On a certain nilpotent extension over $\mathbb{Q}$ of degree 64 and the 4-th multiple residue symbol

By

Fumiya AMANO*

Abstract

This is the report of my talk at RIMS conference “Algebraic Number Theory and Related Topics”. I would like to thank again the organizers for giving me an opportunity to participate in the conference.

§0 Background and main results

In this section, we review briefly the historical background on the subject with which we are concerned.

As is well known, for distinct 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 $\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}$ as follows:

$$
\left(\frac{p_1}{p_2}\right) = \begin{cases} 
1 & \exists x \in \mathbb{Z} \text{ s.t. } x^2 \equiv p_1 \pmod{p_2}, \\
-1 & \text{otherwise}.
\end{cases}
$$

In 1939, Rédei ([R]) introduced a certain triple symbol, called the Rédei symbol, with the intention of a generalization of the Legendre symbol and Gauss’ genus theory. For distinct prime numbers $p_1, p_2$ and $p_3$ satisfying

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

Received March 30, 2012. Revised April 12, 2012.
2000 Mathematics Subject Classification(s): 11R.
Key Words: Rédei symbol, multiple residue symbol.

*Graduate School of Mathematics, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, 819-0395, JAPAN.
e-mail: f-aman0@math.kyushu-u.ac.jp
© 2013 Research Institute for Mathematical Sciences, Kyoto University. All rights reserved.
the Rédei symbol $[p_1, p_2, p_3]$ is defined as follows:

$$
[p_1, p_2, p_3] = \begin{cases} 
1 \cdots & 
\text{if } p_3 \text{ is completely decomposed in a certain } \\
D_8\text{-extension } K/\mathbb{Q}, \\
-1 \cdots & 
\text{otherwise.}
\end{cases}
$$

Here a $D_8$-extension means a Galois extension whose Galois group is the dihedral group of order 8. We will give the precise definition of the extension $K/\mathbb{Q}$ in §1. We note that all prime numbers ramified in $K/\mathbb{Q}$ are $p_1$ and $p_2$.

Although a meaning of the Rédei symbol had been obscure for a long time, in 2000, M. Morishita ([Mo1,2]) 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 analogues $\mu_2(12\cdots r) \in \mathbb{Z}/2\mathbb{Z}$ of Milnor’s link invariants (higher order linking numbers) for prime numbers $p_1, \cdots, p_r$ and showed

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

Now, as we shall see in §2, the analogy with knot theory suggests the following problem (conjecture):

**Problem.** Introduce the multiple residue symbol $[p_1, p_2, \ldots, p_r]$, which should be $(-1)^{\mu_2(12\cdots r)}$ and describe the decomposition law of $p_r$ in a certain

$\mathcal{N}_r(\mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & * & \cdots & * \\
0 & 1 & \cdots \\
\vdots & \ddots & \ddots \\
0 & \cdots & 0 & 1 \end{pmatrix} \in \mathbb{F}_2 \right\} - \text{extension } K/\mathbb{Q},$

unramified outside $p_1, \ldots, p_{r-1}$ and $\infty$. (Note that $\mathbb{Z}/2\mathbb{Z} = N_2(\mathbb{F}_2)$ and $D_8 = N_3(\mathbb{F}_2)$)

My main result is to solve the above problem for the case $r = 4$, namely, we shall
(1) construct concretely an $N_4(\mathbb{F}_2)$-extension $K/\mathbb{Q}$, and
(2) introduce the 4-th multiple residue symbol $[p_1, p_2, p_3, p_4]$ and prove

$$
[p_1, p_2, p_3, p_4] = (-1)^{\mu_2(1234)}.
$$
§1 Rédei’s $D_8$-extension and triple symbol

Let $p_1$ and $p_2$ be distinct prime numbers satisfying
\[ p_i \equiv 1 \pmod{4} \quad (i = 1, 2), \quad \left(\frac{p_i}{p_j}\right) = 1 \quad (1 \leq i \neq j \leq 2). \tag{1.1} \]

By (1.1), there are integers $x, y$ and $z$ satisfying
\[
\begin{cases}
  x^2 - p_1 y^2 - p_2 z^2 = 0. \\
  \gcd(x, y, z) = 1, \quad y \equiv 0 \pmod{2}, \quad x - y \equiv 1 \pmod{4}.
\end{cases}
\tag{1.2}
\]

We fix such a triple $a = (x, y, z)$ satisfying (1.2) and then set
\[ k_a := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha}), \quad \alpha = x + y\sqrt{p_1}. \]

The following theorem is due to L. Rédei.

**Theorem 1.3** ([R]). The extension $k_a/\mathbb{Q}$ is a $D_8$-extension where all ramified prime numbers are $p_1$ and $p_2$ with ramification index 2.

The fact that $k_a$ is independent of choice of $a = (x, y, z)$ was also shown in [R] in an obscure manner. We proved this fact clearly.

**Theorem 1.4** ([A1]). A field $k_a$ is independent of a choice of $a = (x, y, z)$, namely, depends only on a set $\{p_1, p_2\}$.

By Theorem 1.4, we denote $k_a$ by $k_{\{p_1, p_2\}}$ and call it the Rédei extension associated to $\{p_1, p_2\}$.

The following theorem of mine characterizes the Rédei extension by the information on the Galois group and ramification data.

**Theorem 1.5** ([A1]). Let $p_1$ and $p_2$ be prime numbers satisfying (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 $D_8$-extension over $\mathbb{Q}$ such that all prime numbers ramified in $K/\mathbb{Q}$ are $p_1$ and $p_2$ with ramification index 2.

Next, let $p_1, p_2$ and $p_3$ be distinct prime numbers satisfying
\[ p_i \equiv 1 \pmod{4} \quad (i = 1, 2, 3), \quad \left(\frac{p_i}{p_j}\right) = 1 \quad (1 \leq i \neq j \leq 3). \]
We then define the Rédei triple symbol \([p_1, p_2, p_3]\) by
\[
[p_1, p_2, p_3] = \begin{cases} 
1 \cdots & \text{if } p_3 \text{ is completely decomposed in } k(p_1, p_2)/\mathbb{Q}, \\
-1 \cdots & \text{otherwise.}
\end{cases}
\]

The following reciprocity law was shown by Rédei and we gave another simple proof.

**Theorem 1.6** ([R], [A1]). For any permutation \(i, j, k\) of \(1, 2, 3\), we have
\[
[p_1, p_2, p_3] = [p_i, p_j, p_k].
\]

§2 Milnor invariants

In this section, we recall the arithmetic Milnor invariants for primes, which are arithmetic analogues of Milnor invariants of a link, introduced by M. Morishita ([Mo1,2]). The underlying idea is based on the following analogies between knots and primes (cf. [Mo3]):

<table>
<thead>
<tr>
<th>knot (\mathcal{K} : S^1 \hookrightarrow \mathbb{R}^3)</th>
<th>prime (\text{Spec}(\mathbb{F}_p) \hookrightarrow \text{Spec}(\mathbb{Z}))</th>
</tr>
</thead>
<tbody>
<tr>
<td>link (\mathcal{L} = \mathcal{K}_1 \cup \cdots \cup \mathcal{K}_r)</td>
<td>finite set of primes (S = {p_1, \ldots, p_r})</td>
</tr>
<tr>
<td>link group (G_{\mathcal{L}} = \pi_1(\mathcal{X}_{\mathcal{L}}))</td>
<td>Galois group with restricted ramification (G_S = \pi_1^{\text{et}}(X_S) = \text{Gal}(\mathbb{Q}_S/\mathbb{Q}))</td>
</tr>
<tr>
<td></td>
<td>(\mathbb{Q}_S : \text{maximal extension over } \mathbb{Q})</td>
</tr>
<tr>
<td></td>
<td>unramified outside (S \cup {\infty})</td>
</tr>
</tbody>
</table>

### 2.1. Link case.

Let \(\mathcal{L} = \mathcal{K}_1 \cup \cdots \cup \mathcal{K}_r\) be an \(r\)-component link in \(\mathbb{R}^3\). Let \(\mathcal{X}_{\mathcal{L}} = \mathbb{R}^3 \setminus \mathcal{L}\) and \(G_{\mathcal{L}} := \pi_1(\mathcal{X}_{\mathcal{L}})\). Let \(F\) be the free group on the words \(x_1, \ldots, x_r\) where \(x_i\) represents a meridian of \(\mathcal{K}_i\). For a group \(G\), we let \(G^{(1)} := G, G^{(d+1)} := [G, G^{(d)}]\) \((d > 1)\). The following theorem is due to J. Milnor.

**Theorem 2.1.1** ([Mi2]). For each \(d \in \mathbb{N}\), 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 $K_j$ in $G_\mathcal{L}/G_\mathcal{L}^{(d)}$.

We define the Milnor numbers by

$$\mu(i_1 \cdots i_n j) := \epsilon \left( \frac{\partial^n y_j^{(d)}}{\partial x_{i_1} \cdots \partial x_{i_n}} \right),$$

where $\partial/\partial x_i : \mathbb{Z}[F] \to \mathbb{Z}[F]$ is the Fox derivative ([F]) and $\epsilon_{\mathbb{Z}[F]} : \mathbb{Z}[F] \to \mathbb{Z}$ is the augmentation map. Note that the right hand side is independent of $d$ for large enough $d$. We set $\mu(i) := 0$.

We have $\mu(ij) = \text{lk}(K_i, K_j)$ ($i \neq j$), the linking number of $K_i$ and $K_j$, and it can be shown that $\mu(I)$ is an invariant of a link $\mathcal{L}$ if $\mu(J) = 0$ for any $J$ with $|J| < |I|$.

**Example 2.1.2.** Let $\mathcal{L} = K_1 \cup K_2 \cup K_3$ be the following Borromean rings:

![Borromean rings](image)

Then $\mu(I) = 0$ if $|I| \leq 2$ and $\mu(123) = 1$. More generally, let $\mathcal{L} = K_1 \cup \cdots \cup K_r$ be the following link, called the Milnor link:

![Milnor link](image)

Then $\mu(I) = 0$ if $|I| \leq r - 1$ and $\mu(12 \cdots r) = 1$.

A meaning of Milnor invariants in covering spaces is given as follows.
Theorem 2.1.3 ([Mo3, 8.2], [Mu]). For $r \geq 2$, assume $\mu(J) = 0$ for any $J$ with $|J| < r$. Then there is a Galois covering $M \to S^3$ ramified over $\mathcal{K}_1 \cup \cdots \cup \mathcal{K}_{r-1}$ with Galois group

$$N_r(\mathbb{Z}) = \begin{pmatrix} 1 & Z & \cdots & Z \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & Z \\ 0 \cdots 0 & 1 \end{pmatrix}$$

such that $\mathcal{K}_r$ is completely decomposed in $M \to S^3$ if and only if $\mu(12\cdots r) = 0$.

This theorem suggests us to consider an $N_r(\mathbb{F}_2)$-extension in the arithmetic side as explained in §0.

2.2. Primes case. Let $S = \{p_1, \cdots, p_r\}$ be a set of $r$ distinct odd prime numbers. Let $X_S = \text{Spec}(\mathbb{Z}) \setminus S$ and $G_S(2)$ the maximal pro-2 quotient of $G_S := \pi^\text{ét}_1(\text{Spec}(X_S))$. Let $\hat{F}$ denote the free pro-2 group on the words $x_1, \ldots, x_r$ where $x_i$ represents a monodromy over $p_i$. The following theorem, which is due to H. Koch, may be regarded as an arithmetic analogue of Milnor’s Theorem 2.1.1.

Theorem 2.2.1 ([K]). We have

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

where $y_j \in \hat{F}$ is the pro-2 word representing a Frobenius auto. over $p_j$.

We then define the mod 2 Milnor numbers by

$$\mu_2(i_1 \cdots i_n j) := \hat{\epsilon} \left( \frac{\partial^n y_j}{\partial x_{i_1} \cdots \partial x_{i_n}} \right) \mod 2,$$

where $\partial/\partial x_i : \mathbb{Z}_2[[\hat{F}]] \to \mathbb{Z}_2[[\hat{F}]]$ is the pro-2 Fox derivative ([I], [O]) and $\hat{\epsilon} : \mathbb{Z}_2[[\hat{F}]] \to \mathbb{Z}_2$ is the augmentation map. We set $\mu_2(i) := 0$.

We have $(-1)^{\mu_2(ij)} = \left( \frac{p_i}{p_j} \right)$, and it can be shown that $\mu_2(I)$ is an invariant of $S$ if $\mu_2(J) = 0$ for any $J$ with $|J| < |I|$ and $2 \leq |I| \leq 2^{e_S}$ where $e_S := \max\{e \mid p_i \equiv 1 \mod 2^e \ (1 \leq i \leq r)\}$

Example 2.2.2 ([V]). Let $(p_1, p_2, p_3) = (13, 61, 937)$. Then we have $\mu_2(I) = 0$ if $|I| \leq 2$ and $\mu_2(123) = 1$. This triple of primes looks like Borromean rings in Example 2.1.2:
As in the link case, we have the following

**Theorem 2.2.3** ([Mo1,2]). For \(2 \leq r \leq 2^e\), assume \(\mu_2(J) = 0\) for any \(J\) with \(|J| < r\). Then there is a Galois extension \(K/\mathbb{Q}\) ramified over \(p_1, \cdots, p_{r-1}\) with Galois group

\[
N_r(\mathbb{F}_2) = \begin{pmatrix}
1 & \mathbb{F}_2 & \cdots & \mathbb{F}_2 \\
0 & 1 & \ddots & \\
\vdots & \ddots & \ddots & \mathbb{F}_2 \\
0 & \cdots & 0 & 1
\end{pmatrix}
\]

such that \(p_r\) is completely decomposed in \(K/\mathbb{Q}\) if and only if \(\mu_2(12\cdots r) = 0\).

For \(r = 2\) and \(3\), \(K\) is given by \(\mathbb{Q}(\sqrt{p_1})\) and the Rédei extension \(k_{\{p_1,p_2\}}\) associated to \(\{p_1, p_2\}\), respectively. In the next section, we give a concrete construction of \(K/\mathbb{Q}\) for \(r = 4\) and an arithmetic interpretation of \(\mu_2(1234)\).

**§3 \(N_4(\mathbb{F}_2)\)-extension and the 4-th multiple residue symbol**

Let \(p_1, p_2, p_3\) and \(p_4\) be distinct odd prime numbers satisfying

\[
\begin{cases}
p_i \equiv 1 \pmod{4} & (i = 1, 2, 3, 4), \quad \left(\frac{p_i}{p_j}\right) = 1 \quad (1 \leq i \neq j \leq 4), \\
[p_i, p_j, p_k] = 1 & (i, j, k : \text{distinct}).
\end{cases}
\]

(3.1)

Let \(k_{\{p_1,p_2\}} = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha})\) (resp. \(k_{\{p_3,p_2\}} = \mathbb{Q}(\sqrt{p_2}, \sqrt{p_3}, \sqrt{\beta})\)) be the Rédei extension associated to \(\{p_1, p_2\}\) (resp. \(\{p_3, p_2\}\)).

By (3.1), we have a non-trivial integral solution \((X, Y, Z)\) in \(\mathbb{Q}(\sqrt{p_1})\) satisfying

\[
X^2 - p_3 Y^2 - \alpha Z^2 = 0.
\]

We then let

\[
K := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{\alpha}, \sqrt{\beta}, \sqrt{\theta}) = k_{\{p_1,p_2\}}k_{\{p_3,p_2\}}(\sqrt{\theta}), \quad \theta := X + Y \sqrt{p_3}.
\]
Theorem 3.2 ([A2]). The extension $K/\mathbb{Q}$ is an $N_4(\mathbb{F}_2)$-extension unramified outside $p_1, p_2, p_3$ and $\infty$.

The proof of the assertion on the ramification is hard. For the details, we refer to [A2].

We define the 4-th multiple residue symbol by

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

Since $K \subset \mathbb{Q}_S$ for $S = \{p_1, p_2, p_3, p_4\}$ by Theorem 3.2, we can relate the Milnor invariant $\mu_2(1234)$ with our symbol $[p_1, p_2, p_3, p_4]$. As desired, we have the following.

Theorem 3.3 ([A2]). We have

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

For the proof, we use a group presentation of $N_4(\mathbb{F}_2)$ which Y. Mizusawa kindly computed using GAP.

Example 3.4. Let $(p_1, p_2, p_3, p_4) := (5, 8081, 101, 449)$. Then we have

$$k_{\{p_1, p_2\}} = \mathbb{Q}(\sqrt{5}, \sqrt{8081}, \sqrt{241 + 100\sqrt{5}}),$$
$$k_{\{p_3, p_2\}} = \mathbb{Q}(\sqrt{8081}, \sqrt{101}, \sqrt{1009 + 100\sqrt{101}}),$$
$$K = k_{\{p_1, p_2\}} \cdot k_{\{p_3, p_2\}}(\sqrt{25 + 2\sqrt{5} + 2\sqrt{101}}),$$

and

$$\left( \frac{p_i}{p_j} \right) = 1 \quad (1 \leq i \neq j \leq 4), \quad [p_i, p_j, p_k] = 1 \quad (i, j, k : \text{distinct}),$$
$$[p_1, p_2, p_3, p_4] = -1.$$
Finally, we note that we can show the shuffle relation for \([p_1, p_2, p_3, p_4]\) ([Mo3, 8.4]) and \([p_1, p_2, p_3, p_4] = [p_3, p_2, p_1, p_4] \).

References


