On Rédei's dihedral extension and triple reciprocity law

By Fumiya AMANO

Faculty of Mathematics, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka 819-0395, Japan

(Communicated by Heisuke HIRONAKA, M.J.A., Dec. 12, 2013)

Abstract: In this paper, we give an arithmetic characterization of Rédei's dihedral extension over $\mathbf{Q}$ and another simple proof of the reciprocity law of the triple symbol.

Key words: Rédei extension; Rédei triple symbol.

Introduction. As is well known, for two odd prime numbers p and q, the Legendre symbol $(\frac{p}{q})$ describes the decomposition law of q in the quadratic extension $\mathbf{Q}(\sqrt{p})/\mathbf{Q}$. Here we note that the number field $\mathbf{Q}(\sqrt{p})$ for $p \equiv 1 \pmod 4$ is characterized as the unique quadratic extension of $\mathbf{Q}$ where only p is ramified.

In 1939, L. Rédei ([R]) introduced a certain triple symbol with the intension of a generalization of the Legendre symbol and Gauss' genus theory. For three prime numbers $p_1, p_2, p_3 \equiv 1 \pmod 4$ with $(\frac{p_i}{p_j}) = 1$ $(1 \leqq i \neq j \leqq 3)$ Rédei's triple symbol $[p_1, p_2, p_3]$ describes the decomposition law of p_3 in a dihedral extension $K/\mathbf{Q}$ of degree 8, (i.e., a Galois extension $K/\mathbf{Q}$ with the Galois group $\mathrm{Gal}(K/\mathbf{Q})$ being the dihedral group D_8 of order 8) which is constructed as follows. By the assumptions on p_1 and p_2, there are integers x, y, z such that

$$x^2 - p_1 y^2 - p_2 z^2 = 0, \ \text{g.c.d}(x, y, z) = 1,$$
$$y \equiv 0 \pmod 2, \ x - y \equiv 1 \pmod 4.$$

Then Rédei's extension $K/\mathbf{Q}$ is given by

$$K = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha}), \ \alpha = x + y\sqrt{p_1}.$$

It can be shown that $K/\mathbf{Q}$ is a dihedral extension of degree 8 such that only p_1 and p_2 are ramified among all prime numbers. A meaning of Rédei's extension $K/\mathbf{Q}$ was explained by M. Morishita ([Mi]) from the viewpoint of the analogy with link theory where Rédei's triple symbol $[p_1, p_2, p_3]$ is interpreted as a triple linking number.

In this note we give an arithmetic characterization of Rédei's dihedral extension as follows (see Theorem 2.1):

Theorem. *Let p_1 and p_2 be prime number such that*

$$p_i \equiv 1 \ (\mathrm{mod}\ 4) \ (i = 1, 2), \ \left(\frac{p_i}{p_j}\right) = 1 \ (1 \leqq i \neq j \leqq 2).$$

Let K be a dihedral extension over $\mathbf{Q}$ such that all prime numbers ramified in $K/\mathbf{Q}$ are only p_1 and p_2 with ramification index 2. Then, changing p_1 and p_2 if necessary, there are integers x, y, z satisfying

$$x^2 - p_1 y^2 - p_2 z^2 = 0, \ \text{g.c.d}(x, y, z) = 1,$$
$$y \equiv 0 \pmod 2, \ x - y \equiv 1 \pmod 4,$$

such that

$$K = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha}), \ \alpha = x + y\sqrt{p_1}.$$

We also give another simple proof of the reciprocity law of Rédei's triple symbol in Section 3.

Notation. For a number field k we denote by $\mathcal{O}_k$ the ring of integers of k.

1. Rédei's dihedral extension and its uniqueness. In this section, we recall the construction of Rédei's dihedral extension ([R]). Since Rédei's account ([R]) was written in a rather classical and complicated manner, we give here a presentation by clarifying arguments using modern algebraic number theory.

Let p_1 and p_2 be distinct prime number such that $p_1, p_2 \equiv 1 \pmod 4$ and $(\frac{p_1}{p_2}) = (\frac{p_2}{p_1}) = 1$. We set $k_i = \mathbf{Q}(\sqrt{p_i})$ $(i = 1, 2)$.

Lemma 1.1. *There are integers x, y, z satisfying the following condition*:
(1) $x^2 - p_1 y^2 - p_2 z^2 = 0$,
(2) $\text{g.c.d}(x, y, z) = 1$, $y \equiv 0 \pmod 2$, $x - y \equiv 1 \pmod 4$.
Furthermore, for a given prime ideal $\mathfrak{p}$ of $\mathcal{O}_{k_1}$ lying over p_2, we can find integers x, y, z which satisfy (1), (2) and $(x + y\sqrt{p_1}) = \mathfrak{p}^m$ for an odd positive integer m.

Proof. Since $(\frac{p_1}{p_2}) = 1$, p_2 is decomposed in k_1,

2010 Mathematics Subject Classification. Primary 11R32; Secondary 11A15.

doi: 10.3792/pjaa.90.1

say $(p_2)=\mathfrak{p}\mathfrak{p}'$. Since $p_1\equiv 1 \pmod 4$, the class number, say c, of k_1 is odd by genus theory ([O]) and hence $\mathfrak{p}^c=(\alpha)$ for some $\alpha=\frac{s+t\sqrt{p_1}}{2}\in\mathcal{O}_{k_1}, s,t\in\mathbf{Z}, s\equiv t \pmod 2$. Since $N((\alpha))=N\mathfrak{p}^c=p_2^c$, $N_{k_1/\mathbf{Q}}(\alpha)=\frac{s^2-p_1t^2}{4}=\pm p_2^c$. Since $p_1\equiv 1 \pmod 4$, there is a unit $\epsilon\in\mathcal{O}_{k_1}^\times$ such that $N_{k_1/\mathbf{Q}}(\epsilon)=-1$ and so we may assume $N_{k_1/\mathbf{Q}}(\alpha)=p_2^c$.

(i) Case $p_1\equiv 1 \pmod 8$: If $s\equiv t\equiv 1 \pmod 2$, $s^2\equiv t^2\equiv 1 \pmod 8$ and so $s^2-p_1t^2\equiv 0 \pmod 8$. Hence we have $2|p_2^c$, which is a contradiction. Therefore we have $s\equiv t\equiv 0 \pmod 2$. Putting $x=\frac{s}{2}$, $y=\frac{t}{2}$, $\alpha=x+y\sqrt{p_1}$ and $x^2-p_1y^2=p_2^c=p_2z^2$, $z=p_2^{(c-1)/2}$. This implies $y\equiv 0 \pmod 2$ and we can take a suitable sign of x if necessary so that $x-y\equiv 1 \pmod 4$.

(ii) Case $p_1\equiv 5 \pmod 8$: If $s\equiv t\equiv 0 \pmod 2$, we can find $x,y,z\in\mathbf{Z}$ satisfying (1) and (2) as in the case (i). Now assume that $s\equiv t\equiv 1 \pmod 2$. Then we have $s^2+3t^2p_1\equiv 3s^2+t^2p_1\equiv 0 \pmod 8$ and so

$$\begin{aligned}\alpha^3&=\left(\frac{s+t\sqrt{p_1}}{2}\right)^3\\&=\frac{s(s^2+3t^2p_1)+t(3s^2+t^2p_1)\sqrt{p_1}}{8}=x+y\sqrt{p_1},\end{aligned}$$

where we put $x=\frac{s(s^2+3t^2p_1)}{8}$ and $y=\frac{t(3s^2+t^2p_1)}{8}$. Therefore $x^2-p_1y^2=N_{k_1/\mathbf{Q}}(\alpha^3)=p_2^{3c}$, $z=p_2^{(3c-1)/2}$. Then $y\equiv 0 \pmod 2$ and we can take a suitable sign of x so that $x-y\equiv 1 \pmod 4$. □

Let $\boldsymbol{a}=(x,y,z)$ be a triple of integers satisfying the conditions (1), (2) in Lemma 1.1. We let $\alpha=x+y\sqrt{p_1}$ and set

$$K_{\boldsymbol{a}}=\mathbf{Q}(\sqrt{p_1},\sqrt{p_2},\sqrt{\alpha}).$$

Firstly, we have the following theorem due to Rédei ([R]). (1) can be easily proved and (2) can also be proved using the well-known Lemma 1.3 below on the ramification in a Kummer extension.

Theorem 1.2 ([R]). (1) *The extension $K_{\boldsymbol{a}}/\mathbf{Q}$ is a Galois extension whose Galois group is the dihedral group D_8 of order 8.*
(2) *Let $d(k_1(\sqrt{\alpha})/k_1)$ be the relative discriminant of the extension $k_1(\sqrt{\alpha})/k_1$. Then we have $N_{k_1/\mathbf{Q}}(d(k_1(\sqrt{\alpha})/k_1))=(p_2)$.*

In particular, all prime numbers which ramified in $K_{\boldsymbol{a}}/\mathbf{Q}$ are p_1 and p_2.

Lemma 1.3 ([B]). *Let l be a prime number and F a number field containing a primitive l-th root of unity. Let $L=F(\sqrt[l]{a})$ $(a\in\mathcal{O}_F)$ be a Kummer extension over F of degree l.*
(1) *Suppose that the principal ideal (a) of F is decomposed as $\mathfrak{p}^h\mathfrak{a}$ where $\mathfrak{p}$ is a prime ideal in F, $(\mathfrak{p},\mathfrak{a})=1$, $h>0$ and $(h,l)=1$. Then $\mathfrak{p}$ is totally ramified in K/F.*
(2) *Suppose $(a)=\mathfrak{q}^h\mathfrak{b}$ where $\mathfrak{q}$ is a prime ideal in F which does not divide l, $(\mathfrak{q},\mathfrak{b})=1$ and $l|h$. Then $\mathfrak{q}$ is unramified in K/F.*

The fact that $K_{\boldsymbol{a}}$ is independent of choice of $\boldsymbol{a}$ was shown by Rédei ([R]). Here we give an alternative proof based on the proof communicated by D. Vogel (a letter to M. Morishita, 2008, February).

Proposition 1.4. *Let θ be an algebraic integer in k_1 satisfying the following conditions:*
(1) *$N_{k_1/\mathbf{Q}}(\theta)=p_2h^2$ for some $h\in\mathbf{Z}\setminus\{0\}$.*
(2) *$d(k_1(\sqrt{\theta})/k_1)=\mathfrak{q}$, for a prime ideal $\mathfrak{q}$ of $\mathcal{O}_{k_1}$ lying over p_2.*

Then $k_1(\sqrt{\theta})$ is uniquely determined.

Proof. Let θ' be another algebraic integer so that θ' satisfies the above conditions (1), (2) in Proposition 1.4. We will show $k_1(\sqrt{\theta})=k_1(\sqrt{\theta'})$. First, note that the extension $k_1(\sqrt{\theta},\sqrt{\theta'})/k_1$ is unramified outside $\mathfrak{q}$ and ∞. Therefore $k_1(\sqrt{\theta/\theta'})/k_1$ is unramified outside ∞. But, since $p_1\equiv 1 \pmod 4$, the narrow ideal class number of k_1 is odd by genus theory ([O]). Therefore $k_1(\sqrt{\theta/\theta'})=k_1$, hence $k_1(\sqrt{\theta})=k_1(\sqrt{\theta'})$. □

Corollary 1.5. *The field $K_{\boldsymbol{a}}$ is independent of a choice of $\boldsymbol{a}$, namely depends only on an ordered pair (p_1,p_2).*

Proof. Let $\boldsymbol{a}'=(x',y',z')$ be another integers satisfying the conditions (1), (2) in Lemma 1.1. We let $\alpha'=x+y\sqrt{p_1}$ and $\overline{\alpha'}=x-y\sqrt{p_1}$. By Theorem 1.2, we have

$$d(k_1(\sqrt{\alpha})/k_1)=d(k_1(\sqrt{\alpha'})/k_1) \text{ or } d(k_1(\sqrt{\overline{\alpha'}})/k_1).$$

By Proposition 1.4, $k_1(\sqrt{\alpha})=k_1(\sqrt{\alpha'})$ or $k_1(\sqrt{\overline{\alpha'}})$, therefore $K_{\boldsymbol{a}}=K_{\boldsymbol{a}'}$. Hence $K_{\boldsymbol{a}}$ is independent of a choice of $\boldsymbol{a}$. □

By Corollary 1.5, we denote by $k_{(p_1,p_2)}$ the field $K_{\boldsymbol{a}}$. In fact, we show in the following theorem that the field $k_{(p_1,p_2)}$ is independent of an order of p_1 and p_2. We note that Morton showed a related result in Lemma 11 of [Mt].

Theorem 1.6. *We have*

$$K_{(p_1,p_2)}=K_{(p_2,p_1)}.$$

Proof. Let x_2,y_2,z_2 be integers satisfying the conditions (1) $x^2-p_2y^2-p_1z^2=0$, (2) $(x_2,y_2,z_2)=1$, $y_2\equiv 0 \pmod 2$, $x_2-y_2\equiv 1 \pmod 4$ in Lemma 1.1 so that

$$K_{(p_2,p_1)} = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha_2}), \quad \alpha_2 = x_2 + y_2\sqrt{p_2}.$$

We let $\overline{\alpha}_2 := x_2 - y_2\sqrt{p_2}$ and $\alpha_1 := 2x_2 + 2z_2\sqrt{p_2} = \alpha_2 + \overline{\alpha}_2 + 2z_2\sqrt{p_2} = (\sqrt{\alpha_2} + \sqrt{\overline{\alpha}_2})^2 \in k_1$. Since only one prime ideal $\mathfrak{p}$ of k_1 is ramified in $k_1(\sqrt{\alpha_1})/k_1$ and $\mathfrak{p}$ is one of prime ideal of k_1 lying over p_2, we have

$$N_{k_1/\mathbf{Q}}(\alpha_1) = (2x_2)^2 - p_1(2z_2)^2 = p_2(2y_2)^2,$$
$$d(k_1(\sqrt{\alpha})/k_1) = d(k_1(\sqrt{\alpha_1})/k_1) \text{ or } d(k_1(\overline{\alpha_1})/k_1).$$

Therefore, by Proposition 1.4, $k_1(\sqrt{\alpha}) = k_1(\sqrt{\alpha_1})$ or $k_1(\sqrt{\overline{\alpha_1}})$. Hence we have

$$\begin{aligned} K_{(p_1,p_2)} &= \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha}) \\ &= \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha_1}) \\ &= \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha_2}) \\ &= K_{(p_2,p_1)}. \end{aligned}$$

□

Definition 1.7. By Theorem 1.6, we denote by $K_{\{p_1,p_2\}}$ the field $K_{(p_1,p_2)}$ and call the extension $K_{\{p_1,p_2\}}/\mathbf{Q}$ the *Rédei extension* associated to a set $\{p_1,p_2\}$ satisfying and $p_1, p_2 \equiv 1 \pmod 4$ and $(\frac{p_2}{p_1}) = (\frac{p_1}{p_2}) = 1$.

2. A characterization of the Rédei extension. We keep the same notation as in Section 2. Here is our main theorem.

Theorem 2.1. *Let p_1 and p_2 be prime numbers such that*

$$p_i \equiv 1 \pmod 4 \ (i = 1, 2),$$
$$\left(\frac{p_i}{p_j}\right) = 1 \ (1 \leqq i \neq j \leqq 2).$$

For a number field K, the following conditions are equivalent.
(1) K is the Rédei extension $K_{\{p_1,p_2\}}$.
(2) K is a dihedral extension of degree 8 over $\mathbf{Q}$ such that prime numbers ramified in $K/\mathbf{Q}$ are only p_1 and p_2 with ramification index 2.

Proof. (1) ⇒ (2) is nothing but Rédei's theorem (Theorem 1.2). Therefore it suffice to show (2) ⇒ (1). Let $k_i = \mathbf{Q}(\sqrt{p_i})$ $(i = 1, 2)$ and $k_{12} = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2})$. First, we show that $k_{12} \subset K$. Since $\mathrm{Gal}(K/\mathbf{Q}) = D_8$ contains three distinct subgroups of index 2, there are three distinct quadratic subextensions in $K/\mathbf{Q}$ by Galois theory. Since all prime numbers ramified in $K/\mathbf{Q}$ are only p_1 and p_2, these three quadratic extensions must be k_1, k_2 and $\mathbf{Q}(\sqrt{p_1p_2})$. Therefore $k_{12} = k_1k_2 \subset K$. By the structure of the group D_8, we have three distinct quadratic subextensions of K/k_1.

Let L be one of these three fields which is different from k_{12}. Then there is $\alpha = x + y\sqrt{p_1} \in k_1 (x, y \in \mathbf{Z})$ such that $L = k_1(\sqrt{\alpha})$ and $K = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha})$. By the assumption $(\frac{p_1}{p_2}) = 1$, p_2 is decomposed into two prime ideals, say $\mathfrak{p}_1$ and $\mathfrak{p}_2$, in k_1. Then, by Lemma 1.3 and the assumption that all of prime numbers ramified in $K/\mathbf{Q}$ is p_1 and p_2 with ramification index 2, we have the following decomposition in k_1:

$$(\alpha) = \mathfrak{p}_1{}^{a_1}\mathfrak{p}_2{}^{a_2}\mathfrak{a}^2,$$

where a_1, a_2 are non-negative integers and $\mathfrak{a}$ is an integral ideal of k_1 prime to $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Then we have

$$N_{k_1/\mathbf{Q}}(\alpha) = ep_2^{a_1+a_2}b^2, \ e = 1 \text{ or } -1,$$
$$b \text{ is a non-zero integer.}$$

Here we show that e must be 1. Assume $e = -1$. Let $\overline{\alpha} = x - y\sqrt{p_1}$. Since $K/\mathbf{Q}$ is a Galois extension, $\overline{\alpha} \in K$ and so

$$K \ni \sqrt{\alpha}\sqrt{\overline{\alpha}} = \sqrt{N_{k_1/\mathbf{Q}}(\alpha)} = \sqrt{-p_2^{a_1+a_2}b^2}.$$

Since $b \in \mathbf{Z}, \sqrt{p_2} \in K$, we have $\sqrt{-1} \in K$, which implies that 2 is ramified in $K/\mathbf{Q}$. This contradicts to the assumption (2). Therefore $x^2 - p_1y^2 = p_2^{a_1+a_2}b^2$. Let us define $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ by $\sigma : (\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha}) \mapsto (\sqrt{p_1}, -\sqrt{p_2}, \sqrt{\alpha})$ so that the subgroup generated by σ corresponds to the subfield $k_1(\sqrt{\alpha})$ by Galois theory, and we have $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$. Then we have

$$\sigma(\sqrt{\alpha}\sqrt{\overline{\alpha}}) = -\sqrt{\alpha}\sqrt{\overline{\alpha}} = -\sqrt{p_2^{a_1+a_2}b^2}.$$

On the other hand, we have

$$\begin{aligned} \sigma(\sqrt{\alpha}\sqrt{\overline{\alpha}}) &= \sigma(\sqrt{x^2 - p_1y^2}) = \sigma(\sqrt{p_2^{a_1+a_2}b^2}) \\ &= (-1)^{a_1+a_2}\sqrt{p_2^{a_1+a_2}b^2}. \end{aligned}$$

Hence we have $a_1 + a_2 \equiv 1 \pmod 2$, and $x^2 - p_1y^2 - p_2z^2 = 0, z = p_2^{\frac{a_1+a_2-1}{2}}b$. By Lemma 1.3, we have $d(k_1(\sqrt{\alpha})/k_1) = \mathfrak{p}_1$ or $\mathfrak{p}_2$. Therefore, by Proposition 1.4, $K = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha})$ is a Rédei extension. □

Remark 2.2. (1) The assumption on the ramification indexes of p_1 and p_2 are necessary. For example, let $K = \mathbf{Q}(\sqrt{5}, \sqrt{101}, \sqrt{-35 - 12\sqrt{5}})$. Then, $K/\mathbf{Q}$ is not a Rédei extension, although K is a dihedral extension over $\mathbf{Q}$ of degree 8 where $p_1 = 5$ and $p_2 = 101$ are all ramified prime numbers. In fact, the ramification indexes of 5 and 101 are 4 and 2 respectively.

(2) The ramification of the infinite prime in $K_{\{p_1,p_2\}}/\mathbf{Q}$ is described in terms of the class number h and the narrow class number h^+ of $\mathbf{Q}(\sqrt{p_1p_2})$. In fact, since the cyclic extension $K_{\{p_1,p_2\}}/\mathbf{Q}(\sqrt{p_1p_2})$ is unramified at all finite primes, genus theory tells the 2-part of the narrow ideal class group of $\mathbf{Q}(\sqrt{p_1p_2})$ is a cyclic group of order ≥ 4. Therefore, if $h = h^+$ or $h^+ = 2h$ and $h \equiv 0 \pmod 4$, the infinite prime is unramified in $K_{\{p_1,p_2\}}/\mathbf{Q}$, and if $h^+ = 2h$ and $h \not\equiv 0 \pmod 4$, the infinite prime are ramified in $K_{\{p_1,p_2\}}/\mathbf{Q}$.

3. A proof of the reciprocity law of the triple symbol. In this section, we give another simple proof of the reciprocity law of the Rédei triple symbol. We keep the same notations as in the previous sections.

Let p_1, p_2 and p_3 be distinct prime numbers satisfying the conditions

$$p_i \equiv 1 \pmod 4 \ (i = 1,2,3),$$
$$\left(\frac{p_i}{p_j}\right) = 1 \ (1 \leqq i \neq j \leqq 3).$$

Definition 3.1. We define the *Rédei triple symbol* by

$$[p_1,p_2,p_3] := \begin{cases} 1 & \text{if } p_3 \text{ is completely decomposed} \\ & \text{in } K_{\{p_1,p_2\}}/\mathbf{Q}, \\ -1 & \text{otherwise.} \end{cases}$$

The reciprocity law of the Rédei triple symbol is stated as follows:

Theorem 3.2 ([R]). *For any permutation i,j,k of $1,2,3$, we have*

$$[p_1,p_2,p_3] = [p_i,p_j,p_k].$$

We shall give another proof of the above theorem of Rédei. Firstly, by Theorem 1.6, we have immediately the following:

Theorem 3.3. $[p_1,p_2,p_3] = [p_2,p_1,p_3]$.

Since the permutation group on 1 2 3 is generated by the transpositions $1 \leftrightarrow 2$ and $2 \leftrightarrow 3$, in order to prove Theorem 3.2, it suffices to prove the following:

Theorem 3.4. $[p_1,p_2,p_3] = [p_1,p_3,p_2]$.

In the following we prove Theorem 3.4.

Let us write k for $k_1 = \mathbf{Q}(\sqrt{p_1})$ for simplicity. Let $\mathfrak{p}_2$ (resp. $\mathfrak{p}_3$) be one of the prime ideals of k lying over p_2 (resp. p_3). Then there is a triple of integers (x_2,y_2,z_2) with $\alpha = x_2 + y_2\sqrt{p_1}$ (resp. (x_3,y_3,z_3) with $\beta = x_3 + y_3\sqrt{p_1}$) satisfying the conditions (1), (2) in Lemma 1.1 with respect to the pair (p_1,p_2) (resp. (p_1,p_3)) such that

$$(\alpha) = \mathfrak{p}_2{}^{m_2}, (\beta) = \mathfrak{p}_3{}^{m_3} \ (m_2, m_3 \text{ being odd integers}),$$
$$K_{\{p_1,p_2\}} = \mathbf{Q}(\sqrt{p_1},\sqrt{p_2},\sqrt{\alpha}),$$
$$K_{\{p_1,p_3\}} = \mathbf{Q}(\sqrt{p_1},\sqrt{p_3},\sqrt{\beta}).$$

Since $\mathfrak{p}_3$ is unramified in $k(\sqrt{\alpha})/k$ by Theorem 1.2 (2), we have the Frobenius automorphism $\left(\frac{k(\sqrt{\alpha})/k}{\mathfrak{p}_3}\right) \in \mathrm{Gal}(k(\sqrt{\alpha})/k)$. We note that the Rédei triple symbol is rewritten as

$$[p_1,p_2,p_3] = \begin{cases} 1 & \text{if } \left(\frac{k(\sqrt{\alpha})/k}{\mathfrak{p}_3}\right) = \mathrm{id}_{k(\sqrt{\alpha})}, \\ -1 & \text{otherwise.} \end{cases}$$

For a prime $\mathfrak{p}$ of k, we denote by $\left(\frac{\cdot,\cdot}{\mathfrak{p}}\right)$ the Hilbert symbol in the local field $k_{\mathfrak{p}}$, namely,

$$(a, k_{\mathfrak{p}}(\sqrt{b})/k_{\mathfrak{p}})\sqrt{b} = \left(\frac{a,b}{\mathfrak{p}}\right)\sqrt{b} \quad (a,b \in k_{\mathfrak{p}}^{\times}),$$

where $(\ , k_{\mathfrak{p}}(\sqrt{b})/k_{\mathfrak{p}}) : k_{\mathfrak{p}}^{\times} \to \mathrm{Gal}(k_{\mathfrak{p}}(\sqrt{b})/k_{\mathfrak{p}})$ is the norm residue symbol of local class field theory.

Lemma 3.5. *We have*

$$\left(\frac{\alpha,\beta}{\mathfrak{p}_3}\right) = [p_1,p_2,p_3],$$
$$\left(\frac{\alpha,\beta}{\mathfrak{p}_2}\right) = [p_1,p_3,p_2].$$

Proof. Let π be a prime element of $k_{\mathfrak{p}_3}$ and $U_{\mathfrak{p}_3}$ denote the unit group in $k_{\mathfrak{p}_3}^{\times}$. We write $\beta = u\pi^{m_3}, u \in U_{\mathfrak{p}_3}$. Noting that u, $\alpha \in U_{\mathfrak{p}_3}$ and m_3 is odd, we have

$$\begin{aligned}\left(\frac{\alpha,\beta}{\mathfrak{p}_3}\right) &= \left(\frac{\beta,\alpha}{\mathfrak{p}_3}\right) \\ &= \left(\frac{u,\alpha}{\mathfrak{p}_3}\right)\left(\frac{\pi^{m_3},\alpha}{\mathfrak{p}_3}\right) \\ &= \left(\frac{\pi,\alpha}{\mathfrak{p}_3}\right) \\ &= \frac{(\pi, k_{\mathfrak{p}_3}(\sqrt{\alpha})/k_{\mathfrak{p}_3})\sqrt{\alpha}}{\sqrt{\alpha}} \\ &= \left(\frac{k(\sqrt{\alpha})/k}{\mathfrak{p}_3}\right)(\sqrt{\alpha})/\sqrt{\alpha} \\ &= [p_1,p_2,p_3].\end{aligned}$$

Similarly, we can show $\left(\frac{\alpha,\beta}{\mathfrak{p}_2}\right) = [p_1,p_3,p_2]$. □

Now, the proof of Theorem 3.4 goes as follows: By Lemma 3.5 and the product formula for the Hilbert symbol

$$\prod_{\mathfrak{p}}\left(\frac{\alpha,\beta}{\mathfrak{p}}\right) = 1 \quad (\mathfrak{p} \text{ runs over all primes of } k),$$

we have only to prove

$$\prod_{\mathfrak{p} \neq \mathfrak{p}_2, \mathfrak{p}_3} \left(\frac{\alpha, \beta}{\mathfrak{p}} \right) = 1.$$

If $\mathfrak{p}$ is prime to 2 or ∞, we have

$$\left(\frac{\alpha, \beta}{\mathfrak{p}} \right) = 1,$$

since $\alpha, \beta \in U_{\mathfrak{p}}$. The real prime ∞ is decomposed into real primes ∞_1, ∞_2 in k and so we have obviously

$$\left(\frac{\alpha, \beta}{\infty_1} \right) \left(\frac{\alpha, \beta}{\infty_2} \right) = 1.$$

Let $\mathfrak{P}$ be a prime ideal of k lying over 2. Noting that 2 is unramified in $k/\mathbf{Q}$ and that $\alpha, \beta \in U_{\mathfrak{P}}^{(2)} = 1 + \mathfrak{P}^2$ by the condition (2) of Lemma 1.1, we have find $(\frac{\alpha, \beta}{\mathfrak{P}}) = 1$ ([FV]). This completes the proof of Theorem 3.4.

References

[B] B. J. Birch, Cyclotomic fields and Kummer extensions, in *Algebraic Number Theory* (*Proc. Instructional Conf., Brighton, 1965*), 85–93, Thompson, Washington, DC., 1967.

[FV] I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions*, 2nd ed., Translations of Mathematical Monographs, 121, Amer. Math. Soc., Providence, RI, 2002.

[Mi] M. Morishita, On certain analogies between knots and primes, J. Reine Angew. Math. **550** (2002), 141–167.

[Mt] P. Morton, Density result for the 2-classgroups of imaginary quadratic fields, J. Reine Angew. Math. **332** (1982), 156–187.

[O] T. Ono, *An introduction to algebraic number theory*, translated from the second Japanese edition by the author, The University Series in Mathematics, Plenum, New York, 1990.

[R] L. Rédei, Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper I, J. Reine Angew. Math. **180** (1939), 1–43.