East Asian Math. J.
Vol. 40 (2024), No. 1, pp. 095-107
YNMS
http://dx.doi.org/10.7858/eamj.2024.008

# ARTIN SYMBOLS OVER IMAGINARY QUADRATIC FIELDS 

Dong Sung Yoon


#### Abstract

Let $K$ be an imaginary quadratic field with ring of integers $\mathcal{O}_{K}$ and $N$ be a positive integer. By $K_{(N)}$ we mean the ray class field of $K$ modulo $N \mathcal{O}_{K}$. In this paper, for each prime $\mathfrak{p}$ of $K$ relatively prime to $N \mathcal{O}_{K}$ we explicitly describe the action of the Artin symbol $\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)$ on special values of modular functions of level $N$. Furthermore, we extend the Kronecker congruence relation for the elliptic modular function $j$ to some modular functions of higher level.


## 1. Introduction

Let $L / K$ be a Galois extension of number fields. Let $\mathcal{O}_{K}$ be the ring of algebraic integers in $K$ and $\mathfrak{p}$ be a prime of $K$ (i.e., a nontrivial prime ideal of $\mathcal{O}_{K}$ ) which is unramified in $L$. For a prime $\mathfrak{P}$ of $L$ lying above $\mathfrak{p}$, its decomposition group is defined by

$$
D_{\mathfrak{P}}\left(=D_{\mathfrak{P} / K}\right)=\left\{\sigma \in \operatorname{Gal}(L / K) \mid \mathfrak{P}^{\sigma}=\mathfrak{P}\right\} .
$$

Then, $D_{\mathfrak{F}}$ is isomorphic to the Galois group of residue fields, that is,

$$
D_{\mathfrak{P}} \simeq \widetilde{G}=\operatorname{Gal}\left(\left(\mathcal{O}_{L} / \mathfrak{P}\right) /\left(\mathcal{O}_{K} / \mathfrak{p}\right)\right) .
$$

Thus there is a unique element $\sigma \in D_{\mathfrak{F}}$ which maps to the Frobenius automorphism of $\widetilde{G}$, and so $\sigma$ satisfies

$$
\nu^{\sigma} \equiv \nu^{\mathrm{N}(\mathfrak{p})}(\bmod \mathfrak{P}) \quad \text { for all } \nu \in \mathcal{O}_{L}
$$

where $\mathrm{N}(\mathfrak{p})=\left|\mathcal{O}_{K} / \mathfrak{p}\right|$ is the norm of $\mathfrak{p}$ ([3, Lemma 5.19]). This unique element $\sigma$ is called the Artin symbol and is denoted by $\left(\frac{L / K}{\mathfrak{P}}\right)$. In particular, if $L / K$ is an abelian extension, then the Artin symbol depends only on $\mathfrak{p}$ and hence it can be written as $\left(\frac{L / K}{\mathfrak{p}}\right)$. Some concrete examples of Artin symbols for $K=\mathbb{Q}$ can be found in $[4, \S 9.1]$.

In what follows, we let $K$ be an imaginary quadratic field of discriminant $d_{K}$ and $N$ be a positive integer. Let $\mathcal{C}\left(N \mathcal{O}_{K}\right)$ denote the ray class group of $K$

[^0]modulo $N \mathcal{O}_{K}$, namely, $\mathcal{C}\left(N \mathcal{O}_{K}\right)=I\left(N \mathcal{O}_{K}\right) / P_{1}\left(N \mathcal{O}_{K}\right)$ where $I\left(N \mathcal{O}_{K}\right)$ is the group of fractional ideals of $K$ relatively prime to $N \mathcal{O}_{K}$ and $P_{1}\left(N \mathcal{O}_{K}\right)$ is its subgroup defined by
$$
\left.P_{1}\left(N \mathcal{O}_{K}\right)=\left\langle\nu \mathcal{O}_{K}\right| \nu \in \mathcal{O}_{K} \backslash\{0\} \text { and } \nu \equiv 1\left(\bmod N \mathcal{O}_{K}\right)\right\rangle .
$$

Let $K_{(N)}$ be the ray class field of $K$ modulo $N \mathcal{O}_{K}$ so that all primes of $K$ ramified in $K_{(N)}$ divide $N \mathcal{O}_{K}$ and the Artin map

$$
\left(\frac{K_{(N)} / K}{\cdot}\right): I\left(N \mathcal{O}_{K}\right) \rightarrow \operatorname{Gal}\left(K_{(N)} / K\right)
$$

induces an isomorphism $\mathcal{C}\left(N \mathcal{O}_{K}\right) \xrightarrow{\sim} \operatorname{Gal}\left(K_{(N)} / K\right)$. In particular, the Hilbert class field $H_{K}=K_{(1)}$ is the maximal unramified abelian extension of $K$. One may refer to $[3, \S 8]$ or $[8$, Chapter V] for class field theory.

For a lattice $\Lambda$ in $\mathbb{C}$, let $j(\Lambda)$ be the $j$-invariant of any elliptic curve over $\mathbb{C}$ isomorphic to $\mathbb{C} / \Lambda$. Let $\mathfrak{a}$ be a nontrivial ideal of $\mathcal{O}_{K}$. By the theory of complex multiplication, Hasse ([7]) proved that for all but a finite number of primes $\mathfrak{p}$ of $K$ satisfying $\mathfrak{p} \neq \overline{\mathfrak{p}}$

$$
\begin{equation*}
j\left(\mathfrak{p}^{-1} \mathfrak{a}\right) \equiv j(\mathfrak{a})^{p}(\bmod \mathfrak{P}) \quad \text { with } p=\mathrm{N}(\mathfrak{p}) \tag{1}
\end{equation*}
$$

for any prime $\mathfrak{P}$ of $H_{K}$ lying above $\mathfrak{p}$. This congruence is called the Kronecker congruence relation. We also notice that there is an analog of (1) for the Weber function. For a positive integer $m$, let $\Phi_{m}(x, y) \in \mathbb{Z}[x, y]$ be the modular polynomial for which $\Phi_{m}(j(\tau), j(m \tau))=0$. Here, $j$ stands for the elliptic modular function defined on the complex upper half-plane $\mathbb{H}=\{\tau \in \mathbb{C} \mid \operatorname{Im}(\tau)>$ $0\}$. Prior to the work of Hasse, Weber ([15]) had derived a weaker form of (1) in such a way that for each prime $p$

$$
\begin{equation*}
\Phi_{p}(x, y) \equiv\left(x^{p}-y\right)\left(x-y^{p}\right)(\bmod p \mathbb{Z}[x, y]) \tag{2}
\end{equation*}
$$

See also [2] for a generalization of (2) to certain Hauptmoduln including $j$.
In this paper, we shall deal with the following three topics related to Artin symbols.
(i) For a prime $\mathfrak{p}$ of $K$ which is relatively prime to $N \mathcal{O}_{K}$, we shall explicitly describe the Artin symbol $\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)$ by utilizing the extended form class group of level $N$ which was developed by Eum, Koo and Shin in [5] (Theorem 4.2).
(ii) From the description of $\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)$ we shall obtain a certain extension of the Kronecker congruence relation (1) when $\mathfrak{a}=\mathcal{O}_{K}$ to meromorphic modular functions of level $N$ (Corollaries 5.1 and 5.3).
(iii) For a prime $\mathfrak{P}$ of $K_{(N)}$ such that $\mathfrak{P} \cap \mathbb{Q}$ is unramified in $K_{(N)}$, we shall investigate $\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)$ or $D_{\mathfrak{P} / \mathbb{Q}}$. (Theorem 6.2).

## 2. Theory of complex multiplication

In this section, we shall review some necessary facts of the theory of complex multiplication.

Proposition 2.1. Let $\mathfrak{a}$ be a nontrivial ideal of $\mathcal{O}_{K}$. Then, $j(\mathfrak{a})$ is an algebraic integer which generates $H_{K}$ over $K$.

Proof. See [11, Theorem 4 in Chapter 5 and Theorem 1 in Chapter 10].
The idelic formalization of the theory of complex multiplication owing to Shimura and A. Robert yields the following result.

Proposition 2.2. Let $\mathfrak{a}$ be a nontrivial ideal of $\mathcal{O}_{K}$. For any nontrivial ideal $\mathfrak{b}$ of $\mathcal{O}_{K}$, we have

$$
j(\mathfrak{a})^{\left(\frac{H_{K} / K}{\mathfrak{b}}\right)}=j\left(\mathfrak{b}^{-1} \mathfrak{a}\right) .
$$

Proof. See [11, Theorem 5 in Chapter 10] or [13, Theorem 5.7].
Remark 1. We observe by Proposition 2.2 that the Kronecker congruence relation (1) holds for every prime $\mathfrak{p}$ of $K$ such that $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Furthermore, we may let $\mathfrak{a}=\mathcal{O}_{K}$ in (1) because the action of $\operatorname{Gal}\left(H_{K} / K\right)$ transitively permutes primes $\mathfrak{P}$ of $H_{K}$ lying above $\mathfrak{p}$ ( $[8$, Theorem 6.8 in Chapter I $]$ ).

For a prime $p$ we mean by $\left(\frac{d_{K}}{p}\right)$ the Kronecker symbol. For $\nu_{1}, \nu_{2} \in \mathbb{C}$ which are linearly independent over $\mathbb{R}$, we shall denote by $\left[\nu_{1}, \nu_{2}\right]$ the lattice generated by $\nu_{1}$ and $\nu_{2}$, namely, $\left[\nu_{1}, \nu_{2}\right]=\mathbb{Z} \nu_{1}+\mathbb{Z} \nu_{2}$.
Lemma 2.3. Let $p$ be a prime.
(i) $p$ splits completely in $K$ if and only if $\left(\frac{d_{K}}{p}\right)=1$. In this case, there is an integer $u$ such $u^{2} \equiv d_{K}(\bmod 4 p)$. Furthermore, $\mathfrak{p}=\left[\frac{-u+\sqrt{d_{K}}}{2}, p\right]$ is a prime of $K$ such that $p \mathcal{O}_{K}=\mathfrak{p p}$.
(ii) $p$ is inert in $K$ if and only if $\left(\frac{d_{K}}{p}\right)=-1$.
(iii) $p$ is ramified in $K$ if and only if $\left(\frac{d_{K}}{p}\right)=0$ (i.e., $\left.p \mid d_{K}\right)$. In this case,

$$
\mathfrak{p}= \begin{cases}{\left[\frac{2+\sqrt{d_{K}}}{2}, 2\right]} & \text { if } p=2 \text { and } \frac{d_{K}}{4} \equiv 3(\bmod 4), \\ {\left[\frac{-d_{K}+\sqrt{d_{K}}}{2}, p\right]} & \text { otherwise }\end{cases}
$$

is a prime of $K$ satisfying $p \mathcal{O}_{K}=\mathfrak{p}^{2}$.
Proof. See [1, Theorems 3 and 4 in §9.5].
Let $\tau_{K}$ be the element of $\mathbb{H}$ defined by

$$
\tau_{K}=\left\{\begin{array}{cl}
\frac{-1+\sqrt{d_{K}}}{\frac{2}{}} & \text { if } d_{K} \equiv 1(\bmod 4), \\
\frac{\sqrt{d_{K}}}{2} & \text { if } d_{K} \equiv 0(\bmod 4),
\end{array}\right.
$$

and so $\mathcal{O}_{K}=\left[\tau_{K}, 1\right]$ ([3, Lemma 7.2]). For a prime $\mathfrak{p}$ of $K$, the Artin symbol $\left(\frac{H_{K} / K}{\mathfrak{p}}\right)$ can be expressed in more detail as follows.

Proposition 2.4. Let $p$ be a prime and $\mathfrak{p}$ be a prime of $K$ lying above $p$.
(i) If $p$ splits completely in $K$ and so $\mathfrak{p}=\left[\frac{-u+\sqrt{d_{K}}}{2}, p\right]$ for some integer $u$ such that $u^{2} \equiv d_{K}(\bmod 4 p)$ by Lemma $2.3(\mathrm{i})$, then we have

$$
\left.j\left(\tau_{K}\right)^{\left(\frac{H_{K} / K}{\boldsymbol{p}}\right.}\right)=j\left(\frac{u+\sqrt{d_{K}}}{2 p}\right) .
$$

(ii) If $p$ is inert in $K$, then $\left(\frac{H_{K} / K}{\mathfrak{p}}\right)$ is the identity map on $H_{K}$.
(iii) If $p$ is ramified in $K$, then we get that

$$
j\left(\tau_{K}\right)^{\left(\frac{H_{K} / K}{\rho}\right)}= \begin{cases}j\left(\frac{-2+\sqrt{d_{K}}}{4}\right) & \text { if } p=2 \text { and } \frac{d_{K}}{4} \equiv 3(\bmod 4), \\ j\left(\frac{d_{K}+\sqrt{d_{K}}}{2 p}\right) & \text { otherwise. }\end{cases}
$$

Proof. Note that if $\Lambda$ and $\Lambda^{\prime}$ are homothetic lattices in $\mathbb{C}$, then $j(\Lambda)=j\left(\Lambda^{\prime}\right)$ ([3, Theorem 10.9]). By Proposition 2.1, $j\left(\mathcal{O}_{K}\right)=j\left(\tau_{K}\right)$ generates $H_{K}$ over $K$.
(i) Since $p \mathcal{O}_{K}=\mathfrak{p p}$, we obtain by Proposition 2.2 that

$$
\left.j\left(\mathcal{O}_{K}\right)^{\left(\frac{H_{K} / K}{\mathfrak{p}}\right.}\right)=j\left(\mathfrak{p}^{-1}\right)=j\left(p^{-1} \overline{\mathfrak{p}}\right)=j\left(\frac{u+\sqrt{d_{K}}}{2 p}\right) .
$$

(ii) Observe by Proposition 2.2 and the fact $\mathfrak{p}=p \mathcal{O}_{K}$ that

$$
j\left(\mathcal{O}_{K}\right)^{\left(\frac{H_{K} / K}{\mathfrak{p}}\right)}=j\left(\mathfrak{p}^{-1}\right)=j\left(p^{-1} \mathcal{O}_{K}\right)=j\left(\mathcal{O}_{K}\right)
$$

This implies that $\left(\frac{H_{K} / K}{\mathfrak{p}}\right)$ is the identity map on $H_{K}$.
(iii) Since $p \mathcal{O}_{K}=\mathfrak{p}^{2}$, we derive by Proposition 2.2 that

$$
j\left(\mathcal{O}_{K}\right)^{\left(\frac{H_{K} / K}{\mathfrak{p}}\right)}=j\left(\mathfrak{p}^{-1}\right)=j\left(p^{-1} \mathfrak{p}\right)=j(\mathfrak{p})=j(\overline{\mathfrak{p}}) .
$$

Then the result follows from Lemma 2.3 (iii).

Let $\mathcal{F}_{N}$ be the field of meromorphic modular functions for the principal congruence subgroup

$$
\Gamma(N)=\left\{\gamma \in \mathrm{SL}_{2}(\mathbb{Z}) \mid \gamma \equiv I_{2}\left(\bmod N M_{2}(\mathbb{Z})\right)\right\}
$$

whose Fourier expansions with respect to $q_{\tau}^{\frac{1}{N}}\left(q_{\tau}=e^{2 \pi \mathrm{i} \tau}\right)$ have coefficients in the $N$ th cyclotomic field $\mathbb{Q}\left(\zeta_{N}\right)$ where $\zeta_{N}=e^{\frac{2 \pi \mathrm{i}}{N}}$. As is well known, $\mathcal{F}_{N}$ is a Galois extension of $\mathcal{F}_{1}$ whose Galois group is isomorphic to $\mathrm{GL}_{2}(\mathbb{Z} / N \mathbb{Z}) /\left\langle-I_{2}\right\rangle$.
Proposition 2.5. Let $\alpha \in \mathrm{GL}_{2}(\mathbb{Z} / N \mathbb{Z}) /\left\langle-I_{2}\right\rangle$ and $f \in \mathcal{F}_{N}$ with Fourier expansion $f=\sum_{n \gg-\infty} c_{n} q_{\tau}^{\frac{n}{N}}\left(c_{n} \in \mathbb{Q}\left(\zeta_{N}\right)\right)$.
(i) If $\alpha \in \mathrm{SL}_{2}(\mathbb{Z} / N \mathbb{Z}) /\left\langle-I_{2}\right\rangle$, then $f^{\alpha}=f \circ \widetilde{\alpha}$ where $\widetilde{\alpha}$ is any preimage of $\alpha$ via the reduction $\mathrm{SL}_{2}(\mathbb{Z}) \rightarrow \mathrm{SL}_{2}(\mathbb{Z} / N \mathbb{Z}) /\left\langle-I_{2}\right\rangle$.
(ii) If $\alpha=\left[\begin{array}{ll}1 & 0 \\ 0 & d \\ n\end{array}\right]$ for some integer $d$ relatively prime to $N$, then $f^{\alpha}=$ $\sum_{\zeta}{ }_{\zeta}^{d}>-\infty c_{n}^{\sigma_{d}} q_{\tau}^{\frac{n}{N}}$ where $\sigma_{d}$ is the automorphism of $\mathbb{Q}\left(\zeta_{N}\right)$ defined by $\zeta_{N} \mapsto$

Proof. See [11, Theorem 3 in Chapter 6] and [13, Proposition 6.9 (1)].
Essentially due to Hasse ([7]) we get the following proposition.
Proposition 2.6. We have $K_{(N)}=K\left(f\left(\tau_{K}\right) \mid f \in \mathcal{F}_{N}\right.$ is finite at $\left.\tau_{K}\right)$.
Proof. See [11, Corollary to Theorem 2 in Chapter 10].

## 3. The extended form class group of level $N$

We shall introduce the extended form class group of level $N$ and its action on special values of modular functions of level $N$.

Let $\mathcal{Q}_{N}\left(d_{K}\right)$ be the set of binary quadratic forms given by

$$
\left.\left.\mathcal{Q}_{N}\left(d_{K}\right)=\left\{\begin{array}{l|l}
Q(x, y)=Q\left(\left[\begin{array}{l}
x \\
y
\end{array}\right]\right.
\end{array}\right)=a x^{2}+b x y+c y^{2} \in \mathbb{Z}[x, y] \right\rvert\, \begin{array}{l}
b^{2}-4 a c=d_{K}, a>0, \\
\operatorname{gcd}(a, b, c)=\operatorname{gcd}(a, N)=1
\end{array}\right\} .
$$

The congruence subgroup

$$
\Gamma_{1}(N)=\left\{\gamma \in \mathrm{SL}_{2}(\mathbb{Z}) \left\lvert\, \gamma \equiv\left[\begin{array}{ll}
1 & \star \\
0 & 1
\end{array}\right]\left(\bmod N M_{2}(\mathbb{Z})\right)\right.\right\}
$$

of $\mathrm{SL}_{2}(\mathbb{Z})$ acts on the set $\mathcal{Q}_{N}\left(d_{K}\right)$ from the right so as to have

$$
Q\left(\left[\begin{array}{l}
x \\
y
\end{array}\right]\right)^{\gamma}=Q\left(\gamma\left[\begin{array}{l}
x \\
y
\end{array}\right]\right) \quad\left(Q \in \mathcal{Q}_{N}\left(d_{K}\right), \gamma \in \Gamma_{1}(N)\right) .
$$

This action of $\Gamma_{1}(N)$ naturally defines the equivalence relation $\sim_{N}$ on $\mathcal{Q}_{N}\left(d_{K}\right)$ as follows: for $Q, Q^{\prime} \in \mathcal{Q}_{N}\left(d_{K}\right)$

$$
Q \sim_{N} Q^{\prime} \quad \Longleftrightarrow \quad Q^{\prime}=Q^{\gamma} \text { for some } \gamma \in \Gamma_{1}(N) .
$$

Denote by $\mathcal{C}_{N}\left(d_{K}\right)$ the set of equivalence classes, that is, $\mathcal{C}_{N}\left(d_{K}\right)=\mathcal{Q}_{N}\left(d_{K}\right) / \sim_{N}$. For each $Q=a x^{2}+b x y+c y^{2} \in \mathcal{Q}_{N}\left(d_{K}\right)$, let $\omega_{Q}$ be the zero of the quadratic polynomial $Q(x, 1)$ lying in $\mathbb{H}$ so that

$$
\omega_{Q}=\frac{-b+\sqrt{d_{K}}}{2 a} .
$$

Proposition 3.1. One can equip the set $\mathcal{C}_{N}\left(d_{K}\right)$ with the group structure in such a way that the mapping

$$
\begin{array}{rll}
\mathcal{C}_{N}\left(d_{K}\right) & \rightarrow \mathcal{C}\left(N \mathcal{O}_{K}\right) \\
{[Q]} & \mapsto & {\left[\left[\omega_{Q}, 1\right]\right]}
\end{array}
$$

becomes a well-defined isomorphism.
Proof. See [5, Theorem 2.9 and Remark 2.10 (iv)].

Remark 2. (i) We shall call the group $\mathcal{C}_{N}\left(d_{K}\right)$ the extended form class group of discriminant $d_{K}$ and level $N$.
(ii) For a negative integer $D$ such that $D \equiv 0$ or $1(\bmod 4)$, let $\mathcal{Q}(D)$ be the set of primitive binary quadratic forms over $\mathbb{Z}$ of discriminant $D$. Then, the modular group $\mathrm{SL}_{2}(\mathbb{Z})$ gives rise to the proper equivalence $\sim$ on the set $\mathcal{Q}(D)$. Gauss' direct composition (or, the Dirichlet composition) makes the set of equivalence classes $\mathcal{C}(D)=\mathcal{Q}(D) / \sim$ an abelian group, which is now called the form class group ([6]). Moreover, if $\mathcal{O}$ is the order of discriminant $D$ in the imaginary quadratic field $K=\mathbb{Q}(\sqrt{D})$, then $\mathcal{C}(D)$ is isomorphic to the $\mathcal{O}$-ideal class group ([3, Theorem 7.7]). Jung et al. quite recently generalized $\mathcal{C}(D)$ and constructed a form class group isomorphic to the ray class group of $\mathcal{O}$ modulo $N \mathcal{O}$ ([10, Definition 5.7 and Theorem 9.4]).
Let $\min \left(\tau_{K}, \mathbb{Q}\right)=x^{2}+b_{K} x+c_{K}(\in \mathbb{Z}[x])$. By virtue of Shimura's reciprocity law ( $[13$, Theorem 6.31]), we get an extension of Proposition 2.2 over the Hilbert class field $H_{K}$ to something over the ray class field $K_{(N)}$.

Proposition 3.2. Let $\mathfrak{a} \in I\left(N \mathcal{O}_{K}\right)$. By Proposition 3.1, there exists a quadratic form $Q=a x^{2}+b x y+c y^{2} \in \mathcal{Q}_{N}\left(d_{K}\right)$ so that $[\mathfrak{a}]=\left[\left[\omega_{Q}, 1\right]\right]$ in $\mathcal{C}\left(N \mathcal{O}_{K}\right)$. If $f \in \mathcal{F}_{N}$ is finite at $\tau_{K}$, then we establish

$$
f\left(\tau_{K}\right)^{\left(\frac{K_{(N)} / K}{a}\right)}=f^{\left[\begin{array}{cc}
1 & -a^{\prime}\left(\frac{b+b_{K}}{2^{\prime}}\right) \\
a^{\prime}
\end{array}\right]}\left(-\bar{\omega}_{Q}\right)
$$

where $a^{\prime}$ is an integer satisfying $a a^{\prime} \equiv 1(\bmod N)$.
Proof. See Proposition 2.6 and [16, Theorem 3.5].
Remark 3. Note that $b$ and $b_{K}$ have the same parity for $Q=a x^{2}+b x y+c y^{2} \epsilon$ $\mathcal{Q}_{N}\left(d_{K}\right)$ because $b^{2}-4 a c=d_{K}=b_{K}^{2}-4 c_{K}$.

## 4. Description of Artin symbols

In this section, for a prime $\mathfrak{p}$ of $K$ we shall describe the $\operatorname{Arin}$ symbol $\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)$ in a concrete way as some generalization of Proposition 2.4. Due to Stevenhagen we get the following explicit version of Shimura's reciprocity law ([13, Theorem 6.31]).

Lemma 4.1. Let $s$ and $t$ be integers not both zero such that $\left(s \tau_{K}+t\right) \mathcal{O}_{K}$ is relatively prime to $N \mathcal{O}_{K}$. If $f \in \mathcal{F}_{N}$ is finite at $\tau_{K}$, then we have

$$
\left.f\left(\tau_{K}\right)^{\left(\frac{K_{(N)} / K}{\left(s \tau_{K}+t\right) O_{K}}\right.}\right)=f\left[\begin{array}{c}
{\left[\begin{array}{c}
t-b_{K} s \\
s
\end{array}{\underset{t}{-c_{K} s}}_{t}\right.} \\
\left(\tau_{K}\right) .
\end{array}\right.
$$

Proof. See [14, (3.4)].
Remark 4. (i) Let $\widehat{\mathbb{Z}}=\Pi_{p: \text { primes }} \mathbb{Z}_{p}$ and $\widehat{K}=K \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. Let $[\cdot, K]: \widehat{K}^{*} \rightarrow$ $\operatorname{Gal}\left(K^{\mathrm{ab}} / K\right)$ be the Artin reciprocity map for (finite) ideles, where $K^{\mathrm{ab}}$ is the maximal abelian extension of $K$. Then the class field theory
asserts that $[\cdot, K]$ is a surjection with kernel $K^{*}([3, \S 15 . \mathrm{F}]$ and $[12$, §IV.6]). Here we observe that
$\left(\frac{K_{(N)} / K}{\left(s \tau_{K}+t\right) \mathcal{O}_{K}}\right)=\left.\left[\left(x_{p}\right)_{p}, K\right]\right|_{K_{(N)}} \quad$ where $x_{p}=\left\{\begin{array}{cl}1 & \text { if } p \mid N, \\ s \tau_{K}+t & \text { if } p+N .\end{array}\right.$
(ii) More generally, if $\mathcal{O}$ is an order in $K$ and $H_{\mathcal{O}}$ is the ring class field of $\mathcal{O}$, then Stevenhagen actually expressed $\operatorname{Gal}\left(K^{\mathrm{ab}} / H_{\mathcal{O}}\right)$ as the image of a subset of $\widehat{K}^{*}$ via the reciprocity map $[\cdot, K]([14, \S 3])$.

Theorem 4.2. Let $p$ be a prime relatively prime to $N$ and $\mathfrak{p}$ be a prime of $K$ lying above $p$. Let $f \in \mathcal{F}_{N}$ be finite at $\tau_{K}$.
(i) If $p$ splits completely in $K$ and so $\mathfrak{p}=\left[\frac{-u+\sqrt{d_{K}}}{2}, p\right]$ for some integer $u$ satisfying $u^{2} \equiv d_{K}(\bmod 4 p)$ by Lemma 2.3 (i), then

$$
f\left(\tau_{K}\right)^{\left(\frac{K_{(N)} / K}{p}\right)}=f^{\left[\begin{array}{c}
p-\frac{u+b_{K}}{2} \\
1^{2}
\end{array}\right]}\left(\frac{u+\sqrt{d_{K}}}{2 p}\right) .
$$

(ii) If $p$ is inert in $K$, then

$$
f\left(\tau_{K}\right)^{\left(\frac{K_{(N)} / K}{p}\right)}=f^{\left[\begin{array}{ll}
p & 0 \\
0 & p
\end{array}\right]}\left(\tau_{K}\right) .
$$

(iii) If $p$ is ramified in $K$, then

$$
f\left(\tau_{K}\right)\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)= \begin{cases}f^{\left[\begin{array}{l}
2 \\
0 \\
0
\end{array}{\frac{-2+b_{K}}{2}}_{1}^{1}\right]\left(\frac{-2+\sqrt{d_{K}}}{4}\right)} & \text { if } p=2 \text { and } \frac{d_{K}}{4} \equiv 3(\bmod 4) \\
f^{\left[\begin{array}{l}
p-\frac{d_{K}+b_{K}}{0^{2}} \\
0
\end{array}\right]\left(\frac{d_{K}+\sqrt{d_{K}}}{2 p}\right)} & \text { otherwise. }\end{cases}
$$

Proof. (i) We see that

$$
\mathfrak{p}=p \mathcal{O}_{K}\left[\frac{-u+\sqrt{d_{K}}}{2 p}, 1\right]=p \mathcal{O}_{K}\left[\omega_{Q}, 1\right] \quad \text { with } Q=p x^{2}+u x y+\frac{u^{2}-d_{K}}{4 p} y^{2} .
$$

Thus we achieve that

$$
\begin{aligned}
f\left(\tau_{K}\right)\left(\frac{K_{(N) / K}}{p}\right) & =f\left(\tau_{K}\right)\left(\frac{K_{(N)} / K}{p \mathcal{O}_{K}}\right)\left(\frac{K_{(N)} / K}{\left[\omega_{Q}, 1\right]}\right) \\
& =f^{\left[\begin{array}{ll}
p & 0 \\
0 & p
\end{array}\right]\left(\tau_{K}\right)\left(\frac{K_{(N)} / K}{\left[\omega_{Q}, 1\right]}\right)} \quad \text { by Lemma } 4.1 \\
& =f^{\left[\begin{array}{ll}
p & 0 \\
0 & p
\end{array}\right]\left[\begin{array}{ll}
1-p^{\prime}\left(\frac{u+b_{K}}{}\right. \\
p^{\prime}{ }^{2}
\end{array}\right]}\left(\frac{u+\sqrt{d_{K}}}{2 p}\right)
\end{aligned}
$$

where $p^{\prime}$ is an integer such that $p p^{\prime} \equiv 1(\bmod N)$ by Proposition 3.2

$$
=f^{\left[\begin{array}{c}
p-\frac{u+b_{K}}{2} \\
0
\end{array}\right]}\left(\frac{u+\sqrt{d_{K}}}{2 p}\right) .
$$

(ii) Since $\mathfrak{p}=p \mathcal{O}_{K}$, the result directly follows from Lemma 4.1.
(iii) By Lemma 2.3 (iii), we have $p \mathcal{O}_{K}=\mathfrak{p}^{2}$ where

$$
\begin{aligned}
\mathfrak{p} & = \begin{cases}2 \mathcal{O}_{K}\left[\frac{2+\sqrt{d_{K}}}{4}, 1\right] & \text { if } p=2 \text { and } \frac{d_{K}}{4} \equiv 3(\bmod 4), \\
p \mathcal{O}_{K}\left[\frac{-d_{K}+\sqrt{d_{K}}}{2 p}, 1\right] & \text { otherwise }\end{cases} \\
& =p \mathcal{O}_{K}\left[\omega_{Q}, 1\right] \text { with } Q= \begin{cases}2 x^{2}-2 x y+\frac{4-d_{K}}{8} y^{2} & \text { if } p=2 \text { and } \frac{d_{K}}{4} \equiv 3(\bmod 4), \\
p x^{2}+d_{K} x y+\frac{d_{K}^{2}-d_{K}}{4 p} y^{2} & \text { otherwise. }\end{cases}
\end{aligned}
$$

In a similar way to (i), one can derive by using Lemma 4.1 and Proposition 3.2 that

$$
\begin{aligned}
f\left(\tau_{K}\right)^{\left(\frac{K_{(N)} / K}{p}\right)} & =f\left(\tau_{K}\right)^{\left(\frac{K_{(N)} / K}{p O_{K}}\right)\left(\frac{K_{(N)} / K}{\left[\omega_{Q}, 1\right]}\right)} \\
& = \begin{cases}f^{\left[\begin{array}{l}
2-\frac{-2+b_{K}}{2} \\
1^{2}
\end{array}\left(\frac{-2+\sqrt{d_{K}}}{4}\right)\right.} & \text { if } p=2 \text { and } \frac{d_{K}}{4} \equiv 3(\bmod 4), \\
f^{\left[\begin{array}{l}
p-\frac{d_{K}+b_{K}}{2} \\
1^{2}
\end{array}\right]\left(\frac{d_{K}+\sqrt{d_{K}}}{2 p}\right)} & \text { otherwise. }\end{cases}
\end{aligned}
$$

## 5. The Kronecker congruence relations

As corollaries of Theorem 4.2, we shall exhibit the Kronecker congruence relations extending (1) to modular functions of higher level.

Corollary 5.1. Let $p$ be a prime relatively prime to $N$ and $\mathfrak{P}$ be a prime of $K_{(N)}$ lying above $p$. Let $f \in \mathcal{F}_{N}$ be integral over $\mathbb{Z}[j]$.
(i) If $p$ splits completely in $K$ and so $\mathfrak{P} \cap K=\left[\frac{-u+\sqrt{d_{K}}}{2}, p\right]$ for some integer $u$ such that $u^{2} \equiv d_{K}(\bmod 4 p)$ by Lemma 2.3 , then

$$
f^{\left[\begin{array}{c}
p-\frac{u+b_{K}}{2} \\
1^{2}
\end{array}\right]}\left(\frac{u+\sqrt{d_{K}}}{2 p}\right) \equiv f\left(\tau_{K}\right)^{p}(\bmod \mathfrak{P}) .
$$

(ii) If $p$ is inert in $K$, then

$$
f^{\left.\left[\begin{array}{ll}
p & 0 \\
0 & p
\end{array}\right]_{\left(\tau_{K}\right)}\right) \equiv f\left(\tau_{K}\right)^{p^{2}}(\bmod \mathfrak{P}) . . .}
$$

(iii) If $p$ is ramified in $K$, then

$$
\begin{cases}f^{\left[\begin{array}{c}
2-\frac{-2+b_{K}}{2} \\
1
\end{array}\right]}\left(\frac{-2+\sqrt{d_{K}}}{4}\right) \equiv f\left(\tau_{K}\right)^{p}(\bmod \mathfrak{P}) & \text { if } p=2 \text { and } \frac{d_{K}}{4} \equiv 3(\bmod 4), \\
f^{\left[\begin{array}{l}
p-\frac{d_{K}+b_{K}}{1} \\
1^{2}
\end{array}\right]}\left(\frac{d_{K}+\sqrt{d_{K}}}{2 p}\right) \equiv f\left(\tau_{K}\right)^{p}(\bmod \mathfrak{P}) & \text { otherwise. }\end{cases}
$$

Proof. Since $f$ is integral over $\mathbb{Z}[j]$ and $j\left(\tau_{K}\right)$ is an algebraic integer by Proposition 2.1, $f\left(\tau_{K}\right)$ is also an algebraic integer. Furthermore, $f\left(\tau_{K}\right)$ belongs to $K_{(N)}$ by Proposition 2.6. Now, the corollary follows from Theorem 4.2.

Lemma 5.2. The field $K_{(N)}$ is Galois over $\mathbb{Q}$.
Proof. See [9, Lemma 9.1].

Corollary 5.3. Let $p$ be a prime such that $p \equiv 1$ or $-1(\bmod N)$. Let $f$ be a meromorphic modular function for $\Gamma_{1}(N)$ with rational Fourier coefficients which is integral over $\mathbb{Z}[j]$. If p splits completely in $K$ and so there is an integer $u$ satisfying $u^{2} \equiv d_{K}(\bmod 4 p)$ by Lemma 2.3, then we have

$$
\left(f(\omega)^{p}-f\left(\frac{\omega}{p}\right)\right)\left(f(\omega)-f\left(\frac{\omega}{p}\right)^{p}\right) \equiv 0\left(\bmod p \mathcal{O}_{K_{(N)}}\right) \quad \text { where } \omega=\frac{u+\sqrt{d}_{K}}{2} .
$$

Proof. Since $f$ is integral over $\mathbb{Z}[j]$ and belongs to $\mathcal{F}_{N}, f\left(\tau_{K}\right)$ is an algebraic integer in $K_{(N)}$ by Propositions 2.1 and 2.6. If we let $\mathfrak{p}=\left[\frac{-u+\sqrt{d_{K}}}{2}, p\right]$, then we get $p \boldsymbol{\mathcal { O }}_{K}=\mathfrak{p p}$ by Lemma 2.3 (i) and derive that

$$
\begin{aligned}
f\left(\tau_{K}\right)\left(\frac{K_{(N)} / K}{p}\right) & =f^{\left[\begin{array}{c}
p-\frac{u+b_{K}}{2} \\
0
\end{array}\right]}\left(\frac{\omega}{p}\right) \quad \text { by Theorem } 4.2(\mathrm{i}) \\
= & f^{\left[\begin{array}{ll}
1 & 0
\end{array}\right]\left[\begin{array}{cc}
p-\frac{u+b_{K}}{2} \\
0 & p^{\prime}
\end{array}\right]}\left(\frac{\omega}{p}\right) \quad \text { where } p^{\prime} \text { is an integer such that } p p^{\prime} \equiv 1(\bmod N) \\
= & f^{\left[\begin{array}{cc}
p-\frac{u+b_{K}}{2} \\
0 & p^{\prime}
\end{array}\right]}\left(\frac{\omega}{p}\right) \quad \text { by Proposition } 2.5(\mathrm{ii}) \\
& \quad \text { because } f \text { has rational Fourier coefficients } \\
= & f\left(\frac{\omega}{p}\right) \quad \text { by Proposition } 2.5(\mathrm{i}) \\
& \text { since } p \equiv \pm 1(\bmod N) \text { and } f \text { is modular for } \Gamma_{1}(N) .
\end{aligned}
$$

This assertion also implies that $f\left(\frac{\omega}{p}\right)$ is an algebraic integer in $K_{(N)}$. Moreover, we see that

$$
f\left(\tau_{K}\right)=f\left(\omega-\frac{u+b_{K}}{2}\right)=f\left(\left[\begin{array}{cc}
1 & -\frac{u+b_{K}}{2} \\
0 & 1
\end{array}\right](\omega)\right)=f(\omega)
$$

because $f$ is modular for $\Gamma_{1}(N)$. Hence we obtain that

$$
\begin{equation*}
f(\omega)^{\left(\frac{K_{(N)} / K}{p}\right)}=f\left(\frac{\omega}{p}\right) . \tag{3}
\end{equation*}
$$

We further find by $(3)$ and the fact $p \equiv \pm 1(\bmod N)$ that

$$
\begin{equation*}
f\left(\frac{\omega}{p}\right)^{\left(\frac{K_{(N)} / K}{\bar{p}}\right)}=f(\omega)^{\left(\frac{K_{(N)} / K}{p}\right)\left(\frac{K_{(N)} / K}{\bar{p}}\right)}=f(\omega)^{\left(\frac{K_{(N)} / K}{p O_{K}}\right)}=f(\omega) \tag{4}
\end{equation*}
$$

On the other hand, it follows from Lemma 5.2 that for any prime $\mathfrak{P}$ of $K_{(N)}$ lying above $\mathfrak{p}, \overline{\mathfrak{P}}$ is also a prime of $K_{(N)}$ lying above $\overline{\mathfrak{p}}$ which is different from $\mathfrak{P}$. Now that

$$
f(\omega)^{\left(\frac{K_{(N)} / K}{p}\right)} \equiv f(\omega)^{p}(\bmod \mathfrak{P}) \quad \text { and } \quad f\left(\frac{\omega}{p}\right)^{\left(\frac{K_{(N)} / K}{\bar{p}}\right)} \equiv f\left(\frac{\omega}{p}\right)^{p}(\bmod \overline{\mathfrak{P}})
$$

we deduce by (3) and (4) that

$$
\left(f(\omega)^{p}-f\left(\frac{\omega}{p}\right)\right)\left(f(\omega)-f\left(\frac{\omega}{p}\right)^{p}\right) \equiv 0(\bmod \mathfrak{P} \overline{\mathfrak{P}}) .
$$

Therefore we conclude by the fact

$$
p \mathcal{O}_{K_{(N)}}=\left(\mathfrak{p} \mathcal{O}_{K_{(N)}}\right)\left(\overline{\mathfrak{p}} \mathcal{O}_{K_{(N)}}\right)=\left(\mathfrak{P}_{1} \mathfrak{P}_{2} \cdots \mathfrak{P}_{g}\right)\left(\overline{\mathfrak{P}}_{1} \overline{\mathfrak{P}}_{2} \cdots \overline{\mathfrak{P}}_{g}\right)
$$

for some distinct primes $\mathfrak{P}_{1}, \mathfrak{P}_{2}, \ldots, \mathfrak{P}_{g}$ of $K_{(N)}$ and the Chinese remainder theorem that

$$
\left(f(\omega)^{p}-f\left(\frac{\omega}{p}\right)\right)\left(f(\omega)-f\left(\frac{\omega}{p}\right)^{p}\right) \equiv 0\left(\bmod p \mathcal{O}_{K_{(N)}}\right) .
$$

## 6. Artin symbols over $\mathbb{Q}$

The field $K_{(N)}$ is a Galois extension of $\mathbb{Q}$, however, it is not necessarily abelian. In this last section, we shall consider the $\operatorname{Artin} \operatorname{symbol}\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)$ for a prime $\mathfrak{P}$ of $K_{(N)}$.
Lemma 6.1. If $t$ is a nonzero integer relatively prime to $N$, then the order of $\left(\frac{K_{(N)} / K}{t \mathcal{O}_{K}}\right)$ in $\operatorname{Gal}\left(K_{(N)} / K\right)$ is the smallest positive integer $\ell$ such that $t^{\ell} \equiv 1$ or $-1(\bmod N)$.

Proof. See Propositions 2.5, 2.6 and [14, (3.5)].
Let $\mathfrak{c}$ denote the complex conjugation on $K_{(N)}$.
Theorem 6.2. Let $p$ be a prime relatively prime to $N d_{K}, \mathfrak{p}$ be a prime of $K$ lying above $p$, and $\mathfrak{P}$ be a prime of $K_{(N)}$ lying above $\mathfrak{p}$. Let $\ell$ be the smallest positive integer such that $p^{\ell} \equiv 1$ or $-1(\bmod N)$, and let $\sigma$ be an element of $\operatorname{Gal}\left(K_{(N)} / K\right)$ which maps $\overline{\mathfrak{P}}$ to $\mathfrak{P}$.
(i) If $p$ splits completely in $K$, then

$$
\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)=\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right) .
$$

(ii) If $p$ is inert in $K$, then

$$
D_{\mathfrak{P} / \mathbb{Q}}=\left\langle(\mathfrak{c} \sigma)^{\frac{\ell}{2^{2}}}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{2^{e}}\right\rangle
$$

where $e \geq 0$ is the exponent of 2 in the prime factorization of $\ell$.
(iii) If $p$ is inert in $K$ and $\ell$ is odd, then

$$
\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)=(\mathfrak{c} \sigma)^{\ell}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{\frac{\ell+1}{2}} .
$$

Proof. Note that $\operatorname{Gal}\left(K_{(N)} / K\right)$ is a subgroup of $\operatorname{Gal}\left(K_{(N)} / \mathbb{Q}\right)$ and $\operatorname{Gal}\left(\left(\mathcal{O}_{K_{(N)}} / \mathfrak{P}\right) /\left(\mathcal{O}_{K} / \mathfrak{p}\right)\right)$ is a subgroup of $\operatorname{Gal}\left(\left(\mathcal{O}_{K_{(N)}} / \mathfrak{P}\right) /(\mathbb{Z} / p \mathbb{Z})\right)$.
(i) Since $p$ splits completely in $K, \mathcal{O}_{K} / \mathfrak{p}$ is isomorphic to $\mathbb{Z} / p \mathbb{Z}$. Thus $\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)$ coincides with $\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}^{\mathcal{Q}}}\right)$.
(ii) Since $p$ is inert in $K$, we get $\mathfrak{p}=p \mathcal{O}_{K}$. Then we achieve by Lemma 6.1 that

$$
\begin{equation*}
\left|D_{\mathfrak{P} / K}\right|=\ell \quad \text { and so } \quad\left|D_{\mathfrak{P} / \mathbb{Q}}\right|=2 \ell . \tag{5}
\end{equation*}
$$

Moreover, since $\mathfrak{c} \sigma \in D_{\mathfrak{P} / \mathbb{Q}} \backslash D_{\mathfrak{P} / K}$, we obtain

$$
D_{\mathfrak{P} / \mathbb{Q}}=D_{\mathfrak{P} / K} \cup(\mathfrak{c} \sigma) D_{\mathfrak{P} / K},
$$

which yields that

$$
\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)=(\mathfrak{c} \sigma)\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{v} \quad \text { for some integer } v .
$$

Write $\ell=2^{e} g$ for an odd positive integer $g$. If we let $n$ be the order of $(\mathfrak{c} \sigma)^{g}$, then we see by (5) that $n$ is a divisor of $2^{e+1}$. Furthermore, we deduce again by (5) that

$$
2=\left|\left\langle\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)^{\ell}\right\rangle\right|=\left|\left\langle(\mathfrak{c} \sigma)^{\ell}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{v \ell}\right\rangle\right|=\left|\left\langle(\mathfrak{c} \sigma)^{\ell}\right\rangle\right|=\left|\left\langle\left\{(\mathfrak{c} \sigma)^{g}\right\}^{2^{e}}\right\rangle\right|=\frac{n}{\operatorname{gcd}\left(n, 2^{e}\right)},
$$

from which it follows that $n=2^{e+1}$. Since the order of $\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{2^{e}}$ is $g$ which is relatively prime to $2^{e+1}$, the order of $(\mathfrak{c} \sigma)^{g}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{2^{e}}$ is $2^{e+1} g=2 \ell$. Hence

$$
D_{\mathfrak{P} / \mathbb{Q}}=\left\langle(\mathfrak{c} \sigma)^{g}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{2^{e}}\right\rangle .
$$

(iii) By the fact $\left[\operatorname{Gal}\left(K_{(N)} / \mathbb{Q}\right): \operatorname{Gal}\left(K_{(N)} / K\right)\right]=2$ and the definition of Artin symbol, we have

$$
\begin{equation*}
\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)^{2}=\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right) . \tag{6}
\end{equation*}
$$

Since $\mathfrak{c} \sigma$ is in $D_{\mathfrak{Y} / \mathbb{Q}}$, we find by (5) that

$$
\begin{equation*}
\left\{(\mathfrak{c} \sigma)^{\ell}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{\frac{\ell+1}{2}}\right\}^{2}=(\mathfrak{c} \sigma)^{2 \ell}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{\ell+1}=\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right) . \tag{7}
\end{equation*}
$$

Here, $\frac{\ell+1}{2}$ is an integer because $\ell$ is odd. If we let $\phi: D_{\mathfrak{P} / \mathbb{Q}} \rightarrow \mathbb{Z} / 2 \ell \mathbb{Z}$ be the isomorphism sending $\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)$ to $1+2 \ell \mathbb{Z}$, then we establish that

$$
\begin{equation*}
\phi\left(D_{\mathfrak{P} / K}\right)=\left\langle\phi\left(\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)\right)\right\rangle=\left\langle 2 \phi\left(\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)\right)\right\rangle=\langle 2+2 \ell \mathbb{Z}\rangle \tag{8}
\end{equation*}
$$

by (6), and

$$
\begin{equation*}
2 \phi\left((\mathfrak{c} \sigma)^{\ell}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{\frac{\ell+1}{2}}\right)=2+2 \ell \mathbb{Z} \tag{9}
\end{equation*}
$$

by (6) and (7). On the other hand, since $(\mathfrak{c} \sigma)^{\ell}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{\frac{\ell+1}{2}}$ does not belong to $\operatorname{Gal}\left(K_{(N)} / K\right)$ due to the fact that $\ell$ is odd, we derive from (8) and (9) that

$$
\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)=(\mathfrak{c} \sigma)^{\ell}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{\frac{\ell+1}{2}}
$$

as desired.

Remark 5. By Theorem 6.2, we have

$$
\begin{equation*}
\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)=(\mathfrak{c} \sigma)^{u}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{v} \quad \text { for some integers } u \text { and } v . \tag{10}
\end{equation*}
$$

Now, consider the case where $p$ is inert and $\ell$ is even. If $\mathfrak{c} \in D_{\mathfrak{Y} / \mathbb{Q}}$, then we see that

$$
\begin{aligned}
\left(\frac{K_{(N)} / \mathbb{Q}}{\mathfrak{P}}\right)^{\ell} & =\mathfrak{c}^{u \ell} \sigma^{u \ell}\left(\frac{K_{(N)} / K}{\mathfrak{p}}\right)^{v \ell} \text { by }(10) \text { and the fact that } D_{\mathfrak{P} / \mathbb{Q}} \text { is abelian } \\
& =\operatorname{id}_{K_{(N)}} \text { because } \mathfrak{c} \text { is of order } 2 \text { and }\left|D_{\mathfrak{P} / K}\right|=\ell \text { is even. }
\end{aligned}
$$

But this contradicts the fact $\left|D_{\mathfrak{P} / \mathbb{Q}}\right|=2 \ell$. Therefore, in this case, $\mathfrak{c}$ does not belong to $D_{\mathfrak{P} / \mathbb{Q}}$.

Remark 6. We observe that $\operatorname{Gal}\left(K_{(N)} / \mathbb{Q}\right)=\operatorname{Gal}\left(K_{(N)} / K\right) \rtimes\langle\mathfrak{c}\rangle$. The action of the group $\Gamma_{1}(N)$ on the set $\mathcal{Q}_{N}\left(d_{K}\right)$ can be extended to the set of definite quadratic forms
$\mathcal{Q}_{N}^{ \pm}\left(d_{K}\right)=\left\{a x^{2}+b x y+c y^{2} \in \mathbb{Z}[x, y] \mid b^{2}-4 a c=d_{K}, \operatorname{gcd}(a, b, c)=\operatorname{gcd}(a, N)=1\right\}$, which induces the equivalence denote by $\sim_{N}^{ \pm}$. Recently, Jung et al. showed that the set $\mathcal{C}_{N}^{ \pm}\left(d_{K}\right)=\mathcal{Q}_{N}^{ \pm}\left(d_{K}\right) / \sim_{N}^{ \pm}$can be regarded as a group isomorphic to $\operatorname{Gal}\left(K_{(N)} / \mathbb{Q}\right)\left(\left[9\right.\right.$, Theorem 9.2]), and further defined the $\mathcal{C}_{N}^{ \pm}\left(d_{K}\right)$-class invariants as special values of modular functions of level $N$ ( $[9$, Definition 9.4 and Theorem 9.6]).

## References

[1] W. W. Adams and L. J. Goldstein, Introduction to Number Theory, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1976.
[2] B. Cho, Modular equations for congruence subgroups of genus zero (II), J. Number Theory 231 (2022), 48-79.
[3] D. A. Cox, Primes of the Form $x^{2}+n y^{2}-$ Fermat, Class field theory, and Complex Multiplication, 3rd ed. with solutions, with contributions by Roger Lipsett, AMS Chelsea Publishing, Providence, R.I., 2022.
[4] F. Diamond and J. Shurman, A First Course in Modular Forms, Grad. Texts in Math. 228, Springer-Verlag, New York, 2005.
[5] 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.
[6] C. F. Gauss, Disquisitiones Arithmeticae, Leipzig, 1801.
[7] H. Hasse, Neue Begründung der komplexen Multiplikation I, II, J. reine angew. Math. 157 (1927), 115-139, 165 (1931), 64-88.
[8] G. J. Janusz, Algebraic Number Fields, 2nd ed., Grad. Studies in Math. 7, Amer. Math. Soc., Providence, R.I., 1996.
[9] 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.
[10] H. Y. Jung, J. K. Koo, D. H. Shin and D. S. Yoon, Arithmetic properties of orders in imaginary quadratic fields, https://arxiv.org/abs/2205.10754.
[11] S. Lang, Elliptic Functions, With an appendix by J. Tate, 2nd ed., Grad. Texts in Math. 112, Spinger-Verlag, New York, 1987.
[12] J. Neukirch, Class Field Theory, Grundlehren der mathematischen Wissenschaften 280, Springer-Verlag, Berlin, 1986.
[13] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami Shoten and Princeton University Press, Princeton, N.J., 1971.
[14] 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.
[15] H. Weber, Zur Theorie der Elliptischen Functionen, Acta Math. 6 (1885), no. 1, 329-416.
[16] D. S. Yoon, Ray class invariants in terms of extended form class groups, East Asian Math. J. 37 (2021), no. 1, 87-95.

Dong Sung Yoon
Department of Mathematics Education
Pusan National University
Busan 46241
Republic of Korea
Email address: dsyoon@pusan.ac.kr


[^0]:    Received October 12, 2023; Accepted January 23, 2024.
    2010 Mathematics Subject Classification. Primary 11R37; Secondary 11E12, 11F03.
    Key words and phrases. Artin symbols, complex multiplication, form class groups, Kronecker's congruence relation.

    This work was supported by a 2-Year Research Grant of Pusan National University.

