Y. Furuta
Nagoya Math. J.
Vol. 98 (1985), 77-86

GAUSS'S TERNARY FORM REDUCTION AND ITS APPLICATION TO A PRIME DECOMPOSITION SYMBOL

YOSHIOMI FURUTA

Introduction

We defined a prime decomposition symbol $[d_1, d_2, p]$ in a previous paper [3], and characterized in [4] the set of rational primes p which are decomposed completely in a non-abelian central extension which is of degree 8 in substance. The explicit value of the symbol was determined by using a solution of certain ternary quadratic diophantine equation. The solution corresponds to a square root of an ideal class of the principal genus of a quadratic field. This is translated to a problem in classes of integral quadratic forms, namely to find a form whose duplication is a given one contained in a principal genus. An explicit method to find the form is given by Gauss in [5, Art. 286], which is due to his ternary form reduction.

The purpose of the present paper is to look at again this Gauss's method in somewhat different formulation, and apply it to the symbol cited above.

In Section 1 we consider a ternary quadratic lattice with a symmetric bilinear form $\varphi(\alpha, \beta)$ and a certain product $\alpha*\beta$, which coincide respectively with the simultaneous invariant and covariant of two binary quadratic forms whose coefficients are indicated by α and β. It might be noticed further that $\varphi(\alpha, \beta)$ and $\alpha*\beta$ are comparable with the inner product and the outer product of vector analysis. In these point of view, we reformulate in Section 2 Gauss's method cited above, and in Section 3 we apply it to the symbol $[d_1, d_2, a]$, which is the product of $[d_1, d_2, p]$ for prime factors p of an integer a. More precisely, we treat the following three problems:

(I) To estimate the value of $[d_1, d_2, a]$ explicitly by means of Gauss's method.

Received January 23, 1984.

(II) To classify the set of integers a having the same value of $[d_1, d_2, a]$ for a given pair $\{d_1, d_2\}$.

(III) To classify the set of pairs $\{d_1, d_2\}$ having the same value of $[d_1, d_2, a]$ for a given integer a.

Problem (II) has been treated already in [4]. Thus it will be summarized in the present point of view.

§1. Ternary quadratic lattices

Let $L = Z \oplus Z/2 \oplus Z$ and $L_0 = Z \oplus Z \oplus Z$. For an element $\alpha = (a_1, a_2, a_3)$ of L, let $[\alpha] = \begin{bmatrix} a_1 & a_2 \\ a_2 & a_3 \end{bmatrix}$ and $\alpha[x] = [x] \cdot [\alpha] \cdot {}^t[x] = a_1x_1^2 + 2a_2x_1x_2 + a_3x_2^2$, where $[x] = [x_1, x_2]$. α is called primitive if G.C.D. $\{a_1, 2a_2, a_3\} = 1$. We define a symmetric bilinear form φ of L by

$$\varphi(\alpha, \beta) = a_2b_2 - \tfrac{1}{2}(a_1b_3 + a_3b_1)\,, \tag{1.1}$$

where $\alpha = (a_1, a_2, a_3)$ and $\beta = (b_1, b_2, b_3)$ are elements of L. We set

$$\varphi(\alpha) = \varphi(\alpha, \alpha) = a_2^2 - a_1a_3\,.$$

Then

$$\varphi(\alpha) = \operatorname{dis} \alpha[x] = -\det[\alpha] \quad \text{and}$$
$$\varphi(\alpha, \beta) = \tfrac{1}{2}(\varphi(\alpha + \beta) - \varphi(\alpha) - \varphi(\beta))\,.$$

$2\varphi(\alpha, \beta)$ is usually denoted by $\Delta(\alpha, \beta)$ and called a simultaneous invariant of quadratic forms $\alpha[x]$ and $\beta[x]$. α and β are said to be orthogonal if $\varphi(\alpha, \beta) = 0$.

We define a product $\alpha * \beta$ by

$$\alpha * \beta = (2(a_1b_2 - a_2b_1),\ a_1b_3 - a_3b_1,\ 2(a_2b_3 - a_3b_2))\,. \tag{1.2}$$

Then

$$[\alpha * \beta] = [\alpha]\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}[\beta] + [\beta]\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}[\alpha]\,, \tag{1.3}$$

and $\alpha * \beta$ is orthogonal to both α and β. Moreover the direct calculation implies $\alpha * \alpha = 0$, $\alpha * \beta = -\beta * \alpha$, $\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma$ and $\alpha * (\beta * \gamma) + \beta * (\gamma * \alpha) + \gamma * (\alpha * \beta) = 0$.

$-\frac{1}{2}(\alpha * \beta)[x]$ is usually denoted by $J_{\alpha,\beta}[x]$ and called simultaneous covariant of $\alpha[x]$ and $\beta[x]$.

https://doi.org/10.1017/S0027763000021371 Published online by Cambridge University Press

The following formula is well known[1] as a syzygy in the theory of invariants.

$$J_{\alpha,\beta}[x]^2 = \varphi(\beta)\cdot\beta[x]^2 - \Delta(\alpha,\beta)\cdot\alpha[x]\cdot\beta[x] + \varphi(\beta)\cdot\alpha[x]^2. \tag{1.4}$$

Thus we have

$$(\alpha*\beta)(x)^2 = 4(\varphi(\alpha)\cdot\beta[x]^2 - 2\varphi(\alpha,\beta)\cdot\alpha[x]\cdot\beta[x] + \varphi(\beta)\cdot\alpha[x]^2) \tag{1.5}$$

Let $\hat{L}(\alpha) = \{\beta \in L;\ \varphi(\alpha,\beta) = 0\}$. Then we have[2]

PROPOSITION 1.1. *Let $\alpha = (a_1, a_2, a_3)$ be a primitive element of L and put $a_0 = G.C.D\{a_1, a_3\}$, $a_1 = a_0a_1'$ and $a_3 = a_0a_3'$. Let v and w be integers such that $a_1'v + a_3'w = 1$. Then $\hat{L}(\alpha) = Z\omega_1 \oplus Z\omega_2$, where $\omega_1 = (a_1', 0, -a_3')$ and $\omega_2 = (2a_2w, a_0, 2a_2v)$ or $= (a_2w, a_0/2, a_2v)$ according as $\alpha \notin L_0$ or $\alpha \in L_0$.*

PROPOSITION 1.2. *Let $\alpha = (a_1, a_2, a_3) \in L$ and G.C.D. $\{a_1, a_3\} = 1$. Then $\hat{L}(\alpha) = \{\alpha*\beta;\ \beta \in L\}$.*

Proof. This follows from [4, Theorem 2], since

$$\begin{aligned}
&\begin{bmatrix} a_1 & a_2 \\ a_2 & a_3 \end{bmatrix}\begin{bmatrix} \xi/2 & \eta \\ \lambda & -\xi/2 \end{bmatrix} + \begin{bmatrix} \xi/2 & \lambda \\ \eta & -\xi/2 \end{bmatrix}\begin{bmatrix} a_1 & a_2 \\ a_2 & a_3 \end{bmatrix} \\
&\quad = \begin{bmatrix} a_1 & a_2 \\ a_2 & a_3 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} -\lambda & \xi/2 \\ \xi/2 & \eta \end{bmatrix} + \begin{bmatrix} -\lambda & \xi/2 \\ \xi/2 & \eta \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a_1 & a_2 \\ a_2 & a_3 \end{bmatrix} \\
&\quad = [\alpha*\beta] \quad \text{with } \beta = (-\lambda, \xi/2, \eta).
\end{aligned}$$

We note the following formulas, which are obtained by direct calculations in analogous way as in vector analysis taking $\varphi(\alpha,\beta)$ and $\alpha*\beta$ as inner and outer product respectively.

$$\alpha*(\beta*\gamma) = 4(\varphi(\alpha,\beta)\gamma - \varphi(\alpha,\gamma)\beta) \tag{1.6}$$

$$\varphi(\alpha*\beta, \gamma*\delta) = 4(\varphi(\alpha,\delta)\varphi(\gamma,\beta) - \varphi(\alpha,\gamma)\varphi(\beta,\delta)) \tag{1.7}$$

$$\varphi(\alpha*\beta,\gamma) = \varphi(\beta,\gamma*\alpha) = -\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} \tag{1.8}$$

§2. Gauss's ternary form reduction

We call primitive elements α_1 and α_2 to be (properly) equivalent if there exists a matrix T of $SL(2, Z)$ such that $[\alpha_2] = T\cdot[\alpha_1]\cdot{}^tT$. Denote by

1) Cf. Hooley [6].

2) See [4, p. 214], where the second type of the base ω_2 is omitted when $\alpha \in L_0$.

https://doi.org/10.1017/S0027763000021371 Published online by Cambridge University Press

$\{\alpha\}$ the equivalent class containing α. When $\varphi(\alpha) = \varphi(\beta)$, a composition $\{\alpha\}\cdot\{\beta\}$ is defined through the composition[3] of corresponding classes of quadratic forms $\alpha[x]$ and $\beta[x]$. This composition is connected with the ideal product by the well known correspondence between absolute ideal classes in narrow sense of the quadratic field $\boldsymbol{Q}(\sqrt{\varphi(\alpha)})$ and equivalence classes of quadratic forms with discriminant $\varphi(\alpha)$. More precisely, let $\alpha = (a_1, a_2, a_3)$ be a primitive element of L, and put $\mathfrak{a} = \boldsymbol{Z}a_1 + \boldsymbol{Z}(a_2 + \sqrt{d})$. Then $\mathfrak{a}$ is an ideal of $\boldsymbol{Q}(\sqrt{\varphi(\alpha)})$ and $\alpha[x] = |N\mathfrak{a}|^{-1}\cdot N(a_1x_1 + (a_2 + \sqrt{\varphi(\alpha)})x_2)$. Denote by $\{\mathfrak{a}\}$ the ideal class in narrow sense containing $\mathfrak{a}$. Then the correspondence is given by $\{\alpha\}$ and $\{\mathfrak{a}\}$ connected as above. We put $(\alpha) = \{\mathfrak{a}\}$, which is an ideal class of $\boldsymbol{Q}(\sqrt{\varphi(\alpha)})$ corresponding to $\{\alpha\}$. There is a well known method by means of united forms[4] to get a form γ such that $\{\gamma\} = \{\alpha\}\cdot\{\beta\}$. By this method it is easy to get a duplication γ of a given δ in L: $\{\gamma\} = \{\delta\}^2$. In order to get conversely δ from a duplication γ, Gauss has given in [5, Art. 282–286] a method of ternary form reduction. We shall reformulate it in view of the previous section.

For $\alpha, \beta \in L$ we define $\lambda_{\alpha,\beta}$ by

$$\lambda_{\alpha,\beta} = (\varphi(\alpha), \varphi(\alpha, \beta), \varphi(\beta)) . \tag{2.1}$$

Set $\varphi(\Lambda) = \{\varphi(\gamma); \gamma \in \Lambda\}$ for a sublattice Λ of L. Then we have $\varphi(\Lambda) = \{\lambda_{\alpha,\beta}[x]; [x] \in \boldsymbol{Z}^2\}$ when $\Lambda = \boldsymbol{Z}\alpha \oplus \boldsymbol{Z}\beta$. Moreover $\lambda_{\alpha,\beta}$ is equivalent to $\lambda_{\alpha',\beta'}$ in L, if $\boldsymbol{Z}\alpha \oplus \boldsymbol{Z}\beta = \boldsymbol{Z}\alpha' \oplus \boldsymbol{Z}\beta'$ and $\lambda_{\alpha,\beta}, \lambda_{\alpha',\beta'} \in L$. By the formula (1.7) or by direct calculation, we have

$$\varphi(\alpha*\beta) = 4\varphi(\lambda_{\alpha,\beta}) . \tag{2.2}$$

Hence $((\alpha*\beta)/2)$ and $(\lambda_{\alpha,\beta})$ are ideal classes of the same quadratic field when $((\alpha*\beta)/2)$ and $\lambda_{\alpha,\beta}$ are primitive elements of L. In the following we shall show that $(\lambda_{\alpha,\beta}) = ((\alpha*\beta)/2)^2$, and hence $\{\lambda_{\alpha,\beta}\} = \{(\alpha*\beta)/2\}^2$.

LEMMA 2.1. *Let $\alpha = (a_1, a_2, a_3)$ be a primitive element of L, and put $K = \boldsymbol{Q}(\sqrt{d})$, where $d = \varphi(\alpha)$. Let b be a rational integer. Then there exists $[x] \in \boldsymbol{Z}^2$ such that $b = \alpha[x]$ if and only if there exists an ideal $\mathfrak{b}$ of K such that $b = N\mathfrak{b}$, where $\mathfrak{b}$ is contained in the ideal class (α) corresponding to α.*

Proof. Suppose $b = \alpha[x]$. Let $\mathfrak{a} = \boldsymbol{Z}a_1 + \boldsymbol{Z}(a_2 + \sqrt{d})$. Then $a_1 = N\mathfrak{a}$ and $\mathfrak{a} \in (\alpha)$. This means that for the first component b of an primitive

3) See for instance Cassels [1, Chapter 14].

4) Cf. Dulin and Butts [2], Pall [7] or Cassels [1, Chapter 14] in which the united forms are called concordant forms.

element β of L there is an ideal $\mathfrak{b}$ such that $b = N\mathfrak{b}$ and $\mathfrak{b} \in (\beta)$. Therefore it is enough to show the necessity that there exists β of L such that β is equivalent to α and the first component of β is b. We have a well known method[5] to get β as follows: Let $b = \alpha[y_1, y_2]$, where we can assume that G.C.D. $\{y_1, y_2\} = 1$. Take integers u and v such that $y_1 v - y_2 u = 1$, and let $T = \begin{bmatrix} y_1 & y_2 \\ u & v \end{bmatrix}$. Then $T \in SL(2, Z)$ and $T \cdot \alpha \cdot {}^t T = \begin{bmatrix} b & * \\ * & * \end{bmatrix}$, which is to be required.

Conversely suppose that $b = N\mathfrak{b}$ and $\mathfrak{b} \in (\alpha)$. Then there is an integer b_2 such that $\mathfrak{b} = Zb + Z(b_2 + \sqrt{d})$. Let $\beta = |N\mathfrak{b}^{-1}| \cdot N(bx_1 + (b_2 + \sqrt{d})x_2)$. Then $b = \beta[1, 0]$ and $\mathfrak{b} \in (\beta)$. Hence $(\alpha) = (\beta)$, which implies $b = \alpha[x]$ with some $[x] \in Z^2$.

LEMMA 2.2. *Let K be a quadratic field with discriminant d. Let a and b be rational integers which are norms of ideals of K. If a diophantine equation*

$$ax^2 = z^2 - dy^2 \tag{2.3}$$

has a solution such that $z = b$, then there exist ideals $\mathfrak{a}$ and $\mathfrak{b}$ of K such that $a = N\mathfrak{a}$, $b = N\mathfrak{b}$ and $\{\mathfrak{a}\} = \{\mathfrak{b}\}^2$.

Proof. Let $a = N\mathfrak{a}$ and $b = N\mathfrak{b}'$ by assumption. Then the solvability of (2.3) implies $N(\mathfrak{a}(\mathfrak{b}')^2) = N(z + y\sqrt{d})$. This implies $\mathfrak{a}(\mathfrak{b}')^2 = z + y\sqrt{d}$ by regarding decomposition to prime factors of both sides of the above equality and, if necessary, suitable choice of $\mathfrak{a}$ and $\mathfrak{b}'$ such that $a = N\mathfrak{a}$ and $b = N\mathfrak{b}'$. Thus we have $\mathfrak{a} = \mathfrak{b}^2((z + y\sqrt{d})/b) \sim \mathfrak{b}^2$.

THEOREM 2.3. *Let $\alpha, \beta \in L$, and suppose that $\lambda_{\alpha,\beta}$ and $\frac{1}{2}(\alpha * \beta)$ are primitive elements of L. Then $\lambda_{\alpha,\beta}$ is a duplication of $\frac{1}{2}(\alpha * \beta)$,* i.e., *$\{\lambda_{\alpha,\beta}\} = \{\frac{1}{2}(\alpha * \beta)\}^2$.*

Proof. Put $\gamma = \frac{1}{2}(\alpha * \beta)$, $\lambda = \lambda_{\alpha,\beta}$ and $\eta = \alpha * \gamma$. Then since γ is orthogonal to α, the formula (1.5) implies

$$\eta[x]^2 = 4(\varphi(\alpha)\gamma[x]^2 + \varphi(\gamma)\alpha[x]^2) \tag{2.4}$$

for any $[x] = [x_1, x_2] \in Z^2$. Set $[x] = [1, 0]$, and put $z = \eta[1, 0]$, $b = \gamma[1, 0]$, $y = \alpha[1, 0]$, $a = \lambda[1, 0]$ and $d = \varphi(\gamma) = \varphi(\lambda)$. Then by Lemma 2.1, both a and b are norms of ideals of $Q(\sqrt{d})$. We have further $a = \varphi(\alpha)$, since $\lambda[x_1, x_2] = \varphi(\alpha)x_1^2 + 2\varphi(\alpha, \beta)x_1x_2 + \varphi(\beta)x_2^2 = \varphi(\alpha x_1 + \beta x_2)$. Hence (2.4) implies

5) Cf. Watson [9, Chapter 1, Theorem 1].

$z^2 = 4ab^2 + 4dy^2$. Then by Lemma 2.2, there are ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $Q(\sqrt{d})$ such that $\{\mathfrak{a}\} = \{\mathfrak{b}\}^2$. This implies the theorem by Lemma 2.1.

Now the problem to get a form δ from γ such that $\{\delta\}^2 = \{\gamma\}$ is reduced to the problem to get a pair of forms $\{\alpha, \beta\}$ such that $\gamma = \lambda_{\alpha,\beta}$. Since $\lambda_{\alpha,\beta}[x] = \varphi(\alpha x_1 + \beta x_2)$ and φ is a ternary quadratic form, the procedure to have $\{\alpha, \beta\}$ from γ is called by Gauss a representation of a binary form γ by a ternary form φ, and also called a ternary form reduction. Gauss has exhibited in [5] an explicit method for the ternary form reduction. We can arrange it as follows[6] by using matrices.

Let $\gamma = (c_1, c_2, c_3) \in L$, and suppose that there exist $\alpha = (a_1, a_2, a_3)$ and $\beta = (b_1, b_2, b_3)$ such that $\gamma[x] = \lambda_{\alpha,\beta}[x] = \varphi(\alpha x_1 + \beta x_2)$. Put $\alpha x_1 + \beta x_2 = (y_1, y_2, y_3)$. Then $\gamma[x] = [x_1, x_2]\begin{bmatrix} c_1 & c_2 \\ c_2 & c_3 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \varphi(y_1, y_2, y_3) = y_2^2 - y_1 y_3 = [y_1, y_2, y_3]$ $\times \begin{bmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{bmatrix}\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = [x_1, x_2]\begin{bmatrix} \alpha \\ \beta \end{bmatrix}\begin{bmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{bmatrix}[{}^t\alpha, {}^t\beta]\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$. Hence to get α and β from γ is equivalent to get α and β from

$$\begin{bmatrix} c_1 & c_2 \\ c_2 & c_3 \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{bmatrix}\begin{bmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{bmatrix}\begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{bmatrix}. \tag{2.5}$$

In order use inverse matrices, we fill up matrix elements by integers and let

$$S = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ s_1 & s_2 & s_3 \end{bmatrix} \quad \text{and} \quad M = \begin{bmatrix} c_1 & c_2 & m_2 \\ c_2 & c_3 & m_1 \\ m_2 & m_1 & m_0 \end{bmatrix}$$

so that (2.5) is rewrite as follows:

$$M = S \cdot T \cdot {}^tS\,, \tag{2.6}$$

where

$$T = \begin{bmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & & \\ & 1 & \\ & & 1 \end{bmatrix}\begin{bmatrix} & & 1 \\ & 1 & \\ -1 & & \end{bmatrix}\begin{bmatrix} \frac{1}{2} & & \\ & 1 & \\ & & 1 \end{bmatrix}.$$

Put $T_1 = \begin{bmatrix} 2 & & \\ & 1 & \\ & & 1 \end{bmatrix} S^{-1}$. Then (2.6) becomes

6) Shanks [8] refers also Gauss's method with some improvements.

$$T_1 \cdot M \cdot {}^tT_1 = \begin{bmatrix} & & 1 \\ & 1 & \\ -1 & & \end{bmatrix}. \tag{2.7}$$

Now if $\gamma[x]$ belongs to a principal genus, we can determine the above integers m_0, m_1 and m_2 so that $\det M = -1$. In fact the system of the following diophantine equations has a system of solutions A_1, A_2, A_3, B_1 and B_2:

$$\begin{cases} B_1^2 = c_1 + \varphi(\gamma)A_3 \\ B_1B_2 = -c_2 + \varphi(\gamma)A_2 \\ B_2^2 = c_3 + \varphi(\gamma)A_1 \end{cases}$$

Let $M = \begin{bmatrix} A_1 & A_2 & B_2 \\ A_2 & A_3 & B_1 \\ B_2 & B_1 & B_0 \end{bmatrix}^{-1}$, where $B_0 = -\varphi(\gamma) = \begin{vmatrix} c_1 & c_2 \\ c_2 & c_3 \end{vmatrix}$. Then M is to be required. We can get the matrix T_1 of (2.7) by fundamental transformations of matrices. Let $T_2 = \begin{bmatrix} \frac{1}{2} & & \\ & 1 & \\ & & 1 \end{bmatrix} T_1$. Then the third column ${}^t[t_{13}, t_{23}, t_{33}]$ of T_2 implies

$$\alpha * \beta = (2t_{33}, t_{23}, 2t_{13}) \frac{1}{\det T_2}. \tag{2.8}$$

The elements $\alpha = (a_1, a_2, a_3)$ and $\beta = (b_1, b_2, b_3)$ such that $\gamma = \lambda_{\alpha,\beta}$ are obtained from the inverse of T_2,

$$T_2^{-1} = \begin{bmatrix} \alpha \\ \beta \\ \sigma \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ s_1 & s_2 & s_3 \end{bmatrix}, \tag{2.9}$$

because

$${}^t[t_{13}, t_{23}, t_{33}] = {}^t\left[\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}, -\begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix}, \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}\right] \cdot |T_2|.$$

§ 3. Application to a prime decomposition symbol

Let $K = \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2})$ be a bicyclic biquadratic field. For a rational prime p, a symbol $[d_1, d_2, p]$ is defined in [3] when there exists a central extension $\hat{K}$ of $K/\boldsymbol{Q}$ for which the genus field K^* is not equal to $\hat{K}$, p is not ramified in $\hat{K}$ and p is of degree 1 in $K^*/\boldsymbol{Q}$. We define $[d_1, d_2, a]$ multiplicatively for a rational integer a whose prime factors satisfy the above condition.

https://doi.org/10.1017/S0027763000021371 Published online by Cambridge University Press

We call a pair $\{d_1, d_2\}$ type A when $d_1 \equiv d_2 \equiv 1 \bmod 4$, and call it type B when $d_1 \equiv 1 \bmod 8$ and $d_2 \not\equiv 1 \bmod 4$. For the sake of simplicity we treat hereafter only the above two types of pairs $\{d_1, d_2\}$. Moreover we add the following condition (R) called Rédei type:

(R) d_1 and d_2 are mutually prime and $(d_1/q) = 1$ for any prime factors q of d_2 and $(d_2/q) = 1$ for any prime factors q of d_1.

Then the condition of $[d_1, d_2, a]$ to be defined is equivalent that the following three conditions are satisfied.

(p1) $p \equiv 1 \bmod d_1 d_2$ for any prime divisor p of a.
(p2) $(d_1/p) = (d_2/p) = 1$ for any prime divisor p of a.
(p3) $(q^*/p) = 1$ for any prime divisor q of $d_1 d_2$ and any prime divisor p of a but $p \neq q$, where q^* stands for a prime discriminant, i.e., $q^* = (-1)^{(q-1)/2}q$, -4 or ± 8 so that the discriminant of $\boldsymbol{Q}(\sqrt{d_1 d_2})$ is written as a product of those q^*.

We denote by $\mathfrak{D}$ the set of triples $\{d_1, d_2, a\}$ which satisfy the above conditions type A or type B, and (R), (p1), (p2), (p3). Separate $\mathfrak{D}$ to $\mathfrak{D}_A$ and $\mathfrak{D}_B$ according that the pair $\{d_1, d_2\}$ is of type A or type B.

Let $\{d_1, d_2, a\} \in \mathfrak{D}$, and put $\hat{a} = 4a$ or a according that $\{d_1, d_2\}$ is of type A or type B. Then [3, Theorem 5.1] implies

$$[d_1, d_2, a] = \left(\frac{d_1}{b}\right) = \left(\frac{d_2}{b}\right), \tag{3.1}$$

where b is any primitive solution with $X = b$ of the following diophantine equation

$$z^2 = \hat{a}X^2 + d_1 d_2 Y^2 . \tag{3.2}$$

Now we consider Problem (I) in Introduction. Let $\alpha, \beta \in L_0$. Then $\frac{1}{2}(\alpha * \beta)$ is orthogonal to α, and $\varphi(\frac{1}{2}(\alpha * \beta)) = \varphi(\lambda_{\alpha,\beta})$ by (2.2). Hence (1.5) implies

$$(\tfrac{1}{2}(\alpha*(\alpha*\beta))[x])^2 = \varphi(\alpha)\cdot(\tfrac{1}{2}(\alpha*\beta)[x])^2 + \varphi(\lambda_{\alpha,\beta})\alpha[x]^2 . \tag{3.3}$$

Thus we can get the value of $[d_1, d_2, a]$ as follows: There are integers c_1 and c_2 such that $d_1 d_2 = c_2^2 - \hat{a}c_3$ by the condition (p2). Put $\gamma = (\hat{a}, c_2, c_3)$ and find α and β such that $\gamma = \lambda_{\alpha,\beta}$ by Gauss's method as in Section 2. Then by (3.1), (3.2) and (3.3), we have

$$[d_1, d_2, a] = \left(\frac{d_1}{\frac{1}{2}(\alpha*\beta)[x]}\right) \tag{3.4}$$

for $[x] \in Z^2$ such that $\frac{1}{2}(\alpha*\beta)[x]$ is an integer relatively prime to $\alpha[x]$.

EXAMPLE. Calculation of $[3, -23, 13]$. This belongs to type B. $d_1d_2 = -69 = 3^2 - 13\cdot 6$. Put $\gamma = (13, 3, 6)$. As a system of solutions of

$$\begin{cases} B_1^2 = 13 - 69\cdot A_3 \\ B_2^2 = 6 - 69\cdot A_1 \\ B_1B_2 = -3 - 69\cdot A_2 , \end{cases}$$

we have $B_1 = 17$, $B_2 = 12$, $A_1 = -2$, $A_3 = -4$, $A_2 = -3$. Then $M = \begin{bmatrix} 13 & 3 & 3 \\ 3 & 6 & 2 \\ 3 & 2 & 1 \end{bmatrix}$, since $m_0 = 3^2 - 8 = 1$, $m_1 = -34 + 36 = 2$ and $m_2 = -48 + 51 = 3$. In the same way as to obtain a reduced form of integral quadratic forms, a matrix T_1 satisfying (2.7) is obtained, that is $T_1 = \begin{bmatrix} 1 & 1 & -5 \\ 0 & 0 & 1 \\ 1 & 2 & -7 \end{bmatrix}$. Then $T_2 = \begin{bmatrix} \frac{1}{2} & & \\ & 1 & \\ & & 1 \end{bmatrix} T_1$ and $\frac{1}{2}(\alpha*\beta) = (14, 1, 5)$. This implies $[3, -23, 13] = (3/\frac{1}{2}(\alpha*\beta)[0, 1]) = (\frac{3}{5}) = -1$. We have also $\alpha = (4, 3, -1)$ and $\beta = (-2, 2, 1)$, since $S = T_2^{-1} = \begin{bmatrix} 4 & 3 & -1 \\ -2 & 2 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

Problem (II) has been treated in [4] already. This is reformulated as follows using notation in Section 2.

PROPOSITION 3.1. *Let $\{d_1, d_2\}$ be of type* A *or type* B, *and chose $\alpha \in L$ so that $d_1d_2 = \varphi(\alpha)$. Then we have*

$$[d_1, d_2, \varphi(\alpha*\beta)] = \left(\frac{d_1}{\alpha[x]}\right)$$

for $\beta \in L$ when $\alpha[x]$ and $(\alpha*\beta)[x]$ are relatively prime, and $\{d_1, d_2, \varphi(\alpha*\beta)\} \in \mathfrak{D}$.

As in [4], this proposition is followed from (3.1), (3.2) and

$$J_{\alpha*\beta,\alpha}[x]^2 = \varphi(\alpha*\beta)\alpha[x]^2 + \varphi(\alpha)((\alpha*\beta)[x])^2 , \tag{3.5}$$

which is implied from (1.4) and Proposition 1.2.

In order to treat Problem (III), we use again (3.5) with $\hat{a} = \varphi(\alpha)$ and $d_1d_2 = \varphi(\alpha*\beta)$. Denote by $L(d_1)$ the set of (a_1, a_2, a_3) of L such that a_1 is divisible by d_1. We remark that if $\{d_1, d_2, a\} \in \mathfrak{D}$ and $\hat{a} = \varphi(\alpha)$ with $\alpha \in L$, then there is an integer a_2 such that $\varphi(\alpha) \equiv a_2^2 \bmod d_1$, which is followed from the condition of $[d_1, d_2, a]$ to be defined. Hence we can choose the above

https://doi.org/10.1017/S0027763000021371 Published online by Cambridge University Press

α to be in $L(d_1)$. Moreover suppose that $\varphi(\alpha*\beta) \equiv 0$ for $\beta \in L$. Then since $\varphi(\alpha*\beta) = 4(\varphi(\alpha, \beta)^2 - \varphi(\alpha)\varphi(\beta))$ by (1.7), we have $\varphi(\alpha, \beta)^2 \equiv a_2^2\varphi(\beta) \bmod d_1$. Hence we can choose β to be in $L(d_1)$ too. Conversely it is easy to see that $\varphi(\alpha*\beta) \equiv 0 \bmod d_1$ if both α and β belong to $L(d_1)$.

We have the following Proposition as a solution of Problem (III).

PROPOSITION 3.2. *Let* $d_1d_2 = \varphi(\alpha*\beta)$ *and* $d_1d_2' = \varphi(\alpha*\beta')$ *for* α, β, $\beta' \in L(d_1)$. *Suppose that* $\beta' = \beta + d_1\eta$ *with* $\eta \in L$. *Then we have*

$$[d_1, d_2, a] = [d_1, d_2', a]$$

when $\hat{a} = \varphi(\alpha)$, *and both* $\{d_1, d_2, a\}$ *and* $\{d_1, d_2', a\}$ *belong to* $\mathfrak{D}_A$ *or they both belong to* $\mathfrak{D}_B$.

Proof. The formulas (3.1), (3.2) and (3.5) imply $[d_1, d_2, a] = (d_1/(\alpha*\beta)[x])$ and $[d_1, d_2', a] = (d_1/(\alpha*\beta')[x])$. Moreover $(\alpha*\beta')[x] = (\alpha*(\beta + d_1\eta))[x] = (\alpha*\beta)[x] + d_1(\alpha*\eta)[x]$. Hence $((\alpha*\beta')[x]/d_1) = ((\alpha*\beta)[x]/d_1)$. This implies the proposition owing to the condition $d_1 \equiv 1 \bmod 4$.

REFERENCES

[1] J. W. S. Cassels, Rational quadratic forms, Academic Press (1978).
[2] B. J. Dulin and H. S. Butts, Composition of binary quadratic forms over integral domains, Acta Arith., **20** (1972), 223–251.
[3] Y. Furuta, A prime decomposition symbol for a non-abelian central extension which is abelian over a bicyclic biquadratic field, Nagoya Math. J., **79** (1980), 79–109.
[4] ——, A prime decomposition symbol and integral quadratic forms, Japan. J. Math., **7** (1981), 213–216.
[5] C. F. Gauss, Disquitiones arithmeticae, translation to German by H. Haser, 1889, Chelsea.
[6] C. Hooley, On the diophantine equation $ax^2 + by^2 + cz^2 + 2fyz + 2gzx + 2hxz = 0$, Arch. Math., **19** (1968), 472–478.
[7] G. Pall, Composition of binary quadratic forms, Bull. Amer. Math. Soc., **54** (1948), 1171–1175.
[8] D. Shanks, Gauss's ternary form reduction and the 2-Sylow subgroup, Math. Comp., **25** (1971), 837–853.
[9] G. L. Watson, Integral quadratic forms, Cambridge Univ. Press, 1960.

Department of Mathematics
Kanazawa University
Kanazawa 920
Japan