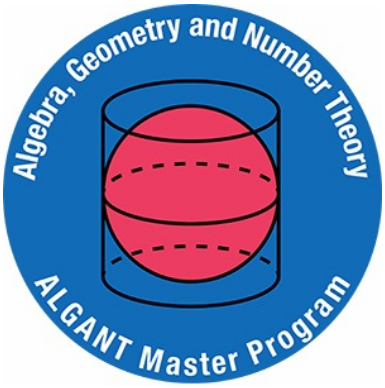

Jana Sotáková

Eta quotients and class fields of imaginary quadratic fields

Master's thesis, 16 June 2017

Supervisor: dr. Marco Streng

Universiteit Leiden **Universität Regensburg**

Acknowledgments

I would like to express my gratitude to my supervisor, Dr. Marco Streng, for giving me an interesting problem to work on and the opportunity to write about topics I have long wished to learn in more depth, for the confidence he had in me when he trusted me with the autonomy over my thesis that best suited my learning style, and for all the patience he has had with me, especially over the first few months when my computations were not exactly correct.

I am grateful to the Algant Master Program for supporting me through the year in Regensburg and the year in Leiden and for providing me with ample opportunities to grow both mathematically and personally. I am in debt to the permanent inhabitants of the common room in Leiden for making my time in Leiden enjoyable. I am particularly grateful to my partner, who has introduced me to the various Dutch idiosyncrasies, cooked boerenkool met worst and who has made my time in Leiden the most wonderful experience.

And I would like to thank my mentor, professor Peter Stevenhagen, for all his support and all the time he has given me through the years and for all the conversations about mathematics and being a mathematician we have had. En ik ben dankbaar dat hij tegen mij zo lang Nederlands heeft gesproken dat ik nu grappiger ben in het Nederlands dan in het Engels.

And of course, my special thanks go to my family, who supported me in all my big plans all through the years, celebrated with me when it worked out and helped me adjust when the plans turned out differently.

Contents

1 Introduction

There are many deep and beautiful theorems in number theory, but only a few of them are as frustrating as class field theory[1]. It takes a long time to get acquainted with all the various formulations of the big theorems, one can easily spend semesters building up all the difficult (but impressive) theory required to prove at least some of the results. But in the end, one realizes that beyond the easiest case of describing all the abelian extensions of $\mathbb{Q}$, most of the objects one encounters remain mystical creatures beyond the reach of explicit mathematics.

There is one other classical class of number fields, though, that allows for an explicit description: imaginary quadratic fields. Such fields all arise from $\mathbb{Q}$ by adjoining a root of a degree two polynomial with integer coefficients and negative discriminant and admit a beautiful connection to the theory of elliptic curves and modular forms. It is by means of this link that one can obtain very explicit descriptions of many interesting abelian extensions. Many beautiful books and papers and theses have already been written about this theory.

Let K be an imaginary quadratic field. In chapter 4, we will see that all abelian extensions of K can be generated using special values of *modular functions*. The following situation of ring class fields will be of most interest for us. Let $\mathcal{O}$ be an order in K and just like for the ring of integers $\mathcal{O}_K$, we can define the class group $Cl(\mathcal{O})$, which is a finite abelian group. Moreover, we can understand $\mathcal{O}$ as a lattice in $\mathbb{C}$ and we associate to $\mathcal{O}$ a certain algebraic number $j(\mathcal{O})$, its j-invariant. Then the field $H_{\mathcal{O}} = K(j(\mathcal{O}))$, called the ring class field, is a finite abelian extension of K and comes with a canonical isomorphism

$$\mathrm{Gal}(H_{\mathcal{O}}/K) \cong Cl(\mathcal{O}).$$

The fields $H_{\mathcal{O}}$ also come with several canonical motivations for their study. Two main sources of attention come from the problem of the representation of primes by binary quadratic forms (with the ground work laid out already by Gauss, see [3]) or the (somewhat more modern) problems arising from elliptic curve cryptography [2]. However, the minimal polynomials of the algebraic numbers $j(\mathcal{O})$ have too large coefficients and soon become useless in practice. A lot of research has been invested into finding class invariants with smaller minimal polynomials and computing the minimal polynomials of $j(\mathcal{O})$.

The starting point of this thesis is the article of Enge and Morain [5], in which they study class invariants obtained by replacing the function j by a suitable power of eta quotients of the form

$$\mathfrak{w}_n = \frac{\eta\left(\frac{\tau}{n}\right)}{\eta(\tau)},$$

where $\eta(\tau)$ is the Dedekind eta function (see 2.3). Enge and Morain systematically determine the sufficient powers e such that $\mathfrak{w}_n^e$, evaluated at a specified element of $\mathcal{O}$, produces an element in $H_{\mathcal{O}}$ (subject to certain congruence conditions on the discriminant of $\mathcal{O}$). The authors then ask whether one could obtain smaller exponents if one multiplies the functions $\mathfrak{w}_n$ by a suitable 24-th root of unity.

For $n = 2$ and $n = 3$, this question has already been answered by Weber (see the modern formulations in [1] and [9]) and Gee [6]. In this thesis, we focus on $n = 4$ and show that the answer is yes, it is sometimes possible to lower the necessary exponent to obtain *smaller* class invariants. The general approach to our method is independent of the choice of n and is based on the work of Alice Gee (see [6]) using Shimura reciprocity (see 4.3) and is explained in section 5. We give concrete examples for $n = 4$ in 6.2, 6.3.1 and 6.3.2. Moreover, if one allows oneself to use small elements of $\mathbb{Q}(\zeta_{24})$, rather than just roots of unity, we can obtain smaller class invariants for more orders $\mathcal{O}$, of which we give examples in 6.3.3.

[1] Disclaimer: The views and opinions expressed in this introduction are those of the author and do not necessarily reflect the official policy or position of Universiteit Leiden and Universität Regensburg.

2 Elliptic curves and modular forms

In this section, we summarize the theory of complex elliptic curves and modular forms.

Let $\mathbb{H}$ be the upper half plane

$$\mathbb{H} = \{\tau \in \mathbb{C} : \Im\tau > 0\}.$$

The group $\mathrm{GL}_2(\mathbb{R})^+$ of real matrices with positive determinant has an action on $\mathbb{H}$ via the Möbius transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d},$$

as the imaginary part computation gives

$$\Im\frac{a\tau+b}{c\tau+d} = \Im\frac{(a\tau+b)(c\bar{\tau}+d)}{|c\tau+d|^2} = \Im\frac{ad\tau+bc\bar{\tau}}{|c\tau+d|^2} = \frac{(ad-bc)\Im\tau}{|c\tau+d|^2} > 0.$$

All the Möbius transformations are bijections on $\mathbb{H}$. In the following, the most important will be the action of the subgroup $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$. As $-\mathrm{id}$ acts trivially on $\mathbb{H}$, this action actually factors via $\mathrm{PSL}_2(\mathbb{Z})$.

2.1 Complex elliptic curves

Given any $\tau \in \mathbb{H}$, the additive group $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z} \subset \mathbb{C}$ is an example of a (full-rank) lattice. To such a lattice in $\mathbb{C}$, we will associate an elliptic curve $\mathbb{C}/\Lambda_\tau$. As a compact Riemann surface, the elliptic curve $\mathbb{C}/\Lambda_\tau$ has also an algebraic structure, coming from the Weierstrass parametrization. We will not discuss the algebraic theory of elliptic curves.

2.1.1 Elliptic curves from lattices

A lattice Λ is a discrete additive subgroup of $\mathbb{C}$ of rank 2 and can be written as

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \quad \text{with} \quad \omega_1, \omega_2 \in \mathbb{C}^* \quad \text{and} \quad \frac{\omega_1}{\omega_2} \in \mathbb{H}.$$

The quotient $\mathbb{C}/\Lambda$ can be given a structure of a compact Riemann surface. We call $E = \mathbb{C}/\Lambda$ the elliptic curve corresponding to the lattice Λ. Note that E also carries an abelian group structure, being the quotient $\mathbb{C}/\Lambda$ of abelian groups.

Let $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ be elliptic curves. Given the Riemann surface structure and the group structure on E, we want any map between elliptic curves to respect the group law and be holomorphic. It is then a nice exercise to show that any such map is necessarily given as

$$\alpha : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda' \quad z \mapsto \alpha z$$

for some $\alpha \in \mathbb{C}^\times$ satisfying $\alpha\Lambda \subset \Lambda'$. In particular, $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic if there exists some $\alpha \in \mathbb{C}^\times$ such that

$$\alpha\Lambda = \Lambda',$$

i.e., if Λ and Λ' are homothetic lattices. As a simple consequence note that any elliptic curve $E = \mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$ is isomorphic to an elliptic curve of the form $E_\tau = \mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$ for some $\tau \in \mathbb{H}$: set $\tau = \frac{\omega_1}{\omega_2} \in \mathbb{H}$ and then

$$\frac{1}{\omega_2} : \mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) \to \mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}) = \mathbb{C}/(\mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z})$$

is the desired isomorphism.

Moreover, the explicit description of maps between complex elliptic curves helps us determine the endomorphism rings easily:

$$\mathrm{End}(\mathbb{C}/\Lambda) = \{\alpha \in \mathbb{C}^\times : \alpha\Lambda \subset \Lambda\}.$$

Because isomorphic curves necessarily have isomorphic endomorphism rings, we reduce to the case that $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$. Then the condition $\alpha\Lambda \subset \Lambda$ implies that

$$\begin{aligned} \alpha\tau &= a\tau + b \\ \alpha &= c\tau + d \end{aligned}$$

for some $a, b, c, d \in \mathbb{Z}$. Therefore, τ satisfies the following quadratic relation

$$c\tau^2 + (d-a)\tau + b = 0.$$

Because $\tau \in \mathbb{H}$, this equation implies that either $c = 0$ (so $a = d$ and $b = 0$) or $c \neq 0$. If $c = 0$, in which case $\alpha = d$ is an integer and the endomorphism is the multiplication by d, which is an endomorphism any group possesses. If on the other hand $c \neq 0$, then $\mathbb{Q}(\tau)$ is an imaginary quadratic field.

Moreover, if $c \neq 0$, we obtain that

$$\alpha\left(\frac{\alpha - d}{c}\right) = a\left(\frac{\alpha - d}{c}\right) + b$$

and so α is an algebraic integer lying in the imaginary quadratic field $\mathbb{Q}(\tau)$ and the endomorphism ring $\mathrm{End}(E) \supsetneq \mathbb{Z}$ contains endomorphisms not induced by the multiplication-by-m on E and we say that E has complex multiplication. We will return to the algebraic properties of $\mathrm{End}(E)$ in section 3.1.

For any lattice Λ and for $k \in \mathbb{Z}$ define the Eisenstein series

$$G_k(\Lambda) = \sum_{0 \neq \omega \in \Lambda} \frac{1}{\omega^k}$$

which converge for all $k > 2$. Replacing Λ with $\alpha\Lambda$, we see that

$$G_k(\alpha\Lambda) = \alpha^{-k} G_k(\Lambda),$$

that is, G_k is homogeneous of degree $-k$. Moreover, we can understand the Eisenstein series as a function of τ, setting

$$G_k(\tau) = G_k(\mathbb{Z}\tau + \mathbb{Z}).$$

Set $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$. It is a standard result that the discriminant function

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$$

does not vanish for any Λ and so the j-invariant

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)} = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}$$

is a well-defined complex number for any lattice Λ.

As j is homogeneous of degree 0, if two elliptic curves $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic, then $j(\Lambda) = j(\Lambda')$. The converse also holds.

2.2 Modular functions

Setting $j(\tau) = j(\mathbb{Z}\tau + \mathbb{Z})$, the j-invariant can be understood as a function of τ. We will show that the j-invariant is $\mathrm{SL}_2(\mathbb{Z})$-invariant. For any lattice Λ, the j-invariant $j(\Lambda)$ is independent of the choice of a basis of Λ. Replace the (oriented) basis ω_1, ω_2 with the basis ω_1', ω_2', which satisfies

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}$$

for some matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$\tau' = \frac{\omega_1'}{\omega_2'} = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\tau + b}{c\tau + d} = \gamma\tau.$$

But then $E_\tau \cong E_{\tau'}$ and so $j(\tau) = j(\tau') = j(\gamma\tau)$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. This implies that $j(\tau + 1) = j(\tau)$ and so for $q = \exp(2\pi i\tau)$ we obtain a Fourier expansion

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots.$$

The properties of the j-invariant motivate the following definition of a modular function.

A meromorphic function f on $\mathbb{H}$ is called a modular function for $\mathrm{SL}_2(\mathbb{Z})$ provided it satisfies the following conditions:

- f is $\mathrm{SL}_2(\mathbb{Z})$-invariant, that is, for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we have $f(\gamma\tau) = f(\tau)$,
- the Laurent expansion in $q = \exp(2\pi i\tau)$ has at most finitely many negative terms, that is, for some $k \in \mathbb{Z}$ we have
$$f(\tau) = \sum_{n \geq k} a_n q^n.$$

One of the ways to think about this definition is to note that in fact f extends to a meromorphic function on the compactification $X(1) = \overline{\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}}$, which is a Riemann surface and which is obtained from $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$ by adding one point at infinity in the direction of the imaginary axis.

In section 4.2, we will see that any modular function for $\mathrm{SL}_2(\mathbb{Z})$ is actually a rational function in j. To get a larger supply of modular functions, we consider modular functions for certain subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

2.2.1 Congruence subgroups

Let $N \in \mathbb{N}$ be a positive integer. The principal congruence subgroup of level N is the group

$$\Gamma(N) = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})).$$

We can also describe the subgroup as

$$\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : b, c \equiv 0 \bmod N, a \equiv d \equiv 1 \bmod N\}$$

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a subgroup. We call Γ a congruence subgroup of level N if

$$\Gamma(N) \subset \Gamma \subset \mathrm{SL}_2(\mathbb{Z}).$$

Note that a congruence subgroup can have different levels. Two important examples are the congruence subgroups

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N\},$$

$$\Gamma^0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : b \equiv 0 \bmod N\}.$$

Let N be an integer. Let f be a function on the upper half plane $\mathbb{H}$, which is meromorphic and invariant under a congruence subgroup $\Gamma \supset \Gamma(N)$. Then f is invariant under $\tau \mapsto \tau + N$ and we have a Laurent expansion

$$f(\tau) = \sum_{m \in \mathbb{Z}} a_m q^{\frac{m}{N}}.$$

If for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the Laurent expansion of $f(\gamma\tau)$ has only finitely many negative terms, we call f a modular function for Γ. Note that this needs to be checked for only finitely many $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

2.3 The Dedekind eta function

For $\tau \in \mathbb{H}$ and $q = \exp(2\pi i\tau)$ we define the eta function by the product

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{m\geq 1}(1-q^m).$$

From the Jacobi formula, we have the following relation between the Δ and the η function:

$$\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}.$$

The eta function is holomorphic on the upper half plane $\mathbb{H}$.

The eta function is important for us, because in chapter 5 we will build modular functions as quotients of eta functions. Therefore, we would first like to understand how η transforms under the action of $\mathrm{SL}_2(\mathbb{Z})$. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ be a matrix. As $\gamma\tau = (-\gamma)\tau$, we may assume that $c > 0$ or that $c = 0$ and $d = 1$. As moreover

$$\Delta(\gamma\tau)(c\tau + d)^{-12} = \Delta(\tau),$$

we obtain that

$$\eta(\gamma\tau) = \epsilon(\gamma) \cdot \sqrt{c\tau + d}\,\eta(\tau)$$

for some 24-th root of unity $\epsilon(\gamma)$ and for the choice $\Re\sqrt{c\tau + d} \geq 0$.

As $\mathrm{SL}_2(\mathbb{Z})$ is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, we only need to understand the transformation under S and T. Because

$$\eta(\tau + 1) = \zeta_{24} q^{\frac{1}{24}} \prod_{m\geq 1}(1-q^m) = \zeta_{24}\eta(\tau),$$

we conclude that $\epsilon(T) = \zeta_{24}$. To compute $\epsilon(S)$, we note that for $\tau \in i\mathbb{R}$ the values $\eta(\tau)$ and $\eta(\frac{-1}{\tau})$ are real and positive. If now we evaluate at i, we obtain that

$$\eta\left(\frac{-1}{i}\right) = \epsilon(S)\sqrt{i}\,\eta(i)$$

and so $1 = \epsilon(S)\sqrt{i}$. But the square root of i with positive real part is $\zeta_8 = \exp(2\pi i/8)$, and so

$$\epsilon(S) = \sqrt{i}^{-1} = (\zeta_8)^{-1} = \zeta_{24}^{-3}.$$

The transformation under any matrix $U \in \mathrm{SL}_2(\mathbb{Z})$ is given by the following formula. We normalize $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ so that $c \geq 0$ and $a > 0$ if $c = 0$.

Proposition 1 (Meyer's formulas)**.** *Let $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ be an unimodular matrix normalized with $c \geq 0$ and $a > 0$ if $c = 0$. Set $c = 2^r c_0$ with c_0 odd if $c \neq 0$, for $c = 0$ set $c_0 = 1$ and $r = 0$. Then the transformation of η is given by*

$$(\eta \circ U)(\tau) = \left(\frac{a}{c_0}\right) \zeta_{24}^{ab+cd(1-a^2)-ca+3c_0(a-1)+(3/2)r(a-1)} \sqrt{c\tau + d}\,\eta(\tau),$$

where $\left(\frac{a}{c_0}\right)$ is the Kronecker symbol.

Proof. See [5, Theorem 3.1]. Note that if $c = 0$ then $U = T^b$ and $\eta(\tau) \circ T^b = \zeta_{24}^b \eta(\tau)$. □

We note that the map $\epsilon : U \mapsto \left(\frac{a}{c_0}\right) \zeta_{24}^{ab+cd(1-a^2)-ca+3c_0(a-1)+3/2r(a-1)}$ is not a homomorphism on $\mathrm{SL}_2(\mathbb{Z})$. This is easily seen by noting that S is of order 4 but $\epsilon(S)^4 = -1$.

3 Algebraic number theory for imaginary quadratic fields

In this part we recall the algebraic number theory we need in the following chapters. We begin with studying orders in imaginary quadratic fields and then we study what class field theory says for imaginary quadratic fields.

Throughout this section, let K be an imaginary quadratic number field, that is, let $K = \mathbb{Q}(\sqrt{d})$ for some $d < 0$ square-free.

3.1 Orders

An order in K is a subring $\mathcal{O} \subset K$ (containing 1) such that $\mathcal{O}$ is finitely generated as a $\mathbb{Z}$-module and $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = K$. This implies that $\mathcal{O}$ is of rank 2 as a $\mathbb{Z}$-module. It can be easily shown that any element of $\mathcal{O}$ is an algebraic integer. Let ω_1, ω_2 be a $\mathbb{Z}$-basis of $\mathcal{O}$. Define the discriminant of $\mathcal{O}$ as

$$\Delta(\mathcal{O}) = \det \begin{pmatrix} \omega_1 & \omega_2 \\ \sigma(\omega_1) & \sigma(\omega_2) \end{pmatrix}^2$$

where σ denotes the nontrivial automorphism in $\mathrm{Gal}(K/\mathbb{Q})$. By Galois invariance of $\Delta(\mathcal{O})$ and the integrality of ω_1 and ω_2, we see that $\Delta(\mathcal{O}) \in \mathbb{Z}$.

Define the field discriminant d_K as

$$d_K = \begin{cases} d & d \equiv 1 \bmod 4 \\ 4d & d \not\equiv 1 \bmod 4 \end{cases}.$$

Then there exists a maximal order $\mathcal{O}_K$ of K (with respect to the inclusion ordering), which is the integral closure of $\mathbb{Z}$ in K and is given as

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right]$$

Any order $\mathcal{O}$ is of finite index f in $\mathcal{O}_K$ and f is called the conductor of $\mathcal{O}$. Then

$$\mathcal{O} = \mathbb{Z} + f \cdot \mathcal{O}_K.$$

Indeed, as $\mathcal{O}$ is of index f in $\mathcal{O}_K$, clearly $f\mathcal{O}_K \subset \mathcal{O}$ and so $\mathbb{Z} + f\mathcal{O}_K \subset \mathcal{O}$. On the other hand, $\mathbb{Z} + f\mathcal{O}_K$ is clearly of index f in $\mathcal{O}_K$ and so $\mathcal{O} = \mathbb{Z} + f \cdot \mathcal{O}_K$.

Therefore, any order in K is given by its conductor in the maximal order. It is also easy to show now that for discriminants we have $\Delta(\mathcal{O}) = f^2\Delta(\mathcal{O}_K)$.

3.1.1 Ideals

Let $\mathcal{O}$ be an order and let $\mathfrak{a}$ be a non-zero finitely generated $\mathcal{O}$-submodule of K. Then we say that $\mathfrak{a}$ is a fractional $\mathcal{O}$-ideal. Clearly any $\mathcal{O}$-ideal is a fractional $\mathcal{O}$-ideal. A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is called invertible if and only if there exists some fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$.

Clearly principal fractional ideals $\alpha\mathcal{O}$ for $\alpha \in K^*$ are invertible.

It is obvious that the set $I(\mathcal{O})$ of all invertible ideals is a group with the identity element $\mathcal{O}$. Denote by $P(\mathcal{O})$ the subgroup of principal fractional ideals. Define the class group of $\mathcal{O}$ as

$$Cl(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}).$$

It is a standard fact that the class group $Cl(\mathcal{O})$ is a finite group and we call the order of $Cl(\mathcal{O})$ the class number of $\mathcal{O}$, denoted by $h(\mathcal{O})$.

If $\mathcal{O}$ is of conductor f, then every $\mathcal{O}$-ideal prime to f is invertible and the subgroup generated by $\mathcal{O}$-ideals coprime to f is denoted by $I(\mathcal{O}, f)$. The subgroup generated by principal $\mathcal{O}$-ideals coprime to f is denoted by $P(\mathcal{O}, f)$. Then we have the isomorphism (see [3, Proposition 7.19])

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I(\mathcal{O})/P(\mathcal{O}) = Cl(\mathcal{O}).$$

To relate the ideals of $\mathcal{O}$ to the ideals of $\mathcal{O}_K$, we first define for any $\mathcal{O}_K$-ideal $\mathfrak{m} \neq 0$ the subgroup $I_K(\mathfrak{m}) \subset I(\mathcal{O}_K)$ generated by $\mathcal{O}_K$-ideals coprime to $\mathfrak{m}$ and the subgroup

$$P_{K,\mathbb{Z}}(\mathfrak{m}) = \{\alpha\mathcal{O}_K \subset I_K(\mathfrak{m}) : \exists a \in \mathbb{Z} : \alpha \equiv a \bmod \mathfrak{m}\}$$

Proposition 2. *Let K be an imaginary quadratic field, let f be an integer and let $\mathcal{O}$ be an order of conductor f. Then*

$$Cl(\mathcal{O}) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I_K(f)/P_{K,\mathbb{Z}}(f)$$

Proof. See [3, Proposition 7.22]. □

Moreover, the class number of an order can be related to the class number of the maximal order in the following way:

Theorem 1. *Let $\mathcal{O} \subset \mathcal{O}_K$ be an order of conductor f. Then*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \cdot f \cdot \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) \tag{1}$$

and so $h(\mathcal{O})$ is always an integer multiple of $h(\mathcal{O}_K)$.

Proof. See [3, Corollary 7.28]. □

Ideals and quadratic forms

Let $F = aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y]$ be a binary quadratic form. Suppose that the discriminant $D = b^2 - 4ac$ of F is equal to the discriminant $\Delta(\mathcal{O})$. Suppose that F satisfies $\gcd(a, b, c) = 1$, so we say that F is primitive. Further require that $a > 0$, making F into a positive definite form.

For any such $F =: [a, b, c]$, the ideal

$$[a, \frac{-b + \sqrt{D}}{2}] := a\mathbb{Z} + \frac{-b + \sqrt{D}}{2}\mathbb{Z}$$

is an invertible ideal of $\mathcal{O}$ (see [3, Theorem 7.7]).

We call F a reduced form if $|b| \leq a \leq c$ and $b \geq 0$ if $|b| = |a|$ or $a = c$. The classical theory of quadratic forms shows that reduced forms are a set of representatives of the $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes under the action

$$F(X, Y) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} F(X, Y) = F(aX + bY, cX + dY).$$

Then there is a bijection between

$$Cl(\mathcal{O}) \leftrightarrow \{\text{reduced forms of discriminant } \Delta(\mathcal{O})\}$$

Ideals and elliptic curves

Let Λ be a lattice in $\mathbb{C}$ of full rank and let $E = \mathbb{C}/\Lambda$ be the corresponding elliptic curve. Embed $K \subset \mathbb{C}$. Then $\mathcal{O} \subset \mathbb{C}$ is a lattice of full rank. Recall that if $\mathrm{End}(E) \supsetneq \mathbb{Z}$, we say that E has complex multiplication. Moreover, any endomorphism $\alpha \in \mathrm{End}(E) \subset \mathbb{C}$ is then an non-real quadratic algebraic integer.

The following equivalent properties follow a connection between orders and elliptic curves.

1. $\mathrm{End}(E) \cong \mathcal{O}$, that is, E has complex multiplication by $\mathcal{O}$,
2. there exists an $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda$ is an invertible ideal of $\mathcal{O}$.

Therefore, we obtain the following bijections of sets

$$\begin{gathered} \{\mathbb{C}/\Lambda \text{ with complex multiplication by } \mathcal{O}\}/\sim \\ \updownarrow \\ Cl(\mathcal{O}) \\ \updownarrow \\ \{\text{ primitive reduced quadratic forms of discriminant } \Delta(\mathcal{O})\} \end{gathered}$$

3.2 Class field theory

In this part, we summarize the main theorems of class field theory for imaginary quadratic fields. We formulate the main theorems of class field theory in the language of ideals. Let K be an imaginary quadratic number field and denote by $\mathcal{O}_K$ the maximal order of K.

3.2.1 Cycles and the Artin map

A modulus or a cycle of K is an $\mathcal{O}_K$-ideal $\mathfrak{m} \neq 0$. To any abelian extension L/K we will assign a modulus $\mathfrak{m}$ called the conductor. Intuitively, the conductor will describe the ramification in L/K.

Let L/K be an abelian extension and let $\mathfrak{m}$ be a modulus divisible by all primes that ramify in L/K. Given any non-zero prime $\mathcal{O}_K$-ideal $\mathfrak{p}$ unramified in L/K, we can define its Artin symbol

$$\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$$

as follows (see the discussion after Lemma 5.19 of [3]). Let $\mathfrak{P}$ be any prime ideal of $\mathcal{O}_L$ such that $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Then, as $\mathfrak{p}$ is unramified in L/K, there exists a unique element $\sigma \in \mathrm{Gal}(L/K)$ such that

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{P})} \bmod \mathfrak{P} \quad \text{for all } \alpha \in \mathcal{O}_L.$$

The automorphism σ is independent of the choice of $\mathfrak{P}$ lying above $\mathfrak{p}$. So we can set $\left(\frac{L/K}{\mathfrak{p}}\right) := \sigma$.

Let $I_K(\mathfrak{m})$ be the group of fractional ideals coprime to $\mathfrak{m}$. Then assigning the Artin symbol to a prime ideal coprime to $\mathfrak{m}$ extends uniquely as a homomorphism to the Artin map

$$\phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K).$$

The Artin map is surjective (see [3, Theorem 8.2]).

Let $\mathfrak{m}$ be a cycle of K. Denote by $I_K(\mathfrak{m})$ the set of $\mathcal{O}_K$-ideals coprime to $\mathfrak{m}$ and let

$$P_{K,1}(\mathfrak{m}) = \langle \alpha\mathcal{O}_K : \alpha \equiv 1 \bmod \mathfrak{m} \rangle \subset I_K(\mathfrak{m}).$$

Then any group H satisfying

$$P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$$

is called a congruence subgroup for $\mathfrak{m}$ and the quotient group $I_K(\mathfrak{m})/H$ is called a generalized class group. Note that for an order $\mathcal{O}$ of conductor f the class group

$$Cl(\mathcal{O}) = I_K(f)/P_{K,\mathbb{Z}}(f)$$

is a generalized class group as $P_{K,1}(f) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f)$.

We are now ready to state the main theorem of class field theory. All these theorems hold for any number field K, however, the definition of a cycle must then be adjusted.

Theorem 2 (Class field theory for K, conductor)**.** *Let L/K be an abelian extension of K. Then there exists a cycle $\mathfrak{f}$, called the conductor of L/K, such that*

- *A prime ramifies in L/K if and only if it divides $\mathfrak{f}$.*
- *If $\mathfrak{m}$ is divisible by all primes that ramify in L/K, then $\ker(\phi_{L/K,\mathfrak{m}})$ is a congruence subgroup if and only if $\mathfrak{m}|\mathfrak{f}$.*

Proof. See [3, Theorem 8.5]. □

Theorem 3 (Class field theory for K, existence)**.** *Fix an algebraic closure $\overline{K}$ of K. Let $\mathfrak{m}$ be a cycle for K and let H be a congruence subgroup modulo $\mathfrak{m}$. There exists a unique abelian extension $L \subset \overline{K}$ of K such that:*

- *All the primes that ramify in L/K divide $\mathfrak{m}$.*

- *Under the Artin map* $\phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ *we have precisely* $H = \ker \phi_{\mathfrak{m}}$ *and so*

$$\mathrm{Gal}(L/K) \cong I_K(\mathfrak{m})/H$$

Proof. See [3, Theorem 8.6]. □

We will also note the following important corollary.

Corollary 1. *Let* M/K *and* L/K *be abelian extensions. Then* $M \hookrightarrow L$ *if and only if there exists a cycle* $\mathfrak{m}$ *divisible by all the primes ramified in* L *and* M*, such that*

$$P_{K,1}(\mathfrak{m}) \subset \ker \phi_{L/K,\mathfrak{m}} \subset \ker \phi_{M/K,\mathfrak{m}}.$$

Proof. For a proof, see [3, Corollary 8.7]. □

3.2.2 Hilbert, ray and ring class fields

We have already seen that $Cl(\mathcal{O}_K) = I_K/P_K = I_K(1)/P_{K,1}(1)$ is a (generalized) class group for modulus (1) and so there exists a unique abelian extension H_K of K, which is unramified at all primes, such that

$$\mathrm{Gal}(H_K/K) \cong Cl(\mathcal{O}_K)$$

The field H_K is called the Hilbert class field and it is the maximal unramified abelian extension of K. The uniqueness follows from Corollary 1: indeed, any other unramified extension M/K has conductor $\mathfrak{f} = 1$ and so $\ker(\phi_{M/K,1})$ is a congruence subgroup for modulus 1, that is,

$$P_{K,1} = \ker(\phi_{H_K/K,1}) \subset \ker(\phi_{M/K,1}).$$

And so $M \subset H_K$ by the corollary. Note that in fact, for the Hilbert class field H_K, the kernel of the Artin map for any modulus $\mathfrak{m}$ is equal to

$$\ker(\phi_{H_K/K,\mathfrak{m}}) = P_K(\mathfrak{m}).$$

From the existence theorem (Theorem 3), we see that for any modulus $\mathfrak{m}$ the choice of $H = P_{K,1}(\mathfrak{m})$ gives us the existence of a class field $H_{\mathfrak{m}}$ such that

$$\mathrm{Gal}(H_{\mathfrak{m}}/K) \cong I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) := Cl_{\mathfrak{m}}.$$

We call the field $H_{\mathfrak{m}}$ the ray class field of modulo $\mathfrak{m}$.

Using Corollary 1 again, as any congruence subgroup H satisfies $P_{K,1}(\mathfrak{m}) \subset H$ for some modulus $\mathfrak{m}$, any abelian extension of K is contained in the ray class field $H_{\mathfrak{m}}$ for some $\mathfrak{m}$. Therefore,

$$K^{ab} = \bigcup H_{\mathfrak{m}} \quad \text{and} \quad \mathrm{Gal}(K^{ab}/K) = \varprojlim Cl_{\mathfrak{m}}$$

We have also seen that $Cl(\mathcal{O})$ is a generalized class group for any order $\mathcal{O}$ of conductor f in $\mathcal{O}_K$. Then there exists a class field $H_{\mathcal{O}}$, called the ring class field, satisfying

$$P_{K,1}(f) \subset \ker(\phi_{H_{\mathcal{O}}/K,f}) = P_{K,\mathbb{Z}}(f) \subset P_K(f)$$

and so $H_{\mathcal{O}} \supset H_K$, that is, any ring class field contains the Hilbert class field and is itself contained in the ray class field of modulus f.

Let $\mathfrak{m}$ be an $\mathcal{O}$-ideal in the order $\mathcal{O}$ of conductor f. Let $I(\mathfrak{m})$ be the set of fractional $\mathcal{O}$-ideals coprime to $\mathfrak{m}$ and let

$$R(\mathfrak{m}) = \{\alpha\mathcal{O} : \alpha \equiv 1 \bmod \mathfrak{m}\} \subset I(\mathfrak{m}).$$

be the ray modulo $\mathfrak{m}$. Note that $P_{K,1}(\mathfrak{m})$ is the ray modulo $\mathfrak{m}$ in $\mathcal{O}_K$.

Then $R(\mathfrak{m}) \subset I(\mathfrak{m})$ is a subgroup of finite index and the quotient group $C_{\mathfrak{m}}(\mathcal{O}) = I(\mathfrak{m})/R(\mathfrak{m})$ we call the ray class group modulo $\mathfrak{m}$ for $\mathcal{O}$. The ray class group fits into the exact sequence

$$\mathcal{O}^\times \longrightarrow (\mathcal{O}/\mathfrak{m})^\times \longrightarrow Cl_{\mathfrak{m}}(\mathcal{O}) \longrightarrow Cl(\mathcal{O}) \longrightarrow 1. \tag{2}$$

The surjectivity is a consequence of the fact that any class in $Cl(\mathcal{O})$ contains an ideal coprime to $\mathfrak{m}$ for any ideal $\mathfrak{m}$. For the rest of the proof see [**?**, Proposition 1.6].

Because we always have a surjection $Cl_{f\mathfrak{m}}(\mathcal{O}_K) \twoheadrightarrow Cl_{\mathfrak{m}}(\mathcal{O}) \twoheadrightarrow Cl_{\mathfrak{m}}(\mathcal{O}_K)$, we obtain that

$$\mathrm{Gal}(K^{ab}/K) = \varprojlim Cl_{\mathfrak{m}} = \varprojlim Cl_{\mathfrak{m}}(\mathcal{O})$$

and it does not matter which ray class groups we are using. Moreover, despite the fact that taking inverse limits is not exact in general, in this case we can prove (for a proof by abstract nonsense see Lemma 12.27.4 of [10, Tag 02MY]) that taking the limit of (2) yields the exact sequence

$$\widehat{\mathcal{O}}^\times \longrightarrow \mathrm{Gal}(K^{ab}/K) \longrightarrow Cl(\mathcal{O}) \longrightarrow 1$$

for the profinite completion

$$\widehat{\mathcal{O}}^\times = \varprojlim (\mathcal{O}/\mathfrak{m}\mathcal{O})^\times$$

and using that

$$Cl(\mathcal{O}) = \mathrm{Gal}(K^{ab}/K)/\mathrm{Gal}(K^{ab}/H_{\mathcal{O}}),$$

looking at the kernel of the map $\widehat{\mathcal{O}}^\times \to \mathrm{Gal}(K^{ab}/K)$ we can also deduce that the following sequence is exact

$$1 \longrightarrow \mathcal{O}^\times \longrightarrow \widehat{\mathcal{O}}^\times \longrightarrow \mathrm{Gal}(K^{ab}/H_{\mathcal{O}}) \longrightarrow 1. \tag{3}$$

3.2.3 Genus theory

We have seen that class field theory describes, if somewhat indirectly, all abelian extensions of the field K. A related question is to describe all abelian extensions L/K such that $L/\mathbb{Q}$ is abelian. An important step is the following theorem, describing all unramified extensions L/K with $L/\mathbb{Q}$ abelian.

Theorem 4 (Genus theory)**.** *Let K be an imaginary quadratic field of discriminant D and let $p_1, \ldots, p_r$ be the odd primes dividing D. Set $p_i^* = (-1)^{\frac{p_i-1}{2}} p_i$. Then the maximal unramified extension K^{gen}/K such that $\mathrm{Gal}(K^{gen}/\mathbb{Q})$ is abelian is the field*

$$K^{gen} = K(\sqrt{p_1^*}, \ldots, \sqrt{p_r^*}).$$

Note that the genus field K^{gen} is always contained in the Hilbert class field $H_K = H_{\mathcal{O}_K}$.

4 The theorems of complex multiplication

Let K be an imaginary quadratic number fields. In the previous chapter, we discussed the class field theory for K. We know, for instance, that for any ideal $\mathfrak{m}$ of the maximal order $\mathcal{O}_K$, there is the ray class field $H_\mathfrak{m}$ satisfying

$$\mathrm{Gal}(H_\mathfrak{m}/K) \cong Cl_\mathfrak{m},$$

where $Cl_\mathfrak{m}$ is the ray class group for $\mathfrak{m}$. For any order $\mathcal{O} \subset K$, we also know that there exists a ring class field $H_\mathcal{O}$ with Galois group

$$\mathrm{Gal}(H_\mathcal{O}/K) \cong Cl(\mathcal{O}).$$

In this part, we will deal with the theory describing the ray class fields and ring class fields more explicitly, using values of certain modular functions: for instance, the ring class field can be generated by the j-invariant $j(\mathcal{O})$.

In general, the minimal polynomial of $j(\mathcal{O})$ has very big coefficients and is therefore less suitable for explicit calculations. In chapters 5 and 6 we will discuss some of the practical improvements that can be achieved.

4.1 The first main theorem of complex multiplication

Let $\mathcal{O}$ be an order in K. Considering an embedding $K \subset \mathbb{C}$, the order $\mathcal{O} \subset \mathbb{C}$ becomes a lattice of full rank, and therefore gives an elliptic curve $\mathbb{C}/\mathcal{O}$. Denote the j-invariant of the order by

$$j(\mathcal{O}) := j(\mathbb{C}/\mathcal{O}).$$

Note that for $\mathcal{O} = \mathbb{Z}[\tau]$ with $\tau \in \mathbb{H}$, we have $j(\mathcal{O}) = j(\tau)$. Similarly, for any $\mathcal{O}$-ideal $\mathfrak{a}$ we obtain the j-invariant $j(\mathfrak{a}) := j(\mathbb{C}/\mathfrak{a})$. It is clear that if $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals in the same class in $Cl(\mathcal{O})$, their j-invariants are the same: indeed, then $\mathfrak{a} = \alpha\mathfrak{b}$ for some $\alpha \in K^\times$ and so $j(\mathfrak{a}) = j(\mathfrak{b})$ by the homogeneity of j. The following theorem summarizes some of the miraculous properties of the values $j(\mathfrak{a})$.

Theorem 5 (First main theorem of complex multiplication)**.** *Let $\mathcal{O} \subset K$ be an order in an imaginary quadratic field of discriminant $D = \Delta(\mathcal{O})$. Then the following holds:*

1. *The number $j(\mathcal{O})$ is an algebraic integer.*
2. *The minimal polynomial $H_D(X)$ of $j(\mathcal{O})$ factors over $\mathbb{C}$ as*
$$H_D(X) = \prod_{\mathfrak{a} \in Cl(\mathcal{O})} (X - j(\mathfrak{a})).$$
3. *The field $K(j(\mathcal{O}))$ is the ring class field of $\mathcal{O}$, that is,*
$$H_\mathcal{O} = K(j(\mathcal{O})).$$
4. *Recall that the Galois group $\mathrm{Gal}(H_\mathcal{O}/K)$ is naturally isomorphic with $Cl(\mathcal{O})$ via the Artin map. Under this isomorphism, the action of $[\mathfrak{b}] \in Cl(\mathcal{O})$ on the conjugates $j(\mathfrak{a})$ of $j(\mathcal{O})$ is given as*
$$j(\mathfrak{a})^\mathfrak{b} = j(\mathfrak{b}^{-1}\mathfrak{a}).$$

Proof. See Theorem 1 in [8, Chapter 10]. □

The significance of this theorem is that it gives the generators of the ring class fields of K as values of the j-function, which is a modular function for the group $\mathrm{SL}_2(\mathbb{Z})$.

4.2 Modular functions of level N

In the previous subsection, we have already seen the power of the j-function, which is a modular function for the congruence subgroup of level 1. In the following, modular functions of higher level will play a similar role: they will be used to produce numbers lying in ray class fields.

Recall that $f : \mathbb{H} \to \mathbb{C}$ is a modular function of level N if it is a meromorphic function on $\mathbb{H}$ invariant under $\Gamma(N)$ that can be extended to a meromorphic function on the compactification $X(N) := \overline{\Gamma(N) \setminus \mathbb{H}}$. Let $F_{N,\mathbb{C}}$ be the field of modular functions of level N. Then $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ acts on $F_{N,\mathbb{C}}$ as

$$f \mapsto f \circ \gamma \in F_{N,\mathbb{C}}.$$

We claim that $f \circ \gamma$ is again a modular function of level N:

$$f \circ \gamma \in F_{N,\mathbb{C}}.$$

As $f \circ \gamma$ is clearly meromorphic, we only need to check the invariance under $\alpha \in \Gamma(N)$. As $\Gamma(N) \subset \mathrm{SL}_2(\mathbb{Z})$ is a normal subgroup, there exists $\alpha' \in \Gamma(N)$ such that $\gamma\alpha = \alpha'\gamma$ and so by $\Gamma(N)$-invariance of f we see that

$$(f \circ \gamma) \circ \alpha = f \circ \alpha' \circ \gamma = f \circ \gamma.$$

Therefore, $\mathrm{SL}_2(\mathbb{Z})$ has a well-defined action on $F_{N,\mathbb{C}}$. We will now quote some structural results for the fields of modular functions.

Theorem 6. $F_{1,\mathbb{C}} = \mathbb{C}(j)$.

Proof. See Theorem 1 in [8, Chapter 6]. □

In fact,

$$j : \overline{\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}} = X(1) \cong \mathbb{P}^1(\mathbb{C})$$

is an analytic isomorphism and $\mathcal{F}_{1,\mathbb{C}} = \mathbb{C}(j)$ is the function field of $X(1)$.

Theorem 7. *$F_{N,\mathbb{C}}$ is Galois over $F_{1,\mathbb{C}}$ with Galois group*

$$\mathrm{SL}_2(\mathbb{Z})/\pm\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1.$$

Proof. See Theorem 2 in [8, Chapter 6]. □

As an aside, we note that for $N \geq 1$ the field of modular functions $F_{N,\mathbb{C}}$ is the function field of $X(N)$, which is a compact Riemann surface and also a projective curve. The (non-compact) curves $Y(N) = \Gamma(N) \setminus \mathbb{H}$ have a moduli interpretation as the moduli spaces of elliptic curves with a fixed basis of their N-torsion. Moreover, it can be shown that the curves $X(N)$ have models over $\mathbb{Q}(\zeta_N)$.

4.2.1 Modular function fields over $\mathbb{Q}(\zeta_N)$

Fix $\zeta_N = \exp(2\pi i/N)$ a primitive N-th root of unity and let $\mathcal{F}_N$ be the field of modular functions of level N such that the coefficients of its q-expansion lie in $\mathbb{Q}(\zeta_N)$. Because the j-invariant has rational q-expansion (in fact integral), we obtain that $\mathcal{F}_1 = \mathbb{Q}(j)$.

For any $f \in \mathcal{F}_N$, the group $\mathrm{SL}_2(\mathbb{Z})$ acts on f as before as

$$f \mapsto f \circ \alpha$$

Moreover, as f is $\Gamma(N)$-invariant, this action factors through $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N)$ and so we also obtain the action of

$$\mathcal{F}_N \circlearrowleft \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\Gamma(N).$$

This action induces an injection

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1 \hookrightarrow \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1).$$

Moreover, $\mathbb{Q}(\zeta_N) \subset \mathcal{F}_N$ and for any $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ we obtain an automorphism $\sigma_d : \zeta_N \mapsto \zeta_N^d$ of $\mathbb{Q}(\zeta_N)$. This automorphism extends to an automorphism of $\mathcal{F}_N$, acting on the q-expansions:

$$\sum_{m\in\mathbb{Z}} a_n q^{m/N} \mapsto \sum_{m\in\mathbb{Z}} \sigma_d(a_n) q^{m/N}.$$

Then these give all the automorphisms of $\mathcal{F}_N/\mathcal{F}_1$: in fact,

$$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong (\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\langle\pm 1\rangle) \rtimes (\mathbb{Z}/N\mathbb{Z})^\times.$$

Moreover, if we embed $(\mathbb{Z}/N\mathbb{Z})^\times$ to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong \left\{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} : d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\},$$

then we have the following split exact sequence

$$1 \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow 1.$$

Then

$$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1.$$

Let $\mathcal{F} = \bigcup_N \mathcal{F}_N$. Taking limits we obtain a short exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}}) \longrightarrow \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1.$$

4.2.2 The second main theorem of complex multiplication

We have seen the connection between special values of the j-invariant function and abelian extensions of K in the First main theorem of complex multiplication (Theorem 5). A similar connection occurs for special values of function in $\mathcal{F}_N$.

Recall that K is an imaginary quadratic field and $\mathcal{O} = \mathbb{Z}[\tau]$ is an order in K. We start from the exact sequence (3), which we recall here again:

$$1 \longrightarrow \mathcal{O}^\times \longrightarrow \widehat{\mathcal{O}}^\times \longrightarrow \mathrm{Gal}(K^{ab}/H_{\mathcal{O}}) \longrightarrow 1.$$

For every finite quotient $(\widehat{\mathcal{O}}/N\widehat{\mathcal{O}})^\times = (\mathcal{O}/N\mathcal{O})^\times$ we get a field $H_{N,\mathcal{O}}$ for which the Artin map gives

$$(\mathcal{O}/N\mathcal{O})^\times/\mathrm{im}[\mathcal{O}^\times] \cong \mathrm{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}}).$$

We call $H_{N,\mathcal{O}}$ the ray class field of conductor N for $\mathcal{O}$.

Theorem 8 (The second main theorem of complex multiplication)**.** *Let $f \in \mathcal{F}_N$ be a modular function of level N and $\mathcal{O} = \mathbb{Z}[\tau]$ be an order in an imaginary quadratic field K with $\tau \in \mathbb{H}$. Suppose that τ is not a pole of f. Then*

$$f(\tau) \in H_{N,\mathcal{O}}$$

and moreover, $H_{N,\mathcal{O}} = K(g(\tau) : g \in \mathcal{F}_N, g(\tau) \neq \infty)$.

Proof. For maximal orders, see Lang's Elliptic functions [8, Corollary to Theorem 10.2]. For non-maximal orders, see also [11]. □

And as $j : \mathbb{H} \to \mathbb{C}$ is a modular function of level 1 without any poles on $\mathbb{H}$ and $\mathcal{F}_1 = \mathbb{Q}(j)$, the first main theorem follows from the the second main theorem.

4.3 Shimura reciprocity

In the previous section, we have seen that for the ray class fields $H_{N,\mathcal{O}}$ for order $\mathcal{O}$, we have $K^{ab} = \bigcup H_{N,\mathcal{O}}$.

We now construct the following connecting map in the diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}^\times & \longrightarrow & \widehat{\mathcal{O}}^\times & \longrightarrow & \mathrm{Gal}(K_{ab}/H_{\mathcal{O}}) & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle g_\tau} & & & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathrm{GL}_2(\widehat{\mathbb{Z}}) & \longrightarrow & \mathrm{Gal}(\mathcal{F}/\mathbb{Q}(j)) & \longrightarrow & 1, \end{array}$$

where the map $g_\tau : \widehat{\mathcal{O}}^\times \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ maps any $x \in \widehat{\mathcal{O}}^\times$ to the matrix $g_\tau(x)$ satisfying

$$g_\tau(x)\begin{pmatrix}\tau\\1\end{pmatrix} = x\begin{pmatrix}\tau\\1\end{pmatrix},$$

so $g_\tau(x)$ is the matrix of the multiplication by $x \in \widehat{\mathcal{O}}^\times$ on $\widehat{\mathcal{O}} = \widehat{\mathbb{Z}}\tau + \widehat{\mathbb{Z}}$ with respect to the basis $[\tau, 1]$. Using that $\tau^2 = -B\tau - C$, we get an explicit description for any $x = s\tau + t \in \widehat{\mathcal{O}}^\times$:

$$g_\tau(s\tau + t) = \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix}.$$

The map g_τ induces an action of $\widehat{\mathcal{O}}^\times$ on the modular function field $\mathcal{F} = \bigcup \mathcal{F}_N$.

Theorem 9 (Shimura's reciprocity law)**.** *Let $f \in \mathcal{F}$ be a modular function such that τ is not a pole of f and let $x \in \widehat{\mathcal{O}}^\times$, then*

$$f(\tau)^{x^{-1}} = \left(f^{g_\tau(x)}\right)(\tau).$$

Proof. See Theorem 2 in [6, Class invariants by Shimura's reciprocity law] for maximal orders. For non-maximal orders, see [11]. □

Let $f \in \mathcal{F}_N$ and suppose τ is not a pole of f. Then $f(\tau) \in H_{N,\mathcal{O}}$ by the second main theorem of complex multiplication (Theorem 8) and therefore the action of $\widehat{\mathcal{O}}^\times$ on $f(\tau)$ factors through the finite quotient $(\mathcal{O}/N\mathcal{O})^\times$ and fits in the following diagram with exact rows

$$\begin{array}{ccccccccc} \mathcal{O}^\times & \longrightarrow & (\mathcal{O}/N\mathcal{O})^\times & \longrightarrow & \mathrm{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}}) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle g_\tau} & & & & \\ \{\pm 1\} & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j)) & \longrightarrow & 1. \end{array}$$

Denote by $W_{N,\tau}$ the image of the map g_τ. Then

$$W_{N,\tau} \cong (\mathcal{O}/N\mathcal{O})^\times \cong \mathrm{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}}).$$

Let $f \in \mathcal{F}_N$ be a modular function and suppose that τ is not a pole of f. We already know that $f(\tau) \in K^{ab}$. If $f(\tau) \in H_{\mathcal{O}}$ is an element of the ring class field of $\mathcal{O}$, we call $f(\tau)$ a class invariant. Note that we no longer require that $f(\tau)$ generates the ring class field $H_{\mathcal{O}}$ over K. The following corollary gives us explicit tools how to show that $f(\tau)$ is a class invariant.

Corollary 2. *Let $f \in \mathcal{F}_N$ be a modular function of level N and suppose that $\tau \in \mathbb{H}$ as before is not a pole of f. Then*

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

Proof. See [6, Class invariants by Shimura's reciprocity law], Corollary 4. □

Generators of the group $(\mathcal{O}/N\mathcal{O})^\times$ can be found easily for modest values of N and so describing the action of $W_{N,\theta}$ can be done explicitly.

5 Class invariants from eta quotients

Let K be an imaginary quadratic field and let n be a positive integer. In 4.2 we defined $\mathcal{F}_n$ as the field of modular functions of level n with q-expansions in $\mathbb{Q}(\zeta_n)$.

The theorems in chapter 4 give us tools for constructing elements lying in ring class fields. Let $\mathcal{O} = \mathbb{Z}[\theta]$ be an order in K of discriminant $D < -4$. Then $\mathcal{O}^\times = \{\pm 1\}$ and the ray class field of $\mathcal{O}$ with modulus n is the field $H_{n,\mathcal{O}}$, which satisfies

$$\mathrm{Gal}(H_{n,\mathcal{O}}/H_{\mathcal{O}}) \cong (\mathcal{O}/n\mathcal{O})^\times/\pm 1 \cong W_{n,\theta}/\pm 1$$

by Shimura reciprocity law (Theorem 9). In particular, we have seen that the value $f(\theta) \in H_{n,\mathcal{O}}$ satisfies $f(\theta) \in H_{\mathcal{O}}$ if and only if f is invariant under $W_{n,\theta}$ (see Corollary 2). If $f(\theta) \in H_{\mathcal{O}}$, we will call $f(\theta)$ a class invariant, in particular, we do not require that $f(\theta)$ generates $H_{\mathcal{O}}$ over K.

We already know that $H_{\mathcal{O}}$ is generated over K by the j-invariant $j(\mathcal{O})$. However, the minimal polynomial of $j(\mathcal{O})$ has large coefficients already for modest values of $D = \Delta(\mathcal{O})$. We show that taking suitable powers of the *generalized Weber functions*

$$\nu_{k,n}(\tau) = \frac{\eta(\frac{\tau+k}{n})}{\eta(\tau)}$$

for $k, n \in \mathbb{Z}$ (and $n > 1$) evaluated at θ can yield class invariants with smaller heights.

5.1 The Weber functions

In his classical "Lehrbuch der Algebra" [12], Weber defines the following functions

$$\mathfrak{f} = \zeta_{48}^{-1}\frac{\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)},\ \mathfrak{f}_1 = \frac{\eta(\tau/2)}{\eta(\tau)} \quad \text{and} \quad \mathfrak{f}_2 = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}$$

and gives a long list of theorems and some conjectural results about generating ring class fields using small powers of the Weber functions $\mathfrak{f}, \mathfrak{f}_1$ and $\mathfrak{f}_2$. For instance, we note the following theorem.

Theorem 10. *Let m be a positive integer not divisible by 3 and let $\mathcal{O} = \mathbb{Z}[\sqrt{-m}]$ and let $K = \mathbb{Q}(\sqrt{-m})$. Then:*

- *If $m \equiv 6 \bmod 8$ then $K(\mathfrak{f}_1(\sqrt{-m})^2)$ is the ring class field of $\mathcal{O}$.*
- *If $m \equiv 3 \bmod 4$ then $K(\mathfrak{f}(\sqrt{-m})^2)$ is the ring class field of $\mathcal{O}$.*

Proof. See [3, Theorem 12.24]. □

There are many relations between the functions $\mathfrak{f}, \mathfrak{f}_1$ and $\mathfrak{f}_2$, such as

$$\mathfrak{f} \cdot \mathfrak{f}_1 \cdot \mathfrak{f}_2 = \sqrt{2},$$

and if we define γ_2 to be the holomorphic cube root of j which is real on the imaginary axis, then $\mathfrak{f}^8$, $-\mathfrak{f}_1^8$ and $-\mathfrak{f}_2^8$ are the roots of

$$X^3 - \gamma_2 X - 16.$$

Such relations and a multitude of tricks were used by Weber and others to explicitly compute various class invariants (see the examples in Section 12 of [3]). A modern and a more systematic treatment of these theorems can be given using Shimura's reciprocity theorem. See, for instance, the extensive Theorem 1 in [9] and Section 8 of [6, Class invariants by Shimura's reciprocity law].

5.2 Generalized Weber functions

In the article [5], Enge and Morain develop a comprehensive theory for the functions

$$\mathfrak{w}_n = \frac{\eta(\frac{\tau}{n})}{\eta(\tau)}.$$

Let K be an imaginary quadratic field and let $\mathcal{O} \subset K$ be an order of discriminant D. The starting point for Enge and Morain is the following theorem of Enge and Schertz:

Theorem 11. *Let $\mathcal{O}$ be an order of discriminant D, let $\mathfrak{f}$ be a modular function for $\Gamma^0(n)$ and let $\mathfrak{f}$ and $\mathfrak{f} \circ S$ have rational q-expansion. Let $\alpha \in \mathbb{H}$ be a root of $Ax^2 + Bx + C$ with $D = B^2 - 4AC$ and suppose $n|C$ and $\gcd(A, n) = 1$. If $\mathfrak{f}(\alpha) \neq \infty$ is not a pole, then*

$$\mathfrak{f}(\alpha) \in H_{\mathcal{O}}.$$

Proof. See [5], Theorem 2.3. □

Enge and Morain apply Theorem 11 to suitable powers of the generalized Weber functions $\mathfrak{w}_n$. Suitable exponents for which these functions are modular are found using the following theorem 12, which also answers the rationality of their q-expansions and the levels. Set $t = \frac{24}{\gcd(n-1,24)}$ and write $n = 2^\lambda n_1$ with n_1 odd.

Theorem 12. *In the notation of this section, the following holds:*

1. *The function $\mathfrak{w}_n$ has rational q-expansion.*
2. *If n is a square then $\mathfrak{w}_n \circ S$ has rational q-expansion.*
   If n is not a square then $\mathfrak{w}_n^2 \circ S$ has rational q-expansion.
3. *Let e and s be positive integers such that $t|s|24$ and $e|s$. If n_1 is a square or e is even, then*

   $$\mathfrak{w}_n^e \text{ is modular for } \Gamma(\tfrac{s}{e}) \cap \Gamma^0(\tfrac{s}{e}n).$$

   Otherwise,

   $$\mathfrak{w}_n^e \text{ is modular for } \Gamma(\tfrac{s}{e}n_1) \cap \Gamma^0(\tfrac{s}{e}n).$$

Proof. See theorem 3.2 of [5]. □

We see that in both cases of part 3, $\mathfrak{w}_n^e$ is modular for $\Gamma(24n)$ and for the choice

$$s = \begin{cases} 2t & t \text{ odd and } n \text{ not a square} \\ t & \text{else} \end{cases}$$

and for α as in the theorem 11, the value $\mathfrak{w}_n^s(\alpha)$ lies in the ring class field $H_{\mathcal{O}}$.

Enge and Morain then ask the question whether it is possible to use smaller exponents e than the choice of s as above and still produce class invariants. They fix the level n and, in the notation of Theorem 11, determine congruence conditions on the discriminant D and trace B for which $\mathfrak{w}_n(\alpha)^e$ is a class invariant with exponent $e < s$. They give extensive tables of possible exponents and discriminants (see [5, section 6]) and their answers only depend on n modulo 24.

Enge and Morain then pose the question whether it would be possible to use smaller powers e, and thus numbers of smaller height, if one authorizes roots of unity to come to play. The answer for $n = 2$ is classical and goes back to Weber and the answers for $n = 3$ and for the case $\gcd(n, 6) = 1$ are given already given by Alice Gee in the last article of her thesis [6, Class invariants from Dedekind's eta function]. We will see more cases for which the answer is positive in chapter 6.

5.3 Level 3 and levels coprime to 6

In the last article of the thesis of Alice Gee [6], "Class invariants from Dedekind's eta function" (which preceded the article of Enge and Morain by fifteen years), Gee studies the functions

$$\nu_{k,n} = \frac{\eta\left(\frac{z+k}{n}\right)}{\eta(z)}$$

for all $k, n \in \mathbb{Z}$ and $n > 1$. These functions lie in the modular function field $\mathcal{F}_{24n}$ of level $24n$. Gee then uses Shimura reciprocity (see Theorem 9) to determine powers e and suitable small constants ϑ from $\mathbb{Q}(\zeta_{24n})$ so that for an order $\mathcal{O} = \mathbb{Z}[\theta]$ with $f^\theta_{\mathbb{Q}} = x^2 + Bx + C$ satisfying $B \in \{0, 1\}$, the resulting value

$$\vartheta \cdot \nu^e_{k,n}(\theta)$$

is a class invariant.

Note that the perceived difference between using the functions $\nu_{k,n}$ for varying k as Gee and $\mathfrak{w}_n = \nu_{0,n}$ with fixed $k = 0$ as Enge and Morain comes from evaluating at different elements. Gee evaluates at the singular modulus θ, whereas Enge and Morain choose α as a root of $A'x^2+B'x+C'$ satisfying $N|C'$ and of discriminant $B'^2 - 4A'C' = \Delta(\mathcal{O})$. If we suppose that $A' = 1$, which can usually be achieved, then for some $k \in \mathbb{Z}$ we have $\alpha = \theta + k$. Then, using the transformation rules for the eta function,

$$\mathfrak{w}_n(\theta + k) = \zeta_{24}^{-k}\nu_{k,n}(\theta).$$

For level $n = 3$, Gee gives a complete table of suitable powers of $\nu_{k,3}$ with $k \in \{0, 1, 2\}$ that upon multiplying by a suitable small $\vartheta \in \mathbb{Q}(\zeta_{24})$ produce class invariants in the case of maximal orders (see [6, Part 4, Table 2.]).

Gee obtains these results by computing the groups $W_{24\cdot 3,\theta}$ and their action on the functions $\nu_{k,3}$. The explicit determination of the group $W_{24\cdot 3,\theta}$ is easy in many cases using the isomorphism

$$W_{24\cdot 3,\theta} \cong (\mathcal{O}/72\mathcal{O})^\times.$$

Note that these groups depend on the splitting behaviour of the primes 2 and 3 in $\mathcal{O}$ and hence the congruence conditions on D.

Moreover, Gee also lists the following theorem for the case $\gcd(n, 6) = 1$:

Theorem 13. *Let $\mathcal{O} = \mathbb{Z}[\theta]$ be an imaginary quadratic order of discriminant D and let θ satisfy $f^\theta_{\mathbb{Q}}(x) = x^2 + Bx + C$ with $B \in \{0, 1\}$. Let $n \in \mathbb{Z}_{>1}$ satisfy*

$$n \equiv 1 \bmod 2 \cdot \gcd(D, 6).$$

Let $k \in \mathbb{Z}$ satisfy $f^\theta_{\mathbb{Q}}(x)(-k) \equiv 0 \bmod n$ and $k \equiv 0 \bmod 24$. Then

$$\zeta_3^{2B(n-1)}\nu^2_{k,n}(\theta) \in H_{\mathcal{O}}.$$

Proof. See [6, Theorem 2]. □

In the case $\gcd(n, 6) = 1$, Gee works with the decomposition

$$W_{24n,\theta} = G^{(n)}_{24n,\theta} \times G^{(8)}_{24n,\theta} \times G^{(3)}_{24n,\theta}$$

using the kernels of the reduction maps

$$G^{(m)}_{24n,\theta} = \ker(\mathrm{red} : W_{24n,\theta} \to W_{24n/m,\theta}).$$

The group $G^{(m)}_{24n,\theta}$ can be identified with $W_{m,\theta}$ provided $\gcd(m, 24n/m) = 1$ by taking the lifts to $\mathrm{GL}_2(\mathbb{Z}/24n\mathbb{Z})$ congruent to the identity matrix modulo $24n/m$.

The action described by Gee for $\gcd(n, 6) = 1$ (with the notation and the choice of k as before) is given as follows:

- $G_{24n,\theta}^{(n)}$ acts on $\nu_{k,n}$ as a quadratic character and so $\nu_{k,n}^2$ is invariant under $G_{24n,\theta}^{(n)}$ (see [6, Part 4, Theorem 10])
- any $M \in G_{24n,\theta}^{(8)}$ acts as
$$\nu_{k,n} \circ M = \zeta_8^{3\kappa(U)(n-1)} \nu_{k,n}$$
for a certain $U \in \Gamma$ and $\kappa(U)$ an explicit exponent (cf. the discussion following [6, Part 4, Theorem 10]) and if $2 \nmid D$, then $\kappa(U)$ is always even ([6, Part 4, Proposition 12]), and so
$$\text{if } D \text{ is odd, } \nu_{k,n}^2 \text{ is invariant under } G_{24n,\theta}^{(8)},$$
- any $M \in G_{24n,\theta}^{(3)}$ acts as
$$\nu_{k,n} \circ M = \zeta_3^{\kappa(U)(n-1)} \nu_{k,n}$$
for a certain $U \in \Gamma$ and $\kappa(U)$ an explicit exponent (cf. the discussion following [6, Part 4, Theorem 10]) and from ([6, Part 4, Proposition 15]) we obtain that
$$\text{if } 3 \nmid D, \text{ then } \zeta_3^{2B(n-1)} \nu_{k,n}^2 \text{ is invariant under } G_{24n,\theta}^{(3)}.$$

Put together, we obtain the same exponents e of $\nu_{k,n}$ as Enge and Morain in the table 6.1.1 of [5] (disregarding for the moment by which root of unity we need to multiply the suitable powers):

$n \equiv 1 \bmod 12$**:** Then $e = 2$ suffices to obtain the trivial action.

$n \equiv 5 \bmod 12$**:** Then $n - 1 \equiv 0 \bmod 4$ but $n - 1 \not\equiv 0 \bmod 3$ and so the action of $G_{24n,\theta}^{(8)}$ is trivial on $\nu_{k,n}^2$ and we see that either $e = 6$ or, if $3 \nmid D$, we can take $e = 2$.

$n \equiv 7 \bmod 12$**:** Then $n - 1 \equiv 0 \bmod 3$ and so the action of $G_{24n,\theta}^{(3)}$ is trivial on $\nu_{k,n}^2$ and as $n - 1 \equiv 6 \bmod 12$, we see that either $e = 4$ or, if $2 \nmid D$, we can take $e = 2$ using proposition 12 of [6].

$n \equiv 11 \bmod 12$**:** In this case, $n - 1 \not\equiv 0$ modulo 3 and so if $6|D$, then we need to take $e = 12$. The opposite case is $6 \nmid D$, which only requires $e = 2$. If $2 \nmid D$ but $3 \mid D$, then we obtain $e = 6$. If $3 \nmid D$, then both Gee and Enge and Morain require $e = 4$.

However, if $2|D$ and $D \equiv 4, 8 \bmod 16$, we can compute the groups $G_{24n,\theta}^{(8)}$ in more detail (see [6, Part 4, Proposition 13]) and this allows Gee to obtain a better result:

Theorem 14. *Let $D \equiv 4, 8 \bmod 16$ and let $n \in \mathbb{Z}_{>1}$ such that $\gcd(n, 6) = 1$. Suppose k satisfies $24|k$ and $f_{\mathbb{Q}}^{\theta}(x)(-k) \equiv 0 \bmod n$ and $n - 1 \equiv 0 \bmod \gcd(D, 3)$. Then*
$$\zeta_4^{(n-1)/2} \nu_{k,n}^2(\theta) \in H_{\mathcal{O}}.$$

Proof. See [6, Part 4, Proposition 3]. □

Let n and D and k be as in the theorem. If further $3 \nmid D$, we see that
$$\zeta_4 \nu_{k,n}^2(\theta) \in H_{\mathcal{O}},$$
and so in this case we only need to use $e = 2$ compared to $e = 4$ by Enge and Morain.

5.4 Generalized Weber functions with roots of unity

Let us fix the notation as follows: let $\mathcal{O} = \mathbb{Z}[\theta]$ be an order in the imaginary quadratic field K and let $D = \operatorname{disc}(\mathcal{O}) < -4$. Let $f = x^2 + Bx + C$ be the minimal polynomial of θ over $\mathbb{Q}$ with $B \in \{0, 1\}$.

5.4.1 Our method

As we saw in the application of theorem 14 (due to Gee), the explicit determination of the groups W_{24n} and their action on $\nu_{k,n}$ and the field $\mathbb{Q}(\zeta_{24n})$ can give smaller powers of $\nu_{k,n}$ than those obtained by Enge and Morain in [5]. As Gee practically exhausts the question of $\gcd(n,6)=1$ above, we focus mostly on the case when $\gcd(n,6)\neq 1$.

The gcd condition means that it is no longer enough to compute the action of $G^{(3)}_{24n,\theta}$ and $G^{(8)}_{24n,\theta}$ separately. Also, the groups $G^{(m)}_{24n,\theta}$ encountered grow bigger and so finding the generators for all the possible values of $x^2+Bx+C \bmod m$ by hand is more difficult. However, for small values of n, these groups are easily handled by a computer.

5.4.2 Theoretical computations

We want to compute the action of $W_{24n,\theta}\subset \mathrm{GL}_2(\mathbb{Z}/24n\mathbb{Z})$ on the functions $\nu_{k,n}$. We will use the decomposition

$$W_{24n,\theta}=\prod_m G^{(m)}_{24n,\theta},$$

where m runs over all the full powers dividing $24n$: for instance, for $n=4$ we obtain the decomposition

$$W_{96,\theta}=G^{(32)}_{96,\theta}\times G^{(3)}_{96,\theta}.$$

Our strategy is the following: we will try to find a suitable power e of $\nu_{k,n}$ such that the action of $W_{24\cdot n,\theta}$ on $\nu^e_{k,n}$ actually coincides with the action of $W_{24\cdot n,\theta}$ on some algebraic number $\vartheta\in\mathbb{Q}(\zeta_{24\cdot n})$. Then the function $\frac{\mathfrak{f}}{\vartheta}$ is $W_{24\cdot n,\theta}$-invariant and evaluating at θ will give a class invariant.

Fix for now $m|24n$ with $\gcd(m,\frac{24n}{m})=1$. In practice, m will be a full prime power dividing $24n$. We have already noted that in this case, we have the identification

$$G^{(m)}_{24n,\theta}\cong W_{m,\theta},$$

lifting the matrix $W\in W_{m,\theta}\subset \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ into a matrix $W'\in \mathrm{GL}_2(\mathbb{Z}/24n\mathbb{Z})$, which satisfies

$$W'\equiv\begin{cases} W & \bmod m\\ I & \bmod \frac{24n}{m}.\end{cases}$$

The groups $W_{m,\theta}$ are much easier enumerated than the groups $G^{(m)}_{24n,\theta}$. Whenever we talk about the action of $W_{m,\theta}$, we will always mean the action of $G^{(m)}_{24n,\theta}$, or, equivalently, the action of the lifts of $W_{m,\theta}$ to $W_{24n,\theta}$.

We now describe the process of lifting the matrices $W\in W_{m,\theta}$ to $W_{24n,\theta}$. Write $d=\det W$. Then W can be written as

$$W=\begin{pmatrix}1&0\\0&d\end{pmatrix}M'\in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

for some $M'\in \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. Then, we lift these matrices to $\mathrm{GL}_2(\mathbb{Z}/24n\mathbb{Z})$ separately:

- we can lift $\begin{pmatrix}1&0\\0&d\end{pmatrix}\in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ to $\begin{pmatrix}1&0\\0&x\end{pmatrix}\in \mathrm{GL}_2(\mathbb{Z}/24n\mathbb{Z})$ with x satisfying

  $$x\equiv\begin{cases}1 & \bmod \frac{24n}{m}\\ d & \bmod m\end{cases}$$

  using the Chinese remainder theorem,
- we can lift $M'\in \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ to $M\in\Gamma(\frac{24n}{m})$: indeed, we can use Chinese remainder theorem to obtain a matrix M'' satisfying

$$M'' \equiv \begin{cases} M' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mod m \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \mod \frac{24n}{m} \end{cases}$$

Then $\det M'' \equiv 1 \mod 24n$, again by the Chinese remainder theorem. We can now use the surjection

$$\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/24n\mathbb{Z})$$

to obtain a lift

$$M \in \mathrm{SL}_2(\mathbb{Z}) \text{ congruent to } M'' \mod 24n.$$

But this means that $M \equiv \begin{cases} M' & \mod m \\ I & \mod \frac{24n}{m} \end{cases}$, so in fact $M \in \Gamma(\frac{24n}{m})$.

Therefore, the action of any $W \in W_{m,\theta}$ on $\mathcal{F}_{24n}$, acting via its lift to $\mathrm{GL}_2(\mathbb{Z}/24n\mathbb{Z})$, decomposes as follows:

- the action of $\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}$, which acts only on the q-expansions of the functions in $\mathcal{F}_{24n}$,
- followed by the action of $M \in \Gamma(\frac{24n}{m}) \subset \Gamma$, acting on the arguments of the functions in $\mathcal{F}_{24n}$.

First compute the action of $X = \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/24n\mathbb{Z})$. We claim that X acts on $\nu_{k,n}$ as

$$\nu_{k,n} \mapsto \nu_{xk,n}.$$

Indeed, to compute how we act on the q-expansion, we see that the action of X on $\eta(\tau)$ is always trivial (as η has a rational q-expansion) and so we only need to compute the action on $\eta(\frac{\tau+k}{n})$. But this is easily read-off from the q-expansions. Set $q^{\frac{1}{n}} = \exp(2\pi i\tau/n)$. We know that

$$\exp(2\pi i(\tau+k)/n) = \zeta_n^k q^{\frac{1}{n}} \mapsto \zeta_n^{x\cdot k} q^{\frac{1}{n}} = \exp(2\pi i(\tau + x\cdot k)/n)$$

and so

$$\eta\left(\frac{\tau+k}{n}\right) \mapsto \eta\left(\frac{\tau+k\cdot x}{n}\right).$$

Therefore,

$$\nu_{k,n} \mapsto \nu_{kx,n}$$

and so for any $W \in W_{m,\theta}$, retaining the notation for x and M, the action on $\nu_{k,n}$ is given as

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

and we call the new matrix

$$N = \begin{pmatrix} 1 & kx \\ 0 & n \end{pmatrix} \circ M \circ \begin{pmatrix} 1 & k \\ 0 & n \end{pmatrix}^{-1}.$$

We see that the entries of the matrix N are all in $\frac{1}{n}\mathbb{Z}$. The following lemma shows that N is always an integer matrix.

Lemma 1. *Let m be a divisor of $24n$ such that $\gcd(m, \frac{24n}{m}) = 1$, let $k \in \mathbb{Z}$ be such that $n|f(-k)$ and let $W = \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix} \in G^{(m)}_{24n,\theta}$. Take $x \in \mathbb{Z}$ with $\gcd(x, 24n) = 1$ with $x \equiv 1 \bmod \frac{24n}{m}$ and $x \equiv \det M \bmod m$ and let $M \in \Gamma(\frac{24n}{m})$ so that*

$$\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \cdot M \equiv W \bmod m$$

and set

$$N := \begin{pmatrix} 1 & kx \\ 0 & n \end{pmatrix} \circ M \circ \begin{pmatrix} 1 & k \\ 0 & n \end{pmatrix}^{-1}.$$

Then $N \in \Gamma$. If further $n|m$, then $N \in \Gamma(\frac{24n}{m})$.

Proof. Suppose we already know that $N \in \Gamma$ and $n|m$, then we show that $N \in \Gamma(\frac{24n}{m})$. As $n|m$ implies that n is invertible modulo $\frac{24n}{m}$, the reduction modulo $\frac{24n}{m}$ shows that

$$N = \begin{pmatrix} 1 & kx \\ 0 & n \end{pmatrix} \cdot M \cdot \begin{pmatrix} 1 & k \\ 0 & n \end{pmatrix}^{-1} \equiv \begin{pmatrix} 1 & k \\ 0 & n \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & k \\ 0 & n \end{pmatrix}^{-1} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod \frac{24n}{m}.$$

To show that $N \in \Gamma$, we note that

$$\begin{pmatrix} 1 & kx \\ 0 & n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \begin{pmatrix} 1 & kx \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & k \\ 0 & n \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & n^{-1} \end{pmatrix}.$$

Because multiplying any matrix by $\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$ on the left multiplies the second row by n and multiplying by $\begin{pmatrix} 1 & 0 \\ 0 & n^{-1} \end{pmatrix}$ on the right multiplies the second column by n^{-1}, we only need to check that the top right entry of

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

is divisible by n. Computing modulo $\frac{24n}{m}$ we see that

$$\begin{pmatrix} 1 & kx \\ 0 & 1 \end{pmatrix} \cdot M \cdot \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & k \cdot 1 \\ 0 & 1 \end{pmatrix} \cdot I \cdot \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \equiv I \,(\bmod \frac{24n}{m}).$$

Modulo m, the matrix M has a bit more complicated form,

$$M \equiv \begin{pmatrix} 1 & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix} = \begin{pmatrix} t - Bs & -Cs \\ x^{-1}s & x^{-1}t \end{pmatrix}$$

and so we need to evaluate the top right entry of the matrix

$$\begin{pmatrix} 1 & kx \\ 0 & 1 \end{pmatrix} \cdot M \cdot \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & kx \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} t - Bs & -Cs \\ x^{-1}s & x^{-1}t \end{pmatrix} \cdot \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}.$$

A simple computation shows the top right entry to be equal to

$$-s(k^2 - Bk + C) = -sf(-k) (\bmod m).$$

Because $n|f(-k)$, we conclude that the top right entry of M' is divisible by n and so $N \in \mathrm{SL}_2(\mathbb{Z})$. □

Recall from section 2.3 that for any integral matrix $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, the transformation of η is given by

$$(\eta \circ U)(\tau) = \epsilon(U) \sqrt{c\tau + d}\, \eta(\tau)$$

for $\Re\sqrt{c\tau+d} \geq 0$ and $\epsilon(U)$ is made explicit by the Meyer formulas in Proposition 1. An extensive computation of the second row of N shows that

$$\begin{aligned} N &= \frac{1}{n}\begin{pmatrix}1 & kx\\ 0 & n\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}n & -k\\ 0 & 1\end{pmatrix} = \frac{1}{n}\begin{pmatrix}1 & kx\\ 0 & n\end{pmatrix}\begin{pmatrix}an & -ak+b\\ cn & -ck+d\end{pmatrix} \\ &= \frac{1}{n}\begin{pmatrix}* & *\\ cn^2 & n(-ck+d)\end{pmatrix} = \begin{pmatrix}* & *\\ cn & -ck+d\end{pmatrix} \end{aligned}$$

and this is enough to conclude that the action by an element $W \in W_{m,\theta}$ is given by multiplying by a root of unity: an explicit computation gives:

$$\begin{aligned} (\nu_{k,n}\cdot W)(\tau) &= \frac{\left[\eta\circ N\circ\begin{pmatrix}1 & k\\ 0 & n\end{pmatrix}\right](\tau)}{(\eta\circ M)(\tau)} = \epsilon(N)\epsilon(M)^{-1}\frac{\left(\sqrt{(cn)\tau-ck+d}\cdot\eta(\tau)\right)\circ\begin{pmatrix}1 & k\\ 0 & n\end{pmatrix}}{\sqrt{c\tau+d}\cdot\eta(\tau)} = \\ &= \epsilon(N)\epsilon(M)^{-1}\frac{\left(\sqrt{cn\left(\frac{\tau+k}{n}\right)-ck+d}\right)\cdot\left(\eta(\tau)\circ\begin{pmatrix}1 & k\\ 0 & n\end{pmatrix}\right)}{\sqrt{c\tau+d}\cdot\eta(\tau)} = \\ &= \epsilon(N)\epsilon(M)^{-1}\frac{\sqrt{c(\tau+k)-ck+d}\cdot\left(\eta(\tau)\circ\begin{pmatrix}1 & k\\ 0 & n\end{pmatrix}\right)}{\sqrt{c\tau+d}\cdot\eta(\tau)} = \epsilon(N)\epsilon(M)^{-1}\nu_{k,n}(\tau), \end{aligned}$$

and so

$$\nu_{k,n}\cdot W = \epsilon(N)\epsilon(M)^{-1}\nu_{k,n},$$

as is explicitly computed in the following computation:

So to compute the action of W, we need to determine the transformation of η by N and M, that is, evaluate the factors $\epsilon(N)$ and $\epsilon(M)$. In general,

$$\epsilon(N), \epsilon(M) \in \mu_{24}.$$

We recall the notation $\epsilon(M) = \left(\frac{a}{c_0}\right)\zeta_{24}^{e(M)}$ and $\epsilon(N) = \left(\frac{a'}{c_0'}\right)\zeta_{24}^{e(N)}$.

As we examine the action of all the matrices in $W_{m,\theta}$ (or alternatively, the action of the generators for $W_{m,\theta}$), we need to keep track of the following data:

- product of the Legendre symbols $\left(\frac{a}{c_0}\right)\cdot\left(\frac{a'}{c_0'}\right)$,
- the exponent of the 24-th root of unity $e(N)-e(M)$,
- the determinant $\det(W)$ mod m, alternatively, the action $\zeta_m \mapsto \zeta_m^{\det W}$.

Remember that we are looking for a small exponent e and an element $\vartheta \in \mathbb{Q}(\zeta_{24n})$ of small height such that $\vartheta\nu_{k,n}^e$ is fixed by the action of $W_{m,\theta}$. Because $W_{m,\theta}$ acts trivially on $\mathbb{Q}(\zeta_{\frac{24n}{m}})$, we see that ϑ is without loss of generality an element of $\mathbb{Q}(\zeta_m)$. We can readily make several useful observations:

1. Suppose there exists a matrix $W \in W_{m,\theta}$ with $\det W \equiv 1 \bmod m$ acting non-trivially on $\nu_{k,n}$. As $\det W = 1$, the action of W on $\mathbb{Q}(\zeta_m)$ is trivial and so there is no $\vartheta \in \mathbb{Q}(\zeta_m)$ such that $\vartheta\nu_{k,n}$ is invariant under the action of W. Therefore, we need to take e to be at least the smallest power e' for which $\nu_{k,n}^{e'}$ is invariant under the action of W.
2. Similarly, if two matrices W, W' of the same determinant $\det W = \det W'$ act differently on $\nu_{k,n}^{e'}$, there cannot be an element $\vartheta \in \mathbb{Q}(\zeta_m)$ such that $\vartheta\nu_{k,m}^{e'}$ is invariant under $W_{m,\theta}$. Therefore, a necessary condition on e is that all matrices in $W_{m,\theta}$ with the same determinant act the same on $\nu_{k,n}^e$.

5.4.3 Galois cohomology to the rescue

Suppose that all the matrices in $W_{m,\theta}$ of the same determinant act the same on $\nu^e_{k,n}$, that is, the action of $W \in W_{m,\theta}$ only depends on the determinant of W. Moreover, we assume for all $W \in W_{m,\theta}$ that $\nu^e_{k,n} \cdot W = \zeta \nu^e_{k,n}$ for some $\zeta \in \mu_m$. If $n|m$, this is satisfied already if matrices with the same determinant act the same, by combining Lemma 1 and Proposition 1.

We will show that then we can find an element $\vartheta \in \mathbb{Q}(\zeta_m)$ such that $\frac{\nu^e_{k,n}}{\vartheta}$ is invariant under the action of $W_{m,\theta}$. More specifically, we use the action of $W_{m,\theta}$ to construct a class $\phi \in H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_m)/L), \mathbb{Q}(\zeta_m)^\times)$ for a suitable subfield $L \subset \mathbb{Q}(\zeta_m)$ and show that this class vanishes. For details on Galois cohomology see the Appendix A.

Recall that $W_{m,\theta}$ acts on $\mathbb{Q}(\zeta_m)$ via the determinant. Under the standard isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ sending $d \in (\mathbb{Z}/m\mathbb{Z})^\times$ to the automorphism

$$\sigma_d : \zeta_m \to \zeta_m^d,$$

we obtain that any $W \in W_{m,\theta}$ of determinant $\det W = d$ acts as σ_d on $\mathbb{Q}(\zeta_m)$.

The group $W_{m,\theta}$ acts on $\mathcal{F}_{24n}$ via the lift to $W_{24n,\theta}$ as in 5.4.2. Denote the action of $W \in W_{m,\theta}$ as $\mathfrak{f} \mapsto \mathfrak{f} \cdot W$. For elements $\vartheta \in \mathbb{Q}(\zeta_m) \subset \mathcal{F}_{24n}$ these actions coincide with the determinant action, that is,

$$\sigma_d(\vartheta) = \vartheta \cdot W.$$

We are now ready to define the cocycle. For $d \in (\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ such that there exists a matrix $M_d \in W_{m,\theta}$ with $\det M_d = d$, we set

$$\phi(d) = \frac{\nu^e_{k,n} \circ M_d}{\nu^e_{k,n}} \in \mu_m \subset \mathbb{Q}(\zeta_m)^\times.$$

Let $\Delta = \mathrm{im}\,(\det : W_{m,\theta} \to (\mathbb{Z}/m\mathbb{Z})^\times) \subset (\mathbb{Z}/m\mathbb{Z})^\times$ be the image of the determinant on $W_{m,\theta}$. Then we obtain a map

$$\phi : \Delta \to \mathbb{Q}(\zeta_m), \quad d \in \Delta \mapsto \phi(d).$$

The map ϕ is well-defined as two matrices with the same determinant act the same on $\nu^e_{k,n}$ by assumption.

We show that ϕ is indeed a cocycle. Let $d, d' \in (\mathbb{Z}/m\mathbb{Z})^\times$ and let $M_d, M_{d'} \in W_{m,\theta}$ be matrices with $\det M_d = d$ and $\det M_{d'} = d'$. Then $\det(M_d M_{d'}) = \det(M_{d'} M_d)$ and so

$$\nu^e_{k,n} \cdot (M_d M_{d'}) = \nu^e_{k,n} \cdot (M_{d'} M_d)$$

and we compute

$$\phi(dd') = \frac{\nu^e_{k,n} \cdot (M_d M_{d'})}{\nu^e_{k,n}} = \frac{\nu^e_{k,n} \cdot (M_{d'} M_d)}{\nu^e_{k,n} \cdot M_d} \cdot \frac{\nu^e_{k,n} \cdot M_d}{\nu^e_{k,n}} =$$
$$= \frac{\nu^e_{k,n} \cdot M_d}{\nu^e_{k,n}} \cdot \left(\frac{\nu^e_{k,n} \cdot (M_{d'})}{\nu^e_{k,n}} \right) \cdot M_d = \phi(d) \cdot \sigma_d(\phi(d')),$$

because $\frac{\nu^e_{k,n} \cdot (M_{d'})}{\nu^e_{k,n}} \in \mathbb{Q}(\zeta_m)$ and M_d acts on $\mathbb{Q}(\zeta_m)$ as $\sigma_d : \zeta_m \to \zeta_m^d$. Therefore, ϕ is a cocycle on Δ.

Now we need a better understanding of the group Δ. From the Second main theorem of complex multiplication (Theorem 8), we know that $\mathbb{Q}(\zeta_m) \subset H_{m,\mathcal{O}}$ and the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Gal}(H_{m,\mathcal{O}}/H_{\mathcal{O}}) & \xrightarrow{\sim} & (\mathcal{O}/m\mathcal{O})^\times/\mathcal{O}^\times \\ \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \det \circ g_\tau} \\ \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) & \xrightarrow{\sim} & (\mathbb{Z}/m\mathbb{Z})^\times. \end{array}$$

Therefore, $\alpha \in \mathbb{Q}(\zeta_m)$ is an element of the ring class field $H_{\mathcal{O}}$ if and only if $\sigma_d(\alpha) = \alpha$ for all $d \in \Delta$. This gives that $H_{\mathcal{O}} \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_m)^{\Delta}$ and so

$$\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/H_{\mathcal{O}} \cap \mathbb{Q}(\zeta_m)).$$

By Hilbert's theorem 90 (Theorem 15), we know that $H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_m)/H_{\mathcal{O}} \cap \mathbb{Q}(\zeta_m)), \mathbb{Q}(\zeta_m)^{\times}) = 0$ and so there exist some $\vartheta \in \mathbb{Q}(\zeta_m)$ such that

$$\phi = \phi_{\vartheta}$$

for the cocycle $\phi_{\vartheta} : \Delta \to \mathbb{Q}(\zeta_m)^{\times}$ given as

$$\phi_{\vartheta}(d) = \frac{\sigma_d(\vartheta)}{\vartheta}.$$

Therefore, for any $d \in \Delta$ we obtain that

$$\frac{\nu_{k,n}^e \cdot M_d}{\nu_{k,n}^e} = \phi(d) = \phi_{\vartheta}(d) = \frac{\sigma_d(\vartheta)}{\vartheta}$$

and so we conclude that

$$\left(\frac{\nu_{k,n}^e}{\vartheta}\right) \cdot M_d = \frac{\nu_{k,n}^e \cdot M_d}{\sigma_d(\vartheta)} = \frac{\nu_{k,n}^e}{\vartheta}$$

and $\frac{\nu_{k,n}^e}{\vartheta}$ is invariant under the action of $W_{m,\theta}$.

5.5 Finding class invariants for a given quadratic order $\mathcal{O}$

Using the observations in 5.4.2 and 5.4.3, we formulate the following strategy to find class invariants. Recall that $\mathcal{O} = \mathbb{Z}[\theta]$ is an order in an imaginary quadratic field, the minimal polynomial of θ is $x^2 + Bx + C$ and satisfies $B \in \{0, 1\}$ and $D = B^2 - 4C$ is the discriminant of $\mathcal{O}$.

Note that the original question of Enge and Morain asked whether there exists a root of unity ζ such that $\zeta \cdot \nu_{k,n}^e$ gives a class invariant. The existence of such a root of unity is checked in the step 2d below but such a root of unity need not exist for the optimal choice of e we will find.

1. Find a suitable n as the level of the Weber functions (e.g. $n = 2, 3, 4, 6$) and $k \in \mathbb{Z}$ such that $f(-k) = 0 \bmod n$ has a solution, factor $24n$ into pairwise coprime prime powers m.
2. For all such prime powers m, perform the following steps.
   (a) Compute the groups $W_{m,\theta}$, e.g. by finding generators of $(\mathcal{O}/m\mathcal{O})^\times$ or by listing all the matrices
   $$W_{m,\theta} = \left\{ \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : s, t \in \mathbb{Z}/m\mathbb{Z} \right\}.$$
   (b) Determine the action of the matrices $W \in W_{m,\theta}$: compute $e(W) \in \mathbb{Z}$ such that
   $$\nu_{k,n} \cdot W = \zeta_{24}^{e(W)} \cdot \nu_{k,n},$$
   it suffices to store the determinant $\det W \bmod m$ and the exponent $e(W)$, which can be computed from the matrices M and N as in 5.4.2.
   (c) Find the smallest exponent e such that all the matrices in $W_{m,\theta}$ with the same determinant act the same on $\nu_{k,n}^e$ and such that $\zeta_{24}^{e(W)} \in \mu_m$ for all $W \in W_{m,\theta}$ (so that we can apply 5.4.3).
   (d) Try to find a root of unity ζ_m^a such that $\zeta_m^a \nu_{k,n}^e$ is invariant under $W_{m,\theta}$. This invariance means the following equalities:
   $$\zeta_m^a \nu_{k,n}^e = (\zeta_m^a \nu_{k,n}^e) \cdot W = \zeta_m^{a \cdot \det W} \zeta_{24}^{e \cdot e(W)} \nu_{k,n}^e$$
   for all $W \in W_{m,\theta}$. Comparing the roots of unity, the invariance is equivalent to the existence of a common solution of
   $$\det W \cdot a - \frac{e(W) \cdot e \cdot m}{24} \equiv a \bmod m$$
   for all $W \in W_{m,\theta}$. Such an solution need not exist.
   (e) Find an element $\vartheta \in \mathbb{Q}(\zeta_m)$ such that
   $$\frac{\nu_{k,n}^e}{\vartheta}$$
   is $W_{m,\theta}$-invariant. This can be done for instance by writing out a general Gaussian sum or by invoking the constructive proof of the Hilbert's theorem 90 (see Theorem 15).
3. Combine the answers for all the prime powers m: obtain
   $$\vartheta \nu_{k,n}^e$$
   invariant under $W_{24n,\theta}$ for some $\vartheta \in \mathbb{Q}(\zeta_{24n})$
4. Evaluate the value $\alpha = \vartheta \nu_{k,n}^e(\theta)$ as a complex number and finds its minimal polynomial. Compute the class number of $\mathcal{O}$ as the number of primitive reduced binary quadratic forms of discriminant D and use this number as a bound for the degree of the minimal polynomial of α. Alternatively, one can compute the conjugates from Shimura reciprocity directly, see [6, Class invariants by Shimura's reciprocity law, Theorem 20].

6 Computations for $n = 4$

In this section we apply the procedure developed in chapter 5 to level $n = 4$. Let us recall the notation as follows: let $\mathcal{O} = \mathbb{Z}[\theta]$ be an order in the imaginary quadratic field K and let $D = \mathrm{disc}(\mathcal{O}) < -4$. Let

$$f = x^2 + Bx + C$$

be the minimal polynomial of θ over $\mathbb{Q}$ with $B \in \{0, 1\}$. Our goal is to find a suitable $k \in \mathbb{Z}$ and a suitable exponent e such that for some $\vartheta \in \mathbb{Q}(\zeta_{96})$ we have

$$\vartheta \nu_{k,4}^e(\theta) \in H_{\mathcal{O}}.$$

Enge and Morain computed the following table of exponents e such that the functions $\nu_{k,4}^e$ for a suitable k yield class invariants (for the table, see [5, 6.2.2], for the discussion of their approach see 5.2):

D mod 128	Enge-Morain e	D mod 128	Enge-Morain e
4 mod 32	8	1 mod 8	1
$16, 32, 80, 96$	4	0	1
20 mod 32	2	48 mod 64	1
64	2		

The goal of this chapter is to show that we can obtain improvements for the exponents in the following cases:

D mod 128	e
4 mod 32	2
$16, 80$	2
20 mod 32	1

We evaluate the action of $W_{96,\theta}$ on $\nu_{k,n}$ using the decomposition

$$W_{96,\theta} = G_{96,\theta}^{(32)} \times G_{96,\theta}^{(3)}.$$

We start with determining the action of $G_{96,\theta}^{(3)} \cong W_{3,\theta}$. The structure of this group is easily determined by hand and so we do this in the following section.

6.1 The action of $G_{96,\theta}^{(3)}$

In this section, we compute the action of $G_{96,\theta}^{(3)}$ on the functions $\nu_{k,4}$ and $\mathbb{Q}(\zeta_3)$ and find invariant functions for this action. We restrict ourselves to the case that $4|D$, that is, $B = 0$, but the discussion is similar in the case $B = 1$.

We know that the group $G_{96,\theta}^{(3)}$ is isomorphic to $(\mathcal{O}/3\mathcal{O})^\times$ and so there are three possibilities for the structure of the group, depending on D modulo 3. For simplicity, we use the identification $(\mathcal{O}/3\mathcal{O})^\times \cong W_{3,\theta}$ (keeping in mind that we need to lift the matrices to $\mathrm{GL}_2(\mathbb{Z}/96\mathbb{Z})$ using the procedures in 5.4.2).

The ramified case $D \equiv 0$ mod 3: then $W_{3,\theta}$ is generated for instance by $g = \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}$ and so any element $W \in W_{3,\theta}$ has determinant 1. Moreover, this matrix lifts as

$$M = \begin{pmatrix} 1985 & 4032 \\ 32 & 65 \end{pmatrix} \in \Gamma(32)$$

and so it is easy to compute for all k the action by g: it is trivial for all k.

k	N	$e(g)$	k	N	$e(g)$
0	$\begin{pmatrix} 1985 & 1008 \\ 128 & 65 \end{pmatrix}$	0	2	$\begin{pmatrix} 2049 & 16 \\ 128 & 1 \end{pmatrix}$	0
1	$\begin{pmatrix} 2017 & 520 \\ 128 & 33 \end{pmatrix}$	0	3	$\begin{pmatrix} 2081 & -504 \\ 128 & -31 \end{pmatrix}$	0

Indeed, we see that for all k, the matrices N lie in $\Gamma(8)$ and their bottom left entries are powers of 2, therefore, $8|e(g)$ in all these cases. Modulo 3, we have $e(M) \equiv -1$ and $e(N) \equiv -1$ for all k. Therefore, the action of g is trivial.

the split case $D \equiv 1 \bmod 3$: in this case, the structure of $W_{3,\theta}$ is V_4 the Klein group. Therefore, it is generated by any two non-trivial elements and so we can take

$$\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in W_{3,\theta}$$

to be the generators. The second generator has determinant 1 and always acts trivially on $\nu_{k,4}$. The first generator lifts to $\Gamma(32)$ as

$$M = \begin{pmatrix} 993 & 512 \\ 64 & 33 \end{pmatrix}$$

and acts as follows (the products of Legendre symbols are always 1), allowing us to easily determine invariant functions:

k	N	$e(W) \bmod 24$	invariant function
0	$\begin{pmatrix} 993 & 128 \\ 256 & 33 \end{pmatrix}$	0	$\nu_{0,4}$
1	$\begin{pmatrix} 5153 & -624 \\ 256 & -31 \end{pmatrix}$	16	$\zeta_3 \cdot \nu_{1,4}$
2	$\begin{pmatrix} 9313 & -3456 \\ 256 & -95 \end{pmatrix}$	8	$\zeta_3^2 \cdot \nu_{2,4}$
3	$\begin{pmatrix} 13473 & -8368 \\ 256 & -159 \end{pmatrix}$	0	$\nu_{3,4}$

the inert case $D \equiv 2 \bmod 3$: in this case, $W_{3,\theta}$ is cyclic generated by

$$g = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

Now $\det g = 2 \bmod 3$ and g lifts into

$$M = \begin{pmatrix} 4033 & 4096 \\ 64 & 65 \end{pmatrix} \in \Gamma(32)$$

and we compute that the action on $\nu_{k,4}$ gives the same invariant functions as before.

k	N	$e(W) \bmod 24$	invariant function
0	$\begin{pmatrix} 4033 & 1024 \\ 256 & 65 \end{pmatrix}$	0	$\nu_{0,4}$
1	$\begin{pmatrix} 8193 & 32 \\ 256 & 1 \end{pmatrix}$	16	$\zeta_3 \cdot \nu_{1,4}$
2	$\begin{pmatrix} 12353 & -3040 \\ 256 & -63 \end{pmatrix}$	8	$\zeta_3^2 \cdot \nu_{2,4}$
3	$\begin{pmatrix} 16513 & -8192 \\ 256 & -127 \end{pmatrix}$	0	$\nu_{3,4}$

To conclude, the following table gives the invariant functions under $W_{3,\theta}$ for D even:

k	$D \equiv 0 \bmod 3$	$D \equiv 1, 2 \bmod 3$
0	$\nu_{0,4}$	$\nu_{0,4}$
1	$\nu_{1,4}$	$\zeta_3\nu_{1,4}$
2	$\nu_{2,4}$	$\zeta_3^2\nu_{2,4}$
3	$\nu_{3,4}$	$\nu_{3,4}$

Table 1: Functions fixed by $W_{3,\theta}$, depending on D mod 3, supposing D even.

6.2 Extended example for $n = 4$ and $D \equiv 80(\bmod 128)$

We would like to see what happens in the case $D \equiv 80(\bmod 128)$. In this case we have $B = 0$ and $D = B^2 - 4C = -4C$, we obtain $C \equiv 12 \bmod 32$ as the only possible value of C. Therefore, all the groups $G_{96,\theta}^{32} \cong W_{32,\theta}$ will be the same. Moreover, as we require $f(-k) \equiv 0 \bmod 4$, we take either $k = 0$ or $k = 2$. For the choice $k = 0$ we will get a uniform answer as then $G_{96,\theta}^{3}$ acts trivially on $\nu_{0,4}$.

Enge and Morain predict $e = 4$ in their table reproduced in the beginning of the section 6. We follow our recipe:

1. We set $n = 4$ and $k = 0$ and we know the factorization $24n = 96 = 32 \cdot 3$.
2. We already know the transformation of $\nu_{0,4}$ under $W_{3,\theta}$: we obtain that

   $$\nu_{0,4} \text{ is invariant under } W_{3,\theta}.$$

   Therefore, set $m = 32$ and do the following computations:

   (a) The group $W_{32,\theta}$ has 512 elements, which is easily handled by the computer and less easily by humans. These are the matrices of the form

   $$W_{32,\theta} = \{\begin{pmatrix} t & -12s \\ s & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/32\mathbb{Z}) : s, t \in \mathbb{Z}/32\mathbb{Z}\}$$

   (b) to determine the action of the matrices $W \in W_{32,\theta}$, using the procedure in 5.4.2. The transformation by $W \in W_{32,\theta}$ is given by

   $$\nu_{0,4} \cdot W = \zeta_{24}^{a}\nu_{0,4}.$$

   A priori the root of unity occurring is only a 24-th root of unity, but because because $4|m$, Lemma 1 gives that the auxiliary matrices M, N (in the notation of the Lemma and the section 5.4.2) lie in $\Gamma(3)$. By Meyer's formula 1, we necessarily have $e(M), e(N) \equiv 0 \bmod 3$ and therefore $\nu_{0,4}$ indeed transforms by an eighth root of unity under $W_{32,\theta}$. Moreover, the product of the Legendre symbols is always ± 1, and so we can include it easily into the exponent of the eight root of unity we are after. The transformations are given in the following table. We only list the determinant of the matrices and the resulting exponent of the root of unity.

Table 2: Transformations of $\nu_{0,4}$ under $W_{32,\theta}$

determinant	$\nu_{0,4} \mapsto \zeta_8^a \nu_{0,4}$	determinant	$\nu_{0,4} \mapsto \zeta_8^a \nu_{0,4}$
1	0	17	0
1	4	17	4
5	2	21	2
5	6	21	6
9	0	25	0
9	4	25	4
13	2	29	2
13	6	29	6

(c) From the table we see that the smallest exponent e such that matrices with the same determinant act the same on $\nu_{0,4}^e$ is

$$e = 2.$$

Therefore, from now on we consider the action on $\nu_{0,4}^2$, which is easily seen to be given by

$$\nu_{0,4}^2 \cdot W = \zeta_8^{\det W - 1} \nu_{0,4}^2$$

(d) To find a root of unity ζ_8^a such that $\zeta_8^a \nu_{0,4}^2$ is invariant under $W_{32,\theta}$, we need to solve the following congruence

$$\begin{aligned} a &\equiv a \cdot \det W + \det W - 1 \bmod 8 \Rightarrow \\ (a+1)(\det W - 1) &\equiv 0 \bmod 8. \end{aligned}$$

Because $4 | \det W - 1$ in all cases, we can take $a \equiv 1 \bmod 2$. Therefore,

$$\zeta_8 \nu_{0,4}^2$$

is invariant under $W_{32,\theta}$.

3. Putting the two transformation behaviours together, we see that

$$\zeta_8 \cdot \nu_{0,4}^2$$

is invariant under $W_{96,\theta}$.

Note that if $D \equiv 80 \bmod 128$, then our choice of θ forces $\theta \in i\mathbb{R}_{>0}$. But for $\tau \in i \cdot \mathbb{R}_{>0}$,

$$\eta(\tau) \in \mathbb{R}$$

Therefore, $\nu_{0,4}^2(\theta) \in \mathbb{R}$. Mutliplying by the complex number ζ_8 then produces complex (non-real) class invariants with complex minimal polynomials over K.

To obtain real minimal polynomials, note that the action of $W_{32,\theta}$ on $\nu_{0,4}^2$ can be written as

$$\nu_{0,4}^2 \cdot W \mapsto \begin{cases} \nu_{0,4}^2 & \det W \equiv 1 \bmod 8, \\ -\nu_{0,4}^2 & \det W \equiv 5 \bmod 8. \end{cases}$$

However, as $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, we see that the action of $W_{32,\theta}$ on $\nu_{0,4}^2$ coincides with the action of $W_{32,\theta}$ on $\sqrt{2}$.

Therefore, also the function

$$\frac{1}{\sqrt{2}} \cdot \nu_{0,4}^2 = \frac{1}{1+i} \cdot \left(\zeta_8 \cdot \nu_{0,4}^2\right)$$

also gives class invariants in this case, which will have real minimal polynomials.

Let us note that if we use $k = 2$ in the discussion above, we obtain exponent $e = 4$ rather than $e = 2$ as we obtained for $k = 0$. The exponent $e = 4$ is optimal, i.e., there are matrices in $W_{32,\theta}$ of equal determinant, which act differently on $\nu_{2,4}^2$.

We now proceed to evaluate at small values of θ satisfying $\theta^2 + 12 \equiv 0 \bmod 32$.

6.2.1 $C = 12$

Even though this case is completely determined by genus theory, we record the case $C = 12$ as it is the smallest example of an order with discriminant $D \equiv 80 \bmod 128$.

Let $\theta = \sqrt{-12}$ be the root of $f(x) = x^2 + 12$ such that $\theta \in \mathbb{H}$. Set $\mathcal{O} = \mathbb{Z}[\theta]$. Then we claim that $\zeta_8 \nu_{0,4}^2(\theta) \in H_{\mathcal{O}}$. The class number of $\mathcal{O}$ is 2, as can be seen for instance by counting the number of primitive reduce positive definite binary forms of discriminant $D = -48$. Evaluating the function $\zeta_8 \cdot \nu_{0,4}^2$ at θ we obtain

$$\alpha = \zeta_8 \frac{\eta\left(\frac{\sqrt{-12}}{4}\right)^2}{\eta(\sqrt{-12})^2} \approx 2.73205080756888 + 2.73205080756888i.$$

Then α has minimal polynomial over $\mathbb{Q}$

$$F(x) = x^4 - 4x^3 + 8x^2 + 16x + 16$$

and over $K = \mathbb{Q}(\theta)$ satisfies the polynomial

$$x^2 + \left(-\sqrt{-12} - 2\right) x - 4.$$

For comparison, the real value

$$\frac{\alpha}{1+i} = \frac{1}{\sqrt{2}} \cdot \frac{\eta\left(\frac{\sqrt{-12}}{4}\right)^2}{\eta(\sqrt{-12})^2} \approx 2.73205080756888$$

satisfies the minimal polynomial

$$x^2 - 2x - 2.$$

This minimal is easily seen to be much smaller than the minimal polynomial of $j(\mathcal{O})$, which is

$$H_D(X) = x^2 - 2835810000x + 6549518250000,$$

showing that we indeed obtain smaller values. However, the real benchmark is comparison with the value of Enge and Morain, which is equal approximately to

$$\beta \approx -14.9282032302755$$

and satisfies the real minimal polynomial

$$x^2 + 16x + 16$$

over K. The fact that the minimal polynomial of β is real is explained by Theorem 6.1 of [5]. For $n = 4$ this is only possible (under their assumptions) if $16|D$, which does happen in the case $D \equiv 80 \bmod 128$.

6.2.2 $C = 44$

In this case, we already get a much more interesting answer. Let $\theta = \sqrt{-44} \in \mathbb{H}$ satisfy $f(x) = x^2 + 44$. Set $\mathcal{O} = \mathbb{Z}[\theta]$. Then we claim that $\zeta_8 \nu_{0,4}^2(\theta) \in H_{\mathcal{O}}$. The class number of $\mathcal{O}$ is 6. Evaluating the function we obtain

$$\alpha = \zeta_8 \frac{\eta\left(\frac{\sqrt{-44}}{4}\right)^2}{\eta(\sqrt{-44})^2} \approx 9.566216100929554333143178001074203614 7 \\ + 9.566216100929554333143178001074203614 7i.$$

Then α has minimal polynomial over $\mathbb{Q}$

$$F(x) = x^{12} - 20x^{11} + 200x^{10} - 176x^9 + 240x^8 - 1408x^7 - 4352x^6 \\ + 5632x^5 + 3840x^4 + 11264x^3 + 51200x^2 + 20480x + 4096,$$

and over $K = \mathbb{Q}(\theta)$ satisfies the polynomial

$$x^6 + \left(-\sqrt{-44} - 10\right) x^5 + \left(-4\sqrt{-44} + 28\right) x^4 \\ + \left(8\sqrt{-44} + 16\right) x^3 + \left(16\sqrt{-44} - 112\right) x^2 + \left(-16\sqrt{-44} - 160\right) x - 64.$$

For comparison, real value

$$\frac{1}{\sqrt{2}} \cdot \frac{\eta\left(\frac{\sqrt{-44}}{4}\right)^2}{\eta(\sqrt{-44})^2} \approx 9.56621610092956 \in \mathbb{R}$$

has minimal polynomial

$$x^6 - 10x^5 + 6x^4 - 16x^3 - 12x^2 - 40x - 8,$$

as compared to the value obtained by Enge and Morain, which has a minimal polynomial

$$x^6 + 176x^5 - 1232x^4 + 9728x^3 - 19712x^2 + 45056x + 4096.$$

For comparison, the Hilbert class polynomial is equal to

$$H_D(X) = x^6 - 1260369120052221040x^5 - 131122722570454783416443 2x^4 \\ - 1417657940638726253547455241728x^3 + 561399144103038015259973368004083 20x^2 \\ - 2338321813960315633591659363679168389 12x \\ + 9843151491369337104149299151236137253642 24.$$

6.2.3 $C = 1324$

Computing the class invariants using the function $\frac{1}{\sqrt{2}}\nu_{0,4}^2$ can be done very quickly for small values. For instance, for the imaginary quadratic order $\mathcal{O} = \mathbb{Z}[\sqrt{-1324}]$, even by computing the value using in-built functions in Sage, we can produce the irreducible polynomial

$$f(x) = x^{18} - 1135390x^{17} - 8809154x^{16} - 172803456x^{15} - 16522480x^{14} + 122779936x^{13} \\ + 253232096x^{12} - 2073641472x^{11} - 643023264x^{10} + 1018580160x^9 + 1286046528x^8 \\ - 8294565888x^7 - 2025856768x^6 + 1964478976x^5 + 528719360x^4 - 11059421184x^3 \\ + 1127571712x^2 - 290659840x - 512,$$

which generates the ring class field of $\mathcal{O}$ over K, in less than half a second. The corresponding Hilbert class polynomial, i.e, the minimal polynomial of $j(\mathcal{O})$ does not fit onto one page in the typesetting of this thesis. Moreover, checking that the ring class field $H_{\mathcal{O}}$ is indeed the correct field (for instance by brute force factoring the Hilbert class polynomial over the field generated by this polynomial over K) still only takes about half a minute.

6.3 Results for $N = 4$

In this part we perform the computations for the functions $\nu_{k,4}$ for $k \in \mathbb{Z}$, which are elements of $\mathcal{F}_{24\cdot 4} = \mathcal{F}_{96}$. Because the groups $W_{96,\theta} \cong W_{32,\theta} \times W_{3,\theta}$ only depend on the minimal polynomial $x^2 + Bx + C$ mod 32 and modulo 3 and because we choose D even in view of the table 6, the answers will depend only on D modulo $4 \cdot 32 = 128$ and 3.

6.3.1 The case $D \equiv 4 \bmod 32$

Let us now discuss the case $D \equiv 4 \bmod 32$. In this case $B = 0$ and so $-4C = D \equiv 4 \bmod 32$, which gives $C \equiv 7, 15, 23, 31 \bmod 32$.

By performing the same computations as in the case $D \equiv 80 \bmod 128$ for the groups $W_{32,\theta}$ with $C \in \{7, 15, 23, 31\}$, we conclude that the following functions are $W_{32,\theta}$ invariant:

C mod 32	$W_{32,\theta}$-invariant	
7	$\zeta_8\nu_{1,4}^2$	$\zeta_8\nu_{3,4}^2$
15	$\zeta_8^3\nu_{1,4}^2$	$\zeta_8^3\nu_{3,4}^2$
23	$\zeta_8\nu_{1,4}^2$	$\zeta_8\nu_{3,4}^2$
31	$\zeta_8^3\nu_{1,4}^2$	$\zeta_8^3\nu_{3,4}^2$

Therefore, accounting for the action of $W_{3,\theta}$, we conclude the following:

C mod 32	$D \equiv 0 \bmod 3$	$D \equiv 1, 2 \bmod 3$
7	$\zeta_8\nu_{1,4}^2$	$\zeta_8\nu_{1,4}^2$
	$\zeta_8\nu_{3,4}^2$	$\zeta_8\nu_{3,4}^2$
15	$\zeta_8^3\nu_{1,4}^2$	$\zeta_3^2\zeta_8^3\nu_{1,4}^2$
	$\zeta_8^3\nu_{3,4}^2$	$\zeta_8^3\nu_{3,4}^2$
23	$\zeta_8\nu_{1,4}^2$	$\zeta_3^2\zeta_8\nu_{1,4}^2$
	$\zeta_8\nu_{3,4}^2$	$\zeta_8\nu_{3,4}^2$
31	$\zeta_8^3\nu_{1,4}^2$	$\zeta_3^2\zeta_8^3\nu_{1,4}^2$
	$\zeta_8^3\nu_{3,4}^2$	$\zeta_8^3\nu_{3,4}^2$

Table 3: Functions yielding class invariants for $D \equiv 4 \bmod 32$, depending on D mod 3.

Even though we managed to reduce the exponent $e = 8$ predicted by Enge and Morain to the exponent $e = 2$, this case is not as interesting as it might seem. As $D \equiv 4 \bmod 32$, we see that $D/4 \equiv 1 \bmod 8$ and so there exists an order $\mathcal{O}' \supset \mathcal{O} = \mathbb{Z}[\theta]$ with $D' = \Delta(\mathcal{O}') \equiv 1 \bmod 8$. Moreover, comparing class numbers of $\mathcal{O}$ and $\mathcal{O}'$ using the formula 1 in section 3.1.1, we see that

$$h(\mathcal{O}) = h(\mathcal{O}').$$

As the class number is the degree of the ring class field over K and because $H_{\mathcal{O}} \supset H_{\mathcal{O}'}$, we have $H_{\mathcal{O}} = H_{\mathcal{O}'}$ and so we can generate $H_{\mathcal{O}}$ already using first powers, as is also seen in the table in 6.

6.3.2 The case $D \equiv 16 \bmod 128$

In this case $C \equiv 28 \bmod 32$ and $B = 0$. This allows us to determine the group $W_{32,\theta}$ easily. Then we obtain that $k = 0$ or $k = 2$. In the case of $k = 0$, we notice there are matrices in $W_{32,\theta}$ with determinant 1 that act as $v_{0,4} \mapsto -v_{0,4}$ and so we need $e = 2$. This choice gives us a $W_{32,\theta}$-invariant function

$$\zeta_8\nu_{0,4}^2$$

As $k = 0$, this function is also $W_{3,\theta}$-invariant and can be used to construct class invariants.

6.3.3 The case $D \equiv 20 \bmod 32$

This implies that $C \equiv 3, 11, 19, 27 \bmod 32$ and the solution $f(-k) \equiv 0 \bmod 4$ can be taken as $k = 1$ or $k = 3$. This case is interesting because matrices with same determinant turn out to act the same already for $e = 1$.

We split the four cases of C mod 32 to compute the action of $W_{32,\theta}$ on $\nu_{1,4}$.

$C \equiv 3 \bmod 32$. We choose $k = 1$. In this case, the action only depends on $\det W$ mod 8:

$\det W \bmod 8$	$\nu_{1,4} \mapsto \pm\nu_{1,4}; a$	$\det W \bmod 8$	$\nu_{1,4} \mapsto \pm\nu_{1,4}; a$
1	1	5	-1
3	-1	7	1

We see that this action coincides with the character

$$\begin{aligned} \chi_8 : (\mathbb{Z}/8\mathbb{Z})^\times &\to \{\pm 1\} \\ a \bmod 8 &\mapsto \begin{cases} 1 & a \equiv 1, 7 \bmod 8 \\ -1 & a \equiv 3, 5 \bmod 8 \end{cases} \end{aligned}$$

And it is easy to check that the element

$$\vartheta = \zeta_8 - \zeta_8^3 - \zeta_8^5 + \zeta_8^7 \in \mathbb{Q}(\zeta_8)$$

is acted on the same way. Indeed, $\sigma(\vartheta) = -\vartheta = \sigma_5(\vartheta)$. A simple computation moreover shows that

$$\vartheta = 2\sqrt{2}.$$

We conclude that the function $\sqrt{2} \cdot \nu_{1,4}$ is $W_{32,\theta}$-invariant.

$C \equiv 11 \bmod 32$. We choose $k = 3$ and then the action again only depends on $\det W$ mod 8:

$\det W \bmod 8$	$\nu_{1,4} \mapsto \pm\nu_{1,4}; a$	$\det W \bmod 8$	$\nu_{1,4} \mapsto \pm\nu_{1,4}; a$
1	1	5	-1
3	1	7	-1

We see that this action coincides with the character

$$\begin{aligned} \chi_:(\mathbb{Z}/8\mathbb{Z})^\times &\to \{\pm 1\} \\ a \bmod 8 &\mapsto \begin{cases} 1 & a \equiv 1, 3 \bmod 8 \\ -1 & a \equiv 5, 7 \bmod 8 \end{cases} \end{aligned}$$

And we see that the element

$$\vartheta = \zeta_8 + \zeta_8^3 - \zeta_8^5 - \zeta_8^7 \in \mathbb{Q}(\zeta_8)$$

is acted on the same way. Indeed, $\sigma(\vartheta) = -\vartheta = \sigma_5(\vartheta)$. A simple computation moreover shows that

$$\vartheta = 2\sqrt{-2}$$

and so

$$\sqrt{-2} \cdot \nu_{3,4}$$

is $W_{32,\theta}$-invariant.

$C \equiv 19 \bmod 32$**.** We choose $k = 1$ and obtain the following action, depending only on $\det W \bmod 8$:

$\det W \bmod 8$	$\nu_{1,4} \mapsto \pm\nu_{1,4}; a$	$\det W \bmod 8$	$\nu_{1,4} \mapsto \pm\nu_{1,4}; a$
1	1	5	-1
3	1	7	-1

and so we recover the character χ. Therefore, in this case

$$\sqrt{-2} \cdot \nu_{1,4}$$

is $W_{32,\theta}$-invariant.

$C \equiv 27 \bmod 32$**.** We choose $k = 3$ and obtain the action only depends on $\det W \bmod 8$:

$\det W \bmod 8$	$\nu_{1,4} \mapsto \pm\nu_{1,4}; a$	$\det W \bmod 8$	$\nu_{1,4} \mapsto \pm\nu_{1,4}; a$
1	1	5	-1
3	-1	7	1

And so we recover the character χ_8. Therefore, in this case

$$\sqrt{2} \cdot \nu_{3,4}$$

is $W_{32,\theta}$-invariant.

In this case it does not matter which root of $f(-k) \bmod 4$ we take. If we choose $k = 1$, we obtain the cocycle given as

$$\nu_{1,4} \mapsto \begin{cases} \nu_{1,4} & \det W \equiv 1 \bmod 4, \\ i \cdot \nu_{1,4} & \det W \equiv 3 \bmod 4. \end{cases}$$

It is easy to see that now we can take $\vartheta = 1 - i$ is acted on in the same way and so

$$(1 + i)\nu_{1,4}$$

is $W_{32,\theta}$-invariant.

Conclusion for $D \equiv 20 \bmod 32$**.** The following functions are $W_{96,\theta}$-invariant:

$C \bmod 32$	$D \equiv 0 \bmod 3$	$D \equiv 1, 2 \bmod 3$
3	$\sqrt{2} \cdot \nu_{1,4}$	$\zeta_3\sqrt{2} \cdot \nu_{1,4}$
11	$\sqrt{-2} \cdot \nu_{3,4}$	$\sqrt{-2} \cdot \nu_{3,4}$
19	$\sqrt{-2} \cdot \nu_{1,4}$	$\zeta_3\sqrt{-2} \cdot \nu_{1,4}$
27	$\sqrt{2} \cdot \nu_{3,4}$	$\sqrt{2} \cdot \nu_{3,4}$

Table 4: Invariant function for $D \equiv 20 \bmod 32$, depending on $D \bmod 3$.

7 Conclusion

We have shown that it is indeed possible to obtain smaller class invariant from the eta quotients $\nu_{k,4}$ by multiplying the powers of these functions with suitable elements of $\mathbb{Q}(\zeta_{24})$, as our computations in section 6 show. In some cases it suffices to multiply by a root of unity, thus giving a positive answer for $n = 4$ to the question of Enge and Morain posed in [5].

Our technique is independent of the choice of n and so we expect that following the strategy outlined in 5.5, it is possible to obtain similar improvements for any n. Another possible way to extend this thesis would be to focus on *double* eta quotients, functions of the form

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

which are (for a suitable choice of l, n and maybe up to a root of unity) modular functions in $\mathcal{F}_n$, rather than $\mathcal{F}_{24n}$, and which can be used to produce units in ring class fields (see for instance [7]). The groundwork for these computations can be found again in [6].

A Hilbert's Theorem 90

In this appendix, we recall the basics of Galois cohomology (we only need H^1) and Hilbert's theorem 90, which we used to justify our approach to finding class invariants in 5.4.3. We follow closely the exposition of Dummit and Foote in [4, Section 17.3].

Let G be a group. An abelian group A (written multiplicatively) with a left action of G as automorphisms is called a G-module. Write the action as $(g, a) \mapsto ga$ for $g \in G$ and $a \in A$.

In our setting, the group G will be the Galois group $\mathrm{Gal}(L/K)$ of some finite extension L/K of number fields. The G-module we are primarily interested in is the group $L^\times$ (and so we use the multiplicative notation).

A 1-cocycle or simply a cocycle is a map

$$\phi : G \to A$$

satisfying for all $g, h \in G$ the following identity:

$$\phi(gh) = \phi(g) \cdot g\phi(h).$$

The set of all cocycles forms an abelian group which we denote $Z^1(G, A)$. For instance, if G acts trivially on A, then $Z^1(G, A) = \mathrm{Hom}(G, A)$. For any $a \in A$, we can construct the following map:

$$\phi_a : g \mapsto \frac{ga}{a}.$$

Then ϕ_a is a cocycle as

$$\phi_a(gh) = \frac{gh(a)}{a} = \frac{g(ha)}{ga} \cdot \frac{ga}{a} = \frac{ga}{a} \cdot g\left(\frac{ha}{a}\right) = \phi_a(g) \cdot g\phi_a(h).$$

Such a cocycle is called a coboundary. Denote by $B^1(G, A)$ the subgroup of coboundaries. The first cohomology group $H^1(G, A)$ is then defined as the group quotient

$$H^1(G, A) = \frac{Z^1(G, A)}{B^1(G, A)}.$$

We return to the case when $G = \mathrm{Gal}(L/K)$ is the Galois group of a finite number field extension and $A = L^\times$. Then the folllowing theorem, called Hilbert's Theorem 90, says that any cocycle is then a coboundary.

Theorem 15 (Hilbert's Theorem 90)**.** *Let L/K be a finite Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. Then*

$$H^1(G, L^\times) = 0$$

The following proof follows that of [4, Section 17.3]. We recall the proof because it is somewhat constructive and gives us tools how to find the coboundary, starting from a cocycle.

Proof. Let $\phi \in Z^1(G, L^\times)$ be a cocycle. Write $\alpha_\sigma = \phi(\sigma)$ for $\sigma \in G$. Then, thanks to the linear independence of automorphisms, we know that there exists some $\gamma \in L$ such that

$$\sum_{\tau \in G} \alpha_\tau \cdot \tau(\gamma) =: \beta \neq 0$$

But then for any $\sigma \in G$, as the cocycle relation gives $\alpha_{\sigma\tau} = \alpha_\sigma \sigma(\alpha_\tau)$ for any $\tau \in G$, we have

$$\sigma(\beta) = \sum_{\tau \in G} \sigma(\alpha_\tau)\sigma\tau(\gamma) = \sum_{\sigma\tau \in G} \frac{\alpha_{\sigma\tau}}{\alpha_\sigma}\sigma\tau(\gamma) = \frac{1}{\alpha_\sigma} \sum_{\tau \in G} \alpha_\tau \tau(\gamma) = \frac{1}{\alpha_\sigma}\beta$$

and so

$$\alpha_\sigma = \frac{\sigma(\beta^{-1})}{\beta^{-1}},$$

that is, ϕ is a coboundary. Therefore, $H^1(G, L^\times) = 0$. □

References

[1] Bryan John Birch. Weber's class invariants. *Mathematika*, 16:283–294, 1969.

[2] Reinier Bröker. Constructing elliptic curves of prescribed order. *Ph.D. thesis, Universiteit Leiden*, 2006.

[3] David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication.* Wiley-Interscience, 1997.

[4] David S. Dummit and Richard M. Foote. *Abstract Algebra, 3rd Edition.* Wiley, 2003.

[5] Andreas Enge and François Morain. Generalised Weber functions. *Acta Arith.*, 164(4):309–342, 2014.

[6] Alice Chia Ping Gee. Class fields by Shimura reciprocity. *Ph.D. thesis, University of Amsterdam*, 2001.

[7] Farshid Hajir and Fernando Rodriguez Villegas. Explicit elliptic units. I. *Duke Math. J.*, 90(3):495–521, 1997.

[8] Serge Lang. *Elliptic Functions (Graduate Texts in Mathematics, Vol. 112).* Springer, 1987.

[9] Reinhard Schertz. Weber's class invariants revisited. *J. Théor. Nombres Bordeaux*, 14(1):325–343, 2002.

[10] The Stacks Project Authors. *Stacks Project.* http://stacks.math.columbia.edu, 2017.

[11] Peter Stevenhagen. Hilbert's 12th problem, complex multiplication and Shimura reciprocity. 30:161–176, 2001.

[12] Heinrich Weber. *Lehrbuch der Algebra.* 1908.