Y. Furuta and T. Kubota
Nagoya Math. J.
Vol. 130 (1993), 177–182

CENTRAL EXTENSIONS AND RATIONAL QUADRATIC FORMS

YOSHIOMI FURUTA AND TOMIO KUBOTA

Introduction

The purpose of this paper is to characterize by means of simple quadratic forms the set of rational primes that are decomposed completely in a non-abelian central extension which is abelian over a quadratic field. More precisely, let $L = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ be a bicyclic biquadratic field, and let $K = \mathbf{Q}(\sqrt{d_1 d_2})$. Denote by $S_K(\tilde{m})$ the ray class field $\bmod m$ of K in narrow sense for a large rational integer m. Let L_m^* be the maximal abelian extension over $\mathbf{Q}$ contained in $S_K(\tilde{m})$ and $\hat{L}_m$ be the maximal extension contained in $S_K(\tilde{m})$ such that $\mathrm{Gal}(\hat{L}_m/L)$ is contained in the center of $\mathrm{Gal}(\hat{L}_m/\mathbf{Q})$. Then we shall show in Theorem 2.1 that any rational prime p not dividing $d_1 d_2 m$ is decomposed completely in $L_m^*/\mathbf{Q}$ if and only if p is representable by rational integers x and y such that $x \equiv 1$ and $y \equiv 0 \bmod m$ as follows

$$p = \frac{ax^2 + bxy + cy^2}{a},$$

where a, b, c are rational integers such that $b^2 - 4ac$ is equal to the discriminant of K and (a) is a norm of a representative of the ray class group of $K \bmod m$. Moreover p is decomposed completely in $\hat{L}_m/L_m^*$ if and only if $\left(\frac{d_1}{a}\right) = 1$.

§1. Central extensions with respect to quadratic fields

Let d_1 and d_2 be square free integers and let $d_1 d_2 = d_0 d^2$, where d_0 is square free and $d_0 \neq 1$. Let $K = \mathbf{Q}(\sqrt{d_0})$, $L = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ and D be the discriminant of K. For a rational integer m, denote by $\mathfrak{S}_K(\tilde{m})$ the ray class $\bmod m$ of K in narrow sense, and by $S_K(\tilde{m})$ the ray class field $\bmod m$ of K in narrow sense.

Let m be a rational integer such that L is contained in $S_K(\tilde{m})$. Let L_m^* and $\hat{L}_m$

Received June 16, 1992

be the genus field and the central class field of $L/\mathbf{Q}$ with respect to $S_K(\tilde{m})$. They are by definition, the maximal subfields of $S_K(\tilde{m})$ such that L_m^* is abelian over $\mathbf{Q}$ and $\mathrm{Gal}(\hat{L}_m/L)$ is contained in the center of $\mathrm{Gal}(\hat{L}_m/\mathbf{Q})$.

We have $[\hat{L}_m : L_m^*] \leq 2$ in general, and $[\hat{L}_m : L_m^*] = 2$ when m is large enough, for instance m is a multiple of $4dd_0$. More precisely, let m_1 be the product of all odd rational primes q such that q divides d_0 and satisfies both $(d_1/q) \neq 1$ and $(d_2/q) \neq 1$. Define m_0 by

$$(1.1)\quad m_0 = \begin{cases} dm_1 & \text{when } d_1 \equiv d_2 \equiv 1 \mod 4, \\ dm_1 & \text{when } d_i \equiv 1 \mod 8, \text{ and } d_j \not\equiv 1 \mod 4, \\ 2dm_1 & \text{when } d_i \equiv 5 \mod 8, \text{ and } d_j \not\equiv 1 \mod 4, \\ 4dm_1 & \text{otherwise}, \end{cases}$$

where $i, j = 1$ or 2 and $i \neq j$. Then [2, Proposition 3.4] implies $[\hat{L}_m : L_m^*] = 2$ when m is a multiple of m_0.

Now let $K_\#^*$ be the genus field of K in absolute sense, and let $\mathbf{Q}(\tilde{m})$ be the ray class field $\mathrm{mod}\, m$ of $\mathbf{Q}$ in narrow sense. Let K_m^* be the genus field of $K/\mathbf{Q}$ with respect to the ray class field $\mathrm{mod}\, m$ of K in narrow sense. Then $K_m^* = L_m^*$ by the definition, and we have

$$L_m^* = K_\#^* \mathbf{Q}(\tilde{m})$$

by [2, Theorem 4.3]. Thus the genus field L_m^* is given explicitly as follows

$$(1.2)\qquad L_m^* = \Pi \mathbf{Q}(\sqrt{q^*}) \cdot \mathbf{Q}(\zeta_m)$$

where q runs over all rational primes dividing d_0, and q^* are prime discriminants, i.e., $D = \Pi q^*$ by $q^* = (-1)^{(q-1)/2} q,\ -4$, or ± 8.

For the later use, let $\mathfrak{S}_K'(m)$ be the group of principal ideals (α) of K such that $\alpha \equiv 1 \mod m$ and $\mathrm{N}_{K/\mathbf{Q}}\alpha > 0$, and $S_K'(m)$ be the class field of K corresponding to $\mathfrak{S}_K'(m)$. Let $L_m^{*\prime}$ and $\hat{L}_m'$ be the genus field and the central class field of $L/\mathbf{Q}$ with respect to $S_K'(m)$. Then we can show that

$$(1.3)\qquad L_m^{*\prime} = L_m^*,$$

and

$$(1.4)\qquad \hat{L}_m' = \hat{L}_m$$

as follows.

The ideal group of K corresponding to $\mathbf{Q}(\tilde{m})$ is the group of ideals $\mathfrak{a}$ of K such that $|\mathrm{N}\mathfrak{a}| \equiv 1 \mod m$. This group contains $\mathfrak{S}_K'(m)$ and clearly $S_K'(m) \supset K_\#^*$. Hence $S_K'(m)$ contains $L_m^* = K_\#^* \mathbf{Q}(\tilde{m})$. This implies (1.3) since $S_K(\tilde{m})$ contains

$S'_K(m)$.

In order to show (1.4), let σ be the non-trivial element of $\mathrm{Gal}(K/\mathbf{Q})$, and denote by $\mathfrak{R}$ resp. $\mathfrak{R}'$ the group of ideals $\mathfrak{a}$ of K such that $\mathfrak{a}^{\sigma} \equiv \mathfrak{a} \bmod \mathfrak{S}_K(\tilde{m})$ resp. $\bmod\, \mathfrak{S}'_K(m)$. Then by [1, Proposition 5.1] we have

$$(1.5) \qquad \mathrm{Gal}(\hat{L}_m/L_m^*) \cong I_K/\mathfrak{H}(L/K)\mathfrak{R}$$

and

$$(1.6) \qquad \mathrm{Gal}(\hat{L}'_m/L_m^{*\prime}) \cong I_K/\mathfrak{H}(L/K)\mathfrak{R}',$$

where I_K is the group of ideals of K prime to m and $\mathfrak{H}(L/K)$ is the subgroup of I_K corresponding to L by class field theory. Let $\alpha = 1 + 4\sqrt{D}m$. Then $(\alpha) \in \mathfrak{H}(L/K)$, because

$$\left(\frac{d_i}{N_{K/\mathbf{Q}}\alpha}\right) = \left(\frac{N_{K/\mathbf{Q}}\alpha}{d_i}\right) = 1$$

for $i = 1,2$, since $N_{K/\mathbf{Q}}\alpha \equiv 1 \bmod 8$. When $\mathfrak{S}'_K(m) \neq \mathfrak{S}_K(\tilde{m})$, the non-trivial class of $\mathfrak{S}'_K(m)/\mathfrak{S}_K(\tilde{m})$ is represented by $1 - m$, and $1 - m = \alpha^{1-\sigma}\alpha_1$, where $\alpha_1 = \alpha^{\sigma-1}(1 - m)$, which is contained in $\mathfrak{S}_K(\tilde{m})$. Thus for any element (γ) of $\mathfrak{S}'_K(m)$, we have $(\gamma) = (\alpha)^{1-\sigma}(\gamma_1)$, where $(\gamma_1) \in \mathfrak{S}_K(\tilde{m})$. Now let $\mathfrak{a}$ be any element of $\mathfrak{R}'$. Then there is γ of $K^{\times}$ such that $\mathfrak{a}^{\sigma} = \mathfrak{a}(\gamma)$, $(\gamma) \in \mathfrak{S}'_K(m)$. The above argument implies $(\mathfrak{a}(\alpha))^{\sigma} = \mathfrak{a}(\alpha)(\gamma_1)$, that is $\mathfrak{a}(\alpha) \in \mathfrak{R}$. Hence $\mathfrak{a} \in (\alpha)^{-1}\mathfrak{R} \subset \mathfrak{H}(L/K)\mathfrak{R}$. Therefore $[\hat{L}'_m : L_m^*] = 2$ if and only if $[\hat{L}_m : L_m^*] = 2$ by (1.3), (1.5) and (1.6). This implies further (1.4) because of definition of central extensions and $\mathfrak{S}_K(\tilde{m}) \subset \mathfrak{S}'_K(m)$.

§2. Decomposition of primes

Notation being as in the preceding section, let $\mathfrak{P}$ be an ideal of $L_m^* = L_m^{*\prime}$ prime to m. Then it follows from the definition of the genus field that there exists an ideal $\mathfrak{a}$ of K such that

$$(2.1) \qquad \mathfrak{a}^{\sigma-1} \equiv \mathbf{N}_{L_m^*/K}\mathfrak{P} \mod \mathfrak{S}'_K(m).$$

Let $\mathfrak{b} = N_{L_m^*/K}\mathfrak{P}$ and $(a) = N_{K/\mathbf{Q}}\mathfrak{a}$. Suppose that no prime divisor of $\mathfrak{a}$ ramified in L. Then by [2, Proposition 1.5] exchanged the notation a and b, we have the following relation of Artin symbols:

$$(2.2) \qquad \left(\frac{\hat{L}_m/L_m^*}{\mathfrak{P}}\right) = \left(\frac{\hat{L}_m/K}{\mathfrak{b}}\right) = \left(\frac{L/K}{\mathfrak{a}}\right) = \left(\frac{d_1}{a}\right) = \left(\frac{d_2}{a}\right).$$

Let $C'_m(\mathfrak{a})$ be the class of ideals of $K \bmod \mathfrak{S}'_K(m)$ which contains $\mathfrak{a}$, and let $\mathfrak{N}(C'_m(\mathfrak{a}))$ be the set of norms of "integral" ideals contained in $C'_m(\mathfrak{a})$. Then any rational prime of $\mathfrak{N}(C'_m(\mathfrak{a}^{1-\sigma}))$ not dividing m is decomposed completely in $L^*_m = L^{*\prime}_m$. It is further decomposed completely in $\hat{L}_m$ when $\left(\frac{d_1}{a}\right) = 1$ by (2.2), where $(a) = N_{K/\mathbf{Q}}\mathfrak{a}$.

Let us call a rational integer D a discriminant integer when there is a quadratic field whose discriminant is equal to D. For a discriminant integer D and a rational integer m, denote by $A(D, m)$ the set of rational integers a satisfying the following condition:

$$(2.3)\qquad \begin{cases} a \text{ is square free, and g.c.d.}(a, m) = 1. \\ \left(\frac{D}{q}\right) = 1 \quad \text{for all odd prime factors } q \text{ of } a. \\ a \text{ is odd, if } D \not\equiv 1 \bmod 8. \end{cases}$$

Note that $a \in A(D, m)$ implies that (a) is a norm of an integral ideal of K prime to m.

For a rational integer a in $A(D, m)$, choose a primitive integral form $ax^2 + bxy + cy^2$ with discriminant D, and define $H(D, m, a)$ by

$$(2.4)\qquad H(D, m, a) = \left\{\frac{ax^2 + bxy + cy^2}{a} \in \mathbf{Z}\,;\, x \equiv 1,\ y \equiv 0 \bmod m\right\}.$$

Note that $H(D, m, a)$ is independent of the choice of b, c, because if $b_1^2 - 4ac_1 = D$ too, then $b = b_1 + 2at$ by $t \in \mathbf{Z}$ and we have

$${}^tU \begin{bmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{bmatrix} U = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

by $U = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$.

THEOREM 2.1. *Let $L = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$, where d_1 and d_2 are distinct square free integers and $d_1 d_2 = d_0 d^2$ by a square free integer d_0. Let m be an integer divisible by m_0 defined in* (1.1). *Let L^*_m and $\hat{L}_m$ be the genus field and the central class field of $L/\mathbf{Q}$ with respect to the ray class field* mod m *of K. Let p be a rational prime not dividing $d_1 d_2 m$. Then p is decomposed completely in $L^*_m/\mathbf{Q}$ if and only if p is contained in $H(D, m, a)$ for some rational integer a of $A(D, m)$. It is further decomposed completely in $\hat{L}_m/L^*_m$ if and only if $\left(\frac{d_1}{a}\right) = 1$.*

Proof. By (2.2) and (2.1), it is enough to show that

(2.5) $$p \in H(D, m, a) \Leftrightarrow p \in \mathfrak{N}(C'_m(\mathfrak{a}^{1-\sigma})),$$

where $\mathfrak{a}$ is an integral ideal of K and $(a) = \mathbf{N}_{K/\mathbf{Q}}\mathfrak{a}$.

Suppose that $p \in \mathfrak{N}(C'_m(\mathfrak{a}^{1-\sigma}))$. Then there are a prime ideal $\mathfrak{p}$ dividing p and an element α of K such that $\mathfrak{p} = (\alpha)\mathfrak{a}^{1-\sigma}$, $\alpha \equiv 1 \bmod m$ and $\alpha\alpha^\sigma > 0$. We can assume that $\mathfrak{a}$ contains no rational divisor. Then we have $\mathfrak{a}^{-1} \cap \mathbf{Q} = \mathbf{Z}$, since any multiple divisor of $\mathfrak{a}^{-1}$ is rational only if it is integral. Hence we can choose a $\mathbf{Z}$-basis of $\mathfrak{a}^{-1}$ in the form $\{1, \omega\}$ by an element ω of K. Let $\alpha = x + \omega y$, where $x, y \in \mathbf{Z}$. Then

$$p = \alpha\alpha^\sigma = (x + \omega y)(x + \omega^\sigma y).$$

Let $(a) = N_{K/\mathbf{Q}}\mathfrak{a}$. Then $a \in A(D, m)$. Since the ideal divisor (Inhalt) of the polynomial $x + \omega y$ is equal to $\mathfrak{a}^{-1}$, the rational quadratic form $a(x + \omega y)(x + \omega^\sigma y)$ must be primitive. Denote this form by $ax^2 + bxy + cy^2$. Then $D = b^2 - 4ac$ and we have

$$p = \frac{ax^2 + bxy + cy^2}{a},$$

where $x \equiv 1$, $y \equiv 0 \bmod m$, since $\alpha \equiv 1 \bmod m$ and g.c.d.$(a, m) = 1$.

Conversely suppose that $p \in H(D, m, a)$, where $D = b^2 - 4ac$ and $a \in A(D, m)$. Let $\alpha = x + \omega y$, where $\omega = (b + \sqrt{b^2 - 4ac})/2a \in K$. Then $\alpha \in S'_K(m)$ and $p = N_{K/\mathbf{Q}}\alpha$. Compare the decomposition of the both sides to prime ideals. Then we see that there exists a prime ideal $\mathfrak{p}$ and an integral ideal $\mathfrak{a}$ of K such that $(p) = N_{K/\mathbf{Q}}\mathfrak{p}$, $\mathfrak{p} = (\alpha)\mathfrak{a}^{1-\sigma}$ and $a = N_{K/\mathbf{Q}}\mathfrak{a}$. This completes the proof.

Remark 2.1. For a given pair of integers d_0 and m, the number of distinct sets $\mathfrak{N}(C'_m(\mathfrak{a}))$ is not exceed the number of the classes mod $\mathfrak{S}'_K(m)$. Hence the set of rational primes decomposed completely in $\hat{L}_m/\mathbf{Q}$ coincides with the union of rational primes contained in $H(D, m, a)$ by a finite number of rational integers a satisfying the condition (2.3) and $\left(\frac{d_1}{a}\right) = 1$.

Remark 2.2. The set of rational primes decomposed completely in $\hat{L}_m/\mathbf{Q}$ coincides also with the set of primes p such that $[d_1, d_2, p] = 1$, where the symbol is defined in [2]. On a treatment by means of this symbol in a restricted case, see [4, Proposition 3.1].

References

[1] Y. Furuta, Note on class number factors and prime decompositions, Nagoya Math. J., **66** (1977), 167–182.
[2] ——, 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.
[3] ——, A norm residue map for central extensions of an algebraic number field, Nagoya Math. J., **93** (1984), 61–69.
[4] ——, Gauss's ternary form reduction and its application to a prime decomposition symbol, Nagoya Math. J., **98** (1985), 77–86.

Y. Furuta
Department of Mathematics
Faculty of Science
Kanazawa University
Kanazawa 920
Japan

T. Kubota
Department of Mathematics
School of Science
Nagoya University
Chikusa-ku, Nagoya 464-01
Japan

current address:
Department of Mathematics
Meijo University
Nagoya, 468
Japan