ACTA ARITHMETICA
105.3 (2002)

Class numbers of pairs of symmetric matrices

by

JIN NAKAGAWA (Joetsu)

In [3], K. Hardy and K. S. Williams studied equivalence classes of pairs of positive definite binary quadratic forms with integral coefficients, where two pairs (P_1, P_2) and (Q_1, Q_2) are said to be *equivalent* if there exists an element γ in $\mathrm{SL}(2, \mathbb{Z})$ such that $Q_i(u, v) = P_i((u, v)\gamma)$, $i = 1, 2$. Let δ_i be the discriminant of P_i and let $\varDelta$ be the codiscriminant of (P_1, P_2). Then δ_1, δ_2 and $\varDelta$ depend only on the equivalence class of (P_1, P_2). Hardy and Williams proved a formula for the number of the equivalence classes of (P_1, P_2) with given δ_1, δ_2 and $\varDelta$ under certain conditions on these invariants. J. Morales extended their result to the case of pairs (P_1, P_2) with arbitrary signatures in [4]. Further in [5], he also generalized it to the case of pairs (P_1, P_2) of symmetric matrices of degree $n \geq 2$ with coefficients in the ring of integers of an arbitrary algebraic number field.

Let n be a positive integer with $n \geq 2$ and let $x = (x_1, x_2)$ be a pair of symmetric matrices of degree n with coefficients in $\mathbb{Z}$. We set $\varGamma = \mathrm{GL}(n, \mathbb{Z})$. For any $\gamma \in \varGamma$, we put $\gamma x = (\gamma x_1 {}^{\mathrm{t}}\gamma, \gamma x_2 {}^{\mathrm{t}}\gamma)$. We say that two pairs $x = (x_1, x_2)$ and $y = (y_1, y_2)$ are *$\varGamma$-equivalent* if there exists an element $\gamma \in \varGamma$ such that $y = \gamma x$. We define a binary form $\varPhi_x(u, v)$ of variables u, v by

$$\varPhi_x(u, v) = \det(u x_1 + v x_2). \tag{0.1}$$

Then $\varPhi_x(u, v)$ is an integral binary form of degree n. It is obvious that $\varPhi_{\gamma x}(u, v) = \varPhi_x(u, v)$ for any $\gamma \in \varGamma$. We say that a binary form with coefficients in $\mathbb{Z}$ is *primitive* if the greatest common divisor of its coefficients is equal to 1. Let $\varPhi(u, v)$ be an integral irreducible binary form of degree n. Let θ be a root of the equation $\varPhi(u, 1) = 0$ and put $K = \mathbb{Q}(\theta)$. We consider those pairs x with $\varPhi_x = \varPhi$. Morales associated an order $\varLambda_x$ of K with the pair x. For a given binary form $\varPhi(u, v)$ and a given order $\varLambda$, he studied the number of $\varGamma$-equivalence classes of pairs x with $\varPhi_x = \varPhi$ and $\varLambda_x = \varLambda$

2000 *Mathematics Subject Classification*: 11E12, 11E76.

Key words and phrases: quadratic form, binary form, class number.

This research was supported by Grant-in-Aid for Scientific Research (No. 12640018), Ministry of Education, Culture, Sports, Science and Technology of Japan.

under the assumptions that Φ is primitive and Λ is weakly self-dual (for the definition of weak self-duality, see Section 1).

In the present paper, we study pairs x without these assumptions. We denote by $h(\Phi)$ the number of Γ-equivalence classes of pairs x with $\Phi_x = \Phi$. Though our results are very restrictive so that we can give formulae for $h(\Phi)$ only for $n = 2$ and 3 under certain assumptions (Theorems 3.1, 4.1), this problem is interesting because it gives a relation between the set of Γ-equivalence classes of pairs of symmetric matrices and the ideal class group of a number field. In particular, the space of pairs of symmetric matrices of degree 3 is the prehomogeneous vector space studied by D. J. Wright and A. Yukie in [9] which parameterizes quartic extensions of fields. So further investigation of our problem for the case of $n = 3$ would be closely related to the theory of zeta functions of that prehomogeneous vector space.

1. Orders associated with binary forms. In this section, we recall some results of A. Fröhlich on invertible ideals of orders of algebraic number fields. Then we apply them to the orders associated with integral binary forms.

Let K be a finite algebraic number field and denote by $\mathcal{O}_K$ and D_K the ring of integers in K and the discriminant of K, respectively. For any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we denote by $N(\mathfrak{a})$ the norm of $\mathfrak{a}$. We call a submodule $\mathfrak{m}$ of K a *lattice* if it is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$. We write $\mathfrak{m} = [\alpha_1, \ldots, \alpha_n]$ if $\mathfrak{m}$ is generated by $\{\alpha_1, \ldots, \alpha_n\}$ over $\mathbb{Z}$. We denote by $D(\mathfrak{m})$ the discriminant of $\mathfrak{m}$. Hence $D_K = D(\mathcal{O}_K)$. We call a lattice $\mathcal{O}$ of K an *order* if it is a subring of K containing 1. Any order $\mathcal{O}$ of K is a subring of $\mathcal{O}_K$ of finite index. For any lattice $\mathfrak{m}$ of K, put

$$\mathcal{O}(\mathfrak{m}) = \{\mu \in K \mid \mu\mathfrak{m} \subset \mathfrak{m}\}.$$

Then $\mathcal{O}(\mathfrak{m})$ is an order of K. Let $\mathcal{O}$ be an order of K. We call a lattice $\mathfrak{m}$ of K an $\mathcal{O}$-*ideal* if $\mathcal{O}\mathfrak{m} \subset \mathfrak{m}$. We say that an $\mathcal{O}$-ideal $\mathfrak{m}$ is *integral* if $\mathfrak{m} \subset \mathcal{O}$. We say that an $\mathcal{O}$-ideal $\mathfrak{m}$ is a *proper* $\mathcal{O}$-ideal if $\mathcal{O}(\mathfrak{m}) = \mathcal{O}$. Let $\mathfrak{m}$ be an $\mathcal{O}$-ideal. Put

$$\mathfrak{m}^{-1} = \{\mu \in K \mid \mu\mathfrak{m} \subset \mathcal{O}\}.$$

We say that $\mathfrak{m}$ is *invertible* if $\mathfrak{m}\mathfrak{m}^{-1} = \mathcal{O}$. An invertible $\mathcal{O}$-ideal is a proper $\mathcal{O}$-ideal. The converse is not true in general. If $\mathfrak{a}$ and $\mathfrak{b}$ are two invertible $\mathcal{O}$-ideals, then the product ideal $\mathfrak{a}\mathfrak{b}$ is also an invertible $\mathcal{O}$-ideal. Hence the set of all invertible $\mathcal{O}$-ideals forms an abelian group, which is denoted by $I_{\mathcal{O}}$. For any $\alpha \in K^{\times}$, the principal $\mathcal{O}$-ideal $\alpha\mathcal{O}$ is an invertible $\mathcal{O}$-ideal. The set of all principal $\mathcal{O}$-ideals forms a subgroup of $I_{\mathcal{O}}$, which is denoted by $P_{\mathcal{O}}$. The quotient group $I_{\mathcal{O}}/P_{\mathcal{O}}$ is a finite abelian group, which is called the *Picard group* of $\mathcal{O}$ and is denoted by $\mathrm{Pic}(\mathcal{O})$. We also define $\mathrm{Pic}^+(\mathcal{O})$ by $\mathrm{Pic}^+(\mathcal{O}) = I_{\mathcal{O}}/P_{\mathcal{O}}^+$, where $P_{\mathcal{O}}^+ = \{(\alpha) \in P_{\mathcal{O}} \mid N_{K/\mathbb{Q}}\alpha > 0\}$. For any $\mathcal{O}$-

ideal $\mathfrak{a}$, we put

$$a(\mathfrak{a},\mathcal{O}) = \frac{(\mathcal{O}_K : \mathcal{O})}{(\mathcal{O}_K\mathfrak{a} : \mathfrak{a})}, \tag{1.1}$$

where $(A : B)$ is the index of B in A. Then Fröhlich obtained the following criterion for an ideal to be invertible (cf. [2, Corollary 1 to Theorem 4]).

LEMMA 1.1. *Let $\mathfrak{a}$ be an $\mathcal{O}$-ideal. Then $a(\mathfrak{a},\mathcal{O})$ is a natural number. Further $a(\mathfrak{a},\mathcal{O}) = 1$ if and only if $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal.*

He also obtained another criterion (cf. [2, Theorem 5]).

LEMMA 1.2. *Let $\mathfrak{a}$ be an $\mathcal{O}$-ideal. Then $(\mathcal{O}_K\mathfrak{a}^2 : \mathfrak{a}^2) \mid (\mathcal{O}_K\mathfrak{a} : \mathfrak{a})$. Further, $(\mathcal{O}_K\mathfrak{a}^2 : \mathfrak{a}^2) = (\mathcal{O}_K\mathfrak{a} : \mathfrak{a})$ if and only if $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal.*

For any lattice $\mathfrak{m}$ of K, denote by $\widehat{\mathfrak{m}}$ the dual lattice of $\mathfrak{m}$ in K with respect to the bilinear form induced by the trace $\mathrm{Tr}_{K/\mathbb{Q}}$:

$$\widehat{\mathfrak{m}} = \{\lambda \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(\lambda\mathfrak{m}) \subset \mathbb{Z}\}.$$

Fröhlich defined in [2] an order $\mathcal{O}$ to be *weakly self-dual* if every proper $\mathcal{O}$-ideal is an invertible $\mathcal{O}$-ideal. He obtained the following necessary and sufficient condition for an order to be weakly self-dual (cf. [2, Theorem 10]).

LEMMA 1.3. *Let $\mathcal{O}$ be an order of K. Then $\mathcal{O}$ is weakly self-dual if and only if $\widehat{\mathcal{O}}$ is an invertible $\mathcal{O}$-ideal.*

Let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal. We take a positive integer $r \in \mathbb{Z}$ such that $r\mathfrak{a} \subset \mathcal{O}$. We define the *norm* of $\mathfrak{a}$ by

$$N_{\mathcal{O}}(\mathfrak{a}) = r^{-n}(\mathcal{O} : r\mathfrak{a}).$$

We claim that the norm is multiplicative provided that we restrict ourselves to invertible ideals. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two invertible $\mathcal{O}$-ideals. Then Lemma 1.1 and the multiplicativity of the norm of $\mathcal{O}_K$-ideals imply $N_{\mathcal{O}}(\mathfrak{a}\mathfrak{b}) = N_{\mathcal{O}}(\mathfrak{a})N_{\mathcal{O}}(\mathfrak{b})$.

Let $\Phi(u,v)$ be a binary form of degree n with coefficients in $\mathbb{Z}$. We assume that $\Phi(u,v)$ is irreducible over $\mathbb{Q}$. Hence the discriminant $D(\Phi)$ of $\Phi(u,v)$ is not zero. We write

$$\Phi(u,v) = a_0u^n + a_1u^{n-1}v + \ldots + a_nv^n, \qquad a_j \in \mathbb{Z},\ a_0 \neq 0.$$

Let θ be a root of the equation $\Phi(u,1) = 0$ and put $K = \mathbb{Q}(\theta)$. Then K is an algebraic number field of degree n over $\mathbb{Q}$. Further we put $\omega_0 = 1$, $\omega_1 = a_0\theta$,

$$\omega_i = \sum_{k=0}^{i-1} a_k\theta^{i-k} \qquad (i = 2,\ldots,n-1)$$

and denote by $\mathcal{O}_\Phi$ the lattice of K generated by $\{\omega_i \mid 0 \le i \le n-1\}$. It is easy to see that $D(\mathcal{O}_\Phi) = D(\Phi)$. Since

$$\omega_i = \theta(\omega_{i-1} + a_{i-1}) \qquad (2 \le i \le n-1),$$

$$\theta\omega_j = \omega_{j+1} - (a_j/a_0)\omega_1 \quad (1 \le j \le n-2),$$
$$\theta\omega_{n-1} = -a_n - a_{n-1}\theta,$$

we have

$$\begin{aligned}\omega_1\omega_j &= a_0\theta\omega_j = a_0\omega_{j+1} - a_j\omega_1,\\ \omega_i\omega_j &= (\omega_{i-1} + a_{i-1})\theta\omega_j\\ &= \omega_{i-1}\omega_{j+1} + a_{i-1}\omega_{j+1} - a_j\omega_i \quad (2 \le i \le j \le n-1).\end{aligned}$$

Here we put $\omega_n = -a_n$. Hence we see that $\mathcal{O}_\Phi$ is an order of K. This is the order used by Birch and Merriman in [1]. By Proposition 1.1 of [6], $\mathrm{Tr}_{K/\mathbb{Q}}\,\omega_j = -ja_j$ for $1 \le j \le n-1$. We define an $\mathcal{O}_\Phi$-ideal $\mathfrak{j}$ by

$$\mathfrak{j} = \mathcal{O}_\Phi + \theta\mathcal{O}_\Phi. \tag{1.2}$$

This is a special case of the ideal $\mathfrak{j}$ used in [5]. A basis of $\mathfrak{j}$ is given by

Lemma 1.4. *If $n \ge 3$, then $\mathfrak{j} = [1, \theta, \omega_2, \ldots, \omega_{n-1}]$. If $n = 2$, then $\mathfrak{j} = [1, \theta]$.*

Proof. Assume $n \ge 3$. It is obvious that $\mathfrak{j} \supset [1, \theta, \omega_2, \ldots, \omega_{n-1}]$. Since

$$\theta\omega_j = \omega_{j+1} - a_j\theta, \quad j = 1, \ldots, n-2, \quad \theta\omega_{n-1} = -a_n - a_{n-1}\theta, \tag{1.3}$$

we have $\theta\mathcal{O}_\Phi \subset [1, \theta, \omega_2, \ldots, \omega_{n-1}]$. Also, $\mathcal{O}_\Phi = [1, \omega_1, \ldots, \omega_{n-1}] \subset [1, \theta, \omega_2, \ldots, \omega_{n-1}]$. Hence $\mathfrak{j} \subset [1, \theta, \omega_2, \ldots, \omega_{n-1}]$. This proves the assertion for $n \ge 3$. The assertion for $n = 2$ can be proved similarly. ∎

We next check whether $\mathfrak{j}$ is a proper $\mathcal{O}_\Phi$-ideal.

Lemma 1.5. *If $n \ge 3$, then $\mathfrak{j}$ is a proper $\mathcal{O}_\Phi$-ideal. For $n = 2$, $\mathfrak{j}$ is a proper $\mathcal{O}_\Phi$-ideal if and only if $\Phi(u, v)$ is primitive.*

Proof. It is obvious that $\mathcal{O}_\Phi \subset \mathcal{O}(\mathfrak{j})$. Since $\mathfrak{j} = \mathcal{O}_\Phi + \theta\mathcal{O}_\Phi$, $\lambda \in \mathcal{O}(\mathfrak{j})$ if and only if $\lambda \in \mathfrak{j}$ and $\lambda\theta \in \mathfrak{j}$. We first assume $n \ge 3$. Take an element $\lambda \in \mathcal{O}(\mathfrak{j})$. Since $\lambda \in \mathfrak{j}$, Lemma 1.4 implies

$$\lambda = c_0 + c_1\theta + \sum_{j=2}^{n-1} c_j\omega_j$$

for some $c_j \in \mathbb{Z}$. Since $\mathcal{O}_\Phi \subset \mathcal{O}(\mathfrak{j})$, we have $c_1\theta \in \mathcal{O}(\mathfrak{j})$. Hence we have

$$(c_1\theta)\theta = a_0^{-1}c_1(a_0\theta^2 + a_1\theta) - a_0^{-1}a_1c_1\theta = a_0^{-1}c_1\omega_2 - a_0^{-1}a_1c_1\theta \in \mathfrak{j}.$$

This implies $a_0 \mid c_1$, hence $\lambda \in \mathcal{O}_\Phi$. Thus $\mathcal{O}(\mathfrak{j}) = \mathcal{O}_\Phi$. We next assume $n = 2$. Take an element $\lambda \in \mathcal{O}(\mathfrak{j})$ and write $\lambda = c_0 + c_1\theta$ for some $c_0, c_1 \in \mathbb{Z}$. Then $c_1\theta = \lambda - c_0 \in \mathcal{O}(\mathfrak{j})$. Hence

$$(c_1\theta)\theta = -a_0^{-1}c_1(a_1\theta + a_2) = -a_0^{-1}a_2c_1 - a_0^{-1}a_1c_1\theta \in \mathfrak{j}.$$

This implies $c_1 \equiv 0 \pmod{a_0/d}$, where d is the greatest common divisor of a_0, a_1 and a_2. Hence $\mathcal{O}(\mathfrak{j}) = \mathcal{O}_\Phi$ if and only if $d = 1$. ∎

We now verify whether $\mathfrak{j}$ is an invertible $\mathcal{O}_\Phi$-ideal. We determine

$$\mathfrak{j}^{-1} = \{\lambda \in K \mid \lambda\mathfrak{j} \subset \mathcal{O}_\Phi\}.$$

Since $\mathfrak{j} = \mathcal{O}_\Phi + \theta\mathcal{O}_\Phi$, we see that $\lambda \in \mathfrak{j}^{-1}$ is equivalent to $\lambda \in \mathcal{O}_\Phi$ and $\lambda\theta \in \mathcal{O}_\Phi$. Take an element $\lambda \in \mathcal{O}_\Phi$ and write

$$\lambda = c_0 + \sum_{j=1}^{n-1} c_j(\omega_j + a_j), \qquad c_j \in \mathbb{Z}.$$

Since $\theta(\omega_j + a_j) = \omega_{j+1}$ for $1 \le j \le n-2$ and $\theta(\omega_{n-1} + a_{n-1}) = -a_n$, we have

$$\lambda\theta = c_0\theta - a_n c_{n-1} + \sum_{j=1}^{n-2} c_j\omega_{j+1}.$$

This implies that $\lambda\theta \in \mathcal{O}_\Phi$ if and only if $a_0 \mid c_0$. Hence

$$\mathfrak{j}^{-1} = [a_0, \omega_1 + a_1, \ldots, \omega_{n-1} + a_{n-1}]. \tag{1.4}$$

LEMMA 1.6. *Let m be the greatest common divisor of $a_0, \ldots, a_n$. Then*

$$\mathfrak{j}\mathfrak{j}^{-1} = [m, \omega_1, \ldots, \omega_{n-1}].$$

In particular, $\mathfrak{j}$ *is an invertible $\mathcal{O}_\Phi$-ideal if and only if Φ is primitive.*

Proof. Since $\mathfrak{j}^{-1}$ is an $\mathcal{O}_\Phi$-ideal, we have

$$\mathfrak{j}\mathfrak{j}^{-1} = (\mathcal{O}_\Phi + \theta\mathcal{O}_\Phi)\mathfrak{j}^{-1} = \mathfrak{j}^{-1} + \theta\mathfrak{j}^{-1}.$$

By (1.3) and (1.4),

$$\begin{aligned} \mathfrak{j}^{-1} &= [a_0, \omega_1 + a_1, \ldots, \omega_{n-1} + a_{n-1}], \\ \theta\mathfrak{j}^{-1} &= [\omega_1, \omega_2, \ldots, \omega_{n-1}, -a_n]. \end{aligned}$$

Hence $\mathfrak{j}\mathfrak{j}^{-1} = [m, \omega_1, \ldots, \omega_{n-1}]$. ■

We next determine the dual ideal $\widehat{\mathfrak{j}}$. Since $\Phi(\theta, 1) = 0$, (1.3) implies

$$(u - \theta)\Big(a_0u^{n-1} + \sum_{j=1}^{n-1}(\omega_j + a_j)u^{n-1-j}\Big) = \Phi(u, 1). \tag{1.5}$$

For $\alpha \in K$, we denote by $\alpha^{(i)}$, $i = 1, \ldots, n$, the conjugates of α over $\mathbb{Q}$. We put $\delta = \frac{\partial\Phi}{\partial u}(\theta, 1)$. Then $\delta \ne 0$ and

$$N_{K/\mathbb{Q}}\,\delta = (-1)^{n(n-1)/2}a_0^{2-n}D(\Phi).$$

We put $\eta_j = \omega_{n-1-j} + a_{n-1-j}$, $0 \le j \le n-2$ and $\eta_{n-1} = a_0$. By (1.5) and Lagrange's interpolation formula, we have

$$\operatorname{Tr}_{K/\mathbb{Q}}(\delta^{-1}\theta^i\eta_j) = \begin{cases} 1, & i = j, \\ 0, & i \ne j. \end{cases}$$

Since $\mathcal{O}_\Phi = [1, \eta_{n-2}, \ldots, \eta_0]$, we have

$$\widehat{\mathcal{O}}_\Phi = \delta^{-1}[1, \theta, \ldots, \theta^{n-2}, a_0\theta^{n-1}]. \tag{1.6}$$

A simple calculation yields

LEMMA 1.7. *If* $n \geq 3$, *then*

$$\widehat{\mathfrak{j}} = \delta^{-1}[1, \theta, \ldots, \theta^{n-3}, a_0\theta^{n-2}, a_0\theta^{n-1} + a_1\theta^{n-2}].$$

In particular, $\widehat{\mathfrak{j}} = \delta^{-1}\mathcal{O}_\Phi$ *if* $n = 3$. *If* $n = 2$, *then* $\widehat{\mathfrak{j}} = \delta^{-1}[a_0, a_0\theta + a_1]$.

We shall show that the order $\mathcal{O}_\Phi$ is weakly self-dual if Φ is primitive. To prove it, we need

LEMMA 1.8. $\widehat{\mathcal{O}}_\Phi = \delta^{-1}\mathfrak{j}^{n-2}$.

Proof. For $1 \leq k \leq n-2$, we show

$$\mathfrak{j}^k = [1, \theta, \ldots, \theta^k, \omega_{k+1}, \ldots, \omega_{n-1}] \tag{1.7}$$

by induction on k. It follows from Lemma 1.4 that the equation above is true for $k = 1$. Let $1 \leq k < n-2$ and assume that (1.7) holds. Since

$$\mathfrak{j}^{k+1} = \mathfrak{j}^k(\mathcal{O}_\Phi + \theta\mathcal{O}_\Phi) = \mathfrak{j}^k + \theta\mathfrak{j}^k,$$

we have

$$\mathfrak{j}^{k+1} = [1, \theta, \ldots, \theta^k, \omega_{k+1}, \ldots, \omega_{n-1}] + [\theta, \theta^2, \ldots, \theta^{k+1}, \theta\omega_{k+1}, \ldots, \theta\omega_{n-1}].$$

Then it follows from (1.3) that

$$\mathfrak{j}^{k+1} = [1, \theta, \ldots, \theta^{k+1}, \omega_{k+2}, \ldots, \omega_{n-1}].$$

Hence (1.7) holds for $1 \leq k \leq n-2$. The case $k = n-2$ of (1.7) and (1.6) imply $\widehat{\mathcal{O}}_\Phi = \delta^{-1}\mathfrak{j}^{n-2}$. ■

By Lemmas 1.3, 1.6 and 1.8, we have

PROPOSITION 1.9. *If* Φ *is primitive*, *then the order* $\mathcal{O}_\Phi$ *is weakly self-dual.*

REMARK 1.10. It is known that an order $\mathcal{O}$ of a number field of degree n over $\mathbb{Q}$ is weakly self-dual if one of the following conditions holds (cf. [2]):

(i) $n = 2$.
(ii) $\mathcal{O} = \mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K$.
(iii) $(\mathcal{O}_K : \mathcal{O})$ is a square-free integer.

2. Results of Morales. In this section, we follow the argument of Morales in [5] and study what can be said about pairs of symmetric matrices $x = (x_1, x_2)$ with coefficients in $\mathbb{Z}$ such that $\Phi_x(u, v)$ is not necessarily primitive.

Let $x = (x_1, x_2)$ be a pair of symmetric matrices of degree n with coefficients in $\mathbb{Z}$. We define a binary form $\Phi_x(u,v)$ by (0.1). We assume that $\Phi_x(u,v)$ is irreducible over $\mathbb{Q}$. We write

$$\Phi_x(u,v) = a_0u^n + a_1u^{n-1}v + \ldots + a_nv^n, \quad a_j \in \mathbb{Z},\ a_0 \neq 0.$$

Let θ be a root of the equation $\Phi_x(u,1) = 0$ and put $K = \mathbb{Q}(\theta)$. Let $m > 0$ be the greatest common divisor of a_j's and write $\Phi_x(u,v) = m\Phi_1(u,v)$ with $\Phi_1(u,v)$ primitive. We put $\Lambda_1 = \mathcal{O}_{\Phi_1}$. Let $V = \mathbb{Q}^n$ be the vector space of rational column vectors and let $M = \mathbb{Z}^n$ be the lattice of V of integral vectors. We define a homomorphism $\varrho_x : K \to \mathrm{End}_{\mathbb{Q}}(V)$ by

$$\varrho_x(\theta)\boldsymbol{v} = -x_1^{-1}x_2\boldsymbol{v}, \quad \boldsymbol{v} \in V. \tag{2.1}$$

Then V is a free K-module of rank 1 via ϱ_x. We fix a non-zero vector $\boldsymbol{v} \in V$ and put

$$\mathfrak{a} = \mathfrak{a}_x = \{\alpha \in K \mid \varrho_x(\alpha)\boldsymbol{v} \in M\},$$
$$\Lambda = \Lambda_x = \{\lambda \in K \mid \varrho_x(\lambda)M \subset M\}.$$

Then $\mathfrak{a}$ is a lattice of K. Since $\Lambda = \mathcal{O}(\mathfrak{a})$, Λ is an order of K and $\mathfrak{a}$ is a proper Λ-ideal. If we take another non-zero vector $\boldsymbol{v}'$, then we have $\boldsymbol{v}' = \varrho_x(c)\boldsymbol{v}$ for some $c \in K^\times$. Hence the ideal $\mathfrak{a}$ is replaced by

$$\mathfrak{a}' = \{\alpha \in K \mid \varrho_x(\alpha)\boldsymbol{v}' \in M\} = c^{-1}\mathfrak{a},$$

while the order Λ is unchanged. We write $M = M_x$ to indicate that M_x has the Λ-module structure via ϱ_x. The following lemma is due to Morales.

Lemma 2.1. *Put* $\varphi(T) = a_0^{-1}\Phi_x(T,1)$ *and* $\mathfrak{J} = \mathcal{O}_K + \theta\mathcal{O}_K$. *Then* $N(\mathfrak{J})^{-1}\varphi(T)$ *is a primitive polynomial in* $\mathbb{Z}[T]$.

We follow the argument of Morales to describe a relation between the pair $x = (x_1, x_2)$ and the ideal $\mathfrak{a}_x$. The trace form $\mathrm{Tr}_{K/\mathbb{Q}}$ induces an isomorphism of Λ-modules

$$\mathrm{Hom}_\Lambda(M_x, \widehat{\Lambda}) \cong \mathrm{Hom}_{\mathbb{Z}}(M_x, \mathbb{Z}).$$

Hence there exists a unique Λ-bilinear form $B_x : M_x \times M_x \to \widehat{\Lambda}$ such that

$$x_1 = (\mathrm{Tr}_{K/\mathbb{Q}} B_x(e_i, e_j)), \quad x_2 = -(\mathrm{Tr}_{K/\mathbb{Q}}\theta B_x(e_i, e_j)), \tag{2.2}$$

where $\{e_1, \ldots, e_n\}$ is the standard basis of $M_x = \mathbb{Z}^n$, i.e. the jth component of e_i is 1 if $j = i$, and 0 otherwise. Since $B_x(e_i, e_j) \in \widehat{\Lambda}$ and $\theta B_x(e_i, e_j) \in \widehat{\Lambda}$ for any i, j, we have $B_x(M_x, M_x) \subset \widehat{\Lambda} \cap \theta^{-1}\widehat{\Lambda}$. We put $\mathfrak{j} = \Lambda + \theta\Lambda$. Then $\widehat{\mathfrak{j}} = \widehat{\Lambda} \cap \theta^{-1}\widehat{\Lambda}$. We take $\alpha_i \in \mathfrak{a}$ such that $\varrho_x(\alpha_i)\boldsymbol{v} = e_i$ for $i = 1, \ldots, n$. Then $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of $\mathfrak{a}$ and $B_x(e_i, e_j) = \alpha_i\alpha_j\beta$, where we put $\beta = \beta_x = B_x(\boldsymbol{v}, \boldsymbol{v})$. Thus we have $\beta\mathfrak{a}^2 \subset \widehat{\mathfrak{j}}$.

We now study how $B_x(M_x, M_x)$ changes if we replace x by y which is Γ-equivalent to x. Take an element $\gamma \in \Gamma$ and put $y = (y_1, y_2)$, $y_k = \gamma x_k {}^{\mathrm{t}}\gamma$, $k = 1, 2$. Then we have $\varrho_y(\theta) = -y_1^{-1}y_2 = {}^{\mathrm{t}}\gamma^{-1}\varrho_x(\theta)\,{}^{\mathrm{t}}\gamma$. Hence $\varrho_y(\alpha) =$

${}^{\mathrm{t}}\gamma^{-1}\varrho_x(\alpha)\,{}^{\mathrm{t}}\gamma$ for any $\alpha \in K$. If we define $f : V_y \to V_x$ by $f(a) = {}^{\mathrm{t}}\gamma a$, $a \in V_y$, then f is an isomorphism of K-modules. It is obvious that $\Phi_y = \Phi_x$, $\Lambda_y = \Lambda_x = \Lambda$ and f induces an isomorphism $M_y \cong M_x$ of Λ-modules. Put

$$\mathfrak{a}_y = \{\alpha \in K \mid \varrho_y(\alpha)\boldsymbol{v} \in M\}.$$

There exists an element $c \in K^\times$ such that $f(\boldsymbol{v}) = \varrho_x(c)\boldsymbol{v}$. Then $\mathfrak{a}_y = c^{-1}\mathfrak{a}_x$. If we define $B' : M_y \times M_y \to \widehat{\Lambda}$ by $B'(a,b) = B_x(f(a), f(b))$ for $a, b \in M_y$, then B' is a Λ-bilinear form. It is easy to see that

$$(\mathrm{Tr}_{K/\mathbb{Q}}\, B'(e_i,e_j)) = \gamma(\mathrm{Tr}_{K/\mathbb{Q}} B_x(e_i,e_j))^{\mathrm{t}}\gamma = \gamma x_1{}^{\mathrm{t}}\gamma = y_1,$$
$$-(\mathrm{Tr}_{K/\mathbb{Q}}\theta B'(e_i,e_j)) = -\gamma(\mathrm{Tr}_{K/\mathbb{Q}}\theta B_x(e_i,e_j))^{\mathrm{t}}\gamma = \gamma x_2{}^{\mathrm{t}}\gamma = y_2.$$

Hence $B' = B_y$. If we put $e'_i = \varrho_y(\alpha_i c^{-1})\boldsymbol{v}$, $i = 1, \ldots, n$, then $f(e'_i) = \varrho_x(\alpha_i)\boldsymbol{v} = e_i$. Hence $\{e'_1, \ldots, e'_n\}$ is a basis of M_y and $\{\alpha_1 c^{-1}, \ldots, \alpha_n c^{-1}\}$ is a basis of $\mathfrak{a}_y$. Since B_y is Λ-bilinear, we have $B_y(e'_i, e'_j) = \alpha_i\alpha_j c^{-2} B_y(\boldsymbol{v},\boldsymbol{v})$. On the other hand, $B_y = B'$ implies that $B_y(e'_i, e'_j) = B_x(e_i, e_j) = \alpha_i\alpha_j B_x(\boldsymbol{v},\boldsymbol{v})$. Thus $\beta_y = B_y(\boldsymbol{v},\boldsymbol{v}) = c^2\beta_x$ and

$$B_y(M_y, M_y) = \beta_y\mathfrak{a}_y^2 = c^2\beta_x(c^{-1}\mathfrak{a}_x)^2 = \beta_x\mathfrak{a}_x^2.$$

So we obtain

Lemma 2.2. *If we replace x by y which is Γ-equivalent to x, then there exists an element $c \in K^\times$ such that $\Lambda_y = \Lambda_x$, $\mathfrak{a}_y = c^{-1}\mathfrak{a}_x$ and $\beta_y = c^2\beta_x$. In particular, the submodule $\beta_x\mathfrak{a}_x^2$ of $\widehat{\mathfrak{j}}$ is unchanged.*

We next determine the index $(\widehat{\mathfrak{j}} : \beta_x\mathfrak{a}_x^2)$. There exists a matrix $R(\beta_x) \in \mathrm{GL}(n,\mathbb{Q})$ such that $\beta_x(\alpha_1, \ldots, \alpha_n) = (\alpha_1, \ldots, \alpha_n)R(\beta_x)$. We have $\det R(\beta_x) = N_{K/\mathbb{Q}}\,\beta_x$ and

$$x_1 = (\mathrm{Tr}_{K/\mathbb{Q}}(\beta_x\alpha_i\alpha_j)) = (\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))R(\beta_x).$$

Hence $a_0 = \det x_1 = D(\mathfrak{a}_x)N_{K/\mathbb{Q}}\,\beta_x$. This implies

$$\Phi_1(1,0)D_K N_{K/\mathbb{Q}}\,\beta_x > 0. \tag{2.3}$$

Since $\mathfrak{J} = \mathcal{O}_K\mathfrak{j}$, Lemma 2.1 implies that $(\mathfrak{J} : \mathcal{O}_K)a_0^{-1}m\Phi_1(T,1)$ is a primitive polynomial in $\mathbb{Z}[T]$. Hence

$$m(\mathfrak{J} : \mathcal{O}_K) = |N_{K/\mathbb{Q}}\,\beta_x| \cdot |D(\mathfrak{a}_x)|. \tag{2.4}$$

Since $\widehat{\mathfrak{J}} = \mathfrak{J}^{-1}\widehat{\mathcal{O}}_K$, we have

$$N(\widehat{\mathfrak{J}}) = N(\mathfrak{J})^{-1}N(\widehat{\mathcal{O}}_K) = (\mathfrak{J} : \mathcal{O}_K)(\widehat{\mathcal{O}}_K : \mathcal{O}_K)^{-1}.$$

By this equation and $(\widehat{\mathcal{O}}_K : \mathcal{O}_K) = |D_K|$, we have $N(\widehat{\mathfrak{J}}) = (\mathfrak{J} : \mathcal{O}_K)|D_K|^{-1}$. The inclusion $\mathfrak{j} \subset \mathfrak{J}$ implies $\widehat{\mathfrak{j}} \supset \widehat{\mathfrak{J}}$, thus $\mathcal{O}_K\widehat{\mathfrak{j}} \supset \widehat{\mathfrak{J}}$. Hence

$$N(\mathcal{O}_K\widehat{\mathfrak{j}}) = N(\widehat{\mathfrak{J}})(\mathcal{O}_K\widehat{\mathfrak{j}} : \widehat{\mathfrak{J}})^{-1} = (\mathfrak{J} : \mathcal{O}_K)|D_K|^{-1}(\mathcal{O}_K\widehat{\mathfrak{j}} : \widehat{\mathfrak{J}})^{-1}. \tag{2.5}$$

If we put $\mathfrak{A} = \mathcal{O}_K\mathfrak{a}_x$, then $\beta_x\mathfrak{A}^2 \subset \mathcal{O}_K\widehat{\mathfrak{j}}$. This implies

$$\beta_x \mathfrak{A}^2 = (\mathcal{O}_K \widehat{\mathfrak{j}})\mathfrak{F} \tag{2.6}$$

for some integral $\mathcal{O}_K$-ideal $\mathfrak{F}$. The norm of the right hand side is given by

$$N(\beta_x \mathfrak{A}^2) = |N_{K/\mathbb{Q}}\,\beta_x| N(\mathfrak{A})^2 = |N_{K/\mathbb{Q}}\,\beta_x| \cdot |D(\mathfrak{A})| \cdot |D_K|^{-1}. \tag{2.7}$$

By (2.4)–(2.7), we have

$$\begin{aligned} N(\mathfrak{F}) &= \frac{(\mathcal{O}_K\widehat{\mathfrak{j}} : \widehat{\mathfrak{J}})|N_{K/\mathbb{Q}}\,\beta_x| \cdot |D(\mathfrak{A})|}{(\mathfrak{J} : \mathcal{O}_K)} = \frac{(\mathcal{O}_K\widehat{\mathfrak{j}} : \widehat{\mathfrak{J}})|N_{K/\mathbb{Q}}\,\beta_x| \cdot |D(\mathfrak{a}_x)|}{(\mathfrak{A} : \mathfrak{a}_x)^2(\mathfrak{J} : \mathcal{O}_K)} \\ &= \frac{(\mathcal{O}_K\widehat{\mathfrak{j}} : \widehat{\mathfrak{J}})m}{(\mathfrak{A} : \mathfrak{a}_x)^2} = \frac{(\mathcal{O}_K\widehat{\mathfrak{j}} : \widehat{\mathfrak{j}})(\widehat{\mathfrak{j}} : \widehat{\mathfrak{J}})m}{(\mathcal{O}_K\mathfrak{a}_x : \mathfrak{a}_x)^2} \\ &= \frac{(\mathcal{O}_K\widehat{\mathfrak{j}} : \widehat{\mathfrak{j}})(\mathcal{O}_K\mathfrak{j} : \mathfrak{j})m}{(\mathcal{O}_K\mathfrak{a}_x : \mathfrak{a}_x)^2} = \frac{a(\mathfrak{a}_x, \Lambda)^2\, m}{a(\mathfrak{j}, \Lambda)a(\widehat{\mathfrak{j}}, \Lambda)}. \end{aligned}$$

Here $a(\mathfrak{a}, \Lambda)$ is Fröhlich's invariant defined in Section 1. We also have

$$\begin{aligned} (\widehat{\mathfrak{j}} : \beta_x\mathfrak{a}_x^2) &= \frac{(\mathcal{O}_K\widehat{\mathfrak{j}} : \beta_x\mathfrak{A}^2)(\beta_x\mathfrak{A}^2 : \beta_x\mathfrak{a}_x^2)}{(\mathcal{O}_K\widehat{\mathfrak{j}} : \widehat{\mathfrak{j}})} = \frac{N(\mathfrak{F})(\mathcal{O}_K\mathfrak{a}_x^2 : \mathfrak{a}_x^2)}{(\mathcal{O}_K\widehat{\mathfrak{j}} : \widehat{\mathfrak{j}})} \\ &= \frac{(\mathcal{O}_K\mathfrak{j} : \mathfrak{j})(\mathcal{O}_K\mathfrak{a}_x^2 : \mathfrak{a}_x^2)m}{(\mathcal{O}_K\mathfrak{a}_x : \mathfrak{a}_x)^2} = \frac{a(\mathfrak{a}_x, \Lambda)^2\, m}{a(\mathfrak{a}_x^2, \Lambda)a(\mathfrak{j}, \Lambda)}. \end{aligned}$$

This yields

PROPOSITION 2.3. *There exists an integral $\mathcal{O}_K$-ideal $\mathfrak{F}$ such that $\beta_x\mathfrak{A}^2 = (\mathcal{O}_K\widehat{\mathfrak{j}})\mathfrak{F}$ with norm*

$$N(\mathfrak{F}) = \frac{a(\mathfrak{a}_x, \Lambda)^2\, m}{a(\mathfrak{j}, \Lambda)a(\widehat{\mathfrak{j}}, \Lambda)}.$$

The Λ-ideal $\beta_x\mathfrak{a}_x^2$ is a submodule of $\widehat{\mathfrak{j}}$ with index

$$(\widehat{\mathfrak{j}} : \beta_x\mathfrak{a}_x^2) = \frac{a(\mathfrak{a}_x, \Lambda)^2\, m}{a(\mathfrak{a}_x^2, \Lambda)a(\mathfrak{j}, \Lambda)}.$$

If Λ is weakly self-dual, then $\mathfrak{a}_x$ is an invertible Λ-ideal. Hence $a(\mathfrak{a}_x, \Lambda) = 1$ and $a(\mathfrak{a}_x^2, \Lambda) = 1$ by Lemma 1.1. Further if $m = 1$, then it was proved in [5] that $\mathfrak{j}$ and $\widehat{\mathfrak{j}}$ are invertible Λ-ideals and $\beta_x\mathfrak{a}_x^2 = \widehat{\mathfrak{j}}$.

COROLLARY 2.4. *If $\Lambda = \mathcal{O}_{\Phi_1}$, then $N(\mathfrak{F}) = (\widehat{\mathfrak{j}} : \beta_x\mathfrak{a}_x^2) = m$.*

Proof. Since Φ_1 is primitive, the order $\mathcal{O}_{\Phi_1}$ is weakly self-dual by Proposition 1.9. Then Lemma 1.3 implies that $\widehat{\mathcal{O}}_{\Phi_1}$ is an invertible $\mathcal{O}_{\Phi_1}$-ideal. The ideal $\mathfrak{j}$ is an invertible $\mathcal{O}_{\Phi_1}$-ideal by Lemma 1.6, hence so is $\widehat{\mathfrak{j}} = \mathfrak{j}^{-1}\widehat{\mathcal{O}}_{\Phi_1}$. The corollary now follows from Lemma 1.1 and Proposition 2.3. ■

As for the invariants $a(\mathfrak{j}, \Lambda)$ and $a(\widehat{\mathfrak{j}}, \Lambda)$, we have

LEMMA 2.5. *Let $n \geq 3$ and $c \in \mathbb{Z}$ be a positive divisor of m. If $\Lambda = \mathcal{O}_{c\Phi_1}$, then $a(\mathfrak{j}, \Lambda) = c$ and $a(\widehat{\mathfrak{j}}, \Lambda) = c^{n-3}$.*

Proof. Let $\Lambda = \mathcal{O}_{c\Phi_1}$ and $\Lambda_1 = \mathcal{O}_{\Phi_1}$. Let a'_j $(0 \le j \le n)$ be the coefficients of $\Phi_1(u,v)$ and let $\{1, \omega'_1, \ldots, \omega'_{n-1}\}$ be the corresponding basis for Λ_1. Then $\{1, c\omega'_1, \ldots, c\omega'_{n-1}\}$ is a basis for Λ. Hence $(\Lambda_1 : \Lambda) = c^{n-1}$. If we put $\mathfrak{j}_1 = \Lambda_1 + \theta\Lambda_1$, then $\mathfrak{j}_1 = \Lambda_1\mathfrak{j}$. By Lemma 1.4, we have

$$\mathfrak{j}_1 = [1, \theta, \omega'_2, \ldots, \omega'_{n-1}], \quad \mathfrak{j} = [1, \theta, c\omega'_2, \ldots, c\omega'_{n-1}].$$

Hence $(\mathfrak{j}_1 : \mathfrak{j}) = c^{n-2}$. Since Φ_1 is primitive, Λ_1 is weakly self-dual by Proposition 1.9. This implies

$$a(\mathfrak{j}, \Lambda) = \frac{(\mathcal{O}_K : \Lambda_1)(\Lambda_1 : \Lambda)}{(\mathcal{O}_K\mathfrak{j}_1 : \mathfrak{j}_1)(\mathfrak{j}_1 : \mathfrak{j})} = a(\mathfrak{j}_1, \Lambda_1)c.$$

By Lemmas 1.6 and 1.1, we have $a(\mathfrak{j}_1, \Lambda_1) = 1$, hence $a(\mathfrak{j}, \Lambda) = c$. Put $\delta_1 = \frac{\partial \Phi_1}{\partial u}(\theta, 1)$. By Lemma 1.7,

$$\begin{aligned}\widehat{\mathfrak{j}_1} &= \delta_1^{-1}[1, \theta, \ldots, \theta^{n-3}, \omega'_{n-2}, \omega'_{n-1}],\\ \widehat{\mathfrak{j}} &= (c\delta_1)^{-1}[1, \theta, \ldots, \theta^{n-3}, c\omega'_{n-2}, c\omega'_{n-1}].\end{aligned}$$

Thus $c\widehat{\mathfrak{j}} \subset \widehat{\mathfrak{j}_1}$, hence $c\Lambda_1\widehat{\mathfrak{j}} \subset \widehat{\mathfrak{j}_1}$. It is easy to see that $\omega'_j \in \Lambda_1[1, \theta, \ldots, \theta^{n-3}, c\omega'_{n-2}, c\omega'_{n-1}]$ for $j = n-2$, $n-1$. This implies $\widehat{\mathfrak{j}_1} \subset c\Lambda_1\widehat{\mathfrak{j}}$, hence $\widehat{\mathfrak{j}_1} = c\Lambda_1\widehat{\mathfrak{j}}$. So

$$\begin{aligned}a(\widehat{\mathfrak{j}}, \Lambda) &= \frac{(\mathcal{O}_K : \Lambda_1)(\Lambda_1 : \Lambda)}{(\mathcal{O}_K\widehat{\mathfrak{j}} : \Lambda_1\widehat{\mathfrak{j}})(\Lambda_1\widehat{\mathfrak{j}} : \widehat{\mathfrak{j}})} = \frac{(\mathcal{O}_K : \Lambda_1)c^{n-1}}{(\mathcal{O}_K c^{-1}\widehat{\mathfrak{j}_1} : c^{-1}\widehat{\mathfrak{j}_1})(c^{-1}\widehat{\mathfrak{j}_1} : \widehat{\mathfrak{j}})}\\ &= a(c^{-1}\widehat{\mathfrak{j}_1}, \Lambda_1)c^{n-3}.\end{aligned}$$

Since $\mathfrak{j}_1$ and $\widehat{\Lambda_1}$ are invertible Λ_1-ideals, so is $\widehat{\mathfrak{j}_1} = \mathfrak{j}_1^{-1}\widehat{\Lambda_1}$. Hence $a(c^{-1}\widehat{\mathfrak{j}_1}, \Lambda_1) = 1$, $a(\widehat{\mathfrak{j}}, \Lambda) = c^{n-3}$. ∎

LEMMA 2.6. *Let $n = 2$ and $c \in \mathbb{Z}$ be a positive divisor of m. If $\Lambda = \mathcal{O}_{c\Phi_1}$, then $a(\mathfrak{j}, \Lambda) = a(\widehat{\mathfrak{j}}, \Lambda) = c$.*

Proof. Let $\Lambda = \mathcal{O}_{c\Phi_1}$ and $\Lambda_1 = \mathcal{O}_{\Phi_1}$. Since $\mathfrak{j} = [1, \theta]$ and $\widehat{\Lambda_1}$ are invertible Λ_1-ideals, so is $\widehat{\mathfrak{j}} = \mathfrak{j}^{-1}\widehat{\Lambda_1}$. Hence

$$a(\mathfrak{j}, \Lambda) = a(\mathfrak{j}, \Lambda_1)(\Lambda_1 : \Lambda) = c, \quad a(\widehat{\mathfrak{j}}, \Lambda) = a(\widehat{\mathfrak{j}}, \Lambda_1)(\Lambda_1 : \Lambda) = c. \ ∎$$

Let $\Phi_1(u,v)$ be an integral primitive irreducible binary form of degree n and let m be a positive integer. Let θ be a root of the equation $\Phi_1(u,1) = 0$ and put $K = \mathbb{Q}(\theta)$. For any order Λ of K, we denote by $L(m\Phi_1, \Lambda)$ the set of pairs $x = (x_1, x_2)$ of symmetric matrices of degree n with coefficients in $\mathbb{Z}$ such that $\Phi_x = m\Phi_1$ and $\Lambda_x = \Lambda$. We denote by $h(m\Phi_1, \Lambda)$ the number of equivalence classes of pairs in $L(m\Phi_1, \Lambda)$. Put $\mathfrak{j} = \Lambda + \theta\Lambda$. We now assume that

(H) $\widehat{\mathfrak{j}}$ is an invertible Λ-ideal.

We do not assume that $\mathfrak{j}$ is an invertible Λ-ideal. We denote by $L_0(m\Phi_1, \Lambda)$ the subset of $L(m\Phi_1, \Lambda)$ consisting of all pairs $x \in L(m\Phi_1, \Lambda)$ such that $\mathfrak{a}_x$ is an invertible Λ-ideal. For any $x \in L_0(m\Phi_1, \Lambda)$, it follows from Proposition 2.3 that $\mathfrak{f}_x = \beta_x \mathfrak{a}_x^2 \widehat{\mathfrak{j}}^{-1}$ is an invertible Λ-ideal with $N_\Lambda(\mathfrak{f}_x) = m/a(\mathfrak{j}, \Lambda)$. For any invertible Λ-ideal $\mathfrak{a}$, we denote by $[\mathfrak{a}] \in \mathrm{Pic}^+(\Lambda)$ the ideal class of $\mathfrak{a}$. By (2.3),

$$[\mathfrak{f}_x] \in [\xi \widehat{\mathfrak{j}}] \mathrm{Pic}^+(\Lambda)^2, \tag{2.8}$$

where ξ is an arbitrary element of $K^\times$ satisfying $\Phi_1(1,0) D_K N_{K/\mathbb{Q}}\, \xi > 0$. For any positive integer f, we denote by $\omega_\Lambda(f)$ the set of all integral invertible Λ-ideals $\mathfrak{f}$ satisfying $N_\Lambda(\mathfrak{f}) = f$ and $[\mathfrak{f}] \in [\xi \widehat{\mathfrak{j}}]\mathrm{Pic}^+(\Lambda)^2$. Further we denote by $S(m\Phi_1, \Lambda)$ the subset of $I_\Lambda \times K^\times \times \omega_\Lambda(m/a(\mathfrak{j}, \Lambda))$ consisting of all $(\mathfrak{a}, \beta, \mathfrak{f})$ satisfying $\beta \mathfrak{a}^2 = \widehat{\mathfrak{j}}\mathfrak{f}$ and $\Phi_1(1,0) D_K N_{K/\mathbb{Q}}\, \beta > 0$. We define a subgroup $G(\Lambda)$ of $I_\Lambda \times K^\times$ by

$$G(\Lambda) = \{(\mathfrak{b}, c) \in I_\Lambda \times K^\times \mid N_{K/\mathbb{Q}}\, c > 0,\ c\mathfrak{b}^2 = \Lambda\}.$$

Then $G(\Lambda)$ acts on $S(m\Phi_1, \Lambda)$ by $(\mathfrak{b}, c)(\mathfrak{a}, \beta, \mathfrak{f}) = (\mathfrak{b}\mathfrak{a}, c\beta, \mathfrak{f})$. We define a subgroup $G_0(\Lambda)$ of $G(\Lambda)$ by $G_0(\Lambda) = \{(c^{-1}\Lambda, c^2) \mid c \in K^\times\}$. It is easy to see that

$$|G_0(\Lambda) \backslash S(m\Phi_1, \Lambda)| = (G(\Lambda) : G_0(\Lambda)) |\omega_\Lambda(m/a(\mathfrak{j}, \Lambda))|. \tag{2.9}$$

The index $(G(\Lambda) : G_0(\Lambda))$ is given by (cf. [5])

$$(G(\Lambda) : G_0(\Lambda)) = 2^{-r_0} (\Lambda^{(1)} : (\Lambda^{(1)})^2) |{}_2\mathrm{Pic}^+(\Lambda)|, \tag{2.10}$$

where ${}_2\mathrm{Pic}^+(\Lambda) = \{a \in \mathrm{Pic}^+(\Lambda) \mid a^2 = 1\}$, $\Lambda^{(1)}$ is the group of units ε in Λ with $N_{K/\mathbb{Q}}\, \varepsilon = 1$ and $r_0 = 0$ if either n is odd or K is totally imaginary, otherwise $r_0 = 1$.

PROPOSITION 2.7. *Assume the hypothesis* (H). *Then the mapping* $x \mapsto (\mathfrak{a}_x, \beta_x, \mathfrak{f}_x)$ *induces a bijection* $\Gamma \backslash L_0(m\Phi_1, \Lambda) \to G_0(\Lambda) \backslash S(m\Phi_1, \Lambda)$. *In particular, the number of* Γ*-equivalence classes of pairs in* $L_0(m\Phi_1, \Lambda)$ *is equal to* $2^{-r_0}(\Lambda^{(1)} : (\Lambda^{(1)})^2)|{}_2\mathrm{Pic}^+(\Lambda)| \cdot |\omega_\Lambda(m/a(\mathfrak{j}, \Lambda))|$.

Proof. Let $x \in L_0(m\Phi_1, \Lambda)$ and $\gamma \in \Gamma$. By Lemma 2.2,

$$(\mathfrak{a}_{\gamma x}, \beta_{\gamma x}, \mathfrak{f}_{\gamma x}) = (c^{-1}\mathfrak{a}_x, c^2\beta_x, \mathfrak{f}_x) = (c^{-1}\Lambda, c^2)(\mathfrak{a}_x, \beta_x, \mathfrak{f}_x)$$

for some $c \in K^\times$. Hence $x \mapsto (\mathfrak{a}_x, \beta_x, \mathfrak{f}_x)$ induces a mapping of $\Gamma \backslash L_0(m\Phi_1, \Lambda)$ to $G_0(\Lambda) \backslash S(m\Phi_1, \Lambda)$. To prove the injectivity, take $x, y \in L_0(m\Phi_1, \Lambda)$ and assume $(\mathfrak{a}_y, \beta_y, \mathfrak{f}_y) = (c^{-1}\mathfrak{a}_x, c^2\beta_x, \mathfrak{f}_x)$ for some $c \in K^\times$. Take a basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathfrak{a}_x$ such that $\varrho_x(\alpha_i)\boldsymbol{v} = e_i$. We also take a basis $\{\alpha'_1, \ldots, \alpha'_n\}$ of $\mathfrak{a}_y$ such that $\varrho_y(\alpha'_i)\boldsymbol{v} = e_i$. Then

$$\begin{aligned} x_1 &= (\mathrm{Tr}_{K/\mathbb{Q}}(\beta_x \alpha_i \alpha_j)), & x_2 &= -(\mathrm{Tr}_{K/\mathbb{Q}}(\theta \beta_x \alpha_i \alpha_j)), \\ y_1 &= (\mathrm{Tr}_{K/\mathbb{Q}}(\beta_y \alpha'_i \alpha'_j)), & y_2 &= -(\mathrm{Tr}_{K/\mathbb{Q}}(\theta \beta_y \alpha'_i \alpha'_j)). \end{aligned}$$

Since $\{c^{-1}\alpha_1,\dots,c^{-1}\alpha_n\}$ is another basis of $\mathfrak{a}_y = c^{-1}\mathfrak{a}_x$, there exists an element $\gamma\in\Gamma$ such that ${}^{\mathrm{t}}(\alpha'_1,\dots,\alpha'_n)=\gamma\,{}^{\mathrm{t}}(c^{-1}\alpha_1,\dots,c^{-1}\alpha_n)$. Since $\beta_y = c^2\beta_x$, we have

$$(\beta_y\alpha'_i\alpha'_j)=\gamma(\beta_x\alpha_i\alpha_j)\,{}^{\mathrm{t}}\gamma,\qquad (\theta\beta_y\alpha'_i\alpha'_j)=\gamma(\theta\beta_x\alpha_i\alpha_j)\,{}^{\mathrm{t}}\gamma.$$

Hence $y_k=\gamma x_k{}^{\mathrm{t}}\gamma$ for $k=1,2$. This proves the injectivity.

To prove the surjectivity, take any $(\mathfrak{a},\beta,\mathfrak{f})\in S(m\Phi_1,\Lambda)$. Take a basis $\{\alpha_1,\dots,\alpha_n\}$ of $\mathfrak{a}$. Since $\mathfrak{f}$ is an integral invertible Λ-ideal satisfying $\beta\mathfrak{a}^2=\widehat{\mathfrak{j}}\mathfrak{f}$, we have $\beta\mathfrak{a}^2\subset\widehat{\mathfrak{j}}$, or $\beta\alpha_i\alpha_j\in\widehat{\mathfrak{j}}=\widehat{\Lambda}\cap\theta^{-1}\widehat{\Lambda}$. Hence

$$x_1=(\mathrm{Tr}_{K/\mathbb{Q}}(\beta\alpha_i\alpha_j)),\qquad x_2=-(\mathrm{Tr}_{K/\mathbb{Q}}(\theta\beta\alpha_i\alpha_j)) \tag{2.11}$$

are symmetric matrices with coefficients in $\mathbb{Z}$. We put $x=(x_1,x_2)$. We denote by $R:K\to\mathrm{GL}(n,\mathbb{Q})$ the regular representation of K with respect to the basis $\{\alpha_1,\dots,\alpha_n\}$. Then $\Phi_x(u,v)=(\det x_1)\det(u1_n-vR(\theta))$, where 1_n is the identity matrix of degree n. The multiplicativity of the norm of invertible Λ-ideals implies $|N_{K/\mathbb{Q}}\beta|N_\Lambda(\mathfrak{a})^2=N_\Lambda(\widehat{\mathfrak{j}})N_\Lambda(\mathfrak{f})$. The definition of x_1 implies $\det x_1=D(\mathfrak{a})N_{K/\mathbb{Q}}\beta$. Since $N_\Lambda(\mathfrak{f})=m/a(\mathfrak{j},\Lambda)$, we have

$$\begin{aligned}|\det x_1|&=\frac{mN_\Lambda(\widehat{\mathfrak{j}})|D(\mathfrak{a})|}{a(\mathfrak{j},\Lambda)N_\Lambda(\mathfrak{a})^2}=\frac{mN_\Lambda(\widehat{\mathfrak{j}})|D(\Lambda)|}{a(\mathfrak{j},\Lambda)}=\frac{m(\widehat{\Lambda}:\widehat{\mathfrak{j}})|D(\Lambda)|}{(\widehat{\Lambda}:\Lambda)a(\mathfrak{j},\Lambda)}\\&=\frac{m(\mathfrak{j}:\Lambda)}{a(\mathfrak{j},\Lambda)}=\frac{m(\mathcal{O}_K\mathfrak{j}:\Lambda)}{(\mathcal{O}_K:\Lambda)}=m(\mathcal{O}_K\mathfrak{j}:\mathcal{O}_K)=mN(\mathcal{O}_K\mathfrak{j})^{-1}.\end{aligned}$$

It follows from Lemma 2.1 that $\Phi_x(u,v)=\pm m\Phi_1(u,v)$. So the condition $\Phi_1(1,0)D_KN_{K/\mathbb{Q}}\beta>0$ implies $\Phi_x(u,v)=m\Phi_1(u,v)$. We have $\theta(\alpha_1,\dots,\alpha_n)=(\alpha_1,\dots,\alpha_n)R(\theta)$, hence $(\theta\beta\alpha_i\alpha_j)=(\beta\alpha_i\alpha_j)R(\theta)$. Taking trace yields $-x_2=x_1R(\theta)$, or $R(\theta)=-x_1^{-1}x_2=\varrho_x(\theta)$. Thus $R(\lambda)=\varrho_x(\lambda)$ for any $\lambda\in K$. We set $\boldsymbol{v}=R(\alpha_1)^{-1}e_1$. Then

$$\begin{aligned}(\alpha_1,\dots,\alpha_n)\varrho_x(\alpha_i)\boldsymbol{v}&=(\alpha_1,\dots,\alpha_n)R(\alpha_i)\boldsymbol{v}=(\alpha_1,\dots,\alpha_n)R(\alpha_i\alpha_1^{-1})R(\alpha_1)\boldsymbol{v}\\&=\alpha_i\alpha_1^{-1}(\alpha_1,\dots,\alpha_n)e_1=\alpha_i.\end{aligned}$$

Since $\varrho_x(\alpha_i)\boldsymbol{v}\in V=\mathbb{Q}^n$ and $\{\alpha_1,\dots,\alpha_n\}$ is a basis of V over $\mathbb{Q}$, we must have $\varrho_x(\alpha_i)\boldsymbol{v}=e_i$ for $i=1,\dots,n$. Hence $\mathfrak{a}_x=\mathfrak{a}$, $\beta_x=\beta$ and $\mathfrak{f}_x=\mathfrak{f}$. This proves the surjectivity. ∎

3. The case of $n=2$. In this section, we consider equivalence classes of pairs of symmetric matrices of degree 2 with coefficients in $\mathbb{Z}$. Let $\Phi_1(u,v)$ be an integral primitive irreducible binary quadratic form and let m be a positive integer. Let θ be a root of the quadratic equation $\Phi_1(u,1)=0$ and put $K=\mathbb{Q}(\theta)$. For any positive integer c, there exists a unique order $\mathcal{O}_{K,c}$ of K with $(\mathcal{O}_K:\mathcal{O}_{K,c})=c$. We note that every order of K is weakly self-dual. For any order Λ of K, let $L(m\Phi_1,\Lambda)$ and $L_0(m\Phi_1,\Lambda)$ be as in the previous section.

We now assume $L(m\Phi_1, \Lambda) \neq \emptyset$. Take a pair $x \in L(m\Phi_1, \Lambda)$. Since $(\det x_1)x_1^{-1}x_2$ is an integral matrix, we have $\mathcal{O}_{m\Phi_1} \subset \Lambda$. We put $\Lambda_1 = \mathcal{O}_{\Phi_1}$, $\mathfrak{j}_1 = \Lambda_1 + \theta\Lambda_1$ and $\mathcal{O} = \Lambda_1\Lambda$. Since $\mathfrak{j}_1 = [1, \theta] \subset \mathfrak{j} = \Lambda + \theta\Lambda$, we have $\mathfrak{j} = \mathcal{O}\mathfrak{j}_1$. Hence $\mathfrak{j}$ is an $\mathcal{O}$-ideal. Since $\mathfrak{j}_1$ is an invertible Λ_1-ideal by Lemma 1.6, we see that $\mathfrak{j} = \mathcal{O}\mathfrak{j}_1$ is an invertible $\mathcal{O}$-ideal. Write $\Lambda_1 = \mathcal{O}_{K,t}$, $\Lambda = \mathcal{O}_{K,c}$. Then $c \mid mt$. Since $\mathcal{O}$ is weakly self-dual, $\widehat{\mathfrak{j}}$ is an invertible $\mathcal{O}$-ideal. It is easy to see that $\mathcal{O} = \mathcal{O}_{K,d}$ with $d = \gcd(c, t)$. Put $c_1 = c/d$. By Proposition 2.3,

$$(\widehat{\mathfrak{j}} : \beta_x \mathfrak{a}_x^2) = \frac{m}{a(\mathfrak{j}, \Lambda)} = \frac{m}{a(\mathfrak{j}, \mathcal{O})(\mathcal{O} : \Lambda)} = \frac{m}{(\mathcal{O} : \Lambda)} = \frac{m}{c_1}.$$

If we put $\mathfrak{A}_x = \mathcal{O}\mathfrak{a}_x$, then $\beta_x\mathfrak{a}_x^2 \subset \beta_x\mathfrak{A}_x^2 \subset \widehat{\mathfrak{j}}$. Since $\mathfrak{a}_x$ is a proper Λ-ideal, it is an invertible Λ-ideal. Hence $\mathfrak{a}_x^2$ is an invertible Λ-ideal and $\mathfrak{A}_x^2$ is an invertible $\mathcal{O}$-ideal. So $(\mathcal{O}_K\mathfrak{a}_x^2 : \mathfrak{a}_x^2) = (\mathcal{O}_K : \Lambda)$ and $(\mathcal{O}_K\mathfrak{A}_x^2 : \mathfrak{A}_x^2) = (\mathcal{O}_K : \mathcal{O})$. Hence

$$(3.1) \qquad (\widehat{\mathfrak{j}} : \beta_x\mathfrak{A}_x^2) = \frac{(\widehat{\mathfrak{j}} : \beta_x\mathfrak{a}_x^2)}{(\beta_x\mathfrak{A}_x^2 : \beta_x\mathfrak{a}_x^2)} = \frac{(\widehat{\mathfrak{j}} : \beta_x\mathfrak{a}_x^2)}{(\mathcal{O} : \Lambda)} = \frac{m}{c_1^2}.$$

We now assume that m is a square-free integer. Then (3.1) implies $c_1 = 1$, $d = c$. Hence $\Lambda = \mathcal{O} \supset \Lambda_1$. Thus $\mathfrak{j}$ and $\widehat{\mathfrak{j}}$ are invertible Λ-ideals, and so is $\mathfrak{f}_x = \beta_x\mathfrak{a}_x^2\widehat{\mathfrak{j}}^{-1}$ with $N_\Lambda(\mathfrak{f}_x) = m$. By Proposition 2.7 and Dirichlet unit theorem, we have

THEOREM 3.1. *Let $\Phi_1(u, v)$ be an integral primitive irreducible binary quadratic form and let m be a square-free positive integer. Then*

$$h(m\Phi_1) = 2\sum_{\Lambda \supset \mathcal{O}_{\Phi_1}} |{}_2\mathrm{Pic}^+(\Lambda)| \cdot |\omega_\Lambda(m)|.$$

REMARK 3.2. By the definition, we have $\omega_\Lambda(m) = \emptyset$ if $D_K < 0$ and $\Phi_1(1, 0) > 0$.

REMARK 3.3. By Corollary III.4 in [4], the order of ${}_2\mathrm{Pic}^+(\Lambda)$ is given by

$$|{}_2\mathrm{Pic}^+(\Lambda)| = 2^{w(D)-1+l(D)},$$

where $w(D)$ is the number of distinct prime divisors of $D = D(\Lambda)$, and $l(D)$ is the integer defined by

$$l(D) = \begin{cases} 0 & \text{if } D \text{ is odd},\\ \mathrm{ord}_2(H^2(\mathrm{Gal}(K/\mathbb{Q}), \Lambda_2^\times)) - 1 & \text{if } D \text{ is even}. \end{cases}$$

Here $\Lambda_2 = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_2$. The group $H^2(\mathrm{Gal}(K/\mathbb{Q}), \Lambda_2^\times)$ is given by

$$H^2(\mathrm{Gal}(K/\mathbb{Q}), \Lambda_2^\times) \cong \begin{cases} \{1\} & \text{if } b = 0 \text{ and } a \le 1,\\ (\mathbb{Z}/4\mathbb{Z})^\times & \text{if } (b = 0 \text{ and } a = 2)\\ & \text{or } (b = 2 \text{ and } a \le 1)\\ & \text{or } (b = 3 \text{ and } a = 0),\\ (\mathbb{Z}/8\mathbb{Z})^\times & \text{in all other cases}, \end{cases}$$

where $a = \mathrm{ord}_2(\mathcal{O}_K : \Lambda)$ and $b = \mathrm{ord}_2 D_K$.

4. The case of $n = 3$. In this section, we consider equivalence classes of pairs of symmetric matrices of degree 3 with coefficients in $\mathbb{Z}$. Let

$$\Phi_1(u,v) = a_0u^3 + a_1u^2v + a_2uv^2 + a_3v^3$$

be an integral primitive irreducible binary cubic form and let m be a positive integer. Let θ be a root of the cubic equation $\Phi_1(u,1) = 0$. Put $\omega_1 = a_0\theta$, $\omega_2 = a_0\theta^2 + a_1\theta + a_2 = -a_3\theta^{-1}$ and $K = \mathbb{Q}(\theta)$. Note that this ω_2 is slightly different from the one in Section 1 (the difference is a_2). For any positive divisor c of m, we put $\Lambda_c = \mathcal{O}_{c\Phi_1}$ and $\mathfrak{j}_c = \Lambda_c + \theta\Lambda_c$. We assume that m is a square-free positive integer and $\mathcal{O}_{\Phi_1} = \mathcal{O}_K$. For any order Λ of K, let $L(m\Phi_1,\Lambda)$ and $L_0(m\Phi_1,\Lambda)$ be as in Section 2.

We assume $L(m\Phi_1,\Lambda) \neq \emptyset$. Take a pair $x \in L(m\Phi_1,\Lambda)$. We write $\mathfrak{a} = \mathfrak{a}_x$, $\beta = \beta_x$ and $\mathfrak{j} = \Lambda + \theta\Lambda$. Since $(\det x_1)x_1^{-1}x_2$ and $(\det x_2)x_2^{-1}x_1$ are integral matrices, we have $\Lambda_m \subset \Lambda \subset \Lambda_1 = \mathcal{O}_K$. Hence $(\mathcal{O}_K : \Lambda)|(\Lambda_1 : \Lambda_m) = m^2$.

Suppose that there exists a prime divisor p of m which exactly divides the index $(\mathcal{O}_K : \Lambda)$. Then $(\mathcal{O}_{K,p}\mathfrak{a}_p : \mathfrak{a}_p)|(\mathcal{O}_{K,p} : \Lambda_p) = p$. Here the subscript p means tensor product with the p-adic integers $\mathbb{Z}_p$. Since $\mathfrak{a}$ is a proper Λ-ideal, we have $\mathcal{O}_{K,p}\mathfrak{a}_p \supsetneq \mathfrak{a}_p$. Hence $(\mathcal{O}_{K,p}\mathfrak{a}_p : \mathfrak{a}_p) = p$. It follows from the local version of Lemma 1.1 that $\mathfrak{a}_p$ is an invertible Λ_p-ideal. For a $\mathbb{Z}_p$-basis of Λ_p, we can take $\{1, p\omega_1, b\omega_1 + \omega_2\}$ if $p \nmid a_0$, $\Phi_1(b,1) \equiv 0 \bmod p$, or $\{1, \omega_1, p\omega_2\}$ if $p \,|\, a_0$. It is easy to see that $\mathfrak{j}_p = \mathfrak{j}_{1,p}$ in both cases. So we have $(\mathcal{O}_{K,p}\mathfrak{j}_p : \mathfrak{j}_p) = 1$, hence $(\mathcal{O}_{K,p}\widehat{\mathfrak{j}}_p : \widehat{\mathfrak{j}}_p) = 1$. By Proposition 2.3, the integral $\mathcal{O}_K$-ideal $\mathfrak{F}$ has norm $\frac{a(\mathfrak{a},\Lambda)m}{a(\mathfrak{j},\Lambda)a(\widehat{\mathfrak{j}},\Lambda)}$, which is not a p-adic integer. This is a contradiction.

Thus $p \nmid (\mathcal{O}_K : \Lambda)$ or $p^2 \,|\, (\mathcal{O}_K : \Lambda)$ for any prime divisor p of m. If $p \nmid (\mathcal{O}_K : \Lambda)$, then $\Lambda_p = \mathcal{O}_{K,p}$, hence $\mathfrak{a}_p$, $\mathfrak{j}_p$ and $\widehat{\mathfrak{j}}_p$ are invertible Λ_p-ideals. By Proposition 2.3, p exactly divides the index $(\widehat{\mathfrak{j}} : \beta\mathfrak{a}^2)$. We now assume $p^2 \,|\, (\mathcal{O}_K : \Lambda)$. Then $\Lambda_p = \Lambda_{m,p}$ and $\mathfrak{j}_p = \mathfrak{j}_{m,p}$. It follows from Lemma 1.7 that $\widehat{\mathfrak{j}}_p = \widehat{\mathfrak{j}}_{m,p}$ is a principal Λ_p-ideal, hence it is an invertible Λ_p-ideal. Since $(\mathcal{O}_{K,p}\mathfrak{a}_p : \mathfrak{a}_p)|(\mathcal{O}_{K,p} : \Lambda_p) = p^2$ and $\mathfrak{a}$ is a proper Λ-ideal, $(\mathcal{O}_{K,p}\mathfrak{a}_p : \mathfrak{a}_p) = p$ or p^2.

Suppose $(\mathcal{O}_{K,p}\mathfrak{a}_p : \mathfrak{a}_p) = p$. Then $\mathfrak{a}_p$ is not an invertible Λ_p-ideal. By the local version of Lemma 1.2, we have $(\mathcal{O}_{K,p}\mathfrak{a}_p^2 : \mathfrak{a}_p^2) = 1$. Hence $\mathfrak{a}_p^2$ is an $\mathcal{O}_{K,p}$-ideal. By Proposition 2.3 and Lemma 2.5, we have $\beta\mathfrak{a}_p^2 = \widehat{\mathfrak{j}}_p$. We have seen that $\beta\mathfrak{a}_p^2$ is an $\mathcal{O}_{K,p}$-ideal, while $\widehat{\mathfrak{j}}_p$ is a principal Λ_p-ideal. This is a contradiction.

Thus we must have $(\mathcal{O}_{K,p}\mathfrak{a}_p : \mathfrak{a}_p) = p^2$, hence $\mathfrak{a}_p$ is an invertible Λ_p-ideal. We also have $\beta\mathfrak{a}_p^2 = \widehat{\mathfrak{j}}_p$. Let f be the product of the prime divisors p of m with $p \nmid (\mathcal{O}_K : \Lambda)$ and let c be that of p with $p^2 \,|\, (\mathcal{O}_K : \Lambda)$. Then $m = cf$,

$(\widehat{\mathfrak{j}} : \beta\mathfrak{a}^2) = f$ and $(\mathcal{O}_K : \Lambda) = c^2$. Since $m\omega_i \in \Lambda$, $c^2\omega_i \in \Lambda$ and c is prime to f, we have $c\omega_i \in \Lambda$ for $i = 1, 2$. Hence $\Lambda = [1, c\omega_1, c\omega_2] = \Lambda_c$. It is obvious that $\mathfrak{a}_p$ is an invertible Λ_p-ideal for any prime number p with $p \nmid m$. So $\mathfrak{a}_p$ is an invertible Λ_p-ideal for all prime numbers p, hence $\mathfrak{a}$ is an invertible Λ-ideal. Thus $L_0(m\Phi_1, \Lambda) = L(m\Phi_1, \Lambda)$. By Proposition 2.7 and the Dirichlet unit theorem, we have

THEOREM 4.1. *Let $\Phi_1(u, v)$ be an integral primitive irreducible binary cubic form and let m be a square-free positive integer. Assume that $\mathcal{O}_{\Phi_1}$ is equal to the maximal order $\mathcal{O}_K$ of a cubic field K. Then*

$$h(m\Phi_1) = 2^r \sum_{cf=m} |{}_2\mathrm{Pic}^+(\Lambda_c)| \cdot |\omega_{\Lambda_c}(f)|,$$

where $\Lambda_c = \mathcal{O}_{c\Phi_1}$, $r = 1$ if $D_K < 0$ and $r = 2$ if $D_K > 0$.

REMARK 4.2. The theorem above is analogous to Theorem 2.6 of Nakagawa [7] which played a crucial role in the proof of the Ohno conjecture on the zeta functions associated with the prehomogeneous vector space of binary cubic forms.

5. Numerical examples. We first give an example pertaining to Theorem 3.1.

EXAMPLE 5.1. Let $\Phi_1(u, v) = -11u^2 + 2uv - 14v^2$ and $m = 62$. Put $\omega = \sqrt{-17}$. Then $\theta = (1 + 3\omega)/11$, $K = \mathbb{Q}(\omega)$ and $\mathcal{O}_K = \mathbb{Z}[\omega]$. Let Λ be an order of K with $\mathcal{O}_{\Phi_1} \subset \Lambda \subset \mathcal{O}_K$. Since $\mathcal{O}_{\Phi_1} = \mathbb{Z}[3\omega]$, Λ is either $\mathcal{O}_{\Phi_1}$ or $\mathcal{O}_K$.

We first assume $\Lambda = \mathcal{O}_{\Phi_1}$. Let A and B be the ideal classes represented by the Λ-ideals $\mathfrak{p}_7 = [7, -1 + 3\omega]$ and $\mathfrak{p}_2 = [2, -1 + 3\omega]$, respectively. Then $A^4 = 1$ and $B^2 = 1$. The Picard group $\mathrm{Pic}^+(\Lambda)$ is generated by A and B and is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We put $\mathfrak{p}_{11} = [11, 1+3\omega]$, $\mathfrak{p}_{13} = [13, -4+3\omega]$ and $\mathfrak{t} = [9, 3\omega]$. Then a complete set of representatives for $\mathrm{Pic}^+(\Lambda)$ is given by the following table:

1	A	A^2	A^3	B	AB	A^2B	A^3B
(1)	$\mathfrak{p}_7$	$\mathfrak{p}_{13}$	$\mathfrak{p}'_7$	$\mathfrak{p}_2$	$\mathfrak{p}_{11}$	$\mathfrak{t}$	$\mathfrak{p}'_{11}$

Here $\mathfrak{p}'$ is the conjugate of $\mathfrak{p}$. We have $\mathfrak{j} = \Lambda + \theta\Lambda = 11^{-1}\mathfrak{p}_{11}$ and $\widehat{\mathfrak{j}} = (6\omega)^{-1}\mathfrak{p}'_{11}$. Hence $[\widehat{\mathfrak{j}}] = A^3B$. Put $\mathfrak{p}_{31} = [31, 8+3\omega]$. Since $\mathfrak{p}'_7\mathfrak{p}_{31} = (8+3\omega)\Lambda$, we have $[\mathfrak{p}_{31}] = A$. By definition, $\omega_\Lambda(62)$ is the set of all integral invertible Λ-ideals $\mathfrak{f}$ such that $N_\Lambda(\mathfrak{f}) = 62$ and $[\mathfrak{f}] \in [\widehat{\mathfrak{j}}]\mathrm{Pic}^+(\Lambda)^2$. Since $[\widehat{\mathfrak{j}}]\mathrm{Pic}^+(\Lambda)^2 = \{AB, A^3B\}$, we have $\omega_\Lambda(62) = \{\mathfrak{p}_2\mathfrak{p}_{31}, \mathfrak{p}_2\mathfrak{p}'_{31}\}$. By definition, $S(62\Phi_1, \Lambda)$ is the subset of $I_\Lambda \times K^\times \times \omega_\Lambda(62)$ consisting of all $(\mathfrak{a}, \beta, \mathfrak{f})$ satisfying $\beta\mathfrak{a}^2 = \widehat{\mathfrak{j}}\mathfrak{f}$. Hence the following 16 triplets form a complete set of representatives for $G_0(\Lambda)\backslash S(62\Phi_1, \Lambda)$:

$\mathfrak{a}$	β	$\mathfrak{f}$
(1)	$\pm(-23+3\omega)/(6\omega)$	$\mathfrak{p}_2\mathfrak{p}_{31}$
$\mathfrak{p}_{13}$	$\pm(245+57\omega)/(1014\omega)$	$\mathfrak{p}_2\mathfrak{p}_{31}$
$\mathfrak{p}_2$	$\pm(-23+3\omega)/(12\omega)$	$\mathfrak{p}_2\mathfrak{p}_{31}$
$\mathfrak{t}$	$\pm(-23+3\omega)/(54\omega)$	$\mathfrak{p}_2\mathfrak{p}_{31}$
$\mathfrak{p}_7$	$\pm(-179+9\omega)/(294\omega)$	$\mathfrak{p}_2\mathfrak{p}'_{31}$
$\mathfrak{p}'_7$	$\pm(145+27\omega)/(294\omega)$	$\mathfrak{p}_2\mathfrak{p}'_{31}$
$\mathfrak{p}_{11}$	$\pm(-287+3\omega)/(726\omega)$	$\mathfrak{p}_2\mathfrak{p}'_{31}$
$\mathfrak{p}'_{11}$	$\pm(23+3\omega)/(66\omega)$	$\mathfrak{p}_2\mathfrak{p}'_{31}$

By (2.11), these triplets correspond to the following pairs of symmetric matrices $((x_{1,ij}),(x_{2,ij}))$ which form a complete set of representatives for $\Gamma\backslash L(62\Phi_1,\Lambda)$:

$$\begin{aligned}(x_{1,11},x_{1,12},x_{1,22},x_{2,11},x_{2,12},x_{2,22})\\ =\pm(1,-23,-153,2,16,-306),\ \pm(19,13,-27,-24,26,8),\\ \pm(2,-24,-53,4,14,-168),\ \pm(9,-23,-17,18,16,-34),\\ \pm(3,-26,-2,16,6,-52),\ \pm(9,22,-22,-14,14,48),\\ \pm(1,-26,-6,26,6,-32),\ \pm(11,22,-18,-24,14,28).\end{aligned}$$

We next assume $\Lambda=\mathcal{O}_K$. For any $\mathcal{O}_{\Phi_1}$-ideal $\mathfrak{a}$, we write $\widetilde{\mathfrak{a}}=\mathcal{O}_K\mathfrak{a}$. Let $\widetilde{A}$ be the ideal class represented by the $\mathcal{O}_K$-ideal $\widetilde{\mathfrak{p}}_7=[7,2+\omega]$. Then the Picard group $\mathrm{Pic}^+(\mathcal{O}_K)$ is a cyclic group of order 4 generated by $\widetilde{A}$. We put $\widetilde{\mathfrak{p}}_{11}=[11,4+\omega]$, $\widetilde{\mathfrak{p}}_2=[2,-1+\omega]$ and $\widetilde{\mathfrak{p}}_{31}=[31,13+\omega]$. Then a complete set of representatives for $\mathrm{Pic}^+(\mathcal{O}_K)$ is given by the following table:

1	$\widetilde{A}$	$\widetilde{A}^2$	$\widetilde{A}^3$
(1)	$\widetilde{\mathfrak{p}}_7$	$\widetilde{\mathfrak{p}}_2$	$\widetilde{\mathfrak{p}}'_7$

Further, we have $\mathfrak{j}=\mathcal{O}_K+\theta\mathcal{O}_K=11^{-1}\widetilde{\mathfrak{p}}_{11}$ and $\widehat{\mathfrak{j}}=(2\omega)^{-1}\widetilde{\mathfrak{p}}'_{11}$. It is easy to see that $[\widetilde{\mathfrak{p}}_{31}]=\widetilde{A}$ and $[\widehat{\mathfrak{j}}]=\widetilde{A}$. Hence $[\widehat{\mathfrak{j}}]\mathrm{Pic}^+(\mathcal{O}_K)^2=\{\widetilde{A},\widetilde{A}^3\}$. This implies $\omega_{\mathcal{O}_K}(62)=\{\widetilde{\mathfrak{p}}_2\widetilde{\mathfrak{p}}_{31},\widetilde{\mathfrak{p}}_2\widetilde{\mathfrak{p}}'_{31}\}$. Hence the following eight triplets form a complete set of representatives for $G_0(\mathcal{O}_K)\backslash S(62\Phi_1,\mathcal{O}_K)$:

$\mathfrak{a}$	β	$\mathfrak{f}$
(1)	$\pm(-23+3\omega)/(2\omega)$	$\widetilde{\mathfrak{p}}_2\widetilde{\mathfrak{p}}_{31}$
$\widetilde{\mathfrak{p}}_2$	$\pm(-23+3\omega)/(4\omega)$	$\widetilde{\mathfrak{p}}_2\widetilde{\mathfrak{p}}_{31}$
$\widetilde{\mathfrak{p}}_7$	$\pm(-179+9\omega)/(98\omega)$	$\widetilde{\mathfrak{p}}_2\widetilde{\mathfrak{p}}'_{31}$
$\widetilde{\mathfrak{p}}'_7$	$\pm(145+27\omega)/(98\omega)$	$\widetilde{\mathfrak{p}}_2\widetilde{\mathfrak{p}}'_{31}$

By (2.11), these triplets correspond to the following pairs of symmetric matrices $((x_{1,ij}),(x_{2,ij}))$ which form a complete set of representatives for

$\Gamma\backslash L(62\Phi_1, \mathcal{O}_K)$:

$$\begin{aligned}(x_{1,11}, x_{1,12}, x_{1,22}, x_{2,11}, x_{2,12}, x_{2,22}) &= \pm(3,-23,-51,6,16,-102),\ \pm(6,-26,-1,12,10,-64),\\ &\quad \pm(9,-23,-17,48,22,-8),\ \pm(27,13,-19,-42,28,2).\end{aligned}$$

By Theorem 3.1, we have $h(62\Phi_1) = 16 + 8 = 24$.

We finally give an example relating to Theorem 4.1.

EXAMPLE 5.2. Let $\Phi_1(u,v) = 2u^3+5u^2v+3uv^2-4v^3$ and $m = 2$. Let θ be a root of the cubic equation $\Phi_1(u,1) = 0$ and put $\omega_1 = 2\theta$, $\omega_2 = 2\theta^2+5\theta+3$. Then $K = \mathbb{Q}(\theta)$ is a cubic field with $D_K = -1879$ and $\mathcal{O}_K = \mathcal{O}_{\Phi_1} = [1,\omega_1,\omega_2]$. We put $\Lambda_1 = \mathcal{O}_K$ and $\Lambda_2 = [1, 2\omega_1, 2\omega_2]$. Then $\Lambda_1^{(1)}$ is a free $\mathbb{Z}$-module of rank one generated by $\varepsilon = -11 - 2\omega_1 + 2\omega_2$.

We first assume $\Lambda = \Lambda_1$. Let A be the ideal class represented by the Λ_1-ideal $\mathfrak{p}_3 = [3, \omega_1+1, \omega_2+2]$. Then the Picard group $\mathrm{Pic}^+(\Lambda_1)$ is a cyclic group of order 4 generated by A. We put $\mathfrak{p}_{2,1} = [2,\omega_1,\omega_2]$, $\mathfrak{p}_{2,2} = [2, \omega_1+1, \omega_2]$ and $\mathfrak{p}_{2,3} = [2,\omega_1,\omega_2+1]$. Since $(\omega_1 - 1) = \mathfrak{p}_{2,2}^2$, $(\omega_2+2) = \mathfrak{p}_{2,1}\mathfrak{p}_{2,2}\mathfrak{p}_3$ and $(\omega_2 - 2\omega_1 - 4) = \mathfrak{p}_{2,1}^2\mathfrak{p}_{2,2}$, we have $[\mathfrak{p}_{2,1}] = [\mathfrak{p}_{2,3}] = A$ and $[\mathfrak{p}_{2,2}] = A^2$. So a complete set of representatives for $\mathrm{Pic}^+(\Lambda_1)$ is given by the following table:

1	A	A^2	A^3
(1)	$\mathfrak{p}_{2,1}$	$\mathfrak{p}_{2,2}$	$\mathfrak{p}_{2,1}\mathfrak{p}_{2,2}$

Put $\mathfrak{j} = \Lambda_1 + \theta\Lambda_1$ and $\delta = 6\theta^2 + 10\theta + 3$. By Lemma 1.7, we have $\widehat{\mathfrak{j}} = \delta^{-1}\Lambda_1$, hence $[\widehat{\mathfrak{j}}] = 1$. Since $[\widehat{\mathfrak{j}}]\mathrm{Pic}^+(\Lambda_1)^2 = \{1, A^2\}$, we have $\omega_{\Lambda_1}(2) = \{\mathfrak{p}_{2,2}\}$. Hence the following four triplets form a complete set of representatives for $G_0(\Lambda_1)\backslash S(2\Phi_1, \Lambda_1)$:

$\mathfrak{a}$	β	$\mathfrak{f}$
$\mathfrak{p}_{2,1}$	$(3+\omega_1-\omega_2)/(4\delta)$	$\mathfrak{p}_{2,2}$
$\mathfrak{p}_{2,1}$	$\varepsilon(3+\omega_1-\omega_2)/(4\delta)$	$\mathfrak{p}_{2,2}$
$\mathfrak{p}_{2,1}\mathfrak{p}_{2,2}$	$-(5+\omega_1+\omega_2)/(4\delta)$	$\mathfrak{p}_{2,2}$
$\mathfrak{p}_{2,1}\mathfrak{p}_{2,2}$	$-\varepsilon(5+\omega_1+\omega_2)/(4\delta)$	$\mathfrak{p}_{2,2}$

By (2.11), these triplets correspond to the following pairs of symmetric matrices $((x_{1,ij}),(x_{2,ij}))$ which form a complete set of representatives for $\Gamma\backslash L(2\Phi_1, \Lambda_1)$:

$$\begin{aligned}(x_{1,11}, x_{1,12}, x_{1,13}, x_{1,22}, x_{1,23}, x_{1,33}, x_{2,11}, x_{2,12}, x_{2,13}, x_{2,22}, x_{2,23}, x_{2,33}) &= (-1,1,0,-1,-2,-3,-1,1,2,1,-2,0),\\ &\quad (7,-15,-4,23,14,-1,15,-23,-14,21,30,8),\\ &\quad (-1,-2,-4,0,-4,-13,1,0,2,2,4,8),\\ &\quad (-1,6,0,-24,-4,1,-3,12,2,-34,-12,0).\end{aligned}$$

We next assume $\Lambda = \Lambda_2$. Since $\varepsilon \in \Lambda_2$, $\Lambda_2^{(1)}$ is also generated by ε. The conductor of the order Λ_2 is $(2) = 2\mathcal{O}_K$. It is easy to see that $\mathrm{Pic}^+(\Lambda_2)$ is a cyclic group of order 4 generated by $a = [\mathfrak{p}_3 \cap \Lambda_2]$ (cf. (12.12) Theorem of [8]). Put $\mathfrak{j} = \Lambda_2 + \theta\Lambda_2$. By Lemma 1.7, we have $\widehat{\mathfrak{j}} = (2\delta)^{-1}\Lambda_2$, hence $[\widehat{\mathfrak{j}}] = 1$. Since $[\widehat{\mathfrak{j}}]\mathrm{Pic}^+(\Lambda_2)^2 = \{1, a^2\}$, we have $\omega_{\Lambda_2}(1) = \{\Lambda_2\}$. Hence the following four triplets form a complete set of representatives for $G_0(\Lambda_2)\backslash S(2\Phi_1, \Lambda_2)$:

$\mathfrak{a}$	β	$\mathfrak{f}$
Λ_2	$-1/(2\delta)$	Λ_2
Λ_2	$-\varepsilon/(2\delta)$	Λ_2
$(\mathfrak{p}_3 \cap \Lambda_2)^2$	$-(125 + 20\omega_1 + 32\omega_2)/(162\delta)$	Λ_2
$(\mathfrak{p}_3 \cap \Lambda_2)^2$	$-\varepsilon(125 + 20\omega_1 + 32\omega_2)/(162\delta)$	Λ_2

By (2.11), these triplets correspond to the following pairs of symmetric matrices $((x_{1,ij}), (x_{2,ij}))$ which form a complete set of representatives for $\Gamma\backslash L(2\Phi_1, \Lambda_2)$:

$$\begin{aligned}(x_{1,11}, x_{1,12}, x_{1,13}, x_{1,22}, x_{1,23}, x_{1,33}, x_{2,11}, x_{2,12}, x_{2,13}, x_{2,22}, x_{2,23}, x_{2,33})\\ = (0, 0, -1, -4, 0, -6, 0, 1, 0, -10, 0, 8),\\ (-1, 4, 5, 4, -32, -18, -1, -1, 8, 66, -32, -40),\\ (-16, -8, -21, -4, -10, -26, 10, 5, 12, 2, 6, 16),\\ (-5, 2, 3, 0, -2, -2, -7, 1, 6, 2, -2, -4).\end{aligned}$$

By Theorem 4.1, we have $h(2\Phi_1) = 4 + 4 = 8$.

References

[1] B. J. Birch and J. Merriman, *Finiteness theorems for binary forms with given discriminant*, Proc. London Math. Soc. (3) 24 (1972), 385–394.

[2] A. Fröhlich, *Invariants for modules over separable algebras*, Quart. J. Math. Oxford (2) 16 (1965), 193–232.

[3] K. Hardy and K. S. Williams, *The class number of pairs of positive-definite binary quadratic forms*, Acta Arith. 52 (1989), 103–117.

[4] J. Morales, *The classification of pairs of binary quadratic forms*, ibid. 59 (1991), 105–121.

[5] —, *On some invariants for systems of quadratic forms over the integers*, J. Reine Angew. Math. 426 (1992), 107–116.

[6] J. Nakagawa, *Binary forms and orders of algebraic number fields*, Invent. Math. 97 (1989), 219–235.

[7] —, *On the relations among the class numbers of binary cubic forms*, ibid. 134 (1998), 101–138.

[8] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.

[9] D. J. Wright and A. Yukie, *Prehomogeneous vector spaces and field extensions*, Invent. Math. 110 (1992), 283–314.

Department of Mathematics
Joetsu University of Education
Joetsu 943-8512, Japan
E-mail: jin@juen.ac.jp

Received on 18.6.2001
and in revised form on 21.1.2002 (4057)