Arithmetic properties of orders in imaginary quadratic fields

HO YUN JUNG, JA KYUNG KOO, DONG HWA SHIN AND DONG SUNG YOON

Abstract

Let \( K \) be an imaginary quadratic field. For an order \( \mathcal{O} \) in \( K \) and a positive integer \( N \), let \( K_{\mathcal{O},N} \) be the ray class field of \( \mathcal{O} \) modulo \( N\mathcal{O} \). We deal with various subjects related to \( K_{\mathcal{O},N} \), mainly about Galois representations attached to elliptic curves with complex multiplication, form class groups and \( L \)-functions for orders.

Contents

1 Introduction 2
2 The generalized ideal class group isomorphic to \( C_N(\mathcal{O}) \) 5
3 The elliptic curve \( E_\mathcal{O} \) with complex multiplication by \( \mathcal{O} \) 9
4 Fields of modular functions 10
5 Form class groups 12
6 Inequalities on special values of modular functions 14
7 Extension fields of \( \mathcal{O} \) generated by torsion points of \( E_\mathcal{O} \) 17
8 Galois representations attached to \( E_\mathcal{O} \) 20
9 An isomorphism of \( C_N(D_\mathcal{O}) \) onto \( C_N(\mathcal{O}) \) 23
10 The Shimura reciprocity law 28
11 Ray class invariants for orders 29
12 An isomorphism of \( C_N(D_\mathcal{O}) \) onto \( \text{Gal}(K_{\mathcal{O},N}/K) \) 33
13 The \( L \)-functions for orders 37

2020 Mathematics Subject Classification. Primary 11R37; Secondary 11E12, 11F80, 11G05, 11R42, 11R29.
Key words and phrases. Class field theory, elliptic curves, form class groups, Galois representations, \( L \)-functions.
1 Introduction

Let $K$ be an imaginary quadratic field. In 1935, H. Söhngen ([26]) first dealt with ray class fields for orders in $K$ which generalizes the usual ray class fields for the maximal order $O_K$. Later in [28] Stevenhagen paid attention to the ray class fields for orders in order to have explicit description of Shimura’s reciprocity law (Proposition 5.1). Furthermore, Cho ([4]) constructed the fields in view of certain Diophantine equations by extending the ideas in [6].

Let $O$ be an order in $K$ of discriminant $D_O$. We denote by $I(O)$ the group of proper fractional $O$-ideals in the sense of [6, §7.A]. It is well known that every fractional $O$-ideal is proper if and only if it is invertible. We say that a nonzero $O$-ideal $a$ is prime to a positive integer $\ell$ if $a + \ell O = O$. Let $P(O)$ be the subgroup of $I(O)$ consisting of principal fractional $O$-ideals. For a positive integer $N$, we define the subgroups of $I(O)$ and $P(O)$ as

$$I(O, N) = \langle a \mid a \text{ is a nonzero proper } O\text{-ideal prime to } N \rangle,$$

$$P_N(O) = \langle \nu O \mid \nu \in O \setminus \{0\} \text{ and } \nu \equiv 1 \pmod{NO} \rangle,$$

respectively. In particular, we have $I(O, 1) = I(O)$ (cf. [6 Exercise 7.7]) and $P_1(O) = P(O)$ because the field of fractions of $O$ is $K$. Then the associated quotient group

$$C_N(O) = I(O, N)/P_N(O)$$

is isomorphic to a generalized ideal class group modulo $\ell_O NO_K$, where $\ell_O = [O_K : O]$ is the conductor of $O$ (cf. [20 Theorem 3.1.8]). And the existence theorem of class field theory asserts that there is a unique abelian extension $K_{O,N}$ for which the Artin map for the modulus $\ell_O NO_K$ induces an isomorphism of the generalized ideal class group onto $\text{Gal}(K_{O,N}/K)$ (cf. [6 §8] or [9 V.9]). We call this extension field $K_{O,N}$ of $K$ the ray class field of $O$ modulo $NO$. In particular, $K_{O,1}$ is just the ring class field $H_O$ of order $O$ and $K_{O,K,N}$ is the ray class field $K_{(N)}$ modulo $(N) = NO_K$.

When $D_O \neq -3, -4$, we consider the elliptic curve $E_O$ with $j$-invariant $j(E_O) = j(O)$ given by the Weierstrass equation

$$E_O : y^2 = 4x^3 - A_O x - B_O$$

as in [3]. Let $E_O[N]$ be the group of $N$-torsion points of $E_O$ and $\mathbb{Q}(E_O[N])$ be the extension field of $\mathbb{Q}$ generated by the coordinates of points in $E_O[N]$. Then it can be shown that if $N \geq 2$, then $\mathbb{Q}(E_O[N])$ contains $\mathbb{Q}(j(O))$ (Lemma 7.4). And, in the first main theorem (Theorem 7.8) of this paper, we shall compare the field $\mathbb{Q}(E_O[N])$ with $K_{O,N}$.

Theorem A. Assume that $D_O \neq -3, -4$.

(i) If $D \equiv 0 \pmod{4}$, then $\mathbb{Q}(E_O[2])$ is the maximal real subfield of $K_{O,2}$.
(ii) If $D \equiv 1 \pmod{4}$, then $\mathbb{Q}(E_\mathcal{O}[2]) = K_{\mathcal{O},2}$.

(iii) If $N \geq 3$, then $\mathbb{Q}(E_\mathcal{O}[N])$ is an extension field of $K_{\mathcal{O},N}$ of degree at most 2.

Here we put an emphasis on the fact that $\mathbb{Q}(E_\mathcal{O}[N])$ is an extension field of $\mathbb{Q}$, not of $\mathbb{Q}(j(\mathcal{O}))$, generated by the coordinates of $N$-torsion points. This fact distinguishes Theorem A from prior works of Bourdon-Clark-Pollack ([3, Lemma 8.4]) and Clark-Pollack ([5, Theorem 4.2]).

Let $E$ be an arbitrary elliptic curve with complex multiplication by $\mathcal{O}$ defined over $\mathbb{Q}(j(\mathcal{O}))$. Through purely algebraic arguments Bourdon-Clark ([2]) and Lozano-Robledo ([17]) independently classified all possible images of $(p$-adic) Galois representations attached to $E$. In §7, we shall revisit these results on Galois representations by making use of modular-analytic approach. Let

$$\rho_{\mathcal{O},N} : \text{Gal}(\mathbb{Q}(E_\mathcal{O}[N])/\mathbb{Q}(j(\mathcal{O}))) \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \text{Aut}(E_\mathcal{O}[N])$$

be the Galois representation attached to a specific model $E_\mathcal{O}$. Let

$$\tau_\mathcal{O} = \begin{cases} \frac{\sqrt{D_\mathcal{O}}}{2} & \text{if } D_\mathcal{O} \equiv 0 \pmod{4}, \\ -1 + \frac{\sqrt{D_\mathcal{O}}}{2} & \text{if } D_\mathcal{O} \equiv 1 \pmod{4} \end{cases}$$

(2)

with $\min(\tau_\mathcal{O}, \mathbb{Q}) = d^2 + b_\mathcal{O}const + c_\mathcal{O}$. Then we have $\mathcal{O} = [\tau_\mathcal{O}, 1] = \mathbb{Z}\tau_\mathcal{O} + \mathbb{Z}$ and $b_\mathcal{O}, c_\mathcal{O} \in \mathbb{Z}$ (cf. [6, Lemma 7.2]). Let $\widehat{W}_{\mathcal{O},N}$ be the Cartan subgroup of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ associated with the $(\mathbb{Z}/N\mathbb{Z})$-algebra $\mathcal{O}/N\mathcal{O}$ with the ordered basis $\{\tau_\mathcal{O} + N\mathcal{O}, 1 + N\mathcal{O}\}$. In the second main theorem [Theorem B], we shall describe the image of $\rho_{\mathcal{O},N}$ by using Stevenhagen’s explicit version of the Shimura reciprocity law.

**Theorem B.** Assume that $D_\mathcal{O} \neq -3, -4$ and $N \geq 2$. Let $\widehat{W}_{\mathcal{O},N}$ be the subgroup of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ defined by

$$\widehat{W}_{\mathcal{O},N} = \left\langle W_{\mathcal{O},N}, \begin{bmatrix} 1 & b_\mathcal{O} \\ 0 & -1 \end{bmatrix} \right\rangle.$$

(i) The image of the Galois representation $\rho_{\mathcal{O},N}$ is a subgroup of $\widehat{W}_{\mathcal{O},N}$ of index at most 2.

(ii) If $-1$ is a quadratic residue modulo $N$, then the image of $\rho_{\mathcal{O},N}$ is exactly $\widehat{W}_{\mathcal{O},N}$.

Let $D$ be a negative integer such that $D \equiv 0$ or 1 (mod 4). Let $\mathcal{C}(D)$ be the set of primitive positive definite binary quadratic forms over $\mathbb{Z}$ of discriminant $D$ on which the modular group $\text{SL}_2(\mathbb{Z})$ induces the proper equivalence $\sim$. It was Gauss ([8]) who first introduced a composition law on $\mathcal{C}(D) = \mathcal{C}(D)/\sim$, which makes $\mathcal{C}(D)$ a group. When $D = D_\mathcal{O}$ and $N = 1$, owing to Dirichlet and Dedekind we have the isomorphism

$$\mathcal{C}(D_\mathcal{O}) \cong \mathcal{C}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}), \quad [Q] \mapsto [\omega_Q, 1] = [\mathbb{Z}\omega_Q + \mathbb{Z}]$$

where $\omega_Q$ is the zero of $Q(x, 1)$ in the complex upper half-plane (cf. [8, Theorem 7.7]). Let

$$\mathcal{Q}(D_\mathcal{O}, N) = \{ax^2 + bxy + cy^2 \in \mathcal{Q}(D_\mathcal{O}) \mid \gcd(a, N) = 1\}$$
on which the congruence subgroup $\Gamma_1(N)$ defines the equivalence relation $\sim_{\Gamma_1(N)}$ (§1). We shall endow the set of equivalence classes

$$C_N(D_O) = \mathbb{Q}(D_O, N)/\sim_{\Gamma_1(N)}$$

with a binary operation which reduces to the Dirichlet composition on the classical form class group $C(D_O)$, and prove the next third main theorem (Theorem 11.4).

**Theorem C.** The form class group $C_N(D_O)$ is isomorphic to the ideal class group $C_N(O)$.

Let $F_N$ be the field of certain modular functions stated in [12]. Then $F_N$ is a Galois extension of $F_1$ whose Galois group is isomorphic to $GL_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$ (cf. [21 Theorem 6.6]). By using the theory of Shimura’s canonical models for modular curves ([21 Chapter 6]), Cho proved in [4 Theorem 4] that

$$K_{O,N} = K(f(\tau_O) \mid f \in F_N \text{ is finite at } \tau_O).$$

Let $C \in C_N(O)$ and $f \in F_N$. In Definition 1.1 we shall define the invariant $f(C)$ which is a generalization of the Siegel-Ramachandra invariant (cf. [19] and [23]) considered when $O = O_K$, $N \geq 2$ and $f$ is the $12N$th power of the Siegel function $g_{[0 \frac{1}{2}]}$ given in (13). In the fourth main theorem (Theorem 11.4), we shall justify that $f(C)$ satisfies a natural transformation rule under the Artin map $\sigma_{O,N}: C_N(O) \rightarrow Gal(K_{O,N}/K)$.

**Theorem D.** Let $C \in C_N(O)$ and $f \in F_N$. If $f$ is finite at $\tau_O$, then $f(C)$ belongs to $K_{O,N}$ and satisfies

$$f(C)^{\sigma_{O,N}(C')} = f(CC') \quad (C' \in C_N(O)).$$

Theorems C and D lead us to achieve the next fifth main theorem (Theorem 12.3) which describes the isomorphism of $C_N(D_O)$ onto $Gal(K_{O,N}/K)$ explicitly.

**Theorem E.** The map

$$C_N(D_O) \rightarrow Gal(K_{O,N}/K)$$

$$[Q] = [ax^2 + bxy + cy^2] \mapsto \left( f(\tau_O) \mapsto f\left[\frac{1 - a'(b + b_O)/2}{a'}\right](-\mathfrak{m}Q) \mid f \in F_N \text{ is finite at } \tau_O \right)$$

is a well-defined isomorphism, where $a'$ is an integer which holds $ad' \equiv 1 \pmod{N}$.

For a ray class character $\chi$ modulo $NO_K$, let $L(s, \chi)$ be the Weber $L$-function (cf. [9 §IV.4]). It is well known by Kronecker’s limit formulae that $L(1, \chi)$ can be expressed by special values of the modular discriminant $\Delta$ when $N = 1$, and by Siegel-Ramachandra invariants when $N \geq 2$ (cf. [13 Chapters 20–22], [20] or [23]). On the other hand, rather than the value at 1, Stark observed in [27] that the derivative evaluated at zero $L'(0, \chi)$ would seem to be more easily applicable form. In Definition 13.1 we shall define the $L$-function $L_O(s, \chi)$ for a given character $\chi$ of $C_N(O)$ by

$$L_O(s, \chi) = \sum_{\mathfrak{a}} \frac{\chi([a])}{N_O(a)^s} \quad (s \in \mathbb{C}, \text{ Re}(s) > 1)$$

where $\mathfrak{a}$ runs over all proper $O$-ideals prime to $N$ and $N_O(a)$ is the norm of $\mathfrak{a}$. Then we shall show that $L'_O(0, \chi)$ satisfies a similar formula to that of Stark ([27 (2)]) in the following last main theorem (Theorem 14.4).
Theorem F. If $\chi$ is a character of $\mathcal{C}_N(\mathcal{O})$, then we have

$$L'_\mathcal{O}(0, \chi) = \frac{1}{\gamma_{\mathcal{O}, N} N^6} \sum_{C \in \mathcal{C}_N(\mathcal{O})} \chi(C) \ln |g_{\mathcal{O}, N}(C)|.$$ 

Here, $\gamma_{\mathcal{O}, N} = |\{\nu \in \mathcal{O}^* \mid \nu \equiv 1 \pmod{N\mathcal{O}}\}|$ and

$$g_{\mathcal{O}, N}(C) = \begin{cases} (2\pi)^{12} N_{\mathcal{O}}(c)^{-6}|\Delta(c)|^{-1} & \text{if } N = 1, \\ g_{12N}^{12}[0 \frac{1}{N}](C) & \text{if } N \geq 2, \end{cases}$$ 

where $c$ is a proper $\mathcal{O}$-ideal in the class $C$.

In the last section, when $K = \mathbb{Q}(\sqrt{-2})$, $\mathcal{O} = [5\sqrt{-2}, 1]$ and $N = 3$, we shall present an example of the group $\mathcal{C}_N(D_\mathcal{O}) = \mathcal{C}_3(-200)$ and its application further in order to find the minimal polynomial of the invariant $g_{\mathcal{O}, 3}([\mathcal{O}])$ over $K$ which generates the field $K_{\mathcal{O}, 3}$. It turns out that this invariant is in fact a unit as algebraic integer.

2 The generalized ideal class group isomorphic to $\mathcal{C}_N(\mathcal{O})$

Throughout this paper, we let $K$ be an imaginary quadratic field, $\mathcal{O}$ be an order in $K$ and $N$ be a positive integer. We denote the conductor and the discriminant of $\mathcal{O}$ by $\ell_\mathcal{O}$ and $D_\mathcal{O}$, respectively. As far as we know, Schertz’s book [20] is the only reference for the fact that the ray class group $\mathcal{C}_N(\mathcal{O})$ modulo $N\mathcal{O}$ is isomorphic to a generalized ideal class group modulo $\ell_\mathcal{O}N\mathcal{O}_K$. In this section, we shall explain this fact in modern terms by adopting the ideas of [6, §7] for $N = 1$, which will be definitely helpful to develop our main theorems.

For a positive integer $\ell$, we denote by

$$\mathcal{M}(\mathcal{O}, \ell) = \text{the monoid of nonzero proper } \mathcal{O}\text{-ideals prime to } \ell,$$

$$I(\mathcal{O}, \ell) = \text{the subgroup of } I(\mathcal{O}) \text{ generated by } \mathcal{M}(\mathcal{O}, \ell),$$

$$P_N(\mathcal{O}, \ell) = \langle \nu\mathcal{O} \mid \nu \in \mathcal{O} \setminus \{0\}, \nu\mathcal{O} \text{ is prime to } \ell \text{ and } \nu \equiv 1 \pmod{N\mathcal{O}} \rangle,$$

$$\mathcal{C}_N(\mathcal{O}, \ell) = I(\mathcal{O}, \ell)/P_N(\mathcal{O}, \ell).$$

Recall that $I(\mathcal{O}, 1) = I(\mathcal{O})$ and $P_1(\mathcal{O}, 1) = P_1(\mathcal{O}) = P(\mathcal{O})$, and so $\mathcal{C}_1(\mathcal{O}, 1) = \mathcal{C}(\mathcal{O})$. Furthermore, since $P_N(\mathcal{O}, N) = P_N(\mathcal{O})$, we have $\mathcal{C}_N(\mathcal{O}, N) = \mathcal{C}_N(\mathcal{O})$. And, for simplicity, we just write $\mathcal{M}(\mathcal{O}), P(\mathcal{O}, \ell), \mathcal{C}(\mathcal{O}, \ell)$ for $\mathcal{M}(\mathcal{O}, 1), P_1(\mathcal{O}, \ell), \mathcal{C}_1(\mathcal{O}, \ell)$, respectively. For $a \in \mathcal{M}(\mathcal{O})$, we denote its norm by $N_{\mathcal{O}}(a)$, namely, $N_{\mathcal{O}}(a) = |\mathcal{O}/a|$.

**Lemma 2.1.** Let $\nu \in \mathcal{O} \setminus \{0\}$ and $a, b \in \mathcal{M}(\mathcal{O})$. We get

(i) $N_{\mathcal{O}}(\nu\mathcal{O}) = N_{K/\mathbb{Q}}(\nu)$.

(ii) $N_{\mathcal{O}}(ab) = N_{\mathcal{O}}(a)N_{\mathcal{O}}(b)$.

(iii) $\overline{ab} = N_{\mathcal{O}}(a)\mathcal{O}$, where $\overline{\cdot}$ means the complex conjugation.

**Proof.** See [6, Lemma 7.14].
Lemma 2.2. If \( a \) is a nonzero \( \mathcal{O} \)-ideal, then

\[
\text{a is prime to } \ell \iff \text{N}_\mathcal{O}(a) \text{ is relatively prime to } \ell.
\]

Proof. The proof is the same as that of \([6] \text{ Lemma 7.18 (i)}\) except replacing \( f \) by \( \ell \). \( \Box \)

Remark 2.3. Observe that every nonzero \( \mathcal{O} \)-ideal prime to \( \ell \mathcal{O} \) is proper \( [6] \text{ Lemma 7.18 (ii)} \).

Lemma 2.4. We have \( I(\mathcal{O}, \ell) \cap \mathcal{M}(\mathcal{O}) = \mathcal{M}(\mathcal{O}, \ell) \) for a positive integer \( \ell \).

Proof. The inclusion \( I(\mathcal{O}, \ell) \cap \mathcal{M}(\mathcal{O}) \supseteq \mathcal{M}(\mathcal{O}, N) \) is obvious.

Now, let \( a \in I(\mathcal{O}, \ell) \cap \mathcal{M}(\mathcal{O}) \). Since \( a \in I(\mathcal{O}, \ell) \), we attain \( a = bc^{-1} \) for some \( b, c \in \mathcal{M}(\mathcal{O}, \ell) \). And we get from the fact \( ac = b \) that

\[
\text{N}_\mathcal{O}(a)\text{N}_\mathcal{O}(c) = \text{N}_\mathcal{O}(b)
\]

for a positive integer \( a \).

by Lemma 2.1 (ii). Since \( b \) is prime to \( \ell \), we deduce by Lemma 2.2 that \( \text{gcd}(\text{N}_\mathcal{O}(b), \ell) = 1 \). Thus we obtain by \([6] \text{ Lemma 7.18 (i)}\) that \( \text{gcd}(\text{N}_\mathcal{O}(a), \ell) = 1 \), which implies again by Lemma 2.2 that \( a \) is prime to \( \ell \). Therefore we achieve the converse inclusion \( I(\mathcal{O}, \ell) \cap \mathcal{M}(\mathcal{O}) \subseteq \mathcal{M}(\mathcal{O}, \ell) \). \( \Box \)

Lemma 2.5. Consider the case where \( N = 1 \).

(i) If \( a \in \mathcal{M}(\mathcal{O}, \ell \mathcal{O}) \), then \( a\mathcal{O}_\mathcal{K} \in \mathcal{M}(\mathcal{O}_\mathcal{K}, \ell \mathcal{O}) \) and \( \text{N}_\mathcal{O}(a) = \text{N}_{\mathcal{O}_\mathcal{K}}(a\mathcal{O}_\mathcal{K}) \).

(ii) If \( b \in \mathcal{M}(\mathcal{O}_\mathcal{K}, \ell \mathcal{O}) \), then \( b \cap \mathcal{O} \in \mathcal{M}(\mathcal{O}, \ell \mathcal{O}) \) and \( \text{N}_{\mathcal{O}_\mathcal{K}}(b) = \text{N}_\mathcal{O}(b \cap \mathcal{O}) \).

(iii) The map

\[
\mathcal{M}(\mathcal{O}, \ell \mathcal{O}) \to \mathcal{M}(\mathcal{O}_\mathcal{K}, \ell \mathcal{O}), \quad a \mapsto a\mathcal{O}_\mathcal{K}
\]

induces an isomorphism \( I(\mathcal{O}, \ell \mathcal{O}) \sim \to \mathcal{I}(\mathcal{O}_\mathcal{K}, \ell \mathcal{O}) \).

Proof. See \([6] \text{ Proposition 7.20]}\). \( \Box \)

Lemma 2.6. The map

\[
\phi : \mathcal{M}(\mathcal{O}, \ell \mathcal{O}N) \to \mathcal{M}(\mathcal{O}_\mathcal{K}, \ell \mathcal{O}N), \quad a \mapsto a\mathcal{O}_\mathcal{K}
\]

is well defined, and uniquely gives an isomorphism \( I(\mathcal{O}, \ell \mathcal{O}N) \sim \to I(\mathcal{O}_\mathcal{K}, \ell \mathcal{O}N) \).

Proof. Let \( a \in \mathcal{M}(\mathcal{O}, \ell \mathcal{O}N) \subseteq \mathcal{M}(\mathcal{O}, \ell \mathcal{O}) \). We get by Lemmas 2.2 and 2.3 (i) that \( \text{N}_\mathcal{O}(a) = \text{N}_{\mathcal{O}_\mathcal{K}}(a\mathcal{O}_\mathcal{K}) \) is relatively prime to \( \ell \mathcal{O}N \). So \( a\mathcal{O}_\mathcal{K} \) belongs to \( \mathcal{M}(\mathcal{O}_\mathcal{K}, \ell \mathcal{O}N) \) again by Lemma 2.2 which shows that the map \( \phi \) is well defined. Note further that

\[
\phi(aa') = (aa')\mathcal{O}_\mathcal{K} = (a\mathcal{O}_\mathcal{K})(a'\mathcal{O}_\mathcal{K}) = \phi(a)\phi(a') \quad (a, a' \in \mathcal{M}(\mathcal{O}, \ell \mathcal{O}N)).
\]

Let \( b \in \mathcal{M}(\mathcal{O}_\mathcal{K}, \ell \mathcal{O}N) \subseteq \mathcal{M}(\mathcal{O}_\mathcal{K}, \ell \mathcal{O}) \). It follows from Lemmas 2.2 and 2.3 (ii) that \( \text{N}_{\mathcal{O}_\mathcal{K}}(b) = \text{N}_\mathcal{O}(b \cap \mathcal{O}) \) is relatively prime to \( \ell \mathcal{O}N \), which implies that \( b \cap \mathcal{O} \) belongs to \( \mathcal{M}(\mathcal{O}, \ell \mathcal{O}N) \). Thus we obtain the well-defined map

\[
\psi : \mathcal{M}(\mathcal{O}_\mathcal{K}, \ell \mathcal{O}N) \to \mathcal{M}(\mathcal{O}, \ell \mathcal{O}N)
\]
Moreover, we attain that \( \nu \). (The proof is the same as that of [6, (7.21)] except replacing \( f \) by \( \ell O N \).) Now, we define a map \( \tilde{\phi} : I(O, \ell O N) \rightarrow I(O_K, \ell O N) \) by

\[
\tilde{\phi}(ac^{-1}) = \phi(a)\phi(c)^{-1} \quad (a, c \in M(O, \ell O N)).
\]

Then \( \tilde{\phi} \) is a well-defined isomorphism by [3] and the bijectivity of \( \phi \).

**Lemma 2.7.** If \( \nu \in O_K \setminus \{0\} \), then

\[
\nu \in O, \nu O \text{ is prime to } \ell O N \text{ and } \nu \equiv 1 \pmod{NO}
\]

\[\iff\]

\[
\nu O_K \text{ is prime to } \ell O N \text{ and } \nu \equiv a \pmod{\ell O N O_K} \text{ for some } a \in \mathbb{Z} \text{ such that } a \equiv 1 \pmod{N}.
\]

**Proof.** Assume that \( \nu \in O \), \( \nu O \) is prime to \( \ell O N \) and \( \nu \equiv 1 \pmod{NO} \). By Lemmas 2.2 and 2.6 (i), \((\nu O)O_K = \nu O_K\) is also prime to \( \ell O N \). Since \( \nu \equiv 1 \pmod{NO} \) and \( NO = [\ell O N O_K, N]\), we have

\[
\nu = s\ell O N + tN + 1 \quad \text{for some } s, t \in \mathbb{Z}.
\]

It follows from the fact \( \ell O N O_K = [\ell O N O_K, \ell O N] \) that

\[
\nu \equiv a \pmod{\ell O N O_K} \quad \text{with } a = tN + 1 \text{ satisfying } a \equiv 1 \pmod{N}.
\]

Conversely, assume that \( \nu O_K \) is prime to \( \ell O N \) and \( \nu \equiv a \pmod{\ell O N O_K} \) for some \( a \in \mathbb{Z} \) such that \( a \equiv 1 \pmod{N} \). Since

\[
\nu - a \in \ell O N O_K = N(\ell O K) \subseteq NO \subseteq \mathbb{O} \quad \text{and} \quad a \in \mathbb{Z} \subset \mathbb{O},
\]

we attain that

\[
\nu \in \mathbb{O} \quad \text{and} \quad \nu \equiv a \equiv 1 \pmod{NO}.
\]

Moreover, \( \nu O \) is prime to \( \ell O N \) by Lemma 2.6.

**Proposition 2.8.** Let \( P_{\mathbb{Z}, N}(O_K, \ell O N) \) be the subgroup of \( I(O_K, \ell O N) \) given by

\[
P_{\mathbb{Z}, N}(O_K, \ell O N) = \left\{ \nu O_K \middle| \nu \in O_K \setminus \{0\}, \nu O_K \text{ is prime to } \ell O N, \right. \\
\left. \nu \equiv a \pmod{\ell O N O_K} \text{ for some } a \in \mathbb{Z} \text{ such that } a \equiv 1 \pmod{N} \right\}.
\]

Then we get a natural isomorphism

\[
\mathcal{C}_N(O, \ell O N) \xrightarrow{\sim} I(O_K, \ell O N)/P_{\mathbb{Z}, N}(O_K, \ell O N).
\]

**Proof.** If \( \tilde{\phi} : I(O, \ell O N) \rightarrow I(O_K, \ell O N) \) is the isomorphism described in Lemma 2.6, then we achieve by Lemma 2.7 that

\[
\tilde{\phi}(P_{N}(O, \ell O N)) = P_{\mathbb{Z}, N}(O_K, \ell O N).
\]

Therefore we establish the isomorphism

\[
\mathcal{C}_N(O, \ell O N) \xrightarrow{\sim} I(O_K, \ell O N)/P_{\mathbb{Z}, N}(O_K, \ell O N)
\]

\[
[a b^{-1}] \mapsto [(a O_K)(b O_K)^{-1}]
\]

where \( a \) and \( b \) are nonzero \( O \)-ideals prime to \( \ell O N \).
Remark 2.9. Since $P_{\mathcal{O}_K}(\ell_0N)$ is a congruence subgroup for $\mathcal{O}_N\mathcal{O}_K$, the generalized ideal class group $I(\mathcal{O}_K, \ell_0N)/P_{\mathcal{O}_K}(\ell_0N)$ has finite order ([9, Corollary 1.6 in Chapter IV]). It then follows from Proposition 2.8 that $\mathcal{C}_N(\mathcal{O}, \ell_0N)$ has finite order as well.

Lemma 2.10. Let $\ell$ be a positive integer. Every class in $\mathcal{C}(\mathcal{O})$ contains a proper $\mathcal{O}$-ideal whose norm is relatively prime to $\ell$.

Proof. See [6, Corollary 7.17].

Lemma 2.11. If $\ell$ is a positive integer, then the inclusion $I(\mathcal{O}, \ell) \hookrightarrow I(\mathcal{O})$ induces an isomorphism $\mathcal{C}(\mathcal{O}, \ell) \cong \mathcal{C}(\mathcal{O})$.

Proof. Let $\rho : I(\mathcal{O}, \ell) \to \mathcal{C}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ be the natural homomorphism. Then the surjectivity of $\rho$ follows from Lemmas 2.2 and 2.10. And the proof of $\ker(\rho) = P(\mathcal{O}, \ell)$ is exactly the same as that of [6, Proposition 7.19] except replacing $f$ by $\ell$. Thus we conclude that $\mathcal{C}(\mathcal{O}, \ell) \cong \mathcal{C}(\mathcal{O})$.

Lemma 2.12. The inclusion $P(\mathcal{O}, \ell_0N) \hookrightarrow P(\mathcal{O}, N)$ gives an isomorphism

$$P(\mathcal{O}, \ell_0N)/P_N(\mathcal{O}, \ell_0N) \cong P(\mathcal{O}, N)/P_N(\mathcal{O}).$$

Proof. See [6, Lemma 15.17 and Exercise 15.10].

Proposition 2.13. The inclusion $I(\mathcal{O}, \ell_0N) \hookrightarrow I(\mathcal{O}, N)$ derives an isomorphism

$$\mathcal{C}_N(\mathcal{O}, \ell_0N) \cong \mathcal{C}_N(\mathcal{O}).$$

Proof. Since $P_N(\mathcal{O}, \ell_0N) \subseteq P_N(\mathcal{O})$, the inclusion $I(\mathcal{O}, \ell_0N) \hookrightarrow I(\mathcal{O}, N)$ renders a homomorphism

$$\mathcal{C}_N(\mathcal{O}, \ell_0N) \to \mathcal{C}_N(\mathcal{O}). \quad (6)$$

Let $a_1, a_2, \ldots, a_r \in I(\mathcal{O}, \ell_0N)$ be representatives of classes in $\mathcal{C}(\mathcal{O}, \ell_0N)$. Since we have the natural isomorphisms

$$\mathcal{C}(\mathcal{O}, \ell_0N) \cong \mathcal{C}(\mathcal{O}) \quad \text{and} \quad \mathcal{C}(\mathcal{O}, N) \cong \mathcal{C}(\mathcal{O})$$

by Lemma 2.11, we obtain an isomorphism

$$\mathcal{C}(\mathcal{O}, \ell_0N) \cong \mathcal{C}(\mathcal{O}, N).$$

Thus $a_1, a_2, \ldots, a_r$ are also representatives of classes in $\mathcal{C}(\mathcal{O}, N)$. Now, let $b_1, b_2, \ldots, b_s \in P(\mathcal{O}, \ell_0N)$ be representatives of classes in $P(\mathcal{O}, \ell_0N)/P_N(\mathcal{O}, \ell_0N)$. Then we see by Lemma 2.12 that they are also representatives of classes in $P(\mathcal{O}, N)/P_N(\mathcal{O})$.

Note that there are natural one-to-one correspondences

$$I(\mathcal{O}, \ell_0N)/P(\mathcal{O}, \ell_0N) \times P(\mathcal{O}, \ell_0N)/P_N(\mathcal{O}, \ell_0N) \to I(\mathcal{O}, \ell_0N)/P_N(\mathcal{O}, \ell_0N), \quad \text{and} \quad I(\mathcal{O}, N)/P(\mathcal{O}, N) \times P(\mathcal{O}, N)/P_N(\mathcal{O}) \to I(\mathcal{O}, N)/P_N(\mathcal{O}).$$
Hence
\[ (i = 1, 2, \ldots, r, \ j = 1, 2, \ldots, s) \]
are representatives of classes in \( C_N(O, \ell_{O_N}) \), and also of classes in \( C_N(O) \). This observation implies that the homomorphism in (3) is in fact an isomorphism.

\[ \square \]

**Remark 2.14.** We achieve by Propositions 2.8 and 2.13 that
\[ C_N(O) \simeq I(O_K, \ell_{O_N})/P_{Z,N}(O_K, \ell_{O_N}). \]

**Remark 2.15.** Let \( C \in C_N(O) \). By Proposition 2.13, we have
\[ C = [ab^{-1}] \text{ for some } a, b \in \mathcal{M}(O, \ell_{O_N}). \]

If \( h \) is the order of the group \( C_N(O) \), then we see that
\[ C = [b^h] [ab^{-1}] = [ab^{h-1}] \text{ and } ab^{h-1} \in \mathcal{M}(O, \ell_{O_N}), \]
which claims that \( C \cap \mathcal{M}(O, \ell_{O_N}) \neq \emptyset. \)

3 **The elliptic curve \( E_O \) with complex multiplication by \( O \)**

We shall introduce specific models of elliptic curves with complex multiplication.

Let \( g_2 = g_2(O) \) and \( g_3 = g_3(O) \) be the usual scaled Eisenstein series and
\[ j(O) = 1728 \frac{g_3^3}{\Delta} \text{ with } \Delta = g_2^3 - 27g_3^2. \]

When \( D_O \neq -3, -4 \), we let \( E_O \) be the elliptic curve with \( j \)-invariant \( j(E_O) = j(O) \) given by the Weierstrass equation
\[ E_O : y^2 = 4x^3 - A_Ox - B_O \]
with base point \( O = [0 : 1 : 0] \), where
\[ A_O = \frac{j(O)(j(O) - 1728)}{2^{12}3^9} \text{ and } B_O = \frac{j(O)(j(O) - 1728)^2}{2^{18}3^{15}}. \]

If \( \wp(\cdot ; O) : \mathbb{C} \rightarrow \mathbb{C} \cup \{\infty\} \) is the Weierstrass \( \wp \)-function for the lattice \( O \) with derivative \( \wp' \), then we get a complex analytic isomorphism
\[ \mathbb{C}/O \xrightarrow{\sim} E(C) \quad (\subset \mathbb{P}^2(C)) \]
\[ z + O \mapsto [x(z; O) : y(z; O) : 1] = \left[ \frac{g_2g_3}{\Delta} \wp(z; O) : \sqrt{\left( \frac{g_2g_3}{\Delta} \right)^3 \wp'(z; O)} : 1 \right] \]
(cf. [25, §VI.3]). Note that \( g_2g_3 \neq 0 \) because we are assuming that \( D_O \neq -3, -4 \) (cf. [6, Exercise 10.19]). For each \( v = \begin{bmatrix} v_1 & v_2 \end{bmatrix} \in M_{1,2}(Q) \setminus M_{1,2}(Z) \), we set
\[ X_v = \frac{g_2g_3}{\Delta} \wp(v_1\tau_O + v_2; O), \]
\[ Y_v = \sqrt{\left( \frac{g_2g_3}{\Delta} \right)^3 \wp'(v_1\tau_O + v_2; O)}, \]
where \( \tau_O \) is the element of \( \mathbb{H} \) described in [2].

9
Lemma 3.1. Let $u, v \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z})$ and $n \in M_{1,2}(\mathbb{Z})$. Then we have

(i) $X_u = X_v$ if and only if $u \equiv v$ or $-v$ (mod $M_{1,2}(\mathbb{Z})$).

(ii) $Y_{v+n} = Y_v$.

(iii) $Y_{-v} = -Y_v$.

(iv) $Y_v = 0$ if and only if $2v \in M_{1,2}(\mathbb{Z})$.

Proof. See [6, §10.A].

Proposition 3.2. The theory of complex multiplication yields the following results.

(i) $H_O = K(j(O))$.

(ii) If $D_O \neq -3, -4$ and $N \geq 2$, then

$$K_{O,N} = H_O\left(X_{\left[\begin{smallmatrix} 0 \\ N \end{smallmatrix}\right]}\right).$$

Proof. See [13, Theorem 5 in Chapter 10] and [20, Theorem 6.2.3].

4 Fields of modular functions

We shall recall some necessary properties of Fricke functions and Siegel functions.

The modular group $SL_2(\mathbb{Z})$ acts on the complex upper half-plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid \text{Im}(\tau) > 0\}$ by fractional linear transformations. Let $j$ be the elliptic modular function on $\mathbb{H}$, that is,

$$j(\tau) = j([\tau, 1]) \quad (\tau \in \mathbb{H}).$$

For each $v \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z})$, the Fricke function $f_v$ on $\mathbb{H}$ is defined by

$$f_v(\tau) = -2^{\tau^3} g_2([\tau, 1]) g_3([\tau, 1]) \frac{\varphi(v_1 \tau + v_2; [\tau, 1])}{\Delta([\tau, 1])} \quad (\tau \in \mathbb{H}).$$

And, for a positive integer $N$, let

$$F_N = \begin{cases} \mathbb{Q}(j) & \text{if } N = 1, \\ \mathbb{Q}(j, f_v \mid v \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z}) \text{ satisfies } Nv \in M_{1,2}(\mathbb{Z})) & \text{if } N \geq 2. \end{cases}$$

Proposition 4.1. The field $F_N$ is a Galois extension of $F_1$ whose Galois group is isomorphic to $GL_2(\mathbb{Z}/NZ)/\langle -I_2 \rangle$. If $\gamma \in SL_2(\mathbb{Z})$, then

$$f_{\tilde{\gamma}} = f \circ \gamma$$

where $\tilde{\gamma}$ is the image of $\gamma$ in $GL_2(\mathbb{Z}/NZ)/\langle -I_2 \rangle$.

Proof. See [21, Theorem 6.6].
Furthermore, $\mathcal{F}_N$ coincides with the field of meromorphic modular functions for the principal congruence subgroup

$$\Gamma(N) = \{ \gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv I_2 \pmod{NM_2(\mathbb{Z})} \}$$

whose Fourier coefficients belong to the $N$th cyclotomic field $\mathbb{Q}(\zeta_N)$ with $\zeta_N = e^{2\pi i/N}$ (cf. [21, Proposition 6.9]).

On the other hand, for $v = \begin{bmatrix} v_1 & v_2 \end{bmatrix} \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z})$, the Siegel function $g_v$ on $\mathbb{H}$ is given by the infinite product expansion

$$g_v(\tau) = -q^{\frac{1}{2}}B_2(v_1)e^{\pi iv_2(v_1-1)}(1 - q_z) \prod_{n=1}^{\infty} (1 - q^n q_z)(1 - q^n q_z^{-1}) \quad (\tau \in \mathbb{H}) \quad (13)$$

where $q_z = e^{2\pi i z}$ with $z = v_1 \tau + v_2$ and $B_2(x) = x^2 - x + \frac{1}{6}$ is the second Bernoulli polynomial. Observe that $g_v$ has neither a zero nor a pole on $\mathbb{H}$. One can refer to [14] for further details on Siegel functions.

For $N \geq 2$, we say that $v \in M_{1,2}(\mathbb{Q})$ is primitive modulo $N$ if $N$ is the smallest positive integer so that $Nv \in M_{1,2}(\mathbb{Z})$. Let $V_N$ be the set of all such primitive vectors $v$. We call a collection $\{h_v\}_{v \in V_N}$ of functions in $\mathcal{F}_N$ a Fricke family of level $N$ if

(i) $h_v$ is holomorphic on $\mathbb{H}$ ($v \in V_N$),

(ii) $h_u = h_v$ if $u \equiv v$ or $-v$ (mod $M_{1,2}(\mathbb{Z})$),

(iii) $h_{v^\gamma} = h_v^\gamma$ ($v \in V_N$ and $\gamma \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/(−I_2) \simeq \text{Gal}(\mathbb{F}_N/\mathbb{F}_1)$).

**PROPOSITION 4.2.** The collections $\{f_v\}_{v \in V_N}$ and $\{g_{12}^{vN}\}_{v \in V_N}$ are Fricke families of level $N$.

**PROOF.** See [14, Proposition 1.3 in Chapter 2] and [21, Theorem 6.6].

**LEMMA 4.3.** We have a relationship between $j$ and $g_{12}^{[0 \ 1]}$ in such a way that

$$j = \left( \frac{g_{12}^{[0 \ 1]} + 16}{g_{12}^{[0 \ 1]}} \right)^3.$$

**PROOF.** See [6, Theorem 12.17].

Let

$$V'_N = \left\{ \begin{bmatrix} v_1 & v_2 \end{bmatrix} \in V_N \mid 0 \leq v_1, v_2 < 1 \right\},$$

$$T_N = \left\{ (u, v) \in V'_N \times V'_N \mid u \not\equiv v, -v \pmod{M_{1,2}(\mathbb{Z})} \right\}.$$

**LEMMA 4.4.** We deduce

$$\prod_{(u, v) \in T_N} (f_u - f_v)^6 = k \{ j^2(j - 1728)^3 \}^{\mid T_N \mid} \quad \text{for some } k \in \mathbb{Q} \setminus \{0\}.$$

**PROOF.** See [12, Lemma 6.2].
5 Form class groups

In this section, we shall review the classical form class groups and try to find certain generalization of these as well.

For a negative integer $D$ such that $D \equiv 0$ or $1 \pmod{4}$, let

$$Q(D) = \left\{ Q = Q \left( \begin{bmatrix} x \\ y \end{bmatrix} \right) = ax^2 + bx + cy^2 \in \mathbb{Z}[x, y] \mid \gcd(a, b, c) = 1, b^2 - 4ac = D, a > 0 \right\}. $$

The modular group $\text{SL}_2(\mathbb{Z})$ acts on the set $Q(D)$ from the right as

$$Q^\gamma = Q \left( \begin{bmatrix} x' \\ y' \end{bmatrix} \right)$$

and induces the proper equivalence $\sim$ on $Q(D)$ as follows:

$$Q \sim Q' \iff Q' = Q^\gamma \text{ for some } \gamma \in \text{SL}_2(\mathbb{Z})$$

(cf. [6, pp. 20–22]). We say that a form $Q = ax^2 + bxy + cy^2 \in Q(D)$ is reduced if

$$\left\{ \begin{array}{l}
|b| \leq a \leq c, \\
 b \geq 0 \text{ if either } |b| = a \text{ or } a = c.
\end{array} \right.$$  

Lemma 5.1. Every form in $Q(D)$ is properly equivalent to a unique reduced form.

Proof. See [6, Theorem 2.8].

For $Q = ax^2 + bxy + cy^2 \in Q(D)$, let $\omega_Q$ be the zero of the quadratic polynomial $Q(x, 1)$ lying in $\mathbb{H}$, namely,

$$\omega_Q = \frac{-b + \sqrt{D}}{2a}.$$  

Lemma 5.2. If $Q = ax^2 + bxy + cy^2 \in Q(D)$, then $a[\omega_Q, 1]$ is a proper $O$-ideal with $N_O(a[\omega_Q, 1]) = a$.

Proof. See [6, Lemma 7.5 and (7.16)].

Lemma 5.3. Let $Q = ax^2 + bxy + cy^2, Q'' = a''x^2 + b''xy + c''y^2 \in Q(D)$ such that

$$\gcd(a, a'', (b + b'')/2) = 1.$$  

(i) There is a unique integer $B$ modulo $2aa''$ such that

$$B \equiv b \pmod{2a}, \quad B \equiv b'' \pmod{2a''}, \quad B^2 \equiv D \pmod{4aa''}. \quad (14)$$

(ii) Let

$$Q''' = aa''x^2 + Bxy + \frac{B^2 - D}{4aa''}y^2 \quad (15)$$

where $B$ is an integer satisfying (14). Then we derive

$$[\omega_Q, 1][\omega_{Q''}, 1] = [\omega_{Q'''}, 1].$$
Proof. (i) See [6, Lemma 3.2].

(ii) See [6, (7.13)].

Remark 5.4. We call the form in (15) a Dirichlet composition of \( Q \) and \( Q' \).

Lemma 5.5. Let \( Q \in \mathbb{Q}(D) \) and \( M \) be a positive integer. Then there is a matrix \( \gamma \) in \( \text{SL}_2(\mathbb{Z}) \) so that the coefficient of \( x^2 \) in \( Q' \) is relatively prime to \( M \).

Proof. See [6, Lemmas 2.3 and 2.25].

Proposition 5.6. Let \( C(D) = \mathbb{Q}(D)/\sim \) be the set of equivalence classes.

(i) The following binary operation on \( C(D) \) is well defined and makes \( C(D) \) into a finite abelian group: let \( C, C' \in C(D) \) and so \( C = [Q], C' = [Q'] \) for some \( Q = ax^2 + bxy + cy^2, Q' \in \mathbb{Q}(D) \), respectively. By Lemma 5.5 one can take a matrix \( \gamma \) in \( \text{SL}_2(\mathbb{Z}) \) for which \( Q'' = Q'\gamma = a''x^2 + b''xy + c''y^2 \) satisfies \( \gcd(a, a'', (b + b'')/2) = 1 \). We define the product \( CC' \) by the class of any Dirichlet composition of \( Q \) and \( Q'' \).

(ii) If \( D = D_\mathcal{O} \), then the map

\[
\begin{align*}
C(D_\mathcal{O}) & \to C(\mathcal{O}) \\
[Q] & \mapsto ([\omega_Q, 1])
\end{align*}
\]

is a well-defined isomorphism of \( C(D_\mathcal{O}) \) onto \( C(\mathcal{O}) \).

Proof. See [6, Theorems 3.9 and 7.7].

Now, let

\[
\mathbb{Q}(D_\mathcal{O}, N) = \{ax^2 + bxy + cy^2 \in \mathbb{Q}(D_\mathcal{O}) \mid \gcd(a, N) = 1\}
\]

and

\[
\Gamma_1(N) = \left\{ \gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{NM_2(\mathbb{Z})} \right\}
\]

which is a congruence subgroup of \( \text{SL}_2(\mathbb{Z}) \) of level \( N \). Observe that for \( Q = ax^2 + bxy + cy^2 \in \mathbb{Q}(D_\mathcal{O}, N) \) and \( \gamma = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \Gamma_1(N), \)

\[
Q^\gamma \equiv Q \begin{bmatrix} 1 & q \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \equiv ax^2 + (2aq + b)xy + (aq^2 + bq + c)y^2 \pmod{N\mathbb{Z}[x, y]}.\]

This implies that \( \Gamma_1(N) \) acts on \( \mathbb{Q}(D_\mathcal{O}, N) \). Let \( \sim_{\Gamma_1(N)} \) be the equivalence relation on \( \mathbb{Q}(D_\mathcal{O}, N) \) induced from the action of \( \Gamma_1(N) \). We mean by \( C_N(D_\mathcal{O}) \) the set of equivalence classes, that is,

\[
C_N(D_\mathcal{O}) = \mathbb{Q}(D_\mathcal{O}, N)/\sim_{\Gamma_1(N)}.\]

For \( \alpha = \begin{bmatrix} s & t \\ u & v \end{bmatrix} \in \text{SL}_2(\mathbb{Z}) \) and \( \tau \in \mathbb{H} \), we write

\[
j(\alpha, \tau) = ut + v.
\]
Definition 5.7. We define a binary operation on $C_N(D_O)$ as follows: let $C, C' \in C_N(D_O)$, and so $C = [Q], C' = [Q']$ for some $Q = ax^2 + bxy + cy^2, Q' \in Q(D_O, N)$, respectively. By Lemma 5.5 there is a matrix $\gamma$ in $SL_2(\mathbb{Z})$ so that $Q'' = Q' \gamma = a''x^2 + b''xy + c''y^2$ satisfies $\gcd(a, a'', (b + b'')/2) = 1$. Let $Q'''$ be a Dirichlet composition of $Q$ and $Q''$. And, set

$$\nu_1 = \frac{\omega_{Q''}}{j(\gamma, \omega_{Q''})} \quad \text{and} \quad \nu_2 = \frac{1}{j(\gamma, \omega_{Q''})}.$$ 

One can show that there is a pair $(u, v)$ of integers satisfying

$$u\nu_1 + v\nu_2 = 1$$

and in $SL_2(\mathbb{Z})$ there exists a matrix $\sigma$ such that

$$\sigma \equiv \begin{bmatrix} * & * \\ u & v \end{bmatrix} (\mod NM_2(\mathbb{Z})).$$

We then define

$$CC' = \left[(Q''')^{\sigma^{-1}}\right].$$

In §9 we shall prove that the binary operation given in Definition 5.7 is well defined and makes $C_N(D_O)$ a finite abelian group isomorphic to $C_N(O)$ (Theorem 9.4). And, through the binary operation on $C_N(D_O)$ we regard the natural map $C_N(D_O) \to C_1(D_O) = C(D_O)$ as a homomorphism.

6 Inequalities on special values of modular functions

We shall develop certain inequalities on the special values of $j$ and Siegel functions. By using these inequalities we shall present another new generators of $H_O$ and $K_{O,N}$, for later use in §7, which are different from the classical ones stated in Proposition 3.2.

Lemma 6.1. Let $\tau \in \mathbb{H}$ and $t = |e^{2\pi i \tau}|$.

(i) $|g_{\frac{1}{2}}(\tau)| \leq 2t \frac{1}{\pi} e^{-2 + \frac{1}{1+4t^2}}$.

(ii) $|g_{\frac{1}{2}}(s)(\tau)| \leq t \frac{1}{\pi} e^{\frac{1}{1+4t^2}}$ for any $s \in \mathbb{Q}$.

Proof. See [11, Lemma 5.2].

Let $Q_0$ be the principal form in $Q(D_O)$ defined by

$$Q_0 = \begin{cases} 
    x^2 - \frac{D_O}{4}y^2 & \text{if } D_O \equiv 0 \pmod{4}, \\
    x^2 + xy + \frac{1-D_O}{4}y^2 & \text{if } D_O \equiv 1 \pmod{4},
\end{cases}$$

which represents the identity class in $C(D_O)$ (cf. [9, Theorem 3.9]). Then we see that

$$\omega_{Q_0} = \tau_O \quad \text{and} \quad [\omega_{Q_0}, 1] = O.$$ 

Let $h_O$ denote the order of the group $C(O)$ and so $h_O = [H_O : K]$. 

14
Lemma 6.2. Assume that $h_O \geq 2$. Let $Q = ax^2 + bxy + cy^2$ be a reduced form in $Q(D_O)$ such that $Q \neq Q_0$.

(i) $|g[0, \frac{1}{2}](\omega Q)| > 1.98e^{-\frac{\pi \sqrt{|D_O|}}{24}}$.

(ii) $\left| \frac{j(\omega Q)^2(j(\omega Q) - 1728)^3}{j(\omega Q_0)^2(j(\omega Q_0) - 1728)^3} \right| < 877383e^{-\frac{5\pi \sqrt{|D_O|}}{2}} \leq (1)$.

Proof. (i) Since $Q$ is a reduced form in $Q(D_O)$ such that $Q \neq Q_0$, we have

$$2 \leq a \leq \sqrt{|D_O|}$$

(13 p. 24). Then we derive that

$$|g[0, \frac{1}{2}](\omega Q)| \geq 2e^{-\frac{\pi \sqrt{|D_O|}}{24}} \prod_{n=1}^{\infty} (1 - e^{-\pi \sqrt{3n}})^2 \text{ by the definition (15) and (16)}$$

$$\geq 2e^{-\frac{\pi \sqrt{|D_O|}}{24}} \prod_{n=1}^{\infty} e^{-2k^n} \text{ with } k = e^{-\frac{\pi \sqrt{3}}{100}}$$

because $1 - X > e^{-X}$ for $0 < X \leq e^{-\pi \sqrt{3}}$

$$= 2e^{-\frac{\pi \sqrt{|D_O|}}{24}} e^{-\frac{2k^n}{n}}$$

$$> 1.98e^{-\frac{\pi \sqrt{|D_O|}}{24}}.$$  

(ii) First, consider the case where $D_O \leq -20$. We then observe by Lemma 6.1 (i) and (15) that

$$|g[0, \frac{1}{2}](\omega Q_0)| \leq 2^{12} e^{-\pi \sqrt{|D_O|} e^{-24 + \frac{4}{n} - \frac{24}{1 - e^{-\pi \sqrt{3n}}}}} \leq 4097e^{-\pi \sqrt{|D_O|}} < 0.0033 \quad (17)$$

and

$$|g[0, \frac{1}{2}](\omega Q)| \leq 2^{12} e^{-\pi \sqrt{|D_O|} e^{-24 + \frac{4}{n} - \frac{24}{1 - e^{-\pi \sqrt{3n}}}}} \leq 2^{12} e^{-\pi \sqrt{3} e^{-24 + \frac{4}{n} - \frac{24}{1 - e^{-\pi \sqrt{3n}}}}} < 19.71. \quad (18)$$

Hence we find that

$$\left| \frac{j(\omega Q)^2(j(\omega Q) - 1728)^3}{j(\omega Q_0)^2(j(\omega Q_0) - 1728)^3} \right| = \left| g[0, \frac{1}{2}](\omega Q_0)^{12} \right|^5 \left| \frac{\left( g[0, \frac{1}{2}](\omega Q)^{12} + 16 \right)^2 \left( g[0, \frac{1}{2}](\omega Q)^{12} + 64 \right) \left( g[0, \frac{1}{2}](\omega Q)^{12} - 8 \right)^2}{\left( g[0, \frac{1}{2}](\omega Q_0)^{12} + 16 \right)^2 \left( g[0, \frac{1}{2}](\omega Q_0)^{12} + 64 \right) \left( g[0, \frac{1}{2}](\omega Q_0)^{12} - 8 \right)^2} \right|^3$$

$$\leq \left( 4097e^{-\pi \sqrt{|D_O|}} \right)^5 \left| \frac{(16 + 19.71)(64 + 19.71)(8 + 19.71)^2}{(16 - 0.0033)(64 - 0.0033)(8 - 0.0033)^2} \right|^3 \text{ by (i), (17) and (18)}$$

$$< 877383e^{-\frac{5\pi \sqrt{|D_O|}}{2}}.$$  

The only remaining case is $K = Q(\sqrt{-15})$ and $O = O_K$, and so $h_O = 2$ and

$$Q_0 = x^2 + xy + 4y^2, \quad Q = 2x^2 + xy + 2y^2.$$
One can then numerically verify that (ii) also holds in this case (cf. [12, Remark 4.2]).

Proposition 6.3. The special value \( j(\tau_\mathcal{O}) = j(\omega_{Q_0}) \) generates \( H_\mathcal{O} \) over \( K \). If \( Q_1, Q_2, \ldots, Q_{h_\mathcal{O}} \) are reduced forms in \( Q(D_\mathcal{O}) \), then the special values \( j(\omega_{Q_1}), j(\omega_{Q_2}), \ldots, j(\omega_{Q_{h_\mathcal{O}}}) \) are distinct Galois conjugates of \( j(\tau_\mathcal{O}) \) over \( K \).

Proof. See Lemma 5.1, Proposition 5.6 (ii) and [15, Theorem 5 in Chapter 10].

Proposition 6.4. The special value \( \{ j(\tau_\mathcal{O})^2(j(\tau_\mathcal{O}) - 1728)^3 \}^n \) generates \( H_\mathcal{O} \) over \( K \) for any positive integer \( n \).

Proof. If \( h_\mathcal{O} = 1 \) and so \( H_\mathcal{O} = K \), then the assertion is trivial.

Now, consider the case where \( h_\mathcal{O} \geq 2 \). Since \( D_\mathcal{O} \neq -3, -4 \), we have \( j(\tau_\mathcal{O})^2(j(\tau_\mathcal{O}) - 1728)^3 \neq 0 \) (cf. [6, Theorem 7.30 (ii), (10.8) and Exercise 10.19]). Let \( \sigma \) be an element of \( \text{Gal}(H_\mathcal{O}/K) \) leaving the value \( \{ j(\tau_\mathcal{O})^2(j(\tau_\mathcal{O}) - 1728)^3 \}^n \) fixed. We then achieve

\[
1 = \left| \frac{j(\omega_{Q_0})^2(j(\omega_{Q_0}) - 1728)^3}{j(\omega_{Q_0})^2(j(\omega_{Q_0}) - 1728)^3} \right|^n \sigma
\]

\[
= \left| \frac{j(\omega_{Q})^2(j(\omega_{Q}) - 1728)^3}{j(\omega_{Q})^2(j(\omega_{Q}) - 1728)^3} \right|^n
\]

for some reduced form \( Q \) in \( Q(D_\mathcal{O}) \) by Proposition 6.3.

By Lemma 6.2 (ii), we must get \( Q = Q_0 \) and hence \( \sigma \) is the identity element. This implies by Galois theory that \( \{ j(\tau_\mathcal{O})^2(j(\tau_\mathcal{O}) - 1728)^3 \}^n \) generates \( H_\mathcal{O} \) over \( K \).

When \( D_\mathcal{O} \neq -3, -4 \), let \( E_\mathcal{O} \) be the elliptic curve given by the special model in [1]. For \( v \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z}) \), recall the definitions of \( X_v \) and \( Y_v \) in [9] and [10], respectively.

Proposition 6.5. Assume that \( D_\mathcal{O} \neq -3, -4 \). If \( N \geq 2 \) and \( K_{\mathcal{O},N} \) properly contains \( H_\mathcal{O} \), then

\[
K_{\mathcal{O},N} = K \left( X_{[0 \frac{1}{2}]}, Y^2_{[0 \frac{1}{2}]} \right).
\]

Proof. Let \( L = K(X, Y^2) \) with \( X = X_{[0 \frac{1}{2}]} \) and \( Y = Y_{[0 \frac{1}{2}]} \). Since \( X \) and \( Y^2 \) belong to \( K_{\mathcal{O},N} \) by Proposition 3.2 and the relation

\[
Y^2_{[0 \frac{1}{2}]} = 4X^3_{[0 \frac{1}{2}]} - A_{\mathcal{O}}X_{[0 \frac{1}{2}]} - B_{\mathcal{O}},
\]

\( L \) is a subfield of \( K_{\mathcal{O},N} \). And, \( A_{\mathcal{O}}, B_{\mathcal{O}} \in H_\mathcal{O} \).

Suppose on the contrary that \( L \neq K_{\mathcal{O},N} \). Then there exists a nonidentity element \( \sigma \) of \( \text{Gal}(K_{\mathcal{O},N}/K) \) which leaves the values \( X \) and \( Y^2 \) fixed. Here we further note that

\[
\sigma \not\in \text{Gal}(K_{\mathcal{O},N}/H_\mathcal{O})
\]

because \( K_{\mathcal{O},N} = H_\mathcal{O}(X) \) by Proposition 3.2. Since

\[
4X^3 - A_{\mathcal{O}}X - B_{\mathcal{O}} = Y^2 = 4X^3 - A_{\mathcal{O}}^2X - B_{\mathcal{O}}^2,
\]

we obtain that

\[
(A_{\mathcal{O}}^2 - A_{\mathcal{O}})X = B_{\mathcal{O}} - B_{\mathcal{O}}^2.
\]
On the other hand, we see that

$$A_O B_O = \frac{j(\tau_O)^2(j(\tau_O) - 1728)^3}{2^{30} 3^{24}},$$

which generates $H_O$ over $K$ by Proposition [12]. Thus $A_O B_O$ is not fixed by $\sigma$ by (19), and so $A_O^\sigma \neq A_O$ or $B_O^\sigma \neq B_O$. It follows from (20) that $A_O^\sigma \neq A_O$ and

$$X = \frac{B_O - B_O^\sigma}{A_O^\sigma - A_O} \in H_O.$$

Then we derive $K_{O,N} = H_O(X) = H_O$, which contradicts the hypothesis that $K_{O,N}$ properly contains $H_O$.

Therefore we conclude that

$$L = K\left(\frac{X}{0 \ 1}, \frac{Y^2}{0 \ 1}\right) = K_{O,N}.$$

\[\square\]

7 Extension fields of $\mathbb{Q}$ generated by torsion points of $E_O$

In §7 and §8, we assume that $D_O \neq -3, -4$. Let $E_O[N]$ be the group of $N$-torsion points of $E_O$ and $\mathbb{Q}(E_O[N])$ be the extension field of $\mathbb{Q}$ generated by the coordinates of points in $E_O[N]$. Then we have

$$\mathbb{Q}(E_O[N]) = \begin{cases} \mathbb{Q} & \text{if } N = 1, \\ \mathbb{Q}(X_v, Y_v) & \mathbb{Q}(X_v, Y_v) \mid v \in W_N) & \text{if } N \geq 2, \end{cases}$$

where

$$W_N = \{v \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z}) \mid Nv \in M_{1,2}(\mathbb{Z})\}.$$

In this section, we shall examine the field $\mathbb{Q}(E_O[N])$ by comparing with $K_{O,N}$.

**Lemma 7.1.** Let $N \geq 2$. If $\{h_v\}_{v \in V_N}$ is a Fricke family of level $N$, then

$$\overline{h_v(\tau_O)} = h_v(\frac{1}{0 \ b_{-1}})(\tau_O) \quad (v \in V_N).$$

**Proof.** See [14, Proposition 1.4 in Chapter 2].

By the definitions (9) and (11), we attain

$$X_v = -\frac{1}{2^{7/3}} f_v(\tau_O) \quad (v \in W_N). \tag{21}$$

**Remark 7.2.** We find that for $v \in W_N$

$$\overline{X_v} = -\frac{1}{2^{7/3}} f_v(\tau_O)$$

$$= -\frac{1}{2^{7/3}} f_v(\frac{1}{0 \ b_{-1}})(\tau_O) \quad \text{by Proposition 4.2 and Lemma 7.1}$$

$$= X_v(\frac{1}{0 \ b_{-1}}).$$

17
Let $R_{O,N}$ be the maximal real subfield of $K_{O,N}$.

**Lemma 7.3.** We have

$$R_{O,N} = \mathbb{Q}\left(j(\tau_O), X_{[0 \frac{1}{N}]}\right) \quad \text{and} \quad K_{O,N} = KR_{O,N}.$$ 

**Proof.** Observe that

$$X_{[0 \frac{1}{N}]} = X_{[0 \frac{1}{N}]} \left[1 \frac{b}{1}ight]^{(\tau_O)} \quad \text{by Remark 7.2}$$

$$= X_{[0 \frac{1}{N}]} \quad \text{by Lemma 3.1 (i),}$$

and hence $X_{[0 \frac{1}{N}]} \in \mathbb{R}$. Furthermore, since $j(\tau_O) \in \mathbb{R}$ (cf. [24, p. 179]) and $K$ is imaginary quadratic, we derive by Proposition 3.2 that

$$R_{O,N} = \mathbb{Q}\left(j(\tau_O), X_{[0 \frac{1}{N}]}\right) \quad \text{and} \quad K_{O,N} = KR_{O,N}.$$ 

□

**Lemma 7.4.** If $N \geq 2$, then $\mathbb{Q}(X_v \mid v \in W_N)$ contains $\mathbb{Q}(j(\tau_O))$.

**Proof.** Let $M$ be the maximal real subfield of $H_O$. Since $j(\tau_O) \in \mathbb{R}$ and

$$H_O = K(j(\tau_O)) = K\left(\{j(\tau_O)^2(j(\tau_O) - 1728)^3\}_{|T_N|}\right) \quad (22)$$

by Propositions 6.3 and 6.4, we deduce that $[H_O : M] = 2$ and

$$M = \mathbb{Q}(j(\tau_O)) = \mathbb{Q}\left(\{j(\tau_O)^2(j(\tau_O) - 1728)^3\}_{|T_N|}\right).$$

Then we find that

$$\mathbb{Q}(X_v \mid v \in W_N) \supseteq \mathbb{Q}\left(\prod_{(u,v) \in T_N} (X_u - X_v)\right)$$

$$= \mathbb{Q}\left(\{j(\tau_O)^2(j(\tau_O) - 1728)^3\}_{|T_N|}\right) \quad \text{by (21) and Lemma 4.4}$$

$$= \mathbb{Q}(j(\tau_O)) \quad \text{by (22).}$$ 

□

**Proposition 7.5.** Assume that $D_O \neq -3, -4$ and $N \geq 2$.

(i) The field $\mathbb{Q}(X_v \mid v \in W_N)$ contains $R_{O,N}$. Furthermore, $K(X_v \mid v \in W_N) = K_{O,N}$.

(ii) If $D_O \equiv 0 \pmod{4}$, then $\mathbb{Q}(X_v \mid v \in W_2) = R_{O,2}$.

(iii) If $D_O \equiv 1 \pmod{4}$ or $N \geq 3$, then $\mathbb{Q}(X_v \mid v \in W_N) = K_{O,N}$.
Proof. (i) We see that 
\[ R_{\mathcal{O},N} = \mathbb{Q} \left( j(\tau_{\mathcal{O}}), X_{\left[0 \frac{1}{N}\right]} \right) \] 
by Lemma 7.3 
\[ \subseteq \mathbb{Q}(X_v \mid v \in W_N) \] 
by Lemma 7.4 
\[ \subseteq K_{\mathcal{O},N} \] 
by (3) and (21) 
\[ = KR_{\mathcal{O},N} \] 
by Lemma 7.3.

Thus it yields that 
\[ K(\mathbb{Q}(X_v \mid v \in W_N)) = K_{\mathcal{O},N}. \]

(ii) If \( D_{\mathcal{O}} \equiv 0 \pmod{4} \), then we claim that for \( v \in W_2 \)
\[ \overline{X}_v = X_{v^{\left[1 \frac{0}{0} \frac{-1}{1}\right]}(\tau_{\mathcal{O}})} \] 
by Remark 7.2
\[ = X_v \] 
by Lemma 3.1 (i).

This implies by (i) that \( \mathbb{Q}(X_v \mid v \in W_2) = R_{\mathcal{O},2} \).

(iii) If \( D_{\mathcal{O}} \equiv 1 \pmod{4} \), then we establish that
\[ \overline{X}_{\left[0 \frac{0}{0} \frac{0}{1}\right]} = \overline{X}_{\left[1 \frac{1}{N} \frac{0}{0}\right]}^{(\tau_{\mathcal{O}})} \] 
by Remark 7.2
\[ = \overline{X}_{\left[0 \frac{0}{0} \frac{0}{1}\right]} \] 
by Lemma 3.1 (i).

Similarly, if \( D_{\mathcal{O}} \equiv 0 \pmod{4} \) and \( N \geq 3 \), then
\[ \overline{X}_{\left[\frac{1}{N} \frac{1}{N} \frac{1}{N}\right]} = \overline{X}_{\left[\frac{1}{N} \frac{1}{0} \frac{1}{0}\right]}^{(\tau_{\mathcal{O}})} \neq X_{\left[\frac{1}{N} \frac{1}{N} \frac{1}{N}\right]} \] 
by Lemma 7.3 (i).

These observations hold that if \( D_{\mathcal{O}} \equiv 1 \pmod{4} \) or \( N \geq 3 \), then
\[ \mathbb{Q}(X_v \mid v \in W_N) \not\subseteq \mathbb{R}. \]

Therefore we conclude by (i) and Lemma 7.3 that \( \mathbb{Q}(X_v \mid v \in W_N) = K_{\mathcal{O},N} \).

Lemma 7.6. If \( u, v \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z}) \) satisfy
\[ 2u \notin M_{1,2}(\mathbb{Z}) \quad \text{and} \quad Nu, Nv \in M_{1,2}(\mathbb{Z}), \]
then the ratio \( \frac{Y_v}{Y_u} \) lies in \( K_{\mathcal{O},N} \).

Proof. See [13, Proof of Lemma 5.3] and (3). □

Remark 7.7. (i) If \( 2u \in M_{1,2}(\mathbb{Z}) \), then \( Y_u = 0 \) by Lemma 3.1 (iv).

(ii) By [13, Lemma 3.3], we have
\[ \frac{Y_v}{Y_u} = \frac{g_{2v}(\tau_{\mathcal{O}})g_u(\tau_{\mathcal{O}})^4}{g_v(\tau_{\mathcal{O}})^4g_{2u}(\tau_{\mathcal{O}})}. \]
Theorem 7.8. Assume that $D_{O} \neq -3, -4$.

(i) If $D_{O} \equiv 0 \pmod{4}$, then $\mathbb{Q}(E_{O}[2])$ is the maximal real subfield of $K_{O,2}$.

(ii) If $D_{O} \equiv 1 \pmod{4}$, then $\mathbb{Q}(E_{O}[2]) = K_{O,2}$.

(iii) If $N \geq 3$, then $\mathbb{Q}(E_{O}[N])$ is an extension field of $K_{O,N}$ of degree at most 2.

Proof. We get by Lemma 3.1 (iv) that

$$\mathbb{Q}(E_{O}[2]) = \mathbb{Q}(X_{v} \mid v \in W_{2}).$$

(i) If $D_{O} \equiv 0 \pmod{4}$, then we obtain by (23) and Proposition 7.5 that $\mathbb{Q}(E_{O}[2]) = R_{O,2}$.

(ii) If $D_{O} \equiv 1 \pmod{4}$, then we derive by (23) and Proposition 7.5 (iii) that $\mathbb{Q}(E_{O}[2]) = K_{O,2}$.

(iii) If $N \geq 3$, then we find that

$$\mathbb{Q}(E_{O}[N]) = K_{O,N}(Y_{v} \mid v \in W_{N}) \text{ by Proposition 7.5 (iii)}$$

$$= K_{O,N} \left( \frac{Y_{v}}{Y_{v}} \right) \text{ by Lemma 7.6}$$

Here we observe by Proposition 3.2 that

$$Y_{v}^{2} = 4X_{v}^{3} - A_{O}X_{v} - B_{O} \in K_{O,N}.$$  

Therefore $\mathbb{Q}(E_{O}[N])$ is an extension field of $K_{O,N}$ of degree at most 2.

\[\square\]

8 Galois representations attached to $E_{O}$

Since the elliptic curve $E_{O}$ is defined over $\mathbb{Q}(j(E_{O}))$, the field $\mathbb{Q}(E_{O}[N])$ is a finite Galois extension of $\mathbb{Q}(j(E_{O}))$ by Lemma 7.4 and [25, pp. 53–54]. So we get the right action of the Galois group $\text{Gal}(\mathbb{Q}(E_{O}[N])/\mathbb{Q}(j(E_{O})))$ on the $\mathbb{Z}/N\mathbb{Z}$-module $E_{O}[N]$. This action gives us the faithful representation

$$\rho_{O,N} : \text{Gal}(\mathbb{Q}(E_{O}[N])/\mathbb{Q}(j(E_{O}))) \to \text{GL}_{2}(\mathbb{Z}/N\mathbb{Z}) \cong \text{Aut}(E_{O}[N])$$

with respect to the ordered basis

$$\left\{ \left[ X_{[\frac{1}{N}0]} : Y_{[\frac{1}{N}0]} : 1 \right], \left[ X_{[0\frac{1}{N}]} : Y_{[0\frac{1}{N}]} : 1 \right] \right\}$$

for $E_{O}[N]$ so that

$$[X_{v} : Y_{v} : 1]^\sigma = [X_{v\rho_{O,N}(\sigma)} : Y_{v\rho_{O,N}(\sigma)} : 1] \quad (v \in W_{N}).$$

In this section, we shall determine the image of $\rho_{O,N}$ by utilizing the Shimura reciprocity law.
If we let
\[
\min(\tau O, Q) = x^2 + b_O x + c_O \quad (\in \mathbb{Z}[x]),
\]
then we have a well-defined homomorphism of groups
\[
\mu_{O,N} : (O/NO)^* \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z})
\]
\[
[s\tau O + t] \mapsto \begin{bmatrix} t - b_O s & -c_O s \\ s & t \end{bmatrix}.
\]
Let
\[
W_{O,N} = \mu_{O,N}((O/NO)^*) \quad \text{and} \quad U_{O,N} = \mu_{O,N}(\pi_{O,N}(O^*))
\]
where \(\pi_{O,N} : O \to O/NO\) is the canonical homomorphism. Then we achieve that
\[
W_{O,N}/U_{O,N} \simeq (O/NO)^*/\pi_{O,N}(O^*) \simeq \text{Gal}(K_{O,N}/H_O)
\]
(27)
(cf. \([6, \text{Lemma 15.17}]\)).

**Proposition 8.1** (The Shimura reciprocity law). The map
\[
W_{O,N}/U_{O,N} \to \text{Gal}(K_{O,N}/H_O)
\]
\[
[\gamma] \mapsto \left( f(\tau O) \mapsto f^\gamma(\tau O) \mid f \in \mathcal{F}_N \text{ is finite at } \tau O \right)
\]
is a well-defined isomorphism. Here, \(\tilde{\gamma}\) means the image of \(\gamma\) in \(\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle \simeq \text{Gal}(\mathcal{F}_N/\mathcal{F}_1)\).

**Proof.** See \([4, \text{p. 859}]\) or \([6, \text{Theorem 15.22}]\). \(\square\)

**Lemma 8.2.** Let \(\beta \in M_2(\mathbb{Z})\) such that \(\gcd(\det(\beta), N) = 1\). If
\[
\mathbf{v}\beta \equiv \mathbf{v} \text{ or } -\mathbf{v} \pmod{M_{1,2}(\mathbb{Z})} \quad \text{for each } \mathbf{v} \in W_N,
\]
then \(\beta \equiv I_2 \text{ or } -I_2 \pmod{NM_2(\mathbb{Z})}\).

**Proof.** See \([13, \text{Lemma 6.1}]\). \(\square\)

**Theorem 8.3.** Assume that \(D_O \neq -3, -4\) and \(N \geq 2\). Let \(\hat{W}_{O,N}\) be the subgroup of \(\text{GL}_2(\mathbb{Z}/N\mathbb{Z})\) defined by
\[
\hat{W}_{O,N} = \left\langle W_{O,N}, \begin{bmatrix} 1 & b_O \\ 0 & -1 \end{bmatrix} \right\rangle.
\]

(i) The image of the Galois representation \(\rho_{O,N}\) is a subgroup of \(\hat{W}_{O,N}\) of index at most 2.

(ii) If \(-1\) is a quadratic residue modulo \(N\), then the image of \(\rho_{O,N}\) is exactly \(\hat{W}_{O,N}\).

**Proof.** (i) Let \(\sigma \in \text{Gal}(\mathbb{Q}(E_O[N])/\mathbb{Q}(j(E_O)))\) and \(\gamma = \rho_{O,N}(\sigma)\). We get by \(25\) that
\[
X_\mathbf{v}^\gamma = X_\mathbf{v} \quad (\mathbf{v} \in W_N).
\]
Recall that \(j(E_O) = j(\tau O) \in \mathbb{R}\) and \(K(j(E_O)) = H_O\) by Proposition 3.2 (i). Moreover, since \(K\) is imaginary quadratic, we have
\[
\sigma = \mu|_{\mathbb{Q}(E_O[N])} \text{ or } c|_{\mathbb{Q}(E_O[N])}\mu|_{\mathbb{Q}(E_O[N])} \quad \text{for some } \mu \in \text{Gal}(K(E_O[N])/H_O)
\]
(30)
where \( c \) is the complex conjugation on \( \mathbb{C} \). Then we see that

\[
X_v^\sigma = -\frac{1}{2^{7/3}} f_v(\tau_\sigma) \quad \text{by} \quad (21)
\]

\[
= -\frac{1}{2^{7/3}} f_{\nu\alpha}(\tau_\sigma) \quad \text{for some} \quad \alpha \in \hat{W}_{\mathcal{O},N}
\]

by (30), Propositions 4.2, 8.1 and Lemma 7.1

\[
= X_{\nu\alpha} \quad \text{again} \quad \text{by} \quad (21).
\]

And, it follows from (29) that

\[
X_{\nu\gamma} = X_{\nu\alpha} \quad (\nu \in W_N)
\]

and so

\[
\nu\gamma \equiv \nu\alpha \text{ or } -\nu\alpha \quad \text{(mod } M_{1,2}(\mathbb{Z}) \text{)} \quad (\nu \in W_N)
\]

by Lemma 3.1 (i). Thus we obtain by Lemma 8.2 that

\[
\gamma = \alpha \text{ or } -\alpha \text{ in } \text{GL}_2(\mathbb{Z}/N\mathbb{Z}).
\]

This observation asserts that the image of \( \rho_{\mathcal{O},N} \) is a subgroup of \( \hat{W}_{K,N} \). Furthermore, we find that

\[
|\rho_{\mathcal{O},N}(\text{Gal}(\mathbb{Q}(E_\mathcal{O}[N])/\mathbb{Q}(j(E_\mathcal{O}))))|
\]

\[
= [\mathbb{Q}(E_\mathcal{O}[N]) : \mathbb{Q}(j(E_\mathcal{O}))] \quad \text{since } \rho_{\mathcal{O},N} \text{ is injective}
\]

\[
= \begin{cases} 
K_{\mathcal{O},N} : H_\mathcal{O} & \text{if } N = 2 \text{ and } D_\mathcal{O} \equiv 0 \pmod{4}, \\
2[K_{\mathcal{O},N} : H_\mathcal{O}] & \text{if } N = 2 \text{ and } D_\mathcal{O} \equiv 1 \pmod{4}, \\
2[K_{\mathcal{O},N} : H_\mathcal{O}] \text{ or } 4[K_{\mathcal{O},N} : H_\mathcal{O}] & \text{if } N \geq 3
\end{cases}
\]

by Proposition 3.2 (i), the fact \( j(E_\mathcal{O}) \in \mathbb{R} \) and Theorem 7.8

\[
= |W_{\mathcal{O},N}/\{I_2, -I_2\}| \times \begin{cases} 
1 & \text{if } N = 2 \text{ and } D_\mathcal{O} \equiv 0 \pmod{4}, \\
2 & \text{if } N = 2 \text{ and } D_\mathcal{O} \equiv 1 \pmod{4}, \\
2 \text{ or } 4 & \text{if } N \geq 3
\end{cases}
\]

by Proposition 8.1 because the assumption \( D_\mathcal{O} \neq -3, -4 \) yields that \( \mathcal{O}^* = \{1, -1\} \) (cf. [6, Exercise 5.9])

\[
= |W_{\mathcal{O},N}| \times \begin{cases} 
1 & \text{if } N = 2 \text{ and } D_\mathcal{O} \equiv 0 \pmod{4}, \\
2 & \text{if } N = 2 \text{ and } D_\mathcal{O} \equiv 1 \pmod{4}, \\
1 \text{ or } 2 & \text{if } N \geq 3
\end{cases}
\]

\[
= |\hat{W}_{\mathcal{O},N}| \times \begin{cases} 
1 & \text{if } N = 2, \\
\frac{1}{2} \text{ or } 1 & \text{if } N \geq 3.
\end{cases}
\]

Hence the image of \( \rho_{\mathcal{O},N} \) is a subgroup of \( \hat{W}_{\mathcal{O},N} \) of index at most 2.

(ii) Let \( R \) be the image of \( \rho_{\mathcal{O},N} \). Suppose on the contrary that \( R \neq \hat{W}_{\mathcal{O},N} \). Then we derive by (i) and its proof that

\[
|\hat{W}_{\mathcal{O},N} : R| = 2
\]

(31)
and

\[ N \geq 3 \quad \text{and} \quad \mathbb{Q}(E_0[N]) = K_{O,N}. \]  (32)

If \( R \) contains \(-I_2\) and so

\[ -I_2 = \rho_{O,N}(\sigma) \quad \text{for some} \quad \sigma \in \text{Gal}(\mathbb{Q}(E_0[N]) / \mathbb{Q}(j(E_0))), \]  (33)

then we see that for \( v \in W_N \)

\[ X_v^\sigma = X_{v(-I_2)} \quad \text{by (25)} \]

\[ = X_v \quad \text{by Lemma \( \ref{lem:group-theory} \) (i)}. \]

This claims by Proposition \( \ref{prop:gauss-sums} \) (iii) that \( \sigma = \text{id}_{K_{O,N}} \), which contradicts (32) and (33). Thus we should have

\[ R \not\ni -I_2, \]  (34)

and hence

\[ \langle R, -I_2 \rangle = \hat{W}_{O,N} \]  (35)

by (31). Let \( t \) be an integer such that \( t^2 \equiv -1 \pmod{N} \). Since \( t + NO \in (O/NO)^* \),

\[ W_{O,N} \ni \mu_{O,N}([t]) = tI_2 \quad \text{and} \quad W_{O,N} \ni \mu_{O,N}([-t]) = -tI_2, \]  (36)

\( R \) contains at least one of \( tI_2 \) or \(-tI_2\) by (35). And it follows that

\[ R \ni (\pm tI_2)^2 = t^2I_2 = -I_2 \quad \text{in} \quad \text{GL}_2(\mathbb{Z}/N\mathbb{Z}), \]

which contradicts (34).

Therefore we conclude that if \(-1\) is a quadratic residue modulo \( N \), then the image of \( \rho_{O,N} \) is the whole of \( \hat{W}_{O,N} \).

\[ \square \]

9 An isomorphism of \( C_N(D_O) \) onto \( C_N(O) \)

By constructing a bijection between \( C_N(D_O) \) and \( C_N(O) \), we shall simultaneously prove that the binary operation on \( C_N(D_O) \) given in Definition \( \ref{def:binary-op} \) is well defined and \( C_N(D_O) \) is isomorphic to \( C_N(O) \).

**Lemma 9.1.** If \( Q = ax^2 + bxy + cy^2 \in \mathbb{Q}(D_O) \), then we have

\[ Q \in \mathbb{Q}(D_O, N) \iff [\omega_Q, 1] \in I(O, N). \]

**Proof.** Let \( a = [\omega_Q, 1] \). Observe by Lemma \( \ref{lem:gauss-sums} \) that \( aa \in M(O) \) and \( N_O(aa) = a \).

Assume that \( Q \in \mathbb{Q}(D_O, N) \). Since \( \gcd(N_O(aa), N) = \gcd(a, N) = 1 \), \( aa \) lies in \( M(O, N) \) by Lemma \( \ref{lem:ideal-prop} \). Therefore \( a = (aa)(aO)^{-1} \) belongs to \( I(O, N) \).

Conversely, assume that \( a \in I(O, N) \). Then we attain \( a = bc^{-1} \) for some \( b, c \in M(O, N) \) and so

\[ (aa)c = (aO)b. \]
Taking norm on both sides, we find that \( aN_\mathcal{O}(c) = a^2N_\mathcal{O}(b) \) by the fact \( N_\mathcal{O}(ab) = a \) and Lemma 2.4, and hence
\[
N_\mathcal{O}(c) = aN_\mathcal{O}(b).
\] (37)

Since \( \gcd(N_\mathcal{O}(c), N) = 1 \) by the fact \( c \in \mathcal{M}(\mathcal{O}, N) \) and Lemma 2.2, we achieve from (37) that \( \gcd(a, N) = 1 \). Thus \( Q \) belongs to \( \mathcal{Q}(D_\mathcal{O}, N) \).

\[ \text{Lemma 9.2.} \] The set \( P_N(\mathcal{O}) \) coincides with
\[
P = \left\{ \frac{\nu_1}{\nu_2} \mathcal{O} \mid \nu_1, \nu_2 \in \mathcal{O} \setminus \{0\} \text{ satisfy } \nu_1\mathcal{O}, \nu_2\mathcal{O} \in \mathcal{P}(\mathcal{O}, N) \text{ and } \nu_1 \equiv \nu_2 \pmod{N\mathcal{O}} \right\}.
\]

\[ \text{Proof.} \] By the definition (11) of \( P_N(\mathcal{O}) \), we deduce the inclusion \( P_N(\mathcal{O}) \subseteq P \).

Now, let \( a \in P \) and so
\[
a = \frac{\nu_1}{\nu_2} \mathcal{O} \quad \text{for some } \nu_1, \nu_2 \in \mathcal{O} \setminus \{0\} \text{ such that } \begin{cases} \nu_1\mathcal{O}, \nu_2\mathcal{O} \in \mathcal{P}(\mathcal{O}, N), \\ \nu_1 \equiv \nu_2 \pmod{N\mathcal{O}}. \end{cases}
\]

Since \( \nu_i\mathcal{O} \ (i = 1, 2) \) is prime to \( N \), that is, \( \nu_i\mathcal{O} + N\mathcal{O} = \mathcal{O} \), the coset \( \nu_i + N\mathcal{O} \) in the quotient ring \( \mathcal{O}/N\mathcal{O} \) is a unit. If we let \( m \) be the order of the unit group \( (\mathcal{O}/N\mathcal{O})^\times \), then we get from the fact \( \nu_1 \equiv \nu_2 \pmod{N\mathcal{O}} \) that
\[
\nu_1\nu_2^{m-1} \equiv \nu_2^m \equiv 1 \pmod{N\mathcal{O}}.
\]

And we obtain that
\[
a = \frac{\nu_1}{\nu_2} \mathcal{O} = (\nu_1\nu_2^{m-1}\mathcal{O})(\nu_2^m\mathcal{O})^{-1} \in P_N(\mathcal{O}),
\]
which proves the converse inclusion \( P \subseteq P_N(\mathcal{O}) \). Therefore we conclude that \( P_N(\mathcal{O}) = P \).

\[ \text{Proposition 9.3.} \] The map
\[
\phi_{\mathcal{O}, N} : \mathcal{C}_N(D_\mathcal{O}) \to \mathcal{C}_N(\mathcal{O})
\]
\[
[Q] \mapsto [\omega_Q, 1]
\]
is a well-defined bijection.

\[ \text{Proof.} \] First, we shall show that \( \phi_{\mathcal{O}, N} \) is well defined. Let \( Q = ax^2 + bxy + cy^2 \in \mathcal{Q}(D_\mathcal{O}, N) \) and \( \gamma \in \Gamma_1(N) \) with \( \gamma^{-1} = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \) (\( \in \Gamma_1(N) \)). Then we see that
\[
[\omega_{Q^\gamma}, 1] = [\gamma^{-1}(\omega_Q), 1] = \frac{1}{j(\gamma^{-1}, \omega_Q)}[\omega_Q, 1].
\] (38)

Since \( \gcd(a, N) = 1 \), we have
\[
a^{\varphi(N)} \equiv 1 \pmod{N}
\] (39)
where \( \varphi \) is the Euler totient function. Furthermore, since
\[
b^2 - 4ac = D_\mathcal{O} = b_\mathcal{O}^2 - 4c_\mathcal{O},
\]

24
and so achieve Proposition 5.6 (ii) and Lemmas 2.11, 5.5, 9.1, we derive that for some $Q$ because $r \equiv 0$, $s \equiv 1 \pmod{N}$. Hence we obtain by \[35\], \[39\] and \[10\] that

$$[[\omega_Q, 1]] = [[\omega_Q, 1]] \in \mathcal{C}_N(O),$$

which shows that $\phi_{O, N}$ is well defined.

Second, we shall prove that $\phi_{O, N}$ is surjective. Let $h$ be the order of the group $\mathcal{C}(O, N)$. By Proposition 5.6 (ii) and Lemmas 2.11, 5.5, 9.1 we derive that

$$\mathcal{C}(O, N) = I(O, N)/P(O, N) = \{[\omega_{Q_1}, 1]P(O, N), \ldots, [\omega_{Q_h}, 1]P(O, N)\}$$

for some $Q_i = a_i x^2 + b_i xy + c_i y^2 \in \mathcal{Q}(D_O, N)$ ($i = 1, 2, \ldots, h$). Thus we deduce the decomposition

$$\mathcal{C}_N(O) = I(O, N)/P_N(O) = (P(O, N)/P_N(O)) \cdot \{[\omega_{Q_i}, 1]P_N(O) \mid i = 1, 2, \ldots, h\}.$$ 

Now, let $C \in \mathcal{C}_N(O)$. By the above decomposition, we have

$$C = C' \cdot [\omega_{Q_i}, 1]P_N(O) \quad \text{for some } C' \in P(O, N)/P_N(O) \text{ and } 1 \leq i \leq h.$$

And one can take an $O$-ideal $\mathfrak{d}$ in $C'^{-1} \cap \mathcal{M}(O, N)$ by Remark 2.15. Since $O = [a_i, \omega_{Q_i}, 1]$, we achieve

$$\mathfrak{d} = (ka_i \omega_{Q_i} + v)O \quad \text{for some } k, v \in \mathbb{Z}$$

and so

$$C = \left[ \frac{1}{u \omega_{Q_i} + v} [\omega_{Q_i}, 1] \right] \quad \text{with } u = ka_i. \quad (41)$$

Since $\gcd(u, v, N) = 1$ by the facts $\mathfrak{d} \in \mathcal{M}(O, N)$ and $\gcd(a_i, N) = 1$, we can take a matrix $\sigma = \begin{bmatrix} * & * \\ \tilde{u} & \tilde{v} \end{bmatrix} \in SL_2(\mathbb{Z})$ such that $\tilde{u} \equiv u \pmod{N}$, $\tilde{v} \equiv v \pmod{N}$. Then we see that

$$\frac{u \omega_{Q_i} + v}{u \omega_{Q_i} + v} O = \frac{u(a_i \omega_{Q_i}) + a_i v}{u(a_i \omega_{Q_i}) + a_i v} O \in P_N(O) \quad (42)$$

by the fact $a_i \omega_{Q_i} \in O$ and Lemma 9.2. And we establish that

$$C = \left[ \frac{u \omega_{Q_i} + v}{u \omega_{Q_i} + v} \right] C \quad \text{by } (12)$$

$$= \left[ \frac{1}{j(\sigma, \omega_{Q_i})} [\omega_{Q_i}, 1] \right] \quad \text{by } (11)$$

$$= [[\sigma(\omega_{Q_i}), 1]]$$

$$= [[\omega_{Q_i}^{-1}, 1]].$$

Thus, if we let $Q = Q_i^{-1}$, then we get by Lemma 9.1 that

$$Q \in \mathcal{Q}(D_O, N) \quad \text{and} \quad \phi_{O, N}([Q]) = C.$$
This proves that $\phi_{\mathcal{O}, N}$ is surjective.

Third, we shall show that $\phi_{\mathcal{O}, N}$ is injective. Suppose that

$$\phi_{\mathcal{O}, N}([Q_1]) = \phi_{\mathcal{O}, N}([Q_2])$$

for some $Q_i = a_i x^2 + b_i xy + c_i y^2 \in \mathcal{O}(D, N) \ (i = 1, 2)$

Then we have

$$[\omega Q_1, 1] = \frac{\nu_1}{\nu_2} [\omega Q_2, 1]$$

for some $\nu_1, \nu_2 \in \mathcal{O} \setminus \{0\}$ such that $\nu_1 \equiv \nu_2 \equiv 1 \pmod{N\mathcal{O}}$, (43)

which implies by Proposition 5.6 (ii) that

$$Q_1 = Q_2^\gamma$$

for some $\gamma \in \text{SL}_2(\mathbb{Z})$.

And it follows from (43) that

$$[\omega Q_1, 1] = \frac{\nu_1}{\nu_2} [\gamma(\omega Q_1), 1] = \frac{\nu_1}{\nu_2} \cdot \frac{1}{j} [\omega Q_1, 1]$$

where $j = j(\gamma, \omega Q_1)$,

and hence

$$\zeta := \frac{\nu_1}{\nu_2} \cdot \frac{1}{j} \in \mathcal{O}^*.$$ (44)

Now, since $[\omega Q_1, 1] = \zeta j [\omega Q_2, 1]$ by (43) and $\omega Q_1, \omega Q_2 \in \mathbb{H}$, there is a matrix $\alpha = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ in $\text{SL}_2(\mathbb{Z})$ so that

$$\begin{bmatrix} \zeta j \omega Q_2 \\ \zeta j \end{bmatrix} = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} \omega Q_1 \\ 1 \end{bmatrix}.$$ (45)

We then find by (46) that

$$\omega Q_2 = \frac{\zeta j \omega Q_2}{\zeta j} = \frac{p \omega Q_1 + q}{r \omega Q_1 + s} = \alpha(\omega Q_1),$$

which gives

$$Q_1 = Q_2^\alpha.$$ (46)

We get again by (43) and the fact $\nu_2 \equiv 1 \pmod{N\mathcal{O}}$ that

$$a_1 \nu_2(\zeta j) \equiv a_1(r \omega Q_1 + s) \equiv r(a_1 \omega Q_1) + a_1 s \pmod{N\mathcal{O}}.$$ (47)

On the other hand, we see by (43) and the fact $\nu_1 \equiv 1 \pmod{N\mathcal{O}}$ that

$$a_1 \nu_2(\zeta j) = a_1 \nu_1 \equiv a_1 \pmod{N\mathcal{O}}.$$ (48)

Thus we obtain by (17) and (48) that

$$r(a_1 \omega Q_1) + a_1 s \equiv a_1 \pmod{N\mathcal{O}},$$

from which it follows that

$$r(a_1 \omega Q_1) + a_1(s - 1) \equiv 0 \pmod{N\mathcal{O}}.$$ (49)

Since $N\mathcal{O} = [N(a_1 \omega Q_1), N]$ and $\gcd(a_1, N) = 1$, (49) implies that $r \equiv 0, s \equiv 1 \pmod{N}$ and hence $\alpha \in \Gamma_1(N)$. Therefore we achieve by (46) that

$$[Q_1] = [Q_2] \quad \text{in} \quad \mathcal{C}_N(D),$$

which proves the injectivity of $\phi_{\mathcal{O}, N}$. □
Theorem 9.4. The form class group $C_N(D_O)$ is isomorphic to the ideal class group $C_N(O)$.

Proof. Let $\phi_{O,N} : C_N(D_O) \rightarrow C_N(O)$ be the bijection given in Proposition 9.3. Let $C, C' \in C_N(D_O)$ and so $C = [Q], C' = [Q']$ for some $Q = ax^2 + bxy + cy^2, Q' = a'x^2 + b'xy + c'y^2 \in \mathcal{O}(D_O, N)$, respectively. By Lemma 5.5, we see that there is a matrix $\gamma$ in $SL_2(\mathbb{Z})$ such that $Q'' = Q'' = a''x^2 + b''xy + c''y^2$ satisfies gcd($a, a'', (b + b'')/2 = 1$. We then find that

$$\phi_{O,N}(C)\phi_{O,N}(C') = [[\omega, 1][\omega', 1]]$$

$$= [\gamma(\omega Q), 1]$$

$$= \begin{pmatrix} 1/j \omega, 1 \end{pmatrix} \begin{pmatrix} 1/j \omega Q', 1 \end{pmatrix} \text{ with } j = j(\gamma, \omega Q')$$

$$= \begin{pmatrix} 1/j \omega Q''', 1 \end{pmatrix}$$

where $Q'''$ is a Dirichlet composition of $Q$ and $Q''$. By Lemma 5.6

$$= [[\nu_1, \nu_2]] \text{ where } \nu_1 = \frac{\omega Q'''}{j} \text{ and } \nu_2 = \frac{1}{j}.$$ 

Since $[\omega, 1][\omega Q', 1] = [\nu_1, \nu_2]$ contains 1, we derive

$$uv_1 + v\nu_2 = 1 \text{ for some unique } (u, v) \in \mathbb{Z}^2. \quad (50)$$

Furthermore, since

$$aa'[\nu_1, \nu_2] = (a[\omega Q, 1])(a'[\omega Q', 1]) \in M(O, N) \quad (51)$$

by Lemmas 2.2, 5.2 and the fact gcd($N, a) = \text{gcd}(N, a') = 1$, we must have gcd($N, u, v) = 1$. Since the reduction $SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}/NM_2(\mathbb{Z}))$ is surjective (Lemma 1.38), there exists a matrix

$$\sigma = \begin{pmatrix} * & * \\ u' & v' \end{pmatrix} \in SL_2(\mathbb{Z})$$

such that

$$\sigma \equiv \begin{pmatrix} * & * \\ u & v \end{pmatrix} \text{ (mod } NM_2(\mathbb{Z})). \quad (52)$$

If we let $Q''' = Q''\sigma^{-1}$, then we find by the fact $\nu_1/\nu_2 = \omega Q'''$ that

$$[\omega Q''', 1] = [\sigma(\omega Q'''), 1] = \frac{1}{j(\sigma, \omega Q''')} \omega Q''', 1] = \frac{aa'}{u'(aa'\nu_1) + v'(aa'\nu_2)}[\nu_1, \nu_2]. \quad (53)$$

Thus we establish that

$$\{u'(aa'\nu_1) + v'(aa'\nu_2)\} - aa' = \{u'(aa'\nu_1) + v'(aa'\nu_2)\} - aa'(u

\nu_1 + v\nu_2) \quad \text{by } (51)$$

$$= (u' - u)(aa'\nu_1) + (v' - v)(aa'\nu_2)$$

$$\in N(aa'\nu_1, \nu_2) \quad \text{by } (52)$$

$$\subseteq N(O) \quad \text{by } (51),$$

and hence

$$nu'(aa'\nu_1) + v'(aa'\nu_2) \equiv aa' \text{ (mod } N(O)).$$
And we attain by (53) and Lemma 9.2 that
\[ \phi_{O,N}([Q''']) = [\omega_{Q'''], 1]] = [[\nu_1, \nu_2]] = \phi_{O,N}(C)\phi_{O,N}(C'). \]
Therefore the binary operation on \( \mathcal{C}_N(D_O) \) given in Definition 5.7 is well defined, which makes \( \mathcal{C}_N(D_O) \) a group isomorphic to \( \mathcal{C}_N(O) \) via the isomorphism \( \phi_{O,N} \).

10 The Shimura reciprocity law

We shall briefly review the original version of Shimura’s reciprocity law in order to prepare for \( \S 11 \).

Let \( \hat{Z} = \prod_{p: \text{primes}} Z_p \) and \( \hat{Q} = Q \otimes_{\mathbb{Z}} \hat{Z} \). Note that
\[ \text{GL}_2(\hat{Q}) = \left\{ \gamma = (\gamma_p)_p \in \prod_p \text{GL}_2(\mathbb{Q}_p) \mid \gamma_p \in \text{GL}_2(\mathbb{Z}_p) \text{ for all but finitely many } p \right\} \]
(\[6, \text{Exercise } 15.6\]). Let \( \mathcal{F} \) be the field of all meromorphic modular functions, namely,
\[ \mathcal{F} = \bigcup_{N=1}^{\infty} \mathcal{F}_N. \]

**Proposition 10.1.** There is a surjective homomorphism
\[ \sigma_{\mathcal{F}} : \text{GL}_2(\hat{Q}) \to \text{Aut}(\mathcal{F}) \]
described as follows: Let \( \gamma \in \text{GL}_2(\hat{Q}) \) and \( f \in \mathcal{F}_N \) for some positive integer \( N \). One can decompose \( \gamma \) as
\[ \gamma = \alpha \beta \quad \text{for some } \alpha = (\alpha_p)_p \in \text{GL}_2(\hat{Z}) \text{ and } \beta \in \text{GL}_2^+(\mathbb{Q}) \]
(\[15, \text{Theorem } 1 \text{ in Chapter } 7\]). By using the Chinese remainder theorem, take a matrix \( A \) in \( M_2(\mathbb{Z}) \) such that \( A \equiv \alpha_p \pmod{NM_2(\mathbb{Z}_p)} \) for all primes \( p \) dividing \( N \). Then we have
\[ f^{\sigma_{\mathcal{F}}(\gamma)} = f^A \circ \beta \]
where \( A \) is the image of \( A \) in \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle \) (\( \simeq \text{Gal}(\mathcal{F}_N/\mathcal{F}_1) \)) and \( \beta \) is regarded as a fractional linear transformation on \( \mathbb{H} \).

**Proof.** See [15, Theorem 6 in Chapter 7] or [21, Theorem 6.23]. \( \square \)

**Remark 10.2.** The kernel of \( \sigma_{\mathcal{F}} \) is the image of \( \mathbb{Q}^* \) through the diagonal embedding into \( \text{GL}_2(\hat{Q}) \).

Let \( \omega \in K \cap \mathbb{H} \). We define the normalized embedding
\[ q_\omega : K^* \to \text{GL}_2^+(\mathbb{Q}) \]
by the relation
\[ \nu \begin{bmatrix} \omega \\ 1 \end{bmatrix} = q_\omega(\nu) \begin{bmatrix} \omega \\ 1 \end{bmatrix} \ (\nu \in K^*). \]

For each prime \( p \), we can continuously extend \( q_\omega \) to the embedding
\[ q_\omega, p : (K \otimes \mathbb{Z}_p)^* \to \text{GL}_2(\mathbb{Q}_p), \]
and hence to the embedding
\[ q_\omega : \hat{K}^* \to \text{GL}_2(\hat{\mathbb{Q}}) \]
where \( \hat{K} = K \otimes \hat{\mathbb{Z}} \). Let \( K^{ab} \) be the maximal abelian extension of \( K \), and denote by
\[ [\cdot, K] : \hat{K}^* \to \text{Gal}(K^{ab}/K) \]
the Artin map for \( K \) defined on the group \( \hat{K}^* \) of finite \( K \)-ideles. By using his theory of canonical models for modular curves, Shimura established the following reciprocity law.

**Proposition 10.3.** Let \( \omega \in K \cap \mathbb{H} \) and \( f \in F \). If \( f \) is finite at \( \omega \), then \( f(\omega) \) belongs to \( K^{ab} \) and satisfies
\[ f(\omega)^{[s^{-1}, K]} = f^{\sigma_f(q_\omega(s))}(\omega) \ (s \in \hat{K}^*). \]

**Proof.** See [21, 6.31].

## 11 Ray class invariants for orders

We shall define invariants for each class in \( C_N(O) \) in terms of special values of modular functions, and examine their Galois conjugates via the Artin map.

**Definition 11.1.** Let \( C \in C_N(O) \). For each \( f \in F_N \), we define the invariant \( f(C) \) as follows:

One can take an \( O \)-ideal \( \mathfrak{c} \in C \cap M(O, N) \) by Remark 2.15. Observe that \( \gcd(N_\mathfrak{c}(\mathfrak{c}), N) = 1 \) by Lemma 2.2. Choose a \( \mathbb{Z} \)-basis \( \{\xi_1, \xi_2\} \) of \( \mathfrak{c}^{-1} \) so that
\[ \xi := \frac{\xi_1}{\xi_2} \in \mathbb{H}. \]

Since \( [\tau_\mathfrak{c}, 1] = \mathfrak{c} \subseteq \mathfrak{c}^{-1} = [\xi_1, \xi_2] \) and \( \tau_\mathfrak{c}, \xi \in \mathbb{H} \), we have
\[ \begin{bmatrix} \tau_\mathfrak{c} \\ 1 \end{bmatrix} = A \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \text{ for some } A \in M_2(\mathbb{Z}) \cap \text{GL}_2^+(\mathbb{Q}). \quad (54) \]

On the other hand, we get by Lemma 2.1 (iii) that
\[ [\tau_\mathfrak{c}, 1] = \mathfrak{c} \supseteq \tau = N_{\mathfrak{c}}(\mathfrak{c})^c_\mathfrak{c} = [N_\mathfrak{c}(\mathfrak{c})\xi_1, N_\mathfrak{c}(\mathfrak{c})\xi_2] \]
and so
\[ \begin{bmatrix} N_\mathfrak{c}(\mathfrak{c})\xi_1 \\ N_\mathfrak{c}(\mathfrak{c})\xi_2 \end{bmatrix} = B \begin{bmatrix} \tau_\mathfrak{c} \\ 1 \end{bmatrix} \text{ for some } B \in M_2(\mathbb{Z}) \cap \text{GL}_2^+(\mathbb{Q}). \quad (55) \]
Thus we obtain by (54) and (55) that
\[ AB \begin{bmatrix} \tau O & \tau O \\ 1 & 1 \end{bmatrix} = N_O(c) \begin{bmatrix} \tau O & \tau O \\ 1 & 1 \end{bmatrix}. \]
By taking determinant and squaring, we attain
\[ \det(A)^2 \det(B)^2 D_O = N_O(c)^4 D_O, \]
which shows that \( \gcd(\det(A), N) = 1 \). We then define
\[ f(C) = f(\tilde{A}(\xi)) \]
where \( \tilde{A} \) is the image of \( A \) in \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle \), if \( f(\tilde{A}) \) is finite at \( \xi \).

**Lemma 11.2.** Let \( a, b \in M(O) \). If \( a + b = O \), then \( a \cap b \subseteq ab \).

**Proof.** Since \( a + b = O \), we deduce
\[ 1 = a + b \quad \text{for some } a \in a \text{ and } b \in b. \] (56)
Let \( c \in a \cap b \). Then we see that
\[ c = c(a + b) \quad \text{by (56)} \]
\[ = ac + cb \]
\[ \in ab \quad \text{since } a \in a, c \in b \text{ and } c \in a, b \in b. \]
This proves that \( a \cap b \subseteq ab \).

**Lemma 11.3.** Let \( C \in C_N(O) \) and \( f \in F_N \). The value \( f(C) \) in Definition 11.1 if it is finite, does not depend on the choice of \( c \) and \( \{\xi_1, \xi_2\} \).

**Proof.** We follow the notation of Definition 11.1. Let \( c' \in C \cap M(O, N) \), and let \( \{\xi'_1, \xi'_2\} \) be a \( \mathbb{Z} \)-basis of \( c'^{-1} \) so that
\[ \xi' := \xi'_1 \xi'_2 \in \mathbb{H}. \]
Let \( A' \) be the matrix in \( M_2(\mathbb{Z}) \cap \text{GL}_2^+(\mathbb{Q}) \) such that
\[ \begin{bmatrix} \tau O \\ 1 \end{bmatrix} = A' \begin{bmatrix} \xi'_1 \\ \xi'_2 \end{bmatrix}. \] (57)
Since \( C = [c] = [c'] \), we have
\[ c' = \frac{\nu_1}{\nu_2} c \] (58)
for some \( \nu_1, \nu_2 \in O \setminus \{0\} \) satisfying
\[ \nu_1 \equiv \nu_2 \equiv 1 \pmod{NO}. \] (59)
If we let \( \nu = \frac{\nu_1}{\nu_2} \) then we get by (58) that
\[ [\xi'_1, \xi'_2] = c'^{-1} = \nu^{-1} c^{-1} = [\nu^{-1} \xi_1, \nu^{-1} \xi_2], \]
and hence
\[
\begin{bmatrix}
ξ'_1 \\
ξ'_2
\end{bmatrix} = B \begin{bmatrix}
ν^{-1}ξ_1 \\
ν^{-1}ξ_2
\end{bmatrix} = ν^{-1}B \begin{bmatrix}
ξ_1 \\
ξ_2
\end{bmatrix}
\] for some \( B \in \text{SL}_2(\mathbb{Z}) \).

(60)

Note that
\[
(ν_1 - ν_2)ξ \subseteq NO \cap (ν_1 - ν_2)ξ \quad \text{by (59)}
\]
\[
\subseteq NO \cap (ν_1ν_1 + ν_2ν_2)ξ \quad \text{by (58)}
\]
\[
\subseteq NO \cap ν_2O \quad \text{by Lemma 11.2 because } ν_2O \text{ is prime to } N \text{ owing to (59)}
\]
and so
\[
[(ν - 1)τO, (ν - 1)] = (ν - 1)O \subseteq Nξ^{-1} = [Nξ_1, Nξ_2].
\]
Thus we obtain that
\[
\begin{bmatrix}
(ν - 1)τO \\
ν - 1
\end{bmatrix} = A'' \begin{bmatrix}
Nξ_1 \\
Nξ_2
\end{bmatrix}
\] for some \( A'' \in M_2(\mathbb{Z}) \cap \text{GL}_2^+(\mathbb{Q}) \).

(61)

And we find that
\[
NA'' \begin{bmatrix}
ξ_1 \\
ξ_2
\end{bmatrix} = ν \begin{bmatrix}
τO \\
1
\end{bmatrix} - \begin{bmatrix}
τO \\
1
\end{bmatrix} \quad \text{by (61)}
\]
\[
= νA' \begin{bmatrix}
ξ'_1 \\
ξ'_2
\end{bmatrix} - A \begin{bmatrix}
ξ_1 \\
ξ_2
\end{bmatrix} \quad \text{by (54) and (57)}
\]
\[
= (A'B - A) \begin{bmatrix}
ξ_1 \\
ξ_2
\end{bmatrix} \quad \text{by (60)}.
\]
It then follows that
\[
NA'' \begin{bmatrix}
ξ_1 \\
ξ_2
\end{bmatrix} = (A'B - A) \begin{bmatrix}
ξ_1 \\
ξ_2
\end{bmatrix},
\]
and hence \( NA'' = A'B - A \) and
\[
A' \equiv AB^{-1} \pmod{NM_2(\mathbb{Z})}.
\]

(62)

Finally we derive that
\[
f^A(ξ) = f^A(B^{-1}B(ξ))
\]
\[
= f^{AB^{-1}}(B(ξ)) \quad \text{by Proposition 4.1}
\]
\[
= f^{AB^{-1}}(ξ') \quad \text{by (60)}
\]
\[
= f^A(ξ') \quad \text{by (62)},
\]
which proves the well-definedness of the invariant \( f(C) \).

By composing three isomorphisms

\[ \hfill \]
(i) \( C_N(\mathcal{O}) \sim C_N(\mathcal{O}, \ell_{\mathcal{O}N}) \) achieved from Proposition 2.13.

(ii) \( C_N(\mathcal{O}, \ell_{\mathcal{O}N}) \sim I(\mathcal{O}_K, \ell_{\mathcal{O}N})/P_{Z_N}(\mathcal{O}_K, \ell_{\mathcal{O}N}) \) established in Proposition 2.8.

(iii) the Artin map \( I(\mathcal{O}_K, \ell_{\mathcal{O}N})/P_{Z_N}(\mathcal{O}_K, \ell_{\mathcal{O}N}) \sim \text{Gal}(K_{\mathcal{O},N}/K) \),

we get the isomorphism

\[ \sigma_{\mathcal{O},N} : C_N(\mathcal{O}) \sim \text{Gal}(K_{\mathcal{O},N}/K). \]

Let \( C_0 \) denote the identity class in \( C_N(\mathcal{O}) \).

**Theorem 11.4.** Let \( C \in C_N(\mathcal{O}) \) and \( f \in F_N \). If \( f \) is finite at \( \tau_{\mathcal{O}} \), then \( f(C) \) belongs to \( K_{\mathcal{O},N} \) and satisfies

\[ f(C)\sigma_{\mathcal{O},N}(C') = f(CC') \quad (C' \in C_N(\mathcal{O})). \]

**Proof.** By Definition 11.1, Lemma 11.3 and (3), we attain

\[ f(C_0) = f(\tau_{\mathcal{O}}) \in K_{\mathcal{O},N}. \] (63)

And one can take \( c \in C \cap M(\mathcal{O}, \ell_{\mathcal{O}N}) \) by Remark 2.15. Let \( \{\xi_1, \xi_2\} \) be a \( \mathbb{Z} \)-basis of \( c^{-1} \) such that

\[ \xi := \frac{\xi_1}{\xi_2} \in \mathbb{H}. \]

Furthermore, let \( A \) be the matrix in \( M_2(\mathbb{Z}) \cap \text{GL}_2^+(\mathbb{Q}) \) satisfying

\[ \begin{bmatrix} \tau_{\mathcal{O}} \\ 1 \end{bmatrix} = A \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix}. \] (64)

Take an idele \( s = (s_p)_{p \text{ primes in } \hat{K}^* = (K \otimes \hat{\mathbb{Z}})^*} \) such that

\[ \begin{cases} s_p = 1 & \text{if } p | \ell_{\mathcal{O}N}, \\ s_p(\mathcal{O}_K \otimes \mathbb{Z}_p) = c\mathcal{O}_K \otimes \mathbb{Z}_p & \text{if } p \not| \ell_{\mathcal{O}N}. \end{cases} \] (65)

If \( p | \ell_{\mathcal{O}N} \), then we see that

\[ s_p(\mathcal{O} \otimes \mathbb{Z}_p) = \mathcal{O} \otimes \mathbb{Z}_p \quad \text{since } s_p = 1 \]

\[ \supseteq c \otimes \mathbb{Z}_p \]

\[ \supseteq N_{\mathcal{O}}(c)\mathcal{O} \otimes \mathbb{Z}_p \quad \text{by Lemma 2.1 (iii)} \]

\[ = \mathcal{O} \otimes \mathbb{Z}_p \quad \text{by the fact } c \in M(\mathcal{O}, \ell_{\mathcal{O}N}) \text{ and Lemma 2.2} \]

and hence

\[ s_p(\mathcal{O} \otimes \mathbb{Z}_p) = c \otimes \mathbb{Z}_p \quad (\text{if } p | \ell_{\mathcal{O}N}). \] (66)

If \( p \not| \ell_{\mathcal{O}N} \), then \( \ell_{\mathcal{O}} \) is a unit in \( \mathbb{Z}_p \) and so

\[ s_p(\mathcal{O} \otimes \mathbb{Z}_p) = s_p(\mathcal{O}_K \otimes \mathbb{Z}_p) = c\mathcal{O}_K \otimes \mathbb{Z}_p = c\mathcal{O} \otimes \mathbb{Z}_p = c \otimes \mathbb{Z}_p \quad (\text{if } p \not| \ell_{\mathcal{O}N}). \] (67)

Then it follows from (66) and (67) that

\[ s_p^{-1}(\mathcal{O} \otimes \mathbb{Z}_p) = c^{-1} \otimes \mathbb{Z}_p \quad \text{for every prime } p. \] (68)

32
Since
\[ s_p^{-1} \begin{bmatrix} \tau_0 \\ 1 \end{bmatrix} = q_{\tau_0, p}(s_p^{-1}) \begin{bmatrix} \tau_0 \\ 1 \end{bmatrix} = q_{\tau_0, p}(s_p^{-1}) A \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \]
by (64), we deduce by (68) and the fact \( c^{-1} = [\xi_1, \xi_2] \) that
\[ q_{\tau_0, p}(s_p^{-1}) A \in \text{GL}_2(\mathbb{Z}_p), \]
and so
\[ q_{\tau_0}(s^{-1}) A \in \text{GL}_2(\hat{\mathbb{Z}}). \] (69)

We then find that
\[
f(C_0)_{\sigma_0, N(C)} = f(C_0)_{\sigma_0, N([q])}
= f(\tau_0)^{[s, K]} \text{ by (63) and (65)}
= f_{\sigma_0}(q_{\tau_0}(s^{-1}))_{\tau_0} \text{ by Proposition 10.3}
= f_{\sigma_0}(q_{\tau_0}(s^{-1}) A A^{-1})_{\tau_0} \text{ by Proposition 10.1 because } A^{-1} \in \text{GL}_2^+(\mathbb{Q})
= f_{\sigma_0}(q_{\tau_0}(s^{-1}) A)_{\xi} \text{ by (64)}
= f_{G}(\xi) \text{ where } G \text{ is a matrix in } M_2(\mathbb{Z}) \text{ such that }
G \equiv q_{\tau_0, p}(s_p^{-1}) A \text{ (mod } NM_2(\mathbb{Z}_p)) \text{ for all primes } p \text{ dividing } N,
\text{ by (69) and Proposition 10.1}
= f_{A}(\xi) \text{ since the fact } s_p = 1 \text{ for all primes } p \text{ dividing } N \text{ implies }
G \equiv A \text{ (mod } NM_2(\mathbb{Z}))
= f(C).
\]

This proves that \( f(C) \) is finite and belongs to \( K_{\mathcal{O}, N} \). And we further derive that for \( C' \in \mathcal{C}_N(\mathcal{O}) \)
\[
f(C)_{\sigma_0, N(C')} = (f(C_0)_{\sigma_0, N(C)})_{\sigma_0, N(C')} = f(C_0)_{\sigma_0, N(CC')} = f(CC').
\]

\[\square\]

12 An isomorphism of \( \mathcal{C}_N(D_{\mathcal{O}}) \) onto \( \text{Gal}(K_{\mathcal{O}, N}/K) \)

In this section, we shall explicitly describe the isomorphism
\[ \sigma_{\mathcal{O}, N} \circ \phi_{\mathcal{O}, N} : \mathcal{C}_N(D_{\mathcal{O}}) \xrightarrow{\sim} \text{Gal}(K_{\mathcal{O}, N}/K). \]

Furthermore, we shall show that there exists a form class group associated with the principal congruence subgroup \( \Gamma(N) \).

**Definition 12.1.** Let \( Q \in \mathcal{Q}(D_{\mathcal{O}}, N) \) and \( f \in \mathcal{F}_N \). If \( f \) is finite at \( \tau_0 \), then we define
\[ f([Q]) = f(\phi_{\mathcal{O}, N}([Q])). \]
Lemma 12.2. Let $Q = ax^2 + bxy + cy^2 \in Q(D_O, N)$ and $f \in \mathcal{F}_N$ which is finite at $\tau_O$. Then we have

$$f([Q]) = f\left[1 - \frac{a'(b + b_O)/2}{a'}\right](-\omega_Q)$$

where $a'$ is an integer satisfying $aa' \equiv 1 \pmod{N}$.

Proof. Let $C = \phi_O,N([Q]) = [\omega_Q, 1]$. We see by the facts $\gcd(a, N) = 1$, $a \varphi(N) \equiv 1 \pmod{N}$ and Lemma 5.2 that

$c := a \varphi(N)[\omega_Q, 1] = a \varphi(N)^{-1}(a[\omega_Q, 1]) \in C \cap M(O, N)$.

Now, we find that

$$c^{-1} = a^{-\varphi(N)+1}b^{-1} \quad \text{where } b = a[\omega_Q, 1] (\in M(O, N))$$

$$= a^{-\varphi(N)+1}N_O(b)^{-1}\bar{b} \quad \text{by Lemma 2.1 (iii)}$$

$$= a^{-\varphi(N)+1}a^{-1}(a[\omega_Q, 1]) \quad \text{by Lemma 5.2}$$

$$= a^{-\varphi(N)+1}[-\omega_Q, 1].$$

Thus, if we take

$$\xi_1 = -a^{-\varphi(N)+1}\omega_Q \quad \text{and} \quad \xi_2 = a^{-\varphi(N)+1},$$

then we achieve

$c^{-1} = [\xi_1, \xi_2] \quad \text{and} \quad \xi := \frac{\xi_1}{\xi_2} = -\omega_Q \in \mathbb{H}.$

Furthermore, since

$$-\omega_Q = \frac{1}{a} \left(\tau_O + \frac{b + b_O}{2}\right),$$

we obtain that

$$\begin{bmatrix} \tau_O \\ 1 \end{bmatrix} = A \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \quad \text{with} \quad A = \begin{bmatrix} a \varphi(N) & -a \varphi(N)^{-1}(b + b_O)/2 \\ 0 & a \varphi(N)^{-1} \end{bmatrix}.$$

Since

$$A \equiv \begin{bmatrix} 1 & -a'(b + b_O)/2 \\ 0 & a' \end{bmatrix} \pmod{NM_2(\mathbb{Z})},$$

we conclude by Definition 11.1 and Lemma 11.3 that

$$f([Q]) = f(C) = f\left[1 - \frac{a'(b + b_O)/2}{a'}\right](-\omega_Q).$$

Theorem 12.3. The map

$$C_N(D_O) \to \text{Gal}(K_O.N/K)$$

$$[Q] = [ax^2 + bxy + cy^2] \mapsto \left( f(\tau_O) \mapsto f\left[1 - \frac{a'(b + b_O)/2}{a'}\right](-\omega_Q) \right) \quad f \in \mathcal{F}_N \text{ is finite at } \tau_O$$

is a well-defined isomorphism, where $a'$ is an integer which holds $aa' \equiv 1 \pmod{N}$. 

\[\square\]
Then we find that \( N \) is bijective because
\[
\phi_{O,N} : C_N(D_O) \overset{\sim}{\to} \text{Gal}(K_{O,N}/K).
\]

Let \( Q = ax^2 + bxy + cy^2 \in Q(D_O, N) \) and \( f \in F_N \) which is finite at \( \tau_O \). If we let \( C = \phi_{O,N}(Q) \), then we find that
\[
f(\tau_O)^{\psi_{O,N}(Q)} = f(C_0)^{\sigma_{O,N}(C)} \quad \text{by (63)}
\]
\[
= f(C) \quad \text{by Theorem 11.4}
\]
\[
= f(Q) \quad \text{by Definition 12.1}
\]
\[
= f\left[1 - a'(b + b\phi)/2\right](-\overrightarrow{Q}) \quad \text{where } a' \text{ is an integer satisfying } aa' \equiv 1 \pmod{N},
\]
by Lemma 12.2.

And, the result follows from (3).

Fix a positive transcendental number \( t \). Then the extension \( K_{O,N}(\sqrt[t]{1})/K(t) \) is Galois because \( K_{O,N} \) contains \( \zeta_N \) by (3). Since the polynomial \( x^N - t \) in \( x \) is irreducible over \( K_{O,N}(t) \), we establish the isomorphism
\[
\mathbb{Z}/NZ \overset{\sim}{\to} \text{Gal}(K_{O,N}(\sqrt[t]{1})/K_{O,N}(t))
\]
\[
[m] \mapsto (\sqrt[t]{1} \mapsto \zeta_N^m \sqrt[t]{1}).
\]

Furthermore, since \( \sqrt[t]{1} \) is also a transcendental number, we get the following isomorphism
\[
\text{Gal}(K_{O,N}(\sqrt[t]{1})/K(\sqrt[t]{1})) \overset{\sim}{\to} \text{Gal}(K_{O,N}/K)
\]
\[
\sigma \mapsto \sigma|_{K_{O,N}}.
\]

Lemma 12.4. We have
\[
\text{Gal}(K_{O,N}(\sqrt[t]{1})/K(t)) = \text{Gal}(K_{O,N}(\sqrt[t]{1})/K_{O,N}(t)) \rtimes \text{Gal}(K_{O,N}(\sqrt[t]{1})/K(\sqrt[t]{1}))
\]
where \( \text{Gal}(K_{O,N}(\sqrt[t]{1})/K(\sqrt[t]{1})) \) acts on \( \text{Gal}(K_{O,N}(\sqrt[t]{1})/K_{O,N}(t)) \) by conjugation.

Proof. Let
\[
G = \text{Gal}(K_{O,N}(\sqrt[t]{1})/K(t)), \quad N = \text{Gal}(K_{O,N}(\sqrt[t]{1})/K_{O,N}(t)) \quad \text{and} \quad H = \text{Gal}(K_{O,N}(\sqrt[t]{1})/K(\sqrt[t]{1})).
\]

Note that the map
\[
N \times H \to NH
\]
\[
(\sigma_1, \sigma_2) \mapsto \sigma_1\sigma_2
\]
is bijective because \( N \cap H = \{\text{id}_{K_{O,N}(\sqrt[t]{1})}\} \). Since the extension \( K_{O,N}(t)/K(t) \) is abelian, \( N \) is normal in \( G \) by Galois theory. Moreover, we see that
\[
|N| \cdot |H| = |N| \cdot |\text{Gal}(K_{O,N}(t)/K(t))| = |G|.
\]

Therefore we conclude that \( G \) is the semidirect product of the normal subgroup \( N \) and \( H \) in the sense of [16] p. 76].
Since the group $\Gamma_1(N)$ acts on the set $\mathcal{Q}(D_O, N)$, so does its subgroup $\Gamma(N)$. Let $\sim_{\Gamma(N)}$ be the equivalence relation on $\mathcal{Q}(D_O, N)$ induced from the action of $\Gamma(N)$.

**Lemma 12.5.** If $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}(D_O, N)$ and $\gamma = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \Gamma_1(N)$, then we have

$$Q^\gamma = (ap^2 + bpr + cr^2)x^2 + (2apq + 2bqr + 2crs + b)xy + (aq^2 + bqs + cs^2)y^2.$$  

**Proof.** It is straightforward from the fact $\det(\gamma) = ps - qr = 1$. 

**Corollary 12.6.** One can regard $\mathcal{Q}(D_O, N)/\sim_{\Gamma(N)}$ as a group isomorphic to the Galois group $\text{Gal}(K_{O,N}(\sqrt[3]{t})/K(t))$.

**Proof.** For $Q \in \mathcal{Q}(D_O, N)$, we denote by $[Q]_{\Gamma(N)}$ and $[Q]_{\Gamma_1(N)}$ its classes in $\mathcal{Q}(D_O, N)/\sim_{\Gamma(N)}$ and $\mathcal{C}_N(D_O)$, respectively. Define a map

$$\psi : \mathcal{Q}(D_O, N)/\sim_{\Gamma(N)} \to \text{Gal}(K_{O,N}(\sqrt[3]{t})/K(t))$$

by

$$[Q]_{\Gamma(N)} = [ax^2 + bxy + cy^2]_{\Gamma(N)} \mapsto \begin{pmatrix} f(\tau_O) \mapsto f([Q]_{\Gamma_1(N)}) & (f \in \mathcal{F}_N \text{ is finite at } \tau_O) \\ \sqrt[3]{t} \mapsto \zeta_N^{b' - b} \sqrt[3]{t} \end{pmatrix}.$$  

First, we shall check that $\psi$ is well defined. Let $Q = ax^2 + bxy + cy^2$, $Q' = a'x^2 + b'xy + c'y^2 \in \mathcal{Q}(D_O, N)$ such that $[Q]_{\Gamma(N)} = [Q']_{\Gamma(N)}$. Since there is a natural surjection $\mathcal{Q}(D_O, N)/\sim_{\text{SL}_2(\mathbb{Z})} \to \mathcal{C}_N(D_O)$, we attain $[Q]_{\Gamma_1(N)} = [Q']_{\Gamma_1(N)}$ and so

$$f([Q]_{\Gamma_1(N)}) = f([Q']_{\Gamma_1(N)}) \quad (f \in \mathcal{F}_N \text{ is finite at } \tau_O).$$

Furthermore, since

$$Q' = Q^\gamma \quad \text{for some } \gamma = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \Gamma(N),$$

we find that

$$\frac{b' - b}{2} = apq + bqr + crs \quad \text{by Lemma 12.5}$$

$$\equiv 0 \pmod{N} \quad \text{because } q \equiv r \equiv 0 \pmod{N}.$$  

Thus we obtain that

$$\frac{b' - b_O}{2} \equiv \frac{b - b_O}{2} \pmod{N},$$

and hence

$$\zeta_N^{b' - b_O} \sqrt[3]{t} = \zeta_N^{b - b_O} \sqrt[3]{t}.$$  

Therefore $\psi$ is well defined.

Second, we shall prove that $\psi$ is injective. Suppose that

$$\psi([Q]_{\Gamma(N)}) = \psi([Q']_{\Gamma(N)})$$

for some $Q = ax^2 + bxy + cy^2$, $Q' = a'x^2 + b'xy + c'y^2 \in \mathcal{Q}(D_O, N)$.

Since

$$f([Q]_{\Gamma_1(N)}) = f([Q']_{\Gamma_1(N)})$$

for all $f \in \mathcal{F}_N$ finite at $\tau_O$,
we get by Theorem 12.3 that 
\[ Q' = Q' \Gamma \] for some \( \gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \Gamma_1(N). \)

Moreover, since \( \zeta_{N}^{-\frac{b - b_{O}}{2}} = \zeta_{N}^{-\frac{b' - b_{O}}{2}} \), we achieve
\[ \frac{b - b_{O}}{2} \equiv \frac{b' - b_{O}}{2} \pmod{N} \] (72)
and derive that
\[
0 \equiv \frac{b' - b}{2} \pmod{N} \quad \text{by (72)}
\]
\[
\equiv apq + bqr + crs \quad \text{by Lemma 12.5}
\]
\[
\equiv aq \pmod{N} \quad \text{because} \quad p \equiv 1 \text{ and } r \equiv 0 \pmod{N}.
\]

It then follows from the fact \( \gcd(a, N) = 1 \) that \( q \equiv 0 \pmod{N} \). Thus \( \gamma \) belongs to \( \Gamma(N) \) and so
\[ [Q]_{\Gamma(N)} = [Q']_{\Gamma(N)}. \]

This observation shows the injectivity of \( \psi \).

Third, we shall show that \( \psi \) is surjective. Let \( \sigma \in \text{Gal}(K_{O,N}(\sqrt[1]{t})/K(t)) \). Then there exists a pair \( (Q, m) \) of \( Q = ax^2 + bxy + cy^2 \in \mathbb{Q}(D_{O,N}) \) and \( m \in \mathbb{Z} \) such that
\[ f(\tau_{O}) \sigma = f([Q]_{\Gamma_1(N)}) \quad (f \in \mathcal{F}_{N} \text{ is finite at } \tau_{O}) \quad \text{and} \quad \sqrt[1]{t} \sigma = \zeta_{N}^{m} \sqrt[1]{t} \]
by Theorem 12.3, (70), (71) and Lemma 12.4. Observe that these actions of \( \sigma \) completely determine \( \sigma \). If we set
\[ Q' = a'x^2 + b'xy + c'y^2 = Q_{1}(a' \{ m - (b - b_{O})/2 \}) \]
where \( a' \) is an integer satisfying \( aa' \equiv 1 \pmod{N} \), then we get that
\[ f(\tau_{O}) \psi([Q']_{\Gamma_1(N)}) = f([Q]_{\Gamma_1(N)}) \quad (f \in \mathcal{F}_{N} \text{ is finite at } \tau_{O}) \]
and
\[ \sqrt[1]{t} \psi([Q']_{\Gamma_1(N)}) = \zeta_{N}^{\frac{b'-b_{O}}{2}} \sqrt[1]{t} = \zeta_{N}^{m} \sqrt[1]{t} \]
by Lemma 12.5. Thus we have \( \sigma = \psi([Q']_{\Gamma_1(N)}) \), which proves that \( \psi \) is surjective as desired.

Finally, through the bijection \( \psi \) we can endow the set \( \mathbb{Q}(D_{O,N})/\sim_{\Gamma(N)} \) with a binary operation so that \( \mathbb{Q}(D_{O,N})/\sim_{\Gamma(N)} \) is isomorphic to \( \text{Gal}(K_{O,N}(\sqrt[1]{t})/K(t)) \).

13 The \( L \)-functions for orders

As an analogue of the Weber \( L \)-function for a ray class character modulo \( NO_{K} \), we shall define an \( L \)-function for a character of \( \mathcal{C}_{N}(O) \).
Definition 13.1. Let $\chi$ be a character of $\mathcal{C}_N(\mathcal{O})$.

(i) We define the $L$-function $L_{\mathcal{O}}(\cdot, \chi)$ by

$$L_{\mathcal{O}}(s, \chi) = \sum_{a \in M(\mathcal{O}, N)} \frac{\chi([a])}{N_{\mathcal{O}}(a)^s} \quad (s \in \mathbb{C}, \operatorname{Re}(s) > 1)$$

where $[a]$ is the class of $a$ in $\mathcal{C}_N(\mathcal{O})$.

(ii) For each $C \in \mathcal{C}_N(\mathcal{O})$, we define the $\zeta$-function $\zeta_{\mathcal{O}}(\cdot, C)$ by

$$\zeta_{\mathcal{O}}(s, C) = \sum_{a \in C \cap M(\mathcal{O}, N)} \frac{1}{N_{\mathcal{O}}(a)^s} \quad (s \in \mathbb{C}, \operatorname{Re}(s) > 1).$$

Remark 13.2. (i) We have

$$L_{\mathcal{O}}(s, \chi) = \sum_{C \in \mathcal{C}_N(\mathcal{O})} \chi(C) \zeta_{\mathcal{O}}(s, C).$$

(ii) In Definition 13.1 (i), what if $\mathcal{C}_N(\mathcal{O})$ and $M(\mathcal{O}, N)$ are replaced by $\mathcal{C}_N(\mathcal{O}, \ell_{\mathcal{O}}N)$ and $M(\mathcal{O}, \ell_{\mathcal{O}}N)$, respectively? For a character $\psi$ of $\mathcal{C}_N(\mathcal{O}, \ell_{\mathcal{O}}N)$, define

$$L_{\mathcal{O}}(s, \psi) = \sum_{a \in M(\mathcal{O}, \ell_{\mathcal{O}}N)} \frac{\psi([a])}{N_{\mathcal{O}}(a)^s} \quad (s \in \mathbb{C}, \operatorname{Re}(s) > 1)$$

where $[a]$ is the class of $a$ in $\mathcal{C}_N(\mathcal{O}, \ell_{\mathcal{O}}N)$. In particular, if $\ell_{\mathcal{O}}$ divides $N$, then we get $\mathcal{C}_N(\mathcal{O}, \ell_{\mathcal{O}}N) = \mathcal{C}_N(\mathcal{O})$ and so $L_{\mathcal{O}}(s, \psi) = L_{\mathcal{O}}(s, \psi)$. Let $\tilde{\psi}$ be the character of the ray class group $\mathcal{C}_{\ell_{\mathcal{O}}N}(\mathcal{O}_K)$ achieved by composing three homomorphisms

$$\mathcal{C}_{\ell_{\mathcal{O}}N}(\mathcal{O}_K) \xrightarrow{\text{natural}} I(\mathcal{O}_K, \ell_{\mathcal{O}}N)/P_{\mathbb{Z}, N}(\mathcal{O}_K, \ell_{\mathcal{O}}N) \xrightarrow{\sim} \mathcal{C}_N(\mathcal{O}, \ell_{\mathcal{O}}N) \xrightarrow{\psi} \mathbb{C}^*.$$

Here the second isomorphism is the one established in Proposition 2.8. And we find by Lemmas 2.3 (i) and 2.6 that

$$L_{\mathcal{O}}(s, \psi) = \sum_{a \in M(\mathcal{O}, \ell_{\mathcal{O}}N)} \frac{\tilde{\psi}([a\mathcal{O}_K])}{N_{\mathcal{O}_K}(a\mathcal{O}_K)^s} = \sum_{b \in M(\mathcal{O}_K, \ell_{\mathcal{O}}N)} \frac{\tilde{\psi}([b])}{N_{\mathcal{O}_K}(b)^s} = L_{\mathcal{O}_K}(s, \tilde{\psi}).$$

When $N = 1$, Meyer (118) gave a concrete formula for the value $L_{\mathcal{O}_K}(1, \tilde{\psi})$.

Lemma 13.3. Let $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}(D_{\mathcal{O}}, N)$, $\epsilon = [w_Q, 1]$ and $[c]$ be the class of $\epsilon$ in $\mathcal{C}_N(\mathcal{O})$. Let

$$P = \{ \lambda \in a\mathbb{T} \mid \lambda \neq 0 \text{ and } \lambda \equiv 1 \pmod{N\mathcal{O}} \}.$$

(i) We get $[c] \cap M(\mathcal{O}, N) = \{ \lambda \epsilon \mid \lambda \in P \}$.

(ii) If $\lambda, \mu \in P$, then

$$\lambda \epsilon = \mu \epsilon \iff \mu = \zeta \lambda \text{ for some } \zeta \in \mathcal{O}^* \text{ such that } \zeta \equiv 1 \pmod{N\mathcal{O}}.$$
Proof. (i) Let \( \lambda \in P \). We see that
\[
\lambda c \in [c] \quad \text{and} \quad \lambda \in a\overline{c} = \frac{1}{a}(ac)(\overline{ac}) = \mathcal{O}
\]
by Lemmas 2.1 (iii) and 5.2. It then follows from Lemma 2.4 that
\[
\lambda c \in I(\mathcal{O}, N) \cap \mathcal{M}(\mathcal{O}) = \mathcal{M}(\mathcal{O}, N).
\]
Thus we attain the inclusion
\[
\{ \lambda c \mid \lambda \in P \} \subseteq [c] \cap \mathcal{M}(\mathcal{O}, N).
\]
Now, let \( a \in [c] \cap \mathcal{M}(\mathcal{O}, N) \). Since \( a \in [c] \), we have
\[
a = \lambda c \quad \text{with} \quad \lambda = \frac{\lambda_1}{\lambda_2}
\]
for some \( \lambda_1, \lambda_2 \in \mathcal{O} \setminus \{0\} \) such that \( \lambda_1 \equiv \lambda_2 \equiv 1 \pmod{NO} \).
Therefore we derive from the fact \( a \subseteq \mathcal{O} \) that
\[
\lambda \in c^{-1} = a\overline{c} \subseteq \mathcal{O}
\]
again by Lemmas 2.1 (iii) and 5.2. Moreover, since
\[
\lambda_2 \lambda = \lambda_1 \quad \text{and} \quad \lambda_1 \equiv \lambda_2 \equiv 1 \pmod{NO},
\]
we deduce \( \lambda \equiv 1 \pmod{NO} \), and hence \( \lambda \in P \) and \( a = \lambda c \in \{ \lambda c \mid \lambda \in P \} \). This proves the converse inclusion
\[
[c] \cap \mathcal{M}(\mathcal{O}, N) \subseteq \{ \lambda c \mid \lambda \in P \}.
\]
(ii) Assume that \( \lambda c = \mu c \). Then we attain \( \lambda \mathcal{O} = \mu \mathcal{O} \) and so \( \mu = \zeta \lambda \) for some \( \zeta \in \mathcal{O}^* \).
Furthermore, since \( \lambda \equiv \mu \equiv 1 \pmod{NO} \), we must have \( \zeta \equiv 1 \pmod{NO} \). And, the converse is obvious.

Let
\[
\gamma_{\mathcal{O},N} = |\{ \nu \in \mathcal{O}^* \mid \nu \equiv 1 \pmod{NO} \}|.
\]

Proposition 13.4. Let \( C \in C_N(\mathcal{O}) \) and so \( C = \phi_{\mathcal{O},N}([Q]) \) for some \( Q = ax^2 + bxy + cy^2 \in \mathcal{O}(D, N) \) by Proposition 9.3. Then we have
\[
\zeta_{\mathcal{O}}(s, C) = \frac{1}{\gamma_{\mathcal{O},N}(N^2a)^{s}} \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,-\frac{a'}{N})\}} \frac{1}{|m(-\overline{Q}) + n + a' \frac{N}{N}|^{2s}}
\]
where \( a' \) is an integer which satisfies \( aa' \equiv 1 \pmod{N} \).

Proof. Let \( c = [\omega Q, 1] \). Then we find that
\[
\zeta_{\mathcal{O}}(s, C) = \sum_{a \in [c] \cap \mathcal{M}(\mathcal{O}, N)} \frac{1}{N_{\mathcal{O}}(a)^s}
\]
\[
\sum_{\lambda \in P} \frac{1}{N_{\mathcal{O}}(\lambda \mathcal{C})^s}
\]
where \(P = \{\lambda \in \mathcal{A} \mid \lambda \neq 0 \text{ and } \lambda \equiv 1 \pmod{\mathcal{O}}\}\),
by Lemma 13.3

\[
\sum_{\lambda \in P} \left( \frac{N_{\mathcal{O}}(\lambda \mathcal{C})}{N_{\mathcal{O}}(\lambda \mathcal{O})N_{\mathcal{O}}(\mathcal{A})} \right)^s
\]
by Lemmas 2.1 (ii) and 5.2

\[
\sum_{\lambda \in P} \left( \frac{a^2}{N_{K/Q}(\lambda) \cdot a} \right)^s
\]
by Lemmas 2.1 (i) and 5.2

\[
\sum_{(m, n) \in \mathbb{Z}^2 \setminus \{(0, 0)\}, \nu \neq 1 \pmod{\mathcal{N}} \text{ such that } m \neq 0, \nu^{-1} m \equiv 0 \pmod{\mathcal{N}}}
\]
because \(\lambda \in P, a\mathcal{C} = [-a\mathcal{O}, a] \) and \(\mathcal{O} = [-a\mathcal{O}, 1]\)

\[
\sum_{(m, n) \in \mathbb{Z}^2 \setminus \{(0, 0)\}, \nu \neq 1 \pmod{\mathcal{N}}}
\]
by Lemmas 2.1 (i) and 5.2

\[
\sum_{(m, n) \in \mathbb{Z}^2 \setminus \{(0, 0)\}, \nu \neq 1 \pmod{\mathcal{N}}}
\]

\[
14 \text{ Derivatives of } L\text{-functions at } s = 0
\]

In this section, we shall derive a formula of the derivative \(L'_{\mathcal{O}}(0, \chi)\) in terms of ray class invariants for the order \(\mathcal{O}\).

By Lemma 2.1 (ii), we can extend the norm map \(N_{\mathcal{O}} : \mathcal{M}(\mathcal{O}) \to \mathbb{Z}\) to the well-defined function
\[
I(\mathcal{O}) \to \mathbb{Q}, \quad ab^{-1} \mapsto N_{\mathcal{O}}(a)N_{\mathcal{O}}(b)^{-1} \quad (a, b \in \mathcal{M}(\mathcal{O}))
\]
and denote it again by \(N_{\mathcal{O}}\).

**Definition 14.1.** Let \(C \in \mathcal{C}_N(\mathcal{O})\).

(i) Let \(N = 1\). Take a proper \(\mathcal{O}\)-ideal \(\mathfrak{c}\) in the class \(C\) and define
\[
g_{\mathcal{O}, N}(C) = g_{\mathcal{O}, 1}(C) = (2\pi)^{12} N_{\mathcal{O}}(\mathfrak{c}^{-1})^6 |\Delta(\mathfrak{c}^{-1})|.
\]

(ii) If \(N \geq 2\), then we define
\[
g_{\mathcal{O}, N}(C) = g_{\mathcal{O}, 1}^{12N}(\mathfrak{c}^{-1})(C).
\]

**Remark 14.2.** (i) Let \(\{\xi_1, \xi_2\}\) be a \(\mathbb{Z}\)-basis for \(\mathfrak{c}^{-1}\) such that
\[
\xi := \frac{\xi_1}{\xi_2} \in \mathbb{H}.
\]
By using Lemma 2.1 (i) and the well-known fact that the function
\[
\mathbb{H} \to \mathbb{C}, \quad \tau \mapsto |\Delta([\tau, 1])|
\]

40
is a modular form for $\text{SL}_2(\mathbb{Z})$ of weight 12 ([15] Theorem 3 in Chapter 3 and Theorem 5 in Chapter 18)), we find that
\[
(2\pi)^{12} N_\mathcal{O}(c^{-1})^6 |\Delta(c^{-1})| = (2\pi)^{12} N_\mathcal{O}([\xi, 1])^6 |\Delta([\xi, 1])|.
\] (73)
And one can readily check that this value depends only on the class $C$, not on the special choice of $c$.

(ii) Since the modular form $\Delta$ and the Siegel function $g_{12}^{[0, \frac{N}{2}]}$ have no zeros and poles on $\mathbb{H}$, the invariant $g_{\mathcal{O}, N}(C)$ is always finite and nonzero.

(iii) If $N \geq 2$, then $g_{\mathcal{O}, N}(C) = g_{12}^{[0, \frac{N}{2}]}(C)$ belongs to $K_{\mathcal{O}, N}$ and satisfies
\[
g_{\mathcal{O}, N}(C)^{\sigma_{\mathcal{O}, N}(C')} = g_{12}^{[0, \frac{N}{2}]}(C)^{\sigma_{\mathcal{O}, N}(C')} = g_{12}^{[1, \frac{N}{2}]}(CC') = g_{\mathcal{O}, N}(CC')
\] by Theorem 11.4.

(iv) Recently, Jung and Kim showed that if $D_\mathcal{O} \neq -3, -4$ and $N \geq 2$, then $g_{\mathcal{O}, N}(C_0)^n$ generates $K_{\mathcal{O}, N}$ over $K$ for any nonzero integer $n$ ([10] Theorem 1.1).

For a pair $(\omega, z) \in \mathbb{C} \times \mathbb{H}$, we define the $\xi$-function $\xi(\cdot, \omega, z)$ by
\[
\xi(s, \omega, z) = \sum_{(m, n) \in \mathbb{Z}^2 \text{ such that } mz + n + \omega \neq 0} \frac{1}{|mz + n + \omega|^{2s}} \quad (s \in \mathbb{C}, \text{Re}(s) > 1).
\]
Put
\[
\eta(z) = e^{\frac{\pi i}{12}} \prod_{n=1}^{\infty} \left(1 - e^{2\pi i nz}\right),
\]
\[
\vartheta_1(\omega, z) = 2e^{\frac{\pi i}{12}} \left(\sin \pi \omega\right) \eta(z) \prod_{n=1}^{\infty} \left(1 - e^{2\pi i (nz + \omega)}\right) \left(1 - e^{2\pi i (nz - \omega)}\right).
\] (74)

**Proposition 14.3** (Kronecker’s limit formula). The $\xi$-function satisfies the following properties.

(i) It has an analytic continuation on the whole complex plane and
\[
\xi(0, \omega, z) = \begin{cases} 
-1 & \text{if } \omega \in [z, 1], \\
0 & \text{if } \omega \notin [z, 1]. 
\end{cases}
\]

(ii) If we let $\xi' = \frac{d\xi}{ds}$, then
\[
\xi'(0, \omega, z) = \begin{cases} 
-\ln \left|4\pi^2 \eta(z)^4\right| & \text{if } \omega \in [z, 1], \\
-\ln \left|\frac{\vartheta_1(\omega, z)}{\eta(z)} e^{\frac{\pi i \omega}{z-\frac{1}{2}}}\right|^2 & \text{if } \omega \notin [z, 1].
\end{cases}
\]

**Proof.** See [1, Theorem 4], [22] or [27].
Theorem 14.4. If \( \chi \) is a character of \( C_N(O) \), then we have

\[
L'_O(0, \chi) = -\frac{1}{\gamma O, N 6N} \sum_{C \in \mathcal{C}_N(O)} \chi(C) \ln |g_{O, N}(C)|.
\]

Proof. Let \( C \in \mathcal{C}_N \) and so \( C = \phi_{O, N}([Q]) \) for some \( Q = ax^2 + bxy + cy^2 \). Let \( a' \) be an integer satisfying \( a\alpha \equiv 1 \pmod{N} \). Since

\[
\zeta(O, s, C) = \frac{1}{\gamma O, N(N^2a)^s} \xi(s, \frac{a}{N}, -\omega_Q)
\]

by Proposition 13.4, we find that

\[
\zeta'_O(0, C) = \frac{1}{\gamma O, N} \left( -\ln(N^2a)\xi(0, \frac{a}{N}, -\omega_Q) + \xi'(0, \frac{a}{N}, -\omega_Q) \right)
\]

by Proposition 14.3 (i)

\[
= \frac{1}{\gamma O, N} \times \left\{ \begin{array}{ll}
\ln a - \ln |4\pi^2\eta(-\omega_Q)| & \text{if } N = 1, \\
-\frac{1}{6} \ln |g_{(0 \frac{a}{N})}(-\omega_Q)|^2 & \text{if } N \geq 2,
\end{array} \right.
\]

by Proposition 14.3 (ii)

\[
= \frac{1}{\gamma O, N} \times \left\{ \begin{array}{ll}
-\frac{1}{6} \ln |g_{O, 1}(C)| & \text{if } N = 1, \\
-\frac{1}{6N} \ln |g_{O, N}(C)| & \text{if } N \geq 2,
\end{array} \right.
\]

by Lemma 5.2 and Definitions 13, 74.

Therefore we conclude that

\[
L'_O(0, \chi) = \sum_{C \in \mathcal{C}_N(O)} \chi(C) \zeta'_O(0, C) = -\frac{1}{\gamma O, N 6N} \sum_{C \in \mathcal{C}_N(O)} \chi(C) \ln |g_{O, N}(C)|.
\]

\[\square\]

15 An example of \( C_N(D_O) \)

We shall present an example of \( C_N(D_O) \) and its application further in order to find the minimal polynomial of the invariant \( g_{O, N}(C_0) \) over \( K \).

Let \( K = \mathbb{Q}(\sqrt{2}) \) and \( O = [5\sqrt{2}, 1] \). Then we get

\[
D_O = -200, \quad \ell_O = 5, \quad \tau_O = 5\sqrt{2}, \quad \min(\tau_O, Q) = x^2 + b_{O}x + c_{O} = x^2 + 50.
\]

On the other hand, there are six reduced forms of discriminant \( D_O = -200 \), namely,

\[
Q_1 = x^2 + 50y^2, \quad Q_2 = 2x^2 + 25y^2, \\
Q_3 = 3x^2 - 2xy + 17y^2, \quad Q_4 = 3x^2 + 2xy + 17y^2, \\
Q_5 = 6x^2 - 4xy + 9y^2, \quad Q_6 = 6x^2 + 4xy + 9y^2.
\]

42
Let $N = 3$, and set

\[
\tilde{Q}_1 = Q_1 = x^2 + 50y^2, \quad \tilde{Q}_2 = Q_2 = 2x^2 + 25y^2,
\]
\[
\tilde{Q}_3 = Q_3 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = 17x^2 + 2xy + 3y^2, \quad \tilde{Q}_4 = Q_4 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = 17x^2 - 2xy + 3y^2,
\]
\[
\tilde{Q}_5 = Q_5 \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix} = 11x^2 - 8xy + 6y^2, \quad \tilde{Q}_6 = Q_6 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 11x^2 + 8xy + 6y^2.
\]

so as to have $\tilde{Q}_i \in \mathcal{Q}(D_O, N)$ ($i = 1, 2, \ldots, 6$). By utilizing the fact

\[
W_{O,N}/U_{O,N} \simeq \text{Gal}(K_{O,N}/H_O) \simeq P(\mathcal{O}, N)/P_N(\mathcal{O}) \simeq P(\mathcal{O}, \ell_O N)/P_N(\mathcal{O}, \ell_O N)
\]

(27) and Lemma 2.12 and Lemma 2.2, we attain

\[
P(\mathcal{O}, \ell_O N)/P_N(\mathcal{O}, \ell_O N) = \left\{ [\mathcal{O}], [\tau_\mathcal{O} \mathcal{O}] = \left[ \left[ \frac{\sqrt{3}}{9}, 1 \right] \right] \right\},
\]

which corresponds to the subgroup $\{[\tilde{Q}_1], [50x^2 + y^2]\}$ of $C_N(D_O) = C_3(-200)$. In the group $C_N(D_O)$, we let

\[
g_i = [\tilde{Q}_j] \quad \text{and} \quad g_{i+6} = g_i \cdot [50x^2 + y^2] \quad (i = 1, 2, \ldots, 6).
\]

By adopting Definition 5.7 one can readily find that $g_j = [\tilde{Q}_j]$ ($j = 7, 8, \ldots, 12$) with

\[
\tilde{Q}_7 = 50x^2 + y^2, \quad \tilde{Q}_8 = 25x^2 + 2y^2,
\]
\[
\tilde{Q}_9 = 22x^2 - 36xy + 17y^2, \quad \tilde{Q}_{10} = 22x^2 + 36xy + 17y^2,
\]
\[
\tilde{Q}_{11} = 25x^2 + 30xy + 11y^2, \quad \tilde{Q}_{12} = 25x^2 - 30xy + 11y^2.
\]

The group table of $C_N(D_O)$ is given as follows.

|       | $g_1$ | $g_2$ | $g_3$ | $g_4$ | $g_5$ | $g_6$ | $g_7$ | $g_8$ | $g_9$ | $g_{10}$ | $g_{11}$ | $g_{12}$ |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-----------|-----------|-----------|
| $g_1$ | $g_1$ | $g_2$ | $g_3$ | $g_4$ | $g_5$ | $g_6$ | $g_7$ | $g_8$ | $g_9$ | $g_{10}$ | $g_{11}$ | $g_{12}$ |
| $g_2$ | $g_2$ | $g_1$ | $g_{12}$ | $g_{11}$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_2$ |
| $g_3$ | $g_3$ | $g_1$ | $g_{12}$ | $g_{11}$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_2$ |
| $g_4$ | $g_4$ | $g_1$ | $g_{12}$ | $g_{11}$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_2$ |
| $g_5$ | $g_5$ | $g_1$ | $g_{12}$ | $g_{11}$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_2$ |
| $g_6$ | $g_6$ | $g_1$ | $g_{12}$ | $g_{11}$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_2$ |
| $g_7$ | $g_7$ | $g_1$ | $g_{12}$ | $g_{11}$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_2$ |
| $g_8$ | $g_8$ | $g_1$ | $g_{12}$ | $g_{11}$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_2$ |
| $g_9$ | $g_9$ | $g_1$ | $g_{12}$ | $g_{11}$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_2$ |
| $g_{10}$ | $g_{10}$ | $g_1$ | $g_{12}$ | $g_{11}$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_2$ |
| $g_{11}$ | $g_{11}$ | $g_1$ | $g_{12}$ | $g_{11}$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_2$ |
| $g_{12}$ | $g_{12}$ | $g_1$ | $g_{12}$ | $g_{11}$ | $g_{10}$ | $g_9$ | $g_8$ | $g_7$ | $g_6$ | $g_5$ | $g_4$ | $g_3$ | $g_2$ |

Since $C_N(D_O)$ has three elements $g_2, g_7, g_8$ of order 2, it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6$. 43
Write $\tilde{Q}_i = a_i x^2 + b_i x y + c_i y^2$ ($i = 1, 2, \ldots, 12$). We then achieve that

$$\min(g_{O,N}(C_0), K) = \prod_{C \in \mathcal{C}_N(O)} \left( x - g_{12N}^{(0)}(C) \right)$$

by Definition 14.1 (ii) and Remark 14.2 (iii), (iv)

$$= \prod_{i=1}^{12} \left( x - \left(g_{12N}^{(0)}[0 a_i']^{(-\omega \tilde{Q}_i)}\right) \right)$$

where $a'_i$ is an integer such that $a_i a'_i \equiv 1 \pmod{N}$

by Definition 12.1 and Lemma 12.2

$$= \prod_{i=1}^{12} \left( x - g_{12N}^{(0)}[0 a_i']\left(1 - a'_i(b_i + b_{O})/2\right)\right)$$

by Proposition 4.2.

By making use of the definition (13), one can numerically estimate $\min(g_{O,3}(C_0), K)$ as

$$x^{12} - 19732842623587344380x^{11} + 85622274889372918445313749346x^{10}$$

$$+ 583422788794106041501392970996250100x^9$$

$$+ 2412956602599045666947505580865471555967855x^8$$

$$+ 462203004758636935674310042178173142345125210120x^7$$

$$+ 5159639382647422206917922996901583694331066838711900x^6$$

$$+ 202375300752001975403428909178152428797277946213173155269640x^5$$

$$+ 4487601627619641192200184812721309459195966653602482165478526149968226x^4$$

$$- 2883328681523953153105049905288236082227616017140993789678594572300x^3$$

$$+ 4487601627619641192200184812721309459195966653602482165478526149968226x^2$$

$$- 198336994240544255644192507478303953455541722620x + 1.$$
Data availability

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

References

[1] B. C. Berndt, *Identities involving the coefficients of a class of Dirichlet series VI*, Trans. Amer. Math. Soc., 160 (1971), 157–167.

[2] A. Bourdon and P. L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. 305 (2020), no. 1, 43–88.

[3] A. Bourdon, P. L. Clark and P. Pollack, *Anatomy of torsion in the CM case*, Math. Z. 285 (2017), no. 3–4, 795–820.

[4] B. Cho, *Primes of the form $x^2 + ny^2$ with conditions $x \equiv 1 \mod{N}, y \equiv 0 \mod{N}$*, J. Number Theory 130 (2010), no. 4, 852–861.

[5] P. L. Clark and P. Pollack, *The truth about torsion in the CM case, II*, Q. J. Math. 68 (2017), no. 4, 1313–1333.

[6] D. A. Cox, *Primes of the Form $x^2 + ny^2$–Fermat, Class field theory, and Complex Multiplication*, 3rd ed. with solutions, with contributions by Roger Lipsett, AMS Chelsea Publishing, Providence, R.I., 2022.

[7] I. S. Eum, J. K. Koo and D. H. Shin, *Binary quadratic forms and ray class groups*, Proc. Roy. Soc. Edinburgh Sect. A 150 (2020), no. 2, 695–720.

[8] C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801.

[9] G. J. Janusz, *Algebraic Number Fields*, 2nd ed., Grad. Studies in Math. 7, Amer. Math. Soc., Providence, R. I., 1996.

[10] H. Y. Jung and C. H. Kim, *Modularity of Galois traces of ray class invariants*, Ramanujan J. 54 (2021), no. 2, 355–383.

[11] H. Y. Jung, J. K. Koo and D. H. Shin, *Generation of ray class fields modulo 2, 3, 4 or 6 by using the Weber function*, J. Korean Math. Soc. 55 (2018), no. 2, 343–372.

[12] H. Y. Jung, J. K. Koo and D. H. Shin, *Class fields generated by coordinates of elliptic curves*, Open Math. 20 (2022), no. 1, 1145–1158.

[13] H. Y. Jung, J. K. Koo, D. H. Shin and D. S. Yoon, *On some $p$-adic Galois representations and form class groups*, Mathematika 68 (2022), no. 2, 535–564.

[14] D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, New York-Berlin, 1981.
[15] S. Lang, *Elliptic Functions*, With an appendix by J. Tate, 2nd ed., Grad. Texts in Math. 112, Springer-Verlag, New York, 1987.

[16] S. Lang, *Algebra*, 3rd ed., Grad. Texts in Math. 211, Springer-Verlag, New York, 2002.

[17] Á. Lozano-Robledo, *Galois representations attached to elliptic curves with complex multiplication*, Algebra Number Theory 16 (2022), no. 4, 777–837.

[18] C. Meyer, *Über einige Anwendungen Dedekindscher Summen*, J. Reine Angew. Math. 198 (1957), 143–203.

[19] K. Ramachandra, *Some applications of Kronecker’s limit formula*, Ann. of Math. (2) 80 (1964), 104–148.

[20] R. Schertz, *Complex multiplication*, New Mathematical Monographs, 15, Cambridge University Press, Cambridge, 2010.

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

[22] T. Shintani, *A proof of the classical Kronecker limit formula*, Tokyo J. Math. 3 (1980), no. 2, 191–199.

[23] C. L. Siegel, *Lectures on Advanced Analytic Number Theory*, Notes by S. Raghavan, Tata Institute of Fundamental Research Lectures on Mathematics 23, Tata Institute of Fundamental Research, Bombay 1965.

[24] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer-Verlag, New York, 1994.

[25] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, Dordrecht, 2009.

[26] H. Söhngen, *Zur Komplexen Multiplikation*, Math. Ann. 111 (1935), no. 1, 302–328.

[27] H. M. Stark, *Class fields and modular forms of weight one*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 277–287, Lecture Notes in Math. 601, Springer, Berlin, 1977.

[28] P. Stevenhagen, *Hilbert’s 12th problem, complex multiplication and Shimura reciprocity*, Class field theory—its centenary and prospect (Tokyo, 1998), 161–176, Adv. Stud. Pure Math. 30, Math. Soc. Japan, Tokyo, 2001.

Department of Mathematics  
Dankook University  
Cheonan-si, Chungnam 31116  
Republic of Korea  
E-mail address: hoyunjung@dankook.ac.kr

Department of Mathematical Sciences  
KAIST  
Daejeon 34141  
Republic of Korea  
E-mail address: jkgoo@kaist.ac.kr
