Proceedings of the Royal Society of Edinburgh, **150**, 695–720, *2020*
DOI:10.1017/prm.2018.163

Binary quadratic forms and ray class groups

Ick Sun Eum
Department of Mathematics Education, Dongguk University-Gyeongju, Gyeongju-si, Gyeongsangbuk-do 38066, Republic of Korea
(zandc@dongguk.ac.kr)

Ja Kyung Koo
Department of Mathematical Sciences, KAIST Daejeon 34141, Republic of Korea
(jkkoo@math.kaist.ac.kr)

Dong Hwa Shin
Department of Mathematics, Hankuk University of Foreign Studies, Yongin-si, Gyeonggi-do 17035, Republic of Korea
(dhshin@hufs.ac.kr)

(MS received 10 March 2018; accepted 8 October 2018)

Let K be an imaginary quadratic field different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. For a positive integer N, let K_N be the ray class field of K modulo $N\mathcal{O}_K$. By using the congruence subgroup $\pm\Gamma_1(N)$ of $\mathrm{SL}_2(\mathbb{Z})$, we construct an extended form class group whose operation is basically the Dirichlet composition, and explicitly show that this group is isomorphic to the Galois group $\mathrm{Gal}(K_N/K)$. We also present an algorithm to find all distinct form classes and show how to multiply two form classes. As an application, we describe $\mathrm{Gal}(K_N^{\mathrm{ab}}/K)$ in terms of these extended form class groups for which K_N^{ab} is the maximal abelian extension of K unramified outside prime ideals dividing $N\mathcal{O}_K$.

Keywords: Binary quadratic forms; class field theory; class groups; complex multiplication

2010 *Mathematics subject classification:* Primary 11R29
Secondary 11E16; 11G15; 11R37

1. Introduction

Let K be an imaginary quadratic field of discriminant d_K with ring of integers $\mathcal{O}_K$. Let $\mathcal{Q}(d_K)$ 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 $b^2 - 4ac = d_K$. Define an equivalence relation on $\mathcal{Q}(d_K)$, called the *proper equivalence*, by

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

Then, the set $\mathrm{C}(d_K) = \mathcal{Q}(d_K)/\sim$ of equivalence classes under Dirichlet composition becomes a group, called the *form class group* of discriminant d_K [**1**, theorem 3.9].

Let I_K be the group of fractional ideals of K and P_K be its subgroup of principal fractional ideals. It is a classical fact that the form class group $\mathrm{C}(d_K)$ is isomorphic to the ideal class group $\mathrm{C}_K = I_K/P_K$ as follows: For each $Q \in \mathcal{Q}(d_K)$, let ω_Q be the zero of $Q(x, 1)$ in the complex upper half-plane $\mathbb{H}$.

THEOREM 1.1. *We have an isomorphism of groups*

$$\phi \ : \ \mathrm{C}(d_K) \to \mathrm{C}_K$$
$$\textit{form class containing } Q = ax^2 + bxy + cy^2 \mapsto \textit{ideal class containing } a[\omega_Q,\, 1].$$

Proof. See [**1**, theorem 7.7]. □

REMARK 1.2. Note that $[a\omega_Q,\, 1] = [(-b + \sqrt{d_K})/2,\, 1] = \mathcal{O}_K$. In theorem 1.1, one can replace the integral ideal $a[\omega_Q,\, 1]$ by the fractional ideal $[\omega_Q,\, 1]$.

On the other hand, let H_K be the Hilbert class field of K whose Galois group is isomorphic to C_K [**1**, theorem 8.10] or [**4**, theorem 9.9 in Chapter V]. The following theorem is a consequence of the theory of complex multiplication and theorem 1.1.

THEOREM 1.3. *We have an isomorphism of groups*

$$\mathrm{C}(d_K) \to \mathrm{Gal}(H_K/K)$$
$$\textit{form class containing } Q \mapsto \left(j(\tau_K) \mapsto j(\omega_Q)\right),$$

where $j(\tau)$ is the elliptic modular function and τ_K is an element of $\mathbb{H}$ such that $\mathcal{O}_K = [\tau_K,\, 1]$.

Proof. See [**2**, **3**] or [**8**, theorem 1 in Chapter 10]. □

Now, for a finite abelian extension L of K such that $L \supseteq H_K$, it is natural to ask whether there is some form class group that is isomorphic to $\mathrm{Gal}(L/K)$. Since $\mathrm{Gal}(H_K/K)$ $(\simeq \mathrm{C}(d_K))$ is a quotient group of $\mathrm{Gal}(L/K)$, if we loosen the proper equivalence on $\mathrm{C}(d_K)$ induced from $\mathrm{SL}_2(\mathbb{Z})$, then we would expect to get a certain new form class group isomorphic to $\mathrm{Gal}(L/K)$. Here we note that L is contained in some ray class field K_N modulo $N\mathcal{O}_K$ for a positive integer N [**1**, p. 149].

PROPOSITION 1.4. *Let $\mathcal{F}_N$ be the field of meromorphic modular functions of level N whose Fourier coefficients lie in the Nth cyclotomic field. Then we have*

$$K_N = K(h(\tau_K)\,|\,h(\tau) \in \mathcal{F}_N \textit{ is finite at } \tau_K).$$

Proof. See [**8**, corollary to theorem 2 in Chapter 10]. □

In this paper, we shall first construct a newly extended form class group $\mathrm{C}_N(d_K)$ isomorphic to the ray class group $\mathrm{Cl}(N)$ modulo $N\mathcal{O}_K$, through the equivalence relation induced from $\pm\Gamma_1(N)$ (theorem 2.9). It turns out that the binary operation on $\mathrm{C}_N(d_K)$ is essentially the Dirichlet composition on $\mathrm{C}(d_K)$ (remark 2.10 (iv)).

In view of theorem 1.3 and proposition 1.4 we shall further establish an isomorphism

$$\begin{aligned} \mathrm{C}_N(d_K) &\to \mathrm{Gal}(K_N/K) \\ \begin{array}{l}\text{form class containing}\\ Q = ax^2+bxy+cy^2\end{array} &\mapsto \left(h(\tau_K) \mapsto h_{\left[\begin{smallmatrix} a & (b-b_K)/2 \\ 0 & 1 \end{smallmatrix}\right]}(\omega_Q) \,|\, h(\tau) \in \mathcal{F}_N \text{ is finite at } \tau_K \right), \end{aligned}$$

where $\min(\tau_K, \mathbb{Q}) = x^2 + b_K x + c_K \in \mathbb{Z}[x]$ (theorem 3.10). This indicates that a form class $[ax^2+bxy+cy^2]$ in $\mathrm{C}_N(d_K)$ has perfect information on an element of $\mathrm{Gal}(K_N/K)$. Of course, we shall present an algorithm in order to list all representatives of form classes in $\mathrm{C}_N(d_K)$ (theorem 4.4) and give some examples.

Let K_N^{ab} be the maximal abelian extension of K unramified outside prime ideals dividing $N\mathcal{O}_K$. As an application, we shall construct a dense subset of $\mathrm{Gal}(K_N^{\mathrm{ab}}/K)$, equipped with Krull topology, in terms of extended form class groups (theorem 6.4).

2. Extended form class groups as ray class groups

Throughout this paper, let K be an imaginary quadratic field of discriminant d_K other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. For a positive integer N, let $\mathcal{Q}_N(d_K)$ be the set of primitive positive definite binary quadratic forms $Q(x, y) = ax^2+bxy+cy^2$ of discriminant d_K such that $\gcd(N, a) = 1$, that is,

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

By $\pm\Gamma_1(N)$ we mean the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ given by

$$\pm\Gamma_1(N) = \left\{ \sigma \in \mathrm{SL}_2(\mathbb{Z}) \,|\, \sigma \equiv \pm \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} \pmod{N} \quad \text{for some } s \in \mathbb{Z} \right\}.$$

PROPOSITION 2.1. *The group $\pm\Gamma_1(N)$ acts on the set $\mathcal{Q}_N(d_K)$ on the right by*

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

Proof. Since $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{Q}(d_K)$, it suffices to show that $\pm\Gamma_1(N)$ preserves the set $\mathcal{Q}_N(d_K)$. Let $Q(x, y) = ax^2+bxy+cy^2 \in \mathcal{Q}_N(d_K)$ and $\sigma \in \pm\Gamma_1(N)$. We then see that

$$\begin{aligned} Q\left(\sigma \begin{bmatrix} x \\ y \end{bmatrix}\right) &\equiv Q\left(\pm \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}\right) \pmod{N\mathbb{Z}[x, y]} \quad \text{for some } s \in \mathbb{Z} \\ &\equiv ax^2 + (2as+b)xy + (as^2+bs+c)y^2 \pmod{N\mathbb{Z}[x, y]}. \end{aligned}$$

This shows that $Q(\sigma \begin{bmatrix} x \\ y \end{bmatrix})$ belongs to $\mathcal{Q}_N(d_K)$, as desired. □

https://doi.org/10.1017/prm.2018.163 Published online by Cambridge University Press

Definition 2.2. *Define an equivalence relation $\sim_N$ on the set $\mathcal{Q}_N(d_K)$ by*

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

Denote by $\mathrm{C}_N(d_K)$ the set of equivalence classes, namely,

$$\mathrm{C}_N(d_K) = \mathcal{Q}_N(d_K)/\sim_N .$$

Now, we are in need of the following basic lemma for later use.

Lemma 2.3. *Let $Q(x, y) = ax^2 + bxy + cy^2 \in \mathcal{Q}(d_K)$ and $\sigma = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.*

(i) *If $\omega \in \mathbb{H}$, then*

$$[\sigma(\omega), 1] = \frac{1}{\mathcal{J}(\sigma, \omega)}[\omega, 1] \quad \text{where } \mathcal{J}(\sigma, \omega) = u\omega + v.$$

(ii) *Let $Q' \in \mathcal{Q}(d_K)$ such that $Q'\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = Q\left(\sigma \begin{bmatrix} x \\ y \end{bmatrix}\right)$. Then we have*

$$\omega_Q = \sigma(\omega_{Q'}).$$

(iii) *We have*

$$\mathcal{N}_{K/\mathbb{Q}}([\omega_Q, 1]) = \frac{1}{a},$$

where $\mathcal{N}_{K/\mathbb{Q}}(\cdot)$ is applied to fractional ideals of K.

Proof.

(i) It follows from the fact $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ that

$$[\sigma(\omega), 1] = \left[\frac{r\omega + s}{u\omega + v}, 1\right] = \frac{1}{u\omega + v}[r\omega + s, u\omega + v] = \frac{1}{\mathcal{J}(\sigma, \omega)}[\omega, 1].$$

(ii)

$$Q\left(\begin{bmatrix} \omega_Q \\ 1 \end{bmatrix}\right) = 0 = Q'\left(\begin{bmatrix} \omega_{Q'} \\ 1 \end{bmatrix}\right) = Q\left(\sigma \begin{bmatrix} \omega_{Q'} \\ 1 \end{bmatrix}\right) = \mathcal{J}(\sigma, \omega_{Q'})^2 Q\left(\begin{bmatrix} \sigma(\omega_{Q'}) \\ 1 \end{bmatrix}\right).$$

Since $\omega_Q, \omega_{Q'} \in \mathbb{H}$, we conclude $\omega_Q = \sigma(\omega_{Q'})$.

(iii)

$$\mathrm{disc}_{K/\mathbb{Q}}([\omega_Q, 1]) = \begin{vmatrix} (-b + \sqrt{d_K})/2a & 1 \\ (-b - \sqrt{d_K})/2a & 1 \end{vmatrix}^2 = \frac{d_K}{a^2}.$$

On the other hand, since

$$\mathrm{disc}_{K/\mathbb{Q}}([\omega_Q, 1]) = \mathcal{N}_{K/\mathbb{Q}}([\omega_Q, 1])^2 d_K$$

[9, proposition 13 in Chapter III], we achieve

$$\mathcal{N}_{K/\mathbb{Q}}([\omega_Q, 1]) = \frac{1}{a}. \qquad \square$$

Let $\mathrm{Cl}(N)$ be the ray class group modulo $N\mathcal{O}_K$, namely,

$$\mathrm{Cl}(N) = I_K(N)/P_{K,\,1}(N)$$

where $I_K(N)$ is the subgroup of I_K consisting of fractional ideals of K prime to $N\mathcal{O}_K$ and $P_{K,\,1}(N)$ is its subgroup consisting of principal fractional ideals $\lambda\mathcal{O}_K$ with $\lambda \in K^*$ such that $\lambda \equiv^* 1 \pmod{N\mathcal{O}_K}$ [4, pp. 136–137].

Definition 2.4. *Define a map*

$$\begin{aligned}\phi_N \;:\; \mathrm{C}_N(d_K) &\to \mathrm{Cl}(N)\\ [Q] &\mapsto \textit{ray class containing } [\omega_Q,\, 1].\end{aligned}$$

Here, $[Q]$ stands for the form class containing $Q \in \mathcal{Q}_N(d_K)$.

Remark 2.5. By remark 1.2, we see that $\phi_1 = \phi$, the classical isomorphism described in theorem 1.1.

Proposition 2.6. *The map ϕ_N is well defined.*

Proof. First, we shall show that if $Q(x,\,y) = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$, then the fractional ideal $[\omega_Q,\,1]$ is prime to $N\mathcal{O}_K$. Observe that $a[\omega_Q,\,1] = [(-b+\sqrt{d_K})/2,\,a]$ is an integral ideal of K with

$$\mathcal{N}_{K/\mathbb{Q}}(a[\omega_Q,\,1]) = a$$

by lemma 2.3 (iii). This, together with the fact $\gcd(N,\,a) = 1$, implies that $[\omega_Q,\,1]$ is prime to $N\mathcal{O}_K$.

Second, we shall show that if $Q,\,Q' \in \mathcal{Q}_N(d_K)$ such that $[Q] = [Q']$, then $[\omega_Q,\,1]$ and $[\omega_{Q'},\,1]$ belong to the same ray class in $\mathrm{Cl}(N)$. Let

$$Q'\left(\begin{bmatrix}x\\ y\end{bmatrix}\right) = a'x^2 + b'xy + c'y^2 = Q\left(\sigma\begin{bmatrix}x\\ y\end{bmatrix}\right) \quad \text{for some } \sigma = \begin{bmatrix}r & s\\ u & v\end{bmatrix} \in \pm\Gamma_1(N).$$

We then derive by lemma 2.3 (i) and (ii) that

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

Since $\sigma \equiv \pm\begin{bmatrix}1 & s\\ 0 & 1\end{bmatrix} \pmod{N}$ for some $s \in \mathbb{Z}$ and $\gcd(N,\,a') = 1$, we obtain

$$u\omega_{Q'} + v \equiv^* u\frac{-b' + \sqrt{d_K}}{2a'} + v \equiv^* \pm 1 \pmod{N\mathcal{O}_K}.$$

This yields that $[\omega_Q,\,1]$ and $[\omega_{Q'},\,1]$ belong to the same ray class in $\mathrm{Cl}(N)$. □

Proposition 2.7. *The map ϕ_N is injective.*

Proof. Suppose that

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

and so

$$[\omega_Q,\, 1] = \lambda[\omega_{Q'},\, 1] \quad \text{for some } \lambda \in K^* \quad \text{such that } \lambda \equiv^* 1 \pmod{N\mathcal{O}_K}. \tag{2.1}$$

Then, we get by theorem 1.1 that

$$Q'\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = Q\left(\sigma \begin{bmatrix} x \\ y \end{bmatrix}\right) \quad \text{for some } \sigma = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

And, it follows from lemma 2.3 (i), (ii) and (2.1) that

$$[\omega_{Q'},\, 1] = \mathcal{J}(\sigma,\, \omega_{Q'})[\sigma(\omega_{Q'}),\, 1] = (u\omega_{Q'} + v)[\omega_Q,\, 1] = \lambda(u\omega_{Q'} + v)[\omega_{Q'},\, 1],$$

and hence

$$\lambda(u\omega_{Q'} + v) \in \mathcal{O}_K^* = \{1, -1\}.$$

Since $\lambda \equiv^* 1 \pmod{N\mathcal{O}_K}$, we deduce

$$u\omega_{Q'} + v \equiv^* \pm 1 \pmod{N\mathcal{O}_K}. \tag{2.2}$$

If we let $Q'(x,\, y) = a'x^2 + b'xy + c'y^2$, then we have $\mathcal{O}_K = [(-b' + \sqrt{d_K})/2,\, 1]$ and

$$u\omega_{Q'} + v \pm 1 = \frac{1}{a'}\left(u\frac{-b' + \sqrt{d_K}}{2} + a'(v \pm 1)\right).$$

Thus, it follows from the fact $\gcd(N,\, a') = 1$ and (2.2) that

$$u \equiv 0 \pmod N \quad \text{and} \quad v \equiv \pm 1 \pmod N.$$

Moreover, since $\det(\sigma) = 1$, we obtain $\sigma \in \pm\Gamma_1(N)$. Therefore, Q and Q' belong to the same class in $\mathrm{C}_N(d_K)$, namely, $[Q] = [Q']$. This proves the proposition. □

PROPOSITION 2.8. *The map ϕ_N is surjective.*

Proof. Let $C \in \mathrm{Cl}(N)$. Take an integral ideal $\mathfrak{a}$ in C^{-1}, and let $\xi_1,\, \xi_2 \in K^*$ such that

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

Since $1 \in \mathfrak{a}^{-1}$, one can write

$$1 = u\xi_1 + v\xi_2 \quad \text{for some } u,\, v \in \mathbb{Z}. \tag{2.3}$$

We then claim $\gcd(N,\, u,\, v) = 1$. Otherwise, $d = \gcd(N,\, u,\, v) > 1$, and so $d\mathfrak{a}^{-1} = [d\xi_1,\, d\xi_2]$ contains 1 by (2.3), which implies $d\mathcal{O}_K \supseteq \mathfrak{a}$. But, this contradicts the fact that $\mathfrak{a}$ is prime to $N\mathcal{O}_K$. Thus we may take a matrix $\sigma = \begin{bmatrix} r & s \\ \widetilde{u} & \widetilde{v} \end{bmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$ such that

$$\widetilde{u} \equiv u \pmod{N} \quad \text{and} \quad \widetilde{v} \equiv v \pmod{N} \tag{2.4}$$

by the surjectivity of $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ [**13**, lemma 1.38]. If we set $\omega = \sigma(\xi)$, then we derive that

$$\begin{aligned}
[\omega,\, 1] &= [\sigma(\xi),\, 1] \\
&= \frac{1}{\widetilde{u}\xi + \widetilde{v}}[\xi,\, 1] \quad \text{by lemma 2.3 (i)} \\
&= \frac{\xi_2}{\widetilde{u}\xi_1 + \widetilde{v}\xi_2}[\xi_1/\xi_2,\, 1] \quad \text{by the fact } \xi = \xi_1/\xi_2 \\
&= \frac{1}{\widetilde{u}\xi_1 + \widetilde{v}\xi_2}[\xi_1,\, \xi_2] \\
&= \frac{1}{\widetilde{u}\xi_1 + \widetilde{v}\xi_2}\mathfrak{a}^{-1}.
\end{aligned}$$

Here, we note that

$$\begin{aligned}
\widetilde{u}\xi_1 + \widetilde{v}\xi_2 - 1 &= \widetilde{u}\xi_1 + \widetilde{v}\xi_2 - (u\xi_1 + v\xi_2) \quad \text{by (2.3)} \\
&= (\widetilde{u} - u)\xi_1 + (\widetilde{v} - v)\xi_2 \\
&\in N\mathfrak{a}^{-1} \quad \text{by (2.4)},
\end{aligned}$$

from which we see that

$$\widetilde{u}\xi_1 + \widetilde{v}\xi_2 \equiv^* 1 \pmod{N\mathcal{O}_K}.$$

Therefore, $[\omega,\, 1]$ and $\mathfrak{a}^{-1}$ belong to the same ray class C. Thus, if we let Q be the element of $\mathcal{Q}_N(d_K)$ satisfying $\omega_Q = \omega$, then we conclude

$$\phi_N([Q]) = C.$$

□

THEOREM 2.9. *The set* $\mathrm{C}_N(d_K)$ *can be regarded as an abelian group isomorphic to the ray class group* $\mathrm{Cl}(N)$.

Proof. Define a binary operation $\cdot$ on $\mathrm{C}_N(d_K)$ by

$$[Q] \cdot [Q'] = \phi_N^{-1}(\phi_N([Q])\phi_N([Q'])),$$

where $\phi_N([Q])\phi_N([Q'])$ is the product of ray classes in $\mathrm{Cl}(N)$. This binary operation makes $\mathrm{C}_N(d_K)$ an abelian group isomorphic to $\mathrm{Cl}(N)$. We shall describe the group operation on $\mathrm{C}_N(d_K)$ explicitly in the following remark 2.10 (iv). □

$$\begin{array}{ccc} \mathrm{C}_N(d_K) & \xrightarrow[\phi_N]{\sim} & \mathrm{Cl}(N) \\ {\scriptstyle \text{natural surjection}}\big\downarrow & & \big\downarrow{\scriptstyle \text{canonical homomorphism}} \\ \mathrm{C}_M(d_K) & \xrightarrow[\phi_M]{\sim} & \mathrm{Cl}(M) \end{array}$$

Figure 1. A commutative diagram of class groups

Remark 2.10.

(i) If M is a positive divisor of N, then we have by definition 2.4 a commutative diagram of homomorphisms (figure 1):

(ii) Let τ_K be the element of $\mathbb{H}$ induced by the principal form

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

Since $[\tau_K,\, 1] = \mathcal{O}_K$, the principal form gives rise to the identity element of $\mathrm{C}_N(d_K)$.

(iii) For a quadratic form $Q(x,\, y) = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$, we want to find its inverse $[Q]^{-1}$ in $\mathrm{C}_N(d_K)$. Let $\mathfrak{c} = a^{\varphi(N)}[\omega_Q,\, 1]$, where φ is the Euler function. Then, $\mathfrak{c}$ is an integral ideal of K which belongs to the same ray class as $[\omega_Q,\, 1]$ because $a^{\varphi(N)} \equiv 1 \pmod N$. Since $\mathfrak{c}\overline{\mathfrak{c}} = \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{c})\mathcal{O}_K$ and $\mathcal{N}_{K/\mathbb{Q}}([\omega_Q,\, 1]) = 1/a$ by lemma 2.3 (iii), we get

$$\mathfrak{c}^{-1} = \frac{1}{\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{c})}\overline{\mathfrak{c}} = \frac{1}{a^{\varphi(N)-1}}[-\overline{\omega}_Q,\, 1];$$

and hence we obtain

$$1 = \frac{1}{a^{\varphi(N)-1}}(0 \cdot (-\overline{\omega}_Q) + a^{\varphi(N)-1} \cdot 1).$$

Take an element $\sigma = \begin{bmatrix} r & s \\ \widetilde{u} & \widetilde{v} \end{bmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$ such that

$$\widetilde{u} \equiv 0 \pmod N \quad \text{and} \quad \widetilde{v} \equiv a^{\varphi(N)-1} \pmod N.$$

Now, if we let $Q' \in \mathcal{Q}_N(d_K)$ satisfying $\omega_{Q'} = \sigma(-\overline{\omega}_Q)$, then we achieve by the proof of proposition 2.8 that Q' and $\mathfrak{c}^{-1}$ give the same ray class. Therefore, $[Q']$ is the inverse of $[Q]$ in $\mathrm{C}_N(d_K)$.

(iv) Let $Q_1(x,y) = a_1x^2 + b_1xy + c_1y^2, Q_2(x,y) = a_2x^2 + b_2xy + c_2y^2 \in \mathcal{Q}_N(d_K)$. We will describe an algorithm how to find $[Q_1] \cdot [Q_2]$ explicitly. One may take a matrix ρ in $\mathrm{SL}_2(\mathbb{Z})$ so that $Q_3(x, y) = a_3x^2 + b_3xy + c_3y^2$ defined by

$$Q_3\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = Q_2\left(\rho \begin{bmatrix} x \\ y \end{bmatrix}\right) \tag{2.5}$$

satisfies $\gcd(a_1, a_3, (b_1 + b_3)/2) = 1$ [**1**, lemmas 2.3 and 2.25]. We then obtain

$$[\omega_{Q_1}, 1][\omega_{Q_3}, 1] = \left[\frac{-B + \sqrt{d_K}}{2a_1a_3}, 1\right], \tag{2.6}$$

where B is an integer for which

$$B \equiv b_1 \pmod{2a_1}, \quad B \equiv b_3 \pmod{2a_3} \quad \text{and} \quad B^2 \equiv d_K \pmod{4a_1a_3}$$

[**1**, lemma 3.2 and (7.13)]. (This ideal multiplication gives us the Dirichlet composition on $\mathrm{C}_1(d_K) = \mathrm{C}(d_K)$ by theorem 2.9.) On the other hand, we know by definition 2.4 that $\phi_N([Q_1])\phi_N([Q_2])$ is the ray class containing the fractional ideal

$$\mathfrak{c} = [\omega_{Q_1}, 1][\omega_{Q_2}, 1].$$

Thus, we get that

$$\begin{aligned} \mathfrak{c} &= [\omega_{Q_1}, 1][\rho(\omega_{Q_3}), 1] \quad \text{by (2.5) and lemma 2.3 (ii)} \\ &= \frac{1}{\mathcal{J}(\rho, \omega_{Q3})}[\omega_{Q_1}, 1][\omega_{Q_3}, 1] \quad \text{by lemma 2.3 (i)} \\ &= \frac{1}{\mathcal{J}(\rho, \omega_{Q_3})}\left[\frac{-B + \sqrt{d_K}}{2a_1a_3}, 1\right] \quad \text{by (2.6).} \end{aligned}$$

By the fact $\mathfrak{c}\bar{\mathfrak{c}} = \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{c})\mathcal{O}_K$ and lemma 2.3 (iii) we see that

$$\mathfrak{a} = \mathfrak{c}^{-1} = \frac{1}{\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{c})}\bar{\mathfrak{c}} = a_1a_2\bar{\mathfrak{c}} = [-a_1\overline{\omega}_{Q_1}, a_1][-a_2\overline{\omega}_{Q_2}, a_2]$$

is an integral ideal in the ray class $(\phi_N([Q_1])\phi([Q_2]))^{-1}$. Now, by using the argument in the proof of proposition 2.8 one can have $Q_4 \in \mathcal{Q}_N(d_K)$ so that $\phi_N([Q_4])$ is the ray class containing $\mathfrak{a}^{-1} = \mathfrak{c}$. Therefore, we achieve by theorem 2.9 that

$$[Q_4] = [Q_1] \cdot [Q_2].$$

3. Extended form class groups as Galois groups

Let K_N be the ray class field of K modulo $N\mathcal{O}_K$, that is, K_N is the unique abelian extension of K whose Galois group $\mathrm{Gal}(K_N/K)$ corresponds to $\mathrm{Cl}(N)$ via the Artin map for modulus $N\mathcal{O}_K$. In this section, we shall establish an isomorphism of $\mathrm{C}_N(d_K)$ onto $\mathrm{Gal}(K_N/K)$ in a concrete way.

Let $\mathcal{F}_N$ be the field of meromorphic modular functions of level N with Fourier coefficients in $\mathbb{Q}(\zeta_N)$, where $\zeta_N = e^{2\pi \mathrm{i}/N}$. It is well known that $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1$ with

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

[**13**, theorem 6.6]. In particular, the subgroup $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$ acts on the field $\mathcal{F}_N$ as follows: Let $h(\tau) \in \mathcal{F}_N$ and $\alpha \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$. Then we have

$$h(\tau)^\alpha = h(\widetilde{\alpha}(\tau)),$$

where $\widetilde{\alpha}$ is any matrix in $\mathrm{SL}_2(\mathbb{Z})$ that reduces to α via $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$.

Definition 3.1. *We call a family*

$$\{h_\alpha(\tau)\}_{\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}}$$

of functions in $\mathcal{F}_N$ a Fricke family of level N if

$$h_\alpha(\tau)^\beta = h_{\alpha\beta}(\tau) \quad \textit{for all } \alpha,\, \beta \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}.$$

Remark 3.2. In their work on modular units and elliptic units, Kubert and Lang first introduced the notion of a Fricke family [**7**]. Recently, Jung, Koo and Shin sharpened and modified the original definition and apply it to generate modular function fields and ray class fields of imaginary quadratic fields [**5**].

Remark 3.3. For a Fricke family $\{h_\alpha(\tau)\}_\alpha$, let $h(\tau) = h_{I_2}(\tau)$. Then we get

$$h(\tau)^\alpha = h_{I_2}(\tau)^\alpha = h_{I_2\alpha}(\tau) = h_\alpha(\tau) \quad (\alpha \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}).$$

This shows that $\{h_\alpha(\tau)\}_\alpha$ is a family of Galois conjugates of $h(\tau) = h_{I_2}(\tau)$ under $\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$.

For a class $C \in \mathrm{Cl}(N)$ take an integral ideal $\mathfrak{a}$ in C^{-1}, and let $\xi_1,\, \xi_2 \in K^*$ such that

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

Let τ_K be the element of $\mathbb{H}$ stated in remark 2.10 (ii). Since $\mathcal{O}_K \subseteq \mathfrak{a}^{-1}$ and $\xi \in \mathbb{H}$, one can write

$$\begin{bmatrix} \tau_K \\ 1 \end{bmatrix} = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \quad \text{for some } A = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \in M_2^+(\mathbb{Z}). \tag{3.1}$$

Here, $M_2^+(\mathbb{Z})$ is the set of 2×2 matrices over $\mathbb{Z}$ with positive determinants. It then follows that

$$\begin{bmatrix} \tau_K & \overline{\tau}_K \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} r & s \\ u & v \end{bmatrix} \begin{bmatrix} \xi_1 & \overline{\xi}_1 \\ \xi_2 & \overline{\xi}_2 \end{bmatrix}.$$

Taking determinant and squaring, we obtain

$$d_K = \det(A)^2 \mathrm{disc}_{K/\mathbb{Q}}(\mathfrak{a}^{-1}) = \det(A)^2 \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})^{-2} d_K$$

[**9**, proposition 13 in Chapter III]. Thus, we deduce $\det(A) = \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})$ which is prime to N.

DEFINITION 3.4. *Let $\{h_\alpha(\tau)\}_\alpha$ be a Fricke family of level N, and let $C \in \mathrm{Cl}(N)$. Following the above notations, we define*

$$h(C) = h_A(\xi).$$

Here, we regard A as an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$.

PROPOSITION 3.5. *The value $h(C)$ depends only on the ray class C, not on the choices of $\mathfrak{a}$ and ξ_1, ξ_2.*

Proof. First, let $\mathfrak{a}'$ be another integral ideal in C^{-1}. Then we have

$$\mathfrak{a}' = \lambda\mathfrak{a} \quad \text{for some } \lambda \in K^* \quad \text{such that } \lambda \equiv^* 1 \pmod{N\mathcal{O}_K},$$

and so

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

We see from the fact $\mathfrak{a}$, $\mathfrak{a}' = \lambda\mathfrak{a} \subseteq \mathcal{O}_K$ that

$$(\lambda - 1)\mathfrak{a} \subseteq \mathcal{O}_K.$$

Moreover, since $\lambda \equiv^* 1 \pmod{N\mathcal{O}_K}$ and $\mathfrak{a}$ is prime to $N\mathcal{O}_K$, we obtain

$$(\lambda - 1)\mathfrak{a} \subseteq N\mathcal{O}_K,$$

and hence

$$(\lambda - 1)\mathcal{O}_K \subseteq N\mathfrak{a}^{-1}.$$

Thus we obtain by the fact $\mathcal{O}_K = [\tau_K, 1]$ that

$$(\lambda - 1)\tau_K = N(a\xi_1 + b\xi_2) \quad \text{and} \quad \lambda - 1 = N(c\xi_1 + d\xi_2) \quad \text{for some } a, b, c, d \in \mathbb{Z}. \tag{3.2}$$

On the other hand, since $\lambda\mathcal{O}_K \subseteq \lambda\mathfrak{a}'^{-1} = \mathfrak{a}^{-1} = [\xi_1, \xi_2]$, we may write

$$\begin{bmatrix} \lambda\tau_K \\ \lambda \end{bmatrix} = \begin{bmatrix} r' & s' \\ u' & v' \end{bmatrix} \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \quad \text{for some } \begin{bmatrix} r' & s' \\ u' & v' \end{bmatrix} \in M_2^+(\mathbb{Z}). \tag{3.3}$$

One can then derive by (3.1), (3.2) and (3.3) that

$$N \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} = \begin{bmatrix} r' & s' \\ u' & v' \end{bmatrix} \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} - \begin{bmatrix} r & s \\ u & v \end{bmatrix} \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix},$$

which yields

$$\begin{bmatrix} r' & s' \\ u' & v' \end{bmatrix} \equiv \begin{bmatrix} r & s \\ u & v \end{bmatrix} \pmod{N}.$$

Second, let $\xi_1', \xi_2' \in K^*$ such that

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

We then express

$$\begin{bmatrix} \tau_K \\ 1 \end{bmatrix} = A' \begin{bmatrix} \xi_1' \\ \xi_2' \end{bmatrix} \text{ and } \begin{bmatrix} \xi_1' \\ \xi_2' \end{bmatrix} = B \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} \text{ for some } A' \in M_2^+(\mathbb{Z}) \text{ and } B \in \mathrm{SL}_2(\mathbb{Z}),$$

and so by (3.1) we deduce

$$A' \begin{bmatrix} \xi_1' \\ \xi_2' \end{bmatrix} = A \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix} = AB^{-1} \begin{bmatrix} \xi_1' \\ \xi_2' \end{bmatrix}.$$

Hence we achieve

$$\xi' = B(\xi) \quad \text{and} \quad A' = AB^{-1}.$$

Therefore we get that

$$h_{A'}(\xi') = h_{AB^{-1}}(B(\xi)) = h_{AB^{-1}}(\tau)^B|_{\tau=\xi} = h_{AB^{-1}B}(\tau)|_{\tau=\xi} = h_A(\xi),$$

which proves the proposition. □

Remark 3.6.

(i) If C_0 denotes the identity class in $\mathrm{Cl}(N)$, namely, C_0 is the ray class containing $\mathcal{O}_K = [\tau_K, 1]$, then

$$h(C_0) = h_{I_2}(\tau_K).$$

(ii) The invariant $h(C)$ is an analogue of the Siegel-Ramachandra invariant given in [7, p. 235] and [11].

Let

$$\widehat{\mathbb{Z}} = \prod_{p\,:\,\text{primes}} \mathbb{Z}_p \quad \text{and} \quad \widehat{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}.$$

We can decompose $\mathrm{GL}_2(\widehat{\mathbb{Q}})$ as

$$\mathrm{GL}_2(\widehat{\mathbb{Q}}) = \mathrm{GL}_2(\widehat{\mathbb{Z}})\mathrm{GL}_2^+(\mathbb{Q}) = \mathrm{GL}_2^+(\mathbb{Q})\mathrm{GL}_2(\widehat{\mathbb{Z}}), \tag{3.4}$$

where

$$\mathrm{GL}_2^+(\mathbb{Q}) = \{\gamma \in \mathrm{GL}_2(\mathbb{Q}) \mid \det(\gamma) > 0\}$$

[1, theorem 15.9 (i)] or [8, theorem 1 in Chapter 7]. Furthermore, we have

$$\mathrm{GL}_2(\widehat{\mathbb{Q}}) \simeq \prod_{p\,:\,\mathrm{primes}}{}' \mathrm{GL}_2(\mathbb{Q}_p), \tag{3.5}$$

where $'$ denotes the restricted product, that is, for almost all p the p-component of an element of $\prod_p \mathrm{GL}_2(\mathbb{Q}_p)$ lies in $\mathrm{GL}_2(\mathbb{Z}_p)$ [1, Exercise 15.4]. Let

$$\mathcal{F} = \bigcup_{M=1}^{\infty} \mathcal{F}_M.$$

Then, we have a surjective homomorphism

$$\sigma_{\mathcal{F}} : \mathrm{GL}_2(\widehat{\mathbb{Q}}) \to \mathrm{Aut}(\mathcal{F})$$

with $\mathrm{Ker}(\sigma_{\mathcal{F}}) = \mathbb{Q}^*$ [8, theorems 4 and 6 in Chapter 7] or [13, theorem 6.23]. More precisely, let $h(\tau) \in \mathcal{F}_N$ and $\gamma \in \mathrm{GL}_2(\widehat{\mathbb{Q}})$, and so $\gamma = \alpha\beta$ with $\alpha = (\alpha_p)_p \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $\beta \in \mathrm{GL}_2^+(\mathbb{Q})$ by (3.4) and (3.5). By using the Chinese remainder theorem, one can find a unique matrix $\widetilde{\alpha}$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $\widetilde{\alpha} \equiv \alpha_p \pmod{N}$ for all primes p such that $p\,|\,N$. We then obtain

$$h(\tau)^{\sigma_{\mathcal{F}}(\gamma)} = h^{\widetilde{\alpha}}(\beta(\tau)) \tag{3.6}$$

[8, theorem 2 in Chapter 7 and p. 79].

For $\omega \in K \cap \mathbb{H}$, we have an embedding

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

defined by

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

By continuity one can extend q_ω to an embedding

$$q_{\omega,\,p} : K_p^* = (K \otimes_{\mathbb{Z}} \mathbb{Z}_p)^* \to \mathrm{GL}_2(\mathbb{Q}_p)$$

for each prime p, and hence to an embedding of idele groups

$$q_\omega : \widehat{K}^* = (K \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^* \to \mathrm{GL}_2(\widehat{\mathbb{Q}})$$

[8, p. 149]. Let K^{ab} be the maximal abelian extension of K.

PROPOSITION 3.7 Shimura's reciprocity law. *Let s be a finite idele of K and $(s^{-1},\,K)$ be the Artin symbol for s^{-1} on K^{ab}. Let $\omega \in K \cap \mathbb{H}$ and $h(\tau) \in \mathcal{F}$ which is finite at ω. Then, $h(\omega)$ lies in K^{ab} and satisfies*

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

Proof. See [8, theorem 1 in Chapter 11] or [13, theorem 6.31 (i)]. □

REMARK 3.8. The group of finite ideles of K is defined by

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

Then, the class field theory of K is summarized by the exact sequence

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

where K^* maps into $\mathbb{I}_K^{\mathrm{fin}}$ through the diagonal embedding $\nu \mapsto (\nu, \nu, \nu, \ldots)$ and $(\,\cdot\,, K)$ is the Artin map [**10**, Chapter IV]. If we let

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

then we have

$$\mathcal{O}_{K,\,p} \simeq \prod_{\mathfrak{p}\,|\,p} \mathcal{O}_{K_{\mathfrak{p}}} \quad \text{and} \quad \widehat{K}^* \simeq \mathbb{I}_K^{\mathrm{fin}}$$

[**12**, Chapter II]. Thus we may identify $\mathbb{I}_K^{\mathrm{fin}}$ with $\widehat{K}^*$ for the class field theory of K.

THEOREM 3.9. *Let $\{h_\alpha(\tau)\}_\alpha$ be a Fricke family of level N, and let $C \in \mathrm{Cl}(N)$. If $h(C)$ is finite, then it belongs to K_N and satisfies*

$$h(C)^{\sigma_N(C'^{-1})} = h(CC') \quad \textit{for all } C' \in \mathrm{Cl}(N)$$

where $\sigma_N : \mathrm{Cl}(N) \to \mathrm{Gal}(K_N/K)$ is the Artin map for modulus $N\mathcal{O}_K$.

Proof. Let $\mathfrak{a}$ and $\mathfrak{a}'$ be integral ideals in C^{-1} and C'^{-1}, respectively. Take $\xi_1, \xi_2, \xi_1'', \xi_2'' \in K^*$ so that

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

and

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

Since $\mathcal{O}_K \subseteq \mathfrak{a}^{-1} \subseteq (\mathfrak{a}\mathfrak{a}')^{-1}$, we may write

$$\begin{bmatrix}\tau_K \\ 1\end{bmatrix} = A \begin{bmatrix}\xi_1 \\ \xi_2\end{bmatrix} \quad \text{for some } A \in M_2^+(\mathbb{Z}) \tag{3.7}$$

and

$$\begin{bmatrix}\xi_1 \\ \xi_2\end{bmatrix} = B \begin{bmatrix}\xi_1'' \\ \xi_2''\end{bmatrix} \quad \text{for some } B \in M_2^+(\mathbb{Z}). \tag{3.8}$$

Let s be an element of $\widehat{K}^*$ such that for every prime p

$$\begin{cases} s_p = 1 & \text{if } p \mid N, \\ s_p\mathcal{O}_{K,\,p} = \mathfrak{a}'_p & \text{if } p \nmid N. \end{cases} \tag{3.9}$$

Since $\mathfrak{a}'$ is prime to $N\mathcal{O}_K$, we get

$$s_p^{-1}\mathcal{O}_{K,\,p} = \mathfrak{a}_p'^{-1} \quad \text{for all primes } p. \tag{3.10}$$

Observe that for every prime p

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

Thus,

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

are bases for the $\mathbb{Z}_p$-module $(\mathfrak{a}\mathfrak{a}')_p^{-1}$ by (3.8) and (3.10). So, there exists $u_p \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that

$$q_{\xi,\,p}(s_p^{-1}) = u_p B^{-1}. \tag{3.11}$$

If we let

$$u = (u_p)_p \in \prod_{p\colon \text{primes}} \mathrm{GL}_2(\mathbb{Z}_p),$$

then we obtain

$$q_\xi(s^{-1}) = uB^{-1}. \tag{3.12}$$

Now, we derive that

$$\begin{aligned}
h(C)^{(s,\,K)} &= h_A(\xi)^{(s,\,K)} \quad \text{by definition 3.4} \\
&= h_A(\tau)^{\sigma_{\mathcal{F}}(q_\xi(s^{-1}))}|_{\tau=\xi} \quad \text{by proposition 3.7} \\
&= h_A(\tau)^{\sigma_{\mathcal{F}}(uB^{-1})}|_{\tau=\xi} \quad \text{by (3.12)} \\
&= h_{Au}(B^{-1}(\tau))|_{\tau=\xi} \quad \text{by (3.6)}, \\
&\qquad\qquad \text{where } u \text{ is regarded as an element of} \\
&\qquad\qquad \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \\
&= h_{AB}(B^{-1}(\tau))|_{\tau=\xi} \quad \text{because for every prime divisor } p \text{ of } N \\
&\qquad\qquad \text{we have } s_p = 1 \text{ by (3.9), and so} \\
&\qquad\qquad u_pB^{-1} = I_2 \text{ by (3.11)} \\
&= h_{AB}(B^{-1}(\xi)) \\
&= h_{AB}(\xi'') \quad \text{by (3.8)} \\
&= h(CC') \quad \text{since } \begin{bmatrix} \tau_K \\ 1 \end{bmatrix} = AB \begin{bmatrix} \xi_1'' \\ \xi_2'' \end{bmatrix} \text{ by (3.7) and (3.8).}
\end{aligned}$$

In particular, if $C' = C^{-1}$, then we see that

$$h(C) = h(CC')^{(s^{-1},\,K)} = h(C_0)^{(s^{-1},\,K)} = h_{I_2}(\tau_K)^{(s^{-1},\,K)}$$

by remark 3.6 (i). This implies that $h(C)$ belongs to K_N because $h_{I_2}(\tau_K)$ lies in K_N by proposition 1.4. Since $\mathrm{ord}_\mathfrak{p}\, s_p = \mathrm{ord}_\mathfrak{p}\, \mathfrak{a}'$ for all primes p such that $p \nmid N$ and prime ideals $\mathfrak{p}$ of K lying above p by (3.9), we achieve

$$(s,\,K)|_{K_N} = \sigma_N(C'^{-1}).$$

Therefore, we conclude

$$h(C)^{\sigma_N(C'^{-1})} = h(CC').$$

□

Let $\min(\tau_K,\,\mathbb{Q}) = x^2 + b_K x + c_K \in \mathbb{Z}[x]$, and so

$$\tau_K = \frac{-b_K + \sqrt{d_K}}{2}.$$

Theorem 3.10. *We have an isomorphism of groups*

$$\mathrm{C}_N(d_K) \to \mathrm{Gal}(K_N/K)$$

$$[ax^2 + bxy + cy^2] \mapsto \left(h(\tau_K) \mapsto h_{\left[\begin{smallmatrix} a & (b-b_K)/2 \\ 0 & 1 \end{smallmatrix}\right]} \left(\tfrac{-b+\sqrt{d_K}}{2a}\right) \,|\, h(\tau) \in \mathcal{F}_N \text{ is finite at } \tau_K \right).$$

Proof. Let $Q(x,\,y) = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$. Then, $C = \phi_N([Q])$ is the ray class containing the fractional ideal $\mathfrak{c} = [\omega_Q,\,1]$. Since

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

by lemma 2.3 (iii), $\mathfrak{a} = a^{\varphi(N)}\mathfrak{c}^{-1}$ is an integral ideal in C^{-1}. It then follows that

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

and

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

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

$$h(C) = h_{\left[\begin{smallmatrix} a & (b-b_K)/2 \\ 0 & 1 \end{smallmatrix}\right]}(\omega_Q).$$

Now, by composing the two isomorphisms

$$\mathrm{C}_N(d_K) \to \mathrm{Cl}(N)$$

$$[ax^2 + bxy + cy^2] \mapsto \text{ray class containing } [(-b + \sqrt{d_K})/2a,\,1]$$

given in theorem 2.9 and

$$\begin{aligned}&\mathrm{Cl}(N) \to \mathrm{Gal}(K_N/K)\\ &\quad C \mapsto \left(h(\tau_K) = h(C_0) \mapsto h(C_0)^{\sigma_N(C^{-1})} = h(C)\,|\, h(\tau) \in \mathcal{F}_N \text{ is finite at } \tau_K\right)\end{aligned}$$

obtained by theorem 3.9, we establish the theorem. □

4. Explicit construction of extended form class groups

In this section, we shall explain how to find representatives of forms classes in $\mathrm{C}_N(d_K)$.

LEMMA 4.1. *Let $Q(x, y) = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$ and $u, v \in \mathbb{Z}$. Then, the fractional ideal $(u\omega_Q + v)\mathcal{O}_K$ is prime to $N\mathcal{O}_K$ if and only if $Q(v, -u)$ is prime to N.*

Proof. We deduce from the fact $\gcd(N, a) = 1$ that

$$\begin{aligned}&(u\omega_Q + v)\mathcal{O}_K \text{ is prime to } N\mathcal{O}_K\\ \iff\ &\text{the integral ideal } a(u\omega_Q + v)\mathcal{O}_K \text{ is prime to } N\mathcal{O}_K\\ \iff\ &\mathcal{N}_{K/\mathbb{Q}}(a(u\omega_Q + v)) \text{ is prime to } N.\end{aligned}$$

Hence, we obtain that

$$\begin{aligned}\mathcal{N}_{K/\mathbb{Q}}(a(u\omega_Q + v)) &= a^2(u\omega_Q + v)(u\overline{\omega}_Q + v)\\ &= a^2(u^2\omega_Q\overline{\omega}_Q + uv(\omega_Q + \overline{\omega}_Q) + v^2)\\ &= a^2(u^2(c/a) + uv(-b/a) + v^2)\\ &= a(cu^2 - buv + av^2)\\ &= aQ(v, -u).\end{aligned}$$

This proves the lemma. □

Let $P_K(N)$ be the subgroup of $I_K(N)$ consisting of principal fractional ideals prime to $N\mathcal{O}_K$.

LEMMA 4.2. *Let $Q(x, y) = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$ and $C \in P_K(N)/P_{K,1}(N) \subseteq \mathrm{Cl}(N)$. Then we have*

$$C = [(u\omega_Q + v)\mathcal{O}_K] \quad \textit{for some } u, v \in \mathbb{Z} \textit{ such that } \gcd(N, Q(v, -u)) = 1.$$

Proof. Take an integral ideal $\mathfrak{c}$ in C. Since $\mathcal{O}_K = [a\omega_Q, 1]$ by remark 1.2, we get

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

Set $u = ta$. Then, the lemma follows from lemma 4.1. □

Define an equivalence relation $\equiv_N$ on $\mathbb{Z}^2$ by

$$\begin{bmatrix} r \\ s \end{bmatrix} \equiv_N \begin{bmatrix} u \\ v \end{bmatrix} \quad \Longleftrightarrow \quad \begin{bmatrix} r \\ s \end{bmatrix} \equiv \pm \begin{bmatrix} u \\ v \end{bmatrix} \pmod{N}.$$

LEMMA 4.3. *Let* $Q(x,\, y) = ax^2 + bxy + cy^2 \in \mathcal{Q}_N(d_K)$*, and let* $\begin{bmatrix} r \\ s \end{bmatrix},\ \begin{bmatrix} u \\ v \end{bmatrix} \in \mathbb{Z}^2$ *such that* $\gcd(N,\, Q(s, -r)) = \gcd(N,\, Q(v, -u)) = 1$*. Then,* $(r\omega_Q + s)\mathcal{O}_K$ *and* $(u\omega_Q + v)\mathcal{O}_K$ *represent the same ray class in* $\mathrm{Cl}(N)$ *if and only if*

$$\begin{bmatrix} r \\ s \end{bmatrix} \equiv_N \begin{bmatrix} u \\ v \end{bmatrix}.$$

Proof. By lemma 4.1, both $(r\omega_Q + s)\mathcal{O}_K$ and $(u\omega_Q + v)\mathcal{O}_K$ are prime to $N\mathcal{O}_K$. Then we see that

$$\begin{aligned}
&(r\omega_Q + s)\mathcal{O}_K \text{ and } (u\omega_Q + v)\mathcal{O}_K \text{ represent the same ray class in } \mathrm{Cl}(N) \\
\Longleftrightarrow\ & \left(\frac{r\omega_Q + s}{u\omega_Q + v}\right)\mathcal{O}_K \in P_{K,\,1}(N) \\
\Longleftrightarrow\ & \frac{r\omega_Q + s}{u\omega_Q + v} \equiv^* \pm 1 \pmod{N\mathcal{O}_K} \quad \text{because } \mathcal{O}_K^* = \{1, -1\} \\
\Longleftrightarrow\ & a(r\omega_Q + s) \equiv^* \pm a(u\omega_Q + v) \pmod{N\mathcal{O}_K} \\
\Longleftrightarrow\ & (r \pm u)(a\omega_Q) + (s \pm v)a \in N\mathcal{O}_K \quad \text{since } a\omega_Q \in \mathcal{O}_K \\
\Longleftrightarrow\ & r \pm u \equiv (s \pm v)a \equiv 0 \pmod{N} \quad \text{due to } N\mathcal{O}_K = [Na\omega_Q,\, N] \\
\Longleftrightarrow\ & \begin{bmatrix} r \\ s \end{bmatrix} \equiv \pm \begin{bmatrix} u \\ v \end{bmatrix} \pmod{N} \quad \text{by the fact } \gcd(N,\, a) = 1 \\
\Longleftrightarrow\ & \begin{bmatrix} r \\ s \end{bmatrix} \equiv_N \begin{bmatrix} u \\ v \end{bmatrix}.
\end{aligned}$$

□

THEOREM 4.4. *One can find all distinct elements of* $\mathrm{C}_N(d_K)$ *through the following steps.*

Step 1. *Find all reduced forms* $Q_1, Q_2, \ldots, Q_h$ *in* $\mathcal{Q}(d_K)$*.*

Step 2. *Take a matrix* σ_i *in* $\mathrm{SL}_2(\mathbb{Z})$ *for which*

$$Q_i'\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = Q_i\left(\sigma_i \begin{bmatrix} x \\ y \end{bmatrix}\right) \quad (i = 1,\, 2, \ldots, h)$$

belongs to $Q_N(d_K)$

Step 3. *For each pair of* $i = 1,\, 2, \ldots, h$ *and* $\left[\begin{bmatrix} u \\ v \end{bmatrix}\right] \in \mathbb{Z}^2/\equiv_N$ *such that* $\gcd(N,\, Q_i'(v, -u)) = 1$*, take a matrix* $\rho_{i,\, [[\begin{smallmatrix} u \\ v \end{smallmatrix}]]} = \begin{bmatrix} r & s \\ \widetilde{u} & \widetilde{v} \end{bmatrix}$ *in* $\mathrm{SL}_2(\mathbb{Z})$ *satisfying* $\widetilde{u} \equiv u \pmod{N}$ *and* $\widetilde{v} \equiv v \pmod{N}$*.*

Step 4. *Let* $\widetilde{Q}_{i,\,[[\begin{smallmatrix}u\\v\end{smallmatrix}]]} = Q_i'\left(\rho^{-1}_{i,\,[[\begin{smallmatrix}u\\v\end{smallmatrix}]]}\begin{bmatrix}x\\y\end{bmatrix}\right)$. *Then we obtain*

$$\mathrm{C}_N(d_K) = \left\{\left[\widetilde{Q}_{i,\,[[\begin{smallmatrix}u\\v\end{smallmatrix}]]}\right] \mid i = 1,\,2,\,\ldots,\,h \textit{ and } \left[\begin{bmatrix}u\\v\end{bmatrix}\right] \in \mathbb{Z}^2/\equiv_N \textit{ such that } \gcd(N,\,Q_i'(v,-u)) = 1\right\}.$$

Proof. Note first that

$$\mathrm{C}(d_K) \simeq \mathrm{Gal}(K_N/K)/\mathrm{Gal}(K_N/H_K) \quad \text{and} \quad P_K(N)/P_{K,\,1}(N) \simeq \mathrm{Gal}(K_N/H_K). \tag{4.1}$$

One can readily find reduced forms $Q_1, Q_2, \ldots, Q_h$ in $\mathcal{Q}(d_K)$ which represent all classes in $\mathrm{C}(d_K)$ [**1**, theorem 2.8]. Furthermore, one can take $\sigma_i \in \mathrm{SL}_2(\mathbb{Z})$ for which

$$Q_i'\left(\begin{bmatrix}x\\y\end{bmatrix}\right) = Q_i\left(\sigma_i\begin{bmatrix}x\\y\end{bmatrix}\right) \quad (i = 1,\,2,\ldots,h)$$

belongs to $\mathcal{Q}_N(d_K)$ [**1**, lemmas 2.3 and 2.25]. Then,

$$\left\{[[\omega_{Q_i'},\,1]] \in \mathrm{Cl}(N) \,|\, i = 1,\,2,\ldots,h\right\}$$

is a subset of $\mathrm{Cl}(N)$ whose image under $\mathrm{Cl}(N) \to \mathrm{Cl}(1)$ is all of $\mathrm{Cl}(1)$. Furthermore, for each $i = 1,\,2,\ldots,h$, we obtain by lemmas 4.1, 4.2 and 4.3 that

$$P_K(N)/P_{K,\,1}(N) = \left\{\left[(u\omega_{Q_i'} + v)\mathcal{O}_K\right] \mid \left[\begin{bmatrix}u\\v\end{bmatrix}\right] \in \mathbb{Z}^2/\equiv_N \text{ such that } \gcd(N,\,Q_i'(v,-u)) = 1\right\}. \tag{4.2}$$

Now, let $C \in \mathrm{Cl}(N)$. By (4.1) and (4.2), there is one and only one pair of $i \in \{1,\,2,\ldots,h\}$ and $\left[\begin{bmatrix}u\\v\end{bmatrix}\right] \in \mathbb{Z}^2/\equiv_N$ with $\gcd(N,\,Q_i'(v,-u)) = 1$ so that

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

Take a matrix $\rho_{i,\,[[\begin{smallmatrix}u\\v\end{smallmatrix}]]} = \begin{bmatrix}r & s\\ \widetilde{u} & \widetilde{v}\end{bmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$ satisfying

$$\widetilde{u} \equiv u \pmod{N} \quad \text{and} \quad \widetilde{v} \equiv v \pmod{N}.$$

Since

$$\frac{\mathcal{J}(\rho_{i,\,[[\begin{smallmatrix}u\\v\end{smallmatrix}]]},\,\omega_{Q_i'})}{u\omega_{Q_i'} + v} \equiv^* 1 \pmod{N\mathcal{O}_K},$$

https://doi.org/10.1017/prm.2018.163 Published online by Cambridge University Press

we get by lemma 2.3 (i) that

$$C = \left[\frac{1}{\mathcal{J}(\rho_{i,\,[[\begin{smallmatrix}u\\v\end{smallmatrix}]]},\,\omega_{Q_i'})}[\omega_{Q_i'},\,1]\right] = \left[[\rho_{i,\,[[\begin{smallmatrix}u\\v\end{smallmatrix}]]}(\omega_{Q_i'}),\,1]\right].$$

Therefore we obtain

$$C = \phi_N([\widetilde{Q}]) = \phi_N\left(\left[Q_i'\left(\rho^{-1}_{i,\,[[\begin{smallmatrix}u\\v\end{smallmatrix}]]}\begin{bmatrix}x\\y\end{bmatrix}\right)\right]\right).$$

This completes the proof. □

EXAMPLE 4.5. *Let $K = \mathbb{Q}(\sqrt{-2})$ and $N = 3$. There is only one reduced form*

$$Q_1 = x^2 + 2y^2$$

of discriminant $d_K = -8$. Set $Q_1' = Q_1$. By theorem 4.4 one can find

$$\begin{aligned}\mathrm{C}_3(-8) &= \left\{Q_1'\left(\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}^{-1}\begin{bmatrix}x\\y\end{bmatrix}\right),\, Q_1'\left(\begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}^{-1}\begin{bmatrix}x\\y\end{bmatrix}\right)\right\}\\ &= \{[x^2+2y^2],\ [2x^2+y^2]\},\end{aligned}$$

and hence $\mathrm{C}_3(-8) \simeq \mathbb{Z}/2\mathbb{Z}$.

EXAMPLE 4.6. *Let $K = \mathbb{Q}(\sqrt{-5})$ and $N = 2$. Then there are two reduced forms of discriminant $d_K = -20$, namely,*

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

Let

$$Q_1' = Q_1 \quad \text{and} \quad Q_2' = Q_2\left(\begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\right) = 3x^2 - 2xy + 2y^2.$$

By theorem 4.4 we have

$$\begin{aligned}\mathrm{C}_2(-20) = \Bigg\{&Q_{1,\,1} = Q_1'\left(\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}^{-1}\begin{bmatrix}x\\y\end{bmatrix}\right),\, Q_{1,\,2} = Q_1'\left(\begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}^{-1}\begin{bmatrix}x\\y\end{bmatrix}\right),\\ &Q_{2,\,1} = Q_2'\left(\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}^{-1}\begin{bmatrix}x\\y\end{bmatrix}\right),\, Q_{2,\,2} = Q_2'\left(\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}^{-1}\begin{bmatrix}x\\y\end{bmatrix}\right)\Bigg\}\\ = \{&[x^2+5y^2],\ [5x^2+y^2],\ [3x^2-2xy+2y^2],\ [7x^2-6xy+2y^2]\}.\end{aligned}$$

Note that

$$Q = Q_{2,\,2}\left(\begin{bmatrix}1 & 0\\2 & 1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\right) = 3x^2 + 2xy + 2y^2 \sim_2 Q_{2,\,2}.$$

We then see by using the argument in remark 2.10 (iii) that

$$[Q_{2,\,2}]^{-1} = [Q]^{-1} = [Q_{2,\,1}] \neq [Q_{2,\,2}].$$

This implies that

$$\mathrm{C}_2(-20) \simeq \mathbb{Z}/4\mathbb{Z}.$$

https://doi.org/10.1017/prm.2018.163 Published online by Cambridge University Press

Example 4.7. *Let $K = \mathbb{Q}(\sqrt{-5})$ and $N = 6$. Let Q_1 and Q_2 be reduced forms of discriminant $d_K = -20$ stated in example 4.6. In this case, we let*

$$Q_1' = Q_1 \quad \text{and} \quad Q_2' = Q_2\left(\begin{bmatrix}1 & -1\\ 1 & 0\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}\right) = 7x^2 - 6xy + 2y^2.$$

By theorem 4.4 we obtain

$$\begin{aligned}\mathrm{C}_6(-20) = \Bigg\{ & Q_1'\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}^{-1}\begin{bmatrix}x\\ y\end{bmatrix}\right), Q_1'\left(\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}^{-1}\begin{bmatrix}x\\ y\end{bmatrix}\right),\\ & Q_1'\left(\begin{bmatrix}1 & 1\\ 2 & 3\end{bmatrix}^{-1}\begin{bmatrix}x\\ y\end{bmatrix}\right), Q_1'\left(\begin{bmatrix}-1 & -1\\ 3 & 2\end{bmatrix}^{-1}\begin{bmatrix}x\\ y\end{bmatrix}\right),\\ & Q_2'\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}^{-1}\begin{bmatrix}x\\ y\end{bmatrix}\right), Q_2'\left(\begin{bmatrix}0 & -1\\ 1 & 3\end{bmatrix}^{-1}\begin{bmatrix}x\\ y\end{bmatrix}\right),\\ & Q_2'\left(\begin{bmatrix}1 & 1\\ 2 & 3\end{bmatrix}^{-1}\begin{bmatrix}x\\ y\end{bmatrix}\right), Q_2'\left(\begin{bmatrix}1 & 0\\ 3 & 1\end{bmatrix}^{-1}\begin{bmatrix}x\\ y\end{bmatrix}\right)\Bigg\}\\ = \{ & [x^2 + 5y^2],\ [5x^2 + y^2],\ [29x^2 - 26xy + 6y^2],\ [49x^2 + 34xy + 6y^2],\\ & [7x^2 - 6xy + 2y^2],\ [83x^2 + 48xy + 7y^2],\ [107x^2 - 80xy + 15y^2],\\ & [43x^2 - 18xy + 2y^2]\}.\end{aligned}$$

5. Form class groups for ring class fields

In this section, we shall slightly modify theorems 2.9, 3.10 and 4.4 to construct form class groups isomorphic to ring class groups of K.

Let $\mathcal{O} = [N\tau_K, 1]$ be the order of conductor N in K. Let $\mathrm{C}(\mathcal{O})$ be the $\mathcal{O}$-ideal class group

$$\mathrm{C}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}),$$

where $I(\mathcal{O})$ is the group of proper fractional $\mathcal{O}$-ideals and $P(\mathcal{O})$ is its subgroup of principal $\mathcal{O}$-ideals [**1**, p. 123]. Since $\mathrm{C}(\mathcal{O})$ is isomorphic to $I_K(N)/P_{K,\mathbb{Z}}(N)$, where

$$\begin{aligned}P_{K,\mathbb{Z}}(N) = \{\lambda\mathcal{O}_K \mid \lambda \in K^* \text{ such that } \lambda \equiv^* m \pmod{N\mathcal{O}_K} \text{ for some } m \in \mathbb{Z} \text{ with}\\ \gcd(N, m) = 1\}\end{aligned}$$

[**1**, proposition 7.22], there is a unique abelian extension $H_{\mathcal{O}}$ of K for which

$$\mathrm{Gal}(H_{\mathcal{O}}/K) \simeq I_K(N)/P_{K,\mathbb{Z}}(N) \simeq \mathrm{C}(\mathcal{O}) \tag{5.1}$$

via the Artin map for modulus $N\mathcal{O}_K$. We call this extension $H_{\mathcal{O}}$ of K the *ring class field* of order $\mathcal{O}$. Let $\mathcal{F}_{0,N}(\mathbb{Q})$ be the field of meromorphic modular functions

$$\begin{array}{ccccc}
\mathrm{C}_N(d_K) & \xrightarrow[\phi_N]{\sim} & I_K(N)/P_{K,1}(N) & \xrightarrow{\sim} & \mathrm{Gal}(K_N/K) \\
\text{natural surjection}\big\downarrow & & \text{canonical homomorphism}\big\downarrow & & \text{restriction}\big\downarrow \\
\mathrm{C}_{\mathcal{O}}(d_K) & \longrightarrow & I_K(N)/P_{K,\mathbb{Z}}(N) & \xrightarrow{\sim} & \mathrm{Gal}(H_{\mathcal{O}}/K)
\end{array}$$

Figure 2. Form class groups and Galois groups

for the congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{bmatrix} r & s \\ u & v \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid u \equiv 0 \pmod{N} \right\}$$

with rational Fourier coefficients. Then we have

$$H_{\mathcal{O}} = K\left(h(\tau_K) \mid h(\tau) \in \mathcal{F}_{0,\,N}(\mathbb{Q}) \text{ is finite at } \tau_K\right) \tag{5.2}$$

[6, theorem 3.4].

Define an equivalence relation $\sim_{0,\,N}$ on $\mathcal{Q}_N(d_K)$ by

$$Q \sim_{0,\,N} Q' \quad \Longleftrightarrow \quad Q'\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = Q\left(\sigma \begin{bmatrix} x \\ y \end{bmatrix}\right) \text{ for some } \sigma \in \Gamma_0(N).$$

Furthermore, we define an equivalence relation $\equiv_{\mathbb{Z},\,N}$ on $\mathbb{Z}^2$ by

$$\begin{bmatrix} r \\ s \end{bmatrix} \equiv_{\mathbb{Z},\,N} \begin{bmatrix} u \\ v \end{bmatrix} \quad \Longleftrightarrow \quad \begin{bmatrix} r \\ s \end{bmatrix} \equiv m \begin{bmatrix} u \\ v \end{bmatrix} \pmod{N} \text{ for some } m \in \mathbb{Z} \text{ such that } \gcd(N,\, m) = 1.$$

THEOREM 5.1. *Consider the set of equivalence classes*

$$\mathrm{C}_{\mathcal{O}}(d_K) = \mathcal{Q}_N(d_K)/ \sim_{0,\,N} .$$

(i) *We can regard* $\mathrm{C}_{\mathcal{O}}(d_K)$ *as a group isomorphic to* $\mathrm{C}(\mathcal{O})$.

(ii) *We have an isomorphism of groups*

$$\begin{aligned} \mathrm{C}_{\mathcal{O}}(d_K) &\to \mathrm{Gal}(H_{\mathcal{O}}/K) \\ [ax^2 + bxy + cy^2] &\mapsto \left(h(\tau_K) \mapsto h(\omega_Q) \mid h(\tau) \in \mathcal{F}_{0,\,N}(\mathbb{Q}) \text{ is finite at } \tau_K\right). \end{aligned}$$

(iii) *We can find all distinct element of* $\mathrm{C}_{\mathcal{O}}(d_K)$ *through the four steps given in* theorem 4.4 *by using the equivalence relation* $\equiv_{\mathbb{Z},\,N}$ *on* $\mathbb{Z}^2$ *instead of* $\equiv_N$.

Proof. The result follows from theorems 2.9, 3.10, 4.4, (5.1), (5.2) and the following commutative diagram (figure 2):

We omit the details. □

EXAMPLE 5.2. *Let $K=\mathbb{Q}(\sqrt{-23})$ with $d_K=-23$ and $\mathcal{O}$ be the order of conductor $N=10$ in K. By using theorem 5.1 (iii) one can find*

$$\begin{aligned}\mathrm{C}_{\mathcal{O}}(-23)=\{&[23x^2-23xy+6y^2],[27x^2-25xy+6y^2],[39x^2-35xy+8y^2],\\&[59x^2-53xy+12y^2],[87x^2-79xy+18y^2],[x^2+xy+6y^2],\\&[3x^2-5xy+4y^2],[31x^2-15xy+2y^2],[131x^2-97xy+18y^2],\\&[303x^2-251xy+52y^2],[547x^2-477xy+104y^2],[9x^2+11xy+4y^2],\\&[3x^2-7xy+6y^2],[39x^2-17xy+2y^2],[179x^2-131xy+24y^2],\\&[423x^2-349xy+72y^2],[771x^2-671xy+146y^2],[13x^2+17xy+6y^2]\}.\end{aligned}$$

6. The maximal abelian extension unramified outside prime ideals dividing $N\mathcal{O}_K$

Let K_N^{ab} be the maximal abelian extension of K unramified outside prime ideals dividing $N\mathcal{O}_K$. If $N=1$, then K_N^{ab} is nothing but the Hilbert class field H_K of K. So, we assume $N\geqslant 2$. As an application, we shall describe $\mathrm{Gal}(K_N^{\mathrm{ab}}/K)$ in view of extended form class groups. Here we shall regard $\mathrm{Gal}(K_N^{\mathrm{ab}}/K)$ as a topological group equipped with Krull topology: for each $\rho\in\mathrm{Gal}(K_N^{\mathrm{ab}}/K)$, we take the cosets

$$\rho\mathrm{Gal}(K_N^{\mathrm{ab}}/F)$$

as a basis of open neighbourhoods of ρ, where F runs through all finite (abelian) subextensions of K_N^{ab}/K [**10**, § I.1].

If L is a finite abelian extension of K unramified outside prime ideals dividing $N\mathcal{O}_K$, then its conductor also divides $N^\ell\mathcal{O}_K$ for some $\ell\geqslant 1$. Thus L is contained in the ray class field K_{N^ℓ} [**13**, p. 116], and hence we get

$$K_N^{\mathrm{ab}}=\bigcup_{\ell\geqslant 1}K_{N^\ell}.$$

Furthermore, since

$$K_N\subseteq K_{N^2}\subseteq\cdots\subseteq K_{N^\ell}\subseteq\cdots,$$

we obtain the isomorphisms

$$\mathrm{Gal}(K_N^{\mathrm{ab}}/K)\simeq\varprojlim_{\ell}\mathrm{Gal}(K_{N^\ell}/K)\simeq\varprojlim_{\ell}\mathrm{C}_{N^\ell}(d_K)\tag{6.1}$$

of topological groups by theorem 3.10 [**14**, §2 in Appendix]. Here, the inverse system $\{\mathrm{C}_{N^\ell}(d_K)\}_\ell$ is given by the natural surjections $\mathrm{C}_{N^n}(d_K)\leftarrow\mathrm{C}_{N^m}(d_K)$ $(1\leqslant n\leqslant m)$. And we observe

$$\mathcal{Q}_{N^\ell}(d_K)=\mathcal{Q}_N(d_K)\quad\text{for all }\ell\geqslant 1.$$

For each $Q\in\mathcal{Q}_N(d_K)$ and $\ell\geqslant 1$, denote by

$$[Q]_{N^\ell}=\text{the form class containing }Q\text{ in }\mathrm{C}_{N^\ell}(d_K).$$

Then we have

$$\varprojlim_{\ell} \mathrm{C}_{N^\ell}(d_K) = \left\{ ([Q_1]_N,\, [Q_2]_{N^2}, \ldots, [Q_\ell]_{N^\ell}, \ldots) \in \prod_{\ell} \mathrm{C}_{N^\ell}(d_K) \,\middle|\, [Q_{\ell+1}]_{N^\ell} = [Q_\ell]_{N^\ell} \text{ for all } \ell \geqslant 1 \right\}.$$

Now, define an equivalence relation $\sim_{N^\infty}$ on the set $\mathcal{Q}_N(d_K)$ by

$$Q \sim_{N^\infty} Q' \quad \Longleftrightarrow \quad Q \sim_{N^\ell} Q' \text{ for all } \ell \geqslant 1.$$

For each $Q \in \mathcal{Q}_N(d_K)$, let $[Q]_{N^\infty}$ be the form class containing Q in $\mathrm{Q}_N(d_K)/\sim_{N^\infty}$. We also define a map

$$\begin{aligned} \iota \;:\; \mathcal{Q}_N(d_K)/\sim_{N^\infty} &\to \varprojlim_{\ell} \mathrm{C}_{N^\ell}(d_K) \\ [Q]_{N^\infty} &\mapsto ([Q]_N,\, [Q]_{N^2}, \ldots, [Q]_{N^\ell}, \ldots). \end{aligned}$$

Then it is straightforward that ι is well defined and injective.

Lemma 6.1. *We derive*

$$\varprojlim_{\ell} \mathrm{C}_{N^\ell}(d_K) = \overline{\iota(\mathcal{Q}_N(d_K)/\sim_{N^\infty})}.$$

Proof. Let $([Q_1]_N,\, [Q_2]_{N^2}, \ldots, [Q_\ell]_{N^\ell}, \ldots) \in \varprojlim_{\ell} \mathrm{C}_{N^\ell}(d_K)$ be given. For every $\ell \geqslant 1$, we see that

$$\begin{aligned} \iota([Q_\ell]_{N^\infty}) &= ([Q_\ell]_N,\, [Q_\ell]_{N^2}, \ldots, [Q_\ell]_{N^\ell}, \quad [Q_\ell]_{N^{\ell+1}}, \ldots) \\ &= ([Q_1]_N,\, [Q_2]_{N^2}, \ldots, [Q_\ell]_{N^\ell}, \quad [Q_\ell]_{N^{\ell+1}}, \ldots). \end{aligned}$$

Considering the Krull topology on $\mathrm{Gal}(K_N^{\mathrm{ab}}/K)$ we conclude that $\iota(\mathcal{Q}_N(d_K)/\sim_{N^\infty})$ is a dense subset of $\varprojlim_{\ell} \mathrm{C}_{N^\ell}(d_K)$. □

For $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, let us define a new equivalence relation $\sim_T$ on $\mathcal{Q}_N(d_K)$ by

$$Q \sim_T Q' \quad \Longleftrightarrow \quad Q'\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = Q\left(\sigma \begin{bmatrix} x \\ y \end{bmatrix}\right) \quad \text{for some } \sigma \in \langle -I_2,\, T\rangle.$$

Lemma 6.2. *Two equivalence relations $\sim_{N^\infty}$ and $\sim_T$ are the same.*

Proof. Let $Q(x,\, y) = ax^2 + bxy + cy^2$ and $Q'(x,\, y) = a'x^2 + b'xy + c'y^2$ be two elements of $\mathcal{Q}_N(d_K)$. Since $\langle -I_2,\, T\rangle$ is contained in $\pm\Gamma_1(N^\ell)$ for all $\ell \geqslant 1$, it is immediate that if $Q \sim_T Q'$, then $Q \sim_{N^\infty} Q'$.

https://doi.org/10.1017/prm.2018.163 Published online by Cambridge University Press

Conversely, assume that $Q \sim_{N^\infty} Q'$. Then, for each $\ell \geqslant 1$, there is $\sigma_\ell \in \pm\Gamma_1(N^\ell)$ such that

$$Q'\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = Q\left(\sigma_\ell \begin{bmatrix} x \\ y \end{bmatrix}\right).$$

Hence it follows from

$$Q\left(\sigma_1 \begin{bmatrix} x \\ y \end{bmatrix}\right) = Q\left(\sigma_\ell \begin{bmatrix} x \\ y \end{bmatrix}\right)$$

that

$$Q\left(\sigma_1\sigma_\ell^{-1} \begin{bmatrix} x \\ y \end{bmatrix}\right) = Q\left(\begin{bmatrix} x \\ y \end{bmatrix}\right),$$

which yields that $\sigma_1\sigma_\ell^{-1}$ belongs to the stabilizer subgroup $\mathrm{Stab}(Q)$ ($\subseteq \mathrm{SL}_2(\mathbb{Z})$) of Q. Since we are assuming $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, $\mathrm{Stab}(Q) = \{I_2, -I_2\}$; and hence $\sigma_1 = \sigma_\ell$ or $\sigma_1 = -\sigma_\ell$. Owing to the assumption $N \geqslant 2$ we achieve

$$\sigma_1 \in \bigcap_{\ell \geqslant 1} \pm\Gamma_1(N^\ell) = \langle -I_2, T\rangle.$$

Therefore, we conclude $Q \sim_T Q'$. □

LEMMA 6.3. *Let $Q(x, y) = ax^2 + bxy + cy^2$ and $Q'(x, y) = a'x^2 + b'xy + c'y^2$ be two elements of $\mathcal{Q}_N(d_K)$. Then,*

$$Q \sim_T Q' \quad \Longleftrightarrow \quad a = a' \text{ and } a \text{ divides } \frac{b - b'}{2}.$$

Proof. Observe that b and b' have the same parity by the discriminant condition

$$b^2 - 4ac = b'^2 - 4a'c' = d_K. \tag{6.2}$$

We then see that

$$\begin{aligned} Q \sim_T Q' &\Longleftrightarrow Q'\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = Q\left(\begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}\right) \text{ for some } s \in \mathbb{Z} \\ &\Longleftrightarrow a'x^2 + b'xy + c'y^2 = ax^2 + (2ax + b)xy + (a^2s + bs + c)y^2 \\ &\qquad\quad \text{for some } s \in \mathbb{Z} \\ &\Longleftrightarrow a' = a \text{ and } b' = 2as + b \text{ for some } s \in \mathbb{Z} \text{ by (6.2)} \\ &\Longleftrightarrow a = a' \text{ and } a \text{ divides } (b - b')/2. \end{aligned}$$

□

THEOREM 6.4. *The set $\mathcal{Q}_N(d_K)/\sim_T$ can be viewed as a dense subset of $\mathrm{Gal}(K_N^{\mathrm{ab}}/K)$.*

Proof. Let

$$\phi : \varprojlim_{\ell} \mathrm{C}_{N^\ell}(d_K) \to \mathrm{Gal}(K_N^{\mathrm{ab}}/K)$$

be the isomorphism obtained in (6.1). Then we get by lemmas 6.1 and 6.2

$$\mathrm{Gal}(K_N^{\mathrm{ab}}/K) = \overline{(\phi \circ \iota)(\mathcal{Q}_N(d_K)/\sim_T)}.$$

Moreover, lemma 6.3 enables us to distinguish different classes in $\mathcal{Q}_N(d_K)/\sim_T$ from one another. □

Acknowledgements

The authors would like to thank the referee for carefully reading the manuscript and for giving detailed comments and suggestions that have been helpful to improve the manuscript.

The first author was supported by the Dongguk University Research Fund of 2016. The third (corresponding) author was supported by the Hankuk University of Foreign Studies Research Fund of 2018 and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2017R1A2B1006578).

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) (Hoboken, NJ: John Wiley & Sons, Inc., 2013).

2 M. Deuring. *Die Klassenkörper der komplexen multiplikation*. Enzyklopädie der mathematischen Wissenschaften: Mit Einschluss ihrer Anwendungen, Band I 2, Heft 10, Teil II (Article I 2, 23) (Stuttgart: B.G. Teubner Verlagsgesellschaft, 1958).

3 H. Hasse. Neue Begründung der Komplexen Multiplikation I, II. *J. für die Reine und Angewandte Math.* **157** (1927), 115–139, 165 (1931), 64–88.

4 G. J. Janusz. *Algebraic number fields*, 2nd edn. Grad. Studies in Math. 7 (Providence, RI: Amer. Math. Soc., 1996).

5 H. Y. Jung, J. K. Koo and D. H. Shin. Primitive and totally primitive Fricke families with applications. *Results Math.* **71** (2017), 841–858.

6 J. K. Koo and D. H. Shin. Singular values of principal moduli. *J. Number Theory* **133** (2013), 475–483.

7 D. Kubert and S. Lang. *Modular units*, Grundlehren der mathematischen Wissenschaften 244 (New York-Berlin: Spinger-Verlag, 1981).

8 S. Lang. *Elliptic functions*, 2nd edn. With an appendix by J. Tate, Grad. Texts in Math. 112 (New York: Spinger-Verlag, 1987).

9 S. Lang. *Algebraic number theory*, 2nd edn. Grad. Texts in Math. 110 (New York: Spinger-Verlag, 1994).

10 J. Neukirch. *Class field theory*, Grundlehren der mathematischen Wissenschaften 280 (Berlin-Heidelberg: Springer-Verlag, 1986).

11 K. Ramachandra. Some applications of Kronecker's limit formula. *Ann. of Math. (2)* **80** (1964), 104–148.

12 J.-P. Serre. *Local fields* (New York: Springer-Verlag, 1979).

13 G. Shimura. *Introduction to the arithmetic theory of automorphic functions* (Princeton, NJ: Iwanami Shoten and Princeton University Press, 1971).

14 L. C. Washington. *Introduction to cyclotomic fields*, 2nd edn, Grad. Texts in Math. 83 (New York: Spinger-Verlag, 1997).