Y. Furuta
Nagoya Math. J.
Vol. 79 (1980), 79-109

A PRIME DECOMPOSITION SYMBOL FOR A NON-ABELIAN CENTRAL EXTENSION WHICH IS ABELIAN OVER A BICYCLIC BIQUADRATIC FIELD

YOSHIOMI FURUTA

Introduction

In a previous paper [6] we had some criteria for the prime decomposition in certain non-abelian extensions over the rational number field Q, and as its special case we had a reciprocity of the biquadratic residue symbol. The reciprocity was obtained by using a descent method of the prime decomposition for a central extension over Q which is abelian over a biquadratic field $Q(\sqrt{-1}, \sqrt{q})$. In the present paper we study on the case over a biquadratic field $Q(\sqrt{d_1}, \sqrt{d_2})$ in general. We define a symbol $[d_1, d_2, p]$ which expresses the decomposition law of a rational prime p in a central extension mentioned above.

In 1939, L. Rédei [12] defined a symbol $\{a_1, a_2, a_3\}$ which expresses the prime decomposition in a certain non-abelian extension over Q of degree 8, and found its multiplication and inversion properties. In 1960, A. Fröhlich [2] defined a symbol $[a_1, a_2, a_3]_c$, where c is a factor system class associated with a group of order 8. Rédei's symbol is essentially the same as this symbol for a certain fixed value of c. Multiplication and inversion formulas and further an explicit expression of the symbol are also stated in [2] without proof. Though the explicit expression is not so simple, but it is remarkable that the expression is given in terms of values of rational residue characters associated with certain rational ternary quadratic forms. Rédei's symbol and Fröhlich's symbol are defined as a quadratic residue symbol in the quadratic field $Q(\sqrt{a_1})$ or in the biquadratic field $Q(\sqrt{a_1}, \sqrt{a_2})$.

In the present paper we define a symbol $[d_1, d_2, d_3]$ by treating certain large abelian extensions of $Q(\sqrt{d_1}, \sqrt{d_2})$ which are central over Q. Then our symbol is also essentially the same as Rédei's and Fröhlich's up to a part associated with abelian extensions over Q. Using a descent method

Received February 19, 1979.

stated in our previous paper [6], we can express the value of the symbol explicitly and rather simply in computable[0] formula (Theorem 5.1). This explicit formula implies a simple inversion formula (Theorems 6.2 and 6.3, Remark 6.4 which contains a conjecture). The explicit formula implies also other formulas related with rational biquadratic residue symbols (Theorems 5.4 and 6.1).

§1. General treatment of $[d_1, d_2, a]$

For an algebraic number field F, we denote by J_F, $F^\times$ and U_F the group of ideles, principal ideles and unit ideles of F respectively. Denote by $F_\mathfrak{p}^\times$ the multiplicative group of non-zero elements of the completion $F_\mathfrak{p}$ of F at a prime $\mathfrak{p}$, and by $U_\mathfrak{p}$ the group of units of $F_\mathfrak{p}$, which are embedded in J_F as usual. For a divisor $\mathfrak{m}$ of F, denote by $\mathfrak{m}_\mathfrak{p}$ its $\mathfrak{p}$-part: $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{m}_\mathfrak{p}$. Denote by $U_F(\mathfrak{m})$ the group of elements $\mathfrak{u}$ of U_F whose $\mathfrak{p}$-component $\mathfrak{u}_\mathfrak{p} \equiv 1 \bmod.^{1)} \mathfrak{m}_\mathfrak{p}$. For an extension L/k of finite degree, we put $H(L/k) = k^\times N_{L/k} J_L$, where $N_{L/k}$ stands for the norm map.

Let L be a Galois extension of k, and M be a Galois extension of L which is normal over k. Let M_0 be the maximal abelian extension over k contained in M. We denote by $L^*_{M/k}$ the genus field of L with respect to M/k, namely $L^*_{M/k} = LM_0$. We denote further by $L^{(1)}_{M/k}$ the central class field of L with respect to M/k, which is, by definition[2)], the maximal field L' such that $L \subseteqq L' \subseteqq M$ and $\mathrm{Gal}(L'/L)$ is contained in the center of $\mathrm{Gal}(L'/k)$. It follows from class field theory that

$$H(L^*_{M/k}/k) = k^\times N_{L/k} H(M/L)\,, \tag{1}$$

$$H(L^{(1)}_{M/k}/L) = J_L^{\Delta} H(M/L)\,, \tag{2}$$

where $\Delta = \Delta(L/k)$ is the submodule generated by $1 - \sigma$ of the group ring of $\mathrm{Gal}(L/k)$ over the ring of integers, σ running over $\mathrm{Gal}(L/k)$.

When the ground field k is the rational number field $\boldsymbol{Q}$, we denote simply by L^*_M and $L^{(1)}_M$ instead of $L^*_{M/\boldsymbol{Q}}$ and $L^{(1)}_{M/\boldsymbol{Q}}$ respectively. Our purpose in this paper is to study the decomposition criteria of prime ideals in $L^{(1)}_M/L^*_M$, when L is a bicyclic biquadratic field $\boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2})$. For this purpose we define a symbol $[d_1, d_2, a]$ as follows at first.

0) In § 7 we add a table of values of the symbol, which are computed by machine.

1) When $\mathfrak{p}$ is an infinite prime, the congruence $\mathfrak{u}_\mathfrak{p} \equiv 1 \bmod. \mathfrak{p}$ stands for $\mathfrak{u}_\mathfrak{p} > 0$ or $\mathfrak{u}_\mathfrak{p} \neq 0$ according as $\mathfrak{p}$ is real or complex.

2) See [5].

DEFINITION 1.1. Let d_1, d_2 be a pair of rational integers such that $L = \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2})$ is biquadratic over $\boldsymbol{Q}$, and let p be a rational prime. We call *the symbol* $[d_1, d_2, p]$ *is defined (in primitive sense)*, when there exists a ray class field R over L in narrow sense[3] such that R is normal over $\boldsymbol{Q}$, $L_R^{(1)} \supsetneqq L_R^*$, and a prime divisor $\mathfrak{p}$ of p in L_R^* is of degree 1 and unramified in $L_R^{(1)}/L_R^*$. When that is the case, we set $[d_1, d_2, p] = 1$ or -1 according as the Artin symbol $\left(\frac{L_R^{(1)}/L_R^*}{\mathfrak{p}}\right)$ is equal to the identity or not.

For the sake of simplicity, we identify hereafter the Artin symbol and its character when the extension is quadratic. Then we have

$$[d_1, d_2, p] = \left(\frac{L_R^{(1)}/L_R^*}{\mathfrak{p}}\right).$$

For a rational integer a with the prime decomposition $a = \pm \prod p_i^{e_i}$, we put

$$[d_1, d_2, a] = \prod [d_1, d_2, p_i]^{e_i},$$

when $[d_1, d_2, p_i]$ is defined for each prime p_i.

Remark 1.2. For any bicyclic biquadratic field $L = \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2})$, we have $L_R^{(1)} \supsetneqq L_R^*$ if R is sufficiently large (c.f. S. Shirai [13, Theorem 29]), and when that is the case, $L_R^{(1)}$ is quadratic over L_R^*.

Remark 1.3. Suppose that $[d_1, d_2, p]$ is defined. Then its value does not depend on the choice of a ray class field R. In fact, for $i = 1, 2$, let R_i be a ray class field over L in narrow sense defined by $\mathfrak{f}_i$ such that R_i is normal over $\boldsymbol{Q}$ and $L_{R_i}^{(1)} \supsetneqq L_{R_i}^*$. Let $\mathfrak{f}_i = \prod \mathfrak{p}_t^{e_{t,i}}$ be the prime decomposition for $i = 1, 2$, and let $\mathfrak{f}_3$ be the least common multiple of $\mathfrak{f}_1$ and $\mathfrak{f}_2$: $\mathfrak{f}_3 = \prod \mathfrak{p}_t^{e_{t,3}}$, where $e_{t,3} = \mathrm{Max}(e_{t,1}, e_{t,2})$. Let R_3 be the ray class field over K defined by $\mathfrak{f}_3$ in narrow sense. For a prime divisor $\mathfrak{p}$ of L, denote by $U_{\mathfrak{p}}(e)$ the group of local units u at $\mathfrak{p}$ such that[1] $u \equiv 1 \bmod \mathfrak{p}^e$, and denote by $N_{\mathfrak{p}}$ the local norm map. Then since $H(R_i/L) = L^\times U_L(\mathfrak{f}_i)$, we have $H(L_{R_i}^*/\boldsymbol{Q}) = \boldsymbol{Q}^\times N_{L/\boldsymbol{Q}} U_L(\mathfrak{f}_i) = \boldsymbol{Q}^\times \prod N_{\mathfrak{p}_t} U_{\mathfrak{p}_t}(e_{t,i})$ for $i = 1, 2, 3$. Moreover since we can suppose that $\mathfrak{f}_i$ contains a real infinite prime if there is such one, we have $H(L_{R_1}^*/\boldsymbol{Q}) \cap H(L_{R_2}^*/\boldsymbol{Q}) = H(L_{R_3}^*/\boldsymbol{Q})$. Hence $L_{R_3}^* = L_{R_1}^* L_{R_2}^*$. Thus $R_3 \supseteq L_{R_3}^{(1)} \supseteq L_{R_1}^{(1)} L_{R_2}^* \supsetneqq L_{R_3}^*$. This implies $L_{R_3}^{(1)} = L_{R_1}^{(1)} L_{R_2}^*$ and $L_{R_3}^{(1)} \supsetneqq L_{R_3}^*$, because $(L_{R_3}^{(1)} : L_{R_3}^*) \leqq 2$. Similarly $L_{R_3}^{(1)} = L_{R_1}^* L_{R_2}^{(1)}$. Hence $L_{R_3}^{(1)} = L_{R_1}^{(1)} L_{R_2}^{(1)}$. Now assume that p

3) This means that R is defined by a divisor which contains all infinite primes of L (or equivalently, all real infinite primes of L).

has prime divisors $\mathfrak{p}_1$ resp. $\mathfrak{p}_2$ of degree 1 in $L_{R_1}^*$ resp. $L_{R_2}^*$, and unramified in $L_{R_1}^{(1)}/L_{R_1}^*$ resp. $L_{R_2}^{(1)}/L_{R_2}^*$. Then p has also a prime divisor $\mathfrak{p}_3$ of degree 1 in $L_{R_3}^*$ and unramified in $L_{R_3}^{(1)}/L_{R_3}^*$. Therefore we have

$$\left(\frac{L_{R_3}^{(1)}/L_{R_3}^*}{\mathfrak{p}_3}\right) = \left(\frac{L_{R_i}^{(1)}/L_{R_i}^*}{\mathfrak{p}_i}\right)$$

for $i = 1, 2$.

The following proposition follows immediately from the definition.

PROPOSITION 1.4. *Suppose that* $[d_1, d_2, a]$ *is defined. Then*

$$\begin{aligned} &[d_1, d_2, a] = [d_2, d_1, a], \\ &[d_1, d_2, a] = [d_1, d_2 d^2, a] \qquad \text{for any integer } d\,, \\ &[d_1, d_2, a] = [d_1, d_1 d_2, a]. \end{aligned}$$

As a special case of [6, Proposition 5.1], we have

PROPOSITION 1.5. *Let* $L = \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2})$ *be a bicyclic biquadratic field, and* K *be a quadratic field contained in* L. *Let* M *be an abelian extension of* K *which contains* L *and is normal over* $\boldsymbol{Q}$. *Let* $\mathfrak{A}$ *be an ideal of* $L_M^* = K_M^*$, *and* $\mathfrak{a}$ *be the norm of* $\mathfrak{A}$ *to* K. *Assume that* $\mathfrak{a}$ *is prime to the conductor of* M/K. *Let* $\mathfrak{b}$ *be an ideal of* K *such that* $\mathfrak{b}^{\sigma-1} \equiv \mathfrak{a} \bmod \mathfrak{H}(M/K)$, *where* σ *is the non-trivial automorphism of* K *over* $\boldsymbol{Q}$, *and* $\mathfrak{H}(M/K)$ *is the congruent ideal group corresponding to* M/K. *Then*

$$\left(\frac{L_M^{(1)}/L_M^*}{\mathfrak{A}}\right) = \left(\frac{L/K}{\mathfrak{b}}\right).$$

Remark 1.6. Let $L, R, L_R^{(1)}$ be as in Definition 1.1, and K be any quadratic field contained in L. Then since $\mathrm{Gal}\,(L_R^{(1)}/L)$ is contained in the center of $\mathrm{Gal}\,(L_R^{(1)}/\boldsymbol{Q})$, it is also contained in the center of $\mathrm{Gal}\,(L_R^{(1)}/K)$. Now since L is cyclic over K, $L_R^{(1)}$ is abelian over K.

THEOREM 1.7. *We have*

$$[d_1, d_2, a]\,[d_1, d_3, a] = [d_1, d_2 d_3, a],$$

when the symbols are all defined.

Proof. Put $d_4 = d_2 d_3/(d_2, d_3)^2$. Let $L_i = \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_i})$ and $K_i = \boldsymbol{Q}(\sqrt{d_1 d_i})$ for $i = 2, 3, 4$. Moreover let R_i be a ray class field over L_i in narrow sense such that R_i is normal over $\boldsymbol{Q}$ and $L_i^{(1)} \supseteq L_i^*$, where $L_i^{(1)}$ resp. L_i^* is the

central class field resp. the genus field of L_i with respect to $R_i/\boldsymbol{Q}$. Put $K = \boldsymbol{Q}(\sqrt{d_1})$. Then each $L_i^{(1)}$ is abelian over K by Remark 1.6. To prove the theorem, it is sufficient to treat only the case where a is a rational prime p. Let $\mathfrak{p}$ be a prime divisor of p in K, and $\mathfrak{p}_i$ be prime divisors of $\mathfrak{p}$ in L_i^* for $i = 2, 3, 4$. Let $\mathfrak{b}$ be an ideal of K such that

$$\mathfrak{b}^{\sigma-1} \equiv \mathfrak{p} \bmod. H(L_2^{(1)}L_3^{(1)}L_4^{(1)}/K) ,$$

where σ is the non-trivial automorphism of K over $\boldsymbol{Q}$. The existence of such $\mathfrak{b}$ follows from definedness of the symbols $[d_1, d_i, p]$. Then Proposition 1.5 implies

$$[d_1, d_i, p] = \left(\frac{L_i^{(1)}/L_i^*}{\mathfrak{p}_i}\right) = \left(\frac{L_i/K}{\mathfrak{b}}\right) ,$$

since $L_i^{(1)}$ is abelian over K. Now we have

$$\begin{aligned}[d_1, d_2, p][d_1, d_3, p] &= \left(\frac{L_2/K}{\mathfrak{b}}\right)\left(\frac{L_3/K}{\mathfrak{b}}\right) \\ &= \left(\frac{L_4/K}{\mathfrak{b}}\right) = [d_1, d_2d_3, p] .\end{aligned}$$

PROPOSITION 1.8. *Let d be the greatest common divisor of d_1 and d_2, and put $d_1 = dd_1'$ and $d_2 = dd_2'$. Then*

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

when the above symbols together with $[d_1, d, a]$ are all defined.

Proof. It follows from Proposition 1.4 and Theorem 1.7 that

$$\begin{aligned}[d_1, d_2, a] &= [d_1, d, a][d_1, d_2', a] = [dd_1', d, a][d_1, d_2', a] \\ &= [d^2d_1', d, a][d_1, d_2', a] = [d_1', d, a][d_1, d_2', a] .\end{aligned}$$

§ 2. Restricted treatment of $[d_1, d_2, a]$

Let L, R, K and $L_R^{(1)}$ be as in Remark 1.6. We shall show that the symbol $[d_1, d_2, a]$ is defined by means of a ray class field S over K not only a ray class field R over L when some restriction to a is added. Let $\mathfrak{f}$ be the conductor of R/L. Then we have

$$\begin{aligned}H(L_R^{(1)}/K) &= K^\times N_{L/K}(H(L_R^{(1)}/L)) \supseteq K^\times N_{L/K}(H(R/L)) \\ &= K^\times N_{L/K}(L^\times U_L(\mathfrak{f})) = K^\times N_{L/K}(U_L(\mathfrak{f})) .\end{aligned}$$

Let $\mathfrak{f}_K$ be a divisor of K such that $N_{L/K}(U_L(\mathfrak{f})) \supseteq U_K(\mathfrak{f}_K)$, and let S be the

ray class field over K in narrow sense with the conductor $\mathfrak{f}_K$. Then $H(L_R^{(1)}/K) \supseteq K^\times U_K(\mathfrak{f}_K) = H(S/K)$. Since $L_R^{(1)}$ is abelian over K, we have $L_R^{(1)} \subseteq S$. This implies $L_S^{(1)} \supseteq L_R^{(1)}L_S^* \supseteq L_S^* \supseteq L_R^*$. Moreover $L_S^{(1)} = L_R^{(1)}L_S^*$, because $(L_S^{(1)}: L_S^*) \leqq 2$. Now assume that a rational prime p has a prime divisor $\mathfrak{P}$ resp. $\mathfrak{p}$ in L_R^* resp. L_S^* of degree 1. Then we have

$$[d_1, d_2, p] = \left(\frac{L_R^{(1)}/L_R^*}{\mathfrak{P}}\right) = \left(\frac{L_S^{(1)}/L_S^*}{\mathfrak{p}}\right).$$

Conversely we have the following

PROPOSITION 2.1. *Let $L = \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2})$ be a bicyclic biquadratic field, and K be a quadratic field contained in L. Let S be a ray class field over K in narrow sense such that S is normal over $\boldsymbol{Q}$, $S \supseteq L$ and $L_S^{(1)} \supseteq L_S^*$. Let p be a rational prime, and assume that p has a prime divisor $\mathfrak{p}$ in L_S^* of degree* 1. *Then the symbol $[d_1, d_2, p]$ is defined and*

$$[d_1, d_2, p] = \left(\frac{L_S^{(1)}/L_S^*}{\mathfrak{p}}\right).$$

Proof. Let $\mathfrak{f}_K$ be the conductor of S/K. Then since $\mathfrak{f}_K$ is a multiple of the conductor of L/K, there is[4] a divisor $\mathfrak{f}_L$ of L such that $N_{L/K}U_L(\mathfrak{f}_L) = U(\mathfrak{f}_K)$. Let R be the ray class field mod. $\mathfrak{f}_L$ over L in narrow sense. We can take $\mathfrak{f}_L$ so that R is normal over $\boldsymbol{Q}$. Then we have $L_S^* = L_R^*$. In fact, it follows from (1) that $H(L_R^*/\boldsymbol{Q}) = \boldsymbol{Q}^\times N_{L/\boldsymbol{Q}}H(R/L) = \boldsymbol{Q}^\times N_{L/\boldsymbol{Q}}(L^\times U_L(\mathfrak{f}_L)) = \boldsymbol{Q}^\times N_{L/\boldsymbol{Q}}U_L(\mathfrak{f}_L) = \boldsymbol{Q}^\times N_{K/\boldsymbol{Q}}N_{L/K}U_L(\mathfrak{f}_L) = \boldsymbol{Q}^\times N_{K/\boldsymbol{Q}}U_K(\mathfrak{f}_K) = \boldsymbol{Q}^\times N_{K/\boldsymbol{Q}}(K^\times U_K(\mathfrak{f}_K)) = \boldsymbol{Q}^\times N_{K/\boldsymbol{Q}}H(S/K) = H(K_S^*/\boldsymbol{Q}) = H(L_S^*/\boldsymbol{Q})$. Hence $L_S^* = L_R^*$. We have further $L_S^{(1)} = L_R^{(1)}$. Because it follows from (2) that $H(L_R^{(1)}/L) = J_L^{\Delta}H(R/L) = J_L^{\Delta}L^\times U_L(\mathfrak{f}_L)$, where $\Delta = \Delta(L/\boldsymbol{Q})$. Hence

$$\begin{aligned} H(L_R^{(1)}/K) &= K^\times N_{L/K}H(L_R^{(1)}/L) = K^\times N_{L/K}J_L^{\Delta}\cdot N_{L/K}U_L(\mathfrak{f}_L) \\ &= K^\times N_{L/K}J_L^{\Delta}\cdot U_K(\mathfrak{f}_K) = N_{L/K}J_L^{\Delta}\cdot H(S/K)\,. \end{aligned}$$

On the other hand we have $H(L_S^{(1)}/L) = J_L^{\Delta}H(S/L)$ and further $H(L_S^{(1)}/K) = K^\times\cdot N_{L/K}H(L_S^{(1)}/L) = K^\times\cdot N_{L/K}J_L^{\Delta}\cdot N_{L/K}H(S/L) = N_{L/K}J_L^{\Delta}\cdot H(S/K)$. Hence we have $H(L_R^{(1)}/K) = H(L_S^{(1)}/K)$. This implies $L_R^{(1)} = L_S^{(1)}$, for they are both abelian over K by Remark 1.6. Now the proposition follows at once from the definition of the symbol and Remark 1.3.

When Proposition 2.1 is satisfied, we proceed to express the symbol $[d_1, d_2, a]$ by a rational quadratic symbol. Let a be a square free integer

4) See H. Hasse [7].

and $a = \prod p_i$ be the prime decomposition of a. Put

$$L = \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2}) \quad \text{and} \quad K = \boldsymbol{Q}(\sqrt{d_1 d_2}) .$$

Suppose that there is a ray class field S over K such that S contains L, $L_S^{(1)} \supsetneqq L_S^*$, S is normal over $\boldsymbol{Q}$ and each p_i has a prime divisor, say $\mathfrak{P}_i$, of degree 1 in L_S^*. Put $\mathfrak{A} = \prod \mathfrak{P}_i$. Then Proposition 2.1 implies

$$[d_1, d_2, a] = \prod [d_1, d_2, p_i] = \prod \left(\frac{L_S^{(1)}/L_S^*}{\mathfrak{P}_i}\right) = \left(\frac{L_S^{(1)}/L_S^*}{\mathfrak{A}}\right) .$$

Since K is cyclic over $\boldsymbol{Q}$, we have $L_S^* = K_S^* = K_S^{(1)}$, which we denote also by S_0. Denote by $\mathfrak{H}(S/K)$ the congruent ideal group corresponding to S over K. Let σ be the non-trivial element of $\mathrm{Gal}\,(K/\boldsymbol{Q})$ and $\mathfrak{b}$ be an ideal of K such that

$$\mathfrak{b}^{\sigma-1} \equiv N_{S_0/K}\mathfrak{A} \qquad \mathrm{mod}\ \mathfrak{H}(S/K)$$

by some ideal $\mathfrak{A}$ of S_0, and no prime divisor of $\mathfrak{b}$ is ramified in L/K. Then Proposition 1.5 implies

$$\left(\frac{L_S^{(1)}/L_S^*}{\mathfrak{A}}\right) = \left(\frac{L/K}{\mathfrak{b}}\right) = \left(\frac{d_1}{b}\right) = \left(\frac{d_2}{b}\right) \tag{3}$$

where $(b) = N_{K/\boldsymbol{Q}}\mathfrak{b}$. Let $\mathfrak{f}$ be the conductor of S/K. Then by the same way as in [6, § 1.3], we get a relation between a and b as follows. Put $\mathfrak{a} = N_{S_0/K}\mathfrak{A}$. Then $(a) = N_{K/\boldsymbol{Q}}\mathfrak{a}$. There exists an element α of K such that $\alpha \equiv 1 \bmod \mathfrak{f}$ and $(\alpha) = \mathfrak{a}\mathfrak{b}^{1-\sigma} = \mathfrak{a}\mathfrak{b}^2/N_{K/\boldsymbol{Q}}\mathfrak{b} = (\beta)/(b)$, where $(\beta) = \mathfrak{a}\mathfrak{b}^2$. We can assume that β has no rational divisor, and we have

$$ab^2 = N_{K/\boldsymbol{Q}}\beta\ , \quad b \equiv \beta \mod \mathfrak{f}\ . \tag{4}$$

Conversely let a be a rational integer such that $a = N_{K/\boldsymbol{Q}}\mathfrak{a}$ with some integral ideal $\mathfrak{a}$ of K, and suppose that a satisfies (4) with a rational integer b and an integer β of K which has no rational divisor. Then by considering the prime ideal decomposition of the both sides of (4), we have $(\beta) = \mathfrak{a}\mathfrak{b}^2$ with some integral ideal $\mathfrak{b}$ of K such that $(b) = N_{K/\boldsymbol{Q}}\mathfrak{b}$. Moreover we have

$$\mathfrak{a}\mathfrak{b}^{1-\sigma} = (\beta)/N_{K/\boldsymbol{Q}}\mathfrak{b} = (\beta/b) . \tag{5}$$

This is contained in the ray mod. $\mathfrak{f}$. Thus we have

PROPOSITION 2.2. *Let $L = \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2})$ be a bicyclic biquadratic field. Put $K = \boldsymbol{Q}(\sqrt{d_1 d_2})$ and D be the discriminant of $K/\boldsymbol{Q}$. Let $\mathfrak{f}$ be a module*

of K and S be the ray class field mod. $\mathfrak{f}$ *over K in narrow sense. Suppose that S is normal over $\boldsymbol{Q}$, contains L, and $L_S^{(1)} \supsetneqq L_S^*$. Let a be a square free rational integer such that any prime divisor of a in L_S^* is of degree* 1. *Then we have*

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

where b is any integer such that $(b, \mathfrak{f}) = 1$ and the following relations hold with some rational integers x and y:

$$\begin{cases} x^2 - Dy^2 - 4ab^2 = 0, \\ \frac{1}{2}(x + y\sqrt{D}) \equiv b \quad \text{mod. } \mathfrak{f}, \\ (b, x, y) = 1. \end{cases}$$

§ 3. Condition of $L_S^{(1)} \supsetneqq L_S^*$

Put $L = \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2})$, $K_1 = \boldsymbol{Q}(\sqrt{d_1})$, $K_2 = \boldsymbol{Q}(\sqrt{d_2})$ and $K = \boldsymbol{Q}(\sqrt{d_1 d_2})$. Let S be a ray class field over K in narrow sense. In order to get the value of the symbol $[d_1, d_2, p]$ explicitly, we determine the condition that S is normal over $\mathbf{Q}$, $S \supsetneqq L$ and $L_S^{(1)} \supsetneqq L_S^*$.

Denote by $\mathfrak{f}$ the conductor of S/K, and by $I_K(\mathfrak{f})$ or briefly I_K the group of fractional ideals of K prime to $\mathfrak{f}$. Denote by $\mathfrak{H}(L/K)$ and $\mathfrak{H}(S/K)$ the subgroups of I_K corresponding to L and S by class field theory respectively. Denote further by $\mathfrak{N}^{(1)}(S/K)$ or briefly $\mathfrak{N}^{(1)}$ the group of ideals $\mathfrak{a}$ of $I_K(\mathfrak{f})$ such that $\mathfrak{a}^\sigma \equiv \mathfrak{a}$ mod. $\mathfrak{H}(S/K)$, σ being the non-trivial element of $\mathrm{Gal}(K/\boldsymbol{Q})$. Then by [6, Proposition 5.1] we have

$$\mathrm{Gal}(L_S^{(1)}/L_S^*) \cong I_K/\mathfrak{H}(L/K)\mathfrak{N}^{(1)}(S/K). \tag{6}$$

Since $(I_K : \mathfrak{H}(L/K)) = (L : K) = 2$, it is necessary and sufficient for $L_S^{(1)} \supsetneqq L_S^*$ that $\mathfrak{N}^{(1)}(S/K) \subseteqq \mathfrak{H}(L/K)$.

PROPOSITION 3.1. *Let K be a cyclic extension of an algebraic number field k with Galois group G of order finite. Let σ be a generator of G and $\mathfrak{f}$ be a divisor of K which is σ-invariant. Denote by $S_K(\mathfrak{f})$ the group of the ray* mod. $\mathfrak{f}$ *in K. Let $\mathfrak{N}$ be the group of all ideals $\mathfrak{a}$ of K such that $\mathfrak{a}^\sigma \equiv \mathfrak{a}$* mod. $S_K(\mathfrak{f})$ *and let $\mathfrak{N}_0$ be the group generated by all ideals $\mathfrak{a}$ of K such that $\mathfrak{a}^\sigma = \mathfrak{a}$ and by principal ideals (α) of K such that $\alpha^\sigma \equiv \alpha$* mod. $\mathfrak{f}$. *Denote by $\mathfrak{S}_K$ the ray class group* mod. $\mathfrak{f}$ *of K, and denote by $C(\mathfrak{N})$ resp. $C(\mathfrak{N}_0)$ the subgroups of $\mathfrak{S}_K$ which consist of all classes represented by elements of $\mathfrak{N}$ resp.*

of $\mathfrak{R}_0$. *Denote further by* E_k *resp.* E_K *the group of units of* k *resp.* K. *Then we have the following exact sequence*

$$1 \longrightarrow C(\mathfrak{R}_0) \longrightarrow C(\mathfrak{R}) \longrightarrow (E_k \cap S_k(\mathfrak{f}))/N_{K/k}(E_K \cap S_K(\mathfrak{f}))\ ,$$

where $N_{K/k}$ *stands for the norm map of* K *to* k.

Proof. Let $\mathfrak{a} \in \mathfrak{R}$, then there exists α in $S_K(\mathfrak{f})$ such that $\mathfrak{a}^{1-\sigma} = (\alpha)$ and $N_{K/k}\alpha \in E_k \cap S_k(\mathfrak{f})$, and $N_{K/k}\alpha \bmod. N_{K/k}(E_K \cap S_K(\mathfrak{f}))$ is uniquely determined by $\mathfrak{a}$. This induces a homomorphism φ from $C(\mathfrak{R})$ to $(E_k \cap S_k(\mathfrak{f}))/N_{K/k}(E_K \cap S_K(\mathfrak{f}))$. The kernel of φ is equal to $C(\mathfrak{R}_0)$. In fact, suppose that $\mathfrak{a} \in \mathfrak{R}$ and the class of $\mathfrak{a}$ is contained in the kernel of φ. Then $N_{K/k}\alpha = N_{K/k}E$ with $E \in E_K \cap S_K(\mathfrak{f})$. This implies $\alpha = E\gamma^{1-\sigma}$, where $\gamma \in K$ and $\gamma^\sigma \equiv \gamma \bmod. \mathfrak{f}$. Put $\mathfrak{b} = \mathfrak{a}(\gamma)^{-1}$. Then $\mathfrak{b}^\sigma = \mathfrak{b}$, which is to be required.

COROLLARY 3.2. *Let* $K/\boldsymbol{Q}$ *be a cyclic extension of a prime degree and* σ *be a generator of* $\mathrm{Gal}\,(K/\boldsymbol{Q})$. *Let* $\mathfrak{f}$ *be a divisor of* K *such that* $\mathfrak{f}^\sigma = \mathfrak{f}$ *and assume that every real infinite prime divisors are contained in* $\mathfrak{f}$. *Let* S *be the ray class field* mod. $\mathfrak{f}$ *of* K. *Then* $\mathfrak{R}^{(1)}(S/K)$ *is generated by all ideals* $\mathfrak{a}$ *of* $I_K(\mathfrak{f})$ *such that* $\mathfrak{a}$ *is a prime ideal of* K *ramified in* $K/\boldsymbol{Q}$ *or* $\mathfrak{a}$ *is a principal ideal* (α) *of* K *satisfying* $\alpha^\sigma \equiv \alpha \bmod. \mathfrak{f}$.

Proof. In Proposition 3.1, we have $E_k \cap S_k(\mathfrak{f}) = \{1\}$, since $k = \boldsymbol{Q}$. Then $C(\mathfrak{R}_0) = C(\mathfrak{R})$, which implies $\mathfrak{R}^{(1)}(S/K) = \mathfrak{R} = \mathfrak{R}_0$. On the other hand, if $\mathfrak{a}$ is an ideal of K such that $\mathfrak{a}^\sigma = \mathfrak{a}$, then $\mathfrak{a}$ is a product of prime ideals of K ramified in $K/\boldsymbol{Q}$ and of ideals of $\boldsymbol{Q}$, because $K/\boldsymbol{Q}$ is cyclic of prime degree. Thus we have the corollary.

Now let $L = \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2})$ and $K = \boldsymbol{Q}(\sqrt{d_1 d_2})$ as before. Let σ be the non-trivial element of $\mathrm{Gal}\,(K/\boldsymbol{Q})$, and $\mathfrak{f}$ be a module of K such that $\mathfrak{f}^\sigma = \mathfrak{f}$. Then we have.

PROPOSITION 3.3. *Notation being as above, let* S *be the ray class field* mod. $\mathfrak{f}$ *of* K *in narrow sense. Then* S *contains* L *and* $L_S^{(1)} \supsetneq L_S^*$ *if and only if* $\mathfrak{f}$ *satisfies the following conditions*:

(i) $\mathfrak{f}$ *is divisible by the conductor of* L/K.

(ii) *The conductor of* S *over* K *is divisible by all prime divisors* $\mathfrak{p}$ *of* K *such that* $\mathfrak{p}$ *is ramified in* $K/\boldsymbol{Q}$ *and is not decomposed completely in* L/K.

(iii) *A principal ideal* (α) *of* K *is contained in* $\mathfrak{H}(L/K)$ *if* $\alpha^\sigma \equiv \alpha \bmod. \mathfrak{f}$, $(\alpha, \mathfrak{f}) = 1$ *and* α *is totally positive.*

Proof. It follows from the formula (6) that S contains L and $L_S^{(1)} \supsetneq L_S^*$

if and only if $\mathfrak{f}$ is divisible by the conductor of L/K and $\mathfrak{R}^{(1)}(S/K) \subseteqq \mathfrak{H}(L/K)$. Hence the proposition follows from Corollary 3.2 immediately.

The rest of this section is devoted to get an explicit formula for $\mathfrak{f}$ to satisfy the conditions of Proposition 3.3. Notation d_1, d_2, L and K being as above, assume that d_1, d_2 are square free. Let further $d = (d_1, d_2)$ and $d_1 d_2 = d_0 d^2$. Let $D_u = 4^{t(u)} d_u$, the discriminant of $Q(\sqrt{d_u})$ for $u = 0, 1, 2$. Thus $t(u) = 0$ or 1 according as $d_u \equiv 1 \bmod 4$ or not. Then we have

$$D_1 D_2 = D_0 f^2 , \tag{7}$$

where f is a rational integer, which coincides with the conductor of L/K, up to the infinite primes by the theorem of conductor and discriminant. Clearly

$$f = 2^t d , \tag{8}$$

where $t = t(1) + t(2) - t(0)$. Let Δ be the set of all odd rational primes p such that p divides d_0 and satisfies both $(d_1/p) \neq 1$ and $(d_2/p) \neq 1$. Put

$$\mathfrak{M} = \prod_{p \in \Delta} \mathfrak{p} , \tag{9}$$

where $\mathfrak{p}$ is the prime divisor of p in K. Then the set of these primes $\mathfrak{p}$ coincides with the set of odd primes which satisfy the condition (ii) of Proposition 3.3. Denote by $\mathfrak{l}$ the prime divisor of 2 in K when 2 is ramified in K. We put

$$\mathfrak{f}_* = 2^t \mathfrak{l}^\delta d \mathfrak{M} , \tag{10}$$

where $\delta = 0$ or 1 and $\delta = 1$ only when the following condition (11) is satisfied for both d_1 and d_2 at once:

$$t = 0 , \quad d_0 \not\equiv 1 \bmod 4 , \quad d_1 \not\equiv 1 \bmod 8 \quad \text{and} \quad d_2 \not\equiv 1 \bmod 8 . \tag{11}$$

Then the case of $\delta = 1$ occurs only when the prime divisor of 2 in K satisfies the condition (ii) of Proposition 3.3 and f is odd. Thus in order that $\mathfrak{f}$ satisfies the condition (ii), it is necessary that $\mathfrak{f}$ is a multiple of $\mathfrak{f}_*$.

Now denote by d_i and d_j either one and the other of d_1 and d_2. We separate the type of the pair (d_1, d_2) by the following table, in which the module $\mathfrak{f}_*$ is given by (10) and we define a module $\mathfrak{f}_0$ of K according to the type.

Table 1

Type	Condition for d_1 and d_2	$\mathfrak{f}_*$	$\mathfrak{f}_0$
A B	$d_1 \equiv d_2 \equiv 1 \bmod 4$ $d_i \equiv 1 \bmod 8,\quad d_j \not\equiv 1 \bmod 4$	$d\mathfrak{M}$	$d\mathfrak{M}$
CS CT	$d_i \equiv 5 \bmod 8,\quad d_j \not\equiv 1 \bmod 4,\quad d_1 d_2 < 0$ $d_i \equiv 5 \bmod 8,\quad d_j \not\equiv 1 \bmod 4,\quad d_1 d_2 > 0$	$\mathfrak{l}d\mathfrak{M}$	$\mathfrak{l}d\mathfrak{M}$
DS DT	$d_1 \equiv d_2 \equiv -1 \bmod 4$ $d_i \equiv -1 \bmod 4,\quad d_j \equiv 2 \bmod 4$	$4d\mathfrak{M}$ $2d\mathfrak{M}$	$4d\mathfrak{M}$
ES ET	$d_1 \equiv d_2 \equiv 2 \bmod 4,\quad d_0 \equiv 1 \bmod 4$ $d_1 \equiv d_2 \equiv 2 \bmod 4,\quad d_0 \equiv -1 \bmod 4$	$4d\mathfrak{M}$ $2d\mathfrak{M}$	$4d\mathfrak{M}$ $2\mathfrak{l}d\mathfrak{M}$

PROPOSITION 3.4. *Let d_1 and d_2 be mutually different square free integers, and put $d = (d_1, d_2)$, $d_1 d_2 = d_0 d^2$. Let $L = \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2})$ and $K = \boldsymbol{Q}(\sqrt{d_0})$. Define modules $\mathfrak{M}$ and $\mathfrak{f}_0$ of K by* (9) *and Table* 1. *Let further $\mathfrak{f}$ be a module of K invariant by* $\mathrm{Gal}(K/\boldsymbol{Q})$, *and S be the ray class field* mod. $\mathfrak{f}$ *of K in narrow sense. Then $S \supseteq L$ and $L_S^{(1)} \supseteq L_S^*$ if and only if $\mathfrak{f}$ is divisible by $\mathfrak{f}_0$ and the prime divisor of 2 in K is ramified in S except the case A and B.*

Proof. It is necessary and sufficient for $S \supseteq L$ and $L_S^{(1)} \supseteq L_S^*$ that f satisfies the conditions (i), (ii) and (iii) of Proposition 3.3. It was sufficient for the condition (i) and necessary for the condition (ii) that $\mathfrak{f}$ is divisible by $\mathfrak{f}_*$. Let us show that the condition (iii) is satisfied if $\mathfrak{f}$ is divisible by $\mathfrak{f}_0$. Let α be an integer of K, $(\alpha, f) = 1$, and σ be the non-trivial element of $\mathrm{Gal}(K/\boldsymbol{Q})$. Then it is easy to see that $\alpha^\sigma \equiv \alpha \bmod \mathfrak{f}_0$ if and only if α is expressed as follows with some rational integers x and y.

$$\alpha = \begin{cases} (x + dy\sqrt{d_0})/2\,, \quad x \equiv y \bmod 2 & \text{for the type } A; \\ x + dy\sqrt{d_0} & \text{for the type } B, C; \\ x + 2dy\sqrt{d_0} & \text{for the type } D, E\,. \end{cases}$$

Then since $d_1 d_2 = d_0 d^2$, we have

$$N\alpha = \begin{cases} (x^2 - d_1 d_2 y^2)/4\,, \quad x \equiv y \bmod 2 & \text{for the type } A; \\ x^2 - d_1 d_2 y^2 & \text{for the type } B, C; \\ x^2 - 4 d_1 d_2 y^2 & \text{for the type } D, \mathrm{E}; \end{cases}$$

where N stands for the norm from K to $\boldsymbol{Q}$. We claim $(d_i/N\alpha) = 1$ for all the types. For the type A, B or C, we have $d_i \equiv 1 \bmod. 4$. Hence $(d_i/N\alpha) = (N\alpha/d_i) = 1$. For the type D, we have $(\mathfrak{f}_0, 2) \neq 1$. Hence $(\alpha, \mathfrak{f}_0) = 1$ implies $(x, 2) = 1$ and $x^2 \equiv 1 \bmod. 8$. Hence $N\alpha \equiv 1 \bmod. 4$, which implies $(d_i/N\alpha) = (N\alpha/d_i) = 1$. Finally for the type E, we have $d_i = 2d_i'$ with $(d_i', 2) = 1$. Moreover we have $N\alpha \equiv 1 \bmod. 8$ by the same way as for the type D. Then $(d_i/N\alpha) = (2/N\alpha)(d_i'/N\alpha) = (N\alpha/d_i') = 1$. Thus we have proved that $\mathfrak{f}$ satisfies the condition (iii) of Proposition 3.3, if $\mathfrak{f}$ is divisible by $\mathfrak{f}_0$. Except for the type DT and ET, we have $\mathfrak{f}_* = \mathfrak{f}_0$. Hence it is also necessary for $S \supseteq L$ and $L_S^{(1)} \supseteq L_S^*$ that $\mathfrak{f}$ is divisible by $\mathfrak{f}_0$. We claim that it is necessary also for the type DT and ET. First we treat of the type DT. Then $2 = \mathfrak{l}^2$ in K. Put $\mathfrak{f}' = \mathfrak{l}^\mu d\mathfrak{M}$ with $\mu < 4$. Then α being as above, we have $\alpha^\sigma \equiv \alpha \bmod. \mathfrak{f}'$ if and only if $y \equiv 0 \bmod. d$. Thus $N\alpha = x^2 - d_1 d_2 y^2$. When both x and y are odd, we see that $N\alpha \equiv -1 \bmod. 4$. Then we have $(d_i/N\alpha) = -(N\alpha/d_i) = -1$, which does not satisfy the condition (iii) of Proposition 3.3. Hence it is necessary that $\mu \geqq 4$. Next we treat of the type ET. We have also $2 = \mathfrak{l}^2$ in K. Put $\mathfrak{f}' = 2d\mathfrak{M}$. Then as above, we see that $\alpha^\sigma \equiv \alpha \bmod. \mathfrak{f}'$ if and only if $y \equiv 0 \bmod. d$, and then $N\alpha \equiv 5 \bmod. 8$ for odd x and y. This implies $(d_i/N\alpha) = -1$. Hence the condition of the theorem is necessary.

Remark 3.5. There does not necessarily exist a ray class field over K with conductor $\mathfrak{f}$. We have to pay special attension to the type CT that there does not necessarily exist a ray class field S over K with a conductor $\mathfrak{l}^\mu$ when $\mu < 3$ and $(E_K : E_K \cap S_K(\mathfrak{l}^\mu)) = 2^{\mu-1}$.

§ 4. Genus field in a ray class field of an abelian field

In order to get an explicit expression for the value of $[d_1, d_2, p]$ we need to know the genus field L_S^* explicitly. For the sake of convenience we treat of the genus fields in general at first (c.f. [4]).

Let k be any algebraic number field of finite degree, and $k_\mathfrak{p}$ its completion at a prime $\mathfrak{p}$. For a non-negative integer m we denote by $U_\mathfrak{p}(m)$ as before the group of all units α of $k_\mathfrak{p}$ such that $\alpha \equiv 1 \bmod. \mathfrak{p}^m$. Then $U_\mathfrak{p}(0)$ is the group of all units of $k_\mathfrak{p}$, which we denote also by $U_\mathfrak{p}$. Let K *be an abelian extension of* k *of finite degree, and* $\mathfrak{P}$ *be a prime divisor of* $\mathfrak{p}$ in K. Let T be the ramification group of $\mathfrak{P}$ in K/k. For $\sigma \in T$ let

$$v_\mathfrak{P}(\sigma) \equiv \mathrm{Max}\{i \mid \alpha^\sigma = \alpha \bmod. \mathfrak{P}^{i+1} \text{ for all integer } \alpha \text{ of } K\}\,. \tag{12}$$

Then the inverse function $\varphi_{\mathfrak{P}}^{-1}$ of Hasse's function $\varphi_{\mathfrak{P}}$ is defined by

$$\varphi_{\mathfrak{P}}^{-1}(v) = \frac{1}{e}\left(\sum_{\sigma \in T} \min\{v_{\mathfrak{P}}(\sigma), v\}\right), \tag{13}$$

where e is the order of T.

Denote by $N_{\mathfrak{P}}$ the norm map from $K_{\mathfrak{P}}$ to $k_{\mathfrak{p}}$. Then it is well-known[5] that

$$N_{\mathfrak{P}}U_{\mathfrak{P}}(m) = N_{\mathfrak{P}}U_{\mathfrak{P}} \cap U_{\mathfrak{p}}(i), \tag{14}$$

when $\varphi_{\mathfrak{P}}(i-1) < m \leqq \varphi_{\mathfrak{P}}(i)$.

Now [4, Proposition 2] is generalized as follows.

THEOREM 4.1. *Let k be an algebraic number field of finite degree and K be a class field over k corresponding to an idele group H of k. Let $\mathfrak{f} = \prod \mathfrak{P}^{m_{\mathfrak{p}}}$ be a divisor of K, and S be the ray class field* mod. $\mathfrak{f}$ *over K. Assume that S is normal over k. Denote by S_0 the maximal abelian extension of k contained in S, and by H^* the idele group of k corresponding to S_0. Then we have*

$$H^* = k^{\times} \prod_{\mathfrak{p}} (H \cap U_{\mathfrak{p}}(i_{\mathfrak{p}})),$$

where $k^{\times}$ denotes the principal idele group of k, and $i_{\mathfrak{p}}$ is the integer determined by

$$\varphi_{\mathfrak{P}}(i_{\mathfrak{p}} - 1) < m_{\mathfrak{P}} \leqq \varphi_{\mathfrak{P}}(i_{\mathfrak{p}}).$$

Proof. Since $H(S/K) = K^{\times} \prod_{\mathfrak{P}} U_{\mathfrak{P}}(m_{\mathfrak{P}})$, we have

$$H^* = k^{\times}N_{K/k}H(S/K) = k^{\times} \prod_{\mathfrak{P}} N_{\mathfrak{P}}U_{\mathfrak{P}}(m_{\mathfrak{P}}).$$

Moreover since $H \cap U_{\mathfrak{p}} = N_{\mathfrak{P}}U_{\mathfrak{P}}$, we have $N_{\mathfrak{P}}U_{\mathfrak{P}}(m_{\mathfrak{P}}) = N_{\mathfrak{P}}U_{\mathfrak{P}} \cap U_{\mathfrak{p}}(i_{\mathfrak{p}}) = H \cap U_{\mathfrak{p}}(i_{\mathfrak{p}})$ by (14), which is to be proved.

When $k = \boldsymbol{Q}$, the rational number field, we have more explicitly the following theorem.

THEOREM 4.2. *Let K be an abelian extension of $\boldsymbol{Q}$ of finite degree. Let $\mathfrak{f} = \prod_{\mathfrak{P}} \mathfrak{P}^{m_{\mathfrak{p}}}$ be a module of K which is invariant by* Gal $(K/\boldsymbol{Q})$, *and S be the ray class field* mod. $\mathfrak{f}$ *over K in narrow sense. Let i_p be the integer such that $\varphi_{\mathfrak{P}}(i_p - 1) < m_{\mathfrak{P}} \leqq \varphi_{\mathfrak{P}}(i_p)$, and put $f = \prod_p p^{i_p}$. Then the genus*

5) C.f. for instance, S. Iyanaga [9, Ch. V, § 2].

field K_S^* of K with respect to $S/\boldsymbol{Q}$ is given by

$$K_S^* = K_\sharp^* \boldsymbol{Q}(fp_\infty) ,$$

where $K_\sharp^*$ is the genus field of K in absolute sense and $\boldsymbol{Q}(fp_\infty)$ is the ray class field mod. f *over $\boldsymbol{Q}$ in narrow sense.*

Proof. Let H^* be the idele group of $\boldsymbol{Q}$ corresponding to K_S^*. Then

$$H^* = \boldsymbol{Q}^\times \prod_p (H \cap U_p(i_p))U_{p_\infty}(1) ,$$

by Theorem 4.1. Clearly

$$\boldsymbol{Q}^\times \prod_p (H \cap U_p(i_p))U_{p_\infty}(1) \subseteqq \boldsymbol{Q}^\times \prod_p (H \cap U_p)U_{p_\infty}(1) \cap \boldsymbol{Q}^\times \prod_p U_p(i_p)U_{p_\infty}(1) .$$

On the other hand, let

$$\alpha, \beta \in \boldsymbol{Q}^\times , \quad u \in \prod_p (H \cap U_p)U_{p_\infty}(1) , \quad v \in \prod_p U_p(i_p)U_{p_\infty}(1)$$

and $\alpha u = \beta v$. Then since

$$\boldsymbol{Q}^\times \cap \prod_p U_p U_{p_\infty}(1) = \{1\} ,$$

we have

$$u = \alpha^{-1}\beta v \in \boldsymbol{Q}^\times \prod_p U_p(i_p)U_{p_\infty}(1) \cap \prod_p (H \cap U_p)U_{p_\infty}(1) \subseteqq \prod_p U_p(i_p)U_{p_\infty}(1).$$

Hence

$$H^* = \boldsymbol{Q}^\times \prod_p (H \cap U_p)U_{p_\infty}(1) \cap \boldsymbol{Q}^\times \prod_p U_p(i_p)U_{p_\infty}(1) .$$

This implies the theorem by [4, Proposition 2].

Let us determine f of Theorem 4.2 explicitly when $K = \boldsymbol{Q}(\sqrt{d_0})$, where d_0 is a square free integer. In this case we have by (12), for a non-trivial element σ of T,

$$v_{\mathfrak{P}}(\sigma) = \begin{cases} 0 & \text{if } \mathfrak{P} \nmid 2 \text{ and } \mathfrak{P} \mid d_0 , \\ 1 & \text{if } \mathfrak{P} \mid 2 \text{ and } d_0 \equiv -1 \bmod 4 , \\ 2 & \text{if } \mathfrak{P} \mid 2 \text{ and } 2 \mid d_0 . \end{cases}$$

Hence by (13),

$$\varphi_{\mathfrak{P}}^{-1}(v) = \begin{cases} v & \text{when } T = \{1\} , \\ \frac{1}{2}(v + \operatorname{Min}\{0, v\}) & \text{when } p \neq 2 \text{ and } p \mid d_0 , \\ \frac{1}{2}(v + \operatorname{Min}\{1, v\}) & \text{when } p = 2 \text{ and } d_0 \equiv -1 \bmod 4 , \\ \frac{1}{2}(v + \operatorname{Min}\{2, v\}) & \text{when } p = 2 \text{ and } 2 \mid d_0 . \end{cases}$$

Now we have

THEOREM 4.3. *Let* $K = \boldsymbol{Q}(\sqrt{d_0})$ *be a quadratic field and* $\mathfrak{f} = \prod_{\mathfrak{P}} \mathfrak{P}^{m_{\mathfrak{P}}}$ *a module of* K *which is invariant by* $\mathrm{Gal}(K/\boldsymbol{Q})$. *Let* S *be the ray class field* mod. $\mathfrak{f}$ *over* K *in narrow sense, and* K_S^* *be the genus field of* K *with respect to* $S/\boldsymbol{Q}$. *Let* p *be the rational prime divided by* $\mathfrak{P}$ *and put*

$$f = \prod p^{i_p} , \tag{15}$$

where i_p *is determined as follows*:

$$\begin{aligned}
&i_p = m_p \quad && \text{when } p \text{ is unramified in } K/\boldsymbol{Q} ;\\
&i_p = m_p \quad && \text{when } m_p = 1 ;\\
&i_p = m_p \quad && \text{when } p = 2,\ 2 \mid d_0 \text{ and } m_p = 2 ;\\
&m_p/2 \leqq i_p < (m_p + 2)/2 \quad && \text{when } p \neq 2 \text{ and } p \mid d_0 ;\\
&(m_p + 1)/2 \leqq i_p < (m_p + 3)/2 \quad && \text{when } p = 2,\ d_0 \equiv -1 \bmod. 4 \text{ and } m_p > 1 ;\\
&(m_p + 2)/2 \leqq i_p < (m_p + 4)/2 \quad && \text{when } p = 2,\ 2 \mid d \text{ and } m_p > 2 .
\end{aligned}$$

Then we have

$$K_S^* = K_\sharp^* \boldsymbol{Q}(fp_\infty) ,$$

where $K_\sharp^*$ *is the genus field of* K *in absolute sense, and* $\boldsymbol{Q}(fp_\infty)$ *is the ray class field* mod. f *over* $\boldsymbol{Q}$ *in narrow sense.*

§ 5. Explicit expression for $[d_1, d_2, a]$

THEOREM 5.1. *Let* d_1, d_2 *be a pair of square free integers. Let* $d = (d_1, d_2)$, $d_1 d_2 = d_0 d^2$ *and* $K = \boldsymbol{Q}(\sqrt{d_0})$. *Denote by* $\Lambda = \Lambda(d_1, d_2)$ *be the set of odd prime divisors* p *of* d_0 *which satisfy both of* $(d_1/p) \neq 1$ *and* $(d_2/p) \neq 1$. *Put*

$$m = \prod_{p \in \Lambda} p .$$

We separate the type of the pair (d_1, d_2) *by Table* 1 *in* § 3, *and put*

$$f = 2^\nu dm ,$$

where ν *is given by*

$$\nu = \begin{cases} 0 & \text{for the type } A, B ;\\ 2 & \text{for the type } CS, DS, ES ;\\ 3 & \text{for the type } CT, DT, ET . \end{cases} \tag{16}$$

Let D_i *be the discriminant of* $\boldsymbol{Q}(\sqrt{d_i})$ *for* $i = 0, 1, 2$, *and let* $D_0 = \prod q_j^*$ *be*

the decomposition of D_0 to prime discriminants[6].

For a square free positive integer a, the symbol $[d_1, d_2, a]$ is defined when each rational prime divisor p of a satisfies the following conditions:

(i) $(d_i/p) = 1$ *when p is not a divisor of D_i, for $i = 0, 1, 2$.*

(ii) $(q_j^*/p) = 1$ *for all q_j^* such that $p \neq q_j$.*

(iii) $p \equiv 1 \bmod f$.

When the conditions are satisfied, we have

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

where b is any solution of the following Diophantine equations, provided that $(b, 2^\nu d_1 d_2) = 1$, $(b, x, y) = 1$ and m_1 is any integer such that $mm_1 \equiv 1 \bmod 8d$:

$$4ab^2 = (2b + dmx)^2 - d_1 d_2 y^2 \qquad \text{for the type } A;$$
$$ab^2 = (b + dmx)^2 - d_1 d_2 y^2 \qquad \text{for the type } B;$$
$$ab^2 = (b + 2dmx)^2 - 4d_1 d_2 y^2 \qquad \text{for the type } CS;$$
$$ab^2 = (b + 4dmx)^2 - 16d_1 d_2 y^2 \qquad \text{for the type } CT, DT, ET;$$
$$ab^2 = (b + 2dm(2x + m_1 y))^2 - 4d_1 d_2 y^2 \qquad \text{for the type } DS, ES.$$

Proof. Let $\mu = 0$ for the type A or B; $\mu = 1$ for the type CS; and $\mu = 2$ for other type. Define divisors $\mathfrak{M}$ and $\mathfrak{f}$ of K by

$$\mathfrak{M} = \prod \mathfrak{P}, \qquad \mathfrak{f} = 2^\mu d\mathfrak{M},$$

where $\mathfrak{P}$ runs over all the distinct prime divisors of p in K for $p \in \Lambda$. Let S be the ray class field mod. $\mathfrak{f}$ over K in narrow sense. First we claim that $L_S^* = K_\sharp^* \boldsymbol{Q}(fp_\infty)$, where $K_\sharp^*$ is the absolute genus field and $\boldsymbol{Q}(fp_\infty)$ is the ray class field mod. f over $\boldsymbol{Q}$ in narrow sense. Let $\mathfrak{f} = \prod \mathfrak{P}^{m_\mathfrak{P}}$ be the prime decomposition of $\mathfrak{f}$ in K and i_p be the integer determined from m_p by Theorem 4.3. If $p \neq 2$, then $m_p = 1$ or 0 and hence $i_p = 1$ or 0 according as $p \mid f$ or not. If $p = 2$ we have the following table for m_p and i_p

Type	m_p	i_p
A, B	0	0
CS, DS	2	2
CT, DT	4	3
ES	3	3
ET	6	4

6) This means that $q_j^* = (-1)^{(q-1)/2} q$ for a prime $q_j \neq 2$ and $q_j^* = -4$ or ± 8 for $q_j = 2$ (c.f. Hasse [8]).

Regarding $2 \mid d$ only for the type ES or ET, we have $\prod p^{i_p} = 2^\nu dm$, hence $L_S^* = K_\sharp^* \boldsymbol{Q}(fp_\infty)$ by Theorem 4.3.

It is easy to see that $K_\sharp^* \supsetneqq \boldsymbol{Q}(2^\nu)$ except the case CS. This implies that the prime divisor of 2 is ramified in S except the case A and B, and Proposition 3.4 implies $L_S^{(1)} \supsetneqq L_S^*$, because $\mathfrak{f}$ is divisible by $\mathfrak{f}_0$.

Now the conditions (i), (ii) and (iii) of the present theorem is equivalent[7] to that p is decomposed in L_S^* in prime divisors of degree 1. Moreover the condition (iii) implies $(p, \mathfrak{f}) = 1$, since f is divisible by $\mathfrak{f}$. Therefore the symbol $[d_1, d_2, p]$ is defined when p satisfies the conditions (i), (ii) and (iii) of the theorem. When that is the case for every prime divisors p of a, it follows from Proposition 2.2 that

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

where b is any integer for which there exist integers u and v such that

$$4ab^2 = u^2 - D_0 v^2 , \tag{17}$$

$$\tfrac{1}{2}(u + v\sqrt{D_0}) \equiv b \mod \mathfrak{f} \tag{18}$$

and

$$(b, u, v) = 1 . \tag{19}$$

Let us reduce the condition (18) to a rational expression.

First we treat of the case $d_0 \equiv 1 \bmod 4$. Then since $\mathfrak{M} \mid \sqrt{d_0}$, the condition (18) is equivalent with $u - 2b \equiv 0 \bmod m$ and

$$\frac{1}{2}(u - 2b - v) + v\frac{1 + \sqrt{d_0}}{2} \equiv 0 \mod 2^\mu d .$$

Moreover it is easy to see that the condition is equivalent with $v = 2^\mu dy$, $u - 2b = mt$ and $mt \equiv 2^\mu dy \bmod 2^{\mu+1}d$ with some integers y and t. Let m_1 be an integer such that $mm_1 \equiv 1 \bmod 2^{\mu+1}d$. Then $mt \equiv 2^\mu dy \bmod 2^{\mu+1}d$ if and only if $t = m_1 2^\mu dy + 2^{\mu+1}dx$ with an integer x. Hence the condition (18) is equivalent with $v = 2^\mu dy$ and $u = 2b + 2^\mu dm(m_1 y + 2x)$. Since $d^2 d_0 = d_1 d_2$, we have $4ab^2 = (2b + 2^\mu dm(2x + m_1 y))^2 - 4^\mu d_1 d_2 y^2$, and this implies the theorem for the type A, DS and ES.

Secondly we treat of the case $d_0 \not\equiv 1 \bmod 4$. Then since $D_0 = 4d_0$, replacing u by $2u$, the condition (17) and (18) are equivalent with $ab^2 =$

7) C.f. Hasse [8].

$u^2 - d_0v^2$ and $u + v\sqrt{d_0} \equiv b \bmod \mathfrak{f}$. The last congruence is equivalent with $v \equiv 0 \bmod. 2^\mu d$ and $u \equiv b \bmod. 2^\mu dm$. Put $u = b + 2^\mu dmx$ and $v = 2^\mu dy$ with integers x and y. Then we have $ab^2 = (b + 2^\mu dmx)^2 - 4^\mu d_1d_2y$. This implies the theorem for the type B, C, DT and ET, and now the proof of the theorem is completed.

DEFINITION 5.2. For a triple of integers d_1, d_2 and a, we call $[d_1, d_2, a]$ is *strictly defined* (in the sense of Theorem 5.1), if the square free parts of d_1 and d_2 satisfy the conditions (i), (ii) and (iii) of Theorem 5.1.

Remark 5.3. There are triples d_1, d_2, a for which the symbol $[d_1, d_2, a]$ is not defined strictly in the sense of Theorem 5.1, but defined in primitive sense (Definition 1.1). Especially by reason of Remark 3.5, it can offen occur for the type CT. In fact, let $K = \boldsymbol{Q}(\sqrt{d_1d_2})$ and suppose that $(E_K : E_K \cap S_K(\mathfrak{f}^\mu)) < 2^{\mu-1}$ in the notation of Remark 3.5. Then $[d_1, d_2, a]$ is defined in primitive sense even if the condition $\nu = 3$ is replaced by $\nu = 2$ for the type CT in Theorem 5.1. When that is the case, the value of $[d_1, d_2, a]$ is obtained by replacing the Diophantine equation by $ab^2 = (b + 2dmx)^2 - 4d_1d_2y^2$ in Theorem 5.1. For instance [3, 13, 61] is not defined strictly in the sense of Theorem 5.1, but it is defined in primitive sense and $[3, 13, 61] = -1$. In this case, the fundamental unit of $\boldsymbol{Q}(\sqrt{3\cdot 13})$ is $25 + 4\sqrt{3\cdot 13}$, which is congruent to 1 mod. 4.

When the special case where $d_i = -1$, we can express the value of the symbol by means of biquadratic residue symbols as follows.

THEOREM 5.4. (i) *Let p and q be rational primes such that $p \equiv q \equiv 1$ mod. 4 and $(q/p) = 1$. Then $[-1, q, p]$ is defined, and we have*

$$[-1, q, p] = \left(\frac{q}{p}\right)_4 \left(\frac{p}{q}\right)_4 .$$

(ii) *Let p be a rational prime such that $p \equiv 1$ mod. 8. Then $[-1, 2, p]$ and $[-1, p, 2]$ are both defined and we have*

$$[-1, 2, p] = [-1, p, 2] = \left(\frac{p}{2}\right)_4 \left(\frac{2}{p}\right)_4 ,$$

where $(p/2)_4$ is defined by setting its value 1 or -1 according as $p \equiv 1$ or -1 mod. 16.

(iii) *Let p be a rational prime such that $p \equiv 1$ mod. 4. Then $[-1, p, p]$ is defined and we have*

$$[-1, p, p] = \left(\frac{-1}{p}\right)_4 = \left(\frac{2}{p}\right).$$

Proof. It is clear by Theorem 5.1 that the symbols are all defined.

(i) This follows from the explicit formula of the symbol in Theorem 5.1 and [6, Proposition 5.4][8]. Another direct proof from the definition of the symbol is as follows. Let $L = \boldsymbol{Q}(\sqrt{-1}, \sqrt{q})$ and B be the subfield of the ray class field in narrow sense mod. q over $\boldsymbol{Q}$ of degree 4. Let Λ be the subfield of $L(\sqrt[4]{q})B$ which is quadratic over L and different from both of $L(\sqrt[4]{q})$ and LB. Then Λ is non-abelian central over $\boldsymbol{Q}$, and we have $\Lambda = L_\Lambda^{(1)} \supsetneqq L_\Lambda^* = L$. Moreover let $K = \boldsymbol{Q}(\sqrt{-q})$ and f be as in Theorem 5.1 for a pair $(-1, q)$. Then $f = 1$ or 4 according as $q \equiv 1$ or 5 mod. 8. Let S be the ray class field mod. f in narrow sense over K. Then we have $\Lambda \subseteqq S$. Now let $\mathfrak{p}$ be a prime divisor of p in L_S^*, which is of degree 1 since the symbol $[-1, q, p]$ is defined. Let further P be the prime of L divisible by $\mathfrak{p}$. Then we have

$$[-1, q, p] = \left(\frac{L_S^{(1)}/L_S^*}{\mathfrak{p}}\right) = \left(\frac{\Lambda/L}{P}\right)$$
$$= \left(\frac{L(\sqrt[4]{q})/L}{P}\right)\left(\frac{B/L}{P}\right) = \left(\frac{q}{p}\right)_4\left(\frac{p}{q}\right)_4.$$

(ii) Let $L = \boldsymbol{Q}(\sqrt{-1}, \sqrt{2})$, and B be the cyclotomic field of the 16-th roots of unity. Let Λ be the subfield of $L(\sqrt[4]{2})B$ which is quadratic over L different from both of $L(\sqrt[4]{2})$ and LB. Then Λ is non-abelian central over $\boldsymbol{Q}$, and we have $\Lambda = L_\Lambda^{(1)} \supsetneqq L_\Lambda^* = L$. Moreover let $K = \boldsymbol{Q}(\sqrt{-2})$ and f be as in Theorem 5.1 for a pair $(-1, 2)$. Then $f = 8$. Let S be the ray class field mod. f over K in narrow sense. Then we have $\Lambda \subseteqq S$. Now let $\mathfrak{p}$ be a prime divisor of p in L_S^*, and P be the prime of L divisible by $\mathfrak{p}$. Then we have

$$[-1, 2, p] = \left(\frac{L_S^{(1)}/L_S^*}{\mathfrak{p}}\right) = \left(\frac{\Lambda/L}{P}\right) = \left(\frac{L(\sqrt[4]{2})/L}{P}\right)\left(\frac{B/L}{P}\right).$$

We have further $((B/L)/P) = 1$ if and only if $p \equiv 1$ mod. 16, which is equivalent, by definition, that $(p/2)_4 = 1$. Hence $[-1, 2, p] = (2/p)_4(p/2)_4$. The formula $[-1, p, 2] = (2/p)_4(p/2)_4$ is proved in the same way as (i).

(iii) Theorem 5.1 implies $[-1, p, p] = (p/b)$, where b is a solution of Diophantine equations $pb^2 = x^2 + py^2$ or $pb^2 = x^2 + 4py^2$ according as $p \equiv 1$

8) C.f. also E. Lehmer [11] and P. Kaplan [10].

or 5 mod. 8, provided that $(b, x, y) = 1$ and $b \neq 2$. These equations are equivalent with $b^2 = px_1^2 + y^2$ or $b^2 = px_1^2 + 4y^2$ by setting $x = px_1$. Hence we have $(p/b) = (b/p) = (b^2/p)_4$, which is equal to $(y^2/p)_4 = (y/p) = (p/y) = 1$ or $(4y^2/p)_4 = (2/p)(y/p) = (2/p) = -1$ according as $p \equiv 1$ or 5 mod. 8.

§ 6. Inversion law

We shall show in this section that a simple relation holds between $[d_1, d_2, d_3]$ and $[d_1, d_3, d_2]$, when both of them are defined. First we prepare the following

THEOREM 6.1. *Let a and d be two positive square free odd integers relatively prime. Suppose that $(q^*/p) = 1$, $(a^*/q) = 1$ and $(d/p) = 1$ for all primes p dividing a and for all primes q dividing d, where $m^* = (-1)^{(m-1)/2}m$ for any odd integer m. Then we have the following formulas.*

(i) $$[a^*, d^*, a] = \begin{cases} \left(\frac{d^*}{a}\right)_4 & \text{when } a \equiv 1 \bmod 4\,, \\ \left(\frac{a^*}{d}\right)_4 & \text{when } a \equiv -1 \bmod 4 \text{ and } d \equiv 1 \bmod 4. \end{cases}$$

(ii) $$[a, 2d, a] = \left(\frac{2d}{a}\right)_4, \quad \text{if } p \equiv 1 \bmod 8 \text{ for all primes } p \text{ dividing } a\,.$$

(iii) $$[2a, d, 2a] = \left(\frac{d}{2a}\right)_4, \quad \text{if } d \equiv 1 \bmod 8 \text{ and } p \equiv 1 \bmod 8 \text{ for all primes } p \text{ dividing } a\,.$$

Proof. (i) By Theorem 5.1, we have $[a^*, d^*, a] = (a^*/b) = (d^*/b)$, where b is a solution of the Diophantine equation $4ab^2 = x^2 - a^*d^*y^2$. Put $\varepsilon = a^*/a$ and $x = ax_1$. Then the above equation is replaced by $4b^2 = ax_1^2 - \varepsilon d^*y^2$. Suppose $a \equiv 1$ mod. 4. Then $\varepsilon = 1$ and we have $(a^*/b) = (b/a) = (b^2/a)_4 = (-4d^*y^2/a)_4 = (-1/a)_4(2/a)(d^*/a)_4(y/a) = (d^*/a)_4(a/y) = (d^*/a)_4$. Next suppose that $a \equiv -1$ mod. 4. Then $\varepsilon = -1$ and $d \equiv 1$ mod. 4. Hence we have $(d^*/b) = (b/d) = (b^2/d)_4 = (4ax_1^2/d)_4 = (2/d)(a/d)_4(x_1/d) = (-1/d)_4(a/d)_4(d/x_1) = (a^*/d)_4$.

(ii) Assume that $a \equiv 1$ mod. 8. Then by Theorem 5.1, we have $[a, 2d, a] = (a/b)$, where $ab^2 = x^2 - 2day^2$ with integers x and y. Put $x = ax_1$. Then $b^2 = ax_1^2 - 2dy^2$, and we have $(a/b) = (b/a) = (b^2/a)_4 = (-2dy^2/a)_4 = (-1/a)_4(2d/a)_4(y/a) = (2d/a)_4(a/y) = (2d/a)_4$.

(iii) Assume that $d \equiv 1$ mod. 8. Then Theorem 5.1 implies that $[-2a, d, 2a] = (d/b)$, where b is any solution of Diophantine equation $2ab^2 = x^2 + 2ady^2$, provided $(b, x, y) = 1$ and $b \neq 2$. Put $x = 2ax_1$. Then $b^2 =$

$2ax_1^2 + dy_2$. This implies $(d/b) = (b^2/d)_4 = (2ax_1^2/d)_4 = (2a/d)_4(x_1/d)$ and further $(x_1/d) = (d/x_1) = 1$. Hence we have $[-2a, d, 2a] = (2a/d)_4$. On the other hand $[2a, d, 2a] = [-2a, d, 2a][-1, d, 2][-1, d, a]$, and Theorem 5.2 implies $[-1, d, 2] = (d/2)_4(2/d)_4$ and $[-1, d, a] = (d/a)_4(a/d)_4$. Hence we have $[2a, d, 2a] = (2a/d)_4(d/2)_4(2/d)_4(d/a)_4(a/d)_4 = (2a/d)(d/2a)_4 = (d/2a)_4$. Thus the theorem is proved.

Now we have the following inversion formula.

THEOREM 6.2. *Let p_1, p_2 and p_3 be odd prime numbers which are relatively prime. Suppose that $p_1 \equiv p_2 \equiv 1 \bmod 4$. Then we have*

(i) $[\pm p_1, p_2, p_3] = [\pm p_1, p_3, p_2]$,

(ii) $[\pm p_3, p_1, p_2] = [\pm p_3, p_2, p_1]$,

when the both sides are defined strictly in each formula.

Proof. (i) Put $p_3^* = p_3$ or $-p_3$ according as $p_3 \equiv 1 \bmod 4$ or not. Put further $A_2 = [p_1, p_2, p_3]$, $B_2 = [p_1, p_3^*, p_3]$, $A_3 = [p_1, p_3^*, p_2]$, $B_3 = [p_1, p_2, p_2]$ and $B_{23} = [p_1, p_2p_3^*, p_2p_3]$. If A_2 and A_3 are both defined strictly, then B_2, B_3 and B_{23} are also defined strictly, and $A_2B_2A_3B_3 = B_{23}$ by Theorems 5.1 and 1.7. Moreover Theorem 6.1 implies $B_2 = (p_1/p_3)_4$ or $(p_3^*/p_1)_4$ according as $p_3^* = p_3$ or not, and $B_3 = (p_1/p_2)_4$. In the same way we have $B_{23} = (p_1/p_2p_3)_4$ or $(p_2p_3^*/p_1)_4$ according as $p_3^* = p_3$ or not. Hence $B_2B_3 = B_{23}$ or $B_{23}(p_1/p_2)_4(p_2/p_1)_4$ according as $p_3^* = p_3$ or not. Since $(p_1/p_2)_4(p_2/p_1)_4 = [p_1, -1, p_2]$ by Theorem 5.4, it follows from Theorem 1.7 that $[p_1, p_2, p_3] = [p_1, p_3, p_2]$. If $[-p_1, p_2, p_3]$ is defined strictly, then necessarily $p_3 \equiv 1 \bmod 4$. Hence

$$[-p_1, p_2, p_3] = [-1, p_2, p_3][p_1, p_2, p_3] = [-1, p_3, p_2][p_1, p_3, p_2] = [-p_1, p_3, p_2] .$$

(ii) Put $A_2 = [-p_3, p_1, p_2]$, $B_2 = [-p_3, p_1, p_1]$, $A_3 = [-p_3, p_2, p_1]$, $B_3 = [-p_3, p_2, p_2]$ and $B_{23} = [-p_3, p_1p_2, p_1p_2]$. Suppose that A_2 and A_3 are defined strictly. Then B_2, B_3 and B_{23} are also defined strictly by Theorem 5.1, and we have $A_2B_2A_3B_3 = B_{23}$. Moreover $B_2 = (-p_3/p_1)_4$, $B_3 = (-p_3/p_2)_4$ and $B_{23} = (-p_3/p_1p_2)_4$ by Theorem 6.1. Hence $A_2A_3 = 1$, namely $[-p_3, p_1, p_2] = [-p_3, p_2, p_1]$. Moreover $[-1, p_1, p_2]$ is defined strictly and equal to $[-1, p_2, p_1]$. Hence Theorem 1.7 implies $[p_3, p_1, p_2] = [p_3, p_2, p_1]$.

When one of p_i is 2, we have the following theorem in the same way as Theorem 6.2 by applying (ii) and (iii) of Theorem 6.1.

THEOREM 6.3. *Let p_1 and p_2 be mutually different odd prime numbers. Then we have*

(i) $[\pm 2, p_1, p_2] = [\pm 2, p_2, p_1]$,

(ii) $[\pm p_1, 2, p_2] = [\pm p_1, p_2, 2]$,

when the both sides are defined strictly in each formula.

Remark 6.4. Theorems 6.2 and 6.3 cover the possible inversion formulas except the case where only one of p_i $(i = 1, 2, 3)$ is congruent to 1 mod. 4. For the exceptional case, say $p_1 \equiv 1$ and $p_2 \equiv p_3 \equiv -1$ mod. 4, it is conjectured with numerical evidence[9] that the formula $[-p_2, p_1, p_3] = [-p_2, p_3, p_1]$ holds, which is only the possible case. However the author has no proof as yet.

§ 7. Table of $[d_1, d_2, p]$

In the following we give a table of the values of the symbols $[d_1, d_2, p]$ for small numbers d_1, d_2 and p, which are computed according to Theorem 5.1. In order to get the values, it is fundamental by Theorem 1.7 and Proposition 1.8 to have the values of $[-1, p_2, p_3]$, and $[\pm p_1, \pm p_2, p_3]$ for prime numbers p_1, p_2 and p_3. In the following table we have the values of the symbols which are defined strictly, p_i running over the prime numbers smaller than 50 for $i = 1, 2, 3$.

We use the following notation:

d_1, d_2, p = prime number with sign ± 1 or $d_1 = -1$.

$R = [d_1, d_2, p]$, which is equal to (d_1/q), q determined as below .

$m = |d_1^{e_1} d_2^{e_2}|$, where $e_i = 1$ when $(d_j/d_i) \neq 1$ for $i \neq j$ $(i, j = 1, 2)$, and $e_i = 0$ otherwise .

q, x, y = the solution of the following Diophantine equation such that y is the smallest positive possible integer and q is the smallest possible prime number for this y, provided $q \leqq 3571$.

$4pq^2 = (2q + mx)^2 - d_1 d_2 y^2$ for the type A ,

$pq^2 = (q + mx)^2 - d_1 d_2 y^2$ for the type B ,

$pq^2 = (q + 2mx)^2 - 4d_1 d_2 y^2$ for the type CS ,

$pq^2 = (q + 4mx)^2 - 16 d_1 d_2 y^2$ for the type CT or DT ,

$pq^2 = (q + 2m(2x + m_1 y))^2 - 4d_1 d_2 y^2$ for the type DS ,

9) C.f. Table of § 7.

where $mm_1 \equiv 1 \bmod 8$, $(q, x, y) = 1$ and $(q, 2^\delta d_1 d_2) = 1$, provided $\delta = 0$ for the type A or B, and $\delta = 1$ otherwise.

d_1	d_2	p	R	Type	m	q	x	y
−1	17	2	−1	B	1	3	−2	1
−1	41	2	1	B	1	5	−2	1
2	−7	2	−1	B	1	3	−1	1
2	17	2	1	B	1	47	31	7
−2	17	2	−1	B	1	5	−1	1
2	−23	2	−1	B	1	5	−3	1
2	−31	2	1	B	1	7	−1	1
2	41	2	−1	B	1	3	7	1
−2	41	2	−1	B	1	7	−3	1
2	−47	2	1	B	1	7	−5	1
−7	23	2	1	B	1	11	−2	1
7	−31	2	−1	B	1	11	−6	1
7	−47	2	−1	B	1	13	−10	1
17	47	2	1	B	1	19	20	1
17	−47	2	−1	A	1	11	−9	1
−23	31	2	−1	B	1	19	−16	1
23	41	2	−1	B	1	3	28	1
−23	41	2	−1	A	1	11	−17	1
−23	47	2	1	B	1	31	−2	1
31	41	2	−1	B	1	7	30	1
−31	41	2	−1	A	1	13	−17	1
−31	47	2	−1	B	1	29	−14	1
−3	13	3	−1	A	1	2	−1	1
−3	37	3	1	A	1	7	−2	2
−11	37	3	−1	A	1	13	−6	2
13	−23	3	−1	A	1	5	−9	1
37	−47	3	−1	A	1	13	−9	1
−1	5	5	−1	CS	1	3	1	1
−1	−5	5	1	DS	1	29	9	1
−1	29	5	1	CS	1	5	−1	1
−1	−29	5	−1	DS	1	7	3	1

d_1	d_2	p	R	Type	m	q	x	y
−1	41	5	−1	*B*	1	3	−1	1
−1	−41	5	1	*DS*	1	5	3	1
5	−11	5	−1	*A*	1	2	1	1
5	−19	5	1	*A*	1	11	8	4
5	29	5	−1	*A*	1	2	11	1
5	−29	5	1	*CS*	1	11	−3	1
−5	29	5	−1	*CS*	1	11	−3	1
−5	−29	5	−1	*DS*	1	17	7	1
5	−31	5	−1	*A*	1	3	−1	1
5	41	5	1	*A*	1	31	88	4
5	−41	5	−1	*CS*	1	13	−4	1
−5	41	5	−1	*B*	1	11	9	1
−5	−41	5	−1	*DS*	1	31	11	1
11	−19	5	−1	*CS*	1	13	−5	1
−11	31	5	−1	*CS*	1	17	−4	1
19	−31	5	−1	*B*	1	11	−7	1
31	41	5	−1	*B*	1	7	66	2
−31	41	5	1	*A*	1	59	104	4
2	−7	7	−1	*B*	1	3	4	1
2	−31	7	−1	*B*	1	3	−2	1
2	−47	7	−1	*B*	1	5	4	1
−3	−7	7	−1	*A*	3	5	6	2
−3	−19	7	−1	*A*	3	2	3	1
−3	−31	7	1	*A*	3	7	11	3
−3	37	7	−1	*A*	1	2	−3	1
−7	29	7	−1	*A*	1	3	1	1
−7	37	7	−1	*A*	1	5	11	1
37	−47	7	1	*A*	1	53	145	3
5	−11	11	−1	*A*	1	2	7	1
5	−19	11	−1	*A*	1	2	5	1
−7	37	11	−1	*A*	1	5	19	1
−11	37	11	1	*A*	1	47	38	14
−1	3	13	−1	*DS*	3	7	0	1

d_1	d_2	p	R	Type	m	q	x	y
−1	13	13	−1	*CS*	1	7	3	3
−1	−13	13	1	*DS*	1	17	12	3
−1	17	13	−1	*B*	1	3	7	1
−1	−17	13	1	*DS*	1	13	10	3
−1	29	13	−1	*CS*	1	3	−1	1
−1	−29	13	1	*DS*	1	5	4	1
3	−13	13	−1	*DS*	3	41	4	3
−3	13	13	−1	*A*	1	2	9	1
3	23	13	1	*DS*	3	13	−4	27
3	−23	13	−1	*B*	1	5	11	1
−3	43	13	1	*CS*	1	7	2	1
−3	−43	13	−1	*A*	3	2	11	3
13	17	13	−1	*A*	1	5	29	1
13	−17	13	1	*CS*	1	53	58	3
−13	17	13	1	*B*	1	19	33	3
−13	−17	13	1	*DS*	1	7	8	1
13	−23	13	1	*A*	1	3	7	1
13	29	13	1	*A*	1	23	240	12
13	−29	13	−1	*CS*	1	37	14	3
−13	29	13	−1	*CS*	1	37	14	3
−13	−29	13	−1	*DS*	1	23	30	3
13	−43	13	1	*A*	1	17	44	4
17	43	13	−1	*B*	1	5	52	2
17	−43	13	1	*A*	1	13	21	3
−23	29	13	−1	*A*	1	11	53	1
23	−43	13	−1	*CS*	1	61	26	3
−1	2	17	−1	*DT*	1	3	2	1
−1	−2	17	−1	*DT*	1	7	6	2
−1	13	17	−1	*CS*	1	7	9	2
−1	−13	17	−1	*DS*	1	3	4	2
−1	17	17	1	*B*	1	13	38	4
−1	−17	17	1	*DS*	1	13	18	8
2	17	17	−1	*B*	1	3	14	2
2	−17	17	1	*DT*	1	31	22	2
−2	17	17	−1	*B*	1	5	12	2

d_1	d_2	p	R	Type	m	q	x	y
−2	−17	17	1	*DT*	1	3	46	8
−2	19	17	−1	*DT*	1	7	2	1
−2	−19	17	1	*CT*	1	11	14	2
−2	43	17	1	*DT*	1	41	10	4
−2	−43	17	−1	*CT*	1	5	18	2
2	47	17	1	*DT*	1	89	70	1
2	−47	17	−1	*B*	1	5	2	2
13	17	17	1	*A*	1	43	288	8
13	−17	17	−1	*CS*	1	19	16	2
−13	17	17	1	*B*	1	19	32	4
−13	−17	17	−1	*DS*	1	43	36	2
13	43	17	−1	*CT*	1	5	448	19
13	−43	17	1	*A*	1	23	−32	8
17	19	17	−1	*B*	1	7	27	1
17	−19	17	−1	*A*	1	3	11	1
17	43	17	−1	*B*	1	5	29	1
17	−43	17	−1	*A*	1	7	37	1
17	47	17	1	*B*	1	19	440	16
17	−47	17	1	*A*	1	53	268	8
−19	43	17	−1	*CS*	1	29	3	2
−19	47	17	−1	*CS*	1	29	−13	2
−43	47	17	−1	*CS*	1	71	80	2
−3	−19	19	−1	*A*	3	2	5	1
−3	−31	19	−1	*A*	3	11	30	6
5	−19	19	1	*A*	1	11	54	6
5	−31	19	−1	*A*	1	3	17	1
17	−19	19	−1	*A*	1	3	13	1
2	−7	23	1	*B*	1	23	76	13
2	−23	23	−1	*B*	1	5	18	1
2	41	23	−1	*B*	1	3	14	1
−7	29	23	−1	*A*	1	3	19	1
−11	−23	23	−1	*A*	11	7	5	1
13	−23	23	1	*A*	1	3	17	1
13	29	23	1	*A*	1	23	178	2

d_1	d_2	p	R	Type	m	q	x	y
13	−43	23	−1	A	1	5	−2	2
−23	29	23	−1	A	1	11	70	2
−23	41	23	1	A	1	59	250	14
41	−43	23	1	A	1	23	158	2
−1	5	29	1	CS	1	29	62	7
−1	−5	29	−1	DS	1	11	14	7
−1	7	29	−1	DS	7	11	−16	5
−1	−7	29	−1	B	7	3	2	2
−1	13	29	−1	CS	1	7	15	1
−1	−13	29	1	DS	1	17	94	53
−1	29	29	−1	CS	1	19	34	5
−1	−29	29	1	DS	1	5	6	1
5	29	29	−1	A	1	2	83	7
5	−29	29	−1	CS	1	7	11	1
−5	29	29	1	CS	1	7	11	1
−5	−29	29	−1	DS	1	17	148	25
−7	23	29	−1	B	1	3	7	1
−7	−23	29	1	A	7	2	3	1
7	−29	29	−1	DS	7	17	−1	1
−7	29	29	−1	A	1	3	23	1
−7	−29	29	1	B	7	11	15	7
13	−23	29	−1	A	1	5	41	1
13	29	29	−1	A	1	2	25	1
13	−29	29	1	CS	1	53	17	7
−13	29	29	1	CS	1	53	17	7
−13	−29	29	1	DS	1	11	48	5
−23	29	29	−1	A	1	11	36	4
2	−23	31	−1	B	1	5	22	1
2	−31	31	1	B	1	7	24	3
2	41	31	−1	B	1	3	16	1
−3	5	31	−1	A	15	2	1	3
−3	−31	31	−1	A	3	11	34	2
−3	−43	31	−1	A	3	2	7	1
5	−11	31	−1	A	1	2	17	1

d_1	d_2	p	R	Type	m	q	x	y
5	−31	31	−1	*A*	1	3	25	1
5	41	31	−1	*A*	1	3	38	2
−23	41	31	−1	*A*	1	7	34	2
−31	41	31	1	*A*	1	113	1014	6
41	−43	31	1	*A*	1	23	177	3
−1	3	37	1	*DS*	3	13	4	1
−1	37	37	−1	*CS*	1	19	9	9
−1	−37	37	1	*DS*	1	137	197	33
−1	41	37	−1	*B*	1	3	10	2
−1	−41	37	1	*DS*	1	5	7	1
−3	7	37	−1	*CS*	1	5	12	1
−3	−7	37	−1	*A*	3	5	17	1
3	11	37	−1	*DS*	3	17	−1	7
3	−11	37	−1	*CS*	1	7	17	1
3	−37	37	−1	*DS*	3	7	1	1
−3	37	37	1	*A*	1	7	60	4
3	47	37	−1	*DS*	3	5	5	11
3	−47	37	−1	*B*	1	5	23	1
−7	11	37	−1	*B*	1	3	13	1
−7	37	37	−1	*A*	1	5	27	3
7	−47	37	1	*B*	1	3	−1	1
−11	37	37	1	*A*	1	47	424	12
−11	47	37	1	*CS*	1	23	4	3
37	41	37	−1	*A*	1	13	196	4
37	−41	37	1	*CS*	1	269	−116	21
−37	41	37	1	*B*	1	31	117	3
−37	−41	37	1	*DS*	1	19	911	47
37	−47	37	−1	*A*	1	31	−25	9
−1	2	41	1	*DT*	1	17	19	10
−1	−2	41	1	*DT*	1	17	23	1
−1	5	41	−1	*CS*	1	3	7	2
−1	−5	41	−1	*DS*	1	11	15	2
−1	37	41	−1	*CS*	1	19	27	8
−1	−37	41	−1	*DS*	1	3	7	2

d_1	d_2	p	R	Type	m	q	x	y
−1	41	41	1	*B*	1	61	308	20
−1	−41	41	1	*DS*	1	5	9	2
2	5	41	−1	*CT*	5	3	1	1
2	−5	41	−1	*DT*	5	11	1	5
−2	5	41	−1	*CS*	5	7	3	4
−2	−5	41	1	*DT*	5	3	1	1
2	23	41	−1	*DT*	1	3	413	61
2	−23	41	−1	*B*	1	5	24	2
2	31	41	−1	*DT*	1	13	19	1
2	−31	41	−1	*B*	1	3	8	2
2	41	41	−1	*B*	1	3	38	4
2	−41	41	−1	*DT*	1	13	7	2
−2	41	41	−1	*B*	1	7	34	2
−2	−41	41	−1	*DT*	1	29	331	37
−2	43	41	−1	*DT*	1	29	−5	5
−2	−43	41	−1	*CT*	1	5	11	1
−5	23	41	1	*DS*	5	83	1	8
−5	−23	41	−1	*B*	5	11	20	8
5	31	41	−1	*CT*	1	7	15	1
5	−31	41	1	*A*	1	19	205	1
5	41	41	−1	*A*	1	3	35	1
5	−41	41	1	*CS*	1	11	15	2
−5	41	41	−1	*B*	1	11	30	4
−5	−41	41	1	*DS*	1	3	71	10
−5	43	41	1	*DS*	5	263	66	2
−5	−43	41	−1	*CT*	5	19	29	10
−23	31	41	−1	*B*	1	7	29	1
23	41	41	1	*B*	1	43	326	8
−23	41	41	1	*A*	1	59	456	16
23	−43	41	1	*CS*	1	41	17	4
31	41	41	1	*B*	1	5	282	8
−31	41	41	1	*A*	1	113	20	40
31	−43	41	1	*CS*	1	23	−2	2
37	41	41	1	*A*	1	73	1412	32
37	−41	41	−1	*CS*	1	31	46	2
−37	41	41	1	*B*	1	31	92	4

d_1	d_2	p	R	Type	m	q	x	y
−37	−41	41	−1	*DS*	1	83	215	10
41	43	41	−1	*B*	1	11	71	1
41	−43	41	−1	*A*	1	19	85	5
−3	−7	43	−1	*A*	3	5	19	3
−3	13	43	1	*A*	1	43	366	54
−3	−19	43	1	*A*	3	7	50	18
−3	−43	43	−1	*A*	3	2	13	3
−7	−43	43	1	*A*	7	11	46	18
13	17	43	−1	*A*	1	5	62	2
13	−43	43	1	*A*	1	17	138	6
17	−19	43	−1	*A*	1	3	29	1
17	−43	43	−1	*A*	1	7	29	3
41	−43	43	−1	*A*	1	19	177	3
2	17	47	1	*B*	1	47	1090	187
2	−23	47	1	*B*	1	31	168	11
2	−31	47	−1	*B*	1	3	16	1
2	−47	47	1	*B*	1	7	40	1
−11	37	47	1	*A*	1	3	2	2
17	−19	47	−1	*A*	1	3	31	1
17	−43	47	−1	*A*	1	3	25	1
17	−47	47	1	*A*	1	53	270	22
−23	−31	47	−1	*A*	23	11	6	2
−23	−47	47	1	*A*	23	71	190	134
37	−47	47	−1	*A*	1	31	361	1

References

[1] A. Fröhlich, On fields of class two, Proc. London Math. Soc. (3), **4** (1954), 235–256.
[2] ——, A prime decomposition symbol for certain non Abelian number fields, Acta Sci. Math., **21** (1960), 229–246.
[3] Y. Furuta, A reciprocity law of the power residue symbol, J. Math. Soc. Japan, **10** (1958), 46–54.
[4] ——, The genus field and genus number in algebraic number fields, Nagoya Math. J., **29** (1967), 281–285.
[5] ——, On nilpotent factors of congruent ideal class groups of Galois extensions, Nagoya Math. J., **62** (1976), 13–28.

[6] ——, Note on class number factors and prime decompositions, Nagoya Math. J., **66** (1977), 167–182.
[7] H. Hasse, Normenresttheorie galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante abelscher Zahlkörper, J. Fac. Sci. Tokyo Imp. Univ., **2** (1934), 477–498.
[8] ——, Zur Geschlechtertheorie in quadratischen Zahlkörper, J. Math. Soc. Japan, **3** (1951), 45–51.
[9] S. Iyanaga, The theory of numbers, North Holland/American Elsevier (1975).
[10] P. Kaplan, Représentation de nombres premiers par des formes quadratiques binaires de discriminant $-\pi$, oú $\pi \equiv 1 \bmod 4$), C. R. Acad. Sc. Paris, **275** (1973), 1535–1537.
[11] E. Lehmer, On some special quartic reciprocity laws, Acta Arith., **21** (1972), 367–377.
[12] L. Redei, Ein neues zahlentheoretisches Symbol mit Anwendungen auf Theorie der quadratischen Zahlkörper, J. reine und angew. Math., **180** (1939), 1–43.
[13] S. Shirai, On the central class field mod. m of Galois extensions of an algebraic number field, Nagoya Math. J., **71** (1978), 61–85.

Kanazawa University