Research Article

Ho Yun Jung*, Ja Kyung Koo, and Dong Hwa Shin

On some extensions of Gauss' work and applications

https://doi.org/10.1515/math-2020-0126
received August 8, 2020; accepted November 24, 2020

Abstract: Let K be an imaginary quadratic field of discriminant d_K with ring of integers $\mathcal{O}_K$, and let τ_K be an element of the complex upper half plane so that $\mathcal{O}_K = [\tau_K, 1]$. 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 with leading coefficients relatively prime to N. Then, with any congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ one can define an equivalence relation $\sim_\Gamma$ on $\mathcal{Q}_N(d_K)$. Let $\mathcal{F}_{\Gamma,\mathbb{Q}}$ denote the field of meromorphic modular functions for Γ with rational Fourier coefficients. We show that the set of equivalence classes $\mathcal{Q}_N(d_K)/\sim_\Gamma$ can be equipped with a group structure isomorphic to $\mathrm{Gal}(K\mathcal{F}_{\Gamma,\mathbb{Q}}(\tau_K)/K)$ for some Γ, which generalizes the classical theory of form class groups.

Keywords: binary quadratic forms, class field theory, complex multiplication, modular functions

MSC 2020: 11E16, 11F03, 11G15, 11R37

1 Introduction

For a negative integer D such that $D \equiv 0$ or $1 \pmod 4$, let $\mathcal{Q}(D)$ be the set of primitive positive definite binary quadratic forms $Q(x, y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$ of discriminant $b^2 - 4ac = D$. The modular group $\mathrm{SL}_2(\mathbb{Z})$ (or $\mathrm{PSL}_2(\mathbb{Z})$) acts on the set $\mathcal{Q}(D)$ from the right and defines the proper equivalence $\sim$ as

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

In his celebrated work *Disquisitiones Arithmeticae* of 1801 [1], Gauss introduced the beautiful law of composition of integral binary quadratic forms. It seems that he first understood the set of equivalence classes $\mathrm{C}(D) = \mathcal{Q}(D)/\sim$ as a group, so called the *form class group*. However, his original proof of the group structure is long and complicated to work in practice. Several decades later, Dirichlet [2] presented a different approach to the study of composition and genus theory, which seemed to be definitely influenced by Legendre (see [3, Section 3]). On the other hand, in 2004 Bhargava [4] derived a wonderful general law of composition on $2 \times 2 \times 2$ cubes of integers, from which he was able to obtain Gauss' composition law on binary quadratic forms as a simple special case. Now, in this paper we will make use of Dirichlet's composition law to proceed the arguments.

Given the order $\mathcal{O}$ of discriminant D in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$, let $I(\mathcal{O})$ be the group of proper fractional $\mathcal{O}$-ideals and $P(\mathcal{O})$ be its subgroup of nonzero principal $\mathcal{O}$-ideals. When $Q = ax^2 + bxy + cy^2$ is an element of $\mathcal{Q}(D)$, let ω_Q be the zero of the quadratic polynomial $Q(x,1)$ in $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$, namely,

*** Corresponding author: Ho Yun Jung,** Department of Mathematics, Dankook University, Cheonan-si, Chungnam 31116, Republic of Korea, e-mail: hoyunjung@dankook.ac.kr
Ja Kyung Koo: Department of Mathematical Sciences, KAIST, Daejeon 34141, Republic of Korea, e-mail: jkgoo@kaist.ac.kr
Dong Hwa Shin: Department of Mathematics, Hankuk University of Foreign Studies, Yongin-si, Gyeonggi-do 17035, Republic of Korea, e-mail: dhshin@hufs.ac.kr

$$\omega_Q = \frac{-b+\sqrt{D}}{2a}. \tag{1}$$

It is well known that $[\omega_Q, 1] = \mathbb{Z}\omega_Q + \mathbb{Z}$ is a proper fractional $\mathcal{O}$-ideal and the form class group $\mathrm{C}(D)$ under the Dirichlet composition is isomorphic to the $\mathcal{O}$-ideal class group $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ through the isomorphism

$$C(D) \xrightarrow{\sim} C(\mathcal{O}), \quad [Q] \mapsto [[\omega_Q, 1]]. \tag{2}$$

On the other hand, if we let $H_\mathcal{O}$ be the ring class field of order $\mathcal{O}$ and j be the elliptic modular function on lattices in $\mathbb{C}$, then we attain the isomorphism

$$C(\mathcal{O}) \xrightarrow{\sim} \mathrm{Gal}(H_\mathcal{O}/K), \quad [\mathfrak{a}] \mapsto (j(\mathcal{O}) \mapsto j(\bar{\mathfrak{a}})) \tag{3}$$

by the theory of complex multiplication ([3, Theorem 11.1 and Corollary 11.37] or [5, Theorem 5 in Chapter 10]). Thus, composing two isomorphisms given in (2) and (3) yields the isomorphism

$$C(D) \xrightarrow{\sim} \mathrm{Gal}(H_\mathcal{O}/K), \quad [Q] \mapsto (j(\mathcal{O}) \mapsto j([-\bar{\omega}_Q, 1])). \tag{4}$$

Now, let K be an imaginary quadratic field of discriminant d_K and $\mathcal{O}_K$ be its ring of integers. If we set

$$\tau_K = \begin{cases} \sqrt{d_K}/2 & \text{if } d_K \equiv 0 \pmod 4, \\ (-1+\sqrt{d_K})/2 & \text{if } d_K \equiv 1 \pmod 4, \end{cases} \tag{5}$$

then we get $\mathcal{O}_K = [\tau_K, 1]$. For a positive integer N and $\mathfrak{n} = N\mathcal{O}_K$, let $I_K(\mathfrak{n})$ be the group of fractional ideals of K relatively prime to $\mathfrak{n}$ and $P_K(\mathfrak{n})$ be its subgroup of principal fractional ideals. Furthermore, let

$$P_{K,\mathbb{Z}}(\mathfrak{n}) = \{\nu\mathcal{O}_K \mid \nu \in K^* \text{ such that } \nu \equiv^* m \pmod{\mathfrak{n}} \text{ for some integer } m \text{ prime to } N\},$$
$$P_{K,1}(\mathfrak{n}) = \{\nu\mathcal{O}_K \mid \nu \in K^* \text{ such that } \nu \equiv^* 1 \pmod{\mathfrak{n}}\},$$

which are subgroups of $P_K(\mathfrak{n})$. As for the multiplicative congruence $\equiv^*$ modulo $\mathfrak{n}$, we refer to [6, Section IV.1]. Then the ring class field $H_\mathcal{O}$ of order $\mathcal{O}$ with conductor N in K and the ray class field $K_\mathfrak{n}$ modulo $\mathfrak{n}$ are defined to be the unique abelian extensions of K for which the Artin map modulo $\mathfrak{n}$ induces the isomorphisms

$$I_K(\mathfrak{n})/P_{K,\mathbb{Z}}(\mathfrak{n}) \simeq \mathrm{Gal}(H_\mathcal{O}/K) \quad \text{and} \quad I_K(\mathfrak{n})/P_{K,1}(\mathfrak{n}) \simeq \mathrm{Gal}(K_\mathfrak{n}/K),$$

respectively ([3, Sections 8 and 9] and [6, Chapter V]). And, for a congruence subgroup Γ of level N in $\mathrm{SL}_2(\mathbb{Z})$, let $\mathcal{F}_{\Gamma,\mathbb{Q}}$ be the field of meromorphic modular functions for Γ whose Fourier expansions with respect to $q^{1/N} = e^{2\pi i\tau/N}$ have rational coefficients and let

$$K\mathcal{F}_{\Gamma,\mathbb{Q}}(\tau_K) = K(h(\tau_K) \mid h \in \mathcal{F}_{\Gamma,\mathbb{Q}} \text{ is finite at } \tau_K).$$

Then it is a subfield of the maximal abelian extension K^{ab} of K ([7, Theorem 6.31(i)]). In particular, for the congruence subgroups

$$\Gamma_0(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{NM_2(\mathbb{Z})}\right\},$$
$$\Gamma_1(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{NM_2(\mathbb{Z})}\right\},$$

we know that

$$H_\mathcal{O} = K\mathcal{F}_{\Gamma_0(N),\mathbb{Q}}(\tau_K) \quad \text{and} \quad K_\mathfrak{n} = K\mathcal{F}_{\Gamma_1(N),\mathbb{Q}}(\tau_K) \tag{6}$$

([8, Corollary 5.2] and [9, Theorem 3.4]). On the other hand, one can naturally define an equivalence relation $\sim_\Gamma$ on the subset

$$\mathcal{Q}_N(d_K) = \{ax^2 + bxy + cy^2 \in \mathcal{Q}(d_K) \mid \gcd(N, a) = 1\} \tag{7}$$

of $\mathcal{Q}(d_K)$ by

$$Q \sim_\Gamma Q' \iff Q' = Q^\gamma \text{ for some } \gamma \in \Gamma. \tag{8}$$

Observe that Γ may not act on $\mathcal{Q}_N(d_K)$. Here, by Q^γ we mean the action of γ is an element of $\mathrm{SL}_2(\mathbb{Z})$.

For a subgroup P of $I_K(\mathfrak{n})$ with $P_{K,1}(\mathfrak{n}) \subseteq P \subseteq P_K(\mathfrak{n})$, let K_P be the abelian extension of K so that $I_K(\mathfrak{n})/P \simeq \mathrm{Gal}(K_P/K)$. In this paper, motivated by (4) and (6) we shall present several pairs of P and Γ for which

(i) $K_P = K\mathcal{F}_{\Gamma,\mathbb{Q}}(\tau_K)$,

(ii) $\mathcal{Q}_N(d_K)/\sim_\Gamma$ becomes a group isomorphic to $\mathrm{Gal}(K_P/K)$ via the isomorphism

$$\begin{aligned} \mathcal{Q}_N(d_K)/\sim_\Gamma &\xrightarrow{\sim} \mathrm{Gal}(K_P/K) \\ [Q] &\mapsto (h(\tau_K) \mapsto h(-\bar{\omega}_Q) \mid h \in \mathcal{F}_{\Gamma,\mathbb{Q}} \text{ is finite at } \tau_K) \end{aligned} \tag{9}$$

(Propositions 4.2, 5.3 and Theorems 2.5, 5.4). This result would be a certain extension of Gauss' original work. We shall also develop an algorithm of finding distinct form classes in $\mathcal{Q}_N(d_K)/\sim_\Gamma$ and give a concrete example (Proposition 6.2 and Example 6.3). To this end, we shall apply Shimura's theory which links the class field theory for imaginary quadratic fields and the theory of modular functions ([7, Chapter 6]). And, we shall not only use but also improve the ideas of our previous work [10]. See Remark 5.5.

2 Extended form class groups as ideal class groups

Let K be an imaginary quadratic field of discriminant d_K and τ_K be as in (5). And, let N be a positive integer, $\mathfrak{n} = N\mathcal{O}_K$ and P be a subgroup of $I_K(\mathfrak{n})$ satisfying $P_{K,1}(\mathfrak{n}) \subseteq P \subseteq P_K(\mathfrak{n})$. Each subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ defines an equivalence relation $\sim_\Gamma$ on the set $\mathcal{Q}_N(d_K)$ described in (7) in the same manner as in (8). In this section, we shall present a necessary and sufficient condition for Γ in such a way that

$$\begin{aligned} \phi_\Gamma : \mathcal{Q}_N(d_K)/\sim_\Gamma &\to I_K(\mathfrak{n})/P \\ [Q] &\mapsto [[\omega_Q, 1]] \end{aligned}$$

becomes a well-defined bijection with ω_Q as in (1). As mentioned in Section 1, the lattice $[\omega_Q, 1] = \mathbb{Z}\omega_Q + \mathbb{Z}$ is a fractional ideal of K.

The modular group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ from the left by fractional linear transformations. For each $Q \in \mathcal{Q}(d_K)$, let I_{ω_Q} denote the isotropy subgroup of the point ω_Q in $\mathrm{SL}_2(\mathbb{Z})$. In particular, if we let Q_0 be the principal form in $\mathcal{Q}(d_K)$ ([3, p. 31]), then we have $\omega_{Q_0} = \tau_K$ and

$$I_{\omega_{Q_0}} = \begin{cases} \{\pm I_2\} & \text{if } d_K \neq -4, -3, \\ \{\pm I_2, \pm S\} & \text{if } d_K = -4, \\ \{\pm I_2, \pm ST, \pm(ST)^2\} & \text{if } d_K = -3, \end{cases} \tag{10}$$

where $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Furthermore, we see that

$$I_{\omega_Q} = \{\pm I_2\} \quad \text{if } w_Q \text{ is not equivalent to } w_{Q_0} \text{ under } \mathrm{SL}_2(\mathbb{Z}) \tag{11}$$

([11, Proposition 1.5 (c)]). For any $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, let

$$j(\gamma, \tau) = c\tau + d \quad (\tau \in \mathbb{H}).$$

One can readily check that if $Q' = Q^\gamma$, then

$$\omega_Q = \gamma(\omega_{Q'}) \quad \text{and} \quad [\omega_Q, 1] = \frac{1}{j(\gamma, \omega_{Q'})}[\omega_{Q'}, 1].$$

Lemma 2.1. *Let $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}(d_K)$. Then $N_{K/\mathbb{Q}}([\omega_Q, 1]) = 1/a$ and*

$$[\omega_Q, 1] \in I_K(\mathfrak{n}) \quad \Leftrightarrow \quad Q \in \mathcal{Q}_N(d_K).$$

Proof. See [10, Lemma 2.3 (iii)]. □

Lemma 2.2. *Let* $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$.

(*i*) *For* $u, v \in \mathbb{Z}$ *not both zero, the fractional ideal* $(u\omega_Q + v)\mathcal{O}_K$ *is relatively prime to* $\mathfrak{n} = N\mathcal{O}_K$ *if and only if* $\gcd(N, Q(v, -u)) = 1$.

(*ii*) *If* $C \in P_K(\mathfrak{n})/P$, *then*

$$C = [(u\omega_Q + v)\mathcal{O}_K] \quad \textit{for some } u, v \in \mathbb{Z} \textit{ not both zero such that } \gcd(N, Q(v, -u)) = 1.$$

Proof.

(i) See [10, Lemma 4.1]

(ii) Since $P_K(\mathfrak{n})/P$ is a finite group, one can take an integral ideal $\mathfrak{c}$ in the class C ([6, Lemma 2.3 in Chapter IV]). Furthermore, since $\mathcal{O}_K = [a\omega_Q, 1]$, we may express $\mathfrak{c}$ as

$$\mathfrak{c} = (ka\omega_Q + v)\mathcal{O}_K \quad \text{for some } k, v \in \mathbb{Z}.$$

If we set $u = ka$, then we attain (ii) by (i). □

Proposition 2.3. *If the map* ϕ_Γ *is well defined, then it is surjective.*

Proof. Let

$$\rho : I_K(\mathfrak{n})/P \to I_K(\mathcal{O}_K)/P_K(\mathcal{O}_K)$$

be the natural homomorphism. Since $I_K(\mathfrak{n})/P_K(\mathfrak{n})$ is isomorphic to $I_K(\mathcal{O}_K)/P_K(\mathcal{O}_K)$ ([6, Proposition 1.5 in Chapter IV]), the homomorphism ρ is surjective. Here, we refer to the following commutative diagram.

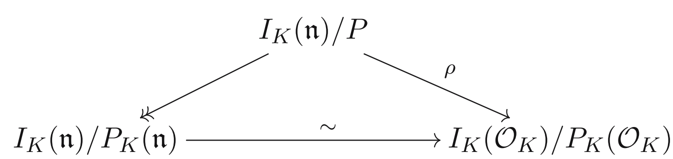

Figure 1: A commutative diagram of ideal class groups.

Let

$$Q_1, Q_2, \ldots, Q_h \quad (\in \mathcal{Q}(d_K))$$

be reduced forms which represent all distinct classes in $\mathcal{C}(d_K) = \mathcal{Q}(d_K)/\sim$ ([3, Theorem 2.8]). Take $\gamma_1, \gamma_2, \ldots, \gamma_h \in \mathrm{SL}_2(\mathbb{Z})$ so that

$$Q_i' = Q_i^{\gamma_i} \quad (i = 1, 2, \ldots, h)$$

belongs to $\mathcal{Q}_N(d_K)$ ([3, Lemmas 2.3 and 2.25]). Then we get

$$I_K(\mathcal{O}_K)/P_K(\mathcal{O}_K) = \{[\omega_{Q_i'}, 1]P_K(\mathcal{O}_K) \mid i = 1, 2, \ldots, h\} \quad \text{and} \quad [\omega_{Q_i'}, 1] \in I_K(\mathfrak{n})$$

by the isomorphism given in (2) (when $D = d_K$) and Lemma 2.1. Moreover, since ρ is a surjection with $\mathrm{Ker}(\rho) = P_K(\mathfrak{n})/P$, we obtain the decomposition

$$I_K(\mathfrak{n})/P = (P_K(\mathfrak{n})/P) \cdot \{[[\omega_{Q_i'}, 1]] \in I_K(\mathfrak{n})/P \mid i = 1, 2, \ldots, h\}. \tag{12}$$

Now, let $C \in I_K(\mathfrak{n})/P$. By the decomposition (12) and Lemma 2.2(ii) we may express C as

$$C = \left[\frac{1}{u\omega_{Q_i'} + v}[\omega_{Q_i'}, 1]\right] \tag{13}$$

for some $i \in \{1, 2, \ldots, h\}$ and $u, v \in \mathbb{Z}$ not both zero with $\gcd(N, Q_i'(v, -u)) = 1$. Take any $\sigma = \begin{bmatrix} * & * \\ \tilde{u} & \tilde{v} \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma \equiv \begin{bmatrix} * & * \\ u & v \end{bmatrix} \pmod{NM_2(\mathbb{Z})}$. We then derive that

$$
\begin{aligned}
C &= \left[\frac{u\omega_{Q_i'}+v}{\tilde{u}\omega_{Q_i'}+\tilde{v}}O_K\right]C \quad \text{because } \frac{u\omega_{Q_i'}+v}{\tilde{u}\omega_{Q_i'}+\tilde{v}} \equiv^* 1 \pmod{\mathfrak{n}} \text{ and } P_{K,1}(\mathfrak{n}) \subseteq P \\
&= \left[\frac{1}{\tilde{u}\omega_{Q_i'}+\tilde{v}}[\omega_{Q_i'},1]\right] \quad \text{by (13)} \\
&= \left[\frac{1}{j(\sigma,\omega_{Q_i'})}[\omega_{Q_i'},1]\right] \\
&= [[\sigma(\omega_{Q_i'}),1]].
\end{aligned}
$$

Thus, if we put $Q = Q_i'^{\sigma^{-1}}$, then we obtain

$$C = [[\omega_Q, 1]] = \phi_\Gamma([Q]).$$

This proves that ϕ_Γ is surjective. □

Proposition 2.4. *The map ϕ_Γ is a well-defined injection if and only if Γ satisfies the following property:*

$$
\begin{aligned}
&\textit{Let } Q \in \mathcal{Q}_N(d_K) \textit{ and } \gamma \in \mathrm{SL}_2(\mathbb{Z}) \textit{ such that } Q^{\gamma^{-1}} \in \mathcal{Q}_N(d_K). \\
&\textit{Then, } j(\gamma,\omega_Q)O_K \in P \iff \gamma \in \Gamma \cdot I_{\omega_Q}.
\end{aligned} \tag{14}
$$

Proof. Assume first that ϕ_Γ is a well-defined injection. Let $Q \in \mathcal{Q}_N(d_K)$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $Q^{\gamma^{-1}} \in \mathcal{Q}_N(d_K)$. If we set $Q' = Q^{\gamma^{-1}}$, then we have $Q = Q'^{\gamma}$ and so

$$[\omega_{Q'}, 1] = [\gamma(\omega_Q), 1] = \frac{1}{j(\gamma,\omega_Q)}[\omega_Q, 1]. \tag{15}$$

And, we deduce that

$$
\begin{aligned}
j(\gamma,\omega_Q)O_K \in P &\iff [[\omega_Q,1]] = [[\omega_{Q'},1]] \text{ in } I_K(\mathfrak{n})/P \text{ by Lemma 2.1 and (15)} \\
&\iff \phi_\Gamma([Q]) = \phi_\Gamma([Q']) \text{ by the definition of } \phi_\Gamma \\
&\iff [Q] = [Q'] \text{ in } \mathcal{Q}_N(d_K)/\sim_\Gamma \text{ since } \phi_\Gamma \text{ is inective} \\
&\iff Q' = Q^\alpha \text{ for some } \alpha \in \Gamma \\
&\iff Q = Q^{\alpha\gamma} \text{ for some } \alpha \in \Gamma \text{ because } Q' = Q^{\gamma^{-1}} \\
&\iff \alpha\gamma \in I_{\omega_Q} \text{ for some } \alpha \in \Gamma \\
&\iff \gamma \in \Gamma \cdot I_{\omega_Q}.
\end{aligned}
$$

Hence, Γ satisfies the property (14).

Conversely, assume that Γ satisfies the property (14). To show that ϕ_Γ is well defined, suppose that

$$[Q] = [Q'] \quad \text{in } \mathcal{Q}_N(d_K)/\sim_\Gamma \text{ for some } Q, Q' \in \mathcal{Q}_N(d_K).$$

Then we attain $Q = Q'^{\alpha}$ for some $\alpha \in \Gamma$ so that

$$[\omega_{Q'}, 1] = [\alpha(\omega_Q), 1] = \frac{1}{j(\alpha,\omega_Q)}[\omega_Q, 1]. \tag{16}$$

Now that $Q^{\alpha^{-1}} = Q' \in \mathcal{Q}_N(d_K)$ and $\alpha \in \Gamma \subseteq \Gamma \cdot I_{\omega_Q}$, we achieve by the property (14) that $j(\alpha,\omega_Q)O_K \in P$. Thus, we derive by Lemma 2.1 and (16) that

$$[[\omega_Q, 1]] = [[\omega_{Q'}, 1]] \quad \text{in } I_K(\mathfrak{n})/P,$$

which claims that ϕ_Γ is well defined.

On the other hand, in order to show that ϕ_Γ is injective assume that

$$\phi_\Gamma([Q]) = \phi_\Gamma([Q']) \quad \text{for some } Q, Q' \in \mathcal{Q}_N(d_K).$$

Then we get

$$[\omega_Q, 1] = \lambda[\omega_{Q'}, 1] \quad \text{for some } \lambda \in K^* \text{ such that } \lambda \mathcal{O}_K \in P, \tag{17}$$

from which it follows that

$$Q = Q'^{\gamma} \quad \text{for some } \gamma \in \mathrm{SL}_2(\mathbb{Z}) \tag{18}$$

by the isomorphism in (2) when $D = d_K$. We then derive by (17) and (18) that

$$[\omega_{Q'}, 1] = [\gamma(\omega_Q), 1] = \frac{1}{j(\gamma, \omega_Q)}[\omega_Q, 1] = \frac{\lambda}{j(\gamma, \omega_Q)}[\omega_{Q'}, 1]$$

and so $\lambda / j(\gamma, \omega_Q) \in \mathcal{O}_K^*$. Therefore, we attain

$$j(\gamma, \omega_Q)\mathcal{O}_K = \lambda \mathcal{O}_K \in P,$$

and hence $\gamma \in \Gamma \cdot I_{\omega_Q}$ by the fact $Q^{\gamma^{-1}} = Q' \in \mathcal{Q}_N(d_K)$ and the property (14). If we write

$$\gamma = \alpha\beta \quad \text{for some } \alpha \in \Gamma \text{ and } \beta \in I_{\omega_Q},$$

then we see by (18) that

$$Q = Q^{\beta^{-1}} = Q^{\gamma^{-1}\alpha} = Q'^{\alpha}.$$

This shows that

$$[Q] = [Q'] \quad \text{in } \mathcal{Q}_N(d_K)/\sim_\Gamma,$$

which proves the injectivity of ϕ_Γ. □

Theorem 2.5. *The map ϕ_Γ is a well-defined bijection if and only if Γ satisfies the property* (14) *stated in* Proposition 2.4. *In this case, we may regard the set $\mathcal{Q}_N(d_K)/\sim_\Gamma$ as a group isomorphic to the ideal class group $I_K(\mathfrak{n})/P$.*

Proof. We achieve the first assertion by Propositions 2.3 and 2.4. Thus, in this case, one can give a group structure on $\mathcal{Q}_N(d_K)/\sim_\Gamma$ through the bijection $\phi_\Gamma : \mathcal{Q}_N(d_K)/\sim_\Gamma \to I_K(\mathfrak{n})/P$. □

Remark 2.6. By using the isomorphism given in (2) (when $D = d_K$) and Theorem 2.5, we obtain the commutative diagram shown in Figure 2.

$$\begin{array}{ccc} \mathcal{Q}_N(d_K)/\sim_\Gamma & \xrightarrow[\phi_\Gamma]{\sim} & I_K(\mathfrak{n})/P \\ \text{The natural map} \downarrow & & \downarrow\!\!\downarrow \rho \text{ in Figure 1} \\ \mathrm{C}(d_K) & \xrightarrow[\text{The classical isomorphism in (2)}]{\sim} & \mathrm{C}(\mathcal{O}_K) \end{array}$$

Figure 2: The natural map between form class groups.

Therefore, the natural map $\mathcal{Q}_N(d_K)/\sim_\Gamma \to C(d_K)$ is indeed a surjective homomorphism, which shows that the group structure of $\mathcal{Q}_N(d_K)/\sim\Gamma$ is not far from that of the classical form class group $\mathrm{C}(d_K)$.

3 Class field theory over imaginary quadratic fields

In this section, we shall briefly review the class field theory over imaginary quadratic fields established by Shimura.

For an imaginary quadratic field K, let $\mathbb{I}_K^{\mathrm{fin}}$ be the group of finite ideals of K given by the restricted product

$$\begin{aligned}\mathbb{I}_K^{\mathrm{fin}} &= \prod_{\mathfrak{p}}{}' K_{\mathfrak{p}}^* \quad \text{where } \mathfrak{p} \text{ runs over all prime ideals of } \mathcal{O}_K \\ &= \left\{ s = (s_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} K_{\mathfrak{p}}^* \mid s_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{p}}}^* \text{ for all but finitely many } \mathfrak{p} \right\}.\end{aligned}$$

As for the topology on $\mathbb{I}_K^{\mathrm{fin}}$ one can refer to [12, p. 78]. Then, the classical class field theory of K is explained by the exact sequence

$$1 \to K^* \to \mathbb{I}_K^{\mathrm{fin}} \to \mathrm{Gal}(K^{\mathrm{ab}}/K) \to 1,$$

where K^* maps into $\mathbb{I}_K^{\mathrm{fin}}$ through the diagonal embedding $\nu \mapsto (\nu, \nu, \nu, \ldots)$ ([12, Chapter IV]). Setting

$$\mathcal{O}_{K,p} = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \text{for each prime } p$$

we have

$$\mathcal{O}_{K,p} \simeq \prod_{\mathfrak{p}|p} \mathcal{O}_{K_{\mathfrak{p}}}$$

([13, Proposition 4 in Chapter II]). Furthermore, if we let $\hat{K} = K \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$ with $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, then

$$\begin{aligned}\hat{K}^* &= \prod_{p}{}' (K \otimes_{\mathbb{Z}} \mathbb{Z}_p)^* \quad \text{where } p \text{ runs over all rational primes} \\ &= \left\{ s = (s_p) \in \prod_p (K \otimes_{\mathbb{Z}} \mathbb{Z}_p)^* \mid s_p \in \mathcal{O}_{K,p}^* \text{ for all but finitely many } p \right\} \simeq \mathbb{I}_K^{\mathrm{fin}}\end{aligned}$$

([3, Exercise 15.12] and [13, Chapter II]). Thus, we may use $\hat{K}^*$ instead of $\mathbb{I}_K^{\mathrm{fin}}$ when we develop the class field theory of K.

Proposition 3.1. *There is a one-to-one correspondence via the Artin map between closed subgroups J of $\hat{K}^*$ of finite index containing K^* and finite abelian extensions L of K such that*

$$\hat{K}^*/J \simeq \mathrm{Gal}(L/K).$$

Proof. See [12, Chapter IV]. □

Let N be a positive integer, $\mathfrak{n} = N\mathcal{O}_K$ and $s = (s_p) \in \hat{K}^*$. For a prime p and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying above p, let $n_{\mathfrak{p}}(s)$ be a unique integer such that $s_p \in \mathfrak{p}^{n_{\mathfrak{p}}(s)}\mathcal{O}_{K_{\mathfrak{p}}}^*$. We then regard $s\mathcal{O}_K$ as the fractional ideal

$$s\mathcal{O}_K = \prod_p \prod_{\mathfrak{p}|p} \mathfrak{p}^{n_{\mathfrak{p}}(s)} \in I_K(\mathcal{O}_K).$$

By the approximation theorem ([6, Chapter IV]) one can take an element ν_s of K^* such that

$$\nu_s s_p \in 1 + N\mathcal{O}_{K,p} \quad \text{for all } p|N. \tag{19}$$

Proposition 3.2. *We get a well-defined surjective homomorphism*

$$\begin{aligned}\phi_{\mathfrak{n}} : \hat{K}^* &\to I_K(\mathfrak{n})/P_{K,1}(\mathfrak{n}) \\ s &\mapsto [\nu_s s\mathcal{O}_K]\end{aligned}$$

with kernel

$$J_{\mathfrak{n}} = K^* \left(\prod_{p|N} (1 + N\mathcal{O}_{K,p}) \times \prod_{p\nmid N} \mathcal{O}_{K,p}^* \right).$$

Thus, $J_{\mathfrak{n}}$ corresponds to the ray class field $K_{\mathfrak{n}}$.

Proof. See [3, Exercises 15.17 and 15.18]. □

Let $\mathcal{F}_N$ be the field of meromorphic modular functions of level N whose Fourier expansions with respect to $q^{1/N}$ have coefficients in the Nth cyclotomic field $\mathbb{Q}(\zeta_N)$ with $\zeta_N = e^{2\pi\mathrm{i}/N}$. Then $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1$ with $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ ([7, Chapter 6]).

Proposition 3.3. *There is a decomposition*

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} = \left\{\pm\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \mid d \in (\mathbb{Z}/N\mathbb{Z})^*\right\}/\{\pm I_2\} \cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}.$$

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

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

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

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

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

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

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

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

Proof. See [7, Proposition 6.21]. □

If we let $\hat{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$ and $\mathcal{F} = \bigcup_{N=1}^{\infty} \mathcal{F}_N$, then we attain the exact sequence

$$1 \to \mathbb{Q}^* \to \mathrm{GL}_2(\hat{\mathbb{Q}}) \to \mathrm{Gal}(\mathcal{F}/\mathbb{Q}) \to 1 \tag{20}$$

([5, Chapter 7] or [7, Chapter 6]). Here, we note that

$$\begin{aligned} \mathrm{GL}_2(\hat{\mathbb{Q}}) &= \prod_p{}' \mathrm{GL}_2(\mathbb{Q}_p), \quad \text{where } p \text{ runs over all rational primes} \\ &= \left\{\gamma = (\gamma_p) \in \prod_p \mathrm{GL}_2(\mathbb{Q}_p) \mid \gamma_p \in \mathrm{GL}_2(\mathbb{Z}_p) \ \text{ for all but finitely many } p\right\} \end{aligned}$$

([3, Exercise 15.4]) and $\mathbb{Q}^*$ maps into $\mathrm{GL}_2(\hat{\mathbb{Q}})$ through the diagonal embedding. More precisely, let $h(\tau) \in \mathcal{F}_N$ and $\gamma \in \mathrm{GL}_2(\hat{\mathbb{Q}})$, and then $\gamma = \alpha\beta$ with $\alpha = (\alpha_p)_p \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ and $\beta \in \mathrm{GL}_2^+(\mathbb{Q})$ ([3, Theorem 15.9 (i)] and [5, Theorem 1 in Chapter 7]). By using the Chinese remainder theorem, one can find a unique matrix $\tilde{\alpha}$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $\tilde{\alpha} \equiv \alpha_p \pmod N$ for all primes p such that $p|N$. Letting $\sigma_{\mathcal{F}} : \mathrm{GL}_2(\hat{\mathbb{Q}}) \to \mathrm{Gal}(\mathcal{F}/\mathbb{Q})$ be the third homomorphism in (20), we obtain

$$h(\tau)^{\sigma_{\mathcal{F}}(\gamma)} = h^{\tilde{\alpha}}(\beta(\tau)) \tag{21}$$

([5, Theorem 2 in Chapter 7 and p. 79]).

For $\omega \in K \cap \mathbb{H}$, we define a normalized embedding

$$q_\omega : K^* \to \mathrm{GL}_2^+(\mathbb{Q})$$

by the relation

$$v\begin{bmatrix} \omega \\ 1 \end{bmatrix} = q_\omega(v)\begin{bmatrix} \omega \\ 1 \end{bmatrix} \quad (v \in K^*). \tag{22}$$

By continuity, q_ω can be extended to an embedding

$$q_{\omega,p} : (K \otimes_{\mathbb{Z}} \mathbb{Z}_p)^* \to \mathrm{GL}_2(\mathbb{Q}_p) \quad \text{for each prime } p$$

and hence to an embedding

$$q_\omega : \hat{K}^* \to \mathrm{GL}_2(\hat{\mathbb{Q}}).$$

Let $\min(\tau_K, \mathbb{Q}) = x^2 + b_K x + c_K$ ($\in \mathbb{Z}[x]$). Since $K \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathbb{Q}_p\tau_K + \mathbb{Q}_p$ for each prime p, one can deduce that if $s = (s_p) \in \hat{K}^*$ with $s_p = u_p\tau_K + v_p$ ($u_p, v_p \in \mathbb{Q}_p$), then

$$q_{\tau_K}(s) = (\gamma_p) \text{ with } \gamma_p = \begin{bmatrix} v_p - b_K u_p & -c_K u_p \\ u_p & v_p \end{bmatrix}. \tag{23}$$

By utilizing the concept of canonical models of modular curves, Shimura achieved the following remarkable results.

Proposition 3.4. (Shimura's reciprocity law) *Let $s \in \hat{K}^*$, $\omega \in K \cap \mathbb{H}$ and $h \in \mathcal{F}$ be finite at ω. Then $h(\omega)$ lies in K^{ab} and satisfies*

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

where $[\cdot, K]$ is the Artin map for K.

Proof. See [7, Theorem 6.31(i)]. □

Proposition 3.5. *Let S be an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Q}})$ containing $\mathbb{Q}^*$ such that $S/\mathbb{Q}^*$ is compact. Let*

$$\begin{aligned}
\Gamma_S &= S \cap \mathrm{GL}_2^+(\mathbb{Q}),\\
\mathcal{F}_S &= \{h \in \mathcal{F} \mid h^\gamma = h \text{ for all } \gamma \in S\},\\
k_S &= \{\nu \in \mathbb{Q}^{\mathrm{ab}} \mid \nu^{[s,\mathbb{Q}]} = \nu \text{ for all } s \in \mathbb{Q}^* \det(S) \subseteq \hat{\mathbb{Q}}^*\},
\end{aligned}$$

where $[\cdot,\mathbb{Q}]$ is the Artin map for $\mathbb{Q}$. Then,

(i) $\Gamma_S/\mathbb{Q}^*$ *is a Fuchsian group of the first kind commensurable with* $\mathrm{SL}_2(\mathbb{Z})/\{\pm I_2\}$.

(ii) $\mathbb{C}\mathcal{F}_S$ *is the field of meromorphic modular functions for* $\Gamma_S/\mathbb{Q}^*$.

(iii) k_S *is algebraically closed in* $\mathcal{F}_S$.

(iv) If $\omega \in K \cap \mathbb{H}$, then the subgroup $K^* q_\omega^{-1}(S)$ of $\hat{K}^*$ corresponds to the subfield

$$K\mathcal{F}_S(\omega) = K(h(\omega) \mid h \in \mathcal{F}_S \text{ is finite at } \omega)$$

of K^{ab} in view of Proposition 3.1.

Proof. See [7, Propositions 6.27 and 6.33]. □

Remark 3.6. In particular, if $k_S = \mathbb{Q}$, then $\mathcal{F}_S = \mathcal{F}_{\Gamma_S,\mathbb{Q}}$ ([7, Exercise 6.26]).

4 Construction of class invariants

Let K be an imaginary quadratic field, N be a positive integer and $\mathfrak{n} = N\mathcal{O}_K$. From now on, let T be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ and P be a subgroup of $P_K(\mathfrak{n})$ containing $P_{K,1}(\mathfrak{n})$ given by

$$\begin{aligned}
P &= \langle \nu\mathcal{O}_K \mid \nu \in \mathcal{O}_K - \{0\} \text{ such that } \nu \equiv t \pmod{\mathfrak{n}} \text{ for some } t \in T\rangle\\
&= \{\lambda\mathcal{O}_K \mid \lambda \in K^* \text{ such that } \lambda \equiv^* t \pmod{\mathfrak{n}} \text{ for some } t \in T\}.
\end{aligned}$$

Let $\mathrm{Cl}(P)$ denote the ideal class group

$$\mathrm{Cl}(P) = I_K(\mathfrak{n})/P$$

and K_P be its corresponding class field of K with $\mathrm{Cl}(P) \simeq \mathrm{Gal}(K_P/K)$. Furthermore, let

$$\Gamma = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{bmatrix} t^{-1} & * \\ 0 & t \end{bmatrix} (\mathrm{mod}\ NM_2(\mathbb{Z})) \text{ for some } t \in T\right\},$$

where t^{-1} stands for an integer such that $tt^{-1} \equiv 1 \pmod N$. In this section, for a given $h \in \mathcal{F}_{\Gamma,\mathbb{Q}}$ we shall define a class invariant $h(C)$ for each class $C \in I_K(\mathfrak{n})/P$.

Lemma 4.1. *The field K_P corresponds to the subgroup*

$$\bigcup_{t \in T} K^* \left(\prod_{p \mid N} (t + NO_{K,p}) \times \prod_{p \nmid N} O_{K,p}^* \right)$$

of $\hat{K}^*$ in view of Proposition 3.1.

Proof. We adopt the notations in Proposition 3.2. Given $t \in T$, let t^{-1} be an integer such that $tt^{-1} \equiv 1 \pmod N$. Let $s = s(t) = (s_p) \in \hat{K}^*$ be given by

$$s_p = \begin{cases} t^{-1} & \text{if } p \mid N, \\ 1 & \text{if } p \nmid N. \end{cases}$$

Then one can take $\nu_s = t$ so as to have (19), and hence

$$\phi_{\mathfrak{n}}(s) = [tsO_K] = [tO_K]. \tag{24}$$

Since P contains $P_{K,1}(\mathfrak{n})$, we obtain $K_P \subseteq K_{\mathfrak{n}}$ and $\mathrm{Gal}(K_{\mathfrak{n}}/K_P) \simeq P/P_{K,1}(\mathfrak{n})$. Thus, we achieve by Proposition 3.2 that the field K_P corresponds to

$$\begin{aligned}
\phi_{\mathfrak{n}}^{-1}(P/P_{K,1}(\mathfrak{n})) &= \phi_{\mathfrak{n}}^{-1}\left(\bigcup_{t \in T} [tO_K] \right) \quad \text{by the definitions of } P_{K,1}(\mathfrak{n}) \text{ and } P \\
&= \bigcup_{t \in T} s(t) J_{\mathfrak{n}} \quad \text{by (24) and the fact } J_{\mathfrak{n}} = \mathrm{Ker}(\phi_{\mathfrak{n}}) \\
&= \bigcup_{t \in T} K^* \left(\prod_{p \mid N} (t^{-1} + NO_{K,p}) \times \prod_{p \nmid N} O_{K,p}^* \right) \\
&= \bigcup_{t \in T} K^* \left(\prod_{p \mid N} (t + NO_{K,p}) \times \prod_{p \nmid N} O_{K,p}^* \right).
\end{aligned}$$

□

Proposition 4.2. *We have $K_P = K\mathcal{F}_{\Gamma,\mathbb{Q}}(\tau_K)$.*

Proof. Let $S = \mathbb{Q}^* W$ $(\subseteq \mathrm{GL}_2(\hat{\mathbb{Q}}))$ with

$$W = \bigcup_{t \in T} \left\{ \gamma = (\gamma_p) \in \prod_p \mathrm{GL}_2(\mathbb{Z}_p) \mid \gamma_p \equiv \begin{bmatrix} * & * \\ 0 & t \end{bmatrix} (\mathrm{mod}\ NM_2(\mathbb{Z}_p)) \text{ for all } p \right\}.$$

Following the notations in Proposition 3.5 one can readily show that

$$\Gamma_S = \mathbb{Q}^* \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{bmatrix} * & * \\ 0 & t \end{bmatrix} (\mathrm{mod}\ NM_2(\mathbb{Z})) \text{ for some } t \in T \right\} \text{ and } \det(W) = \hat{\mathbb{Z}}^*.$$

It then follows that $\Gamma_S/\mathbb{Q}^* \simeq \Gamma/\{\pm I_2\}$ and $k_S = \mathbb{Q}$, and hence

$$\mathcal{F}_S = \mathcal{F}_{\Gamma,\mathbb{Q}} \tag{25}$$

by Proposition 3.5(ii) and Remark 3.6. Furthermore, we deduce that

$$\begin{aligned}
K^*q_{\tau_K}^{-1}(S) &= K^*\{s=(s_p)\in\hat{K}^*\mid q_{\tau_K}(s)\in\mathbb{Q}^*W\}\\
&= K^*\{s=(s_p)\in\hat{K}^*\mid q_{\tau_K}(s)\in W\}\ \text{ since } q_{\tau_K}(r)=rI_2 \text{ for every } r\in\mathbb{Q}^* \text{ by (22)}\\
&= K^*\Big\{s=(s_p)\in\hat{K}^*\mid s_p=u_p\tau_K+v_p \text{ with } u_p,v_p\in\mathbb{Q}_p \text{ such that}\\
&\qquad \gamma_p=\begin{bmatrix} v_p-b_Ku_p & -c_Ku_p\\ u_p & v_p\end{bmatrix}\in W \text{ for all } p\Big\} \text{ by (23)}\\
&= \bigcup_{t\in T}K^*\Big\{s=(s_p)\in\hat{K}^*\mid s_p=u_p\tau_K+v_p \text{ with } u_p,v_p\in\mathbb{Z}_p \text{ such that}\\
&\qquad \gamma_p\in\mathrm{GL}_2(\mathbb{Z}_p) \text{ and } \gamma_p\equiv\begin{bmatrix} * & *\\ 0 & t\end{bmatrix}(\mathrm{mod}\ NM_2(\mathbb{Z}_p)) \text{ for all } p\Big\}\\
&= \bigcup_{t\in T}K^*\{s=(s_p)\in\hat{K}^*\mid s_p=u_p\tau_K+v_p \text{ with } u_p,v_p\in\mathbb{Z}_p \text{ such that}\\
&\qquad \det(\gamma_p)=(u_p\tau_K+v_p)(u_p\bar{\tau}_K+v_p)\in\mathbb{Z}_p^*,\\
&\qquad u_p\equiv 0\,(\mathrm{mod}\ N\mathbb{Z}_p) \text{ and } v_p\equiv t\,(\mathrm{mod}\ N\mathbb{Z}_p) \text{ for all } p\}\\
&= \bigcup_{t\in T}K^*\Big(\prod_{p\mid N}(t+NO_{K,p})\times\prod_{p\nmid N}O_{K,p}^*\Big).
\end{aligned}$$

Therefore, we conclude by Proposition 3.5(iv), (25) and Lemma 4.1 that

$$K_P = K\mathcal{F}_{\Gamma,\mathbb{Q}}(\tau_K). \qquad \square$$

Let $C\in\mathrm{Cl}(P)$. Take an integral ideal $\mathfrak{a}$ in the class C, and let ξ_1 and ξ_2 be elements of K^* so that

$$\mathfrak{a}^{-1}=[\xi_1,\xi_2]\quad\text{and}\quad \xi=\frac{\xi_1}{\xi_2}\in\mathbb{H}.$$

Since $O_K=[\tau_K,1]\subseteq\mathfrak{a}^{-1}$ and $\xi\in\mathbb{H}$, one can express

$$\begin{bmatrix}\tau_K\\ 1\end{bmatrix}=A\begin{bmatrix}\xi_1\\ \xi_2\end{bmatrix}\quad\text{for some } A\in M_2^+(\mathbb{Z}). \tag{26}$$

We find by taking determinant of

$$\begin{bmatrix}\tau_K & \bar{\tau}_K\\ 1 & 1\end{bmatrix}=A\begin{bmatrix}\xi_1 & \bar{\xi}_1\\ \xi_2 & \bar{\xi}_2\end{bmatrix}$$

that

$$\det\left(\begin{bmatrix}\tau_K & \bar{\tau}_K\\ 1 & 1\end{bmatrix}\right)=\det(A)\det\left(\begin{bmatrix}\xi_1 & \bar{\xi}_1\\ \xi_2 & \bar{\xi}_2\end{bmatrix}\right),$$

and so obtain by squaring both sides

$$d_K=\det(A)^2\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})^{-2}d_K$$

([15, Chapter III]). Hence, $\det(A)=\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$ which is relatively prime to N. For $\alpha\in M_2(\mathbb{Z})$ with $\gcd(N,\det(\alpha))=1$, we shall denote by $\tilde{\alpha}$ its reduction onto $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ $(\simeq\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1))$.

Definition 4.3. Let $h\in\mathcal{F}_{\Gamma,\mathbb{Q}}$ $(\subseteq\mathcal{F}_N)$. With the notations as above, we define

$$h(C)=h(\tau)^{\tilde{A}}|_{\tau=\xi}$$

if it is finite.

Proposition 4.4. *If $h(C)$ is finite, then it depends only on the class C regardless of the choice of $\mathfrak{a}$, ξ_1 and ξ_2.*

Proof. Let $\mathfrak{a}'$ be also an integral ideal in C. Take any $\xi_1', \xi_2' \in K^*$ so that

$$\mathfrak{a}'^{-1} = [\xi_1', \xi_2'] \quad \text{and} \quad \xi' = \frac{\xi_1'}{\xi_2'} \in \mathbb{H}. \tag{27}$$

Since $O_K \subseteq \mathfrak{a}'^{-1}$ and $\xi' \in \mathbb{H}$, we may write

$$\begin{bmatrix} \tau_K \\ 1 \end{bmatrix} = A' \begin{bmatrix} \xi_1' \\ \xi_2' \end{bmatrix} \quad \text{for some } A' \in M_2^+(\mathbb{Z}). \tag{28}$$

Now that $[\mathfrak{a}] = [\mathfrak{a}'] = C$, we have

$$\mathfrak{a}' = \lambda\mathfrak{a} \quad \text{with } \lambda \in K^* \text{ such that } \lambda \equiv^* t \ (\mathrm{mod}\ \mathfrak{n}) \text{ for some } t \in T.$$

Then it follows that

$$\mathfrak{a}'^{-1} = \lambda^{-1}\mathfrak{a}^{-1} = [\lambda^{-1}\xi_1, \lambda^{-1}\xi_2] \quad \text{and} \quad \frac{\lambda^{-1}\xi_1}{\lambda^{-1}\xi_2} = \xi. \tag{29}$$

And, we obtain by (27) and (29) that

$$\begin{bmatrix} \xi_1' \\ \xi_2' \end{bmatrix} = B \begin{bmatrix} \lambda^{-1}\xi_1 \\ \lambda^{-1}\xi_2 \end{bmatrix} \quad \text{for some } B \in \mathrm{SL}_2(\mathbb{Z}) \tag{30}$$

and

$$\xi' = B(\xi). \tag{31}$$

On the other hand, consider t as an integer whose reduction modulo N belongs to T. Since $\mathfrak{a}, \mathfrak{a}' = \lambda\mathfrak{a} \subseteq O_K$, we see that $(\lambda - t)\mathfrak{a}$ is an integral ideal. Moreover, since $\lambda \equiv^* t \ (\mathrm{mod}\ \mathfrak{n})$ and $\mathfrak{a}$ is relatively prime to $\mathfrak{n}$, we get $(\lambda - t)\mathfrak{a} \subseteq \mathfrak{n} = NO_K$, and hence

$$(\lambda - t)O_K \subseteq N\mathfrak{a}^{-1}.$$

Thus, we attain by the facts $O_K = [\tau_K, 1]$ and $\mathfrak{a}^{-1} = [\xi_1, \xi_2]$ that

$$\begin{bmatrix} (\lambda - t)\tau_K \\ \lambda - t \end{bmatrix} = A'' \begin{bmatrix} N\xi_1 \\ N\xi_2 \end{bmatrix} \quad \text{for some } A'' \in M_2^+(\mathbb{Z}). \tag{32}$$

We then derive that

$$\begin{aligned} NA'' \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} &= \lambda \begin{bmatrix} \tau_K \\ 1 \end{bmatrix} - t \begin{bmatrix} \tau_K \\ 1 \end{bmatrix} \quad \text{by (32)} \\ &= \lambda A' \begin{bmatrix} \xi_1' \\ \xi_2' \end{bmatrix} - tA \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \quad \text{by (26) and (28)} \\ &= A'B \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} - tA \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \quad \text{by (30)}. \end{aligned}$$

This yields $A'B - tA \equiv O \ (\mathrm{mod}\ NM_2(\mathbb{Z}))$ and so

$$A' \equiv tAB^{-1} \ (\mathrm{mod}\ NM_2(\mathbb{Z})). \tag{33}$$

Therefore, we establish by Proposition 3.3 that

$$
\begin{aligned}
h(\tau)^{\widetilde{A'}}|_{\tau=\xi'} &= h(\tau)^{\widetilde{tAB^{-1}}}|_{\tau=\xi'} \quad \text{by (33)} \\
&\qquad \text{where } \widetilde{\ } \text{ means the reduction onto } \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \\
&= h(\tau)^{\widetilde{\begin{bmatrix}1&0\\0&t^2\end{bmatrix}}\widetilde{\begin{bmatrix}t&0\\0&t^{-1}\end{bmatrix}}\widetilde{AB^{-1}}}|_{\tau=\xi'} \\
&= h(\tau)^{\widetilde{\begin{bmatrix}t&0\\0&t^{-1}\end{bmatrix}}\widetilde{AB^{-1}}}|_{\tau=\xi'} \quad \text{because } h(t) \text{ has rational Fourier coefficients} \\
&= h(\tau)^{\widetilde{AB^{-1}}}|_{\tau=\xi'} \quad \text{since } h(t) \text{ is modular for } \Gamma \\
&= h(\tau)^{\tilde{A}}|_{\tau=B^{-1}(\xi')} \\
&= h(\tau)^{\tilde{A}}|_{\tau=\xi} \quad \text{by (31).}
\end{aligned}
$$

This proves that $h(C)$ depends only on the class C. □

Remark 4.5. If we let C_0 be the identity class in $\mathrm{Cl}(P)$, then we have $h(C_0) = h(\tau_K)$.

Proposition 4.6. *Let $C \in \mathrm{Cl}(P)$ and $h \in \mathcal{F}_{\Gamma,\mathbb{Q}}$. If $h(C)$ is finite, then it belongs to K_P and satisfies*

$$h(C)^{\sigma(C')} = h(CC') \quad \textit{for all } C' \in Cl(P),$$

where $\sigma : \mathrm{Cl}(P) \to \mathrm{Gal}(K_P/K)$ is the isomorphism induced from the Artin map.

Proof. Let $\mathfrak{a}$ be an integral ideal in C and $\xi_1, \xi_2 \in K^*$ such that

$$\mathfrak{a}^{-1} = [\xi_1, \xi_2] \quad \text{with } \xi = \frac{\xi_1}{\xi_2} \in \mathbb{H}. \tag{34}$$

Then we have

$$\begin{bmatrix}\tau_K\\1\end{bmatrix} = A\begin{bmatrix}\xi_1\\\xi_2\end{bmatrix} \quad \text{for some } A \in M_2^+(\mathbb{Z}). \tag{35}$$

Furthermore, let $\mathfrak{a}'$ be an integral ideal in C' and $\xi_1'', \xi_2'' \in K^*$ such that

$$(\mathfrak{a}\mathfrak{a}')^{-1} = [\xi_1'', \xi_2''] \quad \text{with } \xi'' = \frac{\xi_1''}{\xi_2''} \in \mathbb{H}. \tag{36}$$

Since $\mathfrak{a}^{-1} \subseteq (\mathfrak{a}\mathfrak{a}')^{-1}$ and $\xi'' \in \mathbb{H}$, we get

$$\begin{bmatrix}\xi_1\\\xi_2\end{bmatrix} = B\begin{bmatrix}\xi_1''\\\xi_2''\end{bmatrix} \quad \text{for some } B \in M_2^+(\mathbb{Z}), \tag{37}$$

and so it follows from (35) that

$$\begin{bmatrix}\tau_K\\1\end{bmatrix} = AB\begin{bmatrix}\xi_1''\\\xi_2''\end{bmatrix}. \tag{38}$$

Let $s = (s_p)$ be an ideal in $\hat{K}^*$ satisfying

$$\begin{cases} s_p = 1 & \text{if } p|N, \\ s_p\mathcal{O}_{K,p} = \mathfrak{a}_p' & \text{if } p\nmid N, \end{cases} \tag{39}$$

where $\mathfrak{a}_p' = \mathfrak{a}' \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Since $\mathfrak{a}'$ is relatively prime to $\mathfrak{n} = N\mathcal{O}_K$, we obtain by (39) that

$$s_p^{-1}\mathcal{O}_{K,p} = \mathfrak{a}_p'^{-1} \quad \text{for all } p. \tag{40}$$

Now, we see that

$$q_{\xi,p}(s_p^{-1})\begin{bmatrix}\xi_1\\ \xi_2\end{bmatrix} = \xi_2 q_{\xi,p}(s_p^{-1})\begin{bmatrix}\xi\\ 1\end{bmatrix} = \xi_2 s_p^{-1}\begin{bmatrix}\xi\\ 1\end{bmatrix} = s_p^{-1}\begin{bmatrix}\xi_1\\ \xi_2\end{bmatrix},$$

which shows by (34) and (40) that $q_{\xi,p}(s_p^{-1})\begin{bmatrix}\xi_1\\ \xi_2\end{bmatrix}$ is a $\mathbb{Z}_p$-basis for $(\mathfrak{a}\mathfrak{a}')_p^{-1}$. Furthermore, $B^{-1}\begin{bmatrix}\xi_1\\ \xi_2\end{bmatrix}$ is also a $\mathbb{Z}_p$-basis for $(\mathfrak{a}\mathfrak{a}')_p^{-1}$ by (36) and (37). Thus, we achieve

$$q_{\xi,p}(s_p^{-1}) = \gamma_p B^{-1} \quad \text{for some } \gamma_p \in \mathrm{GL}_2(\mathbb{Z}_p). \tag{41}$$

Letting $\gamma = (\gamma_p) \in \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$ we get

$$q_\xi(s^{-1}) = \gamma B^{-1}. \tag{42}$$

We then deduce that

$$\begin{aligned}
h(C)^{[s,K]} &= (h(\tau)^{\tilde{A}}|_{\tau=\xi})^{[s,K]} \quad \text{by Definition 4.3}\\
&= (h(\tau)^{\tilde{A}})^{\sigma_{\mathcal{F}}(q_\xi(s^{-1}))}|_{\tau=\xi} \quad \text{by Proposition 3.4}\\
&= (h(\tau)^{\tilde{A}})^{\sigma_{\mathcal{F}}(\gamma B^{-1})}|_{\tau=\xi} \quad \text{by (42)}\\
&= h(\tau)^{\tilde{A}\tilde{G}}|_{\tau=B^{-1}(\xi)} \quad \text{by (21), where } G \text{ is a matrix in } M_2(\mathbb{Z}) \text{ such that}\\
&\qquad\qquad G \equiv \gamma_p \pmod{NM_2(\mathbb{Z}_p)} \text{ for all } p|N\\
&= h(\tau)^{\tilde{A}\tilde{B}}|_{\tau=\xi''} \quad \text{by (37) and the fact that for each } p|N,\\
&\qquad\qquad s_p = 1 \text{ and so } \gamma_p B^{-1} = I_2 \text{ owing to (39) and (41)}\\
&= h(CC') \quad \text{by Definition 4.3 and (38).}
\end{aligned}$$

In particular, if we consider the case where $C' = C^{-1}$, then we derive that

$$h(C) = h(CC')^{[s^{-1},K]} = h(C_0)^{[s^{-1},K]} = h(\tau_K)^{[s^{-1},K]}.$$

This implies that $h(C)$ belongs to K_P by Proposition 4.2.

For each $p\nmid N$ and $\mathfrak{p}$ lying above p, we have by (39) that $\mathrm{ord}_\mathfrak{p}\ s_p = \mathrm{ord}_\mathfrak{p}\ \mathfrak{a}'$, and hence

$$[s,K]|_{K_P} = \sigma(C').$$

Therefore, we conclude

$$h(C)^{\sigma(C')} = h(CC').$$ □

5 Extended form class groups as Galois groups

With P, K_P and Γ as in Section 4, we shall prove our main theorem which asserts that $\mathcal{Q}_N(d_K)/\sim_\Gamma$ can be regarded as a group isomorphic to $\mathrm{Gal}(K_P/K)$ through the isomorphism described in (9).

Lemma 5.1. *If $Q \in \mathcal{Q}(d_K)$ and $\gamma \in I_{\omega_Q}$, then $j(\gamma,\omega_Q) \in \mathcal{O}_K^*$.*

Proof. We obtain from $Q = Q^\gamma$ that

$$[\omega_Q, 1] = [\gamma(\omega_Q), 1] = \frac{1}{j(\gamma,\omega_Q)}[\omega_Q, 1].$$

This claims that $j(\gamma,\omega_Q)$ is a unit in $\mathcal{O}_K$. □

Remark 5.2. This lemma can also be justified by using (10), (11) and the property

$$j(\alpha\beta,\tau)=j(\alpha,\beta(\tau))j(\beta,\tau)\quad(\alpha,\beta\in \mathrm{SL}_2(\mathbb{Z}),\ \tau\in\mathbb{H}) \tag{43}$$

([7, (1.2.4)]).

Proposition 5.3. *For given P, the group Γ satisfies the property* (14).

Proof. Let $Q=ax^2+bxy+cy^2\in \mathcal{Q}_N(d_K)$ and $\gamma\in\mathrm{SL}_2(\mathbb{Z})$ such that $Q^{\gamma^{-1}}\in\mathcal{Q}_N(d_K)$.

Assume that $j(\gamma,\omega_Q)\mathcal{O}_K\in P$. Then we have

$$j(\gamma,\omega_Q)\mathcal{O}_K=\frac{\nu_1}{\nu_2}\mathcal{O}_K\quad\text{for some } \nu_1,\nu_2\in\mathcal{O}_K-\{0\}$$

satisfying

$$\nu_1\equiv t_1,\ \nu_2\equiv t_2 \pmod{\mathfrak{n}}\ \text{ with } t_1,t_2\in T \tag{44}$$

and hence

$$\zeta j(\gamma,\omega_Q)=\frac{\nu_1}{\nu_2}\quad\text{for some } \zeta\in\mathcal{O}_K^*. \tag{45}$$

For convenience, let $j=j(\gamma,\omega_Q)$ and $Q'=Q^{\gamma^{-1}}$. Then we deduce

$$\gamma(\omega_Q)=\omega_{Q'} \tag{46}$$

and

$$[\omega_Q,1]=j[\gamma(\omega_Q),1]=j[\omega_{Q'},1]=\zeta j[\omega_{Q'},1].$$

So there is $\alpha=\begin{bmatrix} r & s\\ u & v\end{bmatrix}\in\mathrm{GL}_2(\mathbb{Z})$, which yields

$$\begin{bmatrix}\zeta j\omega_{Q'}\\ \zeta j\end{bmatrix}=\alpha\begin{bmatrix}\omega_Q\\ 1\end{bmatrix}. \tag{47}$$

Here, since $\zeta j\omega_{Q'}/\zeta j=\omega_{Q'},\ \omega_Q\in\mathbb{H}$, we get $\alpha\in\mathrm{SL}_2(\mathbb{Z})$ and

$$\omega_{Q'}=\alpha(\omega_Q). \tag{48}$$

Thus, we attain $\gamma(\omega_Q)=\omega_{Q'}=\alpha(\omega_Q)$ by (46) and (48), from which we get $\omega_Q=(\alpha^{-1}\gamma)(\omega_Q)$ and so

$$\gamma\in\alpha\cdot I_{\omega_Q}. \tag{49}$$

Now that $aj\in\mathcal{O}_K$, we see from (44), (45) and (47) that

$$a\nu_2(\zeta j)\equiv a\nu_1\equiv at_1 \pmod{\mathfrak{n}},\ \text{ and}$$
$$a\nu_2(\zeta j)\equiv a\nu_2(u\omega_Q+v)\equiv ut_2(a\omega_Q)+at_2v \pmod{\mathfrak{n}}.$$

It then follows that

$$at_1\equiv ut_2(a\omega_Q)+at_2v \pmod{\mathfrak{n}}$$

and hence

$$ut_2(a\omega_Q)+a(t_2v-t_1)\equiv 0 \pmod{\mathfrak{n}}.$$

Since $\mathfrak{n}=N\mathcal{O}_K=N[a\omega_Q,1]$, we have

$$ut_2\equiv 0 \pmod{N}\quad\text{and}\quad a(t_2v-t_1)\equiv 0 \pmod{N}.$$

Moreover, since $\gcd(N,t_1)=\gcd(N,t_2)=\gcd(N,a)=1$, we achieve that

$$u\equiv 0 \pmod{N}\quad\text{and}\quad v\equiv t_1t_2^{-1} \pmod{N},$$

where t_2^{-1} is an integer satisfying $t_2t_2^{-1}\equiv 1 \pmod{N}$. This, together with the facts $\det(\alpha)=1$ and T is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$, implies $\alpha=\begin{bmatrix} r & s\\ u & v\end{bmatrix}\in\Gamma$. Therefore, we conclude $\gamma\in\Gamma\cdot I_{\omega_Q}$ by (49), as desired.

Conversely, assume that $\gamma \in \Gamma \cdot I_{\omega_Q}$, and so

$$\gamma = \alpha\beta \quad \text{for some } \alpha = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \in \Gamma \text{ and } \beta \in I_{\omega_Q}.$$

Here we observe that

$$u \equiv 0 \pmod N \quad \text{and} \quad v \equiv t \pmod N \ \text{ for some } t \in T. \tag{50}$$

We then derive that

$$\begin{aligned} j(\gamma, \omega_Q) &= j(\alpha\beta, \omega_Q) \\ &= j(\alpha, \beta(\omega_Q)) j(\beta, \omega_Q) \quad \text{by (43)} \\ &= j(\alpha, \omega_Q)\zeta \quad \text{for some } \zeta \in O_K^* \text{ by the fact } \beta \in I_{w_Q} \text{ and Lemma 5.1.} \end{aligned}$$

Thus, we attain

$$\zeta^{-1} j(\gamma, \omega_Q) - v = j(\alpha, \omega_Q) - v = (u\omega_Q + v) - v = \frac{1}{a}\{u(a\omega_Q)\}.$$

And, it follows from the fact $\gcd(N, a) = 1$ and (50) that

$$\zeta^{-1} j(\gamma, \omega_Q) \equiv^* v \equiv^* t \pmod{\mathfrak{n}}.$$

This shows that $\zeta^{-1} j(\gamma, \omega_Q) O_K \in P$, and hence $j(\gamma, \omega_Q) O_K \in P$.

Therefore, the group Γ satisfies the property (14) for P. □

Theorem 5.4. *We have an isomorphism*

$$\begin{aligned} \mathcal{Q}_N(d_K)/\sim_\Gamma &\to Gal(K_P/K) \\ [Q] &\mapsto (h(\tau_K) \mapsto h(-\bar{\omega}_Q) \mid h \in \mathcal{F}_{\Gamma,\mathbb{Q}} \text{ is finite at } \tau_K). \end{aligned} \tag{51}$$

Proof. By Theorem 2.5 and Proposition 5.3, one may consider $\mathcal{Q}_N(d_K)/\sim_\Gamma$ as a group isomorphic to $I_K(\mathfrak{n})/P$ via the isomorphism ϕ_Γ in Section 2. Let $C \in \mathrm{Cl}(P)$ and so

$$C = \phi_\Gamma([Q]) = [[\omega_Q, 1]] \quad \text{for some } Q \in \mathcal{Q}_N(d_K)/\sim_\Gamma.$$

Note that C contains an integral ideal $\mathfrak{a} = a^{\varphi(N)}[\omega_Q, 1]$, where φ is the Euler totient function. We establish by Lemma 2.2 and definition (1) that

$$\mathfrak{a}^{-1} = \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{a})}\bar{\mathfrak{a}} = \frac{1}{a^{\varphi(N)-1}}[-\bar{\omega}_Q, 1]$$

and

$$\begin{bmatrix} \tau_K \\ 1 \end{bmatrix} = \begin{bmatrix} a^{\varphi(N)} & -a^{\varphi(N)-1}(b + b_K)/2 \\ 0 & a^{\varphi(N)-1} \end{bmatrix} \begin{bmatrix} -\bar{\omega}_Q/a^{\varphi(N)-1} \\ 1/a^{\varphi(N)-1} \end{bmatrix},$$

where $\min(\tau_K, \mathbb{Q}) = x^2 + b_K x + c_K \ (\in \mathbb{Z}[x])$. We then derive by Proposition 3.3 that if $h \in \mathcal{F}_{\Gamma,\mathbb{Q}}$ is finite at τ_K, then

$$\begin{aligned} h(C) &= h(\tau)^{\widetilde{\begin{bmatrix} a^{\varphi(N)} & -a^{\varphi(N)-1}(b+b_K)/2 \\ 0 & a^{\varphi(N)-1} \end{bmatrix}}}|_{\tau=-\bar{\omega}_Q} \quad \text{by Definition 4.3} \\ &\qquad \text{where } \widetilde{\ } \text{ means the reduction onto } \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \\ &= h(\tau)^{\widetilde{\begin{bmatrix} 1 & -a^{-1}(b+b_K)/2 \\ 0 & a^{-1} \end{bmatrix}}}|_{\tau=-\bar{\omega}_Q} \quad \text{since } a^{\varphi(N)} \equiv 1 \pmod N \\ &\qquad \text{where } a^{-1} \text{ is an integer such that } aa^{-1} \equiv 1 \pmod N \\ &= h(\tau)^{\widetilde{\begin{bmatrix} 1 & 0 \\ 0 & a^{-1} \end{bmatrix}\begin{bmatrix} 1 & -a^{-1}(b+b_K)/2 \\ 0 & 1 \end{bmatrix}}}|_{\tau=-\bar{\omega}_Q} \\ &= h(\tau)^{\widetilde{\begin{bmatrix} 1 & -a^{-1}(b+b_K)/2 \\ 0 & 1 \end{bmatrix}}}|_{\tau=-\bar{\omega}_Q} \quad \text{because } h(\tau) \text{ has rational Fourier coefficients} \\ &= h(\tau)|_{\tau=-\bar{\omega}_Q} \quad \text{since } h(\tau) \text{ is modular for } \Gamma \\ &= h(-\bar{\omega}_Q). \end{aligned}$$

Now, the isomorphism ϕ_Γ followed by the isomorphism

$$\begin{aligned}\mathrm{Cl}(P) &\to \mathrm{Gal}(K_P/K)\\ C &\mapsto (h(\tau_K) = h(C_0) \mapsto h(C_0)^{\sigma(C)} = h(C) = h(-\bar{\omega}_Q) \mid h \in \mathcal{F}_{\Gamma,\mathbb{Q}} \text{ is finite at } \tau_K),\end{aligned}$$

which is induced from Propositions 4.2, 4.6 and Remark 4.5, yields the isomorphism stated in (51), as desired. □

Remark 5.5. In [10] Eum, Koo and Shin considered only the case where $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, $P = P_{K,1}(\mathfrak{n})$ and $\Gamma = \Gamma_1(N)$. As for the group operation of $\mathcal{Q}_N(d_K)/\sim_{\Gamma_1(N)}$ one can refer to [10, Remark 2.10]. They established an isomorphism

$$\begin{aligned}\mathcal{Q}_N(d_K)/\sim_{\Gamma_1(N)} &\to \mathrm{Gal}(K_{\mathfrak{n}}/K)\\ [Q] = [ax^2+bxy+cy^2] &\mapsto \left(h(\tau_K) \mapsto h(\tau)^{\left[\begin{smallmatrix} a & (b-b_K)/2 \\ 0 & 1\end{smallmatrix}\right]}|_{\tau=\omega_Q} \mid h(\tau) \in \mathcal{F}_N \text{ is finite at } \tau_K\right).\end{aligned} \tag{52}$$

The difference between the isomorphisms described in (51) and (52) arises from Definition 4.3 of $h(C)$. The invariant $h_{\mathfrak{n}}(C)$ appeared in [10, Definition 3.3] coincides with $h(C^{-1})$.

6 Finding representatives of extended form classes

In this last section, by improving the proof of Proposition 2.3 further, we shall explain how to find all quadratic forms which represent distinct classes in $\mathcal{Q}_N(d_K)/\sim_\Gamma$.

For a given $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$ we define an equivalence relation $\equiv_Q$ on $M_{1,2}(\mathbb{Z})$ as follows: Let $[r\ \ s], [u\ \ v] \in M_{1,2}(\mathbb{Z})$. Then, $[r\ \ s] \equiv_Q [u\ \ v]$ if and only if

$$[r\ \ s] \equiv \pm t[u\ \ v]\gamma \pmod{NM_{1,2}(\mathbb{Z})} \quad \text{for some } t \in T \text{ and } \gamma \in \Gamma_Q,$$

where

$$\Gamma_Q = \begin{cases} \{\pm I_2\} & \text{if } d_K \neq -4, -3,\\ \left\{\pm I_2, \pm\begin{bmatrix} -b/2 & -a^{-1}(b^2+4)/4) \\ a & b/2\end{bmatrix}\right\} & \text{if } d_K = -4,\\ \left\{\pm I_2, \pm\begin{bmatrix} -(b+1)/2 & -a^{-1}(b^2+3)/4 \\ a & (b-1)/2\end{bmatrix}, \pm\begin{bmatrix} (b-1)/2 & a^{-1}(b^2+3)/4 \\ -a & -(b+1)/2\end{bmatrix}\right\} & \text{if } d_K = -3.\end{cases}$$

Here, a^{-1} is an integer satisfying $aa^{-1} \equiv 1 \pmod N$.

Lemma 6.1. *Let $Q = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$ and $[r\ \ s], [u\ \ v] \in M_{1,2}(\mathbb{Z})$ such that* $\gcd(N, Q(s,-r)) = \gcd(N, Q(v,-u)) = 1$. *Then,*

$$[(r\omega_Q + s)\mathcal{O}_K] = [(u\omega_Q + v)\mathcal{O}_K] \quad \text{in } P_K(\mathfrak{n})/P \Leftrightarrow [r\ \ s] \equiv_Q [u\ \ v].$$

Proof. Note that by Lemma 2.2(i) the fractional ideals $(r\omega_Q + s)\mathcal{O}_K$ and $(u\omega_Q + v)\mathcal{O}_K$ belong to $P_K(\mathfrak{n})$. Furthermore, we know that

$$\mathcal{O}_K^* = \begin{cases} \{\pm 1\} & \text{if } K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}),\\ \{\pm 1, \pm\tau_K\} & \text{if } K = \mathbb{Q}(\sqrt{-1}),\\ \{\pm 1, \pm\tau_K, \pm\tau_K^2\} & \text{if } K = \mathbb{Q}(\sqrt{-3})\end{cases} \tag{53}$$

([3, Exercise 5.9]) and so

$$U_K = \{(m, n) \in \mathbb{Z}^2 \mid m\tau_K + n \in O_K^*\} = \begin{cases} \{\pm(0,1)\} & \text{if } K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}), \\ \{\pm(0,1), \pm(1,0)\} & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ \{\pm(0,1), \pm(1,0), \pm(1,1)\} & \text{if } K = \mathbb{Q}(\sqrt{-3}). \end{cases} \tag{54}$$

Then we achieve that

$$\begin{aligned}
&[(r\omega_Q + s)O_K] = [(u\omega_Q + v)O_K] \quad \text{in } P_K(\mathfrak{n})/P \\
&\Leftrightarrow \left(\frac{r\omega_Q + s}{u\omega_Q + v}\right)O_K \in P \\
&\Leftrightarrow \frac{r\omega_Q + s}{u\omega_Q + v} \equiv^* \zeta t \ (\mathrm{mod}\ \mathfrak{n}) \quad \text{for some } \zeta \in O_K^* \text{ and } t \in T \\
&\Leftrightarrow a(r\omega_Q + s) \equiv \zeta t a(u\omega_Q + v)(\mathrm{mod}\ \mathfrak{n}) \quad \text{since } a(uw_Q + v)O_K \text{ is relatively prime to } \mathfrak{n} \text{ and } a\omega_Q \in O_K \\
&\Leftrightarrow r\left(\tau_K + \frac{b_K - b}{2}\right) + as \equiv (m\tau_K + n)t\left\{u\left(\tau_K + \frac{b_K - b}{2}\right) + av\right\}(\mathrm{mod}\ \mathfrak{n}) \quad \text{for some } (m,n) \in U_K \\
&\Leftrightarrow r\tau_K + \left(\frac{r(b_K - b)}{2} + as\right) \equiv t(-mub_K + mk + nu)\tau_K + t(-muc_K + nk)(\mathrm{mod}\ \mathfrak{n}) \\
&\qquad\qquad \text{with } k = \frac{u(b_K - b)}{2} + av, \ \text{where } \min(\tau_K, \mathbb{Q}) = x^2 + b_K x + c_K \\
&\Leftrightarrow r \equiv t\left\{-\left(\frac{b_K + b}{2}\right)m + n\right\}u + tmav \ (\mathrm{mod}\ N) \quad \text{and} \\
&\qquad s \equiv ta^{-1}\left(\frac{b_K^2 - b^2}{4} - c_K\right)mu + t\left\{-\left(\frac{b_K - b}{2}\right)m + n\right\}v \ (\mathrm{mod}\ N) \quad \text{by the fact } \mathfrak{n} = N[\tau_K, 1] \\
&\Leftrightarrow [r \ \ s] \equiv_Q [u \ \ v] \quad \text{by (54) and the definition of } \equiv_Q .
\end{aligned}$$

□

For each $Q \in \mathcal{Q}_N(d_K)$, let

$$M_Q = \{[u \ \ v] \in M_{1,2}(\mathbb{Z}) \mid \gcd(N, Q(v, -u)) = 1\}.$$

Proposition 6.2. *One can explicitly find quadratic forms representing all distinct classes in $\mathcal{Q}_N(d_K)/\sim_\Gamma$.*

Proof. We adopt the idea in the proof of Proposition 2.3. Let $Q_1', Q_2', \ldots, Q_h'$ be quadratic forms in $\mathcal{Q}_N(d_K)$ which represent all distinct classes in $C(d_K) = \mathcal{Q}(d_K)/\sim$. Then we get by Lemma 6.1 that for each $i = 1, 2, \ldots, h$

$$P_K(\mathfrak{n})/P = \left\{[(u\omega_{Q_i'} + v)O_K] \mid [u \ \ v] \in M_{Q_i'}/\equiv_{Q_i'}\right\} = \left\{\left[\frac{1}{u\omega_{Q_i'} + v}O_K\right] \mid [u \ \ v] \in M_{Q_i'}/\equiv_{Q_i'}\right\}.$$

Thus, we obtain by (12) that

$$\begin{aligned}
I_K(\mathfrak{n})/P &= (P_K(\mathfrak{n})/P)\cdot\{[[\omega_{Q_i'}, 1]] \in I_K(\mathfrak{n})/P \mid i = 1, 2, \ldots, h\} \\
&= \left\{\left[\frac{1}{u\omega_{Q_i'} + v}[\omega_{Q_i'}, 1]\right] \ \mid i = 1, 2, \ldots, h \ \text{ and } \ [u \ \ v] \in M_{Q_i'}/\equiv_{Q_i'}\right\} \\
&= \left\{\left[\left[\begin{bmatrix} * & * \\ \tilde{u} & \tilde{v} \end{bmatrix}(\omega_{Q_i'}), 1\right]\right] \ \mid i = 1, 2, \ldots, h \ \text{ and } \ [u \ \ v] \in M_{Q_i'}/\equiv_{Q_i'}\right\},
\end{aligned}$$

where $\begin{bmatrix} * & * \\ \tilde{u} & \tilde{v} \end{bmatrix}$ is a matrix in $\mathrm{SL}_2(\mathbb{Z})$ such that $\begin{bmatrix} * & * \\ \tilde{u} & \tilde{v} \end{bmatrix} \equiv \begin{bmatrix} * & * \\ u & v \end{bmatrix}(\mathrm{mod}\ NM_2(\mathbb{Z}))$. Therefore, we conclude

$$\mathcal{Q}_N(d_K)/\sim_\Gamma = \left\{\left[Q_i'^{\begin{bmatrix} * & * \\ \tilde{u} & \tilde{v} \end{bmatrix}^{-1}}\right] \mid \ \ i = 1, 2, \ldots, h \ \text{ and } \ [u \ \ v] \in M_{Q_i'}/\equiv_{Q_i'}\right\}.$$

□

Example 6.3. Let $K = \mathbb{Q}(\sqrt{-5})$, $N = 12$ and $T = (\mathbb{Z}/N\mathbb{Z})^*$. Then we get $P = P_{K,\mathbb{Z}}(\mathfrak{n})$ and $K_P = H_O$, where $\mathfrak{n} = NO_K$ and O is the order of conductor N in K. There are two reduced forms of discriminant $d_K = -20$, namely,

$$Q_1 = x^2 + 5y^2 \quad \text{and} \quad Q_2 = 2x^2 + 2xy + 3y^2.$$

Set

$$Q_1' = Q_1 \quad \text{and} \quad Q_2' = Q_2^{\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}} = 7x^2 + 22xy + 18y^2,$$

which belong to $\mathcal{Q}_N(d_K)$. We then see that

$$M_{Q_1'}/{\equiv_{Q_1'}} = \{[0\ \ 1], [1\ \ 0], [1\ \ 6], [2\ \ 3], [3\ \ 2], [3\ \ 4], [4\ \ 3], [6\ \ 1]\}$$

with the corresponding matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 6 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 4 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 6 & 1 \end{bmatrix}$$

and

$$M_{Q_2'}/{\equiv_{Q_2'}} = \{[0\ \ 1], [1\ \ 5], [1\ \ 11], [2\ \ 1], [3\ \ 1], [3\ \ 7], [4\ \ 5], [6\ \ 1]\}$$

with the corresponding matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 5 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 11 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 4 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 6 & 1 \end{bmatrix}.$$

Hence, there are 16 quadratic forms

$$\begin{array}{llll} x^2 + 5y^2, & 5x^2 + y^2, & 41x^2 + 12xy + y^2, & 29x^2 - 26xy + 6y^2, \\ 49x^2 + 34xy + 6y^2, & 61x^2 - 38xy + 6y^2, & 89x^2 + 46xy + 6y^2, & 181x^2 - 60xy + 5y^2, \\ 7x^2 + 22xy + 18y^2, & 83x^2 + 48xy + 7y^2, & 623x^2 + 132xy + 7y^2, & 35x^2 + 20xy + 3y^2, \\ 103x^2 - 86xy + 18y^2, & 43x^2 - 18xy + 2y^2, & 23x^2 - 16xy + 3y^2, & 523x^2 - 194xy + 18y^2, \end{array}$$

which represent all distinct classes in $\mathcal{Q}_N(d_K)/\sim_\Gamma = \mathcal{Q}_{12}(-20)/\sim_{\Gamma_0(12)}$.

On the other hand, for $[r_1\ \ r_2] \in M_{1,2}(\mathbb{Q}) \setminus M_{1,2}(\mathbb{Z})$ the *Siegel function* $g_{[r_1\ \ r_2]}(\tau)$ is given by the infinite product

$$g_{[r_1\ \ r_2]}(\tau) \;=\; -e^{\pi i r_2(r_1-1)} q^{(1/2)(r_1^2-r_1+1/6)}(1 - q^{r_1}e^{2\pi i r_2}) \prod_{n=1}^{\infty} (1 - q^{n+r_1}e^{2\pi i r_2})(1 - q^{n-r_1}e^{-2\pi i r_2}) \quad (\tau \in \mathbb{H}),$$

which generalizes the Dedekind eta-function $q^{1/24} \prod_{n=1}^{\infty}(1 - q^n)$. Then the function

$$g_{[1/2\ \ 0]}(12\tau)^{12} = \left(\frac{\eta(6\tau)}{\eta(12\tau)}\right)^{24}$$

belongs to $\mathcal{F}_{\Gamma_0(12),\mathbb{Q}}$ ([14, Theorem 1.64] or [16]), and the Galois conjugates of $g_{[1/2\ \ 0]}(12\tau_K)^{12}$ over K are

$$\begin{array}{ll} g_1 = g_{[1/2\ \ 0]}(12\sqrt{-5})^{12}, & g_2 = g_{[1/2\ \ 0]}(12\sqrt{-5}/5)^{12}, \\ g_3 = g_{[1/2\ \ 0]}(12(6 + \sqrt{-5})/41)^{12}, & g_4 = g_{[1/2\ \ 0]}(12(-13 + \sqrt{-5})/29)^{12}, \\ g_5 = g_{[1/2\ \ 0]}(12(17 + \sqrt{-5})/49)^{12}, & g_6 = g_{[1/2\ \ 0]}(12(-19 + \sqrt{-5})/61)^{12}, \\ g_7 = g_{[1/2\ \ 0]}(12(23 + \sqrt{-5})/89)^{12}, & g_8 = g_{[1/2\ \ 0]}(12(-30 + \sqrt{-5})/181)^{12}, \\ g_9 = g_{[1/2\ \ 0]}(12(11 + \sqrt{-5})/7)^{12}, & g_{10} = g_{[1/2\ \ 0]}(12(24 + \sqrt{-5})/83)^{12}, \\ g_{11} = g_{[1/2\ \ 0]}(12(66 + \sqrt{-5})/623)^{12}, & g_{12} = g_{[1/2\ \ 0]}(12(10 + \sqrt{-5})/35)^{12}, \\ g_{13} = g_{[1/2\ \ 0]}(12(-43 + \sqrt{-5})/103)^{12}, & g_{14} = g_{[1/2\ \ 0]}(12(-9 + \sqrt{-5})/43)^{12}, \\ g_{15} = g_{[1/2\ \ 0]}(12(-8 + \sqrt{-5})/23)^{12}, & g_{16} = g_{[1/2\ \ 0]}(12(-97 + \sqrt{-5})/523)^{12} \end{array}$$

possibly with some multiplicity. Now, we evaluate

$$\prod_{i=1}^{16}(x-g_i)=x^{16}+1251968x^{15}-14929949056x^{14}+1684515904384x^{13}-61912544374756x^{12}$$
$$+362333829428160x^{11}+32778846351721632x^{10}-845856631699319872x^{9}$$
$$+4605865492693542918x^{8}+9116425906728562124 8x^{7}-12491793529169969452 8x^{6}$$
$$+1809202855641312806 40x^{5}-300029514405771491 6x^{4}+8871452719720384x^{3}$$
$$+458008762175904x^{2}-1597177179712x+1$$

with nonzero discriminant. Thus, $g_{[1/2\ \ 0]}(12\tau_K)^{12}$ generates $K_P=H_O$ over K.

Remark 6.4. In [17], Schertz deals with various constructive problems on the theory of complex multiplication in terms of the Dedekind eta-function and Siegel function. See also [16] and [18].

Acknowledgment: Ho Yun Jung was supported by the research fund of Dankook University in 2020 and by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1F1A1A01073055). Dong Hwa Shin was supported by the Hankuk University of Foreign Studies Research Fund of 2020 and by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1F1A1A01048633).

References

[1] Carl Friedrich Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801.

[2] Peter Gustav Lejeune Dirichlet, *Zahlentheorie*, 4th edn, Vieweg, Braunschweig, 1894.

[3] David Archibald 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.

[4] Manjul Bhargava, *Higher composition laws I: A new view on Gauss composition, and quadratic generalizations*, Ann. of Math. (2) **159** (2004), no. 1, 217–250.

[5] Serge Lang, *Elliptic Functions*, With an appendix by J. Tate, 2nd edn, Grad. Texts in Math. 112, Springer-Verlag, New York, 1987.

[6] Gerald J. Janusz, *Algebraic Number Fields*, 2nd edn, Grad. Studies in Math. 7, Amer. Math. Soc., Providence, R. I., 1996.

[7] Goro Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, Princeton, NJ, 1971.

[8] Bumkyu Cho and Ja Kyung Koo, *Construction of class fields over imaginary quadratic fields and applications*, Q. J. Math. **61** (2010), no. 2, 199–216.

[9] Ja Kyung Koo and Dong Hwa Shin, *Singular values of principal moduli*, J. Number Theory **133** (2013), no. 2, 475–483.

[10] Ick Sun Eum, Ja Kyung Koo and Dong Hwa Shin, *Binary quadratic forms and ray class groups*, Proc. Roy. Soc. Edinburgh Sect. A **150** (2020), no. 2, 695–720.

[11] Joseph Hillel Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer-Verlag, New York, 1994.

[12] Jürgen Neukirch, *Class Field Theory*, Grundlehren der Mathematischen Wissenschaften 280, Springer-Verlag, Berlin, 1986.

[13] Jean-Pierre Serre, *Local Fields*, Springer-Verlag, New York, 1979.

[14] Ken Ono, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, CBMS Regional Conference Series in Mathematics 102, AMS/CBMS, Providence, RI, 2004.

[15] Serge Lang, *Algebraic Number Theory*, 2nd edn, Grad. Texts in Math. 110, Springer-Verlag, New York, 1994.

[16] Daniel Kubert and Serge Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Springer-Verlag, New York-Berlin, 1981.

[17] Reinhard Schertz, *Complex Multiplication*, New Mathematical Monographs 15, Cambridge University Press, Cambridge, 2010.

[18] Kanakanahalli Ramachandra, *Some applications of Kronecker's limit formula*, Ann. of Math. (2) **80** (1964), no. 1, 104–148.