East Asian Math. J.
Vol. 38 (2022), No. 5, pp. 583–591
http://dx.doi.org/10.7858/eamj.2022.034

FORM CLASS GROUPS ISOMORPHIC TO THE GALOIS GROUPS OVER RING CLASS FIELDS

Dong Sung Yoon

Abstract. Let K be an imaginary quadratic field and $\mathcal{O}$ be an order in K. Let $H_{\mathcal{O}}$ be the ring class field of $\mathcal{O}$. Furthermore, for a positive integer N, let $K_{\mathcal{O},N}$ be the ray class field modulo $N\mathcal{O}$ of $\mathcal{O}$. When the discriminant of $\mathcal{O}$ is different from -3 and -4, we construct an extended form class group which is isomorphic to the Galois group $\mathrm{Gal}(K_{\mathcal{O},N}/H_{\mathcal{O}})$ and describe its Galois action on $K_{\mathcal{O},N}$ in a concrete way.

1. Introduction

Let K be an imaginary quadratic field and $\mathcal{O}$ be an order in K of discriminant D. We say that a nonzero $\mathcal{O}$-ideal $\mathfrak{a}$ is prime to a positive integer ℓ if $\mathfrak{a}+\ell\mathcal{O}=\mathcal{O}$. It is equivalent to saying that its norm $\mathrm{N}(\mathfrak{a})=|\mathcal{O}/\mathfrak{a}|$ is relatively prime to ℓ (cf. [2, Lemma 7.18 (i)] or [4, Lemma 2.2]). Let $I(\mathcal{O})$ be the group of proper fractional $\mathcal{O}$-ideals and $P(\mathcal{O})$ be its subgroup of principal fractional $\mathcal{O}$-ideals. For positive integers ℓ and N, we define the subgroups of $I(\mathcal{O})$ and $P(\mathcal{O})$ by

$$\begin{aligned} I(\mathcal{O},\ell) &= \langle \mathfrak{a} \mid \mathfrak{a} \text{ is a nonzero proper } \mathcal{O}\text{-ideal prime to } \ell\rangle, \\ P_N(\mathcal{O},\ell) &= \langle \nu\mathcal{O} \mid \nu\in\mathcal{O}\setminus\{0\},\ \nu\mathcal{O} \text{ is prime to } \ell \text{ and } \nu\equiv 1 \pmod{N\mathcal{O}}\rangle, \end{aligned} \tag{1}$$

respectively. By the existence theorem of class field theory, there is a unique abelian extension $K_{\mathcal{O},N}$ of K such that the Artin map induces an isomorphism of $\mathcal{C}_N(\mathcal{O})=I(\mathcal{O},N)/P_N(\mathcal{O},N)$ onto $\mathrm{Gal}(K_{\mathcal{O},N}/K)$ ([2, Theorem 8.6] and [4, Propositions 2.8 and 2.13]). We call $K_{\mathcal{O},N}$ the ray class field modulo $N\mathcal{O}$ of $\mathcal{O}$ or the extended ring class field of order $\mathcal{O}$ and level N (cf. [2, §15 B] or [7, §4]). In particular, $K_{\mathcal{O},1}$ is the ring class field $H_{\mathcal{O}}$ of $\mathcal{O}$ because $I(\mathcal{O},1)=I(\mathcal{O})$ (cf. [2, Exercise 7.7]), and $K_{\mathcal{O}_K,N}$ is the ray class field $K_{(N)}$ modulo $(N)=N\mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of K.

Received May 19, 2022; Accepted June 30, 2021.
2010 *Mathematics Subject Classification.* Primary 11R37; Secondary 11E16, 11R29.
Key words and phrases. Class field theory, form class groups.
This work was supported by a 2-Year Research Grant of Pusan National University.

(pISSN 1226-6973, eISSN 2287-2833)

Let $\mathcal{Q}(D)$ be the set of primitive positive definite binary quadratic forms of discriminant D. The proper equivalence $\sim$ on $\mathcal{Q}(D)$ is given by

$$Q \sim Q' \quad \Longleftrightarrow \quad Q' = Q^\alpha = Q\left(\alpha \begin{bmatrix} x \\ y \end{bmatrix}\right) \text{ for some } \alpha \in \mathrm{SL}_2(\mathbb{Z}).$$

It is well known that the set $\mathcal{C}(D) = \mathcal{Q}(D)/\sim$ of equivalence classes with the operation induced from Dirichlet composition becomes an abelian group, called the *form class group* of discriminant D (cf. [2, Theorem 3.9]). Furthermore, $\mathcal{C}(D)$ is isomorphic to the ideal class group $\mathcal{C}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ via the map

$$\begin{array}{ccc} \mathcal{C}(D) & \to & \mathcal{C}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}) \\ [Q = ax^2 + bxy + cy^2] & \mapsto & [a[\omega_Q, 1]] \end{array} \tag{2}$$

where ω_Q is the zero of $Q(x, 1)$ in the complex upper half-plane $\mathbb{H}$ (cf. [2, Theorem 7.7]). Hence one can express $\mathrm{Gal}(H_\mathcal{O}/K)$ $(\cong \mathcal{C}(\mathcal{O}))$ in terms of the form class group $\mathcal{C}(D)$. Recently, Eum et al. established an extended form class group isomorphic to the ray class group $\mathcal{C}_N(\mathcal{O}_K)$ $(\cong \mathrm{Gal}(K_{(N)}/K))$ and explicitly described its Galois action on the ray class field $K_{(N)}$ over K ([3, Theorems 2.9 and 3.10]).

In this paper, we shall construct an extended form class group $\mathcal{C}_{0,N}(D)$ which is isomorphic to the subgroup $P_1(\mathcal{O}, N)/P_N(\mathcal{O}, N)$ of $\mathcal{C}_N(\mathcal{O})$ corresponding to $\mathrm{Gal}(K_{\mathcal{O},N}/H_\mathcal{O})$ (Theorem 2.6). Furthermore, we shall give an isomorphism of $\mathcal{C}_{0,N}(D)$ onto $\mathrm{Gal}(K_{\mathcal{O},N}/H_\mathcal{O})$ in a concrete way (Theorem 3.4).

2. The set $\mathcal{C}_{0,\,N}(D)$ of equivalence classes of quadratic forms

Throughout this paper, we let K be an imaginary quadratic field and $\mathcal{O}$ be an order in K. Let M and D be the conductor and the discriminant of $\mathcal{O}$, respectively. Let $\mathcal{Q}(D)$ be the set of primitive positive definite binary quadratic forms of discriminant D, namely,

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

For each $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}(D)$, let ω_Q be the zero of the quadratic polynomial $Q(x,\, 1)$ lying in the complex upper half-plane $\mathbb{H}$, that is,

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

Then one can readily show that for $Q \in \mathcal{Q}(D)$ and $\alpha = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$

$$\omega_{Q^\alpha} = \alpha^{-1}(\omega_Q) \tag{3}$$

and

$$[\alpha(\omega_Q), 1] = \frac{1}{j(\alpha, \omega_Q)}[\omega_Q, 1], \text{ where } j(\alpha, \omega_Q) = u\omega_Q + v. \tag{4}$$

Here, $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ as fractional linear transformations. Let Q_0 be the principal form of discriminant D given by

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

Let $\omega_{\mathcal{O}} = \omega_{Q_0}$ and $\min(\omega_{\mathcal{O}}, \mathbb{Q}) = x^2 + b_{\mathcal{O}}x + c_{\mathcal{O}}$. Then we have $\mathcal{O} = [\omega_{\mathcal{O}}, 1]$ and $b_{\mathcal{O}}, c_{\mathcal{O}} \in \mathbb{Z}$ ([2, Lemma 7.2]).

Let N be a positive integer and denote by

$$\begin{aligned} \mathcal{Q}_N(D) &= \left\{ax^2 + bxy + cy^2 \in \mathcal{Q}(D) \mid \gcd(a,\, N) = 1\right\}, \\ \mathcal{Q}_{0,N}(D) &= \{Q_0^\alpha \mid \alpha \in \mathrm{SL}_2(\mathbb{Z}) \text{ satisfies } Q_0^\alpha \in \mathcal{Q}_N(D)\}. \end{aligned}$$

Then the congruence subgroup

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

induces an equivalence relation $\sim_N$ on $\mathcal{Q}_{0,N}(D)$ as

$$Q \sim_N Q' \quad \Longleftrightarrow \quad Q' = Q^\alpha = Q\left(\alpha \begin{bmatrix} x \\ y \end{bmatrix}\right) \text{ for some } \alpha \in \Gamma_1(N)$$

([3, Proposition 2.1 and Definition 2.2]). We denote the set of equivalence classes by $\mathcal{C}_{0,N}(D)$, that is,

$$\mathcal{C}_{0,N}(D) = \mathcal{Q}_{0,N}(D)/\sim_N = \{[Q] \mid Q \in \mathcal{Q}_{0,N}(D)\}.$$

For a positive integer ℓ, let $I(\mathcal{O}, \ell)$ and $P_N(\mathcal{O}, \ell)$ be the groups defined in (1).

Lemma 2.1. *If $\nu \in K^\times$ satisfies $\nu - 1 \in N\mathfrak{a}^{-1}$ for a proper $\mathcal{O}$-ideal $\mathfrak{a}$ prime to N, then $\nu\mathcal{O}$ belongs to $P_N(\mathcal{O}, N)$.*

Proof. Let $\nu = 1 + Na$ with $a \in \mathfrak{a}^{-1}$. Since $\mathfrak{a}$ is prime to N, that is, $\mathfrak{a} + N\mathcal{O} = \mathcal{O}$, we can select $b \in \mathcal{O}$ such that

$$\begin{aligned} b &\equiv 1 \pmod{N\mathcal{O}}, \\ b &\equiv 0 \pmod{\mathfrak{a}} \end{aligned}$$

by the Chinese remainder theorem ([5, Chapter II, Theorem 2.1]). Then we have

$$b\nu \equiv b + N(ab) \equiv 1 \pmod{N\mathcal{O}}.$$

Therefore, $\nu\mathcal{O} = (b\nu\mathcal{O})(b\mathcal{O})^{-1} \in P_N(\mathcal{O}, N)$. □

Lemma 2.2. *For $\nu \in \mathcal{O} \setminus \{0\}$, we have*

$$\mathrm{N}(\nu\mathcal{O}) = \mathrm{N}_{K/\mathbb{Q}}(\nu).$$

Proof. See [2, Lemma 7.14]. □

Lemma 2.3. *If* $Q_0^\alpha \in \mathcal{Q}_{0,N}(D)$ *for some* $\alpha = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$*, then we have*

$$[\omega_{Q_0^\alpha}, 1]^{-1} \in P_1(\mathcal{O}, N).$$

Proof. Observe that

$$\begin{array}{rcll} [\omega_{Q_0^\alpha}, 1]^{-1} & = & [\alpha^{-1}(\omega_{\mathcal{O}}), 1]^{-1} & \text{by (3)} \\ & = & j(\alpha^{-1}, \omega_{\mathcal{O}})\mathcal{O} & \text{by (4) and the fact } [\omega_{\mathcal{O}}, 1] = \mathcal{O} \\ & = & (-u\omega_{\mathcal{O}} + r)\mathcal{O} & \end{array} \tag{5}$$

which is a principal $\mathcal{O}$-ideal. Note that the coefficient of x^2 in Q_0^α is $Q_0(r, u)$ which is relatively prime to N by assumption. Since

$$\mathrm{N}_{K/\mathbb{Q}}(-u\omega_{\mathcal{O}} + r) = (-u\omega_{\mathcal{O}} + r)(-u\overline{\omega_{\mathcal{O}}} + r) = r^2 + b_{\mathcal{O}}ru + c_{\mathcal{O}}u^2 = Q_0(r, u),$$

we obtain $[\omega_{Q_0^\alpha}, 1]^{-1} \in P_1(\mathcal{O}, N)$ by Lemma 2.2.

□

From now on, we assume $D \neq -3, -4$ so that $\mathcal{O}^\times = \{1, -1\}$ (cf. [2, p. 105]).

Definition 1. We define a map

$$\begin{array}{rccc} \phi_{0,\mathcal{O},N} : & \mathcal{C}_{0,N}(D) & \to & P_1(\mathcal{O}, N)/P_N(\mathcal{O}, N) \\ & [Q] & \mapsto & [[\omega_Q, 1]^{-1}] \end{array}$$

for $Q \in \mathcal{Q}_{0,N}(D)$.

Proposition 2.4. *The map* $\phi_{0,\mathcal{O},N}$ *is well defined.*

Proof. Let $Q \in \mathcal{Q}_{0,N}(D)$. By Lemma 2.3, we have $[\omega_Q, 1]^{-1} \in P_1(\mathcal{O}, N)$. If $Q' = a'x^2 + b'xy + c'y^2 \in \mathcal{Q}_{0,N}(D)$ satisfies $[Q] = [Q']$, then $Q' = Q^\alpha$ for some $\alpha = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \in \Gamma_1(N)$. Thus we derive by (3) and (4) that

$$[\omega_Q, 1]^{-1} = [\alpha(\omega_{Q'}), 1]^{-1} = j(\alpha, \omega_{Q'})[\omega_{Q'}, 1]^{-1} = (u\omega_{Q'} + v)[\omega_{Q'}, 1]^{-1}.$$

If we write $u = Nu'$ and $v = 1 + Nv'$ for some $u', v' \in \mathbb{Z}$, then we see that

$$(u\omega_{Q'} + v) - 1 = Na'^{-1}(u'(a'\omega_{Q'}) + a'v') \in Na'^{-1}\mathcal{O}$$

because $\mathcal{O} = [a'\omega_{Q'}, 1]$ ([2, p. 124]). Moreover, since $\gcd(a', N) = 1$, we get by Lemma 2.1 that

$$(u\omega_{Q'} + v)\mathcal{O} \in P_N(\mathcal{O}, N).$$

Hence $[[\omega_Q, 1]^{-1}] = [[\omega_{Q'}, 1]^{-1}]$ in $P_1(\mathcal{O}, N)/P_N(\mathcal{O}, N)$, which proves that $\phi_{0,\mathcal{O},N}$ is well defined.

□

Proposition 2.5. *The map* $\phi_{0,\mathcal{O},N}$ *is bijective.*

Proof. Suppose that $\phi_{0,\mathcal{O},N}([Q]) = \phi_{0,\mathcal{O},N}([Q'])$ for some $Q, Q' \in \mathcal{Q}_{0,N}(D)$ and so $[[\omega_Q, 1]^{-1}] = [[\omega_{Q'}, 1]^{-1}]$. Then

$$[\omega_{Q'}, 1]^{-1} = \frac{\beta}{\gamma}[\omega_Q, 1]^{-1} \tag{6}$$

for some $\beta, \gamma \in \mathcal{O} \setminus \{0\}$ satisfying $\beta \equiv \gamma \equiv 1 \pmod{N\mathcal{O}}$. Since the map given in (2) is an isomorphism, we have $Q' = Q^\alpha$ for some $\alpha = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. It then follows from (3), (4), (6) that

$$[\omega_Q, 1]^{-1} = (u\omega_{Q'} + v)[\omega_{Q'}, 1]^{-1} = \frac{\beta}{\gamma}(u\omega_{Q'} + v)[\omega_Q, 1]^{-1}.$$

Thus $\frac{\beta}{\gamma}(u\omega_{Q'} + v) \in \mathcal{O}^\times = \{1, -1\}$. If we write $Q'(x, y) = a'x^2 + b'xy + c'y^2$, then we find that

$$\begin{aligned} u(a'\omega_{Q'}) + a'v &\equiv \beta\{u(a'\omega_{Q'}) + a'v\} \pmod{N\mathcal{O}} \quad \text{because } \beta \equiv 1 \pmod{N\mathcal{O}} \\ &\equiv a'\beta(u\omega_{Q'} + v) \pmod{N\mathcal{O}} \\ &\equiv \pm a'\gamma \pmod{N\mathcal{O}} \\ &\equiv \pm a' \pmod{N\mathcal{O}} \quad \text{because } \gamma \equiv 1 \pmod{N\mathcal{O}}. \end{aligned}$$

Since $\mathcal{O} = [a'\omega_{Q'}, 1]$ and $\gcd(a', N) = 1$, we obtain

$$u \equiv 0 \pmod{N}, \quad v \equiv \pm 1 \pmod{N}$$

and hence

$$\alpha \equiv \pm \begin{bmatrix} 1 & \pm s \\ 0 & 1 \end{bmatrix} \pmod{N}$$

because $\det(\alpha) = 1$. We may assume $\alpha \in \Gamma_1(N)$ since $Q^\alpha = Q^{-\alpha}$. Thus we have $[Q] = [Q']$ in $\mathcal{C}_{0,N}(D)$, which implies that $\phi_{0,\mathcal{O},N}$ is injective.

Now, let C be a class in $P_1(\mathcal{O}, N)/P_N(\mathcal{O}, N)$. Note that one can take an $\mathcal{O}$-ideal $\nu\mathcal{O}$ in C with $\nu \in \mathcal{O}$. Indeed, if $C = \left[\frac{\nu_1}{\nu_2}\mathcal{O}\right]$ for some $\nu_1, \nu_2 \in \mathcal{O} \setminus \{0\}$ such that both $\nu_1\mathcal{O}$ and $\nu_2\mathcal{O}$ are prime to N, then we can choose $a \in \mathcal{O}$ satisfying

$$\begin{aligned} a &\equiv 1 \pmod{N\mathcal{O}}, \\ a &\equiv 0 \pmod{\nu_2\mathcal{O}} \end{aligned}$$

by the Chinese remainder theorem. If we let $\nu = \left(\frac{a}{\nu_2}\right)\nu_1 \in \mathcal{O}$, then we see that

$$C = [a\mathcal{O}]\left[\frac{\nu_1}{\nu_2}\mathcal{O}\right] = [\nu\mathcal{O}]$$

because $[a\mathcal{O}] \in P_N(\mathcal{O}, N)$. Since $\mathcal{O} = [\omega_\mathcal{O}, 1]$, we get $\nu = -u\omega_\mathcal{O} + r$ for some $r, u \in \mathbb{Z}$. Observe that $\gcd(r, u, N) = 1$ because $\nu\mathcal{O}$ is prime to N. Thus we may take a matrix $\alpha = \begin{bmatrix} r' & s' \\ u' & v' \end{bmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$ such that

$$r' \equiv r \pmod{N}, \quad u' \equiv u \pmod{N}$$

by the surjectivity of the reduction $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ (cf. [6, Chapter 6 §1]). Then we deduce by (5) that

$$[\omega_{Q_0^\alpha}, 1]^{-1} = (-u'\omega_{\mathcal{O}} + r')\mathcal{O} = \nu^{-1}(-u'\omega_{\mathcal{O}} + r')(\nu\mathcal{O}).$$

Since $1 = \nu^{-1}(-u\omega_{\mathcal{O}} + r)$, we see that

$$\nu^{-1}(-u'\omega_{\mathcal{O}} + r') - 1 = \nu^{-1}((u - u')\omega_{\mathcal{O}} + r' - r) \in \nu^{-1}N\mathcal{O}.$$

Hence $\nu^{-1}(-u'\omega_{\mathcal{O}} + r')\mathcal{O} \in P_N(\mathcal{O}, N)$ by Lemma 2.1 and so

$$\phi_{0,\mathcal{O},N}([Q_0^\alpha]) = [\nu\mathcal{O}] = C.$$

This proves that $\phi_{0,\mathcal{O},N}$ is surjective.

$\square$

We define a binary operation $\cdot$ on $\mathcal{C}_{0,N}(D)$ by

$$[Q] \cdot [Q'] = \phi_{0,\mathcal{O},N}^{-1}\left(\phi_{0,\mathcal{O},N}([Q])\phi_{0,\mathcal{O},N}([Q'])\right) \quad ([Q], [Q'] \in \mathcal{C}_{0,N}(D)). \tag{7}$$

We then achieve the following theorem.

Theorem 2.6. *Assume that $D \neq -3, -4$. The set $\mathcal{C}_{0,N}(D)$ with the binary operation $\cdot$ in (7) is an abelian group isomorphic to the ideal class group $P_1(\mathcal{O}, N)/P_N(\mathcal{O}, N)$.*

3. An isomorphism of $\mathcal{C}_{0,N}(D)$ with $\mathrm{Gal}(K_{\mathcal{O},N}/H_{\mathcal{O}})$

In this section, we shall establish an isomorphism of $\mathcal{C}_{0,N}(D)$ onto $\mathrm{Gal}(K_{\mathcal{O},N}/H_{\mathcal{O}})$ in a concrete way.

For a positive integer N, let $\mathcal{F}_N$ be the field of meromorphic modular functions of level N with Fourier coefficients in the cyclotomic field $\mathbb{Q}(\zeta_N)$, where $\zeta_N = e^{2\pi \mathrm{i}/N}$ (cf. [6, Chapter 6 §3]). It is well known that $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1$ and

$$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle = G_N \cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2 \rangle$$

where

$$G_N = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \mid d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\} / \langle -I_2 \rangle.$$

More precisely, the element $\left[\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}\right] \in G_N$ acts on $\mathcal{F}_N$ by

$$\sum_{n \gg -\infty} c_n q_\tau^{n/N} \longmapsto \sum_{n \gg -\infty} c_n^{\sigma_d} q_\tau^{n/N}$$

where $\sum_{n\gg-\infty} c_n q_\tau^{n/N}$ $(q_\tau = e^{2\pi \mathrm{i}\tau})$ is the Fourier expansion of a function in $\mathcal{F}_N$ and σ_d is the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ defined by $\zeta_N^{\sigma_d} = \zeta_N^d$. And, $\widetilde{\gamma} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2\rangle$ acts on $\mathcal{F}_N$ by

$$h^{\widetilde{\gamma}} = h \circ \gamma \quad (h \in \mathcal{F}_N)$$

where γ is a preimage of $\widetilde{\gamma}$ of $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2\rangle$ (cf. [6, Chapter 6, Theorem 3]).

Proposition 3.1. *We have*

$$K_{\mathcal{O},N} = K(h(\omega_\mathcal{O}) \mid h \in \mathcal{F}_N \text{ is finite at } \omega_\mathcal{O}).$$

Proof. See [1, Theorem 4]. □

For a positive integer N, let

$$W_{\mathcal{O},\,N} = \left\{\gamma = \begin{bmatrix} t - b_\mathcal{O} s & -c_\mathcal{O} s \\ s & t\end{bmatrix} \mid s,\, t \in \mathbb{Z}/N\mathbb{Z} \text{ such that } \gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})\right\},$$

which is the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ associated with the $(\mathbb{Z}/N\mathbb{Z})$-algebra $\mathcal{O}/N\mathcal{O}$ with the ordered basis $\{\omega_\mathcal{O} + N\mathcal{O},\, 1 + N\mathcal{O}\}$.

Proposition 3.2 (Shimura's reciprocity law)**.** *Assume that $D \neq -3, -4$. Then the map*

$$\begin{array}{rccl} \mu_{0,\mathcal{O},N}: & W_{\mathcal{O},\,N}/\langle -I_2\rangle & \to & \mathrm{Gal}(K_{\mathcal{O},N}/H_\mathcal{O}) \\ & [\gamma] & \mapsto & \big(h(\omega_\mathcal{O}) \mapsto h^{\widetilde{\gamma}}(\omega_\mathcal{O}) \mid h \in \mathcal{F}_N \text{ is finite at } \omega_\mathcal{O}\big) \end{array}$$

is an isomorphism, where $\widetilde{\gamma}$ is the image of γ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\langle -I_2\rangle (\cong \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1))$.

Proof. See [1, p. 859] or [2, Theorem 15.17]. □

Proposition 3.3. *Assume that $D \neq -3, -4$. The map*

$$\begin{array}{rccc} \psi_{0,\mathcal{O},N}: & W_{\mathcal{O},\,N}/\langle -I_2\rangle & \to & P_1(\mathcal{O},N)/P_N(\mathcal{O},N) \\ & \left[\begin{bmatrix} t - b_\mathcal{O} s & -c_\mathcal{O} s \\ s & t\end{bmatrix}\right] & \mapsto & [(s\omega_\mathcal{O} + t)\mathcal{O}] \end{array}$$

is an isomorphism.

Proof. Let $\alpha = \begin{bmatrix} t - b_\mathcal{O} s & -c_\mathcal{O} s \\ s & t\end{bmatrix} \in W_{\mathcal{O},\,N}$. Since

$$\mathrm{N}_{K/\mathbb{Q}}(s\omega_\mathcal{O} + t) = (s\omega_\mathcal{O} + t)(s\overline{\omega_\mathcal{O}} + t) = c_\mathcal{O} s^2 - b_\mathcal{O} st + t^2 = \det(\alpha) \quad (8)$$

is relatively prime to N, $(s\omega_\mathcal{O} + t)\mathcal{O}$ belongs to $P_1(\mathcal{O}, N)$ by Lemma 2.2. Hence $\psi_{0,\mathcal{O},N}$ is well defined.

Furthermore, if $\beta = \begin{bmatrix} t' - b_\mathcal{O} s' & -c_\mathcal{O} s' \\ s' & t'\end{bmatrix} \in W_{\mathcal{O},\,N}$, then we find that

$$\alpha\beta = \begin{bmatrix} (-c_\mathcal{O} ss' + tt') - b_\mathcal{O}(-b_\mathcal{O} ss' + st' + s't) & -c_\mathcal{O}(-b_\mathcal{O} ss' + st' + s't) \\ -b_\mathcal{O} ss' + st' + s't & -c_\mathcal{O} ss' + tt' \end{bmatrix}.$$

Thus we derive that

$$\begin{aligned}\psi_{0,\mathcal{O},N}([\alpha][\beta]) &= [((-b_{\mathcal{O}}ss'+st'+s't)\omega_{\mathcal{O}}-c_{\mathcal{O}}ss'+tt')\mathcal{O}]\\ &= [(s\omega_{\mathcal{O}}+t)(s'\omega_{\mathcal{O}}+t')\mathcal{O}] \quad \text{because } \omega_{\mathcal{O}}^2=-b_{\mathcal{O}}\omega_{\mathcal{O}}-c_{\mathcal{O}}\\ &= \psi_{0,\mathcal{O},N}([\alpha])\psi_{0,\mathcal{O},N}([\beta])\end{aligned}$$

which shows that $\psi_{0,\mathcal{O},N}$ is a homomorphism.

If $[\alpha]\in\ker(\psi_{0,\mathcal{O},N})$, then $\psi_{0,\mathcal{O},N}([\alpha])=(s\omega_{\mathcal{O}}+t)\mathcal{O}\in P_N(\mathcal{O},N)$ and so $(s\omega_{\mathcal{O}}+t)\mathcal{O}=\dfrac{\nu_1}{\nu_2}\mathcal{O}$ for some $\nu_1,\nu_2\in\mathcal{O}\setminus\{0\}$ satisfying $\nu_1\equiv\nu_2\equiv 1\ (\mathrm{mod}\ N\mathcal{O})$. Since $\mathcal{O}^\times=\{1,-1\}$, we have $\nu_2(s\omega_{\mathcal{O}}+t)=\pm\nu_1$. Hence we obtain that

$$s\omega_{\mathcal{O}}+t\equiv\nu_2(s\omega_{\mathcal{O}}+t)\equiv\pm\nu_1\equiv\pm1\ (\mathrm{mod}\ N\mathcal{O}),$$

which follows from the fact that $\mathcal{O}=[\omega_{\mathcal{O}},1]$, $s\equiv 0\ (\mathrm{mod}\ N)$ and $t\equiv\pm1\ (\mathrm{mod}\ N)$. Thus $[\alpha]=[I_2]$, which yields that $\psi_{0,\mathcal{O},N}$ is injective.

Let C be a class in $P_1(\mathcal{O},N)/P_N(\mathcal{O},N)$. Take an $\mathcal{O}$-ideal $\nu\mathcal{O}$ in C with $\nu\in\mathcal{O}$. If we write $\nu=s''\omega_{\mathcal{O}}+t''$ with $s'',t''\in\mathbb{Z}$, then $\gamma=\begin{bmatrix}t''-b_{\mathcal{O}}s'' & -c_{\mathcal{O}}s''\\ s'' & t''\end{bmatrix}\in W_{\mathcal{O},N}$ by (8) and

$$\psi_{0,\mathcal{O},N}([\gamma])=[(s''\omega_{\mathcal{O}}+t'')\mathcal{O}]=C.$$

Therefore, $\psi_{0,\mathcal{O},N}$ is surjective. □

Theorem 3.4. *Assume that $D\neq-3,-4$. Then the map*

$$\begin{aligned}\mathcal{C}_{0,N}(D) &\to \mathrm{Gal}(K_{\mathcal{O},N}/H_{\mathcal{O}})\\ \left[Q_0^{\left[\begin{smallmatrix}r&s\\u&v\end{smallmatrix}\right]}\right] &\mapsto \left(h(\omega_{\mathcal{O}})\mapsto h^{\left[\begin{smallmatrix}r+b_{\mathcal{O}}u & c_{\mathcal{O}}u\\ -u & r\end{smallmatrix}\right]}(\omega_{\mathcal{O}})\ \mid\ h\in\mathcal{F}_N \text{ is finite at } \omega_{\mathcal{O}}\right)\end{aligned}$$

is an isomorphism.

Proof. Note that the map $\Phi=\mu_{0,\mathcal{O},N}\circ\psi_{0,\mathcal{O},N}^{-1}\circ\phi_{0,\mathcal{O},N}$ is an isomorphism from $\mathcal{C}_{0,N}(D)$ onto $\mathrm{Gal}(K_{\mathcal{O},N}/H_{\mathcal{O}})$ by Theorem 2.6, Propositions 3.2 and 3.3. Let $Q_0^\alpha\in\mathcal{Q}_{0,N}(D)$ with $\alpha=\begin{bmatrix}r&s\\u&v\end{bmatrix}\in\mathrm{SL}_2(\mathbb{Z})$. Then we achieve by (5) that

$$\psi_{0,\mathcal{O},N}^{-1}\circ\phi_{0,\mathcal{O},N}([Q_0^\alpha])=\psi_{0,\mathcal{O},N}^{-1}([[\omega_Q,1]^{-1}])=\psi_{0,\mathcal{O},N}^{-1}([(-u\omega_{\mathcal{O}}+r)\mathcal{O}])=\left[\begin{bmatrix}r+b_{\mathcal{O}}u & c_{\mathcal{O}}u\\ -u & r\end{bmatrix}\right].$$

Therefore, we conclude that for $h\in\mathcal{F}_N$ which is finite at $\omega_{\mathcal{O}}$

$$h(\omega_{\mathcal{O}})^{\Phi([Q_0^\alpha])}=h(\omega_{\mathcal{O}})^{\mu_{0,\mathcal{O},N}\left(\left[\left[\begin{smallmatrix}r+b_{\mathcal{O}}u & c_{\mathcal{O}}u\\ -u & r\end{smallmatrix}\right]\right]\right)}=h^{\left[\begin{smallmatrix}r+b_{\mathcal{O}}u & c_{\mathcal{O}}u\\ -u & r\end{smallmatrix}\right]}(\omega_{\mathcal{O}})$$

as desired. □

References

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

[2] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class field theory, and Complex Multiplication*, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013.

[3] 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.

[4] H. Y. Jung, J. K. Koo, D. H. Shin and D. S. Yoon, *Arithmetic of orders in imaginary quadratic fields*, https://arxiv.org/abs/2205.10754.

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

[6] S. Lang, *Elliptic Functions*, With an appendix by J. Tate, 2nd ed., Grad. Texts in Math. **112**, Spinger-Verlag, New York, 1987.

[7] 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.

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