Tohoku Math. J.
66 (2014), 501–522

# ON A CERTAIN NILPOTENT EXTENSION OVER $Q$ OF DEGREE 64 AND THE 4-TH MULTIPLE RESIDUE SYMBOL

FUMIYA AMANO

(Received May 25, 2012, revised October 30, 2013)

**Abstract.** In this paper, we introduce the 4-th multiple residue symbol $[p_1, p_2, p_3, p_4]$ for certain four prime numbers $p_i$'s, which extends the Legendre symbol $\left(\frac{p_1}{p_2}\right)$ and the Rédei triple symbol $[p_1, p_2, p_3]$ in a natural manner. For this we construct concretely a certain nilpotent extension $K$ over $\boldsymbol{Q}$ of degree 64, where ramified prime numbers are $p_1$, $p_2$ and $p_3$, such that the symbol $[p_1, p_2, p_3, p_4]$ describes the decomposition law of $p_4$ in the extension $K/\boldsymbol{Q}$. We then establish the relation of our symbol $[p_1, p_2, p_3, p_4]$ and the 4-th arithmetic Milnor invariant $\mu_2(1234)$ (an arithmetic analogue of the 4-th order linking number) by showing $[p_1, p_2, p_3, p_4] = (-1)^{\mu_2(1234)}$.

**Introduction.** As is well known, for two odd prime numbers $p_1$ and $p_2$, the Legendre symbol $\left(\frac{p_1}{p_2}\right)$ describes the decomposition law of $p_2$ in the quadratic extension $\boldsymbol{Q}(\sqrt{p_1})/\boldsymbol{Q}$. In 1939, L. Rédei ([R]) introduced a triple symbol with the intention of a generalization of the Legendre symbol and Gauss' genus theory. For three prime numbers $p_i \equiv 1 \pmod 4$ $(i = 1, 2, 3)$ with $\left(\frac{p_i}{p_j}\right) = 1$ $(1 \le i \ne j \le 3)$, the Rédei triple symbol $[p_1, p_2, p_3]$ describes the decomposition law of $p_3$ in a Galois extension over $\boldsymbol{Q}$ where all ramified prime numbers are $p_1$ and $p_2$ and the Galois group is the dihedral group $D_8$ of order 8.

Although a meaning of the Rédei symbol had been obscure for a long time, in 2000, M. Morishita ([Mo1, 2, 3]) interpreted the Rédei symbol as an arithmetic analogue of a mod 2 triple linking number, following the analogies between knots and primes. In fact, he introduced arithmetic analogue $\mu_2(12\cdots n) \in \boldsymbol{Z}/2\boldsymbol{Z}$ of Milnor's link invariants (higher order linking numbers) for prime numbers $p_1, \ldots, p_n$ such that

$$\left(\frac{p_1}{p_2}\right) = (-1)^{\mu_2(12)}, \quad [p_1, p_2, p_3] = (-1)^{\mu_2(123)}.$$

Since it is difficult to compute arithmetic Milnor invariants by the definition, it is desirable to construct Galois extensions $K_n/\boldsymbol{Q}$ concretely such that $[p_1, \ldots, p_n] = (-1)^{\mu_2(12\cdots n)}$ describes the decomposition law of $p_n$ in $K_n/\boldsymbol{Q}$, just as in the cases of the Legendre symbol where $K_2$ is a quadratic extension and the Rédei triple symbol where $K_3$ is a dihedral extension of degree 8. As we shall explain in Subsection 2.1, link theory suggests that the desired extension $K_n/\boldsymbol{Q}$ should be a Galois extension such that all ramified prime numbers

2010 *Mathematics Subject Classification.* Primary 11A15; Secondary 11R32, 57M27.
*Key words and phrases.* Rédei triple symbol, Milnor invariant, 4-th multiple residue symbol.

are $p_1, \ldots, p_{n-1}$ and the Galois group is the nilpotent group

$$N_n(\boldsymbol{F}_2) = \left\{ \left( \begin{array}{cccc} 1 & * & \cdots & * \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 1 \end{array} \right) \middle| * \in \boldsymbol{F}_2 \right\}$$

consisting of $n \times n$ unipotent upper-triangular matrices over $\boldsymbol{F}_2$. Note that $N_2(\boldsymbol{F}_2) = \boldsymbol{Z}/2\boldsymbol{Z}$ and $N_3(\boldsymbol{F}_2) = D_8$.

The purpose of this paper is to construct concretely such an extension $K_n/\boldsymbol{Q}$ for $n = 4$ in a natural manner extending Rédei's dihedral extension. We then introduce the 4-th multiple residue symbol $[p_1, p_2, p_3, p_4]$ describing the decomposition law of $p_4$ in $K_4/\boldsymbol{Q}$ and prove that it coincides with the 4-th Milnor invariant $\mu_2(1234)$,

$$[p_1, p_2, p_3, p_4] = (-1)^{\mu_2(1234)}.$$

NOTATION. For a number field $k$, we denote by $\mathcal{O}_k$ the ring of integers of $k$. For a group $G$ and $d \in \boldsymbol{N}$, we denote by $G^{(d)}$ the $d$-th term of the lower central series of $G$ defined by $G^{(1)} := G$, $G^{(d+1)} := [G, G^{(d)}]$. For a ring $R$, $R^\times$ denotes the group of invertible elements of $R$.

**1. Rédei's dihedral extension and triple symbol.** In this section, we recall the construction of Rédei's dihedral extension and triple symbol ([R]), which will be used later. We also give some basic properties of Rédei's dihedral extension and triple symbol.

**1.1. The Rédei extension.** Let $p_1$ and $p_2$ be distinct prime numbers satisfying

$$p_i \equiv 1 \pmod 4 \ (i = 1, 2), \quad \left(\frac{p_1}{p_2}\right) = \left(\frac{p_2}{p_1}\right) = 1. \tag{1.1.1}$$

We set $k_i = \boldsymbol{Q}(\sqrt{p_i})$ $(i = 1, 2)$. It follows from this assumption (1.1.1) that we have the following Lemma.

LEMMA 1.1.2 ([A, Lemma 1.1]). There are integers $x, y, z$ satisfying the following conditions:

(1) $x^2 - p_1 y^2 - p_2 z^2 = 0$.

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

Furthermore, for a given prime ideal $\mathfrak{p}_2$ of $\mathcal{O}_{k_1}$ lying over $p_2$, we can find integers $x, y, z$ which satisfy (1), (2) and $(x + y\sqrt{p_1}) = \mathfrak{p}_2^m$ for an odd positive integer $m$.

Let $\boldsymbol{a} = (x, y, z)$ be a triple of integers satisfying the conditions (1), (2) in Lemma 1.1.2. Then let $\alpha = x + y\sqrt{p_1}$ and set

$$k_{\boldsymbol{a}} = \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha}). \tag{1.1.3}$$

The following theorem was proved by L. Rédei ([R]).

THEOREM 1.1.4 ([R]). (1) *The field $k_{\boldsymbol{a}}$ is a Galois extension over $\boldsymbol{Q}$ whose Galois group is the dihedral group 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* $N_{k_1/\boldsymbol{Q}}(d(k_1(\sqrt{\alpha})/k_1)) = (p_2)$. *In particular, all prime numbers ramified in* $k_{\boldsymbol{a}}/\boldsymbol{Q}$ *are* $p_1$ *and* $p_2$ *with ramification index* 2.

The fact that $k_{\boldsymbol{a}}$ is independent of the choice of $\boldsymbol{a}$ was also shown in [R]. The author gave an alternative proof of this fact in [A], based on a proof communicated by D. Vogel ([V2]).

THEOREM 1.1.5 ([A, Corollary 1.5]). *A field* $k_{\boldsymbol{a}}$ *is independent of the choice of* $\boldsymbol{a} = (x, y, z)$ *satisfying* (1) *and* (2) *in Lemma* 1.1.2, *namely, it depends only on a set* $\{p_1, p_2\}$.

DEFINITION 1.1.6. By Proposition 1.1.5, we denote by $k_{\{p_1,p_2\}}$ the field $k_{\boldsymbol{a}} = \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha})$ given by (1.1.3) and call $k_{\{p_1,p_2\}}$ the *Rédei extension* over $\boldsymbol{Q}$ associated to a set $\{p_1, p_2\}$ satisfying (1.1.1).

The following theorem shows that the Rédei extension $k_{\{p_1,p_2\}}/\boldsymbol{Q}$ is characterized by the information on the Galois group and the ramification given in Theorem 1.1.4.

THEOREM 1.1.7 ([A, Theorem 2.1]). *Let* $p_1$ *and* $p_2$ *be prime numbers satisfying the condition* (1.1.1). *Then the following conditions on a number field* $K$ *are equivalent*:

(1) $K$ *is the Rédei extension* $k_{\{p_1,p_2\}}$.

(2) $K$ *is a Galois extension over* $\boldsymbol{Q}$ *such that the Galois group is the dihedral group* $D_8$ *of order* 8 *and prime numbers ramified in* $K/\boldsymbol{Q}$ *are* $p_1$ *and* $p_2$ *with ramification index* 2.

**1.2. The Rédei triple symbol.** Let $p_1$, $p_2$ and $p_3$ be three prime numbers satisfying

$$p_i \equiv 1 \pmod 4 \ (i = 1, 2, 3)\,, \quad \left(\frac{p_i}{p_j}\right) = 1 \ (1 \le i \ne j \le 3)\,. \tag{1.2.1}$$

Let $k_{\{p_1,p_2\}}$ be the Rédei extension over $\boldsymbol{Q}$ associated to a set $\{p_1, p_2\}$ (Definition 1.1.6).

DEFINITION 1.2.2. We define *Rédei triple symbol* $[p_1, p_2, p_3]$ by

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

The following theorem is a reciprocity law for the Rédei triple symbol:

THEOREM 1.2.3 ([R], [A, Theorem 3.2]). *We have*

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

*for any permutation* $\{i, j, k\}$ *of* $\{1, 2, 3\}$.

**2. Milnor invariants.** In this section, we recall the arithmetic analogues of Milnor invariants of a link introduced by M. Morishita ([Mo1, 2, 3]) and clarify a meaning of the Rédei extension and the Rédei triple symbol in Section 1 from the viewpoint of the analogy between knot theory and number theory. The underlying idea is based on the following analogies between knots and primes (cf. [Mo4]):

| knot<br>$\mathcal{K} : S^1 \hookrightarrow \boldsymbol{R}^3$ | prime<br>$\mathrm{Spec}(\boldsymbol{F}_p) \hookrightarrow \mathrm{Spec}(\boldsymbol{Z})$ |
|---|---|
| link<br>$\mathcal{L} = \mathcal{K}_1 \cup \cdots \cup \mathcal{K}_r$ | finite set of primes<br>$S = \{p_1, \ldots, p_r\}$ |
| $X_{\mathcal{L}} = \boldsymbol{R}^3 \setminus \mathcal{L}$ | $X_S = \mathrm{Spec}(\boldsymbol{Z}) \setminus S$ |
| link group<br>$G_{\mathcal{L}} = \pi_1(X_{\mathcal{L}})$ | Galois group with restricted ramification<br>$G_S = \pi_1^{\text{ét}}(X_S) = \mathrm{Gal}(\boldsymbol{Q}_S/\boldsymbol{Q})$<br>$\boldsymbol{Q}_S$ : maximal extension over $\boldsymbol{Q}$<br>unramified outside $S \cup \{\infty\}$ |

In the following, we firstly explain Milnor invariants of a link and their meaning in nilpotent coverings of $S^3$ ([Mi2], [Mu]). We then discuss their arithmetic analogues for prime numbers where the Rédei triple symbol is interpreted as an arithmetic analogues of a triple Milnor invariant. The analogy also suggests that a natural generalization of the Legendre and Rédei symbols, called a multiple residue symbol $[p_1, \ldots, p_n]$, should describe the decomposition law of $p_n$ in a certain nilpotent extension over $\boldsymbol{Q}$ unramified outside $p_1, \ldots, p_{n-1}$ and $\infty$ ($\infty$ being the infinite prime).

**2.1. Milnor invariants of a link.** Let $\mathcal{L} = \mathcal{K}_1 \cup \cdots \cup \mathcal{K}_r$ be a link with $r$ components in $\boldsymbol{R}^3$ and let $X_{\mathcal{L}} = \boldsymbol{R}^3 \setminus \mathcal{L}$ and $G_{\mathcal{L}} := \pi_1(X_{\mathcal{L}})$ be the link group of $\mathcal{L}$. Let $F$ be the free group on the words $x_1, \ldots, x_r$ where $x_i$ represents a meridian of $\mathcal{K}_i$. The following theorem is due to J. Milnor.

THEOREM 2.1.1 ([Mi2, Theorem 4]). *For each $d \in \boldsymbol{N}$, there is $y_i^{(d)} \in F$ such that*

$$G_{\mathcal{L}}/G_{\mathcal{L}}^{(d)} = \langle x_1, \ldots, x_r \mid [x_1, y_1^{(d)}] = \cdots = [x_r, y_r^{(d)}] = 1,\ F^{(d)} = 1 \rangle\,,$$
$$y_j^{(d)} \equiv y_j^{(d+1)} \mod F^{(d)}\,,$$

*where $y_j^{(d)}$ is a word representing a longitude of $\mathcal{K}_j$ in $G_{\mathcal{L}}/G_{\mathcal{L}}^{(d)}$.*

Let $\boldsymbol{Z}\langle\langle X_1, \ldots, X_r \rangle\rangle$ be the algebra of non-commutative formal power series of variables $X_1, \ldots, X_r$ over $\boldsymbol{Z}$, and let

$$M : F \longrightarrow \boldsymbol{Z}\langle\langle X_1, \ldots, X_r \rangle\rangle^{\times}$$

be the Magnus homomorphism defined by

$$M(x_i) := 1 + X_i,\ M(x_i^{-1}) := 1 - X_i + X_i^2 - \cdots,\ 1 \le i \le r\,.$$

For $f \in F$, $M(f)$ has the form

$$M(f) = 1 + \sum_{n=1}^{\infty} \sum_{1 \le i_1, \ldots, i_n \le r} \mu(i_1 \cdots i_n;\, f) X_{i_1} \cdots X_{i_n}\,,$$

where the coefficients $\mu(i_1 \cdots i_n;\, f)$ are called the *Magnus coefficients*.

Let $\boldsymbol{Z}[F]$ be the group algebra of $F$ over $\boldsymbol{Z}$ and let $\varepsilon_{\boldsymbol{Z}[F]} : \boldsymbol{Z}[F] \to \boldsymbol{Z}$ be the augmentation map. We note that the Magnus coefficients can be written in terms of the Fox derivative

introduced in [F]:

$$\mu(i_1 \cdots i_n;\, f) = \varepsilon_{\mathbf{Z}[F]}\left(\frac{\partial^n f}{\partial x_{i_1} \cdots \partial x_{i_n}}\right).$$

For the word $y_j^{(d)}$ in Theorem 2.1.1, we set

$$\mu^{(d)}(i_1 \cdots i_n j) := \mu(i_1 \cdots i_n;\, y_j^{(d)}).$$

Since $\mu(i_1 \cdots i_n;\, f) = 0$ for $f \in F^{(d)}$ if $d > n$, by Theorem 2.1.1, $\mu^{(d)}(I)$ is independent of $d$ if $d \geq |I|$, where $|I|$ denotes the length of a multi-index $I$. Define $\mu(I) := \mu^{(d)}(I)$ $(d \gg 1)$. For a multi-index $I$ with $|I| \geq 2$, we define $\Delta(I)$ to be the ideal of $\boldsymbol{Z}$ generated by $\mu(J)$ where $J$ runs over cyclic permutations of proper subsequences of $I$. If $|I| = 1$, we set $\mu(I) := 0$ and $\Delta(I) := 0$ . The *Milnor $\overline{\mu}$-invariant* is then defined by

$$\overline{\mu}(I) := \mu(I) \mod \Delta(I).$$

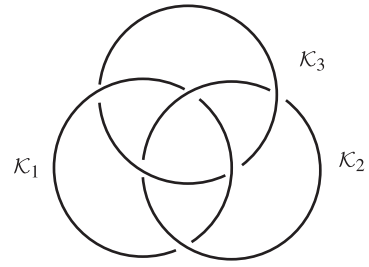
The fundamental results, due to Milnor, are as follows.

THEOREM 2.1.2 ([Mi2, Theorems 5, 6]). (1) $\overline{\mu}(ij) = \mathrm{lk}(\mathcal{K}_i, \mathcal{K}_j)$ $(i \neq j)$.
(2) *If* $2 \leq |I| \leq d$, $\overline{\mu}(I)$ *is a link invariant of* $\mathcal{L}$.
(3) (Shuffle relation) *For any* $I, J$ $(|I|, |J| \geq 1)$ *and* $i$ $(1 \leq i \leq r)$, *we have*

$$\sum_{H \in \mathrm{PSh}(I,J)} \overline{\mu}(Hi) \equiv 0 \mod \text{g.c.d}\{\Delta(Hi) \mid H \in \mathrm{PSh}(I, J)\}$$

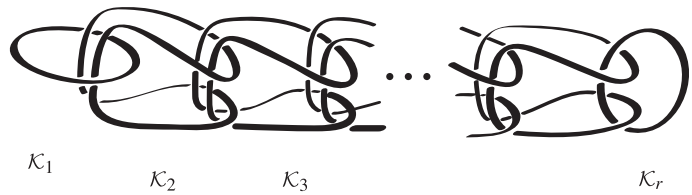
*where* $\mathrm{PSh}(I, J)$ *stands for the set of results of proper shuffles of* $I$ *and* $J$ (cf. [CFL]).
(4) (Cyclic symmetry). $\overline{\mu}(i_1 \cdots i_n) = \overline{\mu}(i_2 \cdots i_n i_1) = \cdots = \overline{\mu}(i_n i_1 \cdots i_{n-1})$.

EXAMPLE 2.1.3. For a multi-index $I$ $(|I| \geq 2)$, $\overline{\mu}(I) = \mu(I)$ is an integral link invariant if $\mu(J) = 0$ for all multi-index $J$ with $|J| < |I|$. For example, let $\mathcal{L} = \mathcal{K}_1 \cup \mathcal{K}_2 \cup \mathcal{K}_3$ be the following *Borromean rings*:




Then $\mu(I) = 0$ if $|I| \leq 2$ and hence $\mu(I) \in \boldsymbol{Z}$ for $|I| = 3$. In fact, we have $\mu(ijk) = \pm 1$ if $ijk$ is a permutation of 123 and $\mu(ijk) = 0$ otherwise.

Move generally, let $\mathcal{L} = \mathcal{K}_1 \cup \cdots \cup \mathcal{K}_r$ be the following link, called the *Milnor link* ([Mi1, 5]). We easily see that the link obtained by removing any one component $\mathcal{K}_i$ from $\mathcal{L}$ is trivial. So $\mu(I) = 0$ if $|I| \leq n - 1$ and $\mu(I) \in \boldsymbol{Z}$ if $|I| = n$. For instance, $\mu(12 \cdots n) = 1$.




Next, we recall that Milnor invariants may be regarded as invariants associated to nilpotent coverings of $S^3$. For a commutative ring $R$, let $N_n(R)$ be the group consisting of $n$ by $n$ unipotent uppertriangular matrices. For a multi-index $I = (i_1 \cdots i_n)(n \geq 2)$, we define the map $\rho_I : F \to N_n(\boldsymbol{Z}/\Delta(I))$ by

$$\rho_I(f) := \begin{pmatrix} 1 & \varepsilon\left(\frac{\partial f}{\partial x_{i_1}}\right) & \varepsilon\left(\frac{\partial^2 f}{\partial x_{i_1}\partial x_{i_2}}\right) & \cdots & \varepsilon\left(\frac{\partial^{n-1} f}{\partial x_{i_1}\cdots\partial x_{i_{n-1}}}\right) \\ 0 & 1 & \varepsilon\left(\frac{\partial f}{\partial x_{i_2}}\right) & \cdots & \varepsilon\left(\frac{\partial^{n-2} f}{\partial x_{i_2}\cdots\partial x_{i_{n-1}}}\right) \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & \varepsilon\left(\frac{\partial f}{\partial x_{i_{n-1}}}\right) \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \mod \Delta(I),$$

where we set $\varepsilon = \varepsilon_{\boldsymbol{Z}[F]}$ for simplicity. It can be shown by the property of the Fox derivative that $\rho_I$ is a homomorphism.

THEOREM 2.1.6 ([Mo4, Theorem 8.8], [Mu]). (1) *The homomorphism $\rho_I$ factors through the link group $G_{\mathcal{L}}$. Furthermore it is surjective if $i_1, \ldots, i_{n-1}$ are all distinct.*

(2) *Suppose that $i_1, \ldots, i_{n-1}$ are all distinct. Let $X_I \to X_{\mathcal{L}}$ be the Galois covering corresponding to* $\mathrm{Ker}(\rho_I)$ *whose Galois group* $\mathrm{Gal}(X_I/X_{\mathcal{L}}) = N_n(\boldsymbol{Z}/\Delta(I))$. *When $\Delta(I) \neq 0$, let $M_I \to S^3$ be the Fox completion of $X_I \to X_{\mathcal{L}}$, a Galois covering ramified over the link $\mathcal{K}_{i_1} \cup \cdots \cup \mathcal{K}_{i_{n-1}}$. For a longitude $\beta_{i_n}$ of $\mathcal{K}_{i_n}$, one has*

$$\rho_I(\beta_{i_n}) = \begin{pmatrix} 1 & 0 & \cdots & 0 & \overline{\mu}(I) \\ 0 & 1 & \cdots & & 0 \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

*and hence the following holds*:

$$\overline{\mu}(I) = 0 \Longleftrightarrow \mathcal{K}_{i_n} \textit{is completely decomposed in } M_I \to S^3.$$

**2.2. Milnor invariants for prime numbers.** Let $S = \{p_1, \ldots, p_r\}$ be a set of $r$ distinct odd prime numbers and let $G_S := \pi_1^{\text{ét}}(\mathrm{Spec}(\boldsymbol{Z}) \setminus S)$. In order to get the analogy of the link case, we consider the maximal pro-2 quotient, denoted by $G_S(2)$, of $G_S$ which is the Galois group of the maximal pro-2 extension $\boldsymbol{Q}_S(2)$ over $\boldsymbol{Q}$ which is unramified outside

$S \cup \{\infty\}$. Here we fix an algebraic closure $\overline{\boldsymbol{Q}}$ of $\boldsymbol{Q}$ containing $\boldsymbol{Q}_S(2)$. We also fix an algebraic closure $\overline{\boldsymbol{Q}}_{p_i}$ of $\boldsymbol{Q}_{p_i}$ and an embedding $\overline{\boldsymbol{Q}} \hookrightarrow \overline{\boldsymbol{Q}}_{p_i}$ for each $i$. Let $\boldsymbol{Q}_{p_i}(2)$ be the maximal pro-2 extension of $\boldsymbol{Q}_{p_i}$ contained in $\overline{\boldsymbol{Q}}_{p_i}$. Then we have

$$\boldsymbol{Q}_{p_i}(2) = \boldsymbol{Q}_{p_i}(\zeta_{2^n},\ \sqrt[2^n]{p_i} \mid n \geq 1)$$

where $\zeta_{2^n} \in \overline{\boldsymbol{Q}}$ is primitive $2^n$-th root of unity such that $\zeta_{2^t}^{2^s} = \zeta_{2^{t-s}}$ $(t \geq s)$. The local Galois group $\mathrm{Gal}(\boldsymbol{Q}_{p_i}(2)/\boldsymbol{Q}_{p_i})$ is then topologically generated by the monodromy $\tau_i$ and the extension of the Frobenius automorphism $\sigma_i$ defined by

$$\begin{aligned} &\tau_i(\zeta_{2^n}) = \zeta_{2^n}\,, \quad \tau_i(\sqrt[2^n]{p_i}) = \zeta_{2^n}\sqrt[2^n]{p_i}\,, \\ &\sigma_i(\zeta_{2^n}) = \zeta_{2^n}^{p_1}\,, \quad \sigma_i(\sqrt[2^n]{p_i}) = \sqrt[2^n]{p_i} \end{aligned} \tag{2.2.1}$$

and $\tau_i, \sigma_i$ are subject to the relation $\tau_i^{p_i-1}[\tau_i, \sigma_i] = 1$.

The embedding $\overline{\boldsymbol{Q}} \hookrightarrow \overline{\boldsymbol{Q}}_{p_i}$ induces the embedding $\boldsymbol{Q}_S(2) \hookrightarrow \boldsymbol{Q}_{p_i}(2)$ and hence the homomorphism $\eta_i : \mathrm{Gal}(\boldsymbol{Q}_{p_i}(2)/\boldsymbol{Q}_{p_i}) \to G_S$. We denote by the same $\tau_i, \sigma_i$ the images of $\tau_i, \sigma_i$ under $\eta_i$. Let $\hat{F}$ denote the free pro-2 group on the words $x_1, \ldots, x_r$ where $x_i$ represents $\tau_i$. The following theorem, due to H. Koch, may be regarded as an arithmetic analogue of Milnor's Theorem 2.1.1.

THEOREM 2.2.2 ([K2, Theorem 6.2]). *The pro-2 group $G_S(2)$ has the following presentation*:

$$G_S(2) = \langle x_1, \ldots, x_r \mid x_1^{p_1-1}[x_1, y_1] = \cdots = x_r^{p_r-1}[x_r, y_r] = 1 \rangle\,,$$

*where $y_j \in \hat{F}$ is the pro-2 word which represents $\sigma_j$.*

Set $e_S := \max\{e \mid p_i \equiv 1 \mod 2^e\ (1 \leq i \leq r)\}$ and fix $m = 2^e$ $(1 \leq e \leq e_S)$. Let $\boldsymbol{Z}_2\langle\langle X_1, \ldots, X_r \rangle\rangle$ be the algebra of non-commutative formal power series of variables $X_1, \ldots, X_r$ over $\boldsymbol{Z}_2$, the ring of 2-adic integers, and let

$$\hat{M} : \hat{F} \longrightarrow \boldsymbol{Z}_2\langle\langle X_1, \ldots, X_r \rangle\rangle^\times$$

be the pro-2 Magnus embedding ([K1, 4.2]). For $f \in \hat{F}$, $\hat{M}(f)$ has the from

$$\hat{M}(f) = 1 + \sum_{1 \leq i_1, \ldots, i_n \leq r} \hat{\mu}(i_1 \cdots i_n;\, f) X_{i_1} \cdots X_{i_n}\,,$$

where the coefficients $\hat{\mu}(i_1 \cdots i_n;\, f)$ are called the 2-*adic Magnus coefficients*. We let

$$M_2 : \hat{F} \longrightarrow \boldsymbol{F}_2\langle\langle X_1, \ldots, X_r \rangle\rangle^\times$$

be the mod 2 Magnus embedding defined by composing $\hat{M}$ with the natural homomorphism $\boldsymbol{Z}_2\langle\langle X_1, \ldots, X_r \rangle\rangle^\times \longrightarrow \boldsymbol{F}_2\langle\langle X_1, \ldots, X_r \rangle\rangle^\times$.

Let $\boldsymbol{Z}_2[[\hat{F}]]$ be the complete group algebra over $\boldsymbol{Z}_2$ and let $\varepsilon_{\boldsymbol{Z}_2[[\hat{F}]]} : \boldsymbol{Z}_2[[\hat{F}]] \to \boldsymbol{Z}_2$ be the augmentation map. In terms of the pro-2 Fox free derivative ([I], [O]), the 2-adic Magnus coefficients are written as

$$\hat{\mu}(i_1 \cdots i_n;\, f) = \varepsilon_{\boldsymbol{Z}_2[[\hat{F}]]}\left(\frac{\partial^n f}{\partial x_{i_1} \cdots \partial x_{i_n}}\right).$$

For the word $y_j$ in Theorem 2.2.2, we set

$$\hat{\mu}(i_1 \cdots i_n j) := \hat{\mu}(i_1 \cdots i_n; y_j)$$

and we set, for a multi-index $I$,

$$\mu_m(I) := \hat{\mu}(I) \mod m\,.$$

For a multi-index with $I$ with $1 \leq |I| \leq 2^{e_S}$, let $\Delta_m(I)$ be the ideal of $\boldsymbol{Z}/m\boldsymbol{Z}$ generated by $\binom{2^{e_S}}{t}$ $(1 \leq t \leq |I|)$ and $\mu_m(J)$ ($J$ running over cyclic permutation of proper subsequences of $I$). The Milnor $\overline{\mu}_m$-invariant is then defined by

$$\overline{\mu}_m(I) := \mu_m(I) \mod \Delta_m(I)\,.$$

The following analogue of Theorem 2.1.2 is due to Morishita.

THEOREM 2.2.3 ([Mo3, Theorems 1.2.1, 1.2.5]). (1) *$\zeta_m^{\mu_m(ij)} = \left(\frac{p_j}{p_i}\right)_m$ where $\zeta_m$ is the primitive $m$-th root of unity given in* (2.2.1) *and $\left(\frac{p_j}{p_i}\right)_m$ is the $m$-th power residue symbol in $\boldsymbol{Q}_{p_i}$.*

(2) *If $2 \leq |I| \leq 2^{e_S}$, $\overline{\mu}_m(I)$ is an invariant depending only on $S$.*

(3) *Let $r$ be an integer such that $2 \leq r \leq 2^{e_S}$. For multi-indices $I$, $J$ such that $|I|+|J| = r-1$, we have, for any $1 \leq i \leq n$,*

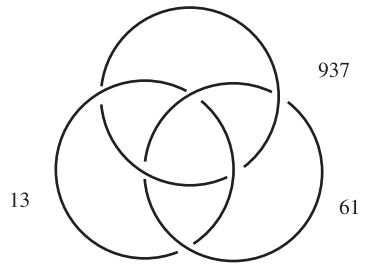
$$\sum_{H \in \mathrm{PSh}(I,J)} \overline{\mu}_m(Hi) \equiv 0 \mod \text{g.c.d}\{\Delta(Hi) \mid H \in \mathrm{PSh}(I,J)\}\,.$$

EXAMPLE 2.2.4. Let $S = \{p_1, p_2, p_3\}$ be a triple of distinct prime numbers satisfying the condition (1.2.1) and let $m = 2$. Then $\mu_2(I) = 0$ if $|I| \leq 2$ and hence, for $|I| = 3$, $\Delta_2(I) = 0$ and $\overline{\mu}_2(I) = \mu_2(I) \in \boldsymbol{Z}/2\boldsymbol{Z}$. The following theorem interprets the Rédei triple symbol as a Milnor invariant.

THEOREM 2.2.4.1 ([Mo2, Theorem 3.2.5]). *Under the above assumption on $\{p_1, p_2, p_3\}$ we have*

$$[p_1, p_2, p_3] = (-1)^{\mu_2(123)}\,.$$

For example, D. Vogel ([V1, Example 3.14]) showed that for $S = \{13, 61, 937\}$ $\mu_2(I) = 0$ ($|I| \leq 2$), $\mu_2(I) = 1$ ($I$ is a permutation of 123), $\mu_2(ijk) = 0$ (otherwise). In view of Example 2.1.3, this triple of prime numbers may be called the *Borromean primes*.



Finally, we give an analogue of Theorem 2.1.6 for prime numbers. Let $I = (i_1 \cdots i_n)$, $2 \leq n \leq l^{e_S}$ and assume $\Delta_m(I) \neq \boldsymbol{Z}/m\boldsymbol{Z}$. We define the map $\rho_{(m,I)} : \hat{F} \to N_n((\boldsymbol{Z}/m\boldsymbol{Z})/\Delta_m(I))$ by

$$\rho_{(m,I)}(f) := \begin{pmatrix} 1 & \varepsilon\left(\frac{\partial f}{\partial x_{i_1}}\right)_m & \varepsilon\left(\frac{\partial^2 f}{\partial x_{i_1}\partial x_{i_2}}\right)_m & \cdots & \varepsilon\left(\frac{\partial^{n-1} f}{\partial x_{i_1}\cdots\partial x_{i_{n-1}}}\right)_m \\ & 1 & \varepsilon\left(\frac{\partial f}{\partial x_{i_2}}\right)_m & \cdots & \varepsilon\left(\frac{\partial^{n-2} f}{\partial x_{i_2}\cdots\partial x_{i_{n-1}}}\right)_m \\ & & \ddots & \ddots & \vdots \\ & 0 & & 1 & \varepsilon\left(\frac{\partial f}{\partial x_{i_{n-1}}}\right)_m \\ & & & & 1 \end{pmatrix} \mod \Delta_m(I),$$

where we set $\varepsilon(\alpha)_m = \varepsilon_{\boldsymbol{Z}[[\hat{F}]]}(\alpha) \bmod m$ for $\alpha \in \boldsymbol{Z}_l[[\hat{F}(l)]]$. It can be shown by the property of the pro-2 Fox derivative that $\rho_{(m,I)}$ is a homomorphism.

THEOREM 2.2.5 ([Mo3, Theorem 1.2.7]). (1) *The homomorphism $\rho_{(m,I)}$ factors through the Galois group $G_S(2)$. Further it is surjective if $i_1, \ldots, i_{n-1}$ are all distinct.*

(2) *Suppose that $i_1, \ldots, i_{n-1}$ are all distinct. Let $K_{(m,I)}$ be the extension over $\boldsymbol{Q}$ corresponding to* $\mathrm{Ker}(\rho_{(m,I)})$. *Then $K_{(m,I)}/\boldsymbol{Q}$ is a Galois extension unramified outside $p_{i_1}, \ldots, p_{i_{n-1}}$ and $\infty$ with Galois group* $\mathrm{Gal}(K_{(m,I)}/\boldsymbol{Q}) = N_n((\boldsymbol{Z}/m\boldsymbol{Z})/\Delta_m(I))$. *For a Frobenius automorphism $\sigma_{i_n}$ over $p_{i_n}$, one has*

$$\rho_{(m,I)}(\sigma_{i_n}) = \begin{pmatrix} 1 & 0 & \cdots & 0 & \overline{\mu}_m(I) \\ & 1 & \cdots & & 0 \\ & & \ddots & & \vdots \\ & 0 & & 1 & 0 \\ & & & & 1 \end{pmatrix}$$

*and hence the following holds*:

$$\overline{\mu}_m(I) = 0 \Longleftrightarrow p_{i_n} \textit{is completely decomposed in } K_{(m,I)}/\boldsymbol{Q}.$$

EXAMPLE 2.2.6. Let $m = 2$ and $K = K_{(2,I)}$. For $S = \{p_1, p_2\}$, $p_i \equiv 1 \pmod 4$ $(i = 1, 2)$ and $I = (12)$, we have

$$K = \boldsymbol{Q}(\sqrt{p_1}),\ \mathrm{Gal}(K/\boldsymbol{Q}) = N_2(\boldsymbol{F}_2) = \boldsymbol{Z}/2\boldsymbol{Z},\ (-1)^{\mu_2(12)} = \left(\frac{p_1}{p_2}\right).$$

For $S = \{p_1, p_2, p_3\}$ satisfying the condition (1.2.1) and $I = (123)$, we have

$$K = k_{\{p_1,p_2\}},\ \mathrm{Gal}(K/\boldsymbol{Q}) = N_3(\boldsymbol{F}_2) = D_8,\ (-1)^{\mu_2(123)} = [p_1, p_2, p_3].$$

Theorem 2.2.5 suggests a problem to construct concretely a Galois extension $K_n/\boldsymbol{Q}$ unramified outside $p_1, \ldots, p_{n-1}$ and $\infty$ with Galois group $N_n(\boldsymbol{F}_2)$ and to introduce the multiple residue symbol $[p_1, \ldots, p_n]$, as a generalization of the Legendre symbol and the Rédei triple symbol, which should describe the decomposition law of $p_n$ in the extension $K_n/\boldsymbol{Q}$ and coincide with $(-1)^{\mu_2(12\cdots n)}$. In the next section, we solve this problem for the case $n = 4$.

**3. Construction of an $N_4(\boldsymbol{F}_2)$-extension and the 4-th multiple residue symbol.** In this section, under certain conditions on three prime numbers $p_1, p_2, p_3$, we construct concretely a Galois extension $K$ over $\boldsymbol{Q}$ where all ramified prime numbers are $p_1, p_2$ and $p_3$ and the Galois group is $N_4(\boldsymbol{F}_2)$, and introduce the 4-th multiple residue symbol $[p_1, p_2, p_3, p_4]$ which describes the decomposition law of $p_4$ in $K/\boldsymbol{Q}$. We then show that $[p_1, p_2, p_3, p_4]$ coincides with $(-1)^{\mu_2(1234)}$, where $\mu_2(1234)$ is the 4-th arithmetic Milnor invariant defined in 2.2. We keep the same notations as in the previous sections.

**3.1. Construction of an $N_4(\boldsymbol{F}_2)$-extension.** Let $p_1, p_2$ and $p_3$ be three prime numbers satisfying the conditions

$$\text{(3.1.1)} \qquad \begin{cases} p_i \equiv 1 \pmod 4 \ (i = 1, 2, 3)\,, \quad \left(\dfrac{p_i}{p_j}\right) = 1 \ (1 \le i \ne j \le 3)\,, \\ [p_i, p_j, p_k] = 1 \ (\{i, j, k\} = \{1, 2, 3\})\,. \end{cases}$$

We let

$$\begin{cases} k_i := \boldsymbol{Q}(\sqrt{p_i}) \ (i = 1, 2, 3),\ k_{ij} := k_i k_j = \boldsymbol{Q}(\sqrt{p_i}, \sqrt{p_j}) \ (1 \le i < j \le 3)\,, \\ k_{123} := k_1 k_2 k_3 = \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})\,. \end{cases}$$

For simplicity, we set $k := k_1$ in the following. Let $\mathfrak{p}_2$ be one of prime ideals of $\mathcal{O}_k$ lying over $p_2$. Then as in Lemma 1.1.2, we can find a triple of integers $(x, y, z)$ with $\alpha = x + y\sqrt{p_1}$ satisfying (1), (2) in Lemma 1.1.2 such that

$$(\alpha) = \mathfrak{p}_2^m \ (m \text{ being an odd integer})\,, \quad k_{\{p_1,p_2\}} = \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha})\,.$$

In the following, we fix such an $\alpha$ once and for all.

For a prime $\mathfrak{p}$ of $k$, we denote by $\left(\frac{\cdot}{\mathfrak{p}}\right)$ 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 3.1.2. *For any prime $\mathfrak{p}$ of $k$, we have*

$$\left(\frac{\alpha, p_3}{\mathfrak{p}}\right) = 1\,.$$

PROOF. We consider the following five cases.

(Case 1) $\mathfrak{p}$ is prime to $\mathfrak{p}_2$, $p_3$, 2, $\infty$: Then we have $\alpha, p_3 \in U_\mathfrak{p}$, where $U_\mathfrak{p}$ is the unit group of $k_\mathfrak{p}$, and hence $\left(\frac{\alpha, p_3}{\mathfrak{p}}\right) = 1$.

(Case 2) $\mathfrak{p} = \mathfrak{p}_2$: Let $\pi$ be a prime element of $k_{\mathfrak{p}_2}$. Write $\alpha = u_1\pi^{m_2}$, $u_1 \in U_{\mathfrak{p}_2}$. Then we have

$$\begin{aligned} \left(\frac{\alpha, p_3}{\mathfrak{p}_2}\right) &= \left(\frac{u_1, p_3}{\mathfrak{p}_2}\right)\left(\frac{\pi^{m_2}, p_3}{\mathfrak{p}_2}\right) \\ &= \left(\frac{\pi, p_3}{\mathfrak{p}_2}\right) \quad (u_1, p_3 \in U_{\mathfrak{p}_2}, m_2 \text{ is odd}) \end{aligned}$$

$$= \frac{(\pi, k_{\mathfrak{p}_2}(\sqrt{p_3})/k_{\mathfrak{p}_2})\sqrt{p_3}}{\sqrt{p_3}}.$$

Since $(\pi, k_{\mathfrak{p}_2}(\sqrt{p_3})/k_{\mathfrak{p}_2})$ is the Frobenius automorphism over $p_2$ in $k(\sqrt{p_3})/k$, $(\pi, k_{\mathfrak{p}_2}(\sqrt{p_3})/k_{\mathfrak{p}_2})(\sqrt{p_3}) = \sqrt{p_3}$ by $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_3}{p_2}\right) = 1$.

(Case 3) $\mathfrak{p} \mid p_3$: Let $\varpi$ be a prime element of $k_{\mathfrak{p}}$. Write $p_3 = u_2\varpi$, $u_2 \in U_{\mathfrak{p}}$. Then we have

$$\begin{aligned}\left(\frac{\alpha, p_3}{\mathfrak{p}}\right) &= \left(\frac{p_3, \alpha}{\mathfrak{p}}\right)\\ &= \left(\frac{u_2, \alpha}{\mathfrak{p}}\right)\left(\frac{\varpi, \alpha}{\mathfrak{p}}\right)\\ &= \left(\frac{\varpi, \alpha}{\mathfrak{p}}\right) \quad (u_2, \alpha \in U_{\mathfrak{p}})\\ &= \frac{(\varpi, k_{\mathfrak{p}}(\sqrt{\alpha})/k_{\mathfrak{p}})\sqrt{\alpha}}{\sqrt{\alpha}}.\end{aligned}$$

Since $\mathfrak{p}$ is decomposed in $k(\sqrt{\alpha})/k$ by $[p_1, p_2, p_3] = 1$ and $(\varpi, k_{\mathfrak{p}}(\sqrt{\alpha})/k_{\mathfrak{p}})$ is the Frobenius automorphism over $\mathfrak{p}$ in $k(\sqrt{\alpha})/k$, $(\varpi, k_{\mathfrak{p}}(\sqrt{\alpha})/k_{\mathfrak{p}})(\sqrt{\alpha}) = \sqrt{\alpha}$.

(Case 4) $\mathfrak{p} = \infty$: Since $p_3 > 0$, $\left(\frac{\alpha, p_3}{\infty}\right) = 1$.

(Case 5) $\mathfrak{p} \mid 2$: If $\mathfrak{p} = (2)$, the above cases and the product formula for the Hilbert symbol yields $\left(\frac{\alpha, p_3}{\mathfrak{p}}\right) = 1$. If $(2) = \mathfrak{p} \cdot \mathfrak{p}'$ $(\mathfrak{p} \neq \mathfrak{p}')$, $k_{\mathfrak{p}} = k_{\mathfrak{p}'} = \boldsymbol{Q}_2$ and so we have

$$\left(\frac{\alpha, p_3}{\mathfrak{p}}\right) = \left(\frac{\alpha, p_3}{\mathfrak{p}'}\right) = (-1)^{\frac{p_3-1}{2}\cdot\frac{\alpha-1}{2}} = 1. \qquad \square$$

PROPOSITION 3.1.3. *Assume that the class number of $k$ is* 1. *Then there are $X, Y, Z \in \mathcal{O}_k$ satisfying the following conditions*:

(1) $X^2 - p_3Y^2 - \alpha Z^2 = 0$,

(2) g.c.d$(X, Y, Z) = 1$.

PROOF. By Lemma 3.1.2, we have $\alpha \in N_{k_{\mathfrak{p}}(\sqrt{p_3})/k_{\mathfrak{p}}}(k_{\mathfrak{p}}(\sqrt{p_3})^{\times})$ for any prime $\mathfrak{p}$ of $k$ and so there are $X_{\mathfrak{p}}, Y_{\mathfrak{p}} \in k_{\mathfrak{p}}$ such that $X_{\mathfrak{p}}^2 - p_3Y_{\mathfrak{p}}^2 = \alpha$. By the Hasse principal, there are $\tilde{X}, \tilde{Y} \in k$ such that $\tilde{X}^2 - p_3\tilde{Y}^2 = \alpha$ from which the condition (1) holds by writing $\tilde{X} = \frac{X}{Z}$, $\tilde{Y} = \frac{Y}{Z}$ with $X, Y, Z \in \mathcal{O}_k$. Since $\mathcal{O}_k$ is the principal ideal domain by the assumption, we may choose $X, Y, Z \in \mathcal{O}_k$ so that the condition (2) is satisfied. $\square$

For $k_{13} = \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_3})$, let $U$ be the unit group of $\mathcal{O}_{k_{13}}/(4)$ and $U(2)$ the 2-Sylow subgroup of $U$. Similarly, let $k'_{13} := \boldsymbol{Q}(\sqrt{p_1}, \sqrt{\alpha})$ and define $U' := (\mathcal{O}_{k'_{13}}/(4))^{\times}$ and $U'(2)$ to be the 2-Sylow subgroup of $U'$.

LEMMA 3.1.4. *The group $U(2)$ is given by*

$$U(2) = \langle -1 \rangle \times \langle \sqrt{p_1} \rangle \times \langle \sqrt{p_3} \rangle \times \left\langle \frac{3 + \sqrt{p_1} + \sqrt{p_3} + \sqrt{p_1p_3}}{2} \right\rangle$$

$$\simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}\,.$$

*Similarly, $U'(2)$ is given by*

$$U'(2) = \langle -1\rangle \times \langle \sqrt{p_1}\rangle \times \langle \sqrt{\alpha}\rangle \times \left\langle \frac{3+\sqrt{p_1}+\sqrt{\alpha}+\sqrt{p_1\alpha}}{2} \right\rangle$$
$$\simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}\,.$$

PROOF. Since 2 is unramified in the extension $k_{13}/\boldsymbol{Q}$, we have the decomposition $(2) = \mathfrak{c}_1 \cdots \mathfrak{c}_r$. Therefore the order of $U$ is given by

$$\Pi_{i=1}^{r} N\mathfrak{c}_i(N\mathfrak{c}_i - 1) = N((2))\Pi_{i=1}^{r}(N\mathfrak{c}_i - 1) = 16m$$

and so $U$ has the order $16m$, where $m$ is an odd integer. Let $A := \{\pm 1 \mod (4), \pm\sqrt{p_1} \mod (4), \pm\sqrt{p_3} \mod (4), \pm\sqrt{p_1p_3} \mod (4)\}$. Since $p_i \equiv 1 \mod 4$, each element of $A$ has the order 2 and so $A \subset U(2)$. We show that the order of $A$ is 8. Suppose $\sqrt{p_1} \equiv \sqrt{p_3} \mod (4)$ for example. Then $\sqrt{p_1} - \sqrt{p_3} = 4\beta$ for some $\beta \in \mathcal{O}_{k_{13}}$. Taking the norm $N_{k_{13}/\boldsymbol{Q}}$, we obtain

$$\frac{-p_1-p_3}{16} + \frac{\sqrt{p_1p_3}}{8} \in \mathcal{O}_{\boldsymbol{Q}(\sqrt{p_1p_3})} = \left\{ \frac{a+b\sqrt{p_1p_3}}{2} \,\middle|\, a, b \in \mathbf{Z}, a \equiv b \mod 2 \right\},$$

which is a contradiction. Similary, using the structure of $\mathcal{O}_{k_1}$ and $\mathcal{O}_{k_3}$, we can check that any two elements in $A$ are distinct. Hence we see that $U(2) = A \cup A\cdot\{(3+\sqrt{p_1}+\sqrt{p_3}+\sqrt{p_1p_3})/2 \mod (4)\}$. Replacing $p_3$ by $\alpha$, the assertion for $U'(2)$ can be shown similarly. □

LEMMA 3.1.5. *Assume $p_1 \equiv 5 \pmod 8$. Then there is a unit $\varepsilon \in \mathcal{O}_k^{\times}$ of the form $\varepsilon = s + t\sqrt{p_1}, s, t \in \mathbf{Z}, s \equiv 0, t \equiv 1 \pmod 2$. Such a unit $\varepsilon$ satisfies $\varepsilon \equiv \pm\sqrt{p_1} \mod (4)$ in $U(2)$ and $U'(2)$.*

PROOF. Since $p_1 \equiv 1 \pmod 4$, the fundamental unit $\varepsilon_1 = \frac{s_1+t_1\sqrt{p_1}}{2}$ ($s_1 \equiv t_1 \pmod 2$) of $k$ satisfies $N_{k/\boldsymbol{Q}}(\varepsilon_1) = -1$. If $s_1 \equiv t_1 \equiv 0 \pmod 2$, we let $\varepsilon := \varepsilon_1 = s + t\sqrt{p_1}$, $s := s_1/2, t := t_1/2 \in \mathbf{Z}$, where we have $s \equiv 0, t \equiv 1 \pmod 2$, since $s^2 - p_1t^2 = -1$. Since $\varepsilon = s + t\sqrt{p_1} = s + s\sqrt{p_1} + (t-s)\sqrt{p_1}$ and $s + s\sqrt{p_1} \in 4\mathcal{O}_{k_{13}}$, $\varepsilon \equiv \pm\sqrt{p_1} \mod (4)$. Suppose $s_1 \equiv t_1 \equiv 1 \pmod 2$. Since $p_1 \equiv 5 \pmod 8$, we have $s_1^2 + 3p_1t_1^2 \equiv 3s_1^2 + p_1t_1^2 \equiv 0 \pmod 8$ and so

$$\varepsilon_1^3 = \frac{s_1(s_1^2+3p_1t_1^2) + t_1(3s_1^2+p_1t_1^2)\sqrt{p_1}}{8} = s + t\sqrt{p_1}\,,$$

where $s = s_1(s_1^2+3p_1t_1^2)/8, t = t_1(3s_1^2+t_1^2)/8 \in \mathbf{Z}$. Since $N_{k/\boldsymbol{Q}}(\varepsilon_1^3) = -1$, $\varepsilon = \varepsilon_1^3$ satisfies the desired conditions. □

The following theorem may be regarded as an analogue of Lemma 1.1.2.

THEOREM 3.1.6. *Assume that the class number of $k$ is 1 and $p_1 \equiv 5 \pmod 8$. Then there are $X, Y, Z \in \mathcal{O}_k$ satisfying the following conditions*:

(1) $X^2 - p_3Y^2 - \alpha Z^2 = 0$,

(2) g.c.d$(X, Y, Z) = 1$, $(Z, 2) = 1$ (resp. g.c.d$(X, Y, Z) = 1$, $(Y, 2) = 1$),

(3) *There is* $\lambda \in \mathcal{O}_{k_{13}}$ (resp. $\lambda \in \mathcal{O}_{k'_{13}}$) *such that* $\lambda^2 \equiv X+Y\sqrt{p_3} \mod (4)$ (resp. $\lambda^2 \equiv X + Z\sqrt{\alpha} \mod (4)$).

PROOF. By Proposition 3.1.3, there are $X, Y, Z \in \mathcal{O}_k$ satisfying (1) and (2).

Case $(Z, 2) = 1$: Let $\theta := X + Y\sqrt{p_3}$ and $\overline{\theta} := \theta \mod (4)$. Then we easily see $\theta \in \mathcal{O}_{k_{13}}$ and $\overline{\theta} \in U$ since $(Z, 2) = 1$. Let $n$ be the order of $\overline{\theta}$ in $U$.

(i) Suppose $n \not\equiv 0 \pmod 2$. Then it is easy to see that there is $\lambda \in \mathcal{O}_{k_{13}}$ such that $\lambda^2 \equiv \theta \mod (4)$.

(ii) Suppose $n \equiv 0 \pmod 2$. By Lemma 3.1.4, $\frac{n}{2} \not\equiv 0 \pmod 2$ and $\overline{\theta}^{\frac{n}{2}} \in U(2)$. Write $\theta^{\frac{n}{2}} = b_1 + b_2\sqrt{p_1} + b_3\sqrt{p_3} + b_4\sqrt{p_1p_3}$, $b_i \in \boldsymbol{Q}$. Since $N_{k_{13}/k}(\theta) = X^2 - p_3Y^2 = \alpha Z^2$, $N_{k_{13}/k}(\theta^{\frac{n}{2}}) = (\alpha Z^2)^{\frac{n}{2}}$. Since $\alpha = x + y\sqrt{p_1} = x - y + 2y \cdot \frac{1+\sqrt{p_1}}{2} \equiv 1 \mod (4)$, $(\alpha Z^2)^{\frac{n}{2}} \equiv (Z^{\frac{n}{2}})^2 \equiv 1 \mod (4)$. Therefore we have

(3.1.6.1)

$$(b_1 + b_2\sqrt{p_1} + b_3\sqrt{p_3} + b_4\sqrt{p_1p_3}) \cdot (b_1 + b_2\sqrt{p_1} - b_3\sqrt{p_3} - b_4\sqrt{p_1p_3}) \equiv 1 \mod (4)\,.$$

We claim that $\theta^{\frac{n}{2}} \equiv -1$ or $\pm\sqrt{p_1} \mod (4)$. Suppose this is not the case. Then, by Lemma 3.1.4, $\theta^{\frac{n}{2}} \equiv \pm\sqrt{p_3}$, $\pm\sqrt{p_1p_3}$ or $a \cdot (3 + \sqrt{p_1} + \sqrt{p_3} + \sqrt{p_1p_3})/2$ $(a \in A) \mod (4)$ and so the coefficients of $\sqrt{p_3}$ or $\sqrt{p_1p_3}$ are not 0. Since any element of $U(2)$ has order 2, we have

$$(b_1 + b_2\sqrt{p_1} + b_3\sqrt{p_3} + b_4\sqrt{p_1p_3}) \cdot (b_1 + b_2\sqrt{p_1} - b_3\sqrt{p_3} - b_4\sqrt{p_1p_3}) \not\equiv 1 \mod (4)\,,$$

which contradicts to (3.1.6.1). Therefore, by Lemma 3.1.5, there is $\varepsilon \in \mathcal{O}_k^\times$ such that $\varepsilon\theta^{\frac{n}{2}} \equiv 1 \mod (4)$ and $\varepsilon^2 \equiv 1 \mod (4)$. Replacing $(X, Y, Z)$ by $(\varepsilon X, \varepsilon Y, \varepsilon Z)$, (1), (2) holds obviously, and (3) is also satisfied because $\varepsilon\theta \mod (4)$ has the order $\frac{n}{2} \not\equiv 0 \pmod 2$.

Case $(Y, 2) = 1$: Let $\theta' := X + Z\sqrt{\alpha}$. Replacing $\theta$ by $\theta'$ and $p_3$ by $\alpha$, the above proof works well by using Lemma 3.1.4. □

Let $\boldsymbol{a} = (X, Y, Z)$ be a triple of integers in $\mathcal{O}_k$ satisfying (1), (2), (3) in Theorem 3.1.6 and fix it once and for all. We let

$$\begin{cases} \theta := X + Y\sqrt{p_3} & \text{if } (Z, 2) = 1\,, \\ \theta' := X + Z\sqrt{\alpha} & \text{if } (Y, 2) = 1\,, \end{cases}$$

and set

$$\begin{cases} \theta_1 := \theta, \\ \theta_2 := X - Y\sqrt{p_3}\,, \\ \theta_3 := \overline{X} + \overline{Y}\sqrt{p_3}\,, \\ \theta_4 := \overline{X} - \overline{Y}\sqrt{p_3}\,, \end{cases} \qquad \begin{cases} \theta'_1 = \theta'\,, \\ \theta'_2 = X - Z\sqrt{\alpha}\,, \\ \theta'_3 = \overline{X} + \overline{Z}\sqrt{\overline{\alpha}}\,, \\ \theta'_4 = \overline{X} - \overline{Z}\sqrt{\overline{\alpha}}\,, \end{cases}$$

where $\overline{X}$, $\overline{Y}$ and $\overline{\alpha}$ are conjugates of $X$, $Y$ and $\alpha$ over $\boldsymbol{Q}$ respectively.

DEFINITION 3.1.7. We then define the number field $K$ by

$$K = K_{\boldsymbol{a}} = \begin{cases} \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{\theta_1\theta_2}, \sqrt{\theta_1\theta_3}, \sqrt{\theta_1}) & \text{if } (Z, 2) = 1\,, \\ \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{\theta'_1\theta'_2}, \sqrt{\theta'_1\theta'_3}, \sqrt{\theta'_1}) & \text{if } (Y, 2) = 1\,. \end{cases}$$

For the latter use, we set, for the case of $(Y, 2) = 1$,

$$\begin{cases} \eta_1 := \left(\sqrt{\theta_1'} + \sqrt{\theta_2'}\right)^2 = 2X + 2Y\sqrt{p_3}\,, \\ \eta_2 := \left(\sqrt{\theta_1'} - \sqrt{\theta_2'}\right)^2 = 2X - 2Y\sqrt{p_3}\,, \\ \eta_3 := \left(\sqrt{\theta_3'} + \sqrt{\theta_4'}\right)^2 = 2\overline{X} + 2\overline{Y}\sqrt{p_3}\,, \\ \eta_4 := \left(\sqrt{\theta_3'} - \sqrt{\theta_4'}\right)^2 = 2\overline{X} - 2\overline{Y}\sqrt{p_3}\,. \end{cases}$$

THEOREM 3.1.8. (1) *We have*

$$K = \begin{cases} \boldsymbol{Q}(\sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4}) & \text{if } (Z, 2) = 1, \\ \boldsymbol{Q}\left(\sqrt{\theta_1'}, \sqrt{\theta_2'}, \sqrt{\theta_3'}, \sqrt{\theta_4'}\right) = \boldsymbol{Q}(\sqrt{\eta_1}, \sqrt{\eta_2}, \sqrt{\eta_3}, \sqrt{\eta_4}) & \text{if } (Y, 2) = 1\,. \end{cases}$$

(2) *The extension $K/\boldsymbol{Q}$ is a Galois extension whose Galois group is isomorphic to $N_4(\boldsymbol{F}_2)$.*

PROOF. (1) Case $(Z, 2) = 1$: It is easy to see $\sqrt{\theta_2}, \sqrt{\theta_3} \in K$. Noting that

$$\begin{aligned} \theta_1\theta_2\theta_3\theta_4 &= N_{k_{13}/\boldsymbol{Q}}(\theta_1) \\ &= N_{k/\boldsymbol{Q}}(N_{k_{13}/k}(\theta_1)) \\ &= N_{k/\boldsymbol{Q}}(\alpha Z^2) \\ &= p_2h^2 \quad (h \in \boldsymbol{Z})\,, \end{aligned} \tag{3.1.8.1}$$

we have $\sqrt{\theta_4} \in K$ and hence $\boldsymbol{Q}(\sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4}) \subset K$. Next we show the converse inclusion. Write $\theta_1 = a_1 + a_2\sqrt{p_1} + a_3\sqrt{p_3} + a_4\sqrt{p_1p_3}$ ($a_i \in \boldsymbol{Q}$). By considering the prime factorization of the ideal $(\alpha Z^2)$ in $k_1$, we find $\alpha Z^2 \notin \boldsymbol{Z}$. Then, by the equality $\theta_1\theta_2 = \alpha Z^2$, we find that the number of $i$ $(1 \le i \le 4)$ with $a_i = 0$ is at most one. Since $\theta_1 + \theta_2 = 2(a_1 + a_2\sqrt{p_1})$, $\theta_1 + \theta_3 = 2(a_1 + a_3\sqrt{p_3})$ and $\theta_1 + \theta_4 = 2(a_1 + a_4\sqrt{p_1p_3})$, $\sqrt{p_1}, \sqrt{p_3} \in \boldsymbol{Q}(\sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4})$. By (3.1.8.1), we get $K \subset \boldsymbol{Q}(\sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4})$.

Case $(Y, 2) = 1$: First, let us show $\boldsymbol{Q}(\sqrt{\theta_1'}, \sqrt{\theta_2'}, \sqrt{\theta_3'}, \sqrt{\theta_4'}) = \boldsymbol{Q}(\sqrt{\eta_1}, \sqrt{\eta_2}, \sqrt{\eta_3}, \sqrt{\eta_4})$. By the definition of $\eta_i$'s, obviously the inclusion $\supset$ holds. Since $\sqrt{\eta_1} + \sqrt{\eta_2} = 2\sqrt{\theta_1'}$, $\sqrt{\eta_1} - \sqrt{\eta_2} = 2\sqrt{\theta_2'}$, $\sqrt{\eta_3} + \sqrt{\eta_4} = 2\sqrt{\theta_3'}$, $\sqrt{\eta_3} - \sqrt{\eta_4} = 2\sqrt{\theta_4'}$, we obtain the converse inclusion $\subset$.

Next, we show $K = \boldsymbol{Q}(\sqrt{\theta_1'}, \sqrt{\theta_2'}, \sqrt{\theta_3'}, \sqrt{\theta_4'})$. It is easy to see $\sqrt{\theta_2'}, \sqrt{\theta_3'} \in K$. Since $\theta_1'\theta_2' = X^2 - \alpha Z^2 = p_3Y^2$, we have $\theta_3'\theta_4' = \overline{X}^2 - \overline{\alpha}\overline{Z}^2 = p_3\overline{Y}^2$. So, $\theta_1'\theta_2'\theta_3'\theta_4' = p_3^2(Y\overline{Y})^2 \in \boldsymbol{Q}$ and $\sqrt{\theta_4'} \in K$. For the converse inclusion, it suffices to show $K \subset \boldsymbol{Q}(\sqrt{\eta_1}, \sqrt{\eta_2}, \sqrt{\eta_3}, \sqrt{\eta_4})$. By considering the prime factorization of the ideal $(\alpha(2Z)^2)$ in $k_1$, we find $\alpha(2Z)^2 \notin \boldsymbol{Z}$. By $N_{k_{13}/\boldsymbol{Q}}(\eta_1) = 4p_2h^2$ and the argument similar to the case of $(Z, 2) = 1$, we have $\sqrt{p_i} \in \boldsymbol{Q}(\sqrt{\eta_1}, \sqrt{\eta_2}, \sqrt{\eta_3}, \sqrt{\eta_4})$ $(i = 1, 2, 3)$.

(2) Case $(Z, 2) = 1$: First, $K/\boldsymbol{Q}$ is a Galois extension, because $K$ is the splitting field of $\Pi_{i=1}^4(T^2 - \theta_i) = \Pi_{\sigma \in \mathrm{Gal}(k_{13}/\boldsymbol{Q})}(T^2 - \sigma(\theta_1)) \in \boldsymbol{Z}[T]$. Next, let $k_{123} = \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$, $K_1 := k_{123}(\sqrt{\theta_1\theta_2})$ and $K_2 := K_1(\sqrt{\theta_1\theta_3})$. Since $\theta_3\theta_4 = \overline{\theta_1\theta_2}$ and

$\sqrt{\theta_3\theta_4} = h\sqrt{p_2}/\sqrt{\theta_1\theta_2} \in K_1$, $K_1/k_{123}$ is a Galois extension. Let us show $[K_1 : k_{123}] = 2$. Define $\sigma \in \mathrm{Gal}(k_{123}/\boldsymbol{Q})$ by

$$\sigma : (\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}) \mapsto (-\sqrt{p_1}, -\sqrt{p_2}, \sqrt{p_3}) .$$

Let $\tilde{\sigma} \in \mathrm{Gal}(K_1/\boldsymbol{Q})$ be an extension of $\sigma$. Then we have

$$(\tilde{\sigma}(\sqrt{\theta_1\theta_2}))^2 = \tilde{\sigma}(\theta_1\theta_2) = \theta_3\theta_4$$

and so $\tilde{\sigma}(\sqrt{\theta_1\theta_2}) = \pm\sqrt{\theta_3\theta_4}$. Therefore we have

$$\tilde{\sigma}^2(\sqrt{\theta_1\theta_2}) = \tilde{\sigma}(\pm\sqrt{\theta_3\theta_4}) = \tilde{\sigma}(\pm h\sqrt{p_2}/\sqrt{\theta_1\theta_2}) = -\sqrt{\theta_1\theta_2} .$$

Since $\tilde{\sigma}^2 \mid_{k_{123}} = \mathrm{id}$, $\sqrt{\theta_1\theta_2} \notin k_{123}$ and hence $[K_1 : k_{123}] = 2$. Similarly we can show that $K_2/K_1$ is a Galois extension and $[K_2 : K_1] = [K : K_2] = 2$. Hence we have $[K : \boldsymbol{Q}] = [K : K_2][K_2 : K_1][K_1 : k_{123}][k_{123} : \boldsymbol{Q}] = 64$.

Case $(Y, 2) = 1$: $K/\boldsymbol{Q}$ is a Galois extension, because $K$ is the splitting field of $\Pi_{i=1}^4(T^2 - \eta_i) = \Pi_{\sigma\in\mathrm{Gal}(k_{13}/\boldsymbol{Q})}(T^2 - \sigma(\eta_1)) \in \boldsymbol{Z}[T]$. Let $K_1' := k_{123}(\sqrt{\eta_1\eta_2})$ and $E_2' := k_{123}(\sqrt{\eta_1\eta_3})$. By the argumet similar to the case $(Z, 2) = 1$, we have $[K : \boldsymbol{Q}] = [K : K_2'][K_2' : K_1'][K_1' : k_{123}][k_{123} : \boldsymbol{Q}] = 64$.

Finally, by the computer calculation using GAP, we have the following presentation of the group $N_4(\boldsymbol{F}_2)$:

$$N_4(\boldsymbol{F}_2) = \left\langle g_1, g_2, g_3 \;\middle|\; \begin{array}{l} g_1^2 = g_2^2 = g_3^2 = (g_1g_3)^2 = 1 \\ (g_1g_2)^4 = (g_2g_3)^4 = (g_1g_2g_3)^4 = 1 \\ ((g_1g_2g_3g_2)^2g_3)^2 = 1 \end{array} \right\rangle,$$

where $g_1$, $g_2$ and $g_3$ are words representing the following matrices respectively:

$$g_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Case $(Z, 2) = 1$: We define $\tau_1, \tau_2, \tau_3 \in \mathrm{Gal}(K/\boldsymbol{Q})$ by

$$\begin{aligned}
\tau_1 :\ & (\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{\theta_1\theta_2}, \sqrt{\theta_1\theta_3}, \sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4}) \\
& \mapsto (-\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{\theta_3\theta_4}, \sqrt{\theta_1\theta_3}, \sqrt{\theta_3}, \sqrt{\theta_4}, \sqrt{\theta_1}, \sqrt{\theta_2}) \\
\tau_2 :\ & (\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{\theta_1\theta_2}, \sqrt{\theta_1\theta_3}, \sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4}) \\
& \mapsto (\sqrt{p_1}, -\sqrt{p_2}, \sqrt{p_3}, -\sqrt{\theta_1\theta_2}, -\sqrt{\theta_1\theta_3}, -\sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4}) \\
\tau_3 :\ & (\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{\theta_1\theta_2}, \sqrt{\theta_1\theta_3}, \sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4}) \\
& \mapsto (\sqrt{p_1}, \sqrt{p_2}, -\sqrt{p_3}, \sqrt{\theta_1\theta_2}, \sqrt{\theta_2\theta_4}, \sqrt{\theta_2}, \sqrt{\theta_1}, \sqrt{\theta_4}, \sqrt{\theta_3}) .
\end{aligned}$$

Then we can easily check $\tau_1^2 = \tau_2^2 = \tau_3^2 = (\tau_1\tau_3)^2 = \mathrm{id}$, $(\tau_1\tau_2)^4 = (\tau_2\tau_3)^4 = (\tau_1\tau_2\tau_3)^4 = \mathrm{id}$, $((\tau_1\tau_2\tau_3\tau_2)^2\tau_3)^2 = \mathrm{id}$. Thus the correspondence $\tau_i \mapsto g_i$ $(i = 1, 2, 3)$ gives an isomorphism $\mathrm{Gal}(K/\boldsymbol{Q}) \simeq N_4(\boldsymbol{F}_2)$.

Case $(Y, 2) = 1$: We note $K = \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{\eta_1\eta_2}, \sqrt{\eta_1\eta_3}, \sqrt{\eta_1})$, because $\sqrt{\eta_3\eta_4} = 4h\sqrt{p_2}/\sqrt{\eta_1\eta_2} \in K_1$. Then the assertion can be shown in a way similar to the case $(Z, 2) = 1$, by replacing $\theta_i$ with $\eta_i$. □

Next, let us study the ramification in our extension $K/\boldsymbol{Q}$. First, we recall the following well-known fact on the ramification in a Kummer extension.

LEMMA 3.1.9 ([B, Lemma 6]). *Let $l$ be a prime number and $E$ a number field containing a primitive $l$-th root of unity. Let $E(\sqrt[l]{a})$ ($a \in \mathcal{O}_E$) be a Kummer extension over $E$ of degree $l$. Suppose $(a) = \mathfrak{q}^m\mathfrak{a}$ where $\mathfrak{q}$ is a prime ideal in $E$ which does not divide $l$, $(\mathfrak{q}, \mathfrak{a}) = 1$ and $l \mid m$. Then $\mathfrak{q}$ is unramified in $E(\sqrt[l]{a})/E$.*

THEOREM 3.1.10. *All prime numbers ramified in the extension $K/\boldsymbol{Q}$ are $p_1$, $p_2$ and $p_3$ with ramification index 2.*

PROOF. Case $(Z, 2) = 1$: Let us study the ramification in the extension $k_{13}(\sqrt{\theta_1})/k_{13}$. Since $(T - \frac{\lambda+\sqrt{\theta_1}}{2})(T - \frac{\lambda-\sqrt{\theta_1}}{2}) = (T - \frac{\lambda}{2})^2 - (\frac{\sqrt{\theta_1}}{2})^2 = T^2 - \lambda T + \frac{\lambda^2}{4} - \frac{\theta_1}{4}$ with $\lambda$, $\frac{\lambda^2-\theta_1}{4} \in \mathcal{O}_{k_{13}}$, we find $\frac{\lambda+\sqrt{\theta_1}}{2} \in \mathcal{O}_{k_{13}(\sqrt{\theta_1})}$. Since the relative discriminant of $\frac{\lambda+\sqrt{\theta_1}}{2}$ in $k_{13}(\sqrt{\theta_1})/k_{13}$ is given by

$$\begin{vmatrix} 1 & \frac{\lambda+\sqrt{\theta_1}}{2} \\ 1 & \frac{\lambda-\sqrt{\theta_1}}{2} \end{vmatrix}^2 = \left(\frac{\lambda - \sqrt{\theta_1}}{2} - \frac{\lambda + \sqrt{\theta_1}}{2}\right)^2 = \theta_1 ,$$

we find that any prime factor of 2 is unramified in $k_{13}(\sqrt{\theta_1})/k_{13}$.

Next, let us look closely at the prime factorization of the ideal $(\theta_1)$ in $k_{13}$. We let

$$(\theta_1) = \mathfrak{Q}_1^{e_1}\mathfrak{Q}_2^{e_2}\cdots\mathfrak{Q}_r^{e_r}$$

be the prime factorization of $(\theta_1)$ and let $\mathfrak{q}_i = \mathfrak{Q}_i \cap k$. Since $N_{k_{13}/k}(\theta) = X^2 - p_3Y^2 = \alpha Z^2$, we have

$$N_{k_{13}/k}((\theta_1)) = (\alpha Z^2) = \mathfrak{p}_2^m\mathfrak{a}^2 , \tag{3.1.10.1}$$

where $\mathfrak{a} := (Z)$ is an ideal in $k$. Now the prime factorization of $\mathfrak{q}_i$ in $k_{13}/k$ has the following three cases:

(i) $\mathfrak{q}_i = \mathfrak{Q}_i^2 \quad N_{k_{13}/k}(\mathfrak{Q}_i) = \mathfrak{q}_i$,
(ii) $\mathfrak{q}_i = \mathfrak{Q}_i \quad N_{k_{13}/k}(\mathfrak{Q}_i) = \mathfrak{q}_i^2$,
(iii) $\mathfrak{q}_i = \mathfrak{Q}_i\mathfrak{Q}_i' \quad N_{k_{13}/k}(\mathfrak{Q}_i) = \mathfrak{q}_i,\ N_{k_{13}/k}(\mathfrak{Q}_i') = \mathfrak{q}_i$

Case (i): If $e_i$ is odd, it contradicts to (3.1.10.1). Hence $e_i$ is even.

Case (ii): Since $\theta_1 \in \mathfrak{Q}_i$ and $\mathfrak{q}_i = \mathfrak{Q}_i$, $\theta_2 = a_1 + a_2\sqrt{p_1} - a_3\sqrt{p_3} - a_4\sqrt{p_1p_3} = X - Y\sqrt{p_3} \in \mathfrak{Q}_i$. Since $\mathfrak{p}_2$ is decomposed in $k_{13}/k$, we see, by (3.1.10.1), $Z \in \mathfrak{Q}_i$. Further, since $\mathfrak{Q}_i$ is not a prime factor of 2 by $(Z, 2) = 1$ and $2X = \theta_1 + \theta_2 \in \mathfrak{Q}_i$, $2Y\sqrt{p_3} = \theta_1 - \theta_2 \in \mathfrak{Q}_i$ and $X, Y, Z \in k$, we have $X, Y, Z \in \mathfrak{q}_i$, which contradicts to g.c.d$(X, Y, Z) = 1$.

Case (iii): Suppose $\mathfrak{P}$ and $\mathfrak{P}'$ are prime factors of $\mathfrak{p}_2$. Since the exponent $m$ in (3.1.10.1) is odd, one of $\mathfrak{P}$ and $\mathfrak{P}'$ appears odd times in the prime factorization of $(\theta_1)$. Let $\mathfrak{P}$ be that one. When $\mathfrak{Q}_i \neq \mathfrak{P}$, assume $e_i$ is odd. By (3.1.10.1), $\mathfrak{Q}_i'$ also appears odd times in the prime factorization of $(\theta_1)$. Therefore we have $\theta_1 \in \mathfrak{Q}_i\mathfrak{Q}_i' = \mathfrak{q}_i$ and $\theta_2 \in \mathfrak{q}_i$, and so $2X = \theta_1 + \theta_2 \in \mathfrak{Q}_i$, $2Y\sqrt{p_3} = \theta_1 - \theta_2 \in \mathfrak{Q}_i$. This deduces $X, Y, Z \in \mathfrak{q}_i$, which contradicts to g.c.d $(X, Y, Z) = 1$. Thus $e_i$ must be even.

Getting all together, we find that $(\theta_1)$ has the form $\mathfrak{P}^{m_1}\mathfrak{A}^2$ ($m_1$: odd). Then, by Lemma 3.1.9, ramified finite primes in $k_{13}(\sqrt{\theta_1})/k_{13}$ must be lying over $p_2$. Similarly, we see that ramified finite primes in $k_{13}(\sqrt{\theta_i})/k_{13}$ $(i = 2, 3, 4)$ are all lying over $p_2$. This shows that any ramified finite prime in the extension $K = k_{13}(\sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4})/k_{13}$ is lying over $p_2$. Since $k_{13}/\boldsymbol{Q}$ is unramified outside $p_1$, $p_3$, we conclude that all ramified prime numbers in $K/\boldsymbol{Q}$ are $p_1$, $p_2$ and $p_3$.

Finally, we show that the ramification indices of $p_i$'s in $K/\boldsymbol{Q}$ are all 2. We easily see that this is true for $p_1$ and $p_3$, because the ramification indices of $p_1$ and $p_2$ in $k_{13}/\boldsymbol{Q}$ are 2 and any prime factor of $p_1$ or $p_3$ is unramified in $K/k_{13}$. So it suffices to show our assertion for $p_2$. Let $\mathfrak{p}_{2i}$ be a prime factor in $k_{13}$ of $p_2$ which is ramified in $k_{13}(\sqrt{\theta_1})/k_{13}$. Since we have $\mathfrak{p}_{2i} = \mathfrak{Q}_i^2$ in $k_{13}(\sqrt{\theta_1})$, by considering the prime factorization of the ideal $(\theta_i)$ in $k_{13}(\sqrt{\theta_1})$, we see by Lemma 3.1.9 that $\mathfrak{Q}_i$ is unramified in $k_{13}(\sqrt{\theta_1}, \sqrt{\theta_i})$. Therefore any prime factor of $p_2$ ramified in $k_{13}(\sqrt{\theta_1})/k_{13}$ is unramified in $k_{13}(\sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4})/k_{13}(\sqrt{\theta_1})$. Thus the ramification index of $p_2$ is 2.

Case $(Y, 2) = 1$: As in the case of $(Z, 2) = 1$, we consider the prime factorization of $(\theta_1')$ in $k_{13}'$. Then, by a similar argument, we find that $(\theta_1')$ has the ideal decomposition of the form $\mathfrak{Q}'\mathfrak{B}^2$ where any prime factor of $\mathfrak{Q}'$ is lying over $p_3$. This shows by Lemma 3.1.9 that any ramified finite prime in $k_{13}'(\sqrt{\theta_1'})/k_{13}'$ is lying over $p_3$. Similarly, we see that finite ramified primes in $k_{13}'(\sqrt{\theta_2'})/k_{13}'$, $\overline{k_{13}'}(\sqrt{\theta_3'})/\overline{k_{13}'}$ and $\overline{k_{13}'}(\sqrt{\theta_4'})/\overline{k_{13}'}$ are all lying over $p_3$. Hence all ramified prime numbers in $K/\boldsymbol{Q}$ are $p_1$, $p_2$ and $p_3$. The assertion on the ramification indices of $p_i$'s can also be shown by an argument similar to the case of $(Z, 2) = 1$. □

THEOREM 3.1.11. *We have*

$$K = \begin{cases} k_{\{p_1,p_2\}}k_{\{p_2,p_3\}}(\sqrt{\theta_1}) & \text{if } (Z,2) = 1\,, \\ k_{\{p_1,p_2\}}k_{\{p_3,p_2\}}(\sqrt{\theta_1'}) & \text{if } (Y,2) = 1\,. \end{cases}$$

PROOF. Case $(Z, 2) = 1$: First we have

$$\begin{aligned} \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\theta_1\theta_2}) &= \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha Z^2}) \\ &= \boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha}) \\ &= k_{\{p_1,p_2\}}\,. \end{aligned}$$

Next, it is easy to see that $\boldsymbol{Q}(\sqrt{p_2}, \sqrt{p_3}, \sqrt{\theta_1\theta_3})$ is a dihedral extension over $\boldsymbol{Q}$ of degree 8. Since all prime numbers ramified in $\boldsymbol{Q}(\sqrt{p_2}, \sqrt{p_3}, \sqrt{\theta_1\theta_3})/\boldsymbol{Q}$ are $p_2$ and $p_3$ with ramification index 2 by Theorem 3.1.10, we have

$$\boldsymbol{Q}(\sqrt{p_2}, \sqrt{p_3}, \sqrt{\theta_1\theta_3}) = k_{\{p_3,p_2\}}$$

by Theorem 1.1.7. Hence we have

$$K = k_{\{p_1,p_2\}}k_{\{p_3,p_2\}}(\sqrt{\theta_1})\,.$$

Case $(Y,2)=1$: Noting that $\eta_1 = 2X + 2Y\sqrt{p_3}$, $\eta_2 = 2X - 2Y\sqrt{p_3}$ and $\eta_3 = 2\overline{X} + 2\overline{Y}\sqrt{p_3}$, we have

$$\begin{aligned}\boldsymbol{Q}(\sqrt{p_1},\sqrt{p_2},\sqrt{\eta_1\eta_2}) &= \boldsymbol{Q}(\sqrt{p_1},\sqrt{p_2},\sqrt{4\alpha Z^2}) \\ &= \boldsymbol{Q}(\sqrt{p_1},\sqrt{p_2},\sqrt{\alpha}) \\ &= k_{\{p_1,p_2\}}\,.\end{aligned}$$

By the same argument as in the case of $(Z,2)=1$ replacing $\theta_i$ with $\eta_i$, we have $\boldsymbol{Q}(\sqrt{p_2},\sqrt{p_3},\sqrt{\eta_1\eta_3}) = k_{\{p_3,p_2\}}$. Hence we have, by Theorem 3.1.8,

$$\begin{aligned}K &= \boldsymbol{Q}(\sqrt{\eta_1},\sqrt{\eta_2},\sqrt{\eta_3},\sqrt{\eta_4}) \\ &= \boldsymbol{Q}(\sqrt{p_1},\sqrt{p_2},\sqrt{p_3},\sqrt{\eta_1\eta_2},\sqrt{\eta_1\eta_3},\sqrt{\eta_1}) \\ &= k_{\{p_1,p_2\}}k_{\{p_3,p_2\}}(\sqrt{\theta_1'})\,.\end{aligned}$$

□

**3.2. The 4-th multiple residue symbol.** Let $p_1$, $p_2$, $p_3$ and $p_4$ be four prime numbers satisfying

$$\text{(3.2.1)}\qquad \begin{cases} p_1 \equiv 5 \pmod 8,\ p_i \equiv 1 \pmod 4\ (i=2,3,4)\,, \\ \left(\dfrac{p_i}{p_j}\right) = 1\ (1 \le i \ne j \le 4),\ [p_i,p_j,p_k] = 1\ (i,j,k:\ \text{distinct})\,, \end{cases}$$

and we assume that the class number of $k_1 = \boldsymbol{Q}(\sqrt{p_1})$ is 1.

Let $K$ be the field defined in Definition 3.1.7.

DEFINITION 3.2.2. We define the 4-*th multiple residue symbol* $[p_1,p_2,p_3,p_4]$ by

$$[p_1,p_2,p_3,p_4] = \begin{cases} 1 & \text{if } p_4 \text{ is completely decomposed in } K/\boldsymbol{Q}\,, \\ -1 & \text{otherwise.}\end{cases}$$

We let

$$L := \begin{cases} \boldsymbol{Q}(\sqrt{p_1},\sqrt{p_2},\sqrt{p_3},\sqrt{\theta_1\theta_2},\sqrt{\theta_1\theta_3}) & \text{if } (Z,2)=1\,, \\ \boldsymbol{Q}(\sqrt{p_1},\sqrt{p_2},\sqrt{p_3},\sqrt{\eta_1\eta_2},\sqrt{\eta_1\eta_3}) & \text{if } (Y,2)=1\,.\end{cases}$$

Case $(Z,2)=1$: Let $\tau_1,\tau_2,\tau_3 \in \mathrm{Gal}(K/\boldsymbol{Q})$ be as in the proof of Theorem 3.1.8 and we let

$$\xi_1 := \sqrt{\theta_1\theta_2} + \sqrt{\theta_3\theta_4}\,,\quad \xi_2 := \sqrt{\theta_1\theta_3} + \sqrt{\theta_2\theta_4}\,,\quad \xi_3 := \sqrt{\theta_1} + \sqrt{\theta_2} + \sqrt{\theta_3} + \sqrt{\theta_4}\,.$$

Then, the subfields of $K/\boldsymbol{Q}$ which corresponds by Galois theory to the subgroups generated by $\tau_1$, $\tau_2$, $\tau_3$ and $(\tau_1\tau_2\tau_3\tau_2)^2$ are $\boldsymbol{Q}(\sqrt{p_2},\sqrt{p_3},\xi_1,\sqrt{\theta_1\theta_3},\xi_3)$, $\boldsymbol{Q}(\sqrt{p_1},\sqrt{p_3},\sqrt{\theta_2},\sqrt{\theta_3},\sqrt{\theta_4})$, $\boldsymbol{Q}(\sqrt{p_1},\sqrt{p_2},\sqrt{\theta_1\theta_2},\xi_2,\xi_3)$ and $F$, respectively. By the assumption (3.2.1), $p_4$ is completely decomposed in the extension $F/\boldsymbol{Q}$.

Case $(Y,2)=1$: We let $\tau_1,\tau_2,\tau_3 \in \mathrm{Gal}(K/\boldsymbol{Q})$ and $\xi_1,\xi_2,\xi_3$ be defined by replacing $\theta_i$ in the case $(Z,2)=1$ with $\eta_i$ $(1 \le i \le 4)$. Then, as in the case $(Z,2)=1$ the subfields of $K/\boldsymbol{Q}$ which corresponds by Galois theory to the subgroups generated by $\tau_1$, $\tau_2$, $\tau_3$ and $(\tau_1\tau_2\tau_3\tau_2)^2$ are $\boldsymbol{Q}(\sqrt{p_2},\sqrt{p_3},\xi_1,\sqrt{\eta_1\eta_3},\xi_3)$, $\boldsymbol{Q}(\sqrt{p_1},\sqrt{p_3},\sqrt{\eta_2},\sqrt{\eta_3},\sqrt{\eta_4})$,

$\boldsymbol{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\eta_1\eta_2}, \xi_2, \xi_3)$ and $F$, respectively. By the assumption (3.2.1), $p_4$ is completely decomposed in the extension $F/\boldsymbol{Q}$.

Let $\mathfrak{P}_4$ be a prime ideal in $F$ lying over $p_4$ and let $\sigma_{\mathfrak{P}_4} = \left(\frac{K/F}{\mathfrak{P}_4}\right) \in \mathrm{Gal}(K/F)$ be the Frobenius automorphism of $\mathfrak{P}_4$. Note that $\mathfrak{P}_4$ is decomposed in $K/F$ if and only if $p_4$ is completely decomposed in $K/\boldsymbol{Q}$. So we have, by Definition 3.2.2,

$$[p_1, p_2, p_3, p_4] = \begin{cases} 1 & \sigma_{\mathfrak{P}_4} = \mathrm{id}_K\,, \\ -1 & \sigma_{\mathfrak{P}_4} \neq \mathrm{id}_K\,. \end{cases} \tag{3.2.3}$$

Let $S := \{p_1, p_2, p_3, p_4\}$. Then, by Theorem 2.2.2, we have

$$\begin{aligned} G_S(2) &= \mathrm{Gal}(\boldsymbol{Q}_S(2)/\boldsymbol{Q}) \\ &= \langle x_1, x_2, x_3, x_4 \mid x_1^{p_1-1}[x_1, y_1] = \cdots = x_4^{p_4-1}[x_4, y_4] = 1\rangle\,. \end{aligned}$$

Let $\hat{F}$ be the free pro-2 group on $x_1, x_2, x_3, x_4$ and let $\pi : \hat{F}(2) \to G_S(2)$ be the natural homomorphism. Since $K \subset \boldsymbol{Q}_S(2)$ by Theorem 3.1.10, we have the natural homomorphism $\psi : G_S(2) \to \mathrm{Gal}(K/\boldsymbol{Q})$. Let $\varphi := \pi \circ \psi : \hat{F} \to \mathrm{Gal}(K/\boldsymbol{Q})$. We then see that

$$\varphi(x_1) = \tau_1\,, \quad \varphi(x_2) = \tau_2\,, \quad \varphi(x_3) = \tau_3, \quad \varphi(x_4) = 1\,.$$

Therefore the relations among $\tau_1$, $\tau_2$ and $\tau_3$ are equivalent to the following relations:

$$\begin{aligned} &\varphi(x_1)^2 = \varphi(x_2)^2 = \varphi(x_3)^2 = \varphi(x_1x_3)^2 = 1\,, \quad \varphi(x_4) = 1\,, \\ &\varphi(x_1x_2)^4 = \varphi(x_2x_3)^4 = \varphi(x_1x_2x_3)^4 = \varphi((x_1x_2x_3x_2)^2x_3)^2 = 1\,. \end{aligned} \tag{3.2.4}$$

On the other hand, by the assumption (3.2.1), we have $\overline{\mu}_2(1234) = \mu_2(1234)$.

THEOREM 3.2.5. *We have*

$$[p_1, p_2, p_3, p_4] = (-1)^{\mu_2(1234)}\,.$$

PROOF. By (3.2.3), we have

$$\varphi(y_4) = \begin{cases} 1 & \text{if } [p_1, p_2, p_3, p_4] = 1\,, \\ (\tau_1\tau_2\tau_3\tau_2)^2 = \varphi((x_1x_2x_3x_2)^2) & \text{if } [p_1, p_2, p_3, p_4] = -1\,. \end{cases}$$

By (3.2.4), $\mathrm{Ker}(\varphi)$ is generated as a normal subgroup of $\hat{F}$ by

$$x_1^2, x_2^2, x_3^2, (x_1x_3)^2, x_4, (x_1x_2)^4, (x_2x_3)^4, (x_1x_2x_3)^4 \text{ and } ((x_1x_2x_3x_2)^2x_3)^2$$

and one has

$$\begin{aligned}
&M_2((x_1)^2) = (1+X_1)^2 = 1+X_1^2\,,\\
&M_2((x_2)^2) = (1+X_2)^2 = 1+X_2^2\,,\\
&M_2((x_3)^2) = (1+X_3)^2 = 1+X_3^2\,,\\
&M_2((x_1x_3)^2) = ((1+X_1)(1+X_3))^2 \equiv 1 \bmod \deg\ \geq 2\,,\\
&M_2((x_1x_2)^4) = ((1+X_1)(1+X_2))^4 \equiv 1 \bmod \deg\ \geq 4\,,\\
&M_2((x_2x_3)^4) = ((1+X_2)(1+X_3))^4 \equiv 1 \bmod \deg\ \geq 4\,,\\
&M_2((x_1x_2x_3)^4) = ((1+X_1)(1+X_2)(1+X_3))^4 \equiv 1 \bmod \deg\ \geq 4\,,\\
&M_2(((x_1x_2x_3x_2)^2x_3)^2)\\
&\equiv 1+X_3^2+X_1^2X_3+X_1X_3^2+X_1X_3^2+X_3X_1^2+X_3^2X_1 \bmod \deg\ \geq 4\,.
\end{aligned}$$

Therefore $\mu_2((1);*)$, $\mu_2((2);*)$, $\mu_2((3);*)$, $\mu_2((12);*)$, $\mu_2((23);*)$, $\mu_2((123);*)$ take their values 0 on $\mathrm{Ker}(\varphi)$. If $\varphi(y_4) = 1$, $\mu_2(1234) = \mu_2((123); y_4) = 0$ by $\varphi(y_4) \in \mathrm{Ker}(\varphi)$. If $\varphi(y_4) = (\tau_1\tau_2\tau_3\tau_2)^2 = \varphi((x_1x_2x_3x_2)^2)$, we can write $y_4 = (x_1x_2x_3x_2)^2R$, where $R \in \mathrm{Ker}(\varphi)$. Then comparing the coefficients of $X_1X_2X_3$ in the equality $M_2(y_4) = M_2((x_1x_2x_3x_2)^2)M_2(R)$, we have

$$\begin{aligned}
\mu_2(1234) &= \mu_2((123); y_4)\\
&= \mu_2((123); (x_1x_2x_3x_2)^2) + \mu_2((12); (x_1x_2x_3x_2)^2)\mu_2((3); R)\\
&\quad + \mu_2((1); (x_1x_2x_3x_2)^2)\mu_2((23); R) + \mu_2((123); R)\\
&= 1\,.
\end{aligned}$$

This yields our assertion. □

EXAMPLE 3.2.6. Let $(p_1, p_2, p_3, p_4) := (5, 8081, 101, 449)$. Then we have

$$\begin{cases} \theta_1 = 25+2\sqrt{5}+2\sqrt{101}\,,\\ \theta_2 = 25+2\sqrt{5}-2\sqrt{101}\,,\\ \theta_3 = 25-2\sqrt{5}+2\sqrt{101}\,,\\ \theta_4 = 25-2\sqrt{5}-2\sqrt{101}\,, \end{cases} \quad \begin{cases} k_{\{p_1,p_2\}} = \boldsymbol{Q}(\sqrt{5}, \sqrt{8081}, \sqrt{241+100\sqrt{5}})\,,\\ k_{\{p_3,p_2\}} = \boldsymbol{Q}(\sqrt{8081}, \sqrt{101}, \sqrt{1009+100\sqrt{101}})\,, \end{cases}$$

and

$$K = k_{\{p_1,p_2\}} \cdot k_{\{p_3,p_2\}}(\sqrt{25+2\sqrt{5}+2\sqrt{101}})\,.$$

Then we have

$$\begin{cases} \left(\frac{p_i}{p_j}\right) = 1 \ \ (1 \leq i \neq j \leq 4)\,, \quad [p_i, p_j, p_k] = 1 \ \ (i, j, k:\ \text{distinct})\,,\\ [p_1, p_2, p_3, p_4] = -1\,. \end{cases}$$

In view of Example 2.1.3, this 4-tuple prime numbers may be called *Milnor primes*.

5 8081 101 449

Finally, two remarks are in order.

REMARK 3.2.7. (1) By Theorem 3.2.5, the shuffle relation for arithmetic Milnor invariants (Theorem 2.2.3 (3)) yields the following shuffle relation for the 4-th multiple residue symbol

$$\prod_{(ijk)\in \mathrm{PSH}(I,J)} [p_i, p_j, p_k, p_l] = 1\,,$$

where $I$, $J$ are multi-indices with $|I| + |J| = 3$ and $\mathrm{PSH}(I, J)$ is the set of proper shuffles of $I$ and $J$, and $1 \leq l \leq 4$. It is also expected that our 4-th multiple residue symbols satisfy the cyclic symmetry, although we are not able to prove it in the present paper. We hope to study the reciprocity law for the 4-th multiple residue symbol in the future.

(2) In this paper, we are concerned only with 2-extensions over $\boldsymbol{Q}$ as a generalization of Rédei's work. If a base number field $k$ contains the group of $l$-th roots of unity $\mu_l$ for an odd prime number $l$ and the maximal pro-$l$ Galois group over $k$ unramified outside a set of certain primes $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} \cup \{\mathfrak{p}|\infty\}$ is a Koch type pro-$l$ group, we can intoduce $\mu_l$-valued multiple residue symbol $[\mathfrak{p}_1, \ldots, \mathfrak{p}_r]$ in a similar manner.

*Acknowledgment.* I would like to thank my advisor Professor Masanori Morishita for proposing the problem studied in this paper and valuable advice. I also thank Professor Yasushi Mizusawa for the computation of the group $N_4(\boldsymbol{F}_2)$ by GAP. Finally I am grateful to the referee for useful comments.

## REFERENCES

[A] F. AMANO, On Rédei's dihedral extension and triple reciprocity law, Proc. Japan Acad. Ser. A Math. Sci. 90 (2014), 1–5.

[B] B. J. BIRCH, Cyclotomic fields and Kummer extensions. Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), pages 85–93. Thompson, Washington, D.C., 1967.

[CFL] K. T. CHEN, R. H. FOX AND R. C. LYNDON, Free differential calculus. IV. The quotient groups of the lower central series, Ann. of Math. (2) 68 (1958), 81–95.

[F] R. H. FOX, Free differential calculus. I: Derivation in the free group ring, Ann. of Math. 57 (1953), 547–560.

[I] Y. IHARA, On Galois representations arising from towers of coverings of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$, Invent. Math. 86 (1986), no. 3, 427–459.

[K1] H. KOCH, Galois theory of $p$-extensions. With a foreword by I. R. Shafarevich. Translated from the 1970 German original by Franz Lemmermeyer. With a postscript by the author and Lemmermeyer. Springer Monographs Math. Springer-Verlag, Berlin, 2002.

[K2] H. KOCH, On $p$-extension with given ramification, Appendix in: K. Haberland, Galois cohomology of algebraic number fields, 89–126, VEB Deutscher Verlag der Wissenschaften, Berlin, 1978.

[Mi1] J. MILNOR, Link groups, Ann. of Math. 59 (1954), 177–195.

[Mi2] J. MILNOR, Isotopy of links, in Algebraic Geometry and Topology, A symposium in honor of S. Lefschetz (edited by R.H. Fox, D.C. Spencer and A.W. Tucker), 280–306, Princeton University Press, Princeton, N.J., 1957.

[Mo1] M. MORISHITA, Milnor's link invariants attached to certain Galois groups over **Q**, Proc. Japan Acad. Ser. A Math. Sci. 76 (2000), 18–21.

[Mo2] M. MORISHITA, On certain analogies between knots and primes, J. Reine Angew. Math. 550 (2002), 141–167.

[Mo3] M. MORISHITA, Milnor invariants and Massey products for prime numbers, Compos. Math. 140 (2004), 69–83.

[Mo4] M. MORISHITA, Knots and Primes—An introduction to arithmetic topology, Universitext, Springer, London, 2012.

[Mu] K. MURASUGI, Nilpotent coverings of links and Milnor's invariant, Low-dimensional topology (Chelwood Gate, 1982), 106–142, London Math. Soc. Lecture Note Ser., 95, Cambridge Univ. Press, Cambridge-New York, 1985.

[O] T. ODA, Note on meta-abelian quotients of pro-$l$ free groups, preprint, 1985.

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

[V1] D. VOGEL, On the Galois group of 2-extensions with restricted ramification, J. Reine Angew. Math. 581 (2005), 117–150.

[V2] D. VOGEL, A letter to M. Morishita, 2008, February.

FACULTY OF MATHEMATICS
KYUSHU UNIVERSITY
744, MOTOOKA, NISHI-KU
FUKUOKA, 819–0395
JAPAN

*E-mail address*: f-amano@math.kyushu-u.ac.jp