On some $p$-adic Galois representations and form class groups

Ho Yun Jung$^1$ | Ja Kyung Koo$^2$ | Dong Hwa Shin$^3$ | Dong Sung Yoon$^4$

$^1$Department of Mathematics, Dankook University, Cheonan-si, South Korea
$^2$Department of Mathematical Sciences, KAIST, Daejeon, South Korea
$^3$Department of Mathematics, Hankuk University of Foreign Studies, Yongin-si, South Korea
$^4$Department of Mathematics Education, Pusan National University, Busan, South Korea

Abstract
Let $K$ be an imaginary quadratic field of discriminant $d_K$ with ring of integers $\mathcal{O}_K$. When $K$ is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, we consider a specific elliptic curve $E_{J_K}$ with $j$-invariant $j(\mathcal{O}_K)$ which is defined over $\mathbb{Q}(j(\mathcal{O}_K))$. In this paper, for each positive integer $N$ we compare the extension field of $\mathbb{Q}$ generated by the coordinates of $N$-torsion points on $E_{J_K}$ with the ray class field $K(N)$ of $K$ modulo $N\mathcal{O}_K$. By using this result, we investigate the image of the $p$-adic Galois representation attached to $E_{J_K}$ for a prime $p$, in terms of class field theory. Second, we construct the definite form class group of discriminant $d_K$ and level $N$ which is isomorphic to $\text{Gal}(K(N)/\mathbb{Q})$.

MSC (2020)
11R37 (primary), 11E08, 11F80, 14K22, 11R29 (secondary)

Contents

1. INTRODUCTION .................................... 536
2. ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION ............................ 538
3. MODULAR FUNCTIONS ................................ 540
4. THE SHIMURA RECIPROCITY LAW ............................................. 542
1 | INTRODUCTION

Let $K$ be an imaginary quadratic field of discriminant $d_K$, and let $\mathcal{O}_K$ be its ring of integers. The theory of complex multiplication shows that the maximal abelian extension $K^{ab}$ of $K$ can be generated by singular values of some modular functions [23, Chapter 10]. Furthermore, through the Shimura reciprocity law, one can connect the class field theory with the theory of modular functions [29]. For a positive integer $N$, let $K_{(N)}$ denote the ray class field of $K$ modulo $\mathfrak{N}$. In particular, $K_{(1)}$ is the Hilbert class field $H_K$ of $K$. We let $W_{K,N}$ be a Cartan subgroup of $GL_2(\mathbb{Z}/\mathfrak{N}\mathbb{Z})$ assigned to the $(\mathbb{Z}/\mathfrak{N}\mathbb{Z})$-algebra $\mathcal{O}_K/\mathfrak{N}\mathcal{O}_K$ defined in §4 (12). In [33], Stevenhagen improved the Shimura reciprocity law and expressed $\text{Gal}(K_{(N)}/H_K)$ as the quotient group of $W_{K,N}$ by the subgroup corresponding to the unit group $\mathcal{O}_K^\times$. His work brings up a natural question whether there is a 2-dimensional representation attached to an elliptic curve with complex multiplication whose image in $GL_2(\mathbb{Z}/\mathfrak{N}\mathbb{Z})$ is related to $W_{K,N}$.

On the other hand, there are remarkable works on torsion subgroups of elliptic curves with complex multiplication defined over number fields and on isogenies between such elliptic curves by Bourdon and Clark [2, 3], Bourdon et al. [4], Bourdon et al. [5] and Clark and Pollack [7]. In this paper, when $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, we shall focus on the elliptic curve $E_{J_K}$ given by the Weierstrass equation

$$E_{J_K} : y^2 = 4x^3 - J_K(J_K - 1) 27 x - J_K \left( \frac{J_K - 1}{27} \right)^2 \quad \text{with} \quad J_K = \frac{1}{1728} j(\mathcal{O}_K)$$

and examine the extension field $\mathbb{Q}(E_{J_K}[N])$ of $\mathbb{Q}$ generated by the coordinates of $N$-torsion points on $E_{J_K}$ as follows (Theorem 5.4).

**Theorem A.** Assume that $K$ is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Let $T_N = \mathbb{Q}(E_{J_K}[N])$.

(i) If $d_K \equiv 0 \pmod{4}$, then $T_2$ is the maximal real subfield of $K_{(2)}$ with $[K_{(2)} : T_2] = 2$.

(ii) If $d_K \equiv 1 \pmod{4}$, then $T_2 = K_{(2)}$.

(iii) If $N \geq 3$, then $T_N$ is an extension field of $K_{(N)}$ with $[T_N : K_{(N)}] \leq 2$.

Note that (i) and (ii) of Theorem A are different from prior works [3, Lemma 8.4] and [5, Theorem 4.2] because $T_N$ is the extension field of $\mathbb{Q}$, not of $Q(J_K)$, generated by the coordinates of $N$-torsion points on $E_{J_K}$. It turns out that $T_N$ contains $Q(J_K)$ (Remark 5.5).

Recently, Lozano–Róbledo [26] has classified all possible images of $p$-adic Galois representations attached to elliptic curves $E$ with complex multiplication defined over $\mathbb{Q}(j(E))$, from which
he deduced an analogue of Serre’s open image theorem [28]. Let \( Q_0 = x^2 + b_K xy + c_K y^2 \) be the principal form of discriminant \( d_K \) given in (26). This is the reduced representative of positive definite binary quadratic forms of discriminant \( d_K \) that represent 1. And, for a prime \( p \) let \( W_{K, p^n} \) be the inverse limit of \( W_{K, p^n} \) (\( n \geq 1 \)) as a subgroup of \( GL_2(\mathbb{Z}_p) \). We shall revisit a part of his work by analyzing a representation of \( Gal(T_{p^n}/\mathbb{Q}(j(E_{J_K}))) \) into \( GL_2(\mathbb{Z}/p^n\mathbb{Z}) \) (Theorem 7.4).

**Theorem B.** Assume that \( K \) is different from \( \mathbb{Q}(\sqrt{-1}) \) and \( \mathbb{Q}(\sqrt{-3}) \). Let

\[
\widehat{W}_{K, p^\infty} = \left< W_{K, p^\infty}, \begin{bmatrix} 1 & b_K \\ 0 & -1 \end{bmatrix} \right> \subseteq GL_2(\mathbb{Z}_p).
\]

Then, the image of the \( p \)-adic Galois representation

\[
\rho_{p^\infty} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}(j(E_{J_K}))) \to GL_2(\mathbb{Q}_p)
\]

attached to the elliptic curve \( E_{J_K} \) is a subgroup of \( \widehat{W}_{K, p^\infty} \) of index 1 or 2. Moreover, if \( p \) is an odd prime for which it does not split in \( K \) and \( [K(p) : H_K] \) is even, then the image of \( \rho_{p^\infty} \) coincides with \( \widehat{W}_{K, p^\infty} \).

We shall verify in Remark 7.3 which odd primes \( p \) satisfy the hypothesis of the second part of Theorem B. It is worth noting that Bourdon and Clark [2] and Lozano–Robledo [26] independently showed the first part of Theorem B in greater generality without the assumption that \( K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}) \). The main difference between their works and this paper is that we apply the modularity criterion for Siegel functions [20, Proposition 3.1] and the concept of a Fricke family (Remark 3.2) to the special model of \( E_{J_K} \) given in (1) in order to attain Theorems A and B. By using Stevenhagen’s elegant description of the Shimura reciprocity law [33, §3], one can further develop Theorem B and derive a similar result to [26, Theorem 1.1] in terms of elliptic curves with complex multiplication by nonmaximal orders in \( K \). For the purpose, it is necessary to define the ray class fields for orders in \( K \). But we would like to omit the details to avoid complications. One may refer to the recent work of Campagna and Pengo concerning the ray class fields for orders in \( K \) [6].

Next, we want to describe finite Galois groups in view of form class groups as Hasse [14, 15] and Deuring [9] did. For a negative integer \( D \) such that \( D \equiv 0 \) or 1 (mod 4), let \( Q(D) \) be the set of primitive positive definite binary quadratic forms of discriminant \( D \). The full modular group \( SL_2(\mathbb{Z}) \) acts on the set \( Q(D) \) from the right and gives rise to the proper equivalence \( \sim \). In Disquisitiones Arithmeticae [13], Gauss introduced a beautiful composition law on \( C(D) = Q(D)/\sim \), and later Dirichlet [10] presented a different approach to the study of composition and genus theory. Letting \( C(\mathcal{O}) \) be the ideal class group of the order \( \mathcal{O} \) of discriminant \( D \) in the imaginary quadratic field \( \mathbb{Q}(\sqrt{D}) \), we also have the isomorphism

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

where \( Q(x, y) \in Q(D) \) and \( \omega_Q \) is the zero of \( Q(x, 1) \) in the complex upper half-plane [8, Theorem 7.7]. In 2004, Bhargava [1] derived a general law of composition on \( 2 \times 2 \times 2 \) cubes of integers, from which he was able to obtain Gauss’ composition law on \( C(D) \) as a simple special case.
Let $K$ be an imaginary quadratic field of discriminant $d_K$. For a positive integer $N$, let

$$Q_N(d_K) = \{ Q = ax^2 + bxy + cy^2 \in Q(d_K) \mid \gcd(a, N) = 1 \}.$$

Recently, Eum et al. [11] constructed the extended form class group $C_N(d_K) = Q_N(d_K)/\sim_N$, where the equivalence relation $\sim_N$ is induced from the congruence subgroup $\Gamma_1(N)$. They equipped $C_N(d_K)$ with a group structure so that it is isomorphic to the ray class group $\text{Cl}(NO_K)$ of $K$ modulo $NO_K$. In this paper, we shall consider the set of definite binary quadratic forms

$$Q^\pm_N(d_K) = \{ Q, -Q = (-1)Q \mid Q \in Q_N(d_K) \}$$

with a naturally extended equivalence relation $\sim_N$, and set

$$C^\pm_N(d_K) = Q^\pm_N(d_K)/\sim_N = \{ [Q]_N \mid Q \in Q^\pm_N(d_K) \}.$$

Let $\bar{c}$ be the complex conjugation on $\mathbb{C}$. Improving the result of [11] we shall show that $C^\pm_N(d_K)$ can be regarded as a group isomorphic to $\text{Gal}(K(N)/\mathbb{Q})$ (Theorem 9.2):

**Theorem C.** The set $C^\pm_N(d_K)$ can be given a group structure isomorphic to $\text{Gal}(K(N)/\mathbb{Q})$ so that it contains $C_N(d_K)$ as a subgroup and the element $[-Q_0]_N$ corresponds to $\bar{c}|_{K(N)}$.  

By $F_N$, we mean the field of meromorphic modular functions for the principal congruence subgroup $\Gamma(N)$ whose Fourier coefficients belong to the $N$th cyclotomic field. We shall define the definite form class invariants $f([Q]_N)$ for $Q \in Q^\pm_N(d_K)$ and $f \in F_N$ (Definition 9.4), and show that these invariants satisfy a natural transformation rule via the isomorphism $\phi^\pm_N$ in (29) established in the proof of Theorem C (Theorem 9.6):

**Theorem D.** Let $Q, Q' \in Q^\pm_N(d_K)$ and $f \in F_N$. If $f([Q]_N)$ is finite, then

$$\phi^\pm_N([Q']_N)(f([Q]_N)) = f([Q']_N[Q]_N).$$

Note that Theorem D is a generalization of the transformation formula of Siegel–Ramachandra invariants, defined by the singular values of Siegel functions, via the Artin map [30] or [20, Chapter 11].

### 2 Elliptic Curves with Complex Multiplication

In this section, we shall find models for elliptic curves with complex multiplication which will be used for Theorem B on $p$-adic Galois representations.

For a lattice $\Lambda$ in $\mathbb{C}$, let $E/\mathbb{C}$ be an elliptic curve that is complex analytically isomorphic to $\mathbb{C}/\Lambda$. Then $E$ has an affine model in Weierstrass form

$$E : y^2 = 4x^3 - g_2x - g_3,$$  

(2)
where \( g_2 = g_2(\Lambda) \) and \( g_3 = g_3(\Lambda) \) are the usual scaled Eisenstein series [32, §VI.3]. Furthermore, the map

\[
\begin{align*}
\mathbb{C}/\Lambda & \rightarrow E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}) \\
z + \Lambda & \mapsto [g(\Lambda) : g'(z + \Lambda) : 1]
\end{align*}
\]

is an isomorphism of complex Lie groups, where \( g(\cdot; \Lambda) : \mathbb{C} \rightarrow \mathbb{C} \cup \{\infty\} \) is the Weierstrass \( g \)-function for the lattice \( \Lambda \) which is even. Letting \( j = j(E) = j(\Lambda) \), the \( j \)-invariant of \( E \), we set

\[
J = \frac{1}{1728}j = \frac{g_2^3}{\Delta} \quad \text{with} \quad \Delta = \Delta(\Lambda) = g_2^3 - 27g_3^2 \neq 0.
\]

In particular, if \( J \neq 0, 1 \) and so \( g_2, g_3 \neq 0 \), then one can obtain by (2) and (3) another model and parametrization of \( E \) in such a way that

\[
\begin{align*}
\mathbb{C}/\Lambda & \sim E(\mathbb{C}) : y^2 = 4x^3 - J(J - 1)27x - J(J - 1)^2 \\
z + \Lambda & \mapsto \left[ \frac{g_2g_3}{\Delta} \mathcal{g}(z + \Lambda) : \sqrt[3]{\left( \frac{g_2g_3}{\Delta} \right)^3} \mathcal{g}'(z + \Lambda) : 1 \right].
\end{align*}
\]

Here, we take the principal branch for \( \sqrt[3]{\left( \frac{g_2g_3}{\Delta} \right)^3} \).

Let \( K \) be an imaginary quadratic field and \( \mathcal{O}_K \) be its ring of integers. Let

\[
\tau_K = \begin{cases} 
-1 + \sqrt{d_K} & \text{if } d_K \equiv 1 \pmod{4}, \\
2 \sqrt{d_K} & \text{if } d_K \equiv 0 \pmod{4},
\end{cases}
\]

and so \( \mathcal{O}_K = [\tau_K, 1] = \mathbb{Z}\tau_K + \mathbb{Z} \). If we put \( \Lambda = \mathcal{O}_K \), then \( E \) has complex multiplication by \( \mathcal{O}_K \) [32, Theorem 4.1 in Chapter VI]. Moreover, if \( K \) is different from \( \mathbb{Q}(\sqrt{-1}) \) and \( \mathbb{Q}(\sqrt{-3}) \), then \( J(\mathcal{O}_K) \neq 0, 1 \) by the homogeneity of \( g_2(\Lambda) \) and \( g_3(\Lambda) \) [8, p. 193]. In this case, we let \( J_K = J(\mathcal{O}_K) \) and denote by \( E_{J_K} \) the elliptic curve with the model and parametrization described in (4). For \( \mathbf{v} = [v_1 \ v_2] \in M_{1,2}(\mathbb{Q}) \ \setminus \ M_{1,2}(\mathbb{Z}) \), let

\[
\begin{align*}
X_{\mathbf{v}} &= \frac{g_2(\mathcal{O}_K)g_3(\mathcal{O}_K)}{\Delta(\mathcal{O}_K)} \mathcal{g}(v_1\tau_K + v_2; \mathcal{O}_K), \\
Y_{\mathbf{v}} &= \sqrt[3]{\left( \frac{g_2(\mathcal{O}_K)g_3(\mathcal{O}_K)}{\Delta(\mathcal{O}_K)} \right)^3} \mathcal{g}'(v_1\tau_K + v_2; \mathcal{O}_K).
\end{align*}
\]

For convenience, we set

\[
X_{\mathbf{v}} = 0, \ Y_{\mathbf{v}} = 1 \quad \text{for } \mathbf{v} \in M_{1,2}(\mathbb{Z}).
\]

By the fundamental properties of the Weierstrass \( g \)-function, we get the following lemma.
Lemma 2.1. Let \( \mathbf{u}, \mathbf{v} \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z}) \).

(i) \( X_\mathbf{u} = X_\mathbf{v} \) if and only if \( \mathbf{u} \equiv \pm \mathbf{v} \pmod{M_{1,2}(\mathbb{Z})} \).

(ii) \( Y_{-\mathbf{v}} = -Y_\mathbf{v} \) and \( Y_{\mathbf{v} + \mathbf{n}} = Y_\mathbf{v} \) for \( \mathbf{n} \in M_{1,2}(\mathbb{Z}) \).

(iii) \( Y_\mathbf{v} = 0 \) if and only if \( 2\mathbf{v} \in M_{1,2}(\mathbb{Z}) \).

Proof. See [8, §10.A]. \( \square \)

For a positive integer \( N \), let \( E_{j_k}[N] \) be the subgroup of \( E_{j_k}(\mathbb{C}) \) consisting of \( N \)-torsion points. Then we have

\[
E_{j_k}[N] = \{[X_0 : Y_0 : 0] \cup \{[X_\mathbf{v} : Y_\mathbf{v} : 1] \mid \mathbf{v} \neq 0 \text{ and } N\mathbf{v}_1, N\mathbf{v}_2 \in \{0, 1, \ldots, N-1\}\}.
\]

3 | MODULAR FUNCTIONS

We shall introduce some meromorphic modular functions which will help us examine the extension field of \( \mathbb{Q} \) generated by the coordinates of \( N \)-torsion points on \( E_{j_k} \).

The modular group \( \text{SL}_2(\mathbb{Z}) \) acts on the complex upper half-plane \( \mathbb{H} \) by fractional linear transformations, that is,

\[
\gamma(\tau) = \frac{a\tau + b}{c\tau + d} \quad \text{with} \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}), \, \tau \in \mathbb{H}.
\]

Let \( j \) be the elliptic modular function defined on \( \mathbb{H} \), namely,

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

Then the map \( \text{SL}_2(\mathbb{Z}) \setminus \mathbb{H} \to \mathbb{C} \) sending an orbit of \( \tau \) to \( j(\tau) \) is a well-defined bijection [23, Theorem 4 in Chapter 3]. For \( \mathbf{v} = [v_1 \ v_2] \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z}) \), the Fricke function \( f_\mathbf{v} \) on \( \mathbb{H} \) is given by

\[
f_\mathbf{v}(\tau) = -2735 \frac{g_2([\tau, 1])g_3([\tau, 1])}{\Delta([\tau, 1])} g(\mathbf{v}_1\tau + \mathbf{v}_2; [\tau, 1]) \quad (\tau \in \mathbb{H}).
\]

(7)

Note that if \( \mathbf{u}, \mathbf{v} \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z}) \) such that \( \mathbf{u} \equiv \pm \mathbf{v} \pmod{M_{1,2}(\mathbb{Z})} \), then two functions \( f_\mathbf{u} \) and \( f_\mathbf{v} \) are equal. For a positive integer \( N \), let

\[
F_N = \begin{cases} Q(j) & \text{if } N = 1, \\ Q(j, f_\mathbf{v}) & \mathbf{v} \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z}) \text{ such that } N\mathbf{v} \in M_{1,2}(\mathbb{Z}) \end{cases} \text{ if } N \geq 2.
\]

Then \( F_N \) is a Galois extension of \( F_1 \) whose Galois group is isomorphic to \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \) [29, Theorem 6.6]. And, \( F_N \) coincides with the field of meromorphic modular functions for the principal congruence subgroup

\[
\Gamma(N) = \{\alpha \in \text{SL}_2(\mathbb{Z}) \mid \alpha \equiv I_2 \pmod{NM_2(\mathbb{Z})}\}.
\]
whose Fourier coefficients belong to the $N$th cyclotomic field $\mathbb{Q}(\zeta_N)$ with $\zeta_N = e^{2\pi i/N}$ [29, Proposition 6.9].

We further observe that the group $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ can be decomposed as

$$\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} = \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \cdot G_N = G_N \cdot \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\},$$

where $G_N$ is the subgroup of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ given by

$$G_N = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \right\} = \text{the class of } \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \text{ in } \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \mid d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$  

The action of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ ($\cong \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$) on $\mathbb{Q}(\zeta_N)$ can be explained as follows: first, if $\sigma$ is an element of $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ obtained from a matrix $\gamma$ in $\text{SL}_2(\mathbb{Z})$, then its action on $F_N$ is

$$f^{\sigma} = f \circ \gamma \quad (f \in F_N).$$  

Second, if $\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}$ is an element of $G_N$ with $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $f \in F_N$ has Fourier expansion

$$f(\tau) = \sum_{n \gg -\infty} c(n)q^{n/N} \quad (c(n) \in \mathbb{Q}(\zeta_N), \quad q = e^{2\pi i\tau})$$

(here, $n \gg -\infty$ means that there are only finitely many negative integers $n$ in the above summation), then

$$f\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}(\tau) = \sum_{n \gg -\infty} c(n)\sigma_d q^{n/N}$$

where $\sigma_d$ is the automorphism of $\mathbb{Q}(\zeta_N)$ given by $\zeta_N \mapsto \zeta_N^d$.

Meanwhile, 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

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

where $q_z = e^{2\pi iz}$ with $z = v_1\tau + v_2$ and $B_2(x) = x^2 - x + 1/6$ is the second Bernoulli polynomial. Note that $g_v$ has neither a zero nor a pole on $\mathbb{H}$. One can refer to [30] or [20] for further details on Siegel functions.

**Proposition 3.1.** For $N \geq 2$, let $\{m(v)\}_{v \in (1/N)M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})}$ be a family of integers such that $m(v) = 0$ except for finitely many $v$. Then the finite product

$$\prod_v g_v^{m(v)}$$

is a meromorphic modular function for $\Gamma(N)$ if
\[
\sum_v m(v)(Nv_1)^2 \equiv \sum_v m(v)(Nv_2)^2 \equiv 0 \pmod{N \gcd(2, N)},
\]
\[
\sum_v m(v)(Nv_1)(Nv_2) \equiv 0 \pmod{N},
\]
\[
\sum_v m(v) \gcd(12, N) \equiv 0 \pmod{12}.
\]

**Proof.** See [20, Theorems 5.2 and 5.3].

Remark 3.2. We say that \( v \in M_{1,2}(\mathbb{Q}) \) is primitive modulo \( N \) \((\geq 2)\) 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 vectors \( v \). As mentioned in [20, p. 33], a family \( \{ h_v \}_{v \in V_N} \) of functions in \( F_N \) is called a Fricke family of level \( N \) if:

(i) \( h_v \) is holomorphic on \( \mathbb{H} \) for every \( v \in V_N \);

(ii) \( h_u = h_v \) whenever \( u, v \in V_N \) satisfy \( u \equiv \pm v \pmod{M_{1,2}(\mathbb{Z})} \);

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

As is well known, \( \{ f_v \}_{v \in V_N} \) and \( \{ g_{12N} v \}_{v \in V_N} \) are Fricke families of level \( N \) [29, Theorem 6.6] and [20, Proposition 1.3 in Chapter 2]. In [17] and [19] Jung et al. examined several properties and applications to class field theory of these typical examples of a Fricke family.

**Lemma 3.3.** If \( v = \begin{bmatrix} v_1 & v_2 \end{bmatrix} \in M_{1,2}(\mathbb{Q}) \) such that \( 2v \notin M_{1,2}(\mathbb{Z}) \), then
\[
\wp'(v_1 \tau + v_2; [\tau, 1]) = -\eta(\tau)^6 \frac{g_{2N}(\tau)}{g_v(\tau)^4} \quad (\tau \in \mathbb{H})
\]
where \( \eta \) is the Dedekind \( \eta \)-function on \( \mathbb{H} \) defined by
\[
\eta(\tau) = \sqrt{2\pi\xi} \prod_{n=1}^{\infty} (1 - q^n) \quad (\tau \in \mathbb{H}).
\]

**Proof.** See [21, p. 852].

4 \quad THE SHIMURA RECIPROCITY LAW

Let \( K \) be an imaginary quadratic field of discriminant \( d_K \) \((< 0)\). In this section, we shall introduce a description of \( \text{Gal}(K_{(p^\infty)}/H_K) \) for a prime \( p \) due to Stevenhagen [33].

By the classical theory of complex multiplication established by Kronecker et al., we have
\[
H_K = K(j(\mathcal{O}_K)) = K(j(\tau_K)),
\]
\[
K_{(N)} = K(f(\tau_K) \mid f \in F_N \text{ is finite at } \tau_K)
\]
for a positive integer \( N \) [23, Theorem 1 and Corollary to Theorem 2 in Chapter 10]. Shimura revisited this result by developing the theory of canonical models for modular curves and the reciprocity law [29, Theorem 6.31, Proposition 6.33]. Let \( \min(\tau_K, \mathbb{Q}) = x^2 + b_K x + c_K \in \mathbb{Z}[x] \), and
let

\[ W_{K,N} = \left\{ \gamma = \begin{bmatrix} t - b_K s & -c_K s \\ s & t \end{bmatrix} \mid s, t \in \mathbb{Z}/N\mathbb{Z} \text{ such that } \gamma \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \right\} \] (12)

which is the Cartan subgroup of \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \) associated with the \((\mathbb{Z}/N\mathbb{Z})\)-algebra \( \mathcal{O}_K/N\mathcal{O}_K \) with the ordered basis \( \{ \tau_K + N\mathcal{O}_K, 1 + N\mathcal{O}_K \} \). And, let

\[ U_K = \begin{cases} \{ \pm I_2 \} & \text{if } K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}), \\ \{ \pm I_2, \pm \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \} & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ \{ \pm I_2, \pm \begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \} & \text{if } K = \mathbb{Q}(\sqrt{-3}) \end{cases} \]

which is a subgroup of \( \text{SL}_2(\mathbb{Z}) \). If \( r_N : \text{SL}_2(\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) \) denotes the reduction modulo \( N \), then \( r_N(U_K) \) is a subgroup of \( W_{K,N} \). The following proposition done by Stevenhagen gives a simple description of a part of the Shimura reciprocity law.

**Proposition 4.1.** In relation to (11), we have a surjection

\[
W_{K,N} \to \text{Gal}(K(N)/H_K)
\]

\[
\gamma \mapsto (f(\tau_K) \mapsto f^{[\gamma]}(\tau_K) \mid f \in \mathcal{F}_N \text{ is finite at } \tau_K)
\]

whose kernel is \( r_N(U_K) \). Here, \([\gamma]\) means the image of \( \gamma \) in \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{ \pm I_2 \} \) \((\simeq \text{Gal}(\mathcal{F}_N/\mathcal{F}_1))\).

**Proof.** See [33, §3].

We let

\[
\psi_N : W_{K,N} \to \text{Gal}(K(N)/H_K)
\]

be the surjection introduced in (13). For each prime \( p \), let

\[ W_{K,p^\infty} = \left\{ \gamma = \begin{bmatrix} t - b_K s & -c_K s \\ s & t \end{bmatrix} \mid s, t \in \mathbb{Z}_p \text{ such that } \gamma \in \text{GL}_2(\mathbb{Z}_p) \right\} \]

which is a subgroup of \( \text{GL}_2(\mathbb{Z}_p) \). The following corollary was shown in [33, (3.2) and (4.3)], however, we shall briefly give its proof in order to compare with Theorem 7.4.

**Corollary 4.2.** Let \( p \) be a prime, and let \( K_{(p^\infty)} \) be the maximal abelian extension of \( K \) unramified outside prime ideals lying above \( p \). Then \( \text{Gal}(K_{(p^\infty)}/H_K) \) is isomorphic to \( W_{K,p^\infty}/U_K \).
Proof. By the fact that \( \text{Gal}(\mathbb{F}_p^n/\mathbb{F}_1) \simeq \text{GL}_2(\mathbb{Z}/p^n \mathbb{Z})/\{\pm I_2\} \) \((n \geq 1)\) and Proposition 4.1, we derive the inverse system of short exact sequences as in Figure 1 in which the first and second vertical maps are reductions and the third vertical maps are restrictions.

Since the inverse system \( \{r_{p^n}(U_K)\}_{n \geq 1} \) satisfies the Mittag–Leffler condition [25, p. 164], we get the exact sequence [25, Proposition 10.3]. Moreover, since

\[
\lim_{n \to \infty} r_{p^n}(U_K) \simeq U_K (\hookrightarrow W_{K, p^\infty}),
\]

\[
\lim_{n \to \infty} r_{p^n}(U_K) \simeq U_K (\hookrightarrow W_{K, p^\infty}),
\]

\[
\lim_{n \to \infty} \text{Gal}(K(p^n)/H_K) \simeq \text{Gal}(\bigcup_{n \geq 1} K(p^n)/H_K) = \text{Gal}(K(p^\infty)/H_K),
\]

we conclude that \( \text{Gal}(K(p^\infty)/H_K) \) is isomorphic to \( W_{K, p^\infty}/U_K \).

Proposition 4.3. Assume \( K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}) \) and \( N \geq 2 \).

(i) We have

\[
K_N = H_K \left( X_{[0, \frac{1}{N}]} \right) = H_K \left( X_v \mid v \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}) \right),
\]

where \( X_v \) is the \( x \)-coordinate function defined in \( \S 2 \) (5).

(ii) We find that

\[
X_v^{\psi_N(y)} = X_{vy} \left( v \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}), y \in W_{K,N} \right).
\]
Proof. We note by the definition (7) of a Fricke function that

$$X_{\nu} = -\frac{1}{2^{35}} f_\nu(\tau_K) \quad (\nu \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})).$$  \hspace{1cm} (14)

(i) For the first equality, see (10) and [23, Corollary to Theorem 7 in Chapter 10]. The second equality follows from (11) and the fact $f_\nu \in F_N$.

(ii) This follows from Remark 3.2 and Proposition 4.1. \hfill \Box

Remark 4.4.

(i) Proposition 4.3(i) is a consequence of the main theorem of the theory of complex multiplication. By using the Kronecker limit formula and some arithmetic properties of Fricke functions, Jung et al. [18] and [22] improved Proposition 4.3(i) so that

$$K_{(N)} = K\left(X[0 \frac{1}{N}\right] \quad \text{or} \quad K_{(N)} = K\left(X[0 \frac{2}{N}\right],$$

which gives a partial answer to the problem of Hasse and Ramachandra [12, p. 91] and [27, p. 105].

(ii) Let $K$ be an arbitrary imaginary quadratic field, and let $E$ be the elliptic curve given by the Weierstrass equation

$$E : y^2 = 4x^3 - g_2 x - g_3,$$

where $g_2 = g_2(O_K)$ and $g_3 = g_3(O_K)$. The Weber function $h : E \rightarrow \mathbb{P}^1(\mathbb{C})$ is defined by

$$h(\varphi(z)) = \begin{cases} \frac{g_2 g_3}{\Delta} x & \text{if } K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}), \\ \frac{g_2^2}{\Delta} x^2 & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ \frac{g_3}{\Delta} x^3 & \text{if } K = \mathbb{Q}(\sqrt{-3}) \end{cases} \quad (z \in \mathbb{C})$$

where $\varphi : \mathbb{C}/O_K \rightarrow E$ is the parametrization given in (3) and $\Delta = g_2^3 - 27 g_3^2$. This function gives rise to an isomorphism of the quotient variety $E/\text{Aut}(E)$ onto $\mathbb{P}^1(\mathbb{C})$ [23, Theorem 7 in Chapter 1]. Originally, [23, Corollary to Theorem 7 in Chapter 10] states

$$K_{(N)} = H_K(h(\varphi(z)) \mid z \in \mathbb{C} \setminus O_K \text{ satisfies } N z \in O_K).$$

We note that if $K$ is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, then

$$X_{\nu} = h(\varphi(v_1 \tau_K + v_2)) \quad (\nu = [v_1 \ v_2] \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})).$$
5 | THE FIELD GENERATED BY N-TORSION POINTS

Unless otherwise specified we assume that $K$ is an imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, and $N$ is a positive integer such that $N \geq 2$. Let $\mathbb{Q}(E_{jk}[N])$ be the extension field of $\mathbb{Q}$ generated by the coordinates of $N$-torsion points on $E_{jk}[N]$, namely,

$$\mathbb{Q}(E_{jk}[N]) = \mathbb{Q}\left(X_v, Y_v \mid v \in \frac{1}{N}M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})\right).$$

We shall describe the field $\mathbb{Q}(E_{jk}[N])$ by comparing it with the ray class field $K_{(N)}$ (Theorem A).

Lemma 5.1. Let $\{h_v\}_{v \in V_N}$ be a Fricke family defined in Remark 3.2. For each $v \in V_N$, we have

$$\overline{h_v}(\tau_K) = h_v \left[ \begin{array}{cc} 1 & b_k \\ 0 & -1 \end{array} \right](\tau_K),$$

where $\overline{\cdot}$ means the complex conjugation.

Proof. See [20, Proposition 1.4 in Chapter 2].

Recall the relation (14) and the fact that $\{f_v\}_{v \in V_N}$ is a Fricke family of level $N$ as mentioned in Remark 3.2. Let

$$R_N = \mathbb{Q}\left(X_v \mid v \in \frac{1}{N}M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})\right).$$

Lemma 5.2. The field $R_N$ can be described as follows.

(i) If $d_K \equiv 0 \pmod{4}$, then $R_2$ is the maximal real subfield of $K_{(2)}$ with $[K_{(2)} : R_2] = 2$.

(ii) If $N \geq 3$ or $d_K \equiv 1 \pmod{4}$, then $R_N = K_{(N)}$.

Proof.

(i) If $d_K \equiv 0 \pmod{4}$, then we have $b_k = 0$ and

$$\overline{X_v} = X_v \left[ \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right] \text{ by Lemma 5.1} \quad \left( v \in \frac{1}{2}M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}) \right)$$

$$= X_v \text{ by Lemma 2.1 (i)}.$$

This shows that $R_2$ is contained in $\mathbb{R}$. Moreover, we get by Remark 4.4(i) that $KR_2 = K_{(2)}$. Thus we obtain that $[K_{(2)} : R_2] = 2$ and $R_2$ is the maximal real subfield of $K_{(2)}$.

(ii) Now, we assume that $N \geq 3$ or $d_K \equiv 1 \pmod{4}$. We derive by Lemmas 5.1 and 2.1 (i) that if $N \geq 3$ and $d_K \equiv 0 \pmod{4}$, then $b_k = 0$ and

$$\overline{X_{\left[ \frac{1}{N} \frac{1}{3} \right]}} = X_{\left[ \frac{1}{N} \frac{1}{3} \right]} \neq X_{\left[ \frac{1}{N} \frac{1}{3} \right]},$$
and if $d_K \equiv 1 \pmod{4}$, then $b_K = 1$ and

$$X_{\left[ \frac{1}{N}, 0 \right]} = X_{\left[ \frac{1}{N}, 1 \right]} \neq X_{\left[ \frac{1}{N}, 0 \right]}.$$  

This observation shows that

$$R_N \not\subseteq \mathbb{R}. \quad (15)$$  

On the other hand, we note by Lemma 5.1 that

$$X_{\left[ 0, \frac{1}{N} \right]} \in \mathbb{R} \quad \text{for all } t \in \mathbb{Z} \text{ such that } t \not\equiv 0 \pmod{N}. \quad (16)$$  

Thus, if we let

$$F = \mathbb{Q}\left(X_{\left[ 0, \frac{1}{N} \right]} \mid t \in \mathbb{Z} \text{ satisfies } t \not\equiv 0 \pmod{N}\right),$$

then we get by Proposition 4.3 (i), Remark 4.4 (i), (15) and (16) that

$$KF = K(N) \supseteq R_N \supseteq R_N \cap \mathbb{R} \supseteq F.$$  

Moreover, since $[KF : F] = 2$ by (16), we conclude that $R_N = K(N)$.

Lemma 5.3. If $u, v \in \frac{1}{N}M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})$ such that $2v \notin M_{1,2}(\mathbb{Z})$, then $\frac{Y_u}{Y_v}$ lies in $K(N)$.

**Proof.** Observe first that $Y_v \neq 0$ by Lemma 2.1(iii). If $2u \in M_{1,2}(\mathbb{Z})$, then the assertion is straightforward because $Y_u = 0$ again by Lemma 2.1(iii). Now, assume that $2u \notin M_{1,2}(\mathbb{Z})$. We assert by Lemma 3.3 and the definition (6) that

$$\frac{Y_u}{Y_v} = g(\tau_K) \quad \text{with} \quad g = \frac{g_u g_v^4}{g_u^4 g_{2v}}.$$  

If we set the family $\{m(a)\}_{a \in (1/N)M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})}$ of integers so that

$$\sum_a m(a) \cdot (a) = 1 \cdot (2u) + 4 \cdot (v) + (4) \cdot (u) + (-1) \cdot (2v)$$

in the free abelian group generated by the set $(1/N)M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})$, then we see that $\{m(a)\}_a$ satisfy the three conditions in Proposition 3.1. Hence $g$ is a meromorphic modular function for $\Gamma(N)$ by Proposition 3.1. Moreover, the infinite product expression of a Siegel function given in (9) shows that $g$ belongs to $F_N$. Therefore we conclude by (11) that $g(\tau_K)$ belongs to $K(N)$.

We have the following description of the field $\mathbb{Q}(E_{\sqrt{K}}[N])$ in comparison with $K(N)$.  

Theorem 5.4. Assume that $K$ is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Let $T_N = \mathbb{Q}(E_{J_K}[N])$.

(i) If $d_K \equiv 0 \pmod{4}$, then $T_2$ is the maximal real subfield of $K(2)$ with $[K(2) : T_2] = 2$.

(ii) If $d_K \equiv 1 \pmod{4}$, then $T_2 = K(2)$.

(iii) If $N \geq 3$, then $T_N$ is an extension field of $K(N)$ with $[T_N : K(N)] \leq 2$.

Proof. Note by Lemma 2.1(iii) that

$$T_2 = R_2. \quad (17)$$

(i) If $d_K \equiv 0 \pmod{4}$, then (17) and Lemma 5.2(i) yield that $T_2$ is the maximal real subfield of $K(2)$ with $[K(2) : T_2] = 2$.

(ii) If $d_K \equiv 1 \pmod{4}$, then (17) and Lemma 5.2(ii) show that $T_2 = K(2)$.

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

$$T_N = K(N)\left(Y_v \mid v \in \frac{1}{N}M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})\right) \quad \text{by Lemma 5.2(ii)}$$

$$= K(N)\left(Y_{\left[0 \frac{1}{N}\right]}\right) \quad \text{by Lemma 5.3.}$$

It then follows from the relation

$$Y_{\left[0 \frac{1}{N}\right]}^2 = 4X_{\left[0 \frac{1}{N}\right]}^3 - \frac{J(J-1)}{27}X_{\left[0 \frac{1}{N}\right]} - J\left(\frac{J-1}{27}\right)^2$$

and Proposition 4.3(i) that $[T_N : K(N)] \leq 2$. \[\square\]

Remark 5.5. Since $j(E_{J_K}) = j(O_K) \in \mathbb{R}$ \[31, p. 179\], we get by (10), (11) and Theorem 5.4 that

$$T_N \supseteq \mathbb{Q}(j(E_{J_K})).$$

6 REPRESENTATIONS ATTACHED TO ELLIPTIC CURVES

By using the Shimura reciprocity law, we shall determine the image of a 2-dimensional representation of $\text{Gal}(T_N / \mathbb{Q}(j(E_{J_K})))$ attached to $E_{J_K}$.

Since $E_{J_K}$ is defined over $\mathbb{Q}(j(E_{J_K}))$, the field $T_N = \mathbb{Q}(E_{J_K}[N])$ is a finite Galois extension of $\mathbb{Q}(j(E_{J_K}))$ by Theorem 5.4, Remark 5.5 and \[32, pp. 53–54\]. So we have the usual (right) action of $\text{Gal}(T_N / \mathbb{Q}(j(E_{J_K})))$ on the $\mathbb{Z}/N\mathbb{Z}$-module $E_{J_K}[N]$. From this action, we achieve the faithful representation

$$\rho_N : \text{Gal}(T_N / \mathbb{Q}(j(E_{J_K}))) \to GL_2(\mathbb{Z}/N\mathbb{Z}) \simeq \text{Aut}(E_{J_K}[N])$$

with respect to the ordered basis

$$B = \left\{ [X_{\left[0 \frac{1}{N}\right]} : Y_{\left[0 \frac{1}{N}\right]} : 1], [X_{\left[0 \frac{1}{N}\right]} : Y_{\left[0 \frac{1}{N}\right]} : 1] \right\}$$
for $E_{J_K}[N]$ so that

$$[X_v : Y_v : 1] = [X_{v \rho_N(\sigma)} : Y_{v \rho_N(\sigma)} : 1] \quad (v \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z})).$$  \hfill (18)

**Lemma 6.1.** Let $\beta \in M_2(\mathbb{Z})$ such that $\gcd(\det(\beta), N) = 1$. If

$$v \beta \equiv \pm v \pmod{M_{1,2}(\mathbb{Z})} \quad \text{for each} \quad v \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}),$$  \hfill (19)

then $\beta \equiv \pm I_2 \pmod{NM_2(\mathbb{Z})}$.

**Proof.** We deduce by putting $v = \left[ \begin{array}{cc} 1/N & 0 \\ 0 & 1/N \end{array} \right]$ and $\left[ \begin{array}{cc} 0 & 1/N \\ 1/N & 0 \end{array} \right]$ in (19) that

$$\beta \equiv \pm \left[ \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right] \pmod{NM_2(\mathbb{Z})}.$$  \hfill □

Then we get the assertion by letting $v = \left[ \begin{array}{cc} 1/N & 1/N \end{array} \right]$ in (19).

Now we denote by $c$ the complex conjugation on $\mathbb{C}$.

**Lemma 6.2.** We have

$$\rho_N(c|_{T_N}) = \left[ \begin{array}{cc} 1 & b_K \\ 0 & -1 \end{array} \right] \text{ or } -\left[ \begin{array}{cc} 1 & b_K \\ 0 & -1 \end{array} \right].$$

**Proof.** Let $\alpha = \rho_N(c|_{T_N}) (\in \text{GL}_2(\mathbb{Z}/N\mathbb{Z}))$. We find by (18) and Lemma 5.1 that

$$X_{v \alpha} = X_v \left[ \begin{array}{cc} 1/b_K \\ 0 \end{array} \right] \left( v \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}) \right).$$

And we obtain by Lemma 2.1 (i) that

$$v \alpha \equiv \pm \left[ \begin{array}{cc} 1 & b_K \\ 0 & -1 \end{array} \right] \pmod{M_{1,2}(\mathbb{Z})} \quad \text{for each} \quad v \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}).$$

Thus, it follows from Lemma 6.1 that

$$\alpha = \rho_N(c|_{T_N}) = \left[ \begin{array}{cc} 1 & b_K \\ 0 & -1 \end{array} \right] \text{ or } -\left[ \begin{array}{cc} 1 & b_K \\ 0 & -1 \end{array} \right].$$  \hfill □

Let $W_{K,N}$ be the subgroup of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ given in (12), and define

$$\hat{W}_{K,N} = \left\langle W_{K,N}, \left[ \begin{array}{cc} 1 & b_K \\ 0 & -1 \end{array} \right] \right\rangle.$$
as a subgroup of $GL_2(\mathbb{Z}/N\mathbb{Z})$. We then see that

\[
\left[\tilde{W}_{K,N} : W_{K,N}\right] = \begin{cases} 
1 & \text{if } N = 2 \text{ and } d_K \equiv 0 \pmod{4}, \\
2 & \text{otherwise}.
\end{cases}
\] (20)

**Theorem 6.3.** Assume that $K$ is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. The image of $\rho_N$ is a subgroup of $\tilde{W}_{K,N}$ of index

\[
\left[\tilde{W}_{K,N} : \rho_N(\text{Gal}(T_N/\mathbb{Q}(j(E_{J_K}))))\right] = \begin{cases} 
1 & \text{if } N = 2, \\
1 \text{ or } 2 & \text{if } N \geq 3.
\end{cases}
\]

**Proof.** Let $\sigma \in \text{Gal}(T_N/\mathbb{Q}(j(E_{J_K})))$. If we let $\gamma = \rho_N(\sigma)$, then we derive by (18) that

\[X^\sigma_v = X_{v\gamma} \quad \left( v \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}) \right).
\]

On the other hand, we achieve by Propositions 4.1, 4.3 (ii) and Lemma 6.2 that

\[X^\sigma_v = X_{v\alpha} \quad \text{for some } \alpha \in \tilde{W}_{K,N} \quad \left( v \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}) \right),
\]

and hence

\[X_{v\gamma} = X_{v\alpha}.
\]

Therefore we attain by Lemma 2.1 (i) that

\[v\gamma \equiv \pm v\alpha \pmod{M_{1,2}(\mathbb{Z})} \quad \text{for each } v \in \frac{1}{N} M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}),
\]

from which we have by Lemma 6.1 that

\[\gamma = \pm \alpha \quad \text{in } GL_2(\mathbb{Z}/N\mathbb{Z}).
\]

This yields that $\rho_N(\text{Gal}(T_N/\mathbb{Q}(j(E_{J_K}))))$ is a subgroup of $\tilde{W}_{K,N}$. Furthermore, we find that

\[
|\rho_N(\text{Gal}(T_N/\mathbb{Q}(j(E_{J_K}))))| = |\text{Gal}(T_N/\mathbb{Q}(j(E_{J_K}))))| \quad \text{because } \rho_N \text{ is injective}
\]

\[
= \begin{cases} 
|\text{Gal}(K(2)/H_K)| & \text{if } N = 2 \text{ and } d_K \equiv 0 \pmod{4}, \\
2|\text{Gal}(K(2)/H_K)| & \text{if } N = 2 \text{ and } d_K \equiv 1 \pmod{4}, \\
2|\text{Gal}(K(\mathbb{N})/H_K)| \text{ or } 4|\text{Gal}(K(\mathbb{N})/H_K)| & \text{if } N \geq 3
\end{cases}
\]

by (10) and Theorem 5.4
\[ |W_{K,N}/\{\pm I_2\}| = \begin{cases} 1 & \text{if } N = 2 \text{ and } d_K \equiv 0 \pmod{4}, \\ 2 & \text{if } N = 2 \text{ and } d_K \equiv 1 \pmod{4}, \\ 2 \text{ or } 4 & \text{if } \ N \geq 3 \end{cases} \]

by Proposition 4.1

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

\[ |\widehat{W}_{K,N}| = \begin{cases} 1 & \text{if } N = 2, \\ \frac{1}{2} \text{ or } 1 & \text{if } N \geq 3 \end{cases} \]

by (20).

This completes the proof. □

Remark 6.4. Consider the case where \[ [\widehat{W}_{K,N} : \rho_N(\Gal(T_{N/\mathbb{Q}(j(E_{J_K}))})] = 2, \] equivalently,

\[ N \geq 3 \quad \text{and} \quad Y[0 \ \frac{1}{N}] \in K(N). \]

If \( \rho_N(\sigma) = -I_2 \) for some \( \sigma \in \Gal(T_{N/\mathbb{Q}(j(E_{J_K}))}) \), then we get by (18), Lemma 2.1 (i) and (ii) that

\[ X^\sigma_v = X_{v(-I_2)} = X_v \quad \text{for all } v \in \frac{1}{N}M_{1,2}(\mathbb{Z}) \setminus M_{1,2}(\mathbb{Z}) \]

and

\[ Y^\sigma_{[0 \ \frac{1}{N}] = Y[0 \ \frac{1}{N}](-I_2) = -Y[0 \ \frac{1}{N}]. \]

This implies by Lemma 5.2 (ii) that \( Y_{[0 \ \frac{1}{N}] \} \) does not belong to \( K(N) \), which gives a contradiction. Therefore we must have

\[ \rho_N(\Gal(T_{N/\mathbb{Q}(j(E_{J_K}))}) \not\cong -I_2 \quad \text{and} \quad \langle \rho_N(\Gal(T_{N/\mathbb{Q}(j(E_{J_K}))}) \rangle, -I_2 \rangle = \widehat{W}_{K,N}. \]

7 \ SOME \( p \)-ADIC GALOIS REPRESENTATIONS

Let \( p \) be a prime. We shall investigate the image of a \( p \)-adic Galois representation of \( \Gal(\mathbb{Q}/\mathbb{Q}(j(E_{J_K}))) \) induced from its right action on the \( p \)-adic Tate module of the elliptic curve \( E_{J_k} \) (Theorem B).

Lemma 7.1. We have

\[ \rho_{p^n}(\Gal(T_{p^n}/\mathbb{Q}(j(E_{J_K})))) \cap \{-I_2\} = \begin{cases} \{-I_2\} & \text{for all } n \geq 1 \\ \emptyset & \text{for all } n \geq k \end{cases} \]

for some \( k \geq 1. \)
\[
\begin{align*}
\text{Gal}(T_{p^n}/\mathbb{Q}(j(E_{JK})))) & \quad \rho_{p^n} \quad \text{GL}_2(\mathbb{Z}/p^n\mathbb{Z}) \\
\text{restriction} \quad \downarrow & \quad \downarrow \text{reduction} \\
\text{Gal}(T_{p^k}/\mathbb{Q}(j(E_{JK})))) & \quad \rho_{p^k} \quad \text{GL}_2(\mathbb{Z}/p^k\mathbb{Z})
\end{align*}
\]

**Figure 2** A commutative diagram of representations \((n \geq k)\)

**Proof.** If \(\rho_{p^k}(\text{Gal}(T_{p^k}/\mathbb{Q}(j(E_{JK})))))\) does not contains \(-I_2\) for some \(k \geq 1\), then the commutative diagram in Figure 2 implies

\[
\rho_{p^n}(\text{Gal}(T_{p^n}/\mathbb{Q}(j(E_{JK})))) \cap \{-I_2\} = \emptyset \quad \text{for all } n \geq k. \quad \square
\]

**Lemma 7.2.** Let \(p\) be an odd prime for which it does not split in \(K\) and \([K_{(p)} : H_K]\) is even. Then, \(\rho_{p^n}(\text{Gal}(T_{p^n}/\mathbb{Q}(j(E_{JK}))))\) contains \(-I_2\) for every \(n \geq 1\).

**Proof.** First, note by Theorem 5.4(iii) that \(T_{p^n}\) contains \(K_{(p^n)}\). Since \(\rho_{p^n}\) is injective and

\[
|\text{Gal}(T_{p^n}/H_K)| = [T_{p^n} : K_{(p)}][K_{(p)} : H_K]
\]

is even by hypothesis, the subgroup \(\rho_{p^n}(\text{Gal}(T_{p^n}/H_K))\) of \(\rho_{p^n}(\text{Gal}(T_{p^n}/\mathbb{Q}(j(E_{JK}))))\) contains an element \(\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{GL}_2(\mathbb{Z}/p^n\mathbb{Z})\) of order 2. Here we observe that in \(M_2(\mathbb{Z}/p^n\mathbb{Z})\), \(\gamma\) satisfies

\[
\gamma^2 - (a + d)\gamma + (ad - bc)I_2 = O_2, \quad \gamma \neq I_2 \quad \text{and} \quad \gamma^2 = I_2,
\]

and so

\[
(a + d)\gamma = (1 + ad - bc)I_2. \tag{21}
\]

Now, there are two possibilities: \(a + d \not\equiv 0 \pmod{p}\) or \(a + d \equiv 0 \pmod{p}\).

Case 1. If \(a + d \not\equiv 0 \pmod{p}\), then \(\gamma\) is a scalar matrix in \(\text{GL}_2(\mathbb{Z}/p^n\mathbb{Z})\) by (21). Thus we get from the hypothesis that \(p\) is odd and the facts \(\gamma \neq I_2, \gamma^2 = I_2\) that \(\gamma = -I_2\).

Case 2. If \(a + d \equiv 0 \pmod{p}\), then by (21) we attain

\[
1 - d^2 - bc \equiv 0 \pmod{p}. \tag{22}
\]

On the other hand, since \(\rho_{p^n}(\text{Gal}(T_{p^n}/H_K))\) is a subgroup of \(W_{K,p^n}\) by Proposition 4.1 and the proof of Theorem 6.3, we have

\[
\gamma = \begin{bmatrix} t - b_Ks & -c_Ks^2 \\ s & t \end{bmatrix} \quad \text{for some} \ s, t \in \mathbb{Z}/p^n\mathbb{Z}.
\]

Thus we establish by the assumption \(a + d \equiv 0 \pmod{p}\) and (22) that

\[
(t - b_Ks) + t \equiv 0 \pmod{p} \quad \text{and} \quad 1 - t^2 + c_Ks^2 \equiv 0 \pmod{p}.
\]
It then follows from the fact \( b_K^2 - 4c_K = d_K \) that
\[
d_K s^2 \equiv 4 \pmod{p},
\]
and hence
\[
p \nmid d_K \quad \text{and} \quad \left( \frac{d_K}{p} \right) = 1
\]
because \( p \) is odd. However, this case does not happen by the hypothesis on \( p \). \( \square \)

Remark 7.3. For an odd prime \( p \), we have the degree formula
\[
[K(p) : H_K] = \begin{cases} 
(p - 1)^2 & \text{if } p \text{ splits in } K, \\
\frac{(p - 1)p}{2} & \text{if } p \text{ is ramified in } K, \\
\frac{p^2 - 1}{2} & \text{if } p \text{ is inert in } K
\end{cases}
\]
[24, Theorem 1 in Chapter VI]. So, \( p \) satisfies the hypothesis of Lemma 7.2 if and only if
\[
\begin{cases} 
p \mid d_K \\
p \equiv 1 \pmod{4}, \quad \text{or} \quad \left( \frac{d_K}{p} \right) = -1.
\end{cases}
\]

Theorem 7.4. Assume that \( K \) is different from \( \mathbb{Q}(\sqrt{-1}) \) and \( \mathbb{Q}(\sqrt{-3}) \). Let
\[
\hat{W}_{K, p} = \left\langle W_{K, p}, \begin{bmatrix} 1 & b_K \\ 0 & -1 \end{bmatrix} \right\rangle \subseteq \text{GL}_2(\mathbb{Z}_p).
\]
Then, the image of the \( p \)-adic Galois representation
\[
\rho_{p, \infty} : \text{Gal}(\overline{\mathbb{Q}} / \mathbb{Q}(j(E_{f_K}))) \to \text{GL}_2(\mathbb{Q}_p)
\]
attached to the elliptic curve \( E_{f_K} \) is a subgroup of \( \hat{W}_{K, p} \) of index 1 or 2. Moreover, if \( p \) is an odd prime for which it does not split in \( K \) and \( [K(p) : H_K] \) is even, then the image of \( \rho_{p, \infty} \) coincides with \( \hat{W}_{K, p} \).

Proof. For each \( n \geq 1 \), we get by Theorem 6.3 and Remark 6.4 that
\[
\hat{W}_{K, p^n} = \langle \rho_{p^n}(\text{Gal}(T_{p^n}/\mathbb{Q}(j(E_{f_K})))), -I_2 \rangle.
\]
(23)
Moreover, we see by Lemma 7.1 that
\[
\hat{W}_{K, p^n} = \begin{cases} 
\rho_{p^n}(\text{Gal}(T_{p^n}/\mathbb{Q}(j(E_{f_K})))) & \text{for all } n \geq 1 \\
\rho_{p^n}(\text{Gal}(T_{p^n}/\mathbb{Q}(j(E_{f_K})))) \oplus \langle -I_2 \rangle & \text{for all } n \geq k
\end{cases}
\]
for some $k \geq 1$. And we obtain by taking the inverse limit on both sides of (23) that

$$
\hat{W}_{K, p} = \left\langle \lim_{\longrightarrow \phi \not \in \text{tr}} \rho_{p^{n}}(\text{Gal}(T_{p^{n}}/\mathbb{Q}(j(E_{K})))) , -I_{2} \right\rangle \text{ in } \text{GL}_{2}(\mathbb{Z}_{p}).
$$

Let $T_{p^{\infty}} = \bigcup_{n \geq 1} T_{p^{n}}$. By composing the homomorphisms in Figure 3, we attain the $p$-adic Galois representation

$$
\rho_{p^{\infty}} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(j(E_{K}))) \rightarrow \text{GL}_{2}(\mathbb{Q}_{p})
$$

which satisfies

$$
[\hat{W}_{K, p^{\infty}} : \rho_{p^{\infty}}(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(j(E_{K}))))] = 1 \text{ or } 2.
$$

This proves the first part of the theorem.

In particular, let $p$ be an odd prime for which it does not split in $K$ and $[K_{(p)} : H_{K}]$ is even. Since $\rho_{p^{n}}(\text{Gal}(T_{p^{n}}/\mathbb{Q}(j(E_{K}))))$ contains $-I_{2}$ for all $n \geq 1$ by Lemma 7.2, we achieve by (23) that

$$
\rho_{p^{\infty}}(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(j(E_{K})))) = \lim_{\longrightarrow \phi \not \in \text{tr}} \rho_{p^{n}}(\text{Gal}(T_{p^{n}}/\mathbb{Q}(j(E_{K})))) = \hat{W}_{K, p^{\infty}}.
$$

8 | EXTENDED FORM CLASS GROUPS

From now on, we let $K$ be an arbitrary imaginary quadratic field including both $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, and let $N$ be a positive integer. We shall introduce the recent work of Eum et al. [11] on constructing a form class group isomorphic to $\text{Gal}(K_{(N)}/K)$.

Let $Q_{N}(d_{K})$ be the set of binary quadratic forms over $\mathbb{Z}$ given by

$$
Q_{N}(d_{K}) = \{ ax^{2} + bxy + cy^{2} \in \mathbb{Z}[x, y] | \gcd(a, b, c) = 1, b^{2} - 4ac = d_{K}, a > 0, \gcd(a, N) = 1 \}.
$$

Note that the conditions $b^{2} - 4ac = d_{K} < 0$ and $a > 0$ force each form in $Q_{N}(d_{K})$ to be positive definite. The congruence subgroup

$$
\Gamma_{1}(N) = \left\{ \gamma \in \text{SL}_{2}(\mathbb{Z}) | \gamma \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{NM_{2}(\mathbb{Z})} \right\}
$$
acts on the set $Q_N(d_K)$ from the right, which induces the equivalence relation $\sim_N$ as

$$Q \sim_N Q' \iff Q' = Q' = Q \left( \gamma \begin{bmatrix} x \\ y \end{bmatrix} \right) \text{ for some } \gamma \in \Gamma_1(N)$$

[11, Proposition 2.1 and Definition 2.2]. Denote the set of equivalence classes by $C_N(d_K)$, namely,

$$C_N(d_K) = Q_N(d_K) / \sim_N = \{ [Q]_N \mid Q \in Q_N(d_K) \}.$$

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

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

Then one can readily check that for $Q, Q' \in Q_N(d_K)$ and $\alpha \in \text{SL}_2(\mathbb{Z})$

$$\omega_Q = \omega_Q' \iff Q = Q'$$

and

$$\omega_{Q^\alpha} = \alpha^{-1}(\omega_Q).$$

Let $\text{Cl}(N\mathcal{O}_K)$ be the ray class group of $K$ modulo $N\mathcal{O}_K$, that is,

$$\text{Cl}(N\mathcal{O}_K) = I_K(N\mathcal{O}_K) / P_{K,1}(N\mathcal{O}_K),$$

where $I_K(N\mathcal{O}_K)$ is the group of all fractional ideals of $K$ relatively prime to $N\mathcal{O}_K$ and $P_{K,1}(N\mathcal{O}_K)$ is its subgroup given by

$$P_{K,1}(N\mathcal{O}_K) = \{ \nu\mathcal{O}_K \mid \nu \in K^\times \text{ satisfies } \nu \equiv^* 1 \text{ (mod } N\mathcal{O}_K) \}.$$ 

Here, $\nu \equiv^* 1 \text{ (mod } N\mathcal{O}_K)$ means that $\text{ord}_\mathfrak{p}(\nu - 1) \geq \text{ord}_\mathfrak{p}(N\mathcal{O}_K)$ for all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ dividing $N\mathcal{O}_K$ [16, p. 136]. Eum et al. showed that the map

$$C_N(d_K) \rightarrow \text{Cl}(N\mathcal{O}_K)$$

$$[Q] \mapsto [[\omega_Q, 1]] = [Z\omega_Q + Z]$$

is a well-defined bijection [11, Theorem 2.9]. Therefore, the set $C_N(d_K)$ can be regarded as a group isomorphic to $\text{Cl}(N\mathcal{O}_K)$ through the above bijection, called the extended form class group of discriminant $d_K$ and level $N$. The principal form

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

becomes the identity element of $C_N(d_K)$. 

**Definition 8.1.** Let \( Q = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K) \) and \( f \in \mathcal{F}_N \). We define

\[
f([Q]_N) = f^{\gamma_Q^{-1}}(-\overline{\omega}_Q),
\]

where

\[
\gamma_Q = \begin{bmatrix}
1 & b + b_K \\
0 & 2
\end{bmatrix} (\in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})/(±I_2) ≃ \text{Gal}(\mathcal{F}_N/F_1)).
\]

This value depends only on the class \([Q]_N\) in \( \mathcal{C}_N(d_K) \) if it is finite [34, Proposition 3.3 and Lemma 3.7]. In particular, one can derive the equality \( f([Q_0]_N) = f(\tau_K) \).

The fact that \( \text{Cl}(N\mathcal{O}_K) ≃ \text{Gal}(K(N)/K) \) and the original version of the Shimura reciprocity law [29, Theorem 6.31] lead to the following proposition.

**Proposition 8.2.** We have the isomorphism

\[
\phi_N : \mathcal{C}_N(d_K) \xrightarrow{\sim} \text{Gal}(K(N)/K)
\]

\[
[Q]_N \mapsto (f([Q_0]_N) = f(\tau_K) \mapsto f([Q]_N) \mid f \in \mathcal{F}_N \text{ is finite at } \tau_K).
\]

**Proof.** See [11, Theorem 3.10] or [34, Theorem 3.8].

**Remark 8.3.** Let \( Q, Q' \in \mathcal{Q}_N(d_K) \) and \( f \in \mathcal{F}_N \) such that \( f([Q]_N) \) is finite. By the homomorphism property of \( \phi_N \), we obtain

\[
\phi_N([Q']_N)(f([Q]_N)) = f([Q']_N[Q]_N).
\]

**9 | DEFINITE FORM CLASS GROUPS**

By improving the results introduced in §8, we shall construct the definite form class group which is isomorphic to \( \text{Gal}(K(N)/K) \), and define the definite form class invariants (Theorems C and D). First, we need the following lemma whose proof is similar to that of [8, Lemma 9.3].

**Lemma 9.1.** The extension \( K(N)/\mathcal{Q} \) is Galois and

\[
\text{Gal}(K(N)/\mathcal{Q}) = \text{Gal}(K(N)/K) \rtimes (\epsilon|_{K(N)}),
\]

where \( \epsilon|_{K(N)} \) acts on \( \text{Gal}(K(N)/K) \) via conjugation.

**Proof.** Since \( \epsilon|_K \neq \text{id}_K \) and \( [K : \mathcal{Q}] = 2 \), we see that

\[
\iota \rho, \epsilon \rho \quad (\rho \in \text{Gal}(K(N)/K))
\]
are all the distinct embeddings of $K_N$ into $C$, where $\iota : C \to C$ is the identity map. To prove the first part of the lemma, it suffices to show that $\iota(K_N) = K_N$. We find that

$$\text{Gal}(\iota(K_N)/\iota(K))$$

$$= \iota \text{Gal}(K_N/K) \iota^{-1}|_{\iota(K_N)}$$

$$\cong I_{\iota(K)}(\iota(N\mathcal{O}_K))/\{\iota(a) \mid a \in P_{K,1}(N\mathcal{O}_K)\}$$

since the Artin symbol satisfies

$$\left(\frac{\iota(K_N)/\iota(K)}{\iota(a)}\right) = \left(\frac{K_N/K}{a}\right)\iota^{-1}|_{\iota(K_N)}$$

$$= I_K(N\mathcal{O}_K)/P_{K,1}(N\mathcal{O}_K)$$

because if $\alpha \in K^\times$ satisfies $\alpha \equiv 1 \mod N\mathcal{O}_K$, then $\iota(\alpha) \equiv 1 \mod N\mathcal{O}_K$.

Now, the existence theorem of class field theory [8, Theorem 8.6] or [16, §V.9] implies $\iota(K_N) = K_N$.

Observe that $\text{Gal}(K_N/K)$ is normal in $\text{Gal}(K_N/Q)$ because

$$[\text{Gal}(K_N/Q) : \text{Gal}(K_N/K)] = [K : Q] = 2.$$ 

Furthermore, we see that $\text{Gal}(K_N/K) \cap \langle \iota|_{K_N} \rangle = \{\text{id}_{K_N}\}$, and so

$$\text{Gal}(K_N/Q) = \text{Gal}(K_N/K)\langle \iota|_{K_N} \rangle.$$ 

Therefore, we get

$$\text{Gal}(K_N/Q) = \text{Gal}(K_N/K) \rtimes \langle \iota|_{K_N} \rangle$$

where $\iota|_{K_N}$ acts on $\text{Gal}(K_N/K)$ via conjugation [25, p. 76].

Let us denote by

$$Q_N^+(d_K) = \{ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y] \mid \gcd(a, b, c) = 1, b^2 - 4ac = d_K, \gcd(a, N) = 1\},$$

$$Q_N^0(d_K) = \{Q \in Q_N^+(d_K) \mid Q \text{ is positive definite}\} = Q_N(d_K),$$

$$Q_N^-(d_K) = \{Q \in Q_N^+(d_K) \mid Q \text{ is negative definite}\}.$$

We then see that

$$Q_N^+(d_K) = Q_N^0(d_K) \cup Q_N^-(d_K).$$

$$Q_N^-(d_K) = \{-Q = (-1)Q \mid Q \in Q_N^+(d_K)\}.$$
The action of $\Gamma_1(N)$ on $Q_N(d_K)$ can be naturally extended to that on $Q_N^{\pm}(d_K)$ as

$$Q^\gamma = Q\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) \quad (Q \in Q_N^{\pm}(d_K), \gamma \in \Gamma_1(N)),$$

which induces the equivalence relation $\sim_N^{\pm}$ on $Q_N^{\pm}(d_K)$. Denote by

$$C_N^{\pm}(d_K) = Q_N^{\pm}(d_K)/\sim_N^{\pm} = \{[Q]^\pm_N \mid Q \in Q_N^{\pm}(d_K)\}$$

the set of equivalence classes. For $Q \in Q_N^{\pm}(d_K)$, we let

$$\text{sgn}(Q) = \begin{cases} 1 & \text{if } Q \in Q_N^{+}(d_K), \\ -1 & \text{if } Q \in Q_N^{-}(d_K). \end{cases}$$

Observe that if $\text{sgn}(Q) = 1$, then $[Q]_N$ in $C_N(d_K)$ coincides with $[Q]_N^{\pm}$ in $C_N^{\pm}(d_K)$. Thus, one can simply write without confusion $\sim_N$ and $[Q]_N$ for $\sim_N^{\pm}$ and $[Q]_N^{\pm}$, respectively. Recall from Proposition 8.2 that we have the explicit isomorphism $\phi_N : C_N(d_K) \to \text{Gal}(K(N)/K)$.

**Theorem 9.2.** The set $C_N^{\pm}(d_K)$ can be given a group structure isomorphic to $\text{Gal}(K(N)/Q)$ so that it contains $C_N(d_K)$ as a subgroup and the element $[-Q_0]_N$ corresponds to $c|_{K(N)}$.

**Proof.** Note that if $Q \sim_N Q'$ for $Q, Q' \in Q_N^{\pm}(d_K)$, then $\text{sgn}(Q) = \text{sgn}(Q')$. This observation, together with (27) and (28), implies that

$$C_N^{\pm}(d_K) \to C_N(d_K) \times \{1, -1\}$$

$$[Q]_N \mapsto ([\text{sgn}(Q)Q]_N, \text{sgn}(Q))$$

is a well-defined bijection. And, by Lemma 9.1 we deduce the bijection

$$C_N^{\pm}(d_K) \to \text{Gal}(K(N)/Q) = \text{Gal}(K(N)/K) \rtimes \langle c|_{K(N)} \rangle$$

$$[Q]_N \mapsto \phi_N([\text{sgn}(Q)Q]_N)^{\frac{1-\text{sgn}(Q)}{2}}.$$  

This proves the theorem. \qed

**Remark 9.3.**

(i) Since $c|_{K(N)}$ is of order 2, we get $[-Q_0]_N[-Q_0]_N = [Q_0]_N$.

(ii) Let $Q, Q' \in Q_N^{\pm}(d_K)$. Since $\text{sgn}(Q)$ depends only on the class $[Q]_N$, we may also write $\text{sgn}([Q]_N)$ for $\text{sgn}(Q)$. And we see from the isomorphism in (29) (and the concept of a semidirect product) that

$$\text{sgn}([Q]_N[Q']_N) = \text{sgn}([Q]_N)\text{sgn}([Q']_N).$$
Now, we let
\[
\phi^\pm_N : C^\pm_N(d_K) \to \text{Gal}(K_N/\mathbb{Q})
\]
be the isomorphism stated in (29). By extending Definition 8.1, we define the definite form class invariants as follows.

**Definition 9.4.** Let \( Q \in Q^\pm_N(d_K) \) and \( f \in F_N \). Define
\[
f([Q]_N) = \phi^\pm_N([-Q_0]_N^{1-\text{sgn}([Q]_N)})(f([-Q_0]_N^{1-\text{sgn}([Q]_N)}[Q]_N))
\]
\[
= \begin{cases} 
  f([Q]_N) & \text{if } \text{sgn}([Q]_N) = 1, \\
  f([-Q_0]_N[Q]_N) & \text{if } \text{sgn}([Q]_N) = -1.
\end{cases}
\]

**Remark 9.5.** Observe that
\[
\text{sgn}([-Q_0]_N^{1-\text{sgn}([Q]_N)}) = \text{sgn}([Q]_N)
\]
and so
\[
\text{sgn}([-Q_0]_N^{1-\text{sgn}([Q]_N)}[Q]_N) = 1
\]
by Remark 9.3.

**Theorem 9.6.** Let \( Q, Q' \in Q^\pm_N(d_K) \) and \( f \in F_N \). If \( f([Q]_N) \) is finite, then
\[
\phi^\pm_N([Q']_N)(f([Q]_N)) = f([Q']_N[Q]_N).
\]

**Proof.** We derive that
\[
\phi^\pm_N([Q']_N)(f([Q]_N))
\]
\[
= \phi^\pm_N([Q']_N)(\phi^\pm_N([-Q_0]_N^{1-\text{sgn}([Q]_N)})(f([-Q_0]_N^{1-\text{sgn}([Q]_N)}[Q]_N)))))
\]
\[
= \left( \phi^\pm_N([-Q_0]_N^{1-\text{sgn}([Q']_N)}) \right) \phi^\pm_N([-Q_0]_N^{1-\text{sgn}([Q']_N)}[Q']_N[-Q_0]_N^{1-\text{sgn}([Q]_N)})
\]
\[
\left( f([-Q_0]_N^{1-\text{sgn}([Q']_N)}[Q]_N))\right)
\]
by the homomorphism property of \( \phi^\pm_N \) and Remark 9.3(i)
\[
= \phi^\pm_N([-Q_0]_N^{1-\text{sgn}([Q']_N)})
\]
\[ \left( f \left( \left[ -Q_0 \right]_N^{1 - \text{sgn}(Q'_N[Q]_N)} \left[ Q'_N[-Q_0]_N^{2} \right] \right) \right) \]

by the fact \( \text{sgn} \left( \left[ -Q_0 \right]_N^{1 - \text{sgn}(Q'_N[Q]_N)} \left[ Q'_N[-Q_0]_N^{2} \right] \right) = 1 \)

obtained from Remarks 9.3 (ii) and 9.5, and by Remark 8.3

\[ = \phi^\pm_N \left( \left[ -Q_0 \right]_N^{1 - \text{sgn}(Q'_N[Q]_N)} \right) \left( f \left( \left[ -Q_0 \right]_N^{1 - \text{sgn}(Q'_N[Q]_N)} \left[ Q'_N[Q]_N \right] \right) \right) \]

by Remark 9.3 (i)

\[ = f([Q'_N][Q]_N) \]

by Definition 9.4.

10 | SOME SUBGROUPS OF DEFINITE FORM CLASS GROUPS

In this last section, we shall find subgroups of \( C_0^\pm(d_K) \) which are isomorphic to \( \text{Gal}(K(\mathcal{N})/H_K) \), \( \text{Gal}(K(\mathcal{N})/\mathcal{Q}(j(\tau_K))) \) and \( \text{Gal}(K(\mathcal{N})/\mathcal{Q}(\zeta_N)) \), respectively.

First, observe that the principal form \( Q_0 = x^2 + b_K xy + c_K y^2 \) induces \( \omega_{Q_0} = \tau_K \). Let

\[ C_{0,N}(d_K) = \{[Q^\alpha]_N \mid \alpha \in \text{SL}_2(\mathbb{Z}) \text{ satisfies } Q^\alpha_0 \in \mathcal{Q}_N(d_K) \} \quad (\subseteq C_N(d_K) \subset C_0^\pm(d_K)). \]

**Theorem 10.1.** We have

\[ \phi^\pm_N^{-1}(\text{Gal}(K(\mathcal{N})/H_K)) = \phi^\pm_N^{-1}(\text{Gal}(K(\mathcal{N})/H_K)) = C_{0,N}(d_K). \]

**Proof.** We deduce that for \( Q \in \mathcal{Q}_N(d_K) \)

\[ [Q]_N \in \phi^\pm_N^{-1}(\text{Gal}(K(\mathcal{N})/H_K)) \iff \phi_N([Q]_N)|_{H_K} = \text{id}_{H_K} \]

\[ \iff \phi_N([Q]_N)(j(\tau_K)) = j(\tau_K) \quad \text{by (10)} \]

\[ \iff j(-\bar{\omega}_Q) = j(\tau_K) = j(-\bar{\tau}_K) \quad \text{by Proposition 8.2,} \]

the facts \( j(\tau) \in P_1 \) and \( -\bar{\tau}_K = \tau_K + b_K \)

\[ \iff \gamma(-\bar{\omega}_Q) = -\bar{\tau}_K \quad \text{for some } \gamma \in \text{SL}_2(\mathbb{Z}) \]

\[ \iff \alpha(\omega_Q) = \tau_K \quad \text{for some } \alpha \in \text{SL}_2(\mathbb{Z}) \]

\[ \iff Q = Q^\alpha_0 \quad \text{for some } \alpha \in \text{SL}_2(\mathbb{Z}) \quad \text{by (24) and (25)}. \]

Hence we conclude that \( \phi^\pm_N^{-1}(\text{Gal}(K(\mathcal{N})/H_K)) = C_{0,N}(d_K). \)

**Remark 10.2.** Now, we have shown by Proposition 4.1 and Theorem 10.1 that

\[ C_{0,N}(d_K) \simeq W_{K,N}/r_N(U_K). \]
Here we shall present an explicit isomorphism of $C_{0,N}(d_K)$ onto $W_{K,N}/r_N(U_K)$ as follows. Let $[Q_0^\alpha] \in C_{0,N}(d_K)$ with $\alpha = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in SL_2(\mathbb{Z})$ satisfying $Q^\alpha_0 \in Q_N(d_K)$. If we write $Q^\alpha_0 = ax^2 + bxy + cy^2$, then we get

$$\begin{aligned}
a &= A^2 + b_KAC + c_KC^2 = Q_0(A, C), \\
b &= 2AB + b_K(AD + BC) + 2c_KCD, \\
c &= B^2 + b_KBD + c_KD^2.
\end{aligned} \tag{30}$$

Furthermore, we obtain by (25) and the fact $-\tau_K = \tau_K + b_K$ that

$$\bar{\omega}_{Q_0^\alpha} = -\bar{\alpha}^{-1}(\omega_{Q_0^\alpha}) = -\alpha^{-1}(\tau_K) = \frac{D(-\tau_K) + B}{C(-\tau_K) + A} \begin{bmatrix} D & B \\ C & A \end{bmatrix} \begin{bmatrix} 1 & b_K \\ 0 & 1 \end{bmatrix}(\tau_K). \tag{31}$$

We then achieve by Proposition 8.2 that for any $f \in \mathcal{F}_N$ which is finite at $\tau_K$

$$\phi_N([Q_0^\alpha)_N](f(\tau_K)) = f \begin{bmatrix} 1 & b_K \\ 0 & a \end{bmatrix}^{-1}(-\bar{\omega}_{Q_0^\alpha}) \quad \text{by Definition 8.1}$$

$$= f \begin{bmatrix} 1 & b_K \\ 0 & a \end{bmatrix}^{-1} \begin{bmatrix} D & B \\ C & A \end{bmatrix} \begin{bmatrix} 1 & b_K \\ 0 & 1 \end{bmatrix}(\tau_K) \quad \text{by (31)}$$

$$= f \begin{bmatrix} 1 & b_K \\ 0 & a \end{bmatrix}^{-1} \begin{bmatrix} D & B \\ C & A \end{bmatrix} \begin{bmatrix} 1 & b_K \\ 0 & 1 \end{bmatrix}(\tau_K) \quad \text{by (31) and the fact } AD - BC = 1.$$

In the above, $Q_0(A, C)^{-1}$ means the inverse of $Q_0(A, C)$ in $(\mathbb{Z}/N\mathbb{Z})^\times$. Observe that if we let $s = Q_0(A, C)^{-1}C$ and $t = Q_0(A, C)^{-1}(A + b_KC)$, then

$$\begin{bmatrix} t - b_Ks & -c_Ks \\ s & t \end{bmatrix} = Q_0(A, C)^{-1} \begin{bmatrix} A & -c_KC \\ C & A + b_KC \end{bmatrix} \quad (\in W_{K,N}).$$

Therefore we establish the desired isomorphism

$$C_{0,N}(d_K) \xrightarrow{\sim} W_{K,N}/r_N(U_K)$$

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}_N \mapsto \begin{bmatrix} A & -c_KC \\ C & A + b_KC \end{bmatrix}_N$$

by Proposition 4.1.

**Corollary 10.3.** We derive

$$\phi_N^{-1}(\text{Gal}(K(N)/\mathbb{Q}(j(\tau_K)))) = \langle [Q_0^\alpha]_N, [-Q_0]_N \mid \alpha \in SL_2(\mathbb{Z}) \text{ satisfies } Q_0^\alpha \in Q_N(d_K) \rangle.$$
Proof. We find by Theorem 9.2 and the fact $j(\tau_K) \in \mathbb{R}$ that
\[
\phi^\pm_N([-Q_0]_N)(j(\tau_K)) = \psi(j(\tau_K)) = j(\tau_K),
\]
which shows that $[-Q_0]_N$ is contained in $\phi^\pm_N(\text{Gal}(K(\zeta_N)/\mathbb{Q}(j(\tau_K))))$. Moreover, since $[-Q_0]_N$ does not belong to $C_{0,\mathbb{N}}(d_K)$ and
\[
[\text{Gal}(K(\zeta_N)/\mathbb{Q}(j(\tau_K)))) : \text{Gal}(K(\zeta_N)/H_K)] = [K(j(\tau_K)) : \mathbb{Q}(j(\tau_K))] = 2,
\]
we conclude by Theorem 10.1 that
\[
\phi^\pm_N^{-1}(\text{Gal}(K(\zeta_N)/\mathbb{Q}(j(\tau_K)))) = \langle [Q_0^\alpha]_N, [-Q_0]_N \mid \alpha \in SL_2(\mathbb{Z}) \text{ satisfies } Q_0^\alpha \in Q_N(d_K) \rangle.
\]

Theorem 10.4. We get
\[
\phi^\pm_N^{-1}(\text{Gal}(K(\zeta_N)/\mathbb{Q}(\zeta_N)))) = \{[Q]_N \mid Q \in \mathbb{Q}_N^\pm(d_K) \text{ satisfies } a_Q \equiv 1 \pmod{N}\}
\]
where $Q = a_Q x^2 + b_Q xy + c_Q y^2$.

Proof. Observe that for $Q = a_Q x^2 + b_Q xy + c_Q y^2 \in \mathbb{Q}_N^\pm(d_K),$
\[
\phi^\pm_N([Q]_N)(\zeta_N) = (\phi_N([\text{sgn}(Q)Q]_N) \psi_{K(\zeta_N)}^{1-\text{sgn}(Q)})(\zeta_N) \quad \text{by the definition of } \phi^\pm_N \text{ described in (29)}
\]
\[
= \phi_N([\text{sgn}(Q)Q]_N)\zeta_N^{\text{sgn}(Q)}
\]
\[
= \zeta_N^{a_Q^{-1}} \quad \text{by Definition 8.1 and Proposition 8.2.}
\]
Here, $a_Q^{-1}$ indicates the inverse of $a_Q$ in $(\mathbb{Z}/N\mathbb{Z})^\times$. Thus we obtain the restriction homomorphism of $\phi^\pm_N$
\[
c_N : C_N^\pm(d_K) \to \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})
\]
\[
[Q]_N \mapsto \left(\zeta_N \mapsto \zeta_N^{a_Q^{-1}}\right),
\]
from which we achieve that
\[
\phi^\pm_N^{-1}(\text{Gal}(K(\zeta_N)/\mathbb{Q}(\zeta_N)))) = \text{Ker}(c_N) = \{[Q]_N \mid Q \in Q_N^\pm(d_K) \text{ satisfies } a_Q \equiv 1 \pmod{N}\}. \quad \square
\]

Remark 10.5. Let $N$ and $M$ be positive integers such that $N \mid M$. By Proposition 8.2 and the proof of Theorem 9.2, we have the commutative diagram in Figure 4 whose first vertical homomorphism is
\[
C_M^\pm(d_K) \to C_N^\pm(d_K)
\]
\[
[Q]_M \mapsto [Q]_N.
\]
\[
\begin{array}{ccc}
C^\pm_M(d_K) & \xrightarrow{\phi^\pm_M} & \text{Gal}(K(M)/\mathbb{Q}) \\
\downarrow & & \downarrow \text{restriction} \\
C^\pm_N(d_K) & \xrightarrow{\phi^\pm_N} & \text{Gal}(K(N)/\mathbb{Q}) \\
\end{array}
\]

\text{FIGURE 4} A commutative diagram of homomorphisms for \(N | M\)

Note that the compositions of horizontal homomorphisms are \(c_M\) and \(c_N\), respectively. Therefore, for each prime \(p\) we derive the surjection

\[
\begin{align*}
\lim_{n \to 1} \frac{C^\pm_p(d_K)}{p^n} &\to \mathbb{Z}_p^\times \\
([Q_1]_p, [Q_2]_p, \ldots) &\leftrightarrow \left( \lim_{n \to \infty} a_{Q_n} \right)^{-1}.
\end{align*}
\]

ACKNOWLEDGEMENTS

The authors would like to thank the referee for carefully reading the manuscript and for giving detailed comments and suggestions that have been helpful to improve the manuscript.

The first-named author was supported by the research fund of Dankook University in 2020 and by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1F1A1A01073055). The third named (corresponding) author was supported by Hankuk University of Foreign Studies Research Fund of 2021 and by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1F1A1A01048633). The fourth-named author was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1C1C1A01006139).

JOURNAL INFORMATION

Mathematika is owned by University College London and published by the London Mathematical Society. All surplus income from the publication of Mathematika is returned to mathematicians and mathematics research via the Society’s research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES

1. M. Bhargava, Higher composition laws I: A new view on Gauss composition, and quadratic generalizations, Ann. of Math. (2) 159 (2004), no. 1, 217–250.
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 and P. L. Clark, Torsion points and isogenies on CM elliptic curves, J. Lond. Math. Soc. (2) 102 (2020), no. 2, 580–622.
4. A. Bourdon, P. L. Clark and P. Pollack, Anatomy of torsion in the CM case, Math. Z. 285 (2017), no. 3–4, 795–820.
5. A. Bourdon, P. L. Clark, and J. Stankevicz, Torsion points on CM elliptic curves over real number fields, Trans. Amer. Math. Soc. 369 (2017), no. 12, 8457–8496.
6. F. Campagna and R. Pengo, Entanglement in the family of division fields of elliptic curves with complex multiplication, Pacific J. Math., to appear.
7. P. L. Clark and P. Pollack, The truth about torsion in the CM case, II, Q. J. Math. 68 (2017), no. 4, 1313–1333.
8. D. A. Cox, Primes of the form \(x^2 + ny^2\): Fermat, class field theory, and complex multiplication, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, N.J., 2013.
9. M. Deuring, Die Klassenkörper der Komplexen Multiplikation, Enzyklopädie der mathematischen Wissenschafteren: Mit Einschluss ihrer Anwendungen, Band I 2, Heft 10, Teil II (Article I 2, 23), B. G. Teubner Verlagsgesellschaft, Stuttgart, 1958.
10. P. G. L. Dirichlet, Zahlentheorie, 4th ed., Vieweg, Braunschweig, 1894.
11. I. S. Eum, J. K. Koo, and D. H. Shin, Binary quadratic forms and ray class groups, Proc. Roy. Soc. Edinb. Sect. A 150 (2020), no. 2, 695–720.
12. G. Frei, F. Lemmermeyer and P. J. Roquette, Emil Artin and Helmut Hasse—the Correspondence 1923–1958, Contributions in Mathematical and Computational Sciences, 5, Springer, Heidelberg, 2014.
13. C. F. Gauss, Disquisitiones arithmeticae, Leipzig. 1801.
14. H. Hasse, Neue Begründung der komplexen Multiplikation I, J. reine angew. Math. 157 (1927), 115–139.
15. H. Hasse, Neue Begründung der komplexen Multiplikation II, J. reine angew. Math. 165 (1931), 64–88.
16. G. J. Janusz, Algebraic number fields, 2nd ed., Grad. Stud. in Math., vol. 7, Amer. Math. Soc., Providence, R.I., 1996.
17. H. Y. Jung, J. K. Koo, and D. H. Shin, Primitive and totally primitive Fricke families with applications, Results Math. 71 (2017), no. 3–4, 841–858.
18. 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.
19. H. Y. Jung, J. K. Koo, and D. H. Shin, Primitive and totally primitive Fricke families with applications (II), J. Math. Anal. Appl. 472 (2019), no. 1, 432–446.
20. D. Kubert and S. Lang, Modular Units, Grundlehren der mathematischen Wissenschaften, vol. 244, Springer, New York–Berlin, 1981.
21. J. K. Koo and D. H. Shin, Construction of class fields over imaginary quadratic fields using $y$-coordinates of elliptic curves, J. Korean Math. Soc. 50 (2013), no. 4, 847–864.
22. J. K. Koo, D. H. Shin, and D. S. Yoon, On a problem of Hasse and Ramachandra, Open Math. 17 (2019), no. 1, 131–140.
23. S. Lang, Elliptic Functions, With an appendix by J. Tate, 2nd ed., Grad. Texts in Math., vol. 112, Springer, New York, N.Y., 1987.
24. S. Lang, Algebraic number theory, 2nd ed., Springer, New York, N.Y., 1994.
25. S. Lang, Algebra, 3rd ed., Grad. Texts Math., vol. 211, Springer, New York, N.Y., 2002.
26. Á. Lozano-Robledo, Galois representations attached to elliptic curves with complex multiplication, Algebra Number Theory, https://arxiv.org/abs/1809.02584, 2018, to appear.
27. K. Ramachandra, Some applications of Kronecker’s limit formula, Ann. of Math. (2) 80 (1964), 104–148.
28. J.-P. Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques, Invent. Math. 15 (1972), no. 4, 259–331.
29. G. Shimura, Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten and Princeton Univ. Press, Princeton, N.J., 1971.
30. C. L. Siegel, Lectures on advanced analytic number theory, Notes by S. Raghavan, Tata Inst. Fund. Res. Lect. Math., vol. 23, Tata Institute of Fundamental Research, Bombay, 1965.
31. J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, Grad. Texts Math., vol. 151, Springer, New York, N.Y., 1994.
32. J. H. Silverman, The arithmetic of elliptic curves, 2nd ed., Grad. Texts Math., vol. 106, Springer, Dordrecht, 2009.
33. P. Stevenhagen, Hilbert’s 12th problem, complex multiplication and Shimura reciprocity, Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 161–176.
34. D. S. Yoon, Ray class invariants in terms of extended form class groups, East Asian Math. J. 37 (2021), no. 1, 87–95.