SUT Journal of Mathematics
Vol. 56, No. 1 (2020), 21–37

# Representation of the norm of ideals by quadratic forms with congruence conditions

**Genki Koda**

(Received August 5, 2019)

**Abstract.** Using a correspondence between the narrow ray class group modulo $m$ of a quadratic field and a certain set of equivalence classes of binary quadratic forms proved by Furuta and Kubota, we find a quadratic form $f$ and a pair of integers $(x_1, y_1)$ such that the norm of all integral ideals $\mathfrak{a}$ in a ray class is represented by $f(mx + x_1, my + y_1)$ with some integers $(x, y)$.

*AMS* 2010 *Mathematics Subject Classification.* 11E25, 11R37, 11R65.

*Key words and phrases.* Ray class group, ring class group, quadratic forms.

## §1. Introduction

Let $K$ be a quadratic field of discriminant $d_K$, and $m$ a positive integer. We denote by $\mathrm{Cl}_K(m)$ the narrow ray class group modulo $m$. For $\mathfrak{C} \in \mathrm{Cl}_K(m)$, the partial zeta function is defined by

$$\zeta(s, \mathfrak{C}) = \sum_{\mathfrak{a} \in \mathfrak{C}} N(\mathfrak{a})^{-s}$$

where $\mathfrak{a}$ runs over the integral ideals in $\mathfrak{C}$. Using the method of Shintani and Zagier, Yamamoto [12] showed that $\zeta(s, \mathfrak{C})$ is a linear combination of the series of the form

$$\sum_{x,y} f(mx + x_1, my + y_1)^{-s}$$

where the sum is taken over $\mathbb{Z}$ if $d_K < 0$ and over the positive integers if $d_K > 0$. Here $f$ is a reduced binary quadratic form associated to $\mathfrak{C}$ and the pair $(x_1, y_1)$ of integers satisfying $0 \leq x_1, y_1 \leq m$ is a congruence condition associated with $\mathfrak{C}$ ([12, Definition 2.1.1]). A method of computing of the congruence condition was studied in [12, §2] and [9, §4] and used in [9, §7] and

[8, §6]. The aim of this paper is to give a new interpretation of the congruence condition based on the isomorphism between a certain ray class group and the equivalence classes of quadratic forms by a certain congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$ by Furuta [6] and Kubota [11]. In fact, we show that there exists a correspondence between the congruence conditions and the cosets of $\mathrm{SL}(2,\mathbb{Z})$ by the congruence subgroup via the isomorphism of Furuta and Kubota.

To state the correspondence precisely, we first define the following congruence subgroups. We denote $\mathrm{SL}(2,\mathbb{Z})$ by $\Gamma$. For a positive integer $m$, let

$$\Gamma_{\pm 1}(m) = \left\{ \gamma \in \Gamma \;\middle|\; \gamma \equiv \begin{pmatrix} \pm 1 & * \\ 0 & \pm 1 \end{pmatrix} \pmod{m} \right\}. \tag{1.1}$$

The group $\Gamma_{\pm 1}(m)$ acts on the set $F(d_K)$ of the primitive binary quadratic forms of discriminant $d_K$ by $(f\gamma)(x,y) = f((x,y)\gamma^\top)$. We denote the set of the orbits which contain a representative $f$ satisfying $\gcd(m, f(1,0)) = 1$ by $(F(d_K)/\Gamma_{\pm 1}(m))'$. Furuta and Kubota showed that there exists a group isomorphism

$$\Phi_m : I_m/P_m(\{\overline{\pm 1}\}) \longrightarrow (F(d_K)/\Gamma_{\pm 1}(m))' \tag{1.2}$$

where $I_m$ is the group of fractional ideals of $K$ prime to $m$ and $P_m(\{\overline{\pm 1}\})$ is the group of principal ideals $(\alpha)$ with $\alpha \equiv \pm 1 \pmod{{}^* m\mathscr{O}_K}$, the multiplicative congruence, and $N(\alpha) > 0$. If $m = 1$, the class group $I_m/P_m(\{\overline{\pm 1}\})$ coincides with $\mathrm{Cl}_K^+$, the narrow ideal class group of $K$ (this coincides with the ordinary ideal class group if $K$ is imaginary). Hence, the isomorphism $\Phi_m$ is a generalization of the well-known isomorphism

$$\Phi_1 : \mathrm{Cl}_K^+ \longrightarrow F(d_K)/\Gamma.$$

Furthermore, Furuta and Kubota showed that the set $(F(d_K)/\Gamma_{\pm 1}(m))'$ in (1.2) forms an abelian group under a generalization of Gaussian composition.

We next define reduced forms of discriminant $d_K$. Let $f(x,y) = ax^2 + bxy + cy^2$ be a quadratic form in $F(d_K)$. When $d_K$ is negative, the form $f$ is reduced if

$$|b| \leq a \leq c, \text{ and } b \geq 0 \text{ if either } |b| = a \text{ or } a = c. \tag{1.3}$$

When $d_K$ is positive, the form $f$ is reduced if

$$a > 0,\ c > 0 \text{ and } b > a + c. \tag{1.4}$$

Here we follow the definition in [13, §13]. Note that each orbit in $F(d_K)/\Gamma$ contains a reduced form by [3, Theorem 2.8] and [13, §13, Theorem 1].

We are now ready to state our main theorem.

**Theorem 1.1.** *Let* $\mathfrak{C}$ *be a ray class in* $\mathrm{Cl}_K(m)$ *and* $\mathfrak{a}$ *an arbitrary integral ideal lying in* $\mathfrak{C}$. *We denote by* $[\mathfrak{a}^{-1}]$ *the ideal class of* $\mathfrak{a}^{-1}$ *in* $I_m/P_m(\{\overline{\pm 1}\})$. *We take a reduced form* $f$ *such that the narrow ideal class of* $\mathfrak{a}^{-1}$ *maps to* $f\Gamma$ *by the isomorphism* $\Phi_1$. *Then, there exists* $\gamma \in \Gamma$ *satisfying the following properties:*

- $\Phi_m([\mathfrak{a}^{-1}]) = (f\gamma)\Gamma_{\pm 1}(m)$;
- $N(\mathfrak{a}) = f(x, y)$ *with the integers* $(x, y)$ *satisfying the congruence condition* $(x, y) \equiv (1, 0)\gamma^{\top} \pmod{m}$.

*Remark* 1.2. There is a natural surjection $\mathrm{Cl}_K(m) \to I_m/P_m(\{\overline{\pm 1}\})$. Its kernel is generated by the ray class of $(\mu)$ in $\mathrm{Cl}_K(m)$ where $\mu$ is a totally positive element satisfying $\mu \equiv -1 \pmod{{}^*m\mathscr{O}_K}$, and its order is at most 2. The kernel is trivial if and only if there is a totally positive unit $u \equiv -1 \pmod{{}^*m\mathscr{O}_K}$, or $K$ is imaginary.

We prove the above theorem in Section 3. In the following section, we introduce the results of Furuta [6] and Kubota [11] in a more general setting. In Section 4, we give some explicit examples of Theorem 1.1. In the final section, we discuss quadratic forms with non-fundamental discriminant.

Throughout this paper, we use the following notation.

Let $K$ be a quadratic field of discriminant $d_K$ fixed once for all. We denote by $\mathscr{O}_K$ the ring of integers of $K$. For positive integers $\ell$ and $m$, let $\mathscr{O}_\ell$ be the order of $K$ of conductor $\ell$ and $I_m(\mathscr{O}_\ell)$ the group of proper fractional $\mathscr{O}_\ell$-ideals prime to $m$. We simply write $I_m = I_m(\mathscr{O}_K)$ if $\ell = 1$. For a subgroup $H_m$ of $(\mathbb{Z}/m\mathbb{Z})^\times$ which contains $-1 \pmod{m}$, we define the subgroup $P_m(\mathscr{O}_\ell, H_m)$ of $I_m(\mathscr{O}_\ell)$ by

$$\left\langle (\alpha) \in I_m(\mathscr{O}_\ell) \;\middle|\; \begin{array}{l} \alpha \in \mathscr{O}_\ell : \text{totally positive}, \\ \alpha \equiv k \pmod{m\mathscr{O}_\ell} \text{ for some } k \in \mathbb{Z} \text{ with } \overline{k} \in H_m \end{array} \right\rangle$$

where $\overline{k}$ is the residue class of $k$ modulo $m$. We simply write $P_m(H_m) = P_m(\mathscr{O}_K, H_m)$ if $\ell = 1$. We denote by $\alpha'$ the conjugate of $\alpha \in K$. To deal with real and imaginary cases simultaneously, we regard every element of imaginary quadratic fields as totally positive. We denote by $\Gamma$ the special linear group $\mathrm{SL}(2, \mathbb{Z})$ and define a *congruence subgroup* $\Gamma(H_m)$ of $\Gamma$ by

$$\Gamma(H_m) = \left\{ \gamma \in \Gamma \;\middle|\; \gamma \equiv \begin{pmatrix} k & * \\ 0 & k^{-1} \end{pmatrix} \pmod{m} \text{ for some } k \in H_m \right\}. \tag{1.5}$$

In particular, we denote $\Gamma(H_m)$ by $\Gamma_0(m)$ (resp. $\Gamma_{\pm 1}(m)$) if we take $H_m = (\mathbb{Z}/m\mathbb{Z})^\times$ (resp. $\{\overline{\pm 1}\}$). We denote by $\mathrm{Cl}_K^+(\mathscr{O}_\ell)$ the narrow ideal class group of $\mathscr{O}_\ell$ and we also call this group the narrow ring class group of conductor $\ell$. Let $\mathrm{Cl}_K(m)$ be the narrow ray class group modulo $m$ and $\mathrm{Cl}_K^+$ the narrow class group of $K$. We denote by $F(D)$ the set of primitive binary quadratic forms of discriminant $D$, and we further impose $a > 0$ for all $ax^2+bxy+cy^2 \in F(D)$ if $D$ is negative.

## §2. Classification of quadratic forms by congruence subgroup

In this section, we study a generalization of the group isomorphism between the ideal class group and the form class group due to Furuta [6] and Kubota [11]. Recently, similar results are obtained in [2], [5] and [7] for the case $d_K < 0$. We follow the presentation in Kubota [11, §8.2] to consider the both cases where $d_K$ is negative and positive. However, there is an additional condition in the description in [11], so we quote it with some modification (see Remark 2.2 for the precise reason).

We use the notation of $f = (a, b, c)$ to represent a quadratic form $f(x, y) = ax^2 + bxy + cy^2$. We define a right action of $\Gamma$ on $F(d_K)$ by

$$(f\gamma)(x, y) = f((x, y)\gamma^\top) \tag{2.1}$$

for any $f(x, y) \in F(d_K)$ and $\gamma \in \Gamma$.

Let $H_m$ be a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ which contains $\overline{-1}$. We define the *generalized ideal class group* by the quotient $I_m/P_m(H_m)$.

**Definition 2.1** ([11, §8.2]). *Let $\mathfrak{a} = [\alpha, \beta]$ be an arbitrary fractional ideal in $I_m$. The basis $[\alpha, \beta]$ is called a* canonical basis for $H_m$ *if $[\alpha, \beta]$ satisfies the following conditions:*

*(i)* $\dfrac{1}{\sqrt{d_K}}(\alpha'\beta - \alpha\beta') > 0$*;*

*(ii) There exists an integer $k$ such that $\alpha \equiv k \pmod{{}^*m\mathscr{O}_K}$ and $\overline{k} \in H_m$.*

Note that the left hand side of (i) is always a non-zero rational number. If the basis $[\alpha, \beta]$ satisfies (i), then we say that it is *positively oriented* according to [3, Exercises 7.19]. Let $\mathfrak{a} = [\alpha_1, \beta_1]$ be a positively oriented basis and $\mathfrak{a} = [\alpha_2, \beta_2]$ another basis. Then, $[\alpha_2, \beta_2]$ is positively oriented if and only if their transition matrix is in $\Gamma$. When $K$ is imaginary, a basis $[\alpha, \beta]$ is positively oriented if and only if $\beta/\alpha$ lies in the upper half plane of $\mathbb{C}$.

*Remark* 2.2. Definition 2.1 is slightly different from the definition in [11, §8.2], in which there is an assumption "$\alpha$ is totally positive". However, when we choose a system of representatives of $F(d_K)/\Gamma(H_m)$ in Section 3, it sometimes contains forms $f = (a, b, c)$ with negative $a$, thus we drop the condition and introduce $\rho_f$ as (2.3) in the proof of Proposition 2.4 to define $\Psi_m$ so that it maps such a form to an ideal with canonical basis.

**Lemma 2.3** ([11, §8.2]). *Let $\mathfrak{a}$ be an arbitrary fractional ideal in $I_m$. The following assertions hold.*

*(i) There exists a canonical basis for $H_m$ of $\mathfrak{a}$.*

*(ii) Let $\mathfrak{a} = [\alpha_1, \beta_1]$ be a canonical basis for $H_m$. Another basis $\mathfrak{a} = [\alpha_2, \beta_2]$ is also a canonical basis for $H_m$ if and only if $[\alpha_2, \beta_2] = [\alpha_1, \beta_1]\gamma$ with $\gamma \in \Gamma(H_m)$ (see (1.5)).*

*Proof.* (i) It is enough to show that there exists a canonical basis $[\alpha, \beta]$ for $H_m$ with $\alpha \equiv 1 \pmod{{}^*m\mathcal{O}_K}$. We first assume that $\mathfrak{a}$ is an integral ideal. Let $[1, \omega]$ be an integral basis of $K$ which is positively oriented and $\mathfrak{a} = [a, b + c\omega]$ the Hermite normal form of $\mathfrak{a}$ with respect to $[1, \omega]$. Note that the basis of $\mathfrak{a}$ is also positively oriented, and $a$ is prime to $m$. We take $c_1, c_2 \in \mathbb{Z}$ satisfying $c_1 a - c_2 m = 1$ and set $\alpha = c_1 a + m(b + c\omega)$, $\beta = c_2 a + a(b + c\omega)$. Thus we obtain a canonical basis $\mathfrak{a} = [\alpha, \beta]$ for $H_m$.

We next consider the case where $\mathfrak{a}$ is a fractional ideal. There is an integer $r \equiv 1 \pmod{m}$ such that $r\mathfrak{a}$ is integral. If we take a canonical basis $r\mathfrak{a} = [\alpha, \beta]$ for $H_m$, then we can find a canonical basis $\mathfrak{a} = [\alpha/r, \beta/r]$ for $H_m$.

(ii) Suppose that $\mathfrak{a} = [\alpha_1, \beta_1] = [\alpha_2, \beta_2]$ are canonical bases for $H_m$. Since both are positively oriented, the transition matrix $\gamma$ lies in $\Gamma$. Writing $\gamma = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix}$, we have $\alpha_2 = u_1\alpha_1 + u_3\beta_1$. On the other hand, since there is $(k \bmod m) \in H_m$ satisfying $\alpha_2 \equiv k\alpha_1 \pmod{{}^*m\mathcal{O}_K}$, we have $(u_1 - k)\alpha_1 + u_3\beta_1 \in m\mathfrak{a}$. Hence we have $u_1 \equiv k$, $u_3 \equiv 0 \pmod{m}$ and this means $\gamma \in \Gamma(H_m)$. The converse is trivial.

□

We denote by $(F(d_K)/\Gamma(H_m))'$ the set of $(a, b, c)\Gamma(H_m)$ with $\gcd(a, m) = 1$.

Now we can define an isomorphism $\Phi_m$ from $I_m/P_m(H_m)$ to $(F(d_K)/\Gamma(H_m))'$, which is a generalization of (1.2).

**Proposition 2.4** ([11, §8.2]). *Let $\mathfrak{a}$ be an arbitrary ideal lying in $I_m$ with a canonical basis $[\alpha, \beta]$ for $H_m$. There is a bijection*

$$\Phi_m : I_m/P_m(H_m) \longrightarrow (F(d_K)/\Gamma(H_m))'$$

*defined by*

$$\Phi_m : [\mathfrak{a}] \longmapsto f\Gamma(H_m)$$

*where $f$ is the quadratic form corresponding to $\mathfrak{a}$ defined by*

$$f(x, y) = \frac{N(\alpha x + \beta y)}{N(\mathfrak{a})}. \tag{2.2}$$

*Proof.* First, we prove that the map $\Phi_m$ is well defined. If we take another canonical basis $[\tilde{\alpha}, \tilde{\beta}]$ for $H_m$, then there is $\gamma \in \Gamma(H_m)$ which satisfies $(\tilde{\alpha}, \tilde{\beta}) = (\alpha, \beta)\gamma$ by Lemma 2.3. Hence we get the corresponding form $f\gamma$ by (2.1) and (2.2). Let $\mathfrak{b} = (\lambda)\mathfrak{a}$ with $(\lambda) \in P_m(H_m)$. Since $\lambda$ is totally positive, we can see that the basis $[\lambda\alpha, \lambda\beta]$ is also canonical for $H_m$, and it corresponds to the form $f(x, y)$ by (2.2). Therefore the map $\Phi_m$ is well defined.

Next, we construct the inverse map of $\Phi_m$. Let $f = (a, b, c) \in F(d_K)$ be an arbitrary quadratic form with $\gcd(a, m) = 1$ and let

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

We define a map from the set of such quadratic forms to $I_m$ by sending $f$ to $\mathfrak{a} = \rho_f[1, \tau]$ where

$$\rho_f = \begin{cases} 1 & \text{if } d_K < 0, \\ 1 & \text{if } d_K > 0 \text{ and } a > 0, \\ 1 + m\sqrt{d_K} & \text{if } d_K > 0 \text{ and } a < 0. \end{cases} \tag{2.3}$$

Consider $g = f\gamma = (A, B, C)$ with $\gamma = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \in \Gamma(H_m)$. We can write

$$A = aN(u_1 + u_3\tau), \quad B = 2au_1u_2 + b(u_1u_4 + u_2u_3) + 2cu_3u_4.$$

Note that $A$ is congruent to $au_1^2$ modulo $m$ and prime to $m$. The map $f \mapsto \mathfrak{a}$ defined above sends $g = f\gamma$ to

$$\mathfrak{b} = \rho_g \left[1, \frac{B + \sqrt{d_K}}{2A}\right].$$

Since we can write $B + \sqrt{d_K} = 2a(u_2 + u_4\tau)(u_1 + u_3\tau')$, we have

$$\mathfrak{b} = \rho_g \left[1, \frac{B + \sqrt{d_K}}{2A}\right] = \rho_g \left[1, \frac{u_2 + u_4\tau}{u_1 + u_3\tau}\right] = \rho_g\rho_f^{-1}(u_1 + u_3\tau)^{-1}\mathfrak{a}$$

and $(\rho_g\rho_f^{-1}(u_1 + u_3\tau)^{-1}) \in P_m(H_m)$. Therefore, the induced map $\Psi_m$ is well defined, and clearly we have $\Psi_m = \Phi_m^{-1}$. □

Furuta [6] and Kubota [11] showed that $(F(d_K)/\Gamma(H_m))'$ forms an abelian group under a generalized Gaussian composition and the map $\Phi_m$ in Proposition 2.4 is a group isomorphism.

*Remark* 2.5. When we take $H_m = (\mathbb{Z}/m\mathbb{Z})^\times$, the class group $I_m/P_m(H_m)$ is isomorphic to the narrow ring class group of conductor $m$ by [3, Proposition 7.22, Exercises 7.19–7.22].

We can extend the result in Proposition 2.4 to a certain generalized ideal class group of proper ideals in order $\mathscr{O}_\ell$ of $K$.

**Corollary 2.6.** *Let $\mathscr{O}_\ell$ be the order of conductor $\ell$ of $K$. Then there is a bijection from $I_m(\mathscr{O}_\ell)/P_m(\mathscr{O}_\ell, H_m)$ to $(F(\ell^2 d_K)/\Gamma(H_m))'$.*

*Proof.* The proof of Proposition 2.4 is still valid if we replace $\mathscr{O}_K$ by $\mathscr{O}_\ell$. □

*Remark* 2.7. (i) If we take $m = 1$, then we get a well-known isomorphism $\mathrm{Cl}_K^+(\mathscr{O}_\ell) \longrightarrow F(\ell^2 d_K)/\Gamma$. Combining this with Proposition 2.4 (see also Remark 2.5), we have an isomorphism from $F(\ell^2 d_K)/\Gamma$ to $(F(d_K)/\Gamma_0(\ell))'$. We discuss this isomorphism in Section 5.

(ii) The group $I_m(\mathscr{O}_\ell)/P_m(\mathscr{O}_\ell, H_m)$ is isomorphic to the quotient group of $I_{\ell m}$ by

(2.4)
$$\left\langle (\alpha) \in I_{\ell m} \;\middle|\; \begin{array}{l} \alpha \in \mathscr{O}_K : \text{totally positive}, \\ \alpha \equiv k \pmod{\ell m \mathscr{O}_K} \text{ for some } k \in \mathbb{Z} \text{ with } \overline{k} \in H_m \end{array} \right\rangle$$

where $\overline{k}$ is the residue class of $k$ modulo $m$. If we set

$$G_{\ell m} = \ker((\mathbb{Z}/\ell m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times/H_m), \tag{2.5}$$

then the group defined in (2.4) coincides with $P_{\ell m}(G_{\ell m})$. The isomorphism from $I_m(\mathscr{O}_\ell)/P_m(\mathscr{O}_\ell, H_m)$ to $I_{\ell m}/P_{\ell m}(G_{\ell m})$ is induced by $\mathfrak{a} \mapsto \mathfrak{a}\mathscr{O}_K$ for $\mathfrak{a} \in I_m(\mathscr{O}_\ell)$.

## §3. The proof of the main theorem

In this section, we prove the main theorem.

First, we define the *reduced ideal* associated to a reduced form.

**Definition 3.1.** *Let $f = (a, b, c)$ be a reduced form of discriminant $d_K$ defined in* (1.3) *and* (1.4). *and let $\tau = \frac{b+\sqrt{d_K}}{2a}$. We call the ideal $[1, \tau]$ the* reduced ideal *associated to $f$.*

By [3, Theorem 2.8] and [13, §13, Theorem 1], each orbit in $F(d_K)/\Gamma$ contains a reduced form. Furthermore, when $d_K$ is negative, the reduced form is unique in each orbit. If $d_K$ is positive, then there are finitely many reduced forms in each orbit. We fix one, say $f$, of the reduced forms for each orbit $f\Gamma$. The proofs of [3, Theorem 2.8] and [13, §13, Theorem 1] give us a simple algorithm to compute reduced form for each orbit $f\Gamma$. Once we take the reduced forms $\{f_i\}$ as a system of representatives of $F(d_K)/\Gamma$, we can take $\{f_i\gamma_j\}$ as a system of representatives of $F(d_K)/\Gamma(H_m)$ with coset representatives $\{\gamma_j\}$ of $\Gamma/\Gamma(H_m)$. It follows easily from [4, §1.2] that

$$[\Gamma : \Gamma(H_m)] = m\frac{\phi(m)}{|H_m|}\prod_{p|m}\left(1+\frac{1}{p}\right),$$

where $\phi$ is the Euler totient function.

After these preparations, we can now prove Theorem 1.1.

*Proof of Theorem 1.1.* We first recall the setting of the theorem. Let $\mathfrak{C}$ be a ray class in $\mathrm{Cl}_K(m)$ and $\mathfrak{a}$ an arbitrary integral ideal lying in $\mathfrak{C}$. Let $f = (a, b, c)$ be a reduced form such that the narrow class of $\mathfrak{a}^{-1}$ maps to $f\Gamma$ by the isomorphism $\Phi_1$. Let $\tau = \frac{b+\sqrt{d_K}}{2a}$ and let $\mathfrak{b} = [1, \tau]$ be the reduced ideal associated to $f$. By the assumption on the form $f$, the narrow class of $\mathfrak{a}^{-1}$ coincides with that of $\mathfrak{b}$. That is, there is a totally positive element $z \in K^\times$ satisfying $\mathfrak{a}\mathfrak{b} = (z)$. Since $\mathfrak{a}$ is integral, $z$ is lying in $\mathfrak{b}$ and written in the form $z = x+y\tau$ with a pair of integers $(x, y)$. Then the norm $N(\mathfrak{a})$ is equal to $f(x, y)$. In this proof, we denote by $[\mathfrak{c}]$ the ideal class of $\mathfrak{c}$ in $I_m/P_m(\{\overline{\pm 1}\})$ for $\mathfrak{c} \in I_m$. We will show that there is a matrix $\gamma \in \Gamma$ satisfying $\Phi_m([\mathfrak{a}^{-1}]) = (f\gamma)\Gamma_{\pm 1}(m)$ and $(x, y) \equiv (1, 0)\gamma^\top \pmod{m}$.

We take non-negative integers $r, s$ such that $f(r, s)$ is prime to $m$. Let $\beta = ar + s\frac{b-\sqrt{d_K}}{2}$ and $\mathfrak{b}' = \beta\mathfrak{b}$. Note that $\beta$ and $\beta\tau = cs + r\frac{b+\sqrt{d_K}}{2}$ are integers of $K$, and $\mathfrak{b}'$ is an integral ideal. Since $f$ is a reduced form, we have $N(\beta) = af(r, s) > 0$. Hence $\mathfrak{b}'$ belongs to the narrow class of $\mathfrak{b}$. We take an integral basis $\mathscr{O}_K = [1, \omega]$ with $\omega = \frac{b+\sqrt{d_K}}{2}$. Let $C$ be a matrix satisfying $(\beta, \beta\tau) = (1, \omega)C$. We can see that $C$ is given by $\begin{pmatrix} ar+bs & cs \\ -s & r \end{pmatrix}$ and $N(\mathfrak{b}') = |\det C| = f(r, s)$ is prime to $m$. Therefore, $\mathfrak{b}'$ is prime to $m$. Let $g$ be a quadratic form satisfying $\Phi_m([\mathfrak{a}^{-1}]) = g\Gamma_{\pm 1}(m)$. By the definition of $\Phi_m$, the form $g$ is also in the image of the narrow class of $\mathfrak{a}^{-1}$ under $\Phi_1$. Hence we can take a matrix $\gamma = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \in \Gamma$ satisfying $g = f\gamma$. As in the proof of Proposition 2.4, we have

$$\Phi_m^{-1}(g) = [\rho_g(u_1 + u_3\tau)^{-1}\mathfrak{b}] = [\rho_g(u_1\beta + u_3\beta\tau)^{-1}\mathfrak{b}']$$

where $\rho_g$ is defined in (2.3). We denote $\rho_g^{-1}(u_1\beta + u_3\beta\tau)$ by $\xi$. Since $[\mathfrak{a}^{-1}] = [(\xi^{-1})\mathfrak{b}']$, there is $\alpha \in K^\times$ satisfying $\alpha \equiv \pm 1 \pmod{^*m\mathscr{O}_K}$ and $\mathfrak{a}\mathfrak{b}' = (\alpha\xi)$. Since $\mathfrak{a}\mathfrak{b}' = (z\beta)$, we have $\alpha\xi = \pm z\beta$ by replacing $z$ by $z\varepsilon$ with some unit $\varepsilon \in \mathscr{O}_K^\times$ of positive norm if necessary, where the sign '±' in the right hand side agrees with that of $\alpha$ modulo $m$. We have

$$(x - u_1)\beta + (y - u_3)\beta\tau \equiv 0 \pmod{m\mathscr{O}_K}.$$

To complete the proof, we will show that $\overline{\beta}$ and $\overline{\beta\tau}$ are linearly independent over $\mathbb{Z}/m\mathbb{Z}$ where $\overline{\beta}$, $\overline{\beta\tau}$ are the residue classes of $\beta$, $\beta\tau$ modulo $m\mathscr{O}_K$, respectively. We have an isomorphism

$$\mathscr{O}_K/(m) \cong 1 \cdot \mathbb{Z}/m\mathbb{Z} \oplus \omega \cdot \mathbb{Z}/m\mathbb{Z}$$

as a $\mathbb{Z}/m\mathbb{Z}$-module. Since $\det C = f(r,s)$ is prime to $m$, we have $(C \bmod m) \in \mathrm{GL}(2, \mathbb{Z}/m\mathbb{Z})$. It follows that $\overline{\beta}$ and $\overline{\beta\tau}$ are linearly independent over $\mathbb{Z}/m\mathbb{Z}$. Thus we obtain $(x,y) \equiv (u_1, u_3) \pmod{m}$. This completes the proof. □

## §4. Examples

In this section, we give explicit examples of Theorem 1.1.

### 4.1. Imaginary case

Let $K = \mathbb{Q}(\sqrt{-5})$ and $m = 2$. We have $d_K = -20$, and the class number of $K$ is 2. The ray class group $\mathrm{Cl}_K(2)$ is generated by the class of $\mathfrak{c} = [3, 1+\sqrt{-5}]$ and isomorphic to $C_4$. The Galois group of the ray class field modulo 2 of $K$ over $\mathbb{Q}$ is isomorphic to $D_4$. This example is also considered in [5]; however, we focus on the congruence conditions implied by the isomorphic correspondence.

The reduced forms of discriminant $-20$ are

$$f_1(x,y) = x^2 + 5y^2, \quad f_2(x,y) = 2x^2 + 2xy + 3y^2,$$

and the associated ideals are $\mathfrak{b}_1 = [1, \sqrt{-5}]$, $\mathfrak{b}_2 = [1, \frac{1+\sqrt{-5}}{2}]$. Coset representatives of $\Gamma/\Gamma_{\pm1}(2)$ are

$$\gamma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \gamma_2 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \ \gamma_3 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Thus, excluding the forms with the first coefficient divisible by 2, we can take $\{f_1\gamma_1,\ f_1\gamma_3,\ f_2\gamma_2,\ f_2\gamma_3\}$ as a system of representatives for $(F(-20)/\Gamma_{\pm1}(2))'$. Explicitly, we obtain

$$(f_1\gamma_1)(x,y) = x^2 + 5y^2, \qquad (f_1\gamma_3)(x,y) = 5x^2 - 10xy + 6y^2,$$
$$(f_2\gamma_2)(x,y) = 7x^2 - 6xy + 2y^2, \qquad (f_2\gamma_3)(x,y) = 3x^2 - 8xy + 7y^2.$$

By the isomorphism $\Phi_2^{-1}$, we have the correspondence

$$\Phi_2^{-1}((f_1\gamma_1)\Gamma_{\pm1}(2)) = [\mathscr{O}_K], \qquad \Phi_2^{-1}((f_1\gamma_3)\Gamma_{\pm1}(2)) = [\mathfrak{c}^2] = [\mathfrak{c}^2]^{-1},$$
$$\Phi_2^{-1}((f_2\gamma_2)\Gamma_{\pm1}(2)) = [\mathfrak{c}] = [\mathfrak{c}^3]^{-1}, \qquad \Phi_2^{-1}((f_2\gamma_3)\Gamma_{\pm1}(2)) = [\mathfrak{c}^3] = [\mathfrak{c}]^{-1}.$$

For an integral ideal $\mathfrak{a}$, there exist integers $x, y$ such that

$$\begin{aligned}
\mathfrak{a} \in [\mathscr{O}_K] \quad &\Longrightarrow N(\mathfrak{a}) = f_1(2x+1, 2y),\\
\mathfrak{a} \in [\mathfrak{c}] \quad &\Longrightarrow N(\mathfrak{a}) = f_2(2x, 2y+1),\\
\mathfrak{a} \in [\mathfrak{c}^2] \quad &\Longrightarrow N(\mathfrak{a}) = f_1(2x, 2y+1),\\
\mathfrak{a} \in [\mathfrak{c}^3] \quad &\Longrightarrow N(\mathfrak{a}) = f_2(2x+1, 2y+1).
\end{aligned}$$

### 4.2. Real case

Let $K = \mathbb{Q}(\sqrt{17})$ and $m = 4$. The discriminant of $K$ is 17, and the narrow class number of $K$ is 1. The Galois group of the narrow ray class field modulo 4 of $K$ over $\mathbb{Q}$ is isomorphic to $D_4$. The ray class group $\mathrm{Cl}_K(4)$ is isomorphic to $C_2 \times C_2$. It is generated by $\mathfrak{C}_1$ and $\mathfrak{C}_2$ defined by

$$\begin{aligned}
\mathfrak{C}_1 = [(\mu_1)], \quad \mu_1 < 0,\ \mu_1' > 0,\ \mu_1 \equiv 1 \pmod{{}^*m\mathscr{O}_K},\\
\mathfrak{C}_2 = [(\mu_2)], \quad \mu_2 > 0,\ \mu_2' < 0,\ \mu_2 \equiv 1 \pmod{{}^*m\mathscr{O}_K}.
\end{aligned}$$

The kernel of the natural surjection

$$\pi : \mathrm{Cl}_K(4) \longrightarrow I_4/P_4(\{\pm 1\})$$

is of order 2 and generated by the class $\mathfrak{C}_1\mathfrak{C}_2$ by Remark 1.2. We set $\mathfrak{A}_1 = \pi([\mathscr{O}_K])$ and $\mathfrak{A}_2 = \pi(\mathfrak{C}_1)$.

The reduced forms corresponding to the narrow class of $\mathscr{O}_K$ are

$$\begin{aligned}
&f_1 = (1, 5, 2),\ f_2 = (2, 7, 4),\ f_3 = (4, 9, 4),\\
&f_4 = (4, 7, 2),\ f_5 = (2, 5, 1).
\end{aligned}$$

Note that these forms belong to the same orbit $f_1\Gamma$. We take $f = f_1$. Coset representatives of $\Gamma/\Gamma_{\pm 1}(4)$ are

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix},\ \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},\ \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix},\ \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}.$$

We call them $\gamma_1, \ldots, \gamma_6 \in \Gamma$. Excluding the forms $f\gamma_j$ with the first coefficient divisible by 2, we can take a set of two forms

$$(f\gamma_1)(x, y) = x^2 + 5xy + 2y^2, \quad (f\gamma_6)(x, y) = 19x^2 - 25xy + 8y^2$$

as a system of representatives for $(F(17)/\Gamma_{\pm 1}(4))'$. By the isomorphism $\Phi_4^{-1}$, the class of the form $f\gamma_1$ maps to $\mathfrak{A}_1$, and the class of $f\gamma_6$ maps to $\mathfrak{A}_2$. Thus, for an integral ideal $\mathfrak{a}$, there exist integers $x, y$ such that

$$\begin{aligned}
\mathfrak{a} \in [\mathscr{O}_K] \text{ or } \mathfrak{C}_1\mathfrak{C}_2 \quad &\Longrightarrow N(\mathfrak{a}) = f(4x+1, 4y),\\
\mathfrak{a} \in \mathfrak{C}_1 \text{ or } \mathfrak{C}_2 \quad &\Longrightarrow N(\mathfrak{a}) = f(4x+1, 4y+2).
\end{aligned}$$

## §5. Congruence conditions for the ring class group

Let $m$ be a positive integer and $D = m^2 d_K$. Recall that $F(D)$ is the set of primitive quadratic forms of discriminant $D$. The narrow ring class group $\mathrm{Cl}_K^+(\mathscr{O}_m)$ is isomorphic to $I_m/P_m(H_m)$ with $H_m = (\mathbb{Z}/m\mathbb{Z})^\times$ (see [3, Proposition 7.22]) and, by class field theory, the group corresponds to the ring class field of the order $\mathscr{O}_m$. It is well known that there is an isomorphism between $\mathrm{Cl}_K^+(\mathscr{O}_m)$ and $F(D)/\Gamma$ (see [3, Theorem 7.7 and Exsecise 7.21]). On the other hand, we proved that there is an isomorphism $\Phi_m$ from $\mathrm{Cl}_K^+(\mathscr{O}_m)$ to $(F(d_K)/\Gamma_0(m))'$ (the case $H_m = (\mathbb{Z}/m\mathbb{Z})^\times$ in Proposition 2.4; see also Remark 2.5). Therefore it is natural to ask whether there is a natural correspondence between the two form class groups $F(D)/\Gamma$ and $(F(d_K)/\Gamma_0(m))'$. In this section, we give such a natural correspondence between them.

In the rest of this section, we assume $H_m = (\mathbb{Z}/m\mathbb{Z})^\times$. A rational matrix $M \in \mathrm{GL}(2,\mathbb{Q})$ acts on a rational binary quadratic form $Q$ by $(QM)(x,y) = Q((x,y)M^\top)$.

**Theorem 5.1.** *Let $D = m^2 d_K$ and let $Q = (a,b,c) \in F(D)$ be a quadratic form satisfying $\gcd(a,m) = 1$. Let $M$ be a matrix with determinant $m$ defined by*

$$M = \begin{cases} \begin{pmatrix} 1 & r(b-m)/2 \\ 0 & m \end{pmatrix} & \text{if } d_K \equiv 1 \pmod 4, \\ \begin{pmatrix} 1 & rb/2 \\ 0 & m \end{pmatrix} & \text{if } d_K \equiv 0 \pmod 4 \end{cases} \tag{5.1}$$

*where $r$ is an integer satisfying $ar \equiv 1 \pmod m$. Then the rational quadratic form $(QM^{-1})(x,y)$ is an integral form of discriminant $d_K$. Furthermore, this correspondence $Q(x,y) \mapsto (QM^{-1})(x,y)$ induces a group isomorphism between $F(D)/\Gamma$ to $(F(d_K)/\Gamma_0(m))'$.*

*Proof.* We define an isomorphism from $F(D)/\Gamma$ to $(F(d_K)/\Gamma_0(m))'$ so that the following diagram is commutative:

$$\begin{array}{ccc} F(D)/\Gamma & \longrightarrow & (F(d_K)/\Gamma_0(m))' \\ \Psi \downarrow & & \uparrow \Phi_m \\ \mathrm{Cl}_K^+(\mathscr{O}_m) & \xrightarrow[\kappa]{} & I_m/P_m(H_m). \end{array} \tag{5.2}$$

In the diagram, $\Psi$ is the isomorphism obtained from Corollary 2.6 (see also Remark 2.7 (i)). By [3, Proposition 7.22], we can take a system of representatives $\{\mathfrak{a}_i\}$ of $\mathrm{Cl}_K^+(\mathscr{O}_m)$ such that $\mathfrak{a}_i$ are prime to $m$ and the map $\mathfrak{a}_i \mapsto \mathfrak{a}_i\mathscr{O}_K$ induces the isomorphism $\kappa$ from $\mathrm{Cl}_K^+(\mathscr{O}_m)$ to $I_m/P_m(H_m)$. The isomorphism $\Phi_m$ is defined in Proposition 2.4. The isomorphism from $F(D)/\Gamma$ to $(F(d_K)/\Gamma_0(m))'$ is, therefore, defined by $\Phi_m \circ \kappa \circ \Psi$.

We shall show that the above-defined map coincides with the isomorphism defined in the statement of the theorem. Let $Q = (a, b, c) \in F(D)$ satisfying $\gcd(a, m) = 1$ and let $\tau = (b + \sqrt{D})/2a$. Then the fractional $\mathscr{O}_m$-ideal $\mathfrak{a} = \rho_Q[1, \tau]$ is prime to $m$. The map $\kappa$ sends the class of $\mathfrak{a}$ to the class of $\mathfrak{a}\mathscr{O}_K = \rho_Q[1, \tilde{\tau}]$ where

$$\tilde{\tau} = \begin{cases} \dfrac{1 + s(b-m) + \sqrt{d_K}}{2a} & \text{if } d_K \equiv 1 \pmod 4, \\ \dfrac{sb + \sqrt{d_K}}{2a} & \text{if } d_K \equiv 0 \pmod 4 \end{cases} \tag{5.3}$$

with an integer $s$ satisfying $ms = 1 - ar$, where $r$ is an integer satisfying $ar \equiv 1 \pmod m$ as in the statement of the theorem. Since $[1, \tau] \otimes_{\mathbb{Z}} \mathbb{Q} \cong [1, \tilde{\tau}] \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$, there is a transition matrix $M$ in $\mathrm{GL}(2, \mathbb{Q})$ satisfying $[1, \tau] = [1, \tilde{\tau}]M$:

$$M = \begin{cases} \begin{pmatrix} 1 & r(b-m)/2 \\ 0 & m \end{pmatrix} & \text{if } d_K \equiv 1 \pmod 4, \\ \begin{pmatrix} 1 & rb/2 \\ 0 & m \end{pmatrix} & \text{if } d_K \equiv 0 \pmod 4. \end{cases} \tag{5.4}$$

Since $N(\mathfrak{a}) = N(\mathfrak{a}\mathscr{O}_K)$, we have

$$\begin{aligned} \frac{N(\rho_Q x + \rho_Q \tilde{\tau} y)}{N(\mathfrak{a}\mathscr{O}_K)} &= \frac{N(\rho_Q X + \rho_Q \tau Y)}{N(\mathfrak{a})} \\ &= \operatorname{sgn}(N(\rho_Q)) \operatorname{sgn}(a)\, Q(X, Y) = Q(X, Y) = (QM^{-1})(x, y) \end{aligned}$$

with a change of variable $(X, Y) = (x, y)(M^{-1})^{\top}$. This completes the proof. □

*Remark* 5.2. (i) For the case $d_K < 0$, a similar result is obtained in [2, Corollary 2.9 (2)]. By contrast, we obtain the result for general $d_K$. Besides, we also obtain the matrix $M$ in (5.1), which is related to the congruence condition given in Theorem 1.1 (see Corollary 5.3 and also Example 5.4).

(ii) Let $\mathfrak{b}$ be an integral ideal in $I_m$. The inverse of $\kappa$ is induced by $\mathfrak{b} \mapsto \mathfrak{b} \cap \mathscr{O}_m$, and we have $N(\mathfrak{b}) = N(\mathfrak{b} \cap \mathscr{O}_m)$. The imaginary quadratic case follows from [3, Proposition 7.20] and the real case can be proved similarly.

(iii) The inverse of $F(D)/\Gamma \to (F(d_K)/\Gamma_0(m))'$ is simpler to describe. In fact, for a quadratic form $f = (a, b, c) \in F(d_K)$ with $\gcd(a, m) = 1$, the map sending $f(x, y)$ to $f(x, my)$ induces the inverse map.

We obtain the following corollary analogous to Theorem 1.1.

**Corollary 5.3.** *Let* $\mathfrak{C} \in I_m/P_m(H_m)$ *and* $\mathfrak{a}$ *an integral ideal lying in* $\mathfrak{C}$. *Let* $Q = (a, b, c) \in F(m^2 d_K)$ *be a quadratic form with* $\gcd(a, m) = 1$ *satisfying* $\mathfrak{C}^{-1} = \kappa(\Psi(Q\Gamma))$, *where* $\Psi$ *and* $\kappa$ *are the maps defined in the proof of Theorem 5.1. If* $M$ *is the matrix determined from* $Q$ *by* (5.1) *and* $g(x, y) = (QM^{-1})(x, y) \in F(d_K)$, *then* $N(\mathfrak{a})$ *is represented by* $Q(X, Y)$ *with some integers* $X, Y$ *and is represented also by* $g(x, y)$ *with some integers with the congruence conditions* $x \not\equiv 0, y \equiv 0 \pmod{m}$.

*Proof.* Since $N(\mathfrak{a}) = N(\mathfrak{a} \cap \mathscr{O}_m)$, it is obvious that $N(\mathfrak{a})$ is represented by $Q(X, Y)$. By the definition of $g$, we can write $N(\mathfrak{a}) = g(x, y)$ with $(x, y) = (X, Y)M^{\top}$. Thus we have $y \equiv 0 \pmod{m}$. Since $N(\mathfrak{a})$ is prime to $m$, the integer $x$ must be prime to $m$. □

The following example illustrates the correspondence in Theorem 5.1 and the representation of the norm of ideals by two quadratic forms of different discriminants in Corollary 5.3.

*Example* 5.4. Let $K = \mathbb{Q}(\sqrt{-5})$ and $m = 2$. Let $\mathscr{O}_2 = [1, 2\sqrt{-5}]$ be the order of conductor 2 in $K$. We have $d_K = -20$ and $m^2 d_K = -80$. Note that the ring class group $\mathrm{Cl}_K^+(\mathscr{O}_2)$ is isomorphic to the ray class group $\mathrm{Cl}_K(2) \cong C_4$ generated by the class of $\mathfrak{c} = [3, 1 + \sqrt{-5}]$ (see Section 4.1). Thus $\mathrm{Cl}_K^+(\mathscr{O}_2)$ is generated by the class of $\tilde{\mathfrak{c}} = \mathfrak{c} \cap \mathscr{O}_2 = [3, -1 + 2\sqrt{-5}]$.

Corollary 5.3 claims that the norm of an ideal in each class of $\mathrm{Cl}_K(2)$ is represented in two ways by forms in $F(-80)$ and $F(-20)$. We start with the reduced forms of $F(-80)$:

$$Q_1(x, y) = x^2 + 20y^2, \qquad Q_2(x, y) = 4x^2 + 5y^2,$$
$$Q_3(x, y) = 3x^2 + 2xy + 7y^2, \qquad Q_4(x, y) = 3x^2 - 2xy + 7y^2.$$

If we replace $Q_2$ by $\left(Q_2 \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right)(x, y) = 5x^2 + 4y^2$, then the condition $\gcd(2, Q_i(1, 0)) = 1$ is satisfied for all $i = 1, \ldots, 4$. The isomorphism $\Psi$ from $F(-80)/\Gamma$ to $\mathrm{Cl}_K^+(\mathscr{O}_2)$ gives the correspondence

$$\Psi(Q_1\Gamma) = [\mathscr{O}_2], \quad \Psi(Q_2\Gamma) = [\tilde{\mathfrak{c}}^2], \quad \Psi(Q_3\Gamma) = [\tilde{\mathfrak{c}}^3], \quad \Psi(Q_4\Gamma) = [\tilde{\mathfrak{c}}].$$

To obtain the corresponding forms in $F(-20)$, we compute the matrix $M_i$ defined in (5.1):

$$M_1 = M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \quad M_4 = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix},$$

and the forms $g_i = Q_i M_i^{-1}$ are

$$g_1(x,y) = x^2 + 5y^2, \qquad g_2(x,y) = 5x^2 + y^2,$$
$$g_3(x,y) = 3x^2 - 2xy + 2y^2, \qquad g_4(x,y) = 3x^2 + 2xy + 2y^2.$$

Corollary 5.3 implies that, for an integral ideal $\mathfrak{a} \in I_2$, there exist integers $X, Y, x, y$ such that

$$\begin{array}{ll} \mathfrak{a} \in [\mathscr{O}_K] & \Longrightarrow N(\mathfrak{a}) = Q_1(X,Y) = g_1(2x+1, 2y), \\ \mathfrak{a} \in [\mathfrak{c}] = [\mathfrak{c}^3]^{-1} & \Longrightarrow N(\mathfrak{a}) = Q_3(X,Y) = g_3(2x+1, 2y), \\ \mathfrak{a} \in [\mathfrak{c}^2] = [\mathfrak{c}^2]^{-1} & \Longrightarrow N(\mathfrak{a}) = Q_2(X,Y) = g_2(2x+1, 2y), \\ \mathfrak{a} \in [\mathfrak{c}^3] = [\mathfrak{c}]^{-1} & \Longrightarrow N(\mathfrak{a}) = Q_4(X,Y) = g_4(2x+1, 2y). \end{array} \tag{5.5}$$

The set of the forms $g_i$ is a system of representatives of $(F(-20)/\Gamma_0(2))'$ by Theorem 5.1. For each representative $g_i$, there exist a reduced form $f$ in $F(-20)$ and a matrix $\gamma$ which is a representative of $\Gamma/\Gamma_0(2)$ satisfying $g_i = f\gamma$. The reduced forms of $F(-20)$ are given in Section 4.1:

$$f_1(x,y) = x^2 + 5y^2, \quad f_2(x,y) = 2x^2 + 2xy + 3y^2.$$

We can take matrices $\gamma_1, \ldots, \gamma_4 \in \Gamma$ satisfying

$$g_1 = f_1\gamma_1, \quad g_2 = f_1\gamma_2, \quad g_3 = f_2\gamma_3, \quad g_4 = f_2\gamma_4. \tag{5.6}$$

Explicitly, we obtain

$$\gamma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \gamma_2 = \gamma_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \gamma_4 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Combining (5.5) and (5.6), we recover the result in the example in Section 4.1.

$$\begin{array}{ll} \mathfrak{a} \in [\mathscr{O}_K] & \Longrightarrow N(\mathfrak{a}) = f_1(2x+1, 2y), \\ \mathfrak{a} \in [\mathfrak{c}] & \Longrightarrow N(\mathfrak{a}) = f_2(2x, 2y+1), \\ \mathfrak{a} \in [\mathfrak{c}^2] & \Longrightarrow N(\mathfrak{a}) = f_1(2x, 2y+1), \\ \mathfrak{a} \in [\mathfrak{c}^3] & \Longrightarrow N(\mathfrak{a}) = f_2(2x, 2y+1) \end{array}$$

with some integers $x, y$. Here the condition of the case $\mathfrak{a} \in [\mathfrak{c}^3]$ looks different from that of Section 4.1. Since $f_2$ is an ambiguous form and thus there is a stabilizer in $\mathrm{GL}(2,\mathbb{Z})$: $f_2 \cdot \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = f_2$, we obtain the same condition

$$\mathfrak{a} \in [\mathfrak{c}^3] \Longrightarrow N(\mathfrak{a}) = f_2(2x+1, 2y+1).$$

As an application of Theorem 5.1, we give another explanation of a result by Cho [1, Theorem 1]. Let $K$ be an imaginary quadratic field of discriminant $d_K$. Let $m$ and $\ell$ be positive integers and

$$H_{\ell m} = \ker((\mathbb{Z}/\ell m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times/\{\overline{\pm 1}\}),$$

the special case of (2.5). Since $P_{\ell m}(\{\overline{\pm 1}\}) \le P_{\ell m}(H_{\ell m}) \le I_{\ell m}$, there exists a class field $K_{m,\mathscr{O}_\ell}$ of $K$ satisfying $\mathrm{Gal}(K_{m,\mathscr{O}_\ell}/K) \cong I_{\ell m}/P_{\ell m}(H_{\ell m})$. We call $K_{m,\mathscr{O}_\ell}$ the *extended ring class field of level* $m$ according to [3, §15]. The class field $K_{m,\mathscr{O}_\ell}$ is studied in [1] and [10]. Note that $K_{1,\mathscr{O}_\ell}$ is the ring class field of the order $\mathscr{O}_\ell$, and $K_{m,\mathscr{O}_K}$ is the ray class field modulo $m$ of $K$. Let $\ell, n$ be positive integers satisfying $-4n = \ell^2 d_K$. Cho [1] proved that a prime number $p$ not dividing $2mn$ splits completely in $K_{m,\mathscr{O}_\ell}/\mathbb{Q}$ if and only if $p = x^2 + ny^2$ with $(x, y) \equiv (1, 0) \pmod{m}$. In the following proposition, we give a representation of $p$ by another quadratic form of discriminant $d_K$ with congruence conditions.

**Proposition 5.5.** *Let $n$ be a positive integer and $K = \mathbb{Q}(\sqrt{-n})$. Let $\ell$ be a positive integer satisfying $-4n = \ell^2 d_K$ and $\mathscr{O}_\ell$ the order of $K$ of conductor $\ell$. Let $m$ be a positive integer and $K_{m,\mathscr{O}_\ell}$ the extended ring class field of level $m$. If $p$ is a prime number not dividing $2mn$, then*

$$\begin{aligned}
&p \text{ splits completely in } K_{m,\mathscr{O}_\ell}\\
&\iff p = x^2 + ny^2 \text{ with some integers } x, y \text{ satisfying } (x, y) \equiv (1, 0) \pmod{m}\\
&\iff \begin{cases} p = x^2 + xy + \dfrac{1 - d_K}{4} y^2 & \text{if } d_K \equiv 1 \pmod 4\\ p = x^2 - \dfrac{d_K}{4} y^2 & \text{if } d_K \equiv 0 \pmod 4 \end{cases}\\
&\qquad \text{with the congruence conditions } x \equiv 1 \pmod{m} \text{ and } y \equiv 0 \pmod{\ell m}.
\end{aligned}$$

*Proof.* The first equivalence is proved in [1, Theorem 1]. We show the second one. Let $Q(x, y) = x^2 + ny^2$, the principal form of $F(-4n)$. If $M$ is the matrix determined from $Q$ by (5.1), then $\widetilde{Q} = QM^{-1} \in F(d_K)$ holds by Theorem 5.1. We can compute

$$M = \begin{cases} \begin{pmatrix} 1 & -\ell/2 \\ 0 & \ell \end{pmatrix} & \text{if } d_K \equiv 1 \pmod 4\\ \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} & \text{if } d_K \equiv 0 \pmod 4 \end{cases}$$

and

$$\widetilde{Q}(x, y) = \begin{cases} x^2 + xy + \dfrac{1 - d_K}{4} y^2 & \text{if } d_K \equiv 1 \pmod 4,\\ x^2 - \dfrac{d_K}{4} y^2 & \text{if } d_K \equiv 0 \pmod 4. \end{cases}$$

Suppose that a prime $p$ is represented by $Q(x,y)$ with the congruence condition $(x,y) \equiv (1,0) \pmod{m}$. Since we can write $Q = \widetilde{Q}M$, we have

$$p = Q(x,y) = \begin{cases} \widetilde{Q}\left(x - \dfrac{\ell}{2}y, \ell y\right) & \text{if } d_K \equiv 1 \pmod{4}, \\ \widetilde{Q}(x, \ell y) & \text{if } d_K \equiv 0 \pmod{4}. \end{cases}$$

If we set $(X,Y) = (x,y)M^{\top}$, then we obtain $X \equiv 1 \pmod{m}$ and $Y \equiv 0 \pmod{\ell m}$ in either case $d_K \equiv 1$ or $0$ modulo 4. By reversing the argument, we can prove the converse. □

There is an isomorphism between $(F(\ell^2 d_K)/\Gamma_{\pm 1}(m))'$ and $(F(d_K)/\Gamma(H_{\ell m}))'$ behind Proposition 5.5. This isomorphism is obtained as an extension of Theorem 5.1:

$$\begin{array}{ccc} (F(\ell^2 d_K)/\Gamma_{\pm 1}(m))' & \longrightarrow & (F(d_K)/\Gamma(H_{\ell m}))' \\ \Psi \downarrow & & \uparrow \Phi_{\ell m} \\ I_m(\mathscr{O}_\ell)/P_m(\mathscr{O}_\ell, \{\overline{\pm 1}\}) & \underset{\kappa}{\longrightarrow} & I_{\ell m}/P_{\ell m}(H_{\ell m}). \end{array}$$

For the definitions of $\Psi$ and $\kappa$ in the diagram, see Corollary 2.6 and Remark 2.7 (ii).

**Acknowledgement.** The author would like to thank the anonymous referee for careful reading our manuscript and for pointing out the references [2], [5], [7] and [10]. His/Her helpful comments and suggestions helped a lot to improve the manuscript.

## References

[1] Bumkyu Cho. Primes of the form $x^2 + ny^2$ with conditions $x \equiv 1 \bmod N$, $y \equiv 0 \bmod N$. *J. Number Theory*, 130(4):852–861, 2010.

[2] Bumkyu Cho. On the $\gamma$-equivalence of binary quadratic forms, 2017, arXiv:1711.00230.

[3] David A. Cox. *Primes of the form* $x^2 + ny^2$. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013.

[4] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[5] Ick Sun Eum, Ja Kyung Koo, and Dong Hwa Shin. Binary quadratic forms and ray class groups. 2017, arXiv:1712.04140.

[6] Yoshiomi Furuta. Gaussian composition of congruence classes. *Sci. Rep. Kanazawa Univ.*, 37(1):1–22, 1992.

[7] Ho Yun Jung, Ja Kyung Koo, and Dong Hwa Shin. On some extension of gauss' work and applications, 2019, arXiv:1905.11690.

[8] Masanari Kida and Genki Koda. Isoclinism classes of Galois groups of number fields. *Acta Arith.*, 191(2):115–149, 2019.

[9] Masanari Kida and Norihiko Namura. On Artin $L$-functions of certain central extensions. *J. Number Theory*, 173:147–169, 2017.

[10] Ja Kyung Koo, Dong Hwa Shin, and Dong Sung Yoon. Form class groups for extended ring class fields. *J. Number Theory*, 197:13–36, 2019.

[11] Tomio Kubota. *Suron ronsetsu (in Japanese).* Makino Shoten, Tokyo, 1999.

[12] Shuji Yamamoto. On Kronecker limit formulas for real quadratic fields. *J. Number Theory*, 128(2):426–450, 2008.

[13] D. B. Zagier. *Zetafunktionen und quadratische Körper.* Springer-Verlag, Berlin-New York, 1981.

Genki Koda
Department of Mathematics, Tokyo University of Science
Kagurazaka 1-3, Shinjuku, Tokyo 162-8601, Japan
*E-mail*: 1117702@ed.tus.ac.jp