

RAY CLASS INVARIANTS IN TERMS OF EXTENDED FORM CLASS GROUPS

DONG SUNG YOON

ABSTRACT. Let K be an imaginary quadratic field with \mathcal{O}_K its ring of integers. For a positive integer N , let $K_{(N)}$ be the ray class field of K modulo $N\mathcal{O}_K$, and let \mathcal{F}_N be the field of meromorphic modular functions of level N whose Fourier coefficients lie in the N th cyclotomic field. For each $h \in \mathcal{F}_N$, we construct a ray class invariant as its special value in terms of the extended form class group, and show that the invariant satisfies the natural transformation formula via the Artin map in the sense of Siegel and Stark. Finally, we establish an isomorphism between the extended form class group and $\text{Gal}(K_{(N)}/K)$ without any restriction on K .

1. Introduction

Let K be an imaginary quadratic field of discriminant d_K and \mathcal{O}_K be its ring of integers. For a positive integer N , let $\mathcal{Q}_N(d_K)$ be the set of primitive positive definite binary quadratic forms of discriminant d_K whose leading coefficients are prime to N , that is,

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

We define the equivalence relation $\sim_{\Gamma_1(N)}$ on $\mathcal{Q}_N(d_K)$ as

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

where $\Gamma_1(N)$ is the congruence subgroup of $\text{SL}_2(\mathbb{Z})$ given by

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

When $N = 1$, it is called the *Gauss proper equivalence* ([1, §2]).

Let $\text{Cl}(N\mathcal{O}_K)$ be the ray class group of K modulo $N\mathcal{O}_K$, and let $K_{(N)}$ be the corresponding ray class field so that $\text{Cl}(N\mathcal{O}_K)$ is isomorphic to $\text{Gal}(K_{(N)}/K)$ via the Artin map for modulus $N\mathcal{O}_K$. It is well known by class field theory that

Received January 6, 2021; Accepted January 20, 2021.

2010 *Mathematics Subject Classification.* Primary 11E16; Secondary 11F03, 11R37.

Key words and phrases. binary quadratic forms, class field theory, modular functions.

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

©2021 The Youngnam Mathematical Society
 (pISSN 1226-6973, eISSN 2287-2833)

every finite abelian extension of K is contained in the ray class field $K_{(N)}$ for some N ([1, §8]). Recently, Eum et al. showed that the map

$$\begin{aligned} \mathcal{Q}_N(d_K)/\sim_{\Gamma_1(N)} &\rightarrow \text{Cl}(N\mathcal{O}_K) \\ [Q] &\mapsto [[\omega_Q, 1]] = [\mathbb{Z}\omega_Q + \mathbb{Z}] \end{aligned} \quad (1)$$

is bijective, where ω_Q is the zero of $Q(x, 1)$ in the complex upper-half plane \mathbb{H} . Hence the set of equivalence classes

$$C_N(d_K) = \mathcal{Q}_N(d_K)/\sim_{\Gamma_1(N)}$$

can be regarded as a group isomorphic to $\text{Cl}(N\mathcal{O}_K)$ ([2, Theorem 2.9]). See also [4]. We call this group $C_N(d_K)$ the *extended form class group* of discriminant d_K and level N . Let \mathcal{F}_N be the field of meromorphic modular functions of level N whose Fourier coefficients lie in the N th cyclotomic field. Moreover, let τ_K be the zero associated with the principal form $x^2 + b_Kxy + c_Ky^2$ in $\mathcal{Q}_N(d_K)$. They further presented the isomorphism

$$\begin{aligned} C_N(d_K) &\rightarrow \text{Gal}(K_{(N)}/K) \\ [Q] = [ax^2 + bxy + cy^2] &\mapsto \left(h(\tau_K) \mapsto h \begin{bmatrix} a & (b-b_K)/2 \\ 0 & 1 \end{bmatrix} (\omega_Q) \mid h \in \mathcal{F}_N \text{ is finite at } \tau_K \right) \end{aligned}$$

when K is different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ ([2, Theorem 3.10]).

In this paper, we shall modify and improve the results of [2]. Without the restriction $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, we shall construct a ray class invariant $h(C)$ in $K_{(N)}$ for each $h \in \mathcal{F}_N$ and $C \in \text{Cl}(N\mathcal{O}_K)$ which satisfies the natural transformation formula

$$h(C)^{\sigma_N(D)} = h(CD) \quad \text{for all } D \in \text{Cl}(N\mathcal{O}_K), \quad (2)$$

where $\sigma_N : \text{Cl}(N\mathcal{O}_K) \rightarrow \text{Gal}(K_{(N)}/K)$ is the Artin map for modulus $N\mathcal{O}_K$ (Theorem 3.2). By using (2), we shall also establish an isomorphism between $C_N(d_K)$ and $\text{Gal}(K_{(N)}/K)$ (Theorem 3.5).

We notice that [2] was definitely inspired by C. L. Siegel's work [8]. When $N \geq 2$, Siegel defined ray class invariants as the special values of one-variable Siegel functions having a transformation formula similar to (2). See also [5, Chapter 19]. Besides, H. M. Stark conjectured that there exists a family of units in some class field of a totally real field which satisfies a transformation formula such as (2) ([9, Conjecture 1]). We hope that this paper together with [4] may provide some clues to Stark's conjecture.

2. Shimura's reciprocity law

In this section, we shall describe the action of an idele group on the field of meromorphic modular functions and Shimura's reciprocity law for later use.

The group $\text{GL}_2^+(\mathbb{R}) = \{\gamma \in \text{GL}_2(\mathbb{R}) \mid \det(\gamma) > 0\}$ acts on the complex upper half plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid \text{Im}(\tau) > 0\}$ by fractional linear transformations. For

a positive integer N , let \mathcal{F}_N be the field of meromorphic modular functions for the principal congruence subgroup

$$\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv I_2 \pmod{N \cdot M_2(\mathbb{Z})}\}$$

whose Fourier coefficients lie in $\mathbb{Q}(\zeta_N)$ with $\zeta_N = e^{2\pi i/N}$.

Proposition 2.1. *The field \mathcal{F}_N is a Galois extension of \mathcal{F}_1 and*

$$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} = G_N \cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\},$$

where

$$G_N = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \mid d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

Let $h(\tau)$ be an element of \mathcal{F}_N whose Fourier expansion is

$$h(\tau) = \sum_{n \gg -\infty} c_n q^{n/N} \quad (c_n \in \mathbb{Q}(\zeta_N))$$

with $q = e^{2\pi i\tau}$.

(i) If $\alpha = \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}$ with $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, then

$$h(\tau)^\alpha = \sum_{n \gg -\infty} c_n^{\sigma_d} q^{n/N},$$

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

(ii) If $\beta \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$, then

$$h(\tau)^\beta = h(\beta'(\tau)),$$

where β' is any element of $\mathrm{SL}_2(\mathbb{Z})$ which maps to β through the reduction $\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$.

Proof. See [6, Proposition 6.21]. □

Let

$$\begin{aligned} \mathcal{F} &= \bigcup_{N=1}^{\infty} \mathcal{F}_N, \\ G_{\mathbb{A}+} &= \prod'_{p: \text{primes}} \mathrm{GL}_2(\mathbb{Q}_p) \times \mathrm{GL}_2^+(\mathbb{R}), \end{aligned}$$

where $'$ denotes the restricted product, that is,

$$\prod'_{p} \mathrm{GL}_2(\mathbb{Q}_p) = \left\{ \alpha = (\alpha_p)_p \in \prod_p \mathrm{GL}_2(\mathbb{Q}_p) \mid \alpha_p \in \mathrm{GL}_2(\mathbb{Z}_p) \text{ for almost all primes } p \right\}.$$

Proposition 2.2. *Let $U = \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$ and $G_+ = \mathrm{GL}_2^+(\mathbb{Q})$ which are subgroups of $G_{\mathbb{A}+}$. Then we have*

$$G_{\mathbb{A}+} = UG_+ = G_+U.$$

Proof. See [6, Lemma 6.19]. □

Proposition 2.3. *There exists a surjective homomorphism*

$$\sigma_{\mathcal{F}} : G_{\mathbb{A}^+} \rightarrow \text{Aut}(\mathcal{F})$$

satisfying the following properties: Let $h \in \mathcal{F}_N$ with a positive integer N .

- (i) $h^{\sigma_{\mathcal{F}}(\gamma)} = h \circ \gamma$ for all $\gamma \in G_+$.
- (ii) For $u = (u_p)_p \in U$, let $\tilde{u} \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\tilde{u} \equiv u_p \pmod{N}$ for all $p \mid N$. Then

$$h^{\sigma_{\mathcal{F}}(u)} = h^{\tilde{u}},$$

where the action of \tilde{u} on h is understood as in Proposition 2.1.

Proof. See [6, §6.6]. □

For a number field F , let $F_{\mathbb{A}}^{\times}$ be the idele group of F and F_{ab} be the maximal abelian extension of F . By class field theory, every element x of $F_{\mathbb{A}}^{\times}$ acts on F_{ab} as an automorphism (cf. [3]). We denote this automorphism by $[x, F]$.

Let K be an imaginary quadratic field. For $\omega \in K \cap \mathbb{H}$, we have the embedding

$$q_{\omega} : K \rightarrow M_2(\mathbb{Q})$$

defined by

$$q_{\omega}(a) \begin{bmatrix} \omega \\ 1 \end{bmatrix} = a \begin{bmatrix} \omega \\ 1 \end{bmatrix} \quad (a \in K).$$

One can continuously extend q_{ω} to an embedding $K_{\mathbb{A}} \rightarrow M_2(\mathbb{Q}_{\mathbb{A}})$, and also denote it by q_{ω} .

Proposition 2.4 (Shimura's Reciprocity Law). *Let $h \in \mathcal{F}$ and $\omega \in K \cap \mathbb{H}$. If h is finite at ω , then $h(\omega)$ belongs to K_{ab} . Moreover, if $s \in K_{\mathbb{A}}^{\times}$, then we get $q_{\omega}(s) \in G_{\mathbb{A}^+}$ and*

$$h(\omega)^{[s, K]} = h^{\sigma_{\mathcal{F}}(q_{\omega}(s^{-1}))}(\omega).$$

Proof. See [7, Lemma 9.5 and Theorem 9.6]. □

3. Ray class invariants in terms of form class group

Let K be an imaginary quadratic field of discriminant d_K , and let $C \in \text{Cl}(N\mathcal{O}_K)$ with a positive integer N . For the principal form $x^2 + b_K xy + c_K y^2$ of discriminant d_K , let τ_K be its associated zero in \mathbb{H} . Take an integral ideal \mathfrak{c} in C and choose a \mathbb{Z} -basis $\{\xi_1, \xi_2\}$ of \mathfrak{c}^{-1} such that $\xi := \xi_1/\xi_2 \in \mathbb{H}$. Since $\mathcal{O}_K = [\tau_K, 1] \subseteq \mathfrak{c}^{-1}$, we have

$$\begin{bmatrix} \tau_K \\ 1 \end{bmatrix} = A \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \tag{3}$$

for some unique $A \in M_2(\mathbb{Z})$. Note that

$$\det(A) > 0 \quad \text{and} \quad \gcd(\det(A), N) = 1 \tag{4}$$

([4, Lemma 6.2 (ii)]). For convenience, we shall denote the reduction of A onto the group $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ by \tilde{A} .

Definition 1. Let $h \in \mathcal{F}_N$ and $C \in \text{Cl}(N\mathcal{O}_K)$. Following the above notations, we define

$$h(C) = h^{\tilde{A}}(\xi).$$

Proposition 3.1. *The value $h(C)$ depends only on C , not on the choice of \mathfrak{c} , ξ_1 , ξ_2 .*

Proof. Let \mathfrak{c}' be an integral ideal in C and choose a \mathbb{Z} -basis $\{\xi'_1, \xi'_2\}$ of \mathfrak{c}'^{-1} such that $\xi' := \xi'_1/\xi'_2 \in \mathbb{H}$. Since $\mathcal{O}_K \subseteq \mathfrak{c}'^{-1}$, we have

$$\begin{bmatrix} \tau_K \\ 1 \end{bmatrix} = A' \begin{bmatrix} \xi'_1 \\ \xi'_2 \end{bmatrix} \quad (5)$$

for some $A' \in M_2(\mathbb{Z})$. By (4), we get $\det(A') > 0$ and $\gcd(\det(A'), N) = 1$. Since $C = [\mathfrak{c}] = [\mathfrak{c}']$, we have

$$\mathfrak{c}' = \nu \mathfrak{c} \quad \text{for some } \nu \in K^\times \text{ such that } \nu \equiv^* 1 \pmod{N\mathcal{O}_K}.$$

Here, $x \equiv^* y \pmod{N\mathcal{O}_K}$ for $x, y \in K^\times$ means that $\text{ord}_{\mathfrak{p}}(\frac{x}{y} - 1) \geq \text{ord}_{\mathfrak{p}}(N\mathcal{O}_K)$ for all prime ideals \mathfrak{p} of \mathcal{O}_K dividing $N\mathcal{O}_K$. Hence we obtain

$$[\xi'_1, \xi'_2] = \mathfrak{c}'^{-1} = \nu^{-1} \mathfrak{c}^{-1} = \nu^{-1}[\xi_1, \xi_2] = [\nu^{-1}\xi_1, \nu^{-1}\xi_2]$$

and so

$$\begin{bmatrix} \xi'_1 \\ \xi'_2 \end{bmatrix} = B \begin{bmatrix} \nu^{-1}\xi_1 \\ \nu^{-1}\xi_2 \end{bmatrix} \quad \text{for some } B = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} \in \text{GL}_2(\mathbb{Z}). \quad (6)$$

One can also show that $\det(B) > 0$ and so $B \in \text{SL}_2(\mathbb{Z})$ using the fact $\xi_1/\xi_2, \xi'_1/\xi'_2 \in \mathbb{H}$. We then see that

$$\xi' = \frac{b_1(\nu^{-1}\xi_1) + b_2(\nu^{-1}\xi_2)}{b_3(\nu^{-1}\xi_1) + b_4(\nu^{-1}\xi_2)} = \frac{b_1(\xi_1/\xi_2) + b_2}{b_3(\xi_1/\xi_2) + b_4} = B(\xi). \quad (7)$$

On the other hand, since \mathfrak{c} and $\mathfrak{c}' = \nu \mathfrak{c}$ are integral ideals of K , so is $(\nu - 1)\mathfrak{c}$. Furthermore, $(\nu - 1)\mathfrak{c} \subseteq N\mathcal{O}_K$ due to the facts that $\nu \equiv^* 1 \pmod{N\mathcal{O}_K}$ and \mathfrak{c} is relatively prime to $N\mathcal{O}_K$. Thus

$$[(\nu - 1)\tau_K, \nu - 1] = (\nu - 1)\mathcal{O}_K \subseteq N\mathfrak{c}^{-1} = [N\xi_1, N\xi_2],$$

from which we have

$$\begin{bmatrix} (\nu - 1)\tau_K \\ \nu - 1 \end{bmatrix} = A'' \begin{bmatrix} N\xi_1 \\ N\xi_2 \end{bmatrix} \quad \text{for some } A'' \in M_2(\mathbb{Z}).$$

Hence we derive that

$$\begin{aligned} NA'' \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} &= \nu \begin{bmatrix} \tau_K \\ 1 \end{bmatrix} - \begin{bmatrix} \tau_K \\ 1 \end{bmatrix} \\ &= \nu A' \begin{bmatrix} \xi'_1 \\ \xi'_2 \end{bmatrix} - A \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \quad \text{by (3) and (5)} \\ &= A'B \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} - A \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \quad \text{by (6)} \\ &= (A'B - A) \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix}, \end{aligned}$$

which implies $NA'' = A'B - A$. Since $B \in \mathrm{SL}_2(\mathbb{Z})$, we have $A' = NA''B^{-1} + AB^{-1}$ and so

$$A' \equiv AB^{-1} \pmod{N \cdot M_2(\mathbb{Z})}. \quad (8)$$

Therefore we achieve by (7) and (8) that

$$h^{\widetilde{A}'}(\xi') = h^{\widetilde{AB^{-1}}}(B(\xi)) = h^{\widetilde{A}}(B^{-1}B(\xi)) = h^{\widetilde{A}}(\xi).$$

This completes the proof. \square

For a positive integer N , we denote by

$$\sigma_N : \mathrm{Cl}(N\mathcal{O}_K) \rightarrow \mathrm{Gal}(K_{(N)}/K)$$

the Artin map for modulus $N\mathcal{O}_K$ (cf. [1]).

Theorem 3.2. *Let K be an imaginary quadratic field, $h \in \mathcal{F}_N$ and $C \in \mathrm{Cl}(N\mathcal{O}_K)$ with a positive integer N . If $h(C)$ is finite, then it belongs to $K_{(N)}$ and satisfies*

$$h(C)^{\sigma_N(D)} = h(CD) \quad \text{for all } D \in \mathrm{Cl}(N\mathcal{O}_K).$$

Proof. Since $h(C) \in K_{\mathrm{ab}}$ by Proposition 2.4, there is a positive integer M such that $N \mid M$ and $h(C) \in K_{(M)}$. By using the surjectivity of the natural map $\mathrm{Cl}(M\mathcal{O}_K) \rightarrow \mathrm{Cl}(N\mathcal{O}_K)$, we can take integral ideals $\mathfrak{c} \in C$ and $\mathfrak{d} \in D$ which are relatively prime to $M\mathcal{O}_K$. Take $\xi_1, \xi_2, \nu_1, \nu_2 \in K^\times$ such that

$$\begin{aligned} \mathfrak{c}^{-1} &= [\xi_1, \xi_2], & \xi &:= \xi_1/\xi_2 \in \mathbb{H}, \\ (\mathfrak{c}\mathfrak{d})^{-1} &= [\nu_1, \nu_2], & \nu &:= \nu_1/\nu_2 \in \mathbb{H}. \end{aligned}$$

Since $\mathcal{O}_K \subseteq \mathfrak{c}^{-1} \subseteq (\mathfrak{c}\mathfrak{d})^{-1}$, we have

$$\begin{bmatrix} \tau_K \\ 1 \end{bmatrix} = A \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} = B \begin{bmatrix} \nu_1 \\ \nu_2 \end{bmatrix} \quad (9)$$

for some $A, B \in M_2(\mathbb{Z})$ such that $\det(A), \det(B) > 0$. Let $s = (s_p)_p$ be an idele of K such that for every prime p

$$\begin{cases} s_p &= 1 & \text{if } p \mid M, \\ s_p(\mathcal{O}_K)_p &= \mathfrak{d}_p & \text{if } p \nmid M. \end{cases} \quad (10)$$

Here, $(\mathcal{O}_K)_p = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and $\mathfrak{d}_p = \mathfrak{d} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. If we let \widetilde{D} be a ray class in $\mathrm{Cl}(M\mathcal{O}_K)$ containing \mathfrak{d} , we get

$$\begin{aligned} [s, K]_{K_{(M)}} &= \sigma_M(\widetilde{D}), \\ s_p^{-1}(\mathcal{O}_K)_p &= \mathfrak{d}_p^{-1} \quad \text{for all primes } p. \end{aligned} \quad (11)$$

It follows by (9) and (11) that for every prime p , the components of each of the vectors

$$B^{-1} \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \quad \text{and} \quad q_\xi(s^{-1})_p \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix}$$

are bases for the \mathbb{Z}_p -module $(\mathfrak{c}\mathfrak{d})_p^{-1}$. Hence

$$q_\xi(s^{-1})_p = u_p B^{-1} \quad \text{for some } u_p \in \mathrm{GL}_2(\mathbb{Z}_p). \quad (12)$$

If we let $u = (u_p)_p \in U = \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$, then we have

$$q_\xi(s^{-1}) = uB^{-1}. \quad (13)$$

Thus we derive that

$$\begin{aligned} h(C)^{\sigma_M(\tilde{D})} &= h(C)^{[s,K]} \quad \text{by (11)} \\ &= (h^{\tilde{A}}(\xi))^{[s,K]} \\ &= h^{\tilde{A}}(\tau)^{\sigma_{\mathcal{F}}(q_\xi(s^{-1}))} \Big|_{\tau=\xi} \quad \text{by Proposition 2.4} \\ &= h^{\tilde{A}}(\tau)^{\sigma_{\mathcal{F}}(uB^{-1})} \Big|_{\tau=\xi} \quad \text{by (13)} \\ &= (h^{\tilde{A}})^{\sigma_{\mathcal{F}}(u)}(B^{-1}(\tau)) \Big|_{\tau=\xi} \quad \text{by Proposition 2.3} \\ &= h^{\tilde{A}\tilde{B}}(B^{-1}(\tau)) \Big|_{\tau=\xi} \quad \text{because } u_p = B \text{ for every prime } p \mid N \text{ by (10) and (12)} \\ &= h^{\widetilde{AB}}(B^{-1}(\xi)) \\ &= h^{\widetilde{AB}}(\nu) \quad \text{by (9)} \\ &= h(CD) \quad \text{since } \begin{bmatrix} \tau_K \\ 1 \end{bmatrix} = AB \begin{bmatrix} \nu_1 \\ \nu_2 \end{bmatrix} \text{ by (9).} \end{aligned}$$

In particular, if D is the identity class of $\mathrm{Cl}(N\mathcal{O}_K)$ then $\sigma_M(\tilde{D})$ leaves $h(C)$ fixed. Therefore, $h(C)$ lies in $K_{(N)}$ as desired. \square

Definition 2. For $h \in \mathcal{F}_N$ and $[Q] \in C_N(d_K)$ with $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$, we define

$$h([Q]) = h^{\tilde{B}^{-1}}(-\overline{\omega_Q}),$$

$$\text{where } B = \begin{bmatrix} 1 & (b + b_K)/2 \\ 0 & a \end{bmatrix}.$$

Let

$$\begin{aligned} \phi_N : C_N(d_K) &\rightarrow \mathrm{Cl}(N\mathcal{O}_K) \\ [Q] &\mapsto [[\omega_Q, 1]] \end{aligned}$$

be the isomorphism given in (1).

Lemma 3.3. *If $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$, then*

$$[\omega_Q, 1][\overline{\omega_Q}, 1] = a^{-1}\mathcal{O}_K.$$

Proof. See [4, Lemma 3.2]. \square

Lemma 3.4. *Let $C = \phi_N([Q])$ with $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$. If $h \in \mathcal{F}_N$ such that $h(C)$ is finite, then*

$$h(C) = h([Q]).$$

Hence $h([Q])$ is well defined.

Proof. Since $\gcd(a, N) = 1$, we have

$$a^{\varphi(N)} \equiv 1 \pmod{N},$$

where φ is Euler's phi function. Moreover, since $a\omega_Q \in \mathcal{O}_K$, we can take an integral ideal \mathfrak{c} in $C = [[\omega_Q, 1]]$ as

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

Now that

$$\begin{aligned} \mathfrak{c}\bar{\mathfrak{c}} &= a^{2\varphi(N)}[\omega_Q, 1][\overline{\omega_Q}, 1] \\ &= a^{2\varphi(N)}(a^{-1}\mathcal{O}_K) \quad \text{by Lemma 3.3} \\ &= a^{2\varphi(N)-1}\mathcal{O}_K, \end{aligned}$$

we get

$$\mathfrak{c}^{-1} = \frac{1}{a^{2\varphi(N)-1}}\bar{\mathfrak{c}} = \frac{1}{a^{\varphi(N)-1}}[-\overline{\omega_Q}, 1].$$

If we take

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

then we obtain $\mathfrak{c}^{-1} = [\xi_1, \xi_2]$ and $\xi := \xi_1/\xi_2 = -\overline{\omega_Q} \in \mathbb{H}$. Thus we find that

$$\begin{bmatrix} \tau_K \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{-b_K + \sqrt{d_K}}{2} \\ 1 \end{bmatrix} = \begin{bmatrix} a^{\varphi(N)} & -a^{\varphi(N)-1} \left(\frac{b+b_K}{2} \right) \\ 0 & a^{\varphi(N)-1} \end{bmatrix} \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix}.$$

Let $A = \begin{bmatrix} a^{\varphi(N)} & -a^{\varphi(N)-1} \left(\frac{b+b_K}{2} \right) \\ 0 & a^{\varphi(N)-1} \end{bmatrix}$ and $B = \begin{bmatrix} 1 & \frac{b+b_K}{2} \\ 0 & a \end{bmatrix}$. Then we have

$$AB \equiv \begin{bmatrix} 1 & -a^{\varphi(N)-1} \left(\frac{b+b_K}{2} \right) \\ 0 & a^{\varphi(N)-1} \end{bmatrix} \begin{bmatrix} 1 & \frac{b+b_K}{2} \\ 0 & a \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N \cdot M_2(\mathbb{Z})}.$$

Hence we have

$$h(C) = h^{\tilde{A}}(-\overline{\omega_Q}) = h^{\tilde{B}^{-1}}(-\overline{\omega_Q}) = h([Q]).$$

If $[Q] = [Q']$ with $Q, Q' \in \mathcal{Q}_N(d_K)$, then

$$h([Q]) = h(\phi_N([Q])) = h(\phi_N([Q'])) = h([Q']).$$

Therefore, $h([Q])$ is well defined. □

Theorem 3.5. *The map*

$$\begin{aligned} C_N(d_K) &\rightarrow \text{Gal}(K_{(N)}/K) \\ [Q] = [ax^2 + bxy + cy^2] &\mapsto (h(\tau_K) \mapsto h([Q]) \mid h \in \mathcal{F}_N \text{ is finite at } \tau_K) \end{aligned}$$

is an isomorphism.

Proof. Note that $\sigma_N \circ \phi_N$ is an isomorphism from $C_N(d_K)$ to $\text{Gal}(K_{(N)}/K)$. If we let C_0 be the identity class in $\text{Cl}(N\mathcal{O}_K)$, then we have $h(C_0) = h(\tau_K)$. Hence it follows from Theorem 3.2 and Lemma 3.4 that for $[Q] \in C_N(d_K)$ with $Q \in \mathcal{Q}_N(d_K)$,

$$h(\tau_K)^{(\sigma_N \circ \phi_N)([Q])} = h(C_0)^{\sigma_N(\phi_N([Q]))} = h(\phi_N([Q])) = h([Q]).$$

Therefore, the map in this theorem coincides with the isomorphism $\sigma_N \circ \phi_N$. \square

References

- [1] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class field theory, and Complex Multiplication*, 2nd edn, Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013.
- [2] 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.
- [3] G. Gras, *Class Field Theory: from Theory to Practice*, corr. 2nd ed., Springer Monographs in Mathematics, Springer, 2005.
- [4] H. Y. Jung, J. K. Koo, D. H. Shin and D. S. Yoon, *Form class groups and class fields of CM-fields*, submitted, <https://arxiv.org/abs/1912.08128>.
- [5] S. Lang, *Elliptic Functions*, With an appendix by J. Tate, 2nd edn, Grad. Texts in Math. 112, Springer-Verlag, New York, 1987.
- [6] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, Princeton, NJ, 1971.
- [7] G. Shimura, *Arithmeticity in the theory of automorphic forms*, Mathematical Surveys and Monographs, 82. Amer. Math. Soc., Providence, RI, 2000.
- [8] C. L. Siegel, *Lectures on Advanced Analytic Number Theory*, Notes by S. Raghavan, Tata Institute of Fundamental Research Lectures on Mathematics 23, Tata Institute of Fundamental Research, Bombay 1965.
- [9] H. M. Stark, *L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem*, Adv. Math. 22 (1976), no. 1, 64–84.

DONG SUNG YOON
 DEPARTMENT OF MATHEMATICS EDUCATION
 PUSAN NATIONAL UNIVERSITY
 BUSAN 46241
 REPUBLIC OF KOREA
E-mail address: dsyoon@pusan.ac.kr