal{O} \) over \( K \) whenever 2 is not inert in \( \mathcal{O} \). The specific Weber function is given in table 1 below. In the table, we assume that the \( \mathbb{Z} \)-basis for \( \mathcal{O} = [\theta, 1] \) is chosen with \( \theta \) in the complex upper half plane and \( \text{Tr}_{K/\mathbb{Q}}(\theta) \in \{-1, 0\} \). If \( \mathcal{O} \) has discriminant \( D \), we get an integral generator for \( H_\mathcal{O} \) by evaluating at \( \theta \) one of the functions in table 1.
In view of table 1, it is natural to ask whether small powers of the generalized Weber functions

$$\nu_{N,0} = \sqrt{N} \cdot \frac{\eta^o(N,0)}{\eta}$$

and

$$\nu_{k,N} = \frac{\eta^o(1,0,1)}{\eta^k}$$

$k \in \mathbb{Z}, N \in \mathbb{Z}_{>0}$

for $N > 2$ can be used to generate ring class fields. In the case $N = 3$ we put

$$g_0(z) = \frac{\eta^o(3)}{\eta(z)} \quad g_1(z) = \frac{\eta^o(4)}{\eta(z)} \quad g_2(z) = \frac{\eta^o(6)}{\eta(z)} \quad g_3(z) = \sqrt{3} \frac{\eta(3z)}{\eta(z)}$$

Like Weber's functions, which satisfy $f_1 f_2 = \sqrt{2}$ and

$$(X + f_2^2)(X - f_2^2)(X - f_1^2) = X^3 + 48X^2 + (768 - j)X + 2^{12},$$

our functions satisfy $g_0 g_1 g_2 g_3 = \sqrt{3}$ and

$$\prod_{k=0}^{3} (X - g_k^{12}) = X^4 + 36X^3 + 270X^2 + (756 - j)X + 3^6$$

according to [15, p. 255]. In section 3 we prove the following theorem. For simplicity we only consider fundamental discriminants for $N = 3$.

**Theorem 1.** Let $\mathcal{O} = \mathcal{O}_K = [\theta, 1]$ be the maximal order of the imaginary quadratic number field of discriminant $D$. We take $\text{Tr}_K/\mathbb{Q}^+(\theta) \in \{-1, 0\}$ with $\theta \in \mathbb{H}$. Evaluating the function in table 2 at $\theta$ gives an integral generator for $H_\mathcal{O}$ over $K$.

**Table 2. Class invariants from $g_0, g_1, g_2, g_3$**

<table>
<thead>
<tr>
<th>$D \equiv 1(4)$</th>
<th>$D \equiv 4(4)$</th>
<th>$D \equiv 7(4)$</th>
<th>$D \equiv 3(9)$</th>
<th>$D \equiv 6(9)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$g_0^2, g_0^4$</td>
<td>$g_0^2, g_0^4$</td>
<td>$g_0^2, g_0^4$</td>
<td>$\frac{1}{3\sqrt{-3}} g_0^6, \frac{1}{-3} g_0^2$</td>
<td>$\frac{1}{3\sqrt{-3}} g_0^6, \frac{1}{-3} g_0^2$</td>
</tr>
<tr>
<td>$g_0^2, g_0^4$</td>
<td>$g_0^2, g_0^4$</td>
<td>$g_0^2, g_0^4$</td>
<td>$\frac{1}{3\sqrt{-3}} g_0^6, \frac{1}{-3} g_0^2$</td>
<td>$\frac{1}{3\sqrt{-3}} g_0^6, \frac{1}{-3} g_0^2$</td>
</tr>
<tr>
<td>$g_0^2, g_0^4$</td>
<td>$g_0^2, g_0^4$</td>
<td>$g_0^2, g_0^4$</td>
<td>$\frac{1}{3\sqrt{-3}} g_0^6, \frac{1}{-3} g_0^2$</td>
<td>$\frac{1}{3\sqrt{-3}} g_0^6, \frac{1}{-3} g_0^2$</td>
</tr>
</tbody>
</table>

**Table 1. Class invariants from $f, f_1, f_2$**

<table>
<thead>
<tr>
<th>$D \equiv 1(8)$</th>
<th>$D \equiv 2(8)$</th>
<th>$D \equiv 5(8)$</th>
<th>$D \equiv 6(8)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\zeta_3$</td>
<td>$\zeta_3^2$</td>
<td>$\zeta_3$</td>
<td>$\zeta_3^2$</td>
</tr>
<tr>
<td>$\zeta_3^2$</td>
<td>$\zeta_3$</td>
<td>$\zeta_3^2$</td>
<td>$\zeta_3$</td>
</tr>
<tr>
<td>$\zeta_3$</td>
<td>$\zeta_3^2$</td>
<td>$\zeta_3$</td>
<td>$\zeta_3^2$</td>
</tr>
<tr>
<td>$\zeta_3^2$</td>
<td>$\zeta_3$</td>
<td>$\zeta_3^2$</td>
<td>$\zeta_3$</td>
</tr>
</tbody>
</table>
For $N > 3$, Hajir and Villegas [4, Thm 20.1] consider invertible $\mathcal{O}$-ideals $[\theta + k, N]$ co-prime to $6D$. They determine a 24th root of unity $\zeta$ and an exponent $e$ dividing 12 for which

$$\zeta \cdot \nu_{k,N}^e(\theta) \in H_\mathcal{O}$$

holds. Here $e$ is equal to the number of 12th roots of unity contained in $H_\mathcal{O}$. One encounters $\zeta_3 \in H_\mathcal{O}$ if and only if $3$ divides the discriminant $D$ of $\mathcal{O}$. Similarly, $\zeta_4 \in H_\mathcal{O}$ occurs for $D \equiv 0, 12 \mod 16$. Clearly, we want $e$ to be as small as possible in order to obtain small class invariants. By restricting the choice of $N$ one can always work with the minimal value $e = 2$.

**Theorem 2.** Let $\mathcal{O} = [\theta, 1]$ be an imaginary quadratic order of discriminant $D$ and let $f = X^2 + BX + C \in \mathbb{Z}[X]$ be the minimum polynomial for $\theta$ over $\mathbb{Q}$. Translating $\theta$ by an integer if necessary, assume $B \in \{0, 1\}$. Let $N \in \mathbb{Z}_{>0}$ be co-prime to $6$ and satisfy

$$N - 1 \equiv 0 \mod 2 \cdot \gcd(D, 6).$$

If $k \in \mathbb{Z}$ satisfies

$$f(-k) \equiv 0 \mod N \quad \text{and} \quad k \equiv 0 \mod 24,$$

then $\zeta_3^{2B(N-1)} \nu_{k,N}^2(\theta)$ lies in $H_\mathcal{O}$.

In the case $N = p$ is a prime number, the existence of $k \in \mathbb{Z}$ such that $f(-k) \equiv 0 \mod p$ means that the prime $p$ is split or ramified in $\mathcal{O}$. An even discriminant $D$ in the previous lemma poses a restriction on our choice for $N$. A slightly weaker restriction applies in the cases $D \equiv 0 \mod 16$ and $D \equiv 12 \mod 16$.

**Proposition 3.** Let $\mathcal{O} = [\theta, 1]$ to be the imaginary quadratic order of discriminant $D$, with $D \equiv 4 \mod 16$ or $D \equiv 8 \mod 16$. Translating $\theta$ if necessary, we assume that $\theta$ has minimum polynomial $f = X^2 + C \in \mathbb{Z}[X]$. Suppose $N > 0$ is prime to 6 and $k$ is divisible by 24. If the congruences

$$N - 1 \equiv 0 \mod \gcd(D, 3) \quad \text{and} \quad f(-k) \equiv 0 \mod N$$

are satisfied then $\zeta_4^{(N-1)/2} \cdot \nu_{k,N}^2(\theta)$ is contained in $H_\mathcal{O}$.

**Remark.** When the value $x = \zeta_3^{B(N-1)} \nu_{k,N}^2(\theta)$ of theorem 2 lies in $H_\mathcal{O}$, one can determine instances for which $x$ generates $H_\mathcal{O}$ over $K$ from the instances for which the value $\phi = x^{12}$ of (2) is a generator.

More generally, one can form functions $\nu_{k,l} \cdot \nu_{k,n}$ with $l$ and $n$ different and both coprime to 6. Because the norm of the singular values of $\nu_{k,n}$ is a power of $n$, it is convenient to use the quotient

$$\frac{\nu_{k,l} \cdot \nu_{k,n}}{\nu_{k,ln}}$$
that is used in recent papers of Schertz [10] to make units in ring class fields. Numbers \(e, l, n \in \mathbb{Z}\) are determined in [1, p. 321] for which singular values of
\[
\left( \nu_{k,l} \cdot \nu_{k,n} \right)^e
\]
can be used to generate ring class fields. There, the condition \(24 \mid e(l - 1)(n - 1)\) must be satisfied. In many cases, this exponent can be reduced so that we can work with the minimum value \(e = 1\).

**Theorem 4.** Let \(\mathcal{O} = [\theta, 1]\) be an imaginary quadratic order of discriminant \(D\) and let \(f = X^2 + BX + C \in \mathbb{Z}[X]\) be the minimum polynomial for \(\theta\) over \(\mathbb{Q}\). We assume \(B \in \{0, 1\}\). Let \(l, n \in \mathbb{Z}_{>0}\) be relatively prime to \(6\) and suppose \(k \in \mathbb{Z}\) satisfies
\[
f(-k) \equiv 0 \mod ln \quad \text{and} \quad k \equiv 0 \mod 24.
\]
If \(l\) and \(n\) are chosen so that
\[
(l - 1)(n - 1) \equiv 0 \mod 4 \cdot \gcd(D, 6)
\]
then
\[
\rho = \zeta_3^y \nu_{k,l} \cdot \nu_{k,n} (\theta)
\]
is an element of \(H_\mathcal{O}\). Here, the exponent \(y\) is defined as
\[
y = \begin{cases} 
2 & \text{if } B = 1 \text{ and } l \equiv n \equiv 2 \mod 3 \\
0 & \text{otherwise.}
\end{cases}
\]

**Remark.** Suppose \(D\) is a fundamental discriminant and \(\mathcal{O} = \mathcal{O}_K\) is the order of discriminant \(D\). If the proper \(\mathcal{O}\)-ideals \([\theta + k, l]\) and \([\theta + k, n]\) are both non-principal and together generate a subgroup of the ideal class group that is not of type \(C_2 \times C_2\), then it follows from [1, p. 320] that (6) generates \(H_\mathcal{O}\) over \(K = \mathbb{Q}(\sqrt{D})\). This condition can always be met if we exclude a few small \(D\). For these discriminants, the order of the class group is at most 2, so \(H_\mathcal{O}\) is trivially generated.

The proofs of theorems 1, 2, and 4 are applications of the Shimura reciprocity law. In section 2, we show that the functions \(\nu_{k,N}\) are elements of \(F_{24N}\), the modular function field of level \(24N\) over \(\mathbb{Q}(\zeta_{24N})\) and we describe the group action of \(GL_2(\mathbb{Z}/24NZ)\) on \(\nu_{k,N}\). In sections 3 and 4, we look at singular values of the functions occurring in theorems 1, 2 and 4. We determine whether they are contained in the ring class field for \(\mathcal{O} = [\theta, 1]\). Theorem 4 leaves us with a choice of parameters \(n, l\) and \(k\) when picking a generator (6) for \(H_\mathcal{O}\). In section 6, we discuss how the minimum polynomial for (6) is affected when we let the \(\mathcal{O}\)-ideals \([\theta + k, n]\) and \([\theta + k, l]\) vary and give some numerical examples.
2. Modularity of $\eta$-Quotients

We study the modularity properties of the generalized Weber functions $\nu_{k,N}$ and $\nu_{N,0}$ of (4). We say that a meromorphic function $h = h(z)$ on $\mathbb{H}$ is in the modular function field $F_N$ if it is invariant under

$$\Gamma(N) = \ker[\text{SL}_2(\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}/N\mathbb{Z})],$$

and has a Fourier expansion in the variable $q^N = e^{2\pi iz/N}$ with coefficients in $\mathbb{Q}(\zeta_N)$. Also, $h$ should satisfy a growth condition at the cusps of $\mathbb{H}/\Gamma(N)$. Namely, for every $M \in \text{SL}_2(\mathbb{Z})$, the Fourier expansion for $h \circ M$ should have only finitely many negative terms.

**Theorem 5.** The functions $\nu_{k,N}$ and $\nu_{N,0}$ with $k \in \mathbb{Z}$ and $N \in \mathbb{Z}_{>0}$ are elements of the modular function field $F_{24N}$.

It is often possible to lower the level from $24N$ to $N$ by considering suitable products of the functions $\nu_{k,N}$. We prove the following analogue of a result [8, Thm. 1] of Newman.

**Theorem 6.** We suppose $(N,6) = 1$ and $k \equiv 0 \mod 24$. Let $\{r_n\}$ be a sequence of integers indexed by the positive divisors $n$ of $N > 0$. We have

$$\sum_{n|N}(n - 1)r_n \equiv 0 \mod 24 \iff \prod_{n|N}(\nu_{k,n})^{r_n} \in F_N.$$

Applying theorem 6 to the case $N = ln$ with $r_l = r_n = 1$ and $r_{ln} = -1$ we get the function

$$\frac{\nu_{k,l} \cdot \nu_{k,n}}{\nu_{k,ln}}.$$

The observation $(l - 1) + (n - 1) - (ln - 1) = -(l - 1)(n - 1)$ gives the next corollary.

**Corollary 7.** Suppose $l$ and $n$ are positive integers prime to 6. If $(l - 1)(n - 1)$ is divisible by 24 we have

$$\frac{\nu_{k,l} \cdot \nu_{k,n}}{\nu_{k,ln}} \in F_{ln}.$$

Also, for $l$ and $n$ prime to 6 we have

$$l + n \equiv 2 \mod 24 \quad \Rightarrow \quad \nu_{k,l} \cdot \nu_{k,n} \in F_{ln}$$

and

$$e(n - 1) \equiv 0 \mod 24 \quad \Rightarrow \quad \nu_{k,n} \in F_n.$$

Because the $\eta$-function is itself holomorphic and without zeroes on the upper half plane, the same holds true for the $\eta$-quotients occurring in (4). An inspection of (3) shows that the Fourier coefficients of $\nu_{N,0}$ lie in $\mathbb{Q}$, and from

$$\eta(\frac{z + k}{N}) = \zeta^k_{24N} \cdot q^{1/24N} \prod_{m=1}^{\infty}(1 - \zeta^{km}q^{m/N}),$$
one sees that \( \nu_{k,N} \) has Fourier coefficients in \( \mathbb{Q}(\zeta_{24N}) \).

The action of the modular group \( \text{SL}_2(\mathbb{Z}) \) on \( \nu_{k,N} \) and \( \nu_{N,0} \) can be derived from the transformation formulas for the generators \( S = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \) and \( T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) of \( \text{SL}_2(\mathbb{Z}) \) acting on \( \eta \). From the classical formulas

\[
\eta \circ T(z) = \zeta_{24} \eta(z) \quad \text{and} \quad \eta \circ S(z) = \zeta_8^{-1} \sqrt{z} \eta(z)
\]

we see that the generalized Weber functions satisfy the growth condition at the cusps. Namely, for \( M \in \text{SL}_2(\mathbb{Z}) \), a singularity at \( \infty \) for \( \nu_{N,0} \circ M \) or \( \nu_{k,N} \circ M \) is at worst a pole. We derive

\[
\nu_{N,0} = \nu_{0, N} \circ S \quad \text{and} \quad \zeta_{24}^{-k} \nu_{k,N} = \nu_{0, N} \circ T^k.
\]

From \( \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \cdot S = S \cdot \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \) we get

\[
\nu_{0,N} \circ S(z) = \frac{\eta \circ \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \cdot S(z)}{\eta \circ S(z)} = \frac{\eta \circ S(Nz)}{\eta \circ S(z)} = \frac{\zeta_8^{-Nz} \cdot \eta(Nz)}{\zeta_8^{-1} \sqrt{z} \cdot \eta(z)} = \nu_{N,0}(z).
\]

Similarly for \( \nu_{k,N} \), the identity \( \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \cdot T^k = \begin{pmatrix} 1 & k \\ 0 & N \end{pmatrix} \) gives

\[
\nu_{0,N} \circ T^k = \frac{\eta \circ \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \cdot T^k}{\eta \circ T^k} = \frac{\eta \circ \begin{pmatrix} 1 & k \\ 0 & N \end{pmatrix}}{\zeta_{24}^k \cdot \eta} = \zeta_{24}^{-k} \nu_{k,N}.
\]

In order to prove theorem 5, it suffices to show that our generalized Weber functions (4) are invariant under the modular action of \( \Gamma(24N) \). As \( \Gamma(24N) \) is a normal subgroup of \( \text{SL}_2(\mathbb{Z}) \), the invariance of \( \nu_{k,N} \) and \( \nu_{N,0} \) under \( \Gamma(24N) \) can be derived from the \( \Gamma(24N) \)-invariance of the single function \( \nu_{0,N} \).

**Lemma 8.** The function \( \nu_{0,N} \) is \( \Gamma(24N) \)-invariant.

We calculate the explicit action of \( \Gamma(24N) \) on \( \nu_{0,N} \) using Meyer's formula [7], which describes the transformation of \( \eta \) under the action of \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \).

Meyer gives functions \( \varepsilon_1 = \varepsilon_1(M) \) and \( \varepsilon_2 = \varepsilon_2(M) \) such that

\[
\eta \circ M(z) = \varepsilon_1 \cdot \varepsilon_2 \cdot \sqrt{cz + d} \cdot \eta(z)
\]

holds. Replacing \( M \) by \( -M \) if necessary, we assume \( c \geq 0 \). If \( c = 0 \), then we assume \( d > 0 \). Then for \( z \in \mathbb{H} \) we have \( cz + d \in \mathbb{H} \cup \mathbb{R}_{>0} \), and we fix the branch of the square root \( \sqrt{cz + d} \) to be in \( \mathbb{H} \cup \mathbb{R}_{>0} \). If \( c > 0 \), let \( c_0, r \in \mathbb{Z} \) be integers with \( c = 2^r \cdot c_0 \) and \( c_0 \) odd. In the case \( c = 0 \), we set \( c_0 = r = 1 \). Then

\[
\varepsilon_1(M) = \begin{pmatrix} a \\ c_0 \end{pmatrix} \quad \text{and} \quad \varepsilon_2(M) = \zeta_{24}^{ab + cd(1-a^2) - ca + 3c_0(a-1) + r \frac{3}{2}(a^2 - 1)}.
\]
are the factors in formula (7). Fixing the square root in (7) has the unfortunate consequence of making neither \( \varepsilon_1 \), nor \( \varepsilon_2 \), nor their product a group homomorphism on \( \text{SL}_2(\mathbb{Z}) \). Nonetheless, observe that \( \varepsilon_2(M) = 1 \) holds whenever \( M \equiv I \mod 24 \).

The transformation behaviour of \( \eta^2 \), which does not involve a choice of square roots is much nicer. In [4], Hajir and Villegas exhibit a character

\[
\chi : \text{SL}_2(\mathbb{Z}/12\mathbb{Z}) \to \mu_{12}
\]

with the property

\[
(\eta^2 \circ M)(z) = \chi(M) \cdot (c z + d) \cdot \eta^2(z), \quad \text{with } \overline{M} = M \mod 12.
\]

**Proof of lemma 8.** Let \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \) such that \( M \equiv \pm I \mod 24N \). Replacing \( M \) with \(-M\) if necessary, one can assume \( c > 0 \), or \( c = 0 \) with \( d > 0 \).

Define

\[
M' = \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}^{-1} = \begin{pmatrix} a & b/N \\ cN & d \end{pmatrix}
\]

so that

\[
\nu_{0,N} \circ M = \frac{\eta \circ \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \cdot M}{\eta \circ M} = \frac{\eta \circ M' \cdot \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}}{\eta \circ M}
\]

holds. Meyer's formula gives

\[
\frac{\eta \circ M'(z/N)}{\eta \circ M(z)} = \frac{\varepsilon_1(M')}{\varepsilon_1(M)} \frac{\varepsilon_2(M')}{\varepsilon_2(M)} \frac{\sqrt{cz + d}}{\eta(z/N)} = \frac{\varepsilon_1(M')}{\varepsilon_1(M)} \frac{\varepsilon_2(M')}{\varepsilon_2(M)} \frac{\sqrt{cz + d}}{\eta(z)}.
\]

If \( c = 0 \), the formulas (7) easily give \( \varepsilon_1(M) = \varepsilon_1(M') \) and \( \varepsilon_2(M) = \varepsilon_2(M') \) under the assumption \( b, c \equiv 0 \mod 24N \). On the other hand, if \( c > 0 \), set \( c_0, r \in \mathbb{Z} \) with \( c_0 \) odd such that \( c = 2^r \cdot c_0 \). Also take \( u, N_0 \in \mathbb{Z} \) with \( N_0 \) odd so that \( N = 2^u \cdot N_0 \) is satisfied. In the case \( M \equiv I \mod 24N \) we have \( M' \equiv M \equiv I \mod 24N \) and

\[
\frac{\varepsilon_1(M')}{\varepsilon_1(M)} = \left( \frac{a}{N_0} \right) = \left( \frac{1}{N_0} \right) = 1 \quad \text{and} \quad \frac{\varepsilon_2(M)}{\varepsilon_2(M')} = \frac{\varepsilon_2(M)}{\varepsilon_2(M')} = 1.
\]

On the other hand, in the case \( M \equiv -I \mod 24N \) we have

\[
\frac{\varepsilon_1(M')}{\varepsilon_1(M)} = \left( \frac{a}{N_0} \right) = \left( \frac{-1}{N_0} \right) \quad \text{and} \quad \frac{\varepsilon_2(M')}{\varepsilon_2(M)} = \frac{\varepsilon_2(M)}{\varepsilon_2(M')} = \frac{3^{c_0}N_0(a-1)}{\zeta_{24}^{-1}N_0(a-1)} = (\pm \zeta_4)^{(N_0-1)}.
\]

Either way, the equality \( \nu_{0,N} \circ M = \nu_{0,N} \) follows. \( \square \)

We now show that the functions in theorem 6 are \( \Gamma(N) \)-invariant. First we study the action of matrices having a special form.
Lemma 9. Let \( U = (\frac{a}{c} \quad \frac{b}{d}) \) \( \in \Gamma(N) \) be a matrix for which \( c > 0 \) holds. Define \( \kappa(U) \in \mathbb{Z} \) as

\[
\kappa(U) = ab + cd(1 - a^2) - ca + 3c_0 \cdot (a - 1), \quad c = 2^r c_0 \text{ and } 2 \nmid c_0
\]

If \( k \equiv 0 \mod 24 \) and \( n \) is a positive divisor of \( N \), then the composition of \( \nu_{k,n} \) with \( U \) is

\[
\nu_{k,n} \circ U = \zeta_{24}^{\kappa(U) \cdot (n-1)} \nu_{k,n}.
\]

Proof. Under the hypothesis \( U \in \Gamma(N) \), the matrix

\[
U_n = \left( \begin{array}{cc} 1 & k \\ 0 & n \end{array} \right) \cdot U \cdot \left( \begin{array}{cc} 1 & k \\ 0 & n \end{array} \right)^{-1} = \left( \begin{array}{cc} a + kc & \frac{b + kd - (a + kc)k}{n - dc} \\ c & d - kc \end{array} \right)
\]

has integral coefficients because of the congruence \( b + kd - (a + kc)k \equiv 0 \mod N \).

We apply Meyer's formula to both \( U, U_n \in SL_2(\mathbb{Z}) \) to compute

\[
\nu_{k,n} \circ U = \frac{\eta \circ \left( \begin{array}{cc} 1 & k \\ 0 & n \end{array} \right) \cdot U}{\eta \circ U} = \frac{\eta \circ U_n \cdot \left( \begin{array}{cc} 1 & k \\ 0 & n \end{array} \right)}{\eta \circ U}
\]

and obtain

\[
\frac{\eta \circ U_n(z)}{\eta \circ U(z)} = \frac{\varepsilon_1(U_n) \cdot \varepsilon_2(U_n) \sqrt{cz + d} \eta(\frac{z + k}{n})}{\varepsilon_1(U) \cdot \varepsilon_2(U) \sqrt{cz + d} \eta(z)}.
\]

We contend \( \varepsilon_1(U)/\varepsilon_1(U_n) = 1 \) because \( U \in \Gamma(N) \) gives congruences \( c \equiv 0 \mod n \) and \( a \equiv 1 \mod n \). These imply

\[
\varepsilon_1(U_n) = \left( \frac{a + kc}{nc} \right) = \left( \frac{a + kc}{n} \right) \left( \frac{a}{c} \right) = \left( \frac{a}{c} \right) = \varepsilon_1(U).
\]

The quantities \( \varepsilon_2(U) \) and \( \varepsilon_2(U_n) \) are 24th roots of unity that depend only upon the coefficients of \( U \) and \( U_n \mod 24 \). From the congruences \( k \equiv 0 \mod 24 \) and \( n^2 \equiv 1 \mod 24 \) we get \( U_n \equiv \left( \begin{array}{cc} a & nb \\ nc & d \end{array} \right) \mod 24 \), and we compute

\[
\frac{\varepsilon_2(U_n)}{\varepsilon_2(U)} = \zeta_{24}^{\left( ab + cd(1 - a^2) - ca + 3c_0(a - 1) \right)(n-1)}.
\]

where \( c = 2^r c_0 \) with \( 2 \nmid c_0 \). This is precisely the root of unity \( \zeta_{24}^{\kappa(U) \cdot (n-1)} \). \( \square \)

The modular function field \( F_N \) is Galois over \( F_1 \) with group

\[
\text{Gal}(F_N/F_1) \simeq \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}.
\]

The action of the subgroup \( SL_2(\mathbb{Z}/N\mathbb{Z}) \) is induced by the modular transformation of \( SL_2(\mathbb{Z}) \). The matrices having the special form \( \left( \begin{array}{cc} 1 & 0 \\ 0 & d \end{array} \right) \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \), act
as $\zeta_N \mapsto \zeta_N^d$ on the Fourier coefficients of functions in $F_N$. In particular, for $\nu_{k,N} \in F_{24N}$ the action of $(\begin{smallmatrix} 1 & 0 \\ 0 & d^2 \end{smallmatrix}) \in \text{GL}_2(\mathbb{Z}/24\mathbb{N})$ is

$$
(10) \quad \left( \begin{array}{cc} 1 & 0 \\ 0 & d^2 \end{array} \right) : \nu_{k,N} \mapsto \nu_{kd,N}
$$

When $N$ and $d$ are relatively prime, the subfield $F_N \subset F_{24N}$ is the fixed field of

$$
G = \ker[\text{GL}_2(\mathbb{Z}/24\mathbb{N}) \to \text{GL}_2(\mathbb{Z}/\mathbb{N})].
$$

We prove that the functions in theorem 6 are stable under $G$.

**Proof of theorem 6.** Given $M \in G$, we write

$$
M = \left( \begin{array}{cc} 1 & 0 \\ 0 & \det(M)^{-1} \end{array} \right) \cdot \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right) \quad \text{with} \quad \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right) \in \text{SL}_2(\mathbb{Z}/24\mathbb{N}).
$$

When $k \equiv 0 \pmod{24}$, the Fourier expansion of $\nu_{k,N}$ has coefficients in $\mathbb{Q}(\zeta_L)$. Because $\det(M) \equiv 1 \pmod{N}$, the matrix $(\begin{smallmatrix} 1 & 0 \\ 0 & \det(M) \end{smallmatrix})$ acts trivially on $\nu_{k,N}$. For the second factor $(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}) \in \text{SL}_2(\mathbb{Z}/24\mathbb{N})$, we determine a lift $U = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \text{SL}_2(\mathbb{Z})$. Here, we can assume $c > 0$ because if $c \leq 0$ one replaces $U$ with

$$
(11) \quad \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \cdot \left( \begin{array}{cc} 1-24N & \mp 24N \\ \pm 24N & 1+24N \end{array} \right) = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right) \left( \begin{array}{cc} c' & 0 \\ 0 & \omega \end{array} \right)
$$

where the new coefficient $c' = c(1 - 24N) \pm 24dN$ satisfies $c' > 0$. Lemma 9 gives

$$
\left( \prod_{n \mid N} \nu_{k,n}^r \right)^M = \prod_{n \mid N} \zeta_4^{\kappa(U) \cdot (n-1) r_n} \nu_{k,n}^{r_n}.
$$

Clearly the condition $\sum_{n \mid N} (n-1) r_n \equiv 0 \pmod{24}$ implies that both $U$ and $M$ act trivially on $\prod_{n \mid M} \nu_{k,n}^{r_n}$. This condition is in fact necessary for $\prod_{n \mid N} \nu_{k,n}^{r_n}$ to be $\Gamma(N)$-invariant. Namely, if we take $U = (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}) \in \Gamma(N)$ with $x \equiv 1 \pmod{24}$ we get $\kappa(U) \equiv -1 \pmod{24}$.

## 3. Shimura reciprocity law

Let $[\theta, 1]$ be a $\mathbb{Z}$-basis for an imaginary quadratic order $\mathcal{O}$ of discriminant $D$. If $h \in F_N$ is an element of the modular function function field of level $N$ over $\mathbb{Q}(\zeta_N)$, the first main theorem of complex multiplication tells us that $h(\theta)$ is an element of $H_{N, \mathcal{O}}$, the ray class field of conductor $N$ over the ring class field $H_{\mathcal{O}}$ [14, §4].

The group $\text{Gal}(H_{N, \mathcal{O}}/H_{\mathcal{O}})$ fits into the short exact sequence

$$
(12) \quad 1 \rightarrow \mathcal{O}^* \rightarrow (\mathcal{O}/\mathcal{N}\mathcal{O})^* \rightarrow \text{Gal}(H_{N, \mathcal{O}}/H_{\mathcal{O}}) \rightarrow 1.
$$
The automorphism of $H_{N,\mathcal{O}}$ induced by $x \in (\mathcal{O}/N\mathcal{O})^*$ under the Artin map $A$ can be described with the help of the Shimura reciprocity law. We write elements of $\mathcal{O}/N\mathcal{O}$ in terms of the $\mathbb{Z}/NZ$-basis $[\theta, 1]$. If $\theta$ has minimum polynomial $X^2 + BX + C \in \mathbb{Z}[X]$, define the homomorphism

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

$$s\theta + t \mapsto \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix}.$$  

When $x = s\theta + t \in \mathcal{O}/N\mathcal{O}$ is represented as the row vector $(s, t) \in (\mathbb{Z}/NZ)^2$, the matrix $g_\theta(x)$ represents multiplication by $x$ on $\mathcal{O}/N\mathcal{O}$. For $h \in F_N$, the Shimura reciprocity law [13] says that the action of $x \in (\mathcal{O}/N\mathcal{O})^*$ on $h(\theta)$ is

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

with $g_\theta(x) \in \text{GL}_2(\mathbb{Z}/NZ)$ acting on $h \in F_N$ as in (9). We denote the image of $(\mathcal{O}/N\mathcal{O})^*$ under $g_\theta$ by

$$W_{N,\theta} = \left\{ \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/NZ) \mid t, s \in \mathbb{Z}/NZ \right\}.$$  

For $D < -4$ we have $\mathcal{O}^* = \{\pm 1\}$ and the exact sequence (12) gives an isomorphism

$$\text{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}}) \cong W_{N,\theta}/\{\pm 1\}.$$  

4. The case $N = 3$

In this section we prove theorem 1. Let $\mathcal{O} = \mathcal{O}_K = [\theta, 1]$ be the maximal order for $K = \mathbb{Q}(\theta)$ and let $\theta$ have minimum polynomial $X^2 + BX + C \in \mathbb{Z}[X]$ with $B \in \{0, 1\}$. When $f(-k) \equiv 0 \mod 3$ is satisfied with $k \in \{1, 2, 3\}$, the lattice $a = [\theta + k, 3]$ is a proper $\mathcal{O}$-ideal lying over 3. Deuring's tables [2, p. 43] give the prime ideal factorization of the algebraic integer $g_k^{24}(\theta) \in H_{\mathcal{O}}$.

In particular, if 3 ramifies in $K$ then $g_k^{24}$ and $(\sqrt{-3})^{12}$ both generate the same ideal in the ring of integers for $H_{\mathcal{O}}$. In order to determine whether $g_k^{24}(\theta)$ is a perfect power in $H_{\mathcal{O}}$, we examine which powers of $g_k(\theta)$ lie in $H_{\mathcal{O}}$ by computing the orbit of $g_k$ under $W_{72,\theta}$.

First, we use the Chinese remainder theorem to write

$$W_{72,\theta} = G_{72,\theta}^{(9)} \times G_{72,\theta}^{(8)}$$

where

$$G_{72,\theta}^{(9)} = \ker[W_{72,\theta} \to W_{8,\theta}] \quad \text{and} \quad G_{72,\theta}^{(8)} = \ker[W_{72,\theta} \to W_{9,\theta}].$$
By way of example, we verify the entry in table 2 for the case $D \equiv 1 \mod 9$ and $D \equiv 1 \mod 4$. Because $D$ is odd, we have $B = 1$. Since $D \equiv 1 \mod 9$, the coefficients for the irreducible polynomial for $\theta$ satisfy $(B, C) \equiv (1, 0) \mod 9$. We identify elements of $G_{72, \theta} \simeq W_{9, \theta}$ with their reduction in $GL_2(\mathbb{Z}/9\mathbb{Z})$. The prime 3 splits in $O$, so the structure of $(O/9O)^* \simeq W_{9, \theta}$ is $C_6 \times C_6$ and we determine generators for

$$W_{9, \theta} = \langle \left( \begin{array}{cc} 2 & 0 \\ 0 & 2 \end{array} \right), \left( \begin{array}{cc} 1 & 0 \\ 0 & 2 \end{array} \right) \rangle.$$ 

Their action on $g_0, g_1, g_2, g_3$ is computed using [3, p. 18, Lemma 6] and the relations

$$\left( \begin{array}{ccc} \nu_3,0 \\ \nu_0,3 \\ \nu_1,3 \\ \nu_2,3 \end{array} \right) \circ S = \left( \begin{array}{ccc} \nu_0,3 \\ \nu_3,0 \\ \zeta_2^{-1} \nu_3,0 \\ \zeta_2^{-1} \nu_2,3 \end{array} \right) \quad \text{and} \quad \left( \begin{array}{ccc} \nu_3,0 \\ \nu_0,3 \\ \nu_1,3 \\ \nu_2,3 \end{array} \right) \circ T = \left( \begin{array}{ccc} \zeta_2^4 \nu_3,0 \\ \zeta_2^4 \nu_0,3 \\ \zeta_2^4 \nu_1,3 \\ \nu_0,3 \end{array} \right).$$

An explicit computation yields

**Table 3. Action of $W_{9, \theta}$ for $D \equiv 1 \mod 9$**

<table>
<thead>
<tr>
<th>Generator</th>
<th>$\zeta_9$</th>
<th>$g_0$</th>
<th>$g_1$</th>
<th>$g_2$</th>
<th>$g_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\left( \begin{array}{cc} 2 &amp; 0 \ 0 &amp; 2 \end{array} \right)$</td>
<td>$\zeta_9^4$</td>
<td>$-g_0$</td>
<td>$-g_1$</td>
<td>$-g_2$</td>
<td>$-g_3$</td>
</tr>
<tr>
<td>$\left( \begin{array}{cc} 1 &amp; 0 \ 0 &amp; 2 \end{array} \right)$</td>
<td>$\zeta_9^2$</td>
<td>$\zeta_3 g_0$</td>
<td>$\zeta_6 g_1$</td>
<td>$\zeta_3^3 g_3$</td>
<td>$\zeta_6 g_2$</td>
</tr>
</tbody>
</table>

from which we conclude that both $\zeta_3 g_0^2$ and $\zeta_3^2 g_1^2$ are invariant with respect to $W_{9, \theta}$.

We proceed to $W_{8, \theta} \simeq G_{72, \theta}^{(8)}$. The conditions $D \equiv 1 \mod 4$ and $B = 1$ place no restriction on the constant coefficient $C$ for the irreducible polynomial for $\theta$. We consider the cases cases $D \equiv 1 \mod 8$ and $D \equiv 5 \mod 8$ separately. If $D \equiv 1 \mod 8$, then $C$ is even and 2 splits in $O$, so we have $(O/8O)^* \simeq C_2 \times C_2 \times C_2$. The equivalence class of $C$ mod 4 determines $W_{8, \theta}$. Explicit generators as $C$ ranges over the possibilities modulo 4 are given in table 4. Clearly, we see that these matrices act trivially on both $g_0^2$ and $g_1^2$.

**Table 4. Action of $W_{8, \theta}$ when $D \equiv 1 \mod 8$**

<table>
<thead>
<tr>
<th>Generator</th>
<th>$(B, C) \mod 4$</th>
<th>$\zeta_8$</th>
<th>$g_0$</th>
<th>$g_1$</th>
<th>$g_2$</th>
<th>$g_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\left( \begin{array}{cc} 7 &amp; 0 \ 0 &amp; 7 \end{array} \right)$</td>
<td>$(1, 0), (1, 2)$</td>
<td>$\zeta_8$</td>
<td>$-g_0$</td>
<td>$-g_1$</td>
<td>$-g_2$</td>
<td>$-g_3$</td>
</tr>
<tr>
<td>$\left( \begin{array}{cc} 3 &amp; 0 \ 0 &amp; 3 \end{array} \right)$</td>
<td>$(1, 0), (1, 2)$</td>
<td>$\zeta_8$</td>
<td>$-g_0$</td>
<td>$-g_1$</td>
<td>$-g_2$</td>
<td>$-g_3$</td>
</tr>
<tr>
<td>$\left( \begin{array}{cc} 5 &amp; 0 \ 0 &amp; 5 \end{array} \right)$</td>
<td>$(1, 0), (1, 2)$</td>
<td>$\zeta_8^2$</td>
<td>$g_0$</td>
<td>$g_1$</td>
<td>$g_2$</td>
<td>$g_3$</td>
</tr>
<tr>
<td>$\left( \begin{array}{cc} 7 &amp; 0 \ 2 &amp; 1 \end{array} \right)$</td>
<td>$(1, 0)$</td>
<td>$\zeta_7^2$</td>
<td>$g_0$</td>
<td>$-g_1$</td>
<td>$-g_2$</td>
<td>$g_3$</td>
</tr>
<tr>
<td>$\left( \begin{array}{cc} 5 &amp; 4 \ 0 &amp; 3 \end{array} \right)$</td>
<td>$(1, 2)$</td>
<td>$\zeta_8^2$</td>
<td>$-g_0$</td>
<td>$g_1$</td>
<td>$g_2$</td>
<td>$-g_3$</td>
</tr>
</tbody>
</table>
In the case $D \equiv 5 \mod 8$ we get $W_{5,\theta} \simeq C_2 \times C_4 \times C_6$. Again, we write out the action on $g_0, g_1, g_2, g_3$ of explicit generators. Again, $g_0^2, g_1^2$ are stable under $W_{5,\theta}$ when $D \equiv 1 \mod 4$ is satisfied.

From tables 3, 4 and 5 we see $\zeta_3 g_0^2(\theta), \zeta_3 g_1^2(\theta) \in H_0$ when $D \equiv 1 \mod 12$ holds. Actually, one concludes that these function values generate $H_0 = K(\mathfrak{j}(\theta))$ over $K$ because both $g_0^{12}$ and $g_1^{12}$ are roots of (5). In particular, $\mathfrak{j}$ can be written as a rational function of either $g_0^{12}$ or $g_1^{12}$, so $H_0$ can be generated over $K$ by either of the values $\zeta_3 g_0^2(\theta)$ or $\zeta_3 g_1^2(\theta)$. This completes our verification of the first entry of table 2.

### Table 5. Action of $W_{5,\theta}$ when $D \equiv 5 \mod 8$

<table>
<thead>
<tr>
<th>Generator</th>
<th>$(B, C)$ mod 8</th>
<th>$\zeta_8$</th>
<th>$g_0$</th>
<th>$g_1$</th>
<th>$g_2$</th>
<th>$g_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(5, 4)$</td>
<td>$(1, 1), (1, 3), (1, 5), (1, 7)$</td>
<td>$\zeta_8^5$</td>
<td>$g_0$</td>
<td>$g_1$</td>
<td>$g_2$</td>
<td>$g_3$</td>
</tr>
<tr>
<td>$(7, 6)$</td>
<td>$(1, 1), (1, 5)$</td>
<td>$\zeta_8^3$</td>
<td>$-g_0$</td>
<td>$g_1$</td>
<td>$g_2$</td>
<td>$-g_3$</td>
</tr>
<tr>
<td>$(2, 2)$</td>
<td>$(1, 3), (1, 7)$</td>
<td>$\zeta_8^3$</td>
<td>$-g_0$</td>
<td>$g_1$</td>
<td>$g_2$</td>
<td>$-g_3$</td>
</tr>
<tr>
<td>$(1, 0)$</td>
<td>$(1, 1)$</td>
<td>$\zeta_8$</td>
<td>$-g_0$</td>
<td>$-g_1$</td>
<td>$-g_2$</td>
<td>$-g_3$</td>
</tr>
<tr>
<td>$(7, 4)$</td>
<td>$(1, 3)$</td>
<td>$\zeta_8$</td>
<td>$-g_0$</td>
<td>$-g_1$</td>
<td>$-g_2$</td>
<td>$-g_3$</td>
</tr>
<tr>
<td>$(3, 8)$</td>
<td>$(1, 5)$</td>
<td>$\zeta_8$</td>
<td>$-g_0$</td>
<td>$-g_1$</td>
<td>$-g_2$</td>
<td>$-g_3$</td>
</tr>
<tr>
<td>$(3, 3)$</td>
<td>$(1, 7)$</td>
<td>$\zeta_8$</td>
<td>$-g_0$</td>
<td>$-g_1$</td>
<td>$-g_2$</td>
<td>$-g_3$</td>
</tr>
</tbody>
</table>

5. The case $N$ prime to 6

From now on we suppose $N \geq 5$ is relatively prime to 6 and $\mathcal{O} = [\theta, 1]$ is an imaginary quadratic order of discriminant $D < -4$. Motivated by our search for functions stabilized by $W_{24N,\theta}$, we study the orbit of the generalized Weber functions $\nu_{k,N}$. If $k \in \mathbb{Z}$ satisfies

$$f(-k) \equiv 0 \mod N \quad \text{where} \quad f = f_{\mathbb{Q}} = X^2 + BX + C \in \mathbb{Z}[X],$$

then $\nu_{k,N}^2(\theta)$ lies in $H_0$ [6, p. 158]. One expects $W_{24N,\theta}$ to act on $\nu_{k,N}$ via a character of order 24. To determine this character exactly, we use the Chinese remainder theorem to write

$$W_{24N,\theta} = G_{24N,\theta}^{(N)} \times G_{24N,\theta}^{(3)} \times G_{24N,\theta}^{(8)}$$

with

$$G_{24N,\theta}^{(m)} = \text{ker}[W_{24N,\theta} \to W_{24N/m,\theta}] \quad \text{for} \ m \mid 24N.$$

First we describe the action of $G_{24N,\theta}^{(N)}$ on $\nu_{k,N}$. This turns out to be a quadratic character.
Theorem 10. Let $n$ and $N$ be positive integers such that $n | N$. Suppose $\theta \in \mathbb{H}$ is imaginary quadratic with irreducible polynomial $f = X^2 + BX + C \in \mathbb{Z}[X]$. For $k \in \mathbb{Z}$ with $f(-k) \equiv 0 \mod N$, the action of $G_{24N,0}^{(N)}$ is given by the quadratic character

$$\chi: \begin{pmatrix} t-Bs & -Cs \\ s & t \end{pmatrix} \mapsto \begin{pmatrix} (t+(k-B)s) \\ n \end{pmatrix}$$

on $G_{24N,0}^{(N)}$. In other words, for $\omega \in G_{24N,0}^{(N)}$ the relation

$$\nu_{k,n}^\omega = \chi(\omega) \cdot \nu_{k,n}$$

is satisfied.

Proof. We write $\omega = \begin{pmatrix} t-Bs & -Cs \\ s & t \end{pmatrix} \in G_{24N,0}^{(N)}$ as

$$\begin{pmatrix} t-Bs & -Cs \\ s & t \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \det(\omega) \end{pmatrix} \cdot \begin{pmatrix} t-Bs & -Cs \\ s & t \cdot \det(\omega)^{-1} \end{pmatrix}.$$ 

Suppose $x \in \mathbb{Z}$ satisfies the congruences

$$x \equiv \det(\omega) \mod N \quad \text{and} \quad x \equiv 1 \mod 24.$$ 

The product expansion (8) shows that $\begin{pmatrix} 1 & 0 \\ 0 & \det(\omega) \end{pmatrix}$ has action $\nu_{k,n} \mapsto \nu_{kz,n}$. We take $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(24)$ to be a representative of

$$\omega = \begin{pmatrix} t-Bs & -Cs \\ s & t \cdot \det(\omega)^{-1} \end{pmatrix} \in \text{SL}_2(\mathbb{Z}/24NZ).$$

One can presume $c > 0$ by (11). We have

$$(\nu_{kz,n})^\omega = \frac{\eta \circ \begin{pmatrix} 1 & kx \\ 0 & n \end{pmatrix} \cdot M}{\eta \circ M} = \frac{\eta \circ \begin{pmatrix} 1 & kx \\ 0 & n \end{pmatrix} \cdot M \cdot \begin{pmatrix} 1 & k \\ 0 & n \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & k \\ 0 & n \end{pmatrix}}{\eta \circ M}$$

and claim that

$$M' = \begin{pmatrix} 1 & kx \\ 0 & n \end{pmatrix} \cdot M \cdot \begin{pmatrix} 1 & k \\ 0 & n \end{pmatrix}^{-1}$$

like $M$, is an element of $\Gamma(24)$. In order to see $M' \in \text{SL}_2(\mathbb{Z})$, observe

$$n \cdot M' = \begin{pmatrix} 1 & kx \\ 0 & n \end{pmatrix} \begin{pmatrix} t-Bs & -Cs \\ s \cdot t^{-1} & t \cdot s^{-1} \end{pmatrix} \begin{pmatrix} n & -k \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 0 & -s \cdot f(-k) \\ 0 & 1 \end{pmatrix} \mod n.$$ 

Because $n | f(-k)$, we conclude that $M'$ has coefficients in $\mathbb{Z}$. Furthermore, $x \equiv 1 \mod 24$ implies $M' \in \Gamma(24)$. We evaluate

$$\frac{\eta \circ \begin{pmatrix} 1 & kx \\ 0 & n \end{pmatrix} \cdot M}{\eta \circ M} = \frac{\eta \circ M' \cdot \begin{pmatrix} 1 & k \\ 0 & n \end{pmatrix}}{\eta \circ M}.$$
by applying Meyer's formula to both $M$ and $M' = (a+ckz \ n \ c \ n)^*$. Both matrices are contained in $\Gamma(24)$ so we have $\epsilon_2(M) = \epsilon_2(M') = 1$. Meyer's formula gives

$$\frac{\eta \circ M'(z+k)}{\eta \circ M(z)} = \frac{\epsilon_1(M') \sqrt{cz+d} \eta(z+k+n)}{\epsilon_1(M) \sqrt{cz+d} \eta(z)} = \left(\frac{a+ckz}{n}\right) \nu_{k,n}(z).$$

One concludes $(t-Bs \ -Cs \ t) \in W_{N,\theta}$ has Galois action

$$\nu_{k,n} \mapsto \left(\frac{t+(k-B)s}{n}\right) \nu_{k,n}(z).$$

For the $\eta$-quotients in corollary 7 which have level $N$ rather than $24N$, theorem 10 is all we need to find function values lying in $H_{\mathcal{O}}$. The combination of corollary 7 and theorem 10 gives the following statement.

**Corollary 11.** Let $\mathcal{O} = [0,1]$ be an imaginary quadratic order and let $\theta$ have

minimum polynomial $f = X^2 + BX + C \in \mathbb{Z}[X]$. Let $l$ and $n$ be positive integers prime to 6, and suppose $k \in \mathbb{Z}$ is divisible by $24$ and satisfies $f(-k) \equiv 0 \bmod l$. If $e \in \mathbb{Z}$ is even and satisfies the congruence $e(n-1) \equiv 0 \bmod 24$ then $\nu_{k,n}(\theta)$ is an element of $H_{\mathcal{O}}$. When $(l-1)(n-1) \equiv 0 \bmod 24$ holds we have

$$\frac{\nu_{k,l} \cdot \nu_{k,n}(\theta)}{\nu_{k,ln}} \in H_{\mathcal{O}}.$$  

Theorem 10 shows that the functions

$$\nu_{k,n}^2 \quad \text{and} \quad \nu_{k,n} \cdot \nu_{k,l} \over \nu_{k,ln}$$

are stable with respect to $G_{24N,\theta}^{(N)} \subset W_{24N,\theta}$ when $l$ and $n$ are positive divisors or $N$. In order to find $\eta$-quotients invariant under the full group $W_{24N,\theta}$ we now look at the other component $G_{24N,\theta}^{(24)}$ of $W_{24N,\theta}$. The action of this last component is easily derived from the formulas (10) and (8).

From now on we assume that $k \in \mathbb{Z}$ is divisible by 24. Then matrices of the form $(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}) \in \text{GL}_2(\mathbb{Z}/24NZ)$ that satisfy $d \equiv 1 \bmod N$ act trivially on $\nu_{k,N}$. In particular, for any

$$(13) \quad M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \text{det}(M) \end{smallmatrix}\right) \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in G_{24N,\theta}^{(24)}$$

the action of $M$ on $\nu_{k,N}$ is determined by the action of $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in G_{24N,\theta}^{(24)}$. We compute the action of $M$ by lifting $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \text{SL}_2(\mathbb{Z}/24NZ)$ to $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(N)$. 

By (9), we can assume $c > 0$. For any $M \in G_{24N,\theta}^{(24)}$ and any positive divisor $n$ of $N$, lemma 9 implies
\begin{equation}
(v_{k,n})^M = v_{k,n} \circ U = \zeta_{24}^{\kappa(U) \cdot (n-1)} v_{k,n},
\end{equation}
with $\kappa(U) \in \mathbb{Z}$ given by formula (8). We also get the relation
\begin{equation}
\left( \frac{v_{k,l} \cdot v_{k,n}}{v_{k,ln}} \right)^M = \frac{v_{k,l} v_{k,n}}{v_{k,ln}} \circ U = \zeta_{24}^{\kappa(U) \cdot (l-1)(n-1) \cdot v_{k,n} \cdot v_{k,l}} v_{k,ln}
\end{equation}
when $l$ and $n$ divide $N$. In particular, the observations
\begin{align*}
(n-1) &\equiv 0 \pmod{12} \Rightarrow v_{k,n}^2 \text{ is stable under } G_{24N,\theta}^{(24)} \\
(l-1)(n-1) &\equiv 0 \pmod{24} \Rightarrow \frac{v_{k,l} \cdot v_{k,n}}{v_{k,ln}} \text{ is stable under } G_{24N,\theta}^{(24)}
\end{align*}
prove theorems 2 and 4 in the special case $\text{gcd}(D,6) = 6$. In order to prove theorems 2 and 4 for $\text{gcd}(D,6) < 6$, where weaker restrictions on $N, l, n$ apply, it is convenient to split the action of $G_{24N,\theta}^{(24)}$ into separate components, $G_{24N,\theta}^{(8)}$ and $G_{24N,\theta}^{(3)}$, and write $\eta_{24} = \zeta_8^3 \cdot \zeta_3^2$. If our matrix $M$ of (13) lies in $G_{24N,\theta}^{(8)}$, then (14) gives
\begin{equation}
(v_{k,n})^M = v_{k,n} \circ U = \zeta_8^{2 \cdot \kappa(U) \cdot (n-1)} v_{k,n}.
\end{equation}
For $M \in G_{24N,\theta}^{(3)}$ we have
\begin{equation}
(v_{k,n})^M = v_{k,n} \circ U = \zeta_3^{2 \cdot \kappa(U) \cdot (n-1)} v_{k,n}.
\end{equation}
In proposition 12, we show that the value $\kappa(U)$ in (14) or (15) is even for any $M \in G_{24N,\theta}^{(8)}$ when $D$ is odd. In proposition 15, we show how to normalize the $\eta$-quotients in (14) and (15) with a suitable power of $\zeta_3$ to get a $G_{24N,\theta}^{(3)}$-invariant function. Propositions 13 and 14 give normalizations of $v_{k,n}^2$ and $\frac{v_{k,l} \cdot v_{k,n}}{v_{k,ln}}$ that are stable under $G_{24N,\theta}^{(8)}$ when $D \equiv 4, 8 \pmod{16}$.

**Proposition 12.** Let $O = [\theta, 1]$ be an imaginary quadratic order of odd discriminant $D$, and let $f_{\theta} = X^2 + X + C \in \mathbb{Z}[X]$ be the minimum polynomial for $\theta$. Suppose $N > 0$ is prime to 6. We write $M \in G_{24N,\theta}^{(8)}$ as
\begin{equation}
M = \begin{pmatrix} 1 & 0 \\ 0 & \det(M) \end{pmatrix} \left( \begin{array}{c} \alpha \\ \gamma \\ \delta \end{array} \right).
\end{equation}
For any lift $U \in \Gamma(3N)$ congruent to $\left( \begin{array}{c} \alpha \\ \gamma \\ \delta \end{array} \right)$, the number $\kappa(U)$ is even. Thus if $k$ is divisible by 24 and $l, n$ are positive divisors of $N$, then $v_{k,n}^2$ and $\frac{v_{k,l} \cdot v_{k,n}}{v_{k,ln}}$ are invariant under $G_{24N,\theta}^{(8)}$. 

CLASS INVARIANTS FROM DEDEKIND’S ETA-FUNCTION

Proof. For \( O = [\theta, 1] \) of odd discriminant, explicit generators for all possible groups \( W_{8, \theta} \cong G^{(8)}_{24N, \theta} \) are given in tables 4 and 5. For each of these generating matrices \( M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \) we determine a lift \( U \in \Gamma(3N) \) for \( (\alpha \beta \gamma \delta) \). A routine calculation shows \( \kappa(U) \) is even in every case. It is clear that \( \kappa(U) \equiv 0 \mod 3 \), so writing \( \zeta_{24} = \zeta_{8}^3 \zeta_{3}^2 \) gives

\[
(v_{k,n})^M = \zeta_{24}^{\kappa(U)-(n-1)} v_{k,n} = \zeta_{8}^{3 \cdot \kappa(U)-(n-1)} v_{k,n}.
\]

Thus \( v_{k,n}^2 \) is stable under \( M \) because both \( \kappa(U) \) and \( (n-1) \) are even. Similarly

\[
\left( \frac{v_{k,n} \cdot v_{k,n}}{v_{k,n}} \right)^M = \zeta_{8}^{3 \cdot \kappa(U)-((l-1)+(n-1)-(l(n-1))) \cdot v_{k,n} \cdot v_{k,n}}
\]

shows that \( \frac{v_{k,n} \cdot v_{k,n}}{v_{k,n}} \) is stable under \( M \).

Proposition 13. Let \( O = [\theta, 1] \) be an imaginary quadratic order of discriminant \( D \equiv 4, 8 \mod 16 \). Let \( \theta \) have minimum polynomial \( f_{\theta} = X^2 + C \in \mathbb{Z}[X] \), so that \( C \equiv 2, 3 \mod 4 \) holds. Let \( N, k, x \in \mathbb{Z} \) be integers such that \( N > 0 \) is prime to \( 6, k \) is divisible by \( 24 \) and \( x \) satisfies the congruence \( x \equiv \frac{N-1}{2} \mod 2 \). Then the function

\[
\zeta_4^2 \cdot v_{k,n}^2 \text{ is invariant under } G^{(8)}_{24N, \theta}.
\]

Proof. First we find explicit generators for \( W_{8, \theta} \cong G^{(8)}_{24N, \theta} \). In the case \( C \equiv 2 \mod 4 \), the group \( W_{8, \theta} \) has structure \( C_2 \times C_2 \times C_8 \) with generators

\[
W_{8, \theta} = \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \right\} \text{ if } C \equiv 2 \mod 8
\]

Both \( \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \) and \( \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \) have determinant 1 mod 8, so they act trivially on \( \zeta_8 \). A routine calculation shows that the \( \kappa \)-value of any lift \( U \in \Gamma(3N) \) for either \( \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \) or for \( \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \) is even. Thus from (14) we see that both of these scalar matrices act trivially on \( v_{k,N}^2 \). However for \( \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \) and \( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 7 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 7 \\ 1 & 0 \end{pmatrix} \), the associated \( \kappa \)-values are odd. Also, these remaining generators send \( \zeta_4 \mapsto \zeta_4^3 \). Thus if \( N - 1 \equiv 0 \mod 4 \), then \( v_{k,N}^2 \) is invariant under \( G^{(8)}_{24N, \theta} \). In the case \( N - 1 \equiv 2 \mod 4 \) the function \( \zeta_4 \cdot v_{k,N}^2 \) is \( G^{(8)}_{24N, \theta} \)-invariant. In other words, the function \( \zeta_4 \cdot v_{k,N} \) of the proposition is stable under \( G^{(8)}_{24N, \theta} \). A similar computation can be performed in the case \( C \equiv 3 \mod 8 \). Here, one can use

\[
W_{8, \theta} = \left\{ \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix} \right\} \text{ if } C \equiv 3 \mod 8
\]

\[
W_{8, \theta} = \left\{ \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix} \right\} \text{ if } C \equiv 7 \mod 8.
\]
as generators.

An similar argument gives the following proposition.

**Proposition 14.** Let \( \mathcal{O} = [\theta, 1] \) be an imaginary quadratic order of discriminant \( D \equiv 4, 8 \mod 16 \). Let \( \theta \) have minimum polynomial \( f_{\mathcal{O}}^\theta = X^2 + C \in \mathbb{Z}[X] \), so that \( C \equiv 2, 3 \mod 4 \) holds. Let \( l, n, k, x \in \mathbb{Z} \) be integers such that \( l, n > 0 \) are prime to 6, \( k \) is divisible by 24 and \( x \equiv (l-1)(n-1) \mod 2 \). Then the function

\[
\frac{\zeta_4^{2B} \nu_{k,n} \cdot \nu_{k,l}}{\nu_{k,l,n}}
\]

is invariant under \( G_{24N,\theta}^{(8)} \).

We finally look at the action of \( G_{24N,\theta}^{(3)} \) for \( D \) not divisible by 3.

**Proposition 15.** Let \( \mathcal{O} = [\theta, 1] \) be an imaginary quadratic order of discriminant \( D \) not divisible by 3 and let \( f_{\mathcal{O}}^\theta = X^2 + BX + C \in \mathbb{Z}[X] \) be the minimum polynomial for \( \theta \). We take \( k \) to be divisible by 24 and \( n \) a positive divisor of \( N \). Every element of \( G_{24N,\theta}^{(3)} \) acts on \( Q(\zeta_3, \nu_{k,n}) \) as a power of the automorphism \( \sigma_B \) defined by

\[
\zeta_3 \mapsto \zeta_3^2 \quad \nu_{k,N} \mapsto \zeta_3^{2B \cdot (n-1)} \nu_{k,n}.
\]

In particular, for positive divisors \( l \) and \( n \) of \( N \) the functions

\[
(16) \quad \zeta_3^{2B(n-1)} \nu_{k,n} \quad \text{and} \quad \zeta_3^{2B(l-1)(n-1)} \frac{\nu_{k,l} \cdot \nu_{k,n}}{\nu_{k,l,n}},
\]

are stable with respect to \( G_{24N,\theta}^{(3)} \).

**Proof.** If \( D \equiv 1 \mod 3 \) then \( W_{3,\theta} \simeq C_2 \times C_2 \) is one of the groups

\[
W_{3,\theta} = \begin{cases} 
\langle (\frac{2}{0}, 0), (0, 1) \rangle & \text{if } (B, C) \equiv (0, 2) \mod 3 \\
\langle (\frac{2}{0}, 0), (1, 0) \rangle & \text{if } (B, C) \equiv (1, 0) \mod 3 \\
\langle (\frac{2}{0}, 0), (1, 1) \rangle & \text{if } (B, C) \equiv (2, 0) \mod 3.
\end{cases}
\]

First, consider the action of the \( \langle \frac{2}{0}, 0 \rangle \in \text{SL}_2(\mathbb{Z}/3\mathbb{Z}) \) which appears as a generator for \( W_{3,\theta} \) in every case of (17). If \( U \in \Gamma(8N) \) is a lift for \( \langle \frac{2}{0}, 0 \rangle \), the formula (8) gives \( \kappa(U) \equiv 0 \mod 3 \). We conclude that this matrix acts trivially on both \( \zeta_3 \) and \( \nu_{k,N} \). A similar calculation shows that the remaining generator \( \langle \frac{1}{0}, 1 \rangle \), \( \langle \frac{1}{1}, 0 \rangle \) or \( \langle \frac{1}{1}, 1 \rangle \) acts as \( \sigma_B \) in each of the possible cases for (17). Namely, each generator has determinant 2, and the value \( \kappa(U) \) from (14) satisfies \( \kappa(U) \equiv B \mod 3 \). One easily checks that the functions (16) are indeed invariant under \( \sigma_B \).
If \( D \equiv 2 \mod 3 \) we have \( W_{3,\theta} \simeq C_8 \) with

\[
W_{3,\theta} = \begin{cases} 
\langle \left( \begin{array}{c} 1 \\ 2 \\ \end{array} \right) \rangle & \text{if } (B, C) \equiv (0, 1) \mod 3 \\
\langle \left( \begin{array}{c} 0 \\ 1 \\ \end{array} \right) \rangle & \text{if } (B, C) \equiv (1, 2) \mod 3 \\
\langle \left( \begin{array}{c} 0 \\ 2 \\ \end{array} \right) \rangle & \text{if } (B, C) \equiv (2, 2) \mod 3 .
\end{cases}
\]

Again, a routine computation shows that each of these generators acts as \( \sigma_B \).

**Proof of theorem 2 and theorem 4.** The result is obtained by combining the formulas (14) and (15) with propositions 12 and 15.

**Proof of proposition 3.** Combine (14) with propositions 13 and 15.

### 6. Examples and Observations

Given a maximal order \( \mathcal{O} = [\theta, 1] \) of discriminant \( D \), we discuss how different choices for the parameters \( l, n \) and \( k \) in theorem 4 affects the generator \( \rho \) from (6) of the Hilbert class field for \( K = \mathbb{Q}(\sqrt{D}) \). Our examples illustrate how the singular values of this type give rise to small generators of the Hilbert class field \( \mathcal{H}_K \).

Before we study the minimum polynomial for (6), is useful to first recount some facts regarding the value (2) and the function \( \Delta = \eta^{24} \). The value of \( \Delta \) at an ideal \( \alpha \subset \mathcal{O} \) is defined as

\[
\Delta(\alpha) = \omega_2^{-12} \Delta(\omega_1/\omega_2)
\]

where \( [\omega_1, \omega_2] \) is an \( \mathbb{Z} \)-basis for \( \alpha \) such that \( \omega_1/\omega_2 \) in the complex upper half plane. This value is independent of the choice of basis for \( \alpha \), and for scalars \( \lambda \in K^* \) the equation \( \Delta(\lambda \alpha) = \lambda^{-12} \Delta(\alpha) \) is satisfied. From [6, p. 158] we have

\[
\frac{\Delta(\alpha)}{\Delta(\mathcal{O})} \in H_{\mathcal{O}}.
\]

Moreover, under the Artin isomorphism on the ideal class group

\[
\sigma : C(\mathcal{O}) \cong \text{Gal}(\mathcal{H}/K),
\]

the class \( [\mathcal{b}] \in C(\mathcal{O}) \) of an ideal \( \mathcal{b} \subset \mathcal{O} \) acts as

\[
\frac{\Delta(\alpha)}{\Delta(\mathcal{O})} = \frac{\Delta(\mathcal{a}\mathcal{b})}{\Delta(\mathcal{b})}.
\]

Here, \( \mathcal{b} \subset \mathcal{O} \) is the conjugate of \( \mathcal{b} \).
Given a maximal quadratic order $\mathcal{O} = [\theta, 1]$ of discriminant $D$, we assume $l, n$ and $k$ are integers that satisfy the conditions of theorem 4. Then $a = [\theta + k, l]$ and $b = [\theta + k, n]$ are proper ideals of $\mathcal{O}$ with product $ab = [\theta + k, ln]$. The quantity

$$
\rho^{24} = \left(\frac{\nu_{k,n} \cdot \nu_{k,l}}{\nu_{k,ln}}\right)^{24} (\theta) = \frac{\Delta(a)\Delta(b)}{\Delta(\mathcal{O})\Delta(ab)}
$$

(18)

depends only on the ideal classes $[a]$ and $[b]$. Thus if we fix the classes $[a]$ and $[b]$ and let $[\theta + k, l]$ and $[\theta + k, n]$ range over ideals equivalent to $a$ and $b$ respectively, the value (6) is fixed up to a 24th root of unity in $H_\mathcal{O}$.

For example, with $D = -308$ and $\theta = \sqrt{-77}$ we fix the class $[a]$ to be equivalent to $[3, -1 + \sqrt{-77}]$ and $[b]$ equivalent to $[6, -1 + \sqrt{-77}]$. For $l = 31$, $n = 41$ and $k = 21456$ the generator $\rho$ in (6) has polynomial

$$
X^8 + 2 X^7 + 8 X^6 - 14 X^5 + 25 X^4 - 26 X^3 + 40 X^2 - 12 X + 1.
$$

(19)

Equivalent ideals arise when we choose $l' = 59$, $n' = 61$, and $k' = 52992$. This time however, the generator $\rho' = i\rho$ has polynomial

$$
X^8 - 10 X^7 + 44 X^6 - 102 X^5 + 137 X^4 - 106 X^3 + 40 X^2 - 4 X + 1
$$

Taking $l = 31$ $n = 41$ again, if we replace $k$ with $k = 22440$. The ideals $[\theta + \bar{k}, l]$ and $[\theta + \bar{k}, n]$ belong the classes $[\bar{a}]$ and $[b]$ respectively. The polynomial for the resulting generator

$$
X^8 - 12 X^7 + 40 X^6 - 26 X^5 + 25 X^5 - 14 X^3 + 8 X^2 + 2 X + 1
$$

has $\rho^{-1}$ as one of its roots. In general, note that

$$
\left(\frac{\Delta(\bar{a})\Delta(b)}{\Delta(\mathcal{O})\Delta(ab)}\right)^{\sigma([\bar{a}])} = \frac{\Delta(\bar{a})\Delta(ab)}{\Delta(a)\Delta(\bar{a}ab)} = \frac{\Delta(\mathcal{O})\Delta(ab)}{\Delta(a)\Delta(b)}
$$

(20)

shows that replacing the class of $[a]$ with $[\bar{a}]$ changes the the polynomial for $\rho$ to a polynomial for $\zeta \rho^{-1}$ with $\zeta \in H_\mathcal{O}$ a 24th root of unity.

One obtains polynomials with nice symmetry properties by choosing $k, l, n$ in theorem 4 so that the class of $a = [\theta + k, l]$ in $C(\mathcal{O})$ has order 2. Taking $\bar{a} = a$ in (20) shows that the value $\rho$ is conjugate to $\zeta \rho^{-1}$ for some 24th root of unity $\zeta \in H_\mathcal{O}$. Returning to the example $D = -308$ with $\theta = \sqrt{-77}$ we take $l = 7$, $n = 13$, $k = 2016$. Then $a$ is equivalent to $[7, \sqrt{-77}]$, which has order 2 in $C(\mathcal{O})$. The other ideal $b = [\theta + k, n]$ is equivalent to $[6, -1 + \sqrt{-77}]$. In this case, the polynomial for (6)

$$
X^8 + 6 X^7 + 32 X^6 + 14 X^5 + 62 X^4 - 14 X^3 + 32 X^2 - 6 X + 1
$$
is anti-symmetric.

If we do not fix ideal classes \([a]\) and \([b]\) and let \(l, n, k\) range over all triples that satisfies the conditions of theorem 4, the polynomial for the generator (6) can vary enormously. For example, consider \(D = -1103\) with class number 23. For \(l = 139\) and \(n = 193\) and \(k = 229488\) the value (6) has polynomial

\[
X^{23} + 5X^{21} - 17X^{20} + 33X^{19} - 14X^{18} + 53X^{17} - 34X^{16} - 19X^{15} \\
+ 140X^{14} - 19X^{13} + 257X^{12} - 106X^{11} - 16X^{10} + 274X^9 + 165X^8 \\
+ 515X^7 - 28X^6 + 129X^5 + 89X^4 + 524X^3 + 244X^2 + 50X - 1
\]

of discriminant

\[
\delta = 5^{18} \cdot 7^{12} \cdot 13^2 \cdot 19^6 \cdot 71^2 \cdot 79^2 \cdot 89^2 \cdot 127^2 \cdot 241^2 \cdot 331^2 \cdot 491^2 \cdot 811^2 \cdot 1103^{11}.
\]

Note that the primes in \(\delta\) are smaller than the absolute value of \(D\). However, choosing \(l = 67, n = 17\) and \(k = 10416\) produces a generator

\[
X^{23} - 26X^{22} + 943X^{21} - 1273X^{20} + 3024X^{19} + 22030X^{18} + 77345X^{17} \\
+ 537919X^{16} + 2948167X^{15} + 8418094X^{14} + 16805933X^{13} \\
+ 23112410X^{12} + 21128602X^{11} + 18315689X^{10} + 27068290X^9 \\
+ 10439594X^8 + 5747695X^7 + 1799653X^6 - 1320431X^5 \\
- 14375X^4 + 201992X^3 - 26248X^2 + 900X - 1
\]

for \(H_D\) whose discriminant

\[
\delta' = 5^{20} \cdot 7^6 \cdot 11^2 \cdot 13^4 \cdot 571^2 \cdot 1103^{11} \cdot 4937^2 \cdot 31663^2 \cdot 150379^2 \cdot 2039509^2 \cdot 3944513^2 \\
\cdot 125483879^2 \cdot 1012281929^2 \cdot 1083536101^2 \cdot 1104156973^2 \cdot 11520380629^2 \\
\cdot 1168349531^2 \cdot 14477063641^2
\]

is full of primes larger than \(D\).

For all fundamental discriminants \(D > -1000\), we have computed generators for \(H_D\) arising from Theorem 4. In general the discriminant \(\delta\) of this generating polynomial can contain large primes. However, it is usually possible to choose appropriate prime numbers \(l, n\) and \(k \in \mathbb{Z}\) so that the discriminant of the minimum polynomial for (6) has prime divisors smaller than \(D\). Thusfar, it has not been possible for the discriminants \(D \in \{-551, -759, -879, -899, -935\}\). At present, it is unclear as to why most field discriminants admit polynomials with good discriminants and how one should choose these "lucky" primes which give rise to good discriminants.
REFERENCES

3. A.C.P. Gee, *This thesis*.
SAMENVATTING

Dit proefschrift bestaat uit vier artikelen. Het centrale thema is het zoeken van expliciete voortbrengers van kasseldichamen van imaginair kwadratische getallenlichamen.

Het eerste hoofdstuk is geschreven in 1998 en is verschenen als
Hierin worden voortbrengers van het Hilbert kasseldichaam gevonden met behulp van singuliere waarden van de klassieke functies $\gamma_2$ and $\gamma_3$, Webers $f$-functies van niveau 48, en zijn $\omega$-functies van niveau 5. De ontwikkelde methode voor het berekenen van het minimumpolyoom van deze voortbrengers bewijst de correctheid van een aantal formules, die in de recente literatuur vermoed werd.

Hoofdstuk twee bestaat uit gezamenlijk werk met mijn promotor P. Stevenhagen. Dit artikel is gepubliceerd als
Hierin wordt de technische kern van het eerste hoofdstuk op een eenvoudigere en natuurlijker manier uit de doeken gedaan. Voorbeelden van klasse-invarianten worden berekend met behulp van een aantal modulaire functies van hoger niveau.

Het derde artikel, "Singular values of the Rogers-Ramanujan continued fraction" is geschreven met Mascha Honsbeek. Het is in juni 1999 ingediend ter publicatie. We bepalen de kasseldichamen voortgebracht door singuliere waarden van de beroemde Rogers-Ramanujan kettingbreuk en geven een methode voor het schrijven van deze waarden als geneste worteluitdrukkingen.

In het vierde en laatste hoofdstuk wordt een veralgemening van de Weber $j$-functies bestudeerd. Met behulp van deze generalisaties wordt voor elk kwadratisch imaginair getallenlichaam een scala aan klasse-invarianten verkregen.

In de gepubliceerde artikelen zijn verschillende wijzigingen aangebracht om meer eenheid te krijgen in de vorm van dit proefschrift. In het bijzonder zijn paginanummers en interne verwijzingen veranderd.
ACKNOWLEDGEMENTS

There are several people to whom I owe many thanks for their direct or indirect contribution to this thesis. Foremost, I am indebted to my promotor Peter Stevenhagen, who provided active guidance and supervision. Without the aid of his stimulation and insight, this thesis would still be unfinished. I also thank Peter for his heroic efforts in improving my writing.

I thank my hosts Heng Huat Chan and Victor Tan for the opportunity to work with them in Singapore. Our lively discussions gave rise to the work in chapter 3. I am grateful for the stamina of my co-author Mascha Honsbeek in coping with the laborious computations.

Many thanks to Don Zagier and Frits Beukers for being generous with their time and knowledge.

My colleagues at the Korteweg-de Vries Institute made my sojourn at the University of Amsterdam a pleasant one. In particular, I would like to thank my office-mates Bart de Smit, Hans Roskam and Valerio Talamanca who were always ready to lend an ear to questions. Thanks also to Chris Zaal (translation services) and Richard Groenwegen (tex wizardry).

Finally I thank my family for their support and encouragement—my parents Jane and Frede, and my husband Claudie.
CURRICULUM VITAE

Alice Chia Ping Gee was born February 14, 1963 in Taipei, Taiwan. She attended secondary school in Ottawa, Canada, and graduated from Glebe Collegiate Institute in 1981. Afterwards, she worked internationally as a fashion model with the agencies Marilyn (Paris), Premier (London) and Ford (New York).

In 1988 she enrolled in the math department of the University of Amsterdam, and was married to Claude August Crommelin. After graduating in 1995, an AiO-ship ensued at the University of Amsterdam in January of 1996. During this period, the author worked at the University of Singapore as a visiting research fellow in the winter of 1999.