

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 $(\frac{K_{(N)}/K}{\mathfrak p})$ 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

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

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

$$D_{\mathfrak{P}} \simeq \widetilde{G} = \operatorname{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})).$$

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

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

where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is the norm of \mathfrak{p} ([3, Lemma 5.19]). This unique element σ 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, §9.1].

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

Received October 12, 2023; Accepted January 23, 2024.

 $^{2010\ \}textit{Mathematics Subject Classification}.\ \text{Primary 11R37; Secondary 11E12, 11F03}.$

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.

modulo $N\mathcal{O}_K$, namely, $\mathcal{C}(N\mathcal{O}_K) = I(N\mathcal{O}_K)/P_1(N\mathcal{O}_K)$ where $I(N\mathcal{O}_K)$ is the group of fractional ideals of K relatively prime to $N\mathcal{O}_K$ and $P_1(N\mathcal{O}_K)$ is its subgroup defined by

$$P_1(N\mathcal{O}_K) = \langle \nu \mathcal{O}_K \mid \nu \in \mathcal{O}_K \setminus \{0\} \text{ and } \nu \equiv 1 \pmod{N\mathcal{O}_K} \rangle.$$

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

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

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

For a lattice Λ in \mathbb{C} , let $j(\Lambda)$ be the j-invariant of any elliptic curve over \mathbb{C} isomorphic to \mathbb{C}/Λ . 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 $\mathfrak{p} \neq \overline{\mathfrak{p}}$

$$j(\mathfrak{p}^{-1}\mathfrak{a}) \equiv j(\mathfrak{a})^p \pmod{\mathfrak{P}} \quad \text{with } p = N(\mathfrak{p})$$
 (1)

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 $\mathbb{H}=\{\tau\in\mathbb{C}\mid \mathrm{Im}(\tau)>0\}$. Prior to the work of Hasse, Weber ([15]) had derived a weaker form of (1) in such a way that for each prime p

$$\Phi_p(x, y) \equiv (x^p - y)(x - y^p) \pmod{p\mathbb{Z}[x, y]}.$$
 (2)

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 $\left(\frac{K_{(N)}/\mathbb{Q}}{\mathfrak{B}}\right)$ 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]. \Box

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

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

Proof. See [11, Theorem 5 in Chapter 10] or [13, Theorem 5.7]. \square

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 $\operatorname{Gal}(H_K/K)$ 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 $[\nu_1, \nu_2]$ the lattice generated by ν_1 and ν_2 , namely, $[\nu_1, \nu_2] = \mathbb{Z}\nu_1 + \mathbb{Z}\nu_2$.

Lemma 2.3. Let p be a prime.

- (i) p splits completely in K if and only if $(\frac{d_K}{p}) = 1$. In this case, there is an integer u such $u^2 \equiv d_K \pmod{4p}$. Furthermore, $\mathfrak{p} = \left[\frac{-u + \sqrt{d_K}}{2}, p\right]$ is a prime of K such that $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$.
- (ii) p is inert in K if and only if $(\frac{d_K}{n}) = -1$.
- (iii) p is ramified in K if and only if $(\frac{d_K}{p}) = 0$ (i.e., $p \mid d_K$). In this case,

$$\mathfrak{p} = \left\{ \begin{array}{ll} \left[\frac{2+\sqrt{d_K}}{2},\,2\right] & \text{if } p=2 \text{ and } \frac{d_K}{4} \equiv 3 \pmod{4}, \\ \left[\frac{-d_K+\sqrt{d_K}}{2},\,p\right] & \text{otherwise} \end{array} \right.$$

is a prime of K satisfying $p\mathcal{O}_K = \mathfrak{p}^2$.

Proof. See $[1, Theorems 3 and 4 in <math>\S9.5]$.

Let τ_K be the element of \mathbb{H} defined by

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

and so $\mathcal{O}_K = [\tau_K, 1]$ ([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 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 $u^2 \equiv d_K \pmod{4p}$ by Lemma 2.3 (i), then we have

$$j(\tau_K)^{\left(\frac{H_K/K}{\mathfrak{p}}\right)} = j\left(\frac{u+\sqrt{d_K}}{2p}\right).$$

- (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

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

Proof. Note that if Λ and Λ' are homothetic lattices in \mathbb{C} , then $j(\Lambda) = j(\Lambda')$ ([3, Theorem 10.9]). By Proposition 2.1, $j(\mathcal{O}_K) = j(\tau_K)$ generates H_K over K.

(i) Since $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, we obtain by Proposition 2.2 that

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

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

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

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

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

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

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

whose Fourier expansions with respect to $q_{\tau}^{\frac{1}{N}}$ $(q_{\tau} = e^{2\pi i \tau})$ have coefficients in the Nth cyclotomic field $\mathbb{Q}(\zeta_N)$ where $\zeta_N = e^{\frac{2\pi i}{N}}$. As is well known, \mathcal{F}_N is a Galois extension of \mathcal{F}_1 whose Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$.

Proposition 2.5. Let $\alpha \in GL_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$ and $f \in \mathcal{F}_N$ with Fourier expansion $f = \sum_{n \gg -\infty} c_n q_{\tau}^{\frac{n}{N}}$ $(c_n \in \mathbb{Q}(\zeta_N))$.

(i) If $\alpha \in \operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$, then $f^{\alpha} = f \circ \widetilde{\alpha}$ where $\widetilde{\alpha}$ is any preimage of α via the reduction $\operatorname{SL}_2(\mathbb{Z}) \to \operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$.

(ii) If $\alpha = \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}$ for some integer d relatively prime to N, then $f^{\alpha} = \sum_{n \gg -\infty} c_n^{\sigma_d} q_{\tau}^{\frac{n}{N}}$ where σ_d is the automorphism of $\mathbb{Q}(\zeta_N)$ defined by $\zeta_N \mapsto \zeta_N^d$.

Proof. See [11, Theorem 3 in Chapter 6] and [13, Proposition 6.9 (1)]. \Box

Essentially due to Hasse ([7]) we get the following proposition.

Proposition 2.6. We have $K_{(N)} = K(f(\tau_K) \mid f \in \mathcal{F}_N \text{ is finite at } \tau_K)$.

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 $Q_N(d_K)$ be the set of binary quadratic forms given by

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

The congruence subgroup

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

of $\mathrm{SL}_2(\mathbb{Z})$ acts on the set $\mathcal{Q}_N(d_K)$ from the right so as to have

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

This action of $\Gamma_1(N)$ naturally defines the equivalence relation \sim_N on $\mathcal{Q}_N(d_K)$ as follows: for $Q, Q' \in \mathcal{Q}_N(d_K)$

$$Q \sim_N Q' \iff Q' = Q^{\gamma} \text{ for some } \gamma \in \Gamma_1(N).$$

Denote by $C_N(d_K)$ the set of equivalence classes, that is, $C_N(d_K) = Q_N(d_K) / \sim_N$. For each $Q = ax^2 + bxy + cy^2 \in Q_N(d_K)$, let ω_Q be the zero of the quadratic polynomial Q(x, 1) lying in \mathbb{H} so that

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

Proposition 3.1. One can equip the set $C_N(d_K)$ with the group structure in such a way that the mapping

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

 $[Q] \mapsto [[\omega_Q, 1]]$

becomes a well-defined isomorphism.

Proof. See [5, Theorem 2.9 and Remark 2.10 (iv)]. \Box

- Remark 2. (i) We shall call the group $C_N(d_K)$ the extended form class group of discriminant d_K and level N.
 - (ii) For a negative integer D such that $D \equiv 0$ or $1 \pmod{4}$, 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 $\min(\tau_K, \mathbb{Q}) = x^2 + b_K x + c_K \ (\in \mathbb{Z}[x])$. 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 $\mathfrak{a} \in I(N\mathcal{O}_K)$. By Proposition 3.1, there exists a quadratic form $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$ so that $[\mathfrak{a}] = [[\omega_Q, 1]]$ in $\mathcal{C}(N\mathcal{O}_K)$. If $f \in \mathcal{F}_N$ is finite at τ_K , then we establish

$$f(\tau_K)^{\left(\frac{K_{(N)}/K}{\mathfrak{a}}\right)} = f^{\left[\frac{1-a'(\frac{b+b_K}{2})}{a'}\right]\left(-\overline{\omega}_O\right)}$$

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

Proof. See Proposition 2.6 and [16, Theorem 3.5].

Remark 3. Note that b and b_K have the same parity for $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$ because $b^2 - 4ac = d_K = b_K^2 - 4c_K$.

4. Description of Artin symbols

In this section, for a prime \mathfrak{p} of K we shall describe the 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 $(s\tau_K + t)\mathcal{O}_K$ is relatively prime to $N\mathcal{O}_K$. If $f \in \mathcal{F}_N$ is finite at τ_K , then we have

$$f(\tau_K)^{\left(\frac{K_{(N)}/K}{(s\tau_K+t)\mathcal{O}_K}\right)} = f\begin{bmatrix} t-b_K s & -c_K s \\ s & t \end{bmatrix} (\tau_K).$$

Proof. See [14, (3.4)].

Remark 4. (i) Let $\widehat{\mathbb{Z}} = \prod_{p: \text{primes}} \mathbb{Z}_p$ and $\widehat{K} = K \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. Let $[\cdot, K]: \widehat{K}^* \to \text{Gal}(K^{\text{ab}}/K)$ be the Artin reciprocity map for (finite) ideles, where K^{ab} is the maximal abelian extension of K. Then the class field theory

asserts that $[\cdot, K]$ is a surjection with kernel K^* ([3, §15.F] and [12, §IV.6]). Here we observe that

$$\left(\frac{K_{(N)}/K}{(s\tau_K + t)\mathcal{O}_K}\right) = [(x_p)_p, K]|_{K_{(N)}} \quad \text{where } x_p = \begin{cases} 1 & \text{if } p \mid N, \\ s\tau_K + t & \text{if } p \nmid N. \end{cases}$$

(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 $\operatorname{Gal}(K^{\operatorname{ab}}/H_{\mathcal{O}})$ as the image of a subset of \widehat{K}^* via the reciprocity map $[\cdot, K]$ ([14, §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 τ_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 $u^2 \equiv d_K \pmod{4p}$ by Lemma 2.3 (i), then

$$f(\tau_K)^{\left(\frac{K_{(N)}/K}{\mathfrak{p}}\right)} = f^{\left[\begin{array}{c} p - \frac{u + b_K}{2} \\ 0 & 1 \end{array}\right]} \left(\frac{u + \sqrt{d_K}}{2p}\right).$$

(ii) If p is inert in K, then

$$f(\tau_K)^{\left(\frac{K_{(N)}/K}{\mathfrak{p}}\right)} = f^{\begin{bmatrix}p & 0\\ 0 & p\end{bmatrix}}(\tau_K).$$

(iii) If p is ramified in K, then

$$f(\tau_K)^{\left(\frac{K_{(N)}/K}{\mathfrak{p}}\right)} = \left\{ \begin{array}{ll} f^{\left[\frac{2}{0} - \frac{-2+b_K}{2}\right]} \left(\frac{-2+\sqrt{d_K}}{4}\right) & if \ p = 2 \ and \ \frac{d_K}{4} \equiv 3 \ (\bmod \ 4), \\ f^{\left[\frac{p}{0} - \frac{d_K+b_K}{2}\right]} \left(\frac{d_K+\sqrt{d_K}}{2p}\right) & otherwise. \end{array} \right.$$

Proof. (i) We see that

$$\mathfrak{p}=p\mathcal{O}_K\left[\frac{-u+\sqrt{d_K}}{2p},\,1\right]=p\mathcal{O}_K\left[\omega_Q,\,1\right]\quad\text{with }Q=px^2+uxy+\frac{u^2-d_K}{4p}y^2.$$

Thus we achieve that

$$\begin{split} f(\tau_K)^{\left(\frac{K_{(N)}/K}{\mathfrak{p}}\right)} &= f(\tau_K)^{\left(\frac{K_{(N)}/K}{\mathfrak{p}\mathcal{O}_K}\right)\left(\frac{K_{(N)}/K}{[\omega_Q,1]}\right)} \\ &= f^{\left[\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right]}(\tau_K)^{\left(\frac{K_{(N)}/K}{[\omega_Q,1]}\right)} \text{ by Lemma 4.1} \\ &= f^{\left[\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & -p'\left(\frac{u+b_K}{[\omega_Q,1]}\right) \end{smallmatrix}\right]}\left(\frac{u+\sqrt{d_K}}{2p}\right) \\ &\text{where } p' \text{ is an integer such that } pp' \equiv 1 \text{ (mod } N) \text{ by Proposition 3.2} \\ &= f^{\left[\begin{smallmatrix} p & -\frac{u+b_K}{2} \\ 0 & 1 \end{smallmatrix}\right]}\left(\frac{u+\sqrt{d_K}}{2p}\right). \end{split}$$

(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

$$\mathfrak{p} = \begin{cases} 2\mathcal{O}_{K} \left[\frac{2+\sqrt{d_{K}}}{4}, 1 \right] & \text{if } p = 2 \text{ and } \frac{d_{K}}{4} \equiv 3 \pmod{4}, \\ p\mathcal{O}_{K} \left[\frac{-d_{K}+\sqrt{d_{K}}}{2p}, 1 \right] & \text{otherwise} \end{cases}$$

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

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

$$\begin{split} f(\tau_K)^{\left(\frac{K_{(N)}/K}{\mathfrak{p}}\right)} &= f(\tau_K)^{\left(\frac{K_{(N)}/K}{\mathfrak{p}\mathcal{O}_K}\right)\left(\frac{K_{(N)}/K}{\lfloor \omega_{\mathcal{Q}}, 1\rfloor}\right)} \\ &= \begin{cases} f^{\left[\frac{2}{0} - \frac{-2+b_K}{2}\right]} \left(\frac{-2+\sqrt{d_K}}{4}\right) & \text{if } p = 2 \text{ and } \frac{d_K}{4} \equiv 3 \pmod{4}, \\ f^{\left[\frac{p}{0} - \frac{d_K+b_K}{2}\right]} \left(\frac{d_K+\sqrt{d_K}}{2p}\right) & \text{otherwise.} \end{cases} \end{split}$$

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 $u^2 \equiv d_K \pmod{4p}$ by Lemma 2.3, then

$$f^{\left[p-\frac{u+b_K}{2}\right]}\left(\frac{u+\sqrt{d_K}}{2p}\right) \equiv f(\tau_K)^p \pmod{\mathfrak{P}}.$$

(ii) If p is inert in K, then

$$f^{\begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix}}(\tau_K) \equiv f(\tau_K)^{p^2} \pmod{\mathfrak{P}}.$$

(iii) If p is ramified in K, then

$$\begin{cases} f \begin{bmatrix} 2 - \frac{-2+b_K}{2} \end{bmatrix} \left(\frac{-2+\sqrt{d_K}}{4} \right) \equiv f(\tau_K)^p \pmod{\mathfrak{P}} & if \ p = 2 \ and \ \frac{d_K}{4} \equiv 3 \ (\text{mod } 4), \\ f \begin{bmatrix} p - \frac{d_K + b_K}{2} \\ 1 \end{bmatrix} \left(\frac{d_K + \sqrt{d_K}}{2p} \right) \equiv f(\tau_K)^p \ (\text{mod } \mathfrak{P}) & otherwise. \end{cases}$$

Proof. Since f is integral over $\mathbb{Z}[j]$ and $j(\tau_K)$ is an algebraic integer by Proposition 2.1, $f(\tau_K)$ is also an algebraic integer. Furthermore, $f(\tau_K)$ 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 (mod 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 $u^2 \equiv d_K \pmod{4p}$ by Lemma 2.3, then we have

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

Proof. Since f is integral over $\mathbb{Z}[j]$ and belongs to \mathcal{F}_N , $f(\tau_K)$ 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 $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ by Lemma 2.3 (i) and derive that

$$f(\tau_K)^{\left(\frac{K_{(N)}/K}{p}\right)} = f^{\left[\frac{p}{0} - \frac{u+b_K}{2}\right]} \left(\frac{\omega}{p}\right) \text{ by Theorem 4.2 (i)}$$

$$= f^{\left[\frac{1}{0} \frac{0}{p}\right] \left[\frac{p}{0} - \frac{u+b_K}{2}\right]} \left(\frac{\omega}{p}\right) \text{ where } p' \text{ is an integer such that } pp' \equiv 1 \pmod{N}$$

$$= f^{\left[\frac{p}{0} - \frac{u+b_K}{2}\right]} \left(\frac{\omega}{p}\right) \text{ by Proposition 2.5 (ii)}$$

$$= f\left(\frac{\omega}{p}\right) \text{ by Proposition 2.5 (i)}$$

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

$$f(\tau_K) = f\left(\omega - \frac{u + b_K}{2}\right) = f\left(\begin{bmatrix} 1 & -\frac{u + b_K}{2} \\ 0 & 1 \end{bmatrix}(\omega)\right) = f(\omega)$$

because f is modular for $\Gamma_1(N)$. Hence we obtain that

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

since $p \equiv \pm 1 \pmod{N}$ and f is modular for $\Gamma_1(N)$.

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

$$f\left(\frac{\omega}{p}\right)^{\left(\frac{K_{(N)}/K}{\overline{p}}\right)} = f(\omega)^{\left(\frac{K_{(N)}/K}{\overline{p}}\right)\left(\frac{K_{(N)}/K}{\overline{p}}\right)} = f(\omega)^{\left(\frac{K_{(N)}/K}{\overline{pO_K}}\right)} = f(\omega). \tag{4}$$

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

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

we deduce by (3) and (4) that

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

Therefore we conclude by the fact

$$p\mathcal{O}_{K_{(N)}} = (\mathfrak{p}\mathcal{O}_{K_{(N)}})(\overline{\mathfrak{p}}\mathcal{O}_{K_{(N)}}) = (\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g)(\overline{\mathfrak{P}}_1\overline{\mathfrak{P}}_2\cdots\overline{\mathfrak{P}}_g)$$

for some distinct primes $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ of $K_{(N)}$ and the Chinese remainder theorem that

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

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 Artin 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 $\operatorname{Gal}(K_{(N)}/K)$ is the smallest positive integer ℓ such that $t^\ell \equiv 1$ or $-1 \pmod{N}$.

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 Nd_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 ℓ be the smallest positive integer such that $p^{\ell} \equiv 1$ or $-1 \pmod{N}$, and let σ be an element of $\operatorname{Gal}(K_{(N)}/K)$ 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

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

where $e \ge 0$ is the exponent of 2 in the prime factorization of ℓ .

(iii) If p is inert in K and ℓ 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 $\operatorname{Gal}(K_{(N)}/K)$ is a subgroup of $\operatorname{Gal}(K_{(N)}/\mathbb{Q})$ and $\operatorname{Gal}((\mathcal{O}_{K_{(N)}}/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ is a subgroup of $\operatorname{Gal}((\mathcal{O}_{K_{(N)}}/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z}))$.

- (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 $\left(\frac{K_{(N)}/\mathbb{Q}}{\mathfrak{B}}\right)$.
- (ii) Since p is inert in K, we get $\mathfrak{p} = p\mathcal{O}_K$. Then we achieve by Lemma 6.1 that

$$|D_{\mathfrak{P}/K}| = \ell$$
 and so $|D_{\mathfrak{P}/\mathbb{Q}}| = 2\ell$. (5)

Moreover, since $\mathfrak{c}\sigma \in D_{\mathfrak{B}/\mathbb{O}} \setminus D_{\mathfrak{B}/K}$, 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

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

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

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

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

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

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

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

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

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

by (6), and

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

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 $\operatorname{Gal}(K_{(N)}/K)$ due to the fact that ℓ 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

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

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

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

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

Remark 6. We observe that $\operatorname{Gal}(K_{(N)}/\mathbb{Q}) = \operatorname{Gal}(K_{(N)}/K) \rtimes \langle \mathfrak{c} \rangle$. The action of the group $\Gamma_1(N)$ on the set $\mathcal{Q}_N(d_K)$ can be extended to the set of definite quadratic forms

 $Q_N^{\pm}(d_K) = \{ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y] \mid b^2 - 4ac = d_K, \gcd(a, b, c) = \gcd(a, N) = 1\},$ which induces the equivalence denote by \sim_N^{\pm} . Recently, Jung et al. showed that the set $\mathcal{C}_N^{\pm}(d_K) = Q_N^{\pm}(d_K) / \sim_N^{\pm}$ can be regarded as a group isomorphic to $\operatorname{Gal}(K_{(N)}/\mathbb{Q})$ ([9, Theorem 9.2]), and further defined the $\mathcal{C}_N^{\pm}(d_K)$ -class invariants as special values of modular functions of level N ([9, Definition 9.4 and Theorem 9.6]).

References

- 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 $x^2 + ny^2$ -Fermat, Class field theory, and Complex Multiplication, 3rd ed. with solutions, with contributions by Roger Lipsett, AMS Chelsea Publishing, Providence, R.I., 2022.

- [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