あるべき零拡大と多重べき剰余記号の数論に関する研究

天野, 郁弥

https://doi.org/10.15017/1470519

出版情報：Kyushu University, 2014, 博士（数理学）, 課程博士
バージョン：
権利関係：Fulltext available.

Arithmetic of certain nilpotent extensions and multiple residue symbols

Fumiya Amano

Gradute School of Mathematics
Kyushu University
September, 2014

Acknowledgments

I would like to express my sincere gratitude to my advisor, Professor Masanori Morishita for his advice and encouragement. I am indebted to Professor Yasushi Mizusawa for the computation of the group $N_4(\mathbb{F}_2)$ in Section 2.3 by GAP. I would also like to thank Professors Masanari Kida, Iwao Kimura, Hirotada Naito, Hiroaki Nakamura, Akito Nomura, Manabu Ozaki, Noriyuki Suwa, and Takao Yamazaki for their interests in my work and encouragements. Finally I would like to give my special thanks to my family for their patience, encouragement and support during my study at Kyushu University.

Notation

$\mathbb{Z}$	:	the ring of rational integers.
$\mathbb{Q}$	:	the field of rational numbers.
$\mathbb{C}$	:	the field of complex numbers.
		For a prime number p,
$\mathbb{F}_p$	:	the field of p elements.
$\mathbb{Z}_p$	:	the ring of p-adic integers.
$\mathbb{Q}_p$	:	the field of p-adic numbers.
$N_d(\mathbb{F}_p)$	:	the group of $d \times d$ uppertriangular unipotent matrices over $\mathbb{F}_p$.
$\mathcal{O}_k$	:	the ring of integers of a number field k.
$\mathrm{Gal}(K/F)$	:	the Galois group of a Galois extension K/F.
$\#S$	:	order of the finite set S.
$\pi_1(X)$	:	the fundamental group of a topological space X.
$\pi_1^{\text{ét}}(X)$	:	the étale fundamental group of a scheme X.

For a finite group G and a field F, we mean by a G-extension over F a Galois extension K/F whose Galois group $\mathrm{Gal}(K/F)$ is isomorphic to G.

Contents

Introduction

This thesis is concerned with arithmetic of multiple generalizations of quadratic residue symbols, called multiple residue symbols, which describe the prime decomposition law in (non-Abelian) nilpotent extensions of number fields. Such a symbol was firstly introduced by L. Rédei [Ré] in 1939. Aiming a generalization of the quadratic residue symbol and Gauss' genus theory, Rédei introduced his triple symbol $[p_1, p_2, p_3] \in \{\pm 1\}$ for certain prime numbers p_1, p_2, p_3 which describes the decomposition law of p_3 in a dihedral extension of degree 8, determined by p_1 and p_2, over the rationals $\mathbb{Q}$. It seemed, however, unclear why such a dihedral extension could be a natural object to generalize quadratic fields.

After a long silence, in 2000, M. Morishita [Mo1] interpreted the Rédei triple symbol as an arithmetic analogue of triple linking number in topology. In fact, he introduced arithmetic analogue, $\mu_2(12\cdots n) \in \mathbb{Z}/2\mathbb{Z}$, of Milnor's higher linking number for numbers $p_1, \ldots, p_n$, and showed that the arithmetic Milnor invariant $\mu_2(12\cdots n)$ describes the decomposition law of p_n in a nilpotent extension K_n over $\mathbb{Q}$, where the Galois group $\mathrm{Gal}(K_n/\mathbb{Q})$ is isomorphic to the group $N_n(\mathbb{F}_2)$ of n by n uppertriangular unipotent matrices over $\mathbb{F}_2$ and ramified primes in $K_n/\mathbb{Q}$ are only $p_1, \ldots, p_{n-1}$. The quadratic residue symbol $\left(\frac{p_2}{p_1}\right)$ and the Rédei symbol $[p_1, p_2, p_3]$ are proved to be $(-1)^{\mu_2(12)}$ and $(-1)^{\mu_2(123)}$, respectively. (Note that $N_2(\mathbb{F}_2) = \mathbb{Z}/2\mathbb{Z}$ and $N_3(\mathbb{F}_2)$ is the dihedral group of degree 8.) Although Morishita's work tells us a conceptual meaning of multiple residue symbols, it does not tell us an effective way to compute them. For example, even a question such as whether K_3 coincides with Rédei's dihedral extension remained unsolved. So, a really number-theoretic problem is to construct the nilpotent extensions $K_n/\mathbb{Q}$ concretely and characterize them.

Here are our main results in this thesis. We first give an arithmetic characterization of Rédei's dihedral extension over $\mathbb{Q}$, which implies that the field K_3 coincides with Rédei's. Next we construct concretely an $N_4(\mathbb{F}_2)$-extension K over $\mathbb{Q}$ where ramified primes are p_1, p_2, p_3, 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 $K/\mathbb{Q}$. We then show the relation of our symbol and the 4-th arithmetic Milnor invariant. We also give an analytic expression of the Rédei symbol in terms of a Fourier coefficient of a modular form of weight one. Finally we construct concretely an $N_3(\mathbb{F}_3)$-extension over $\mathbb{Q}(\sqrt{-3})$ and introduce a triple cubic residue symbol for certain prime ideals in $\mathbb{Q}(\sqrt{-3})$.

Now we describe the contents of this thesis in more detail.

In Chapter 1, we study arithmetic of Rédei's dihedral extension and triple symbol. In Section 1.1, we recall the construction and properties of Rédei's dihedral extensions. In Section 1.2, we give an arithmetic characterization of Rédei's dihedral extension (Theorem 1.2.1). In Section 1.3, we introduce the Rédei triple symbol and give another simple proof of the triple reciprocity law.

In Chapter 2, we introduce the 4-th multiple residue symbol $[p_1, p_2, p_3, p_4]$ for certain prime number p_i's. For this, we construct concretely a certain $N_4(\mathbb{F}_2)$-extension over $\mathbb{Q}$. In Section 2.1 and 2.2, we recall Milnor invariants of a link and for a set of odd prime numbers. In Section 2.3, we construct concretely an $N_4(\mathbb{F}_2)$-extension $K/\mathbb{Q}$, where ramified prime numbers are p_1, p_2 and p_3 (Definition 2.3.7, Theorem 2.3.8, Theorem 2.3.9). In Section 2.4, we introduce the 4-th multiple residue symbol $[p_1, p_2, p_3, p_4]$ which describes the decomposition law of p_4 in $K/\mathbb{Q}$, and show the relation of our symbol $[p_1, p_2, p_3, p_4]$ and the 4-th Milnor invariant $\mu_2(1234)$ by proving $[p_1, p_2, p_3, p_4] = (-1)^{\mu_2(1234)}$ (Theorem 2.4.5).

In Chapter 3, we consider Rédei's dihedral extension K which contains an imaginary quadratic field $k = \mathbb{Q}(\sqrt{-p_1p_2})$, and give an analytic expression of the Rédei triple symbol $[-p_1, p_2, p_3]$ in terms of a Fourier coefficient of a modular form of weight one. In Section 3.1, we recall Rédei's dihedral extension K containing an imaginary quadratic field k above and triple symbol $[-p_1, p_2, p_3]$. In Section 3.2, we interpret $[-p_1, p_2, p_3]$ using the Arith L-function $L(\rho, s)$ associated to a 2-dimensional representation of $\mathrm{Gal}(K/\mathbb{Q})$. In Section 3.2, 3.4, we express $L(\rho, s)$ as the L-function of a modular form associated to binary quadratic forms corresponding to ideal classes of k. In particular, the Rédei symbol $[-p_1, p_2, p_3]$ is expressed as a Fourier coefficient of the modular form.

In Chapter 4, we introduce a triple cubic residue symbol $[\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3]_3 \in \{1, \omega, \omega^2\}$, where $\mathfrak{p}_i$'s are certain prime ideals of $\mathbb{Q}(\sqrt{-3})$ and $\omega = \frac{-1+\sqrt{-3}}{2}$ denotes a primitive cubic root of unity. For this, we construct concretely an $N_3(\mathbb{F}_3)$-extension of $\mathbb{Q}(\sqrt{-3})$ where ramified primes are $\mathfrak{p}_1$ and $\mathfrak{p}_2$.

Chapter 1

Rédei's dihedral extension and triple reciprocity law

In this chapter, we study arithmetic of certain dihedral extensions over $\mathbb{Q}$ and triple symbols introduced by L. Rédei in 1939.

In Section 1.1, we recall the construction and some properties of Rédei's dihedral extensions. In Section 1.2, we give an arithmetic characterization of Rédei's dihedral extension. In Section 1.3, we introduce the Rédei triple symbol and give another simple proof of the triple reciprocity law.

1.1 Rédei's dihedral extensions and its uniqueness

In this section, we recall the construction of Rédei's dihedral extension ([Ré]). Since Rédei's account ([Ré]) 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 numbers satisfying the condition

$$p_1, p_2 \equiv 1 \bmod 4, \ \left(\frac{p_1}{p_2}\right) = \left(\frac{p_2}{p_1}\right) = 1. \tag{1.1.1}$$

We set $k_i = \mathbb{Q}(\sqrt{p_i})$ $(i = 1, 2)$.

Lemma 1.1.2. *There are integers x, y, z satisfying the following conditions*:
(1) $x^2 - p_1 y^2 - p_2 z^2 = 0$,
(2) 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 $\left(\frac{p_1}{p_2}\right) = 1$, p_2 is decomposed in k_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 ([On]) and hence $\mathfrak{p}^c = (\alpha)$ for some $\alpha = \frac{s+t\sqrt{p_1}}{2} \in \mathcal{O}_{k_1}, s, t \in \mathbb{Z}, s \equiv t \pmod 2$. Since $\mathrm{N}((\alpha)) = \mathrm{N}\mathfrak{p}^c = p_2^c$, $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha) = \frac{s^2-p_1t^2}{4} = \pm p_2^c$. Since $p_1 \equiv 1 \pmod 4$, there is a unit $\epsilon \in \mathcal{O}_{k_1}^\times$ such that $\mathrm{N}_{k_1/\mathbb{Q}}(\epsilon) = -1$ and so we may assume $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha) = p_2^c$.
(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 $x, y, z \in \mathbb{Z}$ 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

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

where we put $x = \frac{s(s^2+3t^2p_1)}{8}$ and $y = \frac{t(3s^2+t^2p_1)}{8}$. Therefore $x^2 - p_1y^2 = \mathrm{N}_{k_1/\mathbb{Q}}(\alpha^3) = p_2^{3c}$, $z = p_2^{(3c-1)/2}$. 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 1.1.2. We let $\alpha = x + y\sqrt{p_1}$ and set

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

Firstly, we have the following theorem due to Rédei ([Ré]). (1) can be easily proved and (2) can also be proved using the well-known Lemma 1.1.3 below on the ramification in a Kummer extension.

Lemma 1.1.3 ([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 L/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* L/F.

Theorem 1.1.4 ([Ré]). (1) *The extension* $K_{\boldsymbol{a}}/\mathbb{Q}$ *is a Galois extension whose Galois group is the dihedral group* D_8 *of order* 8.
(2) *All prime numbers ramified in* $K_{\boldsymbol{a}}/\mathbb{Q}$ *are only* p_1 *and* p_2 *with ramification index* 2.

Proof. (1) Let K_f be the splitting field over $\mathbb{Q}$ of $f(T) := T^4 - 2xT^2 + p_2z^2 = (T - \sqrt{\alpha})(T + \sqrt{\alpha})(T - \sqrt{\overline{\alpha}})(T + \sqrt{\overline{\alpha}}) \in \mathbb{Z}[T]$, where $\overline{\alpha} := x - y\sqrt{p_1}$. Since $\alpha^2 = x + y\sqrt{p_1}$ and $\sqrt{\alpha}\sqrt{\overline{\alpha}} = z\sqrt{p_2}$, we have $K_{\boldsymbol{a}} = K_f$ and so $K_{\boldsymbol{a}}$ is a Galois extension over $\mathbb{Q}$. Define $s, t \in \mathrm{Gal}(K_{\boldsymbol{a}}/\mathbb{Q})$ by

$$\begin{array}{lll} s(\sqrt{p_1}) = \sqrt{p_1}, & s(\sqrt{p_2}) = -\sqrt{p_2}, & s(\sqrt{\alpha}) = \sqrt{\alpha}, \\ t(\sqrt{p_1}) = -\sqrt{p_1}, & t(\sqrt{p_2}) = -\sqrt{p_2}, & t(\sqrt{\alpha}) = -\sqrt{\overline{\alpha}}. \end{array}$$

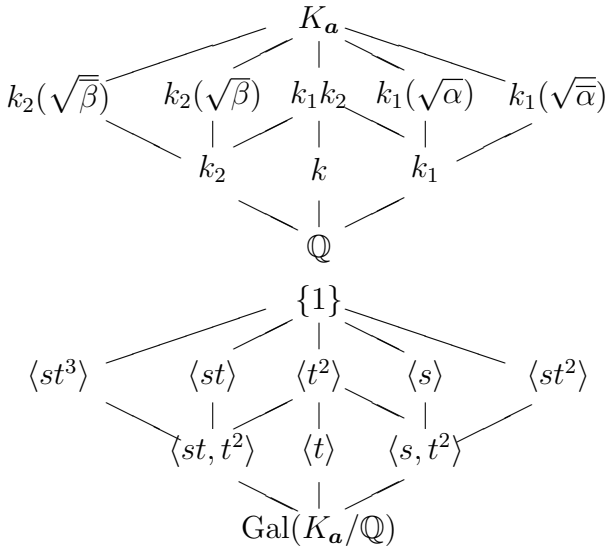
Then we easily see that

$$s^2 = t^4 = 1,\ sts = t^{-1}$$

and so s, t generate the dihedral group D_8 of order 8. Since it is easy to see $[K_{\boldsymbol{a}} : \mathbb{Q}] = 8$, we conclude $\mathrm{Gal}(K_{\boldsymbol{a}}/\mathbb{Q}) = D_8$.

Putting $\beta := (\sqrt{\alpha} + \sqrt{\overline{\alpha}})^2 = 2(x + z\sqrt{p_2})$, all subfields of $K_{\boldsymbol{a}}/\mathbb{Q}$ and the corresponding subgroups of $\mathrm{Gal}(K_{\boldsymbol{a}}/\mathbb{Q})$ are illustrated as follows.

(1.1.4.1)



(2) By the condition (1.1.1), p_i is the only ramified prime number in $k_i/\mathbb{Q}$ $(i = 1, 2)$ and that p_1 (resp. p_2) splits in $k_2/\mathbb{Q}$ (resp. $k_1/\mathbb{Q}$). So, looking at the diagram (1.1.4.1), it suffices to show that the only one prime of k_1 lying over

p_2 is ramified in $k_1(\sqrt{\alpha})/k_1$. First we note that $\lambda := (1+\sqrt{\alpha})/2 \in \mathcal{O}_{k_1(\sqrt{\alpha})}$, since λ satisfies $\lambda^2 + \lambda + (1-\alpha)/4 = 0$ and $(1-\alpha)/4 \in \mathcal{O}_{k_1}$ by $x - y \equiv 1 \mod 4$. Since the relative discriminant of λ in $k_1(\sqrt{\alpha})/k_1$ is

$$d(\lambda, k_1(\sqrt{\alpha})/k_1) = \begin{vmatrix} 1 & \lambda \\ 1 & \overline{\lambda} \end{vmatrix}^2 = \alpha$$

where $\lambda := (1-\sqrt{\alpha})/2$, and (α) is prime to 2, any prime of k_1 lying over 2 is unramified in $k_1(\sqrt{\alpha})/k_1$. Next let

$$(\alpha) = \mathfrak{p}^e \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

be the decomposition of (α) into the product of positive powers of distinct prime ideals $\mathfrak{p}, \mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of $\mathcal{O}_{k_1}$. Since $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha) = p_2 z^2$, we can take $\mathfrak{p}$ to be one of primes lying over p_2 and e to be odd. We claim that all e_i's are even. Suppose that there is an odd e_j. Let q_j be the prime number lying below $\mathfrak{q}_j$. If (q_j) splits to $\mathfrak{q}_j\overline{\mathfrak{q}_j}$ in k_1, we have $\alpha \in \overline{\mathfrak{q}_j}$ by $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha) = p_2 z^2$. Then $\alpha, \overline{\alpha} \in \mathfrak{q}_j\overline{\mathfrak{q}_j} = (q_j)$ and so $2x, 2y \in (q_j)$. This contradicts $(x, y, z) = 1$. If q_j is inert in $k_1/\mathbb{Q}$, $\alpha, \overline{\alpha} \in (q_j)$ and so $2x, 2y \in (q_j)$ again, which is a contradiction. If $(q_j) = \mathfrak{q}_j^2$ in k_1, q_j must be p_1. So $\mathrm{N}\mathfrak{q}^{e_j} = p_1^{e_j}$, which contradicts $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha) = p_2 z^2$. Thus we have the decomposition

$$(\alpha) = \mathfrak{p}^e \mathfrak{a}^2, \ \ (\mathfrak{p}, \mathfrak{a}) = 1, \ e \text{ is odd.}$$

By the ramification theory in a Kummer extension (Lemma 1.1.3, [Fu, Ch.4, Theorem 2.1, Lemma 2.1]), $\mathfrak{p}$ is the unique prime ideal of $\mathcal{O}_{k_1}$ which is ramified in $k_1(\sqrt{\alpha})/k_1$. □

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

Proposition 1.1.5. *Let θ be an algebraic integer in k_1 satisfying the following conditions*:
(1) $\mathrm{N}_{k_1/\mathbb{Q}}(\theta) = p_2 h^2$ *for some* $h \in \mathbb{Z} \setminus \{0\}$.
(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 1.1.5. 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 ([On]). Therefore $k_1(\sqrt{\theta/\theta'}) = k_1$, hence $k_1(\sqrt{\theta}) = k_1(\sqrt{\theta'})$. □

Corollary 1.1.6. *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 1.1.2. We let $\alpha' = x + y\sqrt{p_1}$ and $\overline{\alpha'} = x - y\sqrt{p_1}$. By Theorem 1.1.4, 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 1.1.5, $k_1(\sqrt{\alpha}) = k_1(\sqrt{\alpha'})$ 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 1.1.6, 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 1.1.7. *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 1.1.2 so that

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

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

$\mathrm{N}_{k_1/\mathbb{Q}}(\alpha_1) = (2x_2)^2 - p_1(2z_2)^2 = p_2(2y_2)^2$,

$d(k_1(\sqrt{\alpha})/k_1) = d(k_1(\sqrt{\alpha_1})/k_1)$ or $d(k_1(\overline{\alpha_1})/k_1)$.

Therefore, by Proposition 1.1.5, $k_1(\sqrt{\alpha}) = k_1(\sqrt{\alpha_1})$ or $k_1(\sqrt{\overline{\alpha_1}})$. Hence we have

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

□

Definition 1.1.8. By Theorem 1.1.7, we denote by $K_{\{p_1,p_2\}}$ the field $K_{(p_1,p_2)}$ and call the extension $K_{\{p_1,p_2\}}/\mathbb{Q}$ the *Rédei extension* associated to a set $\{p_1, p_2\}$ satisfying and $p_1, p_2 \equiv 1 \pmod 4$ and $\left(\frac{p_2}{p_1}\right) = \left(\frac{p_1}{p_2}\right) = 1$.

1.2 A characterization of the Rédei extension

We keep the same notation as in Section 1.1. Here is our main theorem.

Theorem 1.2.1. *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 $\mathbb{Q}$ such that prime numbers ramified in $K/\mathbb{Q}$ are only p_1 and p_2 with ramification index 2.*

Proof. (1) $\Rightarrow$ (2) is nothing but Rédei's theorem (Theorem 1.1.4). Therefore it suffice to show (2) $\Rightarrow$ (1). Let $k_i = \mathbb{Q}(\sqrt{p_i})$ $(i = 1, 2)$ and $k_{12} = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$. First, we show that $k_{12} \subset K$. Since $\mathrm{Gal}(K/\mathbb{Q}) = D_8$ contains three distinct subgroups of index 2, there are three distinct quadratic subextensions in $K/\mathbb{Q}$ by Galois theory. Since all prime numbers ramified in $K/\mathbb{Q}$ are only p_1 and p_2, these three quadratic extensions must be k_1, k_2 and $\mathbb{Q}(\sqrt{p_1p_2})$. 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 $\alpha = x + y\sqrt{p_1} \in k_1 (x, y \in \mathbb{Z})$ such that $L = k_1(\sqrt{\alpha})$ and $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha})$. By the assumption $\left(\frac{p_1}{p_2}\right) = 1$, p_2 is decomposed into two prime ideals, say $\mathfrak{p}_1$ and $\mathfrak{p}_2$, in k_1. Then, by Lemma 1.1.3 and the assumption that all of prime numbers ramified in $K/\mathbb{Q}$ 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

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

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

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

Since $b \in \mathbb{Z}$, $\sqrt{p_2} \in K$, we have $\sqrt{-1} \in K$, which implies that 2 is ramified in $K/\mathbb{Q}$. This contradicts to the assumption (2). Therefore $x^2 - p_1y^2 = p_2^{a_1+a_2}b^2$. Let us define $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ 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 $\sigma(\sqrt{\overline{\alpha}}) = -\sqrt{\overline{\alpha}}$. 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

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

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 1.1.3, we have $d(k_1(\sqrt{\alpha})/k_1) = \mathfrak{p}_1$ or $\mathfrak{p}_2$. Therefore, by Proposition 1.1.5, $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha})$ is a Rédei extension. □

Remark 1.2.2. (1) The assumption on the ramification indexes of p_1 and p_2 are necessary. For example, let $K = \mathbb{Q}(\sqrt{5}, \sqrt{101}, \sqrt{-35 - 12\sqrt{5}})$. Then, $K/\mathbb{Q}$ is not a Rédei extension, although K is a dihedral extension over $\mathbb{Q}$ 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 $K_{\{p_1,p_2\}}/\mathbb{Q}$ is described in terms of the class number h and the narrow class number h^+ of $\mathbb{Q}(\sqrt{p_1p_2})$. In fact, since the cyclic extension $K_{\{p_1,p_2\}}/\mathbb{Q}(\sqrt{p_1p_2})$ is unramified at all finite primes, genus theory tells the 2-part of the narrow ideal class group of $\mathbb{Q}(\sqrt{p_1p_2})$ 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 $K_{\{p_1,p_2\}}/\mathbb{Q}$, and if $h^+ = 2h$ and $h \not\equiv 0 \pmod 4$, the infinite prime are ramified in $K_{\{p_1,p_2\}}/\mathbb{Q}$.

1.3 A proof of the reciprocity law of the Rédei 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 1.3.1. We define the *Rédei triple symbol* by

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

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

Theorem 1.3.2 ([Ré])**.** *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 1.1.7, we have immediately the following:

Theorem 1.3.3. $[p_1, p_2, p_3] = [p_2, p_1, p_3]$.

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 1.3.2, it suffices to prove the following:

Theorem 1.3.4. $[p_1, p_2, p_3] = [p_1, p_3, p_2]$.

In the following we prove Theorem 1.3.4.

Let us write k for $k_1 = \mathbb{Q}(\sqrt{p_1})$ 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 1.1.2 with respect to the pair (p_1, p_2) (resp. (p_1, p_3)) such that

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

Since $\mathfrak{p}_3$ is unramified in $k(\sqrt{\alpha})/k$ by Theorem 1.1.4 (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 $\left(\frac{\cdot}{\mathfrak{p}}\right)$ 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 1.3.5. *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 1.3.4 goes as follows: By Lemma 1.3.5 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 $k/\mathbb{Q}$ and that $\alpha, \beta \in U_{\mathfrak{P}}^{(2)} = 1 + \mathfrak{P}^2$ by the condition (2) of Lemma 1.1.2, we have find $\left(\frac{\alpha, \beta}{\mathfrak{P}} \right) = 1$ ([FV]). This completes the proof of Theorem 1.3.4.

Chapter 2

Certain $N_4(\mathbb{F}_2)$-extensions over $\mathbb{Q}$ and the 4-th multiple residue symbols

In this chapter, we introduce the 4-th multiple residue symbol $[p_1, p_2, p_3, p_4] \in \{\pm 1\}$ 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 Chapter 1. For this, we construct concretely a certain nilpotent extension over $\mathbb{Q}$ of degree 64.

In Section 2.1 and 2.2, we recall Milnor invariants of a link and, following the analogies between knots and primes, introduce arithmetic Milnor invariants for certain prime numbers. In Section 2.3 we construct concretely a certain nilpotent extension K over $\mathbb{Q}$ of degree 64, where ramified prime numbers are p_1, p_2 and p_3. Then in Section 2.4, we introduce the 4-th multiple residue symbol $[p_1, p_2, p_3, p_4]$ which describes the decomposition law of p_4 in the extension $K/\mathbb{Q}$. Finally we show the relation of our symbol $[p_1, p_2, p_3, p_4]$ and the 4-th arithmetic Milnor invariant $\mu_2(1234)$ by proving $[p_1, p_2, p_3, p_4] = (-1)^{\mu_2(1234)}$.

2.1 Milnor invariants of a link.

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 Chapter 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 $\mathcal{K} : S^1 \hookrightarrow \mathbb{R}^3$	prime $\mathrm{Spec}(\mathbb{F}_p) \hookrightarrow \mathrm{Spec}(\mathbb{Z})$
link $\mathcal{L} = \mathcal{K}_1 \cup \cdots \cup \mathcal{K}_r$	finite set of primes $S = \{p_1, \ldots, p_r\}$
$X_{\mathcal{L}} = \mathbb{R}^3 \setminus \mathcal{L}$	$X_S = \mathrm{Spec}(\mathbb{Z}) \setminus S$
link group $G_{\mathcal{L}} = \pi_1(X_{\mathcal{L}})$	Galois group with restricted ramification $G_S = \pi_1^{\text{ét}}(X_S) = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ $\mathbb{Q}_S$: maximal extension over $\mathbb{Q}$ 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 $\mathbb{Q}$ unramified outside $p_1, \ldots, p_{n-1}$ and ∞ (∞ being the infinite prime).

Let $\mathcal{L} = \mathcal{K}_1 \cup \cdots \cup \mathcal{K}_r$ be a link with r components in $\mathbb{R}^3$ and let $X_{\mathcal{L}} = \mathbb{R}^3 \setminus \mathcal{L}$ 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 $d \in \mathbb{N}$, 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 $\mathcal{K}_j$ in $G_{\mathcal{L}}/G_{\mathcal{L}}^{(d)}$.

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

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

be the Magnus homomorphism defined by

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

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

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

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

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

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

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 $\mathbb{Z}$ 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

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

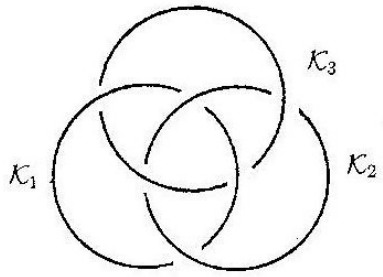
The fundamental results, due to Milnor, are as follows.

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*

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

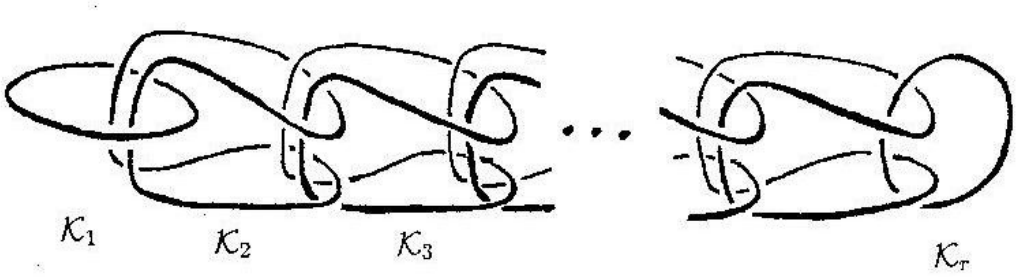
where $\mathrm{PSh}(I, J)$ *stands for the set of results of proper shuffles of I and J* (cf. [CFL]).
(4) (Cyclic symmetry). $\overline{\mu}(i_1 \cdots i_n) = \overline{\mu}(i_2 \cdots i_n i_1) = \cdots = \overline{\mu}(i_n i_1 \cdots i_{n-1})$

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 $\mu(I) \in \mathbb{Z}$ 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 $\mu(I) \in \mathbb{Z}$ 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 $\rho_I : F \to N_n(\mathbb{Z}/\Delta(I))$ by

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

where we set $\epsilon = \epsilon_{\mathbb{Z}[F]}$ for simplicity. It can be shown by the property of the Fox derivative that ρ_I is a homomorphism.

Theorem 2.1.4 ([Mo4, Theorem 8.8], [Mu]). (1) *The homomorphism ρ_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 $\mathrm{Gal}(X_I/X_{\mathcal{L}}) = N_n(\mathbb{Z}/\Delta(I))$. 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 β_{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 Arithmetic Milnor invariants for prime numbers.

Let $S = \{p_1, \cdots, p_r\}$ be a set of r distinct odd prime numbers and let $G_S := \pi_1^{\text{ét}}(\mathrm{Spec}(\mathbb{Z}) \setminus S)$. 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 $\mathbb{Q}_S(2)$ over $\mathbb{Q}$ which is unramified outside $S \cup \{\infty\}$. Here we fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ containing $\mathbb{Q}_S(2)$. We also fix an algebraic closure $\overline{\mathbb{Q}}_{p_i}$ of $\mathbb{Q}_{p_i}$ and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{p_i}$ for each i. Let $\mathbb{Q}_{p_i}(2)$ be the maximal pro-2 extension of $\mathbb{Q}_{p_i}$ contained in $\overline{\mathbb{Q}}_{p_i}$. Then we have

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

where $\zeta_{2^n} \in \overline{\mathbb{Q}}$ 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 $\mathrm{Gal}(\mathbb{Q}_{p_i}(2)/\mathbb{Q}_{p_i})$ is then topologically generated by the monodromy τ_i and the extension of the Frobenius automorphism σ_i defined by

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

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

The embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{p_i}$ induces the embedding $\mathbb{Q}_S(2) \hookrightarrow \mathbb{Q}_{p_i}(2)$ and hence the homomorphism $\eta_i : \mathrm{Gal}(\mathbb{Q}_{p_i}(2)/\mathbb{Q}_{p_i}) \to G_S$. We denote by the same τ_i, σ_i the images of τ_i, σ_i under η_i. Let $\hat{F}$ denote the free pro-2 group on the words $x_1, \ldots, x_r$ where x_i represents τ_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 σ_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 $\mathbb{Z}_2\langle\langle X_1, \ldots, X_r \rangle\rangle$ be the algebra of non-commutative formal power series of variables $X_1, \ldots, X_r$ over $\mathbb{Z}_2$, the ring of 2-adic integers, and let

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

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

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

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

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

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

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 $\mathbb{Z}/m\mathbb{Z}$ 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* ζ_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* $\mathbb{Q}_{p_i}$*.*
(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* $1 \leq i \leq n$*,*

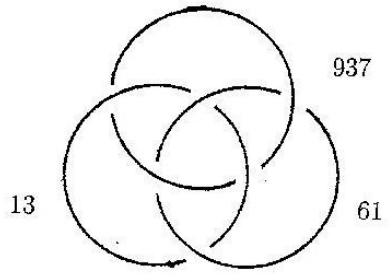
$$\sum_{H \in \mathrm{PSh}(I,J)} \overline{\mu}_m(Hi) \equiv 0 \mod \text{g.c.d}\{\Delta(Hi) \mid H \in \mathrm{PSh}(I,J)\}.$$

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 $\overline{\mu}_2(I) = \mu_2(I) \in \mathbb{Z}/2\mathbb{Z}$. 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 $\Delta_m(I) \neq \mathbb{Z}/m\mathbb{Z}$. We define the map $\rho_{(m,I)} : \hat{F} \to N_n((\mathbb{Z}/m\mathbb{Z})/\Delta_m(I))$ by

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

where we set $\epsilon(\alpha)_m = \epsilon_{\mathbb{Z}[[\hat{F}]]}(\alpha) \bmod m$ for $\alpha \in \mathbb{Z}_l[[\hat{F}(l)]]$. 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 $i_1, \cdots, i_{n-1}$ are all distinct.*
(2) *Suppose that $i_1, \ldots, i_{n-1}$ are all distinct. Let $K_{(m,I)}$ be the extension over $\mathbb{Q}$ corresponding to* $\mathrm{Ker}(\rho_{(m,I)})$*. Then $K_{(m,I)}/\mathbb{Q}$ is a Galois extension unramified outside $p_{i_1}, \ldots, p_{i_{n-1}}$ and ∞ with Galois group* $\mathrm{Gal}(K_{(m,I)}/\mathbb{Q}) = N_n((\mathbb{Z}/m\mathbb{Z})/\Delta_m(I))$*. For a Frobenius automorphism σ_{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:

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

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

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

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

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

Theorem 2.2.5 suggests a problem to construct concretely a Galois extension $K_n/\mathbb{Q}$ unramified outside $p_1, \ldots, p_{n-1}$ and ∞ with Galois group $N_n(\mathbb{F}_2)$ 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 $K_n/\mathbb{Q}$ and coincide with $(-1)^{\mu_2(12\cdots n)}$. In the next section, we solve this problem for the case $n = 4$.

2.3 Construction of a certain $N_4(\mathbb{F}_2)$-extension.

In this section, under certain conditions on three prime numbers p_1, p_2, p_3, we construct concretely a Galois extension K over $\mathbb{Q}$ where all ramified prime numbers are p_1, p_2 and p_3 and the Galois group is $N_4(\mathbb{F}_2)$, 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 $K/\mathbb{Q}$. 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 section 2.2. We keep the same notations as in the previous sections.

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

$$\text{(2.3.1)} \qquad \begin{cases} p_i \equiv 1 \pmod 4\ (i = 1, 2, 3),\ \left(\dfrac{p_i}{p_j}\right) = 1\ (1 \le i \ne j \le 3), \\ [p_i, p_j, p_k] = 1\ (\{i, j, k\} = \{1, 2, 3\}). \end{cases}$$

We let

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

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

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

In the following, we fix such an α once and for all.

For a prime $\mathfrak{p}$ of k, we denote by $\left(\frac{\ ,\ }{\mathfrak{p}}\right)$ 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 2.3.2. *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, ∞: 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 π 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

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

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 ϖ 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 $(2) = \mathfrak{p} \cdot \mathfrak{p}'$ $(\mathfrak{p} \neq \mathfrak{p}')$, $k_{\mathfrak{p}} = k_{\mathfrak{p}'} = \mathbb{Q}_2$ 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 2.3.3. *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 2.3.2, we have $\alpha \in \mathrm{N}_{k_{\mathfrak{p}}(\sqrt{p_3})/k_{\mathfrak{p}}}(k_{\mathfrak{p}}(\sqrt{p_3})^{\times})$ 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 $k_{13} = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_3})$, let U be the unit group of $\mathcal{O}_{k_{13}}/(4)$ and $U(2)$ the 2-Sylow subgroup of U. Similarly, let $k'_{13} := \mathbb{Q}(\sqrt{p_1}, \sqrt{\alpha})$ and define $U' := (\mathcal{O}_{k'_{13}}/(4))^{\times}$ and $U'(2)$ to be the 2-Sylow subgroup of U'.

Lemma 2.3.4. *The group $U(2)$ is given by*

$$\begin{aligned}U(2) &= \langle -1 \rangle \times \langle \sqrt{p_1} \rangle \times \langle \sqrt{p_3} \rangle \times \left\langle \frac{3 + \sqrt{p_1} + \sqrt{p_3} + \sqrt{p_1p_3}}{2} \right\rangle \\ &\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.\end{aligned}$$

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

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

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

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

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 $\mathrm{N}_{k_{13}/\mathbb{Q}}$, we obtain

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

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 α, the assertion for $U'(2)$ can be shown similarly. □

Lemma 2.3.5. *Assume $p_1 \equiv 5 \pmod 8$. Then there is a unit $\epsilon \in \mathcal{O}_k^\times$ of the form $\epsilon = s + t\sqrt{p_1}, s, t \in \mathbb{Z}, s \equiv 0, t \equiv 1 \pmod 2$. Such a unit ϵ satisfies $\epsilon \equiv \pm\sqrt{p_1} \mod (4)$ in $U(2)$ and $U'(2)$.*

Proof. Since $p_1 \equiv 1 \pmod 4$, the fundamental unit $\epsilon_1 = \frac{s_1 + t_1\sqrt{p_1}}{2}$ ($s_1 \equiv t_1 \pmod 2$) of k satisfies $\mathrm{N}_{k/\mathbb{Q}}(\epsilon_1) = -1$. If $s_1 \equiv t_1 \equiv 0 \pmod 2$, we let $\epsilon := \epsilon_1 = s + t\sqrt{p_1}$, $s := s_1/2, t := t_1/2 \in \mathbb{Z}$, where we have $s \equiv 0, t \equiv 1 \pmod 2$, since $s^2 - p_1t^2 = -1$. Since $\epsilon = s + t\sqrt{p_1} = s + s\sqrt{p_1} + (t - s)\sqrt{p_1}$ and $s + s\sqrt{p_1} \in 4\mathcal{O}_{k_{13}}$, $\epsilon \equiv \pm\sqrt{p_1} \mod (4)$. 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

$$\epsilon_1^3 = \frac{s_1(s_1^2 + 3p_1t_1^2) + t_1(3s_1^2 + p_1t_1^2)\sqrt{p_1}}{8} = s + t\sqrt{p_1},$$

where $s = s_1(s_1^2 + 3p_1t_1^2)/8, t = t_1(3s_1^2 + t_1^2)/8 \in \mathbb{Z}$. Since $\mathrm{N}_{k/\mathbb{Q}}(\epsilon_1^3) = -1$, $\epsilon = \epsilon_1^3$ satisfies the desired conditions. □

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

Theorem 2.3.6. *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 2.3.3, 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 2.3.4, $\frac{n}{2} \not\equiv 0 \pmod 2$ and $\overline{\theta}^{\frac{n}{2}} \in U(2)$. Write $\theta^{\frac{n}{2}} = b_1 + b_2\sqrt{p_1} + b_3\sqrt{p_3} + b_4\sqrt{p_1p_3}$, $b_i \in \mathbb{Q}$. Since $\mathrm{N}_{k_{13}/k}(\theta) = X^2 - p_3Y^2 = \alpha Z^2$, $\mathrm{N}_{k_{13}/k}(\theta^{\frac{n}{2}}) = (\alpha Z^2)^{\frac{n}{2}}$. 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 2.3.4, $\theta^{\frac{n}{2}} \equiv \pm\sqrt{p_3}$, $\pm\sqrt{p_1p_3}$ 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 2.3.5, there is $\epsilon \in \mathcal{O}_k^\times$ such that $\epsilon\theta^{\frac{n}{2}} \equiv 1 \mod (4)$ and $\epsilon^2 \equiv 1 \mod (4)$. Replacing (X, Y, Z) by $(\epsilon X, \epsilon Y, \epsilon Z)$, (1), (2) holds obviously, and (3) is also satisfied because $\epsilon\theta \mod (4)$ has the order $\frac{n}{2} \not\equiv 0 \pmod 2$.

Case $(Y, 2) = 1$: Let $\theta' := X + Z\sqrt{\alpha}$. Replacing θ by θ' and p_3 by α, the above proof works well by using Lemma 2.3.4. □

Let $\boldsymbol{a} = (X, Y, Z)$ be a triple of integers in $\mathcal{O}_k$ satisfying (1), (2), (3) in Theorem 2.3.6 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 α over $\mathbb{Q}$ respectively.

Definition 2.3.7. We then define the number field K by

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

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

$$\begin{cases} \eta_1 := (\sqrt{\theta'_1} + \sqrt{\theta'_2})^2 = 2X + 2Y\sqrt{p_3}, \\ \eta_2 := (\sqrt{\theta'_1} - \sqrt{\theta'_2})^2 = 2X - 2Y\sqrt{p_3}, \\ \eta_3 := (\sqrt{\theta'_3} + \sqrt{\theta'_4})^2 = 2\overline{X} + 2\overline{Y}\sqrt{p_3}, \\ \eta_4 := (\sqrt{\theta'_3} - \sqrt{\theta'_4})^2 = 2\overline{X} - 2\overline{Y}\sqrt{p_3}. \end{cases}$$

Theorem 2.3.8 (1) *We have*

$$K = \begin{cases} \mathbb{Q}(\sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4}) & \text{if } (Z,2) = 1, \\ \mathbb{Q}(\sqrt{\theta'_1}, \sqrt{\theta'_2}, \sqrt{\theta'_3}, \sqrt{\theta'_4}) = \mathbb{Q}(\sqrt{\eta_1}, \sqrt{\eta_2}, \sqrt{\eta_3}, \sqrt{\eta_4}) & \text{if } (Y,2) = 1. \end{cases}$$

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

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

$$\begin{aligned} \theta_1\theta_2\theta_3\theta_4 &= \mathrm{N}_{k_{13}/\mathbb{Q}}(\theta_1) \\ &= \mathrm{N}_{k/\mathbb{Q}}(\mathrm{N}_{k_{13}/k}(\theta_1)) \\ &= \mathrm{N}_{k/\mathbb{Q}}(\alpha Z^2) \\ &= p_2 h^2 \quad (h \in \mathbb{Z}), \end{aligned} \tag{2.3.8.1}$$

we have $\sqrt{\theta_4} \in K$ and hence $\mathbb{Q}(\sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4}) \subset K$. Next we show the converse inclusion. Write $\theta_1 = a_1 + a_2\sqrt{p_1} + a_3\sqrt{p_3} + a_4\sqrt{p_1p_3}$ $(a_i \in \mathbb{Q})$. By considering the prime factorization of the ideal (αZ^2) in k_1, we find $\alpha Z^2 \notin \mathbb{Z}$. 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 $\theta_1 + \theta_4 = 2(a_1 + a_4\sqrt{p_1p_3})$, $\sqrt{p_1}, \sqrt{p_3} \in \mathbb{Q}(\sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4})$. By (2.3.8.1), we get $K \subset \mathbb{Q}(\sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4})$.

Case $(Y,2)=1$: First, let us show $\mathbb{Q}(\sqrt{\theta_1'},\sqrt{\theta_2'},\sqrt{\theta_3'},\sqrt{\theta_4'})=\mathbb{Q}(\sqrt{\eta_1},\sqrt{\eta_2},\sqrt{\eta_3},\sqrt{\eta_4})$. By the definition of η_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 $K=\mathbb{Q}(\sqrt{\theta_1'},\sqrt{\theta_2'},\sqrt{\theta_3'},\sqrt{\theta_4'})$. 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, $\theta_1'\theta_2'\theta_3'\theta_4'=p_3^2(Y\overline{Y})^2\in\mathbb{Q}$ and $\sqrt{\theta_4'}\in K$. For the converse inclusion, it suffices to show $K\subset\mathbb{Q}(\sqrt{\eta_1},\sqrt{\eta_2},\sqrt{\eta_3},\sqrt{\eta_4})$. By considering the prime factorization of the ideal $(\alpha(2Z)^2)$ in k_1, we find $\alpha(2Z)^2\notin\mathbb{Z}$. By $\mathrm{N}_{k_{13}/\mathbb{Q}}(\eta_1)=4p_2h^2$ and the argument similar to the case of $(Z,2)=1$, we have $\sqrt{p_i}\in\mathbb{Q}(\sqrt{\eta_1},\sqrt{\eta_2},\sqrt{\eta_3},\sqrt{\eta_4})$ $(i=1,2,3)$.

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

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

Let $\tilde{\sigma}\in\mathrm{Gal}(K_1/\mathbb{Q})$ be an extension of σ. 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 $[K:\mathbb{Q}]=[K:K_2][K_2:K_1][K_1:k_{123}][k_{123}:\mathbb{Q}]=64$.

Case $(Y,2)=1$: $K/\mathbb{Q}$ is a Galois extension, because K is the splitting field of $\Pi_{i=1}^4(T^2-\eta_i)=\Pi_{\sigma\in\mathrm{Gal}(k_{13}/\mathbb{Q})}(T^2-\sigma(\eta_1))\in\mathbb{Z}[T]$. 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 $[K:\mathbb{Q}]=[K:K_2'][K_2':K_1'][K_1':k_{123}][k_{123}:\mathbb{Q}]=64$.

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

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

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 $\tau_1, \tau_2, \tau_3 \in \mathrm{Gal}(K/\mathbb{Q})$ 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 $\mathrm{Gal}(K/\mathbb{Q}) \simeq N_4(\mathbb{F}_2)$.

Case $(Y, 2) = 1$: We note $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{\eta_1\eta_2}, \sqrt{\eta_1\eta_3}, \sqrt{\eta_1})$, 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 θ_i with η_i. □

Theorem 2.3.9. *All prime numbers ramified in the extension $K/\mathbb{Q}$ 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 (θ_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 (θ_1) and let $\mathfrak{q}_i = \mathfrak{Q}_i \cap k$. Since $\mathrm{N}_{k_{13}/k}(\theta) = X^2 - p_3Y^2 = \alpha Z^2$, we have

$$\mathrm{N}_{k_{13}/k}((\theta_1)) = (\alpha Z^2) = \mathfrak{p}_2^m\mathfrak{a}^2, \tag{2.3.9.1}$$

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

Case (i): If e_i is odd, it contradicts to (2.3.9.1). 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 (2.3.9.1), $Z \in \mathfrak{Q}_i$. 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 (2.3.9.1) is odd, one of $\mathfrak{P}$ and $\mathfrak{P}'$ appears odd times in the prime factorization of (θ_1). Let $\mathfrak{P}$ be that one. When $\mathfrak{Q}_i \neq \mathfrak{P}$, assume e_i is odd. By (2.3.9.1), $\mathfrak{Q}_i'$ also appears odd times in the prime factorization of (θ_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 (θ_1) has the form $\mathfrak{P}^{m_1}\mathfrak{A}^2$ (m_1: odd). Then, by Lemma 1.1.3, 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 $k_{13}/\mathbb{Q}$ is unramified outside p_1, p_3, we conclude that all ramified prime numbers in $K/\mathbb{Q}$ are p_1, p_2 and p_3.

Finally, we show that the ramification indices of p_i's in $K/\mathbb{Q}$ 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 $k_{13}/\mathbb{Q}$ 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 (θ_i) in $k_{13}(\sqrt{\theta_1})$, we see by Lemma 1.1.3 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 (θ_1') in k_{13}'. Then, by a similar argument, we find that (θ_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 1.1.3 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 $K/\mathbb{Q}$ 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 2.3.10. *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

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

Next, it is easy to see that $\mathbb{Q}(\sqrt{p_2}, \sqrt{p_3}, \sqrt{\theta_1\theta_3})$ is a dihedral extension over $\mathbb{Q}$ of degree 8. Since all prime numbers ramified in $\mathbb{Q}(\sqrt{p_2}, \sqrt{p_3}, \sqrt{\theta_1\theta_3})/\mathbb{Q}$ are p_2 and p_3 with ramification index 2 by Theorem 2.3.9, we have

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

by Theorem 1.2.1. 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

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

By the same argument as in the case of $(Z, 2) = 1$ replacing θ_i with η_i, we have $\mathbb{Q}(\sqrt{p_2}, \sqrt{p_3}, \sqrt{\eta_1\eta_3}) = k_{\{p_3,p_2\}}$. Hence we have, by Theorem 2.3.8,

$$\begin{aligned} K &= \mathbb{Q}(\sqrt{\eta_1}, \sqrt{\eta_2}, \sqrt{\eta_3}, \sqrt{\eta_4}) \\ &= \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{\eta_1\eta_2}, \sqrt{\eta_1\eta_3}, \sqrt{\eta_1}) \\ &= k_{\{p_1,p_2\}}k_{\{p_3,p_2\}}(\sqrt{\theta'_1}). \end{aligned}$$

□

2.4 4-th multiple residue symbol.

Let p_1, p_2, p_3 and p_4 be four prime numbers satisfying

$$\text{(2.4.1)} \quad \begin{cases} p_1 \equiv 5 \pmod 8,\ p_i \equiv 1 \pmod 4\ (i = 2, 3, 4), \\ \left(\dfrac{p_i}{p_j}\right) = 1\ (1 \leq i \neq j \leq 4),\ [p_i, p_j, p_k] = 1\ (i, j, k : \text{ distinct}), \end{cases}$$

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

Let K be the field defined in Definition 2.3.7.

Definition 2.4.2. We define the 4-*th multiple residue symbol* $[p_1, p_2, p_3, p_4]$ by

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

We let

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

Case $(Z, 2) = 1$: Let $\tau_1, \tau_2, \tau_3 \in \mathrm{Gal}(K/\mathbb{Q})$ be as in the proof of Theorem 2.3.8 and we let

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

Then, the subfields of $K/\mathbb{Q}$ which corresponds by Galois theory to the subgroups generated by τ_1, τ_2, τ_3 and $(\tau_1\tau_2\tau_3\tau_2)^2$ are $\mathbb{Q}(\sqrt{p_2}, \sqrt{p_3}, \xi_1, \sqrt{\theta_1\theta_3}, \xi_3)$, $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_3}, \sqrt{\theta_2}, \sqrt{\theta_3}, \sqrt{\theta_4})$, $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\theta_1\theta_2}, \xi_2, \xi_3)$ and F, respectively. By the assumption (2.4.1), p_4 is completely decomposed in the extension $F/\mathbb{Q}$.
Case $(Y, 2) = 1$: We let $\tau_1, \tau_2, \tau_3 \in \mathrm{Gal}(K/\mathbb{Q})$ and ξ_1, ξ_2, ξ_3 be defined by replacing θ_i in the case $(Z, 2) = 1$ with η_i $(1 \leq i \leq 4)$. Then, as in the case $(Z, 2) = 1$ the subfields of $K/\mathbb{Q}$ which corresponds by Galois theory to the subgroups generated by τ_1, τ_2, τ_3 and $(\tau_1\tau_2\tau_3\tau_2)^2$ are $\mathbb{Q}(\sqrt{p_2}, \sqrt{p_3}, \xi_1, \sqrt{\eta_1\eta_3}, \xi_3)$, $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_3}, \sqrt{\eta_2}, \sqrt{\eta_3}, \sqrt{\eta_4})$, $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\eta_1\eta_2}, \xi_2, \xi_3)$ and F, respectively. By the assumption (2.4.1), p_4 is completely decomposed in the extension $F/\mathbb{Q}$.

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 $K/\mathbb{Q}$. So we have, by Definition 2.4.2,

$$[p_1, p_2, p_3, p_4] = \begin{cases} 1 & \sigma_{\mathfrak{P}_4} = \mathrm{id}_K, \\ -1 & \sigma_{\mathfrak{P}_4} \neq \mathrm{id}_K. \end{cases} \tag{2.4.3}$$

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

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

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 $K \subset \mathbb{Q}_S(2)$ by Theorem 2.3.9, we have the natural homomorphism $\psi : G_S(2) \to \mathrm{Gal}(K/\mathbb{Q})$. Let $\varphi := \pi \circ \psi : \hat{F} \to \mathrm{Gal}(K/\mathbb{Q})$. 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 τ_1, τ_2 and τ_3 are equivalent to the following relations:

$$\begin{gathered} \varphi(x_1)^2 = \varphi(x_2)^2 = \varphi(x_3)^2 = \varphi(x_1x_3)^2 = 1, \quad \varphi(x_4) = 1, \\ \varphi(x_1x_2)^4 = \varphi(x_2x_3)^4 = \varphi(x_1x_2x_3)^4 = \varphi((x_1x_2x_3x_2)^2x_3)^2 = 1. \end{gathered} \tag{2.4.4}$$

On the other hand, by the assumption (2.4.1), we have $\overline{\mu}_2(1234) = \mu_2(1234)$.

Theorem 2.4.5. *We have*

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

Proof. By (2.4.3), 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 (2.4.4), $\mathrm{Ker}(\varphi)$ 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 2.4.6. Let $(p_1, p_2, p_3, p_4) := (5, 8081, 101, 449)$. Then we have

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

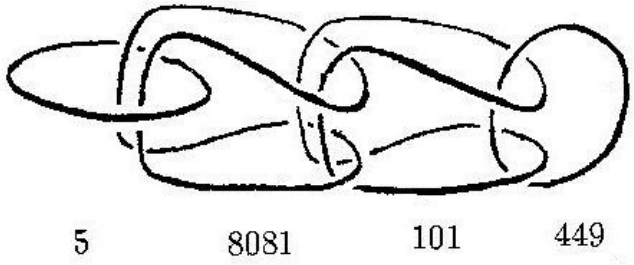
and

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

Then we have

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

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



Finally, two remarks are in order.

Remark 2.4.7. (1) By Theorem 2.4.5, 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 $\mathbb{Q}$ as a generalization of Rédei's work. If a base number field k contains the group of l-th roots of unity μ_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 μ_l-valued multiple residue symbol $[\mathfrak{p}_1, \ldots, \mathfrak{p}_r]$ in a similar manner.

Chapter 3

Rédei's triple symbols and modular forms

In this chapter, we give an analytic expression of the Rédei triple symbol $[-p_1, p_2, p_3]$ for certain prime numbers p_i's in terms of a Fourier coefficient of a modular form.

In Section 3.1, we recall the construction of Rédei's dihedral extension over $\mathbb{Q}$, which contains an imaginary quadratic field $k = \mathbb{Q}(\sqrt{-p_1p_2})$, and give its arithmetic characterization as in Sections 1.1 and 1.2. We then introduce the Rédei triple symbol $[-p_1, p_2, p_3]$ for certain prime numbers p_i's. In Section 3.2, we interpret the triple symbol $[-p_1, p_2, p_3]$ in terms of the Artin L-function $L(\rho, s)$ associated to a two dimensional Galois representation ρ. In Section 3.3, we express the Artin L-function $L(\rho, s)$ in terms of binary quadratic forms corresponding to ideal classes of k. In Section 3.4, we express the Artin L-function $L(\rho, s)$ as the L-function of a modular form associated to binary quadratic forms in Section 3.3. In particular, the Rédei triple symbol $[-p_1, p_2, p_3]$ is expressed as a Fourier coefficient of the modular form, and a reciprocity law for the triple symbol yields certain reciprocal relations among Fourier coefficients.

3.1 Rédei's dihedral extensions and triple symbols

In this section, we recall the construction of Rédei's dihedral extension over $\mathbb{Q}$, which contains an imaginary field $k = \mathbb{Q}(\sqrt{-p_1p_2})$, and give its arithmetic characterization as in Sections 1.1 and 1.2. We then introduce the Rédei triple symbol $[-p_1, p_2, p_3]$ and show a reciprocity law.

Let p_1 and p_2 be distinct prime numbers satisfying the condition

$$p_1 \equiv 3 \bmod 4,\ p_2 \equiv 1 \bmod 4,\ \left(\frac{p_1}{p_2}\right) = \left(\frac{p_2}{p_1}\right) = 1. \tag{3.1.1}$$

We set

$$k_1 := \mathbb{Q}(\sqrt{-p_1}),\ k_2 := \mathbb{Q}(\sqrt{p_2}) \text{ and } k := \mathbb{Q}(\sqrt{-p_1p_2}).$$

Lemma 3.1.2. *There are integers x, y, z satisfying the following conditions*:
(1) $x^2 + p_1y^2 - p_2z^2 = 0$,
(2) g.c.d$(x, y, z) = 1,\ y \equiv 0 \bmod 2,\ x - y \equiv 1 \bmod 4$.
Furthermore, for a given prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$ 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 $\left(\frac{-p_1}{p_2}\right) = 1$, p_2 is decomposed in k_1, say $(p_2) = \mathfrak{p}\overline{\mathfrak{p}}$. Since $-p_1 \equiv 1 \bmod 4$, the class number, say h_1, of k_1 is odd by genus theory ([O, 4.7]). Write $\mathfrak{p}^{h_1} = (\alpha)$ for some $\alpha = (a + b\sqrt{-p_1})/2,\ a, b \in \mathbb{Z},\ a \equiv b \bmod 2$. Since $\mathrm{N}((\alpha)) = \mathrm{N}\mathfrak{p}^{h_1} = p_2^{h_1}$, we have $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha) = p_2^{h_1} \cdots (\star)$.
(i) The case $p_1 \equiv -1 \bmod 8$: If $a \equiv b \equiv 1 \bmod 2$, $a^2 \equiv b^2 \equiv 1 \bmod 8$ and so $a^2 + p_1b^2 \equiv 0 \bmod 8$. Hence $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha) = (a^2 + p_1b^2)/4 \equiv 0 \bmod 2$, which contradicts $(\star)$. Therefore we have $a \equiv b \equiv 0 \bmod 2$. Put $x = a/2, y = b/2 \in \mathbb{Z}$. By $(\star)$, $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha) = x^2+p_1y^2 = p_2z^2$, $z = p_2^{(h_1-1)/2}$. Therefore $x^2+3y^2 \equiv 1 \bmod 4$ which yields $x \equiv 1 \bmod 2$, $y \equiv 0 \bmod 2$ and so $(x, y, z) = 1$. We can take a suitable sign of x if necessary so that $x - y \equiv 1 \bmod 4$.
(ii) The case $p_1 \equiv 3 \bmod 8$: If $a \equiv b \equiv 0 \bmod 2$, we can find $x, y, z \in \mathbb{Z}$ satisfying (1) and (2) as in the case (i). Now assume that $a \equiv b \equiv 1 \bmod 2$. Then we have $a^2 - 3b^2p_1 \equiv 3a^2 - b^2p_1 \equiv 0 \bmod 8$ and so

$$\alpha^3 = \left(\frac{a + b\sqrt{-p_1}}{2}\right)^3 = \frac{a(a^2 - 3b^2p_1) + b(3a^2 - b^2p_1)\sqrt{-p_1}}{8} = x + y\sqrt{-p_1},$$

where we put $x = a(a^2 - 3b^2p_1)/8$ and $y = b(3a^2 - b^2p_1)/8$. Therefore $x^2 + p_1y^2 = \mathrm{N}_{k_1/\mathbb{Q}}(\alpha^3) = p_2z^2$, $z = p_2^{(3h_1-1)/2}$. As in the case (i), $x \equiv 1 \bmod 2$, $y \equiv 0 \bmod 2$ and $(x, y, z) = 1$. We can take a suitable sign of x so that $x - y \equiv 1 \bmod 4$.
The latter assertion follows immediately from the above argument. □

Let $\boldsymbol{a} = (x, y, z)$ be a triple of integers satisfying the conditions (1), (2) in Lemma 3.1.2. We then set

$$K_{\boldsymbol{a}} := \mathbb{Q}(\sqrt{-p_1}, \sqrt{p_2}, \sqrt{\alpha}),\ \ \alpha := x + y\sqrt{-p_1}.$$

The following theorem is due to Rédei ([Ré]). Since Rédei's account was written in a rather classical style, we give here a proof for the sake of readers.

Theorem 3.1.3. (1) *The extension $K_{\boldsymbol{a}}/\mathbb{Q}$ is a Galois extension whose Galois group is the dihedral group D_8 of order 8.*
(2) *All prime numbers ramified in $K_{\boldsymbol{a}}/\mathbb{Q}$ are only p_1 and p_2 with ramification index 2.*

Proof. (1) Let K_f be the splitting field over $\mathbb{Q}$ of $f(T) := T^4 - 2xT^2 + p_2z^2 = (T-\sqrt{\alpha})(T+\sqrt{\alpha})(T-\sqrt{\overline{\alpha}})(T+\sqrt{\overline{\alpha}}) \in \mathbb{Z}[T]$, where $\overline{\alpha} := x - y\sqrt{-p_1}$. Since $\alpha^2 = x + y\sqrt{-p_1}$ and $\sqrt{\alpha}\sqrt{\overline{\alpha}} = z\sqrt{p_2}$, we have $K_{\boldsymbol{a}} = K_f$ and so $K_{\boldsymbol{a}}$ is a Galois extension over $\mathbb{Q}$. Define $s, t \in \mathrm{Gal}(K_{\boldsymbol{a}}/\mathbb{Q})$ by

$$\begin{array}{lll} s(\sqrt{-p_1}) = \sqrt{-p_1}, & s(\sqrt{p_2}) = -\sqrt{p_2}, & s(\sqrt{\alpha}) = \sqrt{\alpha}, \\ t(\sqrt{-p_1}) = -\sqrt{-p_1}, & t(\sqrt{p_2}) = -\sqrt{p_2}, & t(\sqrt{\alpha}) = -\sqrt{\overline{\alpha}}. \end{array}$$

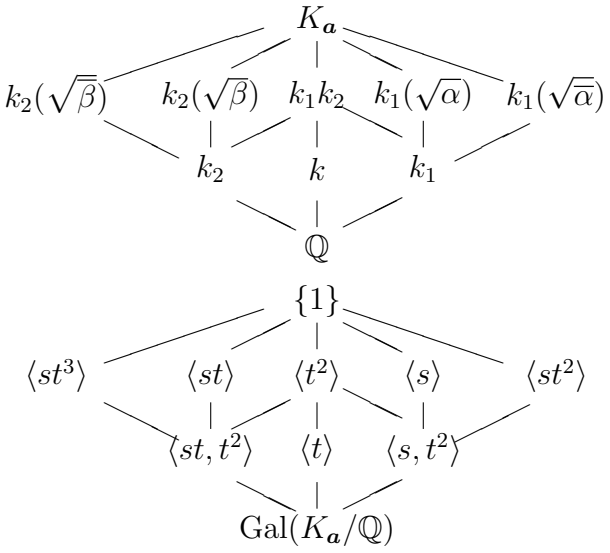
Then we easily see that

$$s^2 = t^4 = 1, sts = t^{-1}$$

and so s, t generate the dihedral group D_8 of order 8. Since it is easy to see $[K_{\boldsymbol{a}} : \mathbb{Q}] = 8$, we conclude $\mathrm{Gal}(K_{\boldsymbol{a}}/\mathbb{Q}) = D_8$.

Putting $\beta := (\sqrt{\alpha} + \sqrt{\overline{\alpha}})^2 = 2(x + z\sqrt{p_2})$, all subfields of $K_{\boldsymbol{a}}/\mathbb{Q}$ and the corresponding subgroups of $\mathrm{Gal}(K_{\boldsymbol{a}}/\mathbb{Q})$ are illustrated as follows.

(3.1.4)



(2) By the condition (3.1.1), p_i is the only ramified prime number in $k_i/\mathbb{Q}$ $(i = 1, 2)$ and that p_1 (resp. p_2) splits in $k_2/\mathbb{Q}$ (resp. $k_1/\mathbb{Q}$). So, looking at

the diagram (3.1.4), it suffices to show that the only one prime of k_1 lying over p_2 is ramified in $k_1(\sqrt{\alpha})/k_1$. First we note that $\lambda := (1+\sqrt{\alpha})/2 \in \mathcal{O}_{k_1(\sqrt{\alpha})}$, since λ satisfies $\lambda^2 + \lambda + (1-\alpha)/4 = 0$ and $(1-\alpha)/4 \in \mathcal{O}_{k_1}$ by $x - y \equiv 1 \bmod 4$. Since the relative discriminant of λ in $k_1(\sqrt{\alpha})/k_1$ is

$$d(\lambda, k_1(\sqrt{\alpha})/k_1) = \begin{vmatrix} 1 & \lambda \\ 1 & \overline{\lambda} \end{vmatrix}^2 = \alpha,$$

where $\lambda := (1-\sqrt{\alpha})/2$, and (α) is prime to 2, any prime of k_1 lying over 2 is unramified in $k_1(\sqrt{\alpha})/k_1$. Next let

$$(\alpha) = \mathfrak{p}^e \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

be the decomposition of (α) into the product of positive powers of distinct prime ideals $\mathfrak{p}, \mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of $\mathcal{O}_{k_1}$. Since $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha) = p_2 z^2$, we can take $\mathfrak{p}$ to be one of primes lying over p_2 and e to be odd. We claim that all e_i's are even. Suppose that there is an odd e_j. Let q_j be the prime number lying below $\mathfrak{q}_j$. If (q_j) splits to $\mathfrak{q}_j\overline{\mathfrak{q}_j}$ in k_1, we have $\alpha \in \overline{\mathfrak{q}_j}$ by $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha) = p_2 z^2$. Then $\alpha, \overline{\alpha} \in \mathfrak{q}_j\overline{\mathfrak{q}_j} = (q_j)$ and so $2x, 2y \in (q_j)$. This contradicts $(x, y, z) = 1$. If q_j is inert in $k_1/\mathbb{Q}$, $\alpha, \overline{\alpha} \in (q_j)$ and so $2x, 2y \in (q_j)$ again, which is a contradiction. If $(q_j) = \mathfrak{q}_j^2$ in k_1, q_j must be p_1. So $\mathrm{N}\mathfrak{q}^{e_j} = p_1^{e_j}$, which contradicts $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha) = p_2 z^2$. Thus we have the decomposition

$$(\alpha) = \mathfrak{p}^e \mathfrak{a}^2, \ \ (\mathfrak{p}, \mathfrak{a}) = 1, \ e \text{ is odd.}$$

By the ramification theory in a Kummer extension ([Fu, Ch.4, Theorem 2.1, Lemma 2.1]), $\mathfrak{p}$ is the unique prime ideal of $\mathcal{O}_{k_1}$ which is ramified in $k_1(\sqrt{\alpha})/k_1$. □

The following theorem shows that the properties (1), (2) in Proposition 1.3 characterize Rédei's extension $K_{\boldsymbol{a}}/\mathbb{Q}$.

Theorem 3.1.5. *Let p_1 and p_2 be prime numbers satisfying the condition* (3.1.1). *Suppose that an extension $K/\mathbb{Q}$ satisfies the following properties*:
(1) *$K/\mathbb{Q}$ is a Galois extension whose Galois group is the dihedral group D_8 of order* 8.
(2) *All prime numbers ramified in $K/\mathbb{Q}$ are only p_1 and p_2 with ramification index* 2.
Then K is uniquely determined.

Proof. By the properties (1) and (2), K contains quadratic fields k_1, k_2 and k, and K/k is an unramified cyclic extension of degree 4. Since the 2-primary

part of the ideal class group of k is cyclic by genus theory ([On, 4.7]), the unramified cyclic extension K/k of degree 4 must be unique by class field theory. □

By Theorem 3.1.5, the extension $K_{\boldsymbol{a}}/\mathbb{Q}$ is independent of a choice of $\boldsymbol{a}$.

Definition 3.1.6. We denote $K_{\boldsymbol{a}}$ by $K_{\{-p_1,p_2\}}$ the field and call $K_{\{-p_1,p_2\}}$ the *Rédei extension* over $\mathbb{Q}$ associated to prime numbers p_1 and p_2 satisfying the condition (3.1.1).

The following collorary will be used later. Let H_k denote the ideal class group of k with $h_k := \#H_k$, the class number of k, and let $H_k(2)$ denote the 2-primary part of H_k with $h_k(2) := \#H_k(2)$, the 2-class number of k.

Corollary 3.1.7. *Notations being as above,*
(1) $K_{\{-p_1,p_2\}}$ *is an unramified cyclic extension over* k *of order* 4.
(2) $H_k(2)$ *is a cyclic group of order* 2^m, $m \geq 2$.
(3) *Let* $\mathfrak{p}_i$ *be the prime ideal of* $\mathcal{O}_k$ *lying over* p_i. *Then the class* $[\mathfrak{p}_i]$ *has order* 2 *in* H_k *for* $i = 1, 2$ *and the Frobenius automorphism of* $\mathfrak{p}_i$ *in* K/k *is given by*

$$\left(\frac{K/k}{\mathfrak{p}_i}\right) = \begin{cases} 1 & \text{if } h_k(2) \geq 8, \\ t^2 & \text{if } h_k(2) = 4. \end{cases}$$

Proof. (1) and (2) were shown in the proof of Theorem 3.1.5. For (3), suppose that $\mathfrak{p}_i = (x + y\omega)$ with $x, y \in \mathbb{Z}$, $\omega := (1 + \sqrt{-p_1p_2})/2$. Then we have $(2x+y)^2 + p_1p_2y^2 = 4p_i$. This never occurs. Hence $[\mathfrak{p}_i]$ has order 2 and the Frobenius automorphism $\left(\frac{K/k}{\mathfrak{p}_i}\right)$ is $t^{h_k(2)/2}$ by class field theory. So the last assertion follows. □

Finally, we introduce the Rédei triple symbol and show a reciprocity law. Let p_1, p_2 and p_3 be distinct prime numbers satisfying the condition

$$(3.1.8)\quad p_1 \equiv 3 \bmod 4,\ p_i \equiv 1 \bmod 4\ (i = 2, 3),\ \left(\frac{p_i}{p_j}\right) = 1\ (1 \leqq i \neq j \leqq 3).$$

Definition 3.1.9. We define the *Rédei triple symbol* by

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

Let $\mathfrak{p}_2$ (resp. $\mathfrak{p}_3$) be one of the prime ideals of k_1 lying over p_2 (resp. p_3). Then there is a triple of integers (x_2, y_2, z_2) with $\alpha_{12} = x_2 + y_2\sqrt{-p_1}$ (resp. (x_3, y_3, z_3) with $\alpha_{13} = x_3 + y_3\sqrt{-p_1}$) 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

$$(\alpha_{12}) = {\mathfrak{p}_2}^{m_2},\ (\alpha_{13}) = {\mathfrak{p}_3}^{m_3}\ (m_2, m_3 \text{ being odd integers}),$$
$$K_{\{-p_1,p_2\}} = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha_{12}}),\ K_{\{-p_1,p_3\}} = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_3}, \sqrt{\alpha_{13}}).$$

Since $\mathfrak{p}_3$ is unramified in $k_1(\sqrt{\alpha_{12}})/k_1$ by Theorem 1.2 (2), we have the Frobenius automorphism $\left(\frac{k_1(\sqrt{\alpha_{12}})/k_1}{\mathfrak{p}_3}\right) \in \mathrm{Gal}(k_1(\sqrt{\alpha_{12}})/k_1)$. We note that the Rédei triple symbol is rewritten as

$$[-p_1, p_2, p_3] = \begin{cases} 1 & \text{if } \left(\frac{k_1(\sqrt{\alpha_{12}})/k_1}{\mathfrak{p}_3}\right) = \mathrm{id}_{k_1(\sqrt{\alpha_{12}})}\ , \\ -1 & \text{otherwise.} \end{cases} \tag{3.1.10}$$

For a prime $\mathfrak{p}$ of k_1, we denote by $\left(\frac{\ ,\ }{\mathfrak{p}}\right)$ the Hilbert symbol in the local field $k_{1\mathfrak{p}}$ (:= the completion of k_1 at $\mathfrak{p}$), namely,

$$(a, k_{1\mathfrak{p}}(\sqrt{b})/k_{1\mathfrak{p}})\sqrt{b} = \left(\frac{a, b}{\mathfrak{p}}\right)\sqrt{b} \quad (a, b \in k_{1\mathfrak{p}}^{\times}),$$

where $(\ , k_{1\mathfrak{p}}(\sqrt{b})/k_{1\mathfrak{p}}) : k_{1\mathfrak{p}}^{\times} \to \mathrm{Gal}(k_{1\mathfrak{p}}(\sqrt{b})/k_{1\mathfrak{p}})$ is the norm residue symbol of local class field theory.

Lemma 3.1.11. *We have*

$$[-p_1, p_2, p_3] = \left(\frac{\alpha_{12}, \alpha_{13}}{\mathfrak{p}_3}\right),\ \ [-p_1, p_3, p_2] = \left(\frac{\alpha_{12}, \alpha_{13}}{\mathfrak{p}_2}\right).$$

Proof. Let π be a prime element of $k_{1\mathfrak{p}_3}$ and $U_{\mathfrak{p}_3}$ denote the unit group in $k_{1\mathfrak{p}_3}^{\times}$. We write $\alpha_{13} = u\pi^{m_3}, u \in U_{\mathfrak{p}_3}$. Noting that $u, \alpha_{12} \in U_{\mathfrak{p}_3}$ and m_3 is odd, we have

$$\begin{aligned}
\left(\frac{\alpha_{12}, \alpha_{13}}{\mathfrak{p}_3}\right) &= \left(\frac{\alpha_{13}, \alpha_{12}}{\mathfrak{p}_3}\right) \\
&= \left(\frac{u, \alpha_{12}}{\mathfrak{p}_3}\right)\left(\frac{\pi^{m_3}, \alpha_{12}}{\mathfrak{p}_3}\right) \\
&= \left(\frac{\pi, \alpha_{12}}{\mathfrak{p}_3}\right) \\
&= \frac{(\pi, k_{1\mathfrak{p}_3}(\sqrt{\alpha_{12}})/k_{1\mathfrak{p}_3})\sqrt{\alpha_{12}}}{\sqrt{\alpha_{12}}} \\
&= \left(\frac{k_1(\sqrt{\alpha_{12}})/k_1}{\mathfrak{p}_3}\right)(\sqrt{\alpha_{12}})/\sqrt{\alpha_{12}} \\
&= [-p_1, p_2, p_3]\ \ ((3.1.10)).
\end{aligned}$$

Similarly, we can show $\left(\frac{\alpha_{12},\alpha_{13}}{\mathfrak{p}_2}\right) = [-p_1, p_3, p_2]$. $\square$

Finally, we show a reciprocity law for the Rédei symbol.

Theorem 3.1.12. *We have*

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

In particular, p_3 is completely decomposed in $K_{\{-p_1,p_2\}}/\mathbb{Q}$ if and only if p_2 is completely decomposed in $K_{\{-p_1,p_3\}}/\mathbb{Q}$.

Proof. By Lemma 3.1.11 and the product formula for the Hilbert symbol

$$\prod_{\mathfrak{p}} \left(\frac{\alpha_{12}, \alpha_{13}}{\mathfrak{p}}\right) = 1 \quad (\mathfrak{p} \text{ runs over all primes of } k_1),$$

we have only to prove

$$\prod_{\mathfrak{p}\neq\mathfrak{p}_2,\mathfrak{p}_3} \left(\frac{\alpha_{12}, \alpha_{13}}{\mathfrak{p}}\right) = 1.$$

If $\mathfrak{p}$ is prime to 2 or ∞ (the infinite prime of k_1), we have

$$\left(\frac{\alpha_{12}, \alpha_{13}}{\mathfrak{p}}\right) = 1,$$

since $\alpha_{12}, \alpha_{13} \in U_{\mathfrak{p}}$. Since ∞ is the complex prime, it is obvious that $\left(\frac{\alpha_{12},\alpha_{13}}{\infty}\right) = 1$. Let $\mathfrak{P}$ be a prime ideal of k_1 lying over 2. Noting that 2 is unramified in $k_1/\mathbb{Q}$ and that $\alpha_{12}, \alpha_{13} \in 1 + \mathfrak{P}^2$ by the condition (2) of Lemma 3.1.2, we have $\left(\frac{\alpha_{12},\alpha_{13}}{\mathfrak{P}}\right) = 1$ ([Sa, Theorem 10.29]). This completes the proof. The latter assertion just follows from Definition 3.1.9. $\square$

3.2 Galois representations and Artin L-functions

In this section, we interpret the Rédei triple symbol in terms of a two dimensional Galois representation, and consider the associated Artin L-function to relate the triple symbol with modular forms in the subsequent sections. We keep the same notations as in Section 3.1.

Let p_1 and p_2 be prime numbers satisfying the condition (3.1.1), and let $K_{\{-p_1,p_2\}}$ be the Rédei dihedral extension over $\mathbb{Q}$ in Definition 3.1.6. In this section, we denote $K_{\{-p_1,p_2\}}$ by K for simplicity.

We let

$$\rho \ : \ \mathrm{Gal}(K/\mathbb{Q}) \ \longrightarrow \ \mathrm{GL}(V(\rho)), \ V(\rho) = \mathbb{C}^2$$

be the two dimensional complex representation of the Galois group $\mathrm{Gal}(K/\mathbb{Q}) = \langle s, t \mid s^2 = t^4 = 1, sts = t^{-1} \rangle$ defined by

$$\rho(s) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \rho(t) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{3.2.1}$$

We note that ρ is irreducible and odd ($\det(\rho(\text{complex conjugate})) = -1$). First, we have the following

Lemma 3.2.2. *For a prime number p_3 satisfying the condition* (3.1.8)*, we have*

$$[-p_1, p_2, p_3] = \frac{1}{2}\mathrm{tr}(\rho(\sigma_{\mathfrak{P}}))$$

where $\sigma_{\mathfrak{P}}$ is the Frobenius automorphism of a prime $\mathfrak{P}$ of K lying over p_3.

Proof. The assertion follows immediately from (3.1.10) and $\rho(t^2) = -I_2$. □

Next, we consider the Artin L-function associated to ρ, which is defined by

(3.2.3)

$$\begin{cases} L(\rho, s) := \prod_p L_p(\rho, s) \ \ (p \text{ runs over all prime numbers, } \mathrm{Re}(s) > 1), \\ L_p(\rho, s) := \det(I_2 - \rho(\sigma_{\mathfrak{P}})p^{-s} | V(\rho)^{I_{\mathfrak{P}}})^{-1}, \end{cases}$$

where $I_{\mathfrak{P}}$ denotes the inertia group of a prime $\mathfrak{P}$ of K lying over p and $\sigma_{\mathfrak{P}}$ mod $I_{\mathfrak{P}}$ is the Frobenius automorphism.

Lemma 3.2.4. *We have*

$$L_p(\rho, s) = \begin{cases} (1 - p^{-s})^{-1} & \text{if } p = p_1 \text{ or } p_2 \text{ and } h_k(2) \geq 8, \\ (1 + p^{-s})^{-1} & \text{if } p = p_1 \text{ or } p_2 \text{ and } h_k(2) = 4, \\ (1 + \mathrm{tr}(\rho(\sigma_{\mathfrak{P}}))p^{-s} + (\dfrac{-p_1p_2}{p})p^{-2s})^{-1} & \text{if } p \neq p_1, p_2. \end{cases}$$

Proof. If $p = p_1$ or p_2, $V(\rho)^{I_{\mathfrak{P}}}$ is one dimensional and, by Corollary 3.1.7, (3), $\sigma_{\mathfrak{P}}$ mod $I_{\mathfrak{P}} \equiv 1$ mod $I_{\mathfrak{P}}$ or t^2 mod $I_{\mathfrak{P}}$ according to $h_k(2) \geq 8$ or $h_k(2) = 4$. Since $\rho(t^2) = -I_2$, the assertion follows. If $p \neq p_1, p_2, I_{\mathfrak{P}} = \{1\}$ by Theorem 3.1.3, (2) and so $L_p(\rho, s) = (1 - \mathrm{tr}(\rho(\sigma_{\mathfrak{P}}))p^{-s} + \det(\rho(\sigma_{\mathfrak{P}}))p^{-2s})^{-1}$. Since $\det \circ \rho$ is a non-trivial character $\mathrm{Gal}(k/\mathbb{Q}) \to \mathbb{C}^\times$, the assertion follows. □

By Lemmas 3.2.2 and 3.2.4, we have the following.

Corollary 3.2.5. *For a prime number p_3 satisfying the condition* (3.1.8)*, we have*

$$L_{p_3}(\rho, s) = \left(1 - 2[-p_1, p_2, p_3]p_3^{-s} + \left(\frac{-p_1p_2}{p_3}\right)p_3^{-2s}\right)^{-1}.$$

Now, let $k = \mathbb{Q}(\sqrt{-p_1p_2})$ as in Section 3.1 and let

$$\chi \ : \ \mathrm{Gal}(K/k) \ \longrightarrow \ \mathbb{C}^\times$$

be the character defined by

$$\chi(t) = \sqrt{-1}. \tag{3.2.6}$$

We let

$$\mathrm{Ind}(\chi) \ : \ \mathrm{Gal}(K/\mathbb{Q}) \ \longrightarrow \ \mathrm{GL}_2(\mathbb{C})$$

be the induced representation of χ.

Lemma 3.2.7. *The representation ρ is equivalent to* $\mathrm{Ind}(\chi)$.

Proof. The induced representation $\mathrm{Ind}(\chi)$ is given by

$$\mathrm{Ind}(\chi)(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \mathrm{Ind}(\chi)(t) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}.$$

Since $P\rho(g) = \mathrm{Ind}(\chi)(g) \cdot P$ for $g = s, t$ with $P = \begin{pmatrix} 1 & \sqrt{-1} \\ -1 & \sqrt{-1} \end{pmatrix}$, the assertion follows. □

By Lemma 3.2.7, we have

$$L(\rho, s) = L(\chi, s), \tag{3.2.8}$$

where $L(\chi, s)$ is the abelian Artin L-function defined by

$$L(\chi, s) = \prod_{\mathfrak{p}}(1 - \chi(\sigma_{\mathfrak{p}})\mathrm{N}\mathfrak{p}^{-s})^{-1} \ (\mathfrak{p} \text{ runs over all prime ideals of } \mathcal{O}_k) \tag{3.2.9}$$

Since K/k is an unramified abelian extension (Theorem 3.1.3), we have the Artin reciprocity homorphism

$$\left(\frac{K/k}{\cdot}\right) \ : \ H_k \ \longrightarrow \ \mathrm{Gal}(K/k); \ [\mathfrak{a}] \ \mapsto \ \left(\frac{K/k}{\mathfrak{a}}\right) = \sigma_{\mathfrak{a}}$$

Let $\boldsymbol{\chi}$ be the Hecke character on H_k obtained as the composite of $\left(\frac{K/k}{\cdot}\right)$ with χ :

$$\boldsymbol{\chi} := \chi \circ \left(\frac{K/k}{\cdot}\right) \ : \ H_k \ \longrightarrow \ \mathbb{C}^{\times} \tag{3.2.10}$$

and let $L(\boldsymbol{\chi}, s)$ be the Hecke L-function defined by

$$L(\boldsymbol{\chi}, s) = \prod_{\mathfrak{p}} (1 - \chi([\mathfrak{p}])\mathrm{N}\mathfrak{p}^{-s})^{-1} = \sum_{\mathfrak{a}} \boldsymbol{\chi}([\mathfrak{a}])\mathrm{N}\mathfrak{a}^{-s} \tag{3.2.11}$$

where $\mathfrak{a}$ runs over all integral ideals of k and $\mathrm{Re}(s) > 1$.
Getting (3.2.8) $\sim$ (3.2.11) together, we have the following

Proposition 3.2.12. *We have*

$$L(\rho, s) = L(\boldsymbol{\chi}, s).$$

3.3 Ideal classes and quadratic forms

In this section, we express the Hecke L-function $L(\boldsymbol{\chi}, s)$ in terms of the binary quadratic forms corresponding to ideal classes of k. We also show some formulas on the numbers of integral representations by these quadratic forms, which will be used in the next section. We keep the same notations as in the previous sections.

Let k be the imaginary quadratic field $\mathbb{Q}(\sqrt{-p_1p_2})$ for prime numbers p_1, p_2 satisfying the condition (3.1.1). Let H_k be the ideal class group of k with class number $h_k = \#H_k$. We write

$$H_k = \{C_0, C_1, \cdots, C_{h_k-1}\}, \quad C_0 = [\mathcal{O}_k].$$

Let $Q_i = Q_i(x, y)$ be a representative of the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of binary quadratic forms corresponding to the ideal class C_i for $i = 0, \cdots, h_{k-1}$

([On, Notes D]). For a positive integer n, we set

$$\begin{aligned} &A(C_i,n) := \{(x,y) \in \mathbb{Z}^2 \mid Q_i(x,y) = n\}, \\ &a(C_i,n) := \#A(C_i,n), \text{ and} \\ &B(C_i,n) := \{\mathfrak{a} \in {C_i}^{-1} \mid \mathfrak{a} \subset \mathcal{O}_k, N\mathfrak{a} = n\}, \\ &b(C_i,n) := \#B(C_i,n). \end{aligned} \tag{3.3.1}$$

Lemma 3.3.2. *There is a surjective and two to one map*

$$A(C_i,n) \longrightarrow B(C_i,n).$$

In particular, we have $a(C_i,n) = 2b(C_i,n)$.

Proof. Take an integral ideal $\mathfrak{b} = \mathbb{Z}\mu + \mathbb{Z}\nu \in C_i$ where $\{\mu,\nu\}$ is a well ordered basis of $\mathfrak{b}$ ([O, Notes D]). We define the map $\varphi : A(C_i,n) \to B(C_i,n)$ by $\varphi((x,y)) := (x\mu + y\nu)\mathfrak{b}^{-1}$. Since $(\mathrm{N}\mathfrak{b})^{-1}\mathrm{N}_{k/\mathbb{Q}}(x\mu + y\nu) = Q_i(x,y)$, φ is well defined. For any $\mathfrak{a} \in B(C_i,n)$, $\mathfrak{a}\cdot\mathfrak{b} \in {C_i}^{-1}\cdot C_i = C_0$ and so $\mathfrak{a}\mathfrak{b} = (z)$ for some $z \in \mathcal{O}_k$. Since $z \in \mathfrak{b}$, we can write $z = x\mu + y\nu$ so that $\varphi((x,y)) = \mathfrak{a}$, hence φ is surjective. Further, we have $\varphi((x,y)) = \varphi((x',y')) \Leftrightarrow (x\mu + y\nu) = (x'\mu + y'\nu) \Leftrightarrow x'\mu + y'\nu = \pm(x\mu + y\nu)$ because ${\mathcal{O}_k}^{\times} = \{\pm 1\}$. Hence φ is two to one. □

Let $\boldsymbol{\chi} : H_k \to \mathbb{C}^{\times}$ be the Hecke character defined in (3.2.10). For a positive integer n, we set

$$a_{\boldsymbol{\chi}}(n) := \frac{1}{2}\sum_{i=0}^{h_k-1} \boldsymbol{\chi}(C_i)a(C_i,n) = \sum_{i=0}^{h_k-1} \boldsymbol{\chi}(C_i)b(C_i,n). \tag{3.3.3}$$

Proposition 3.3.4. *Let I be the set of indices i $(0 \le i \le h_k - 1)$ such that $\boldsymbol{\chi}(C_i) \in \{\pm 1\}$. Then we have*

$$a_{\boldsymbol{\chi}}(n) = \sum_{i\in I} \boldsymbol{\chi}(C_i)a(C_i,n)$$

and

$$L(\boldsymbol{\chi},s) = \sum_{n=1}^{\infty} a_{\boldsymbol{\chi}}(n)n^{-s}.$$

Proof. By Lemma 3.3.2, we have

$$\begin{aligned} L(\boldsymbol{\chi}, s) &= \sum_{i=0}^{h_k-1} \boldsymbol{\chi}(C_i^{-1}) \sum_{\substack{\mathfrak{a}\in C_i^{-1} \\ \mathfrak{a}\subset \mathcal{O}_k}} \mathrm{N}\mathfrak{a}^{-s} \\ &= \sum_{i=0}^{h_k-1} \boldsymbol{\chi}(C_i^{-1}) \sum_{n=1}^{\infty} b(C_i, n) n^{-s} \\ &= \sum_{n=1}^{\infty} \left(\frac{1}{2} \sum_{i=0}^{h_k-1} \boldsymbol{\chi}(C_i^{-1}) a(C_i, n) \right) n^{-s}. \end{aligned}$$

Since $L(\boldsymbol{\chi}, s) = L(\rho, s)$ by Proposition 2.12 and $\mathrm{Im}(\rho) \subset \mathrm{GL}_2(\mathbb{Z})$ by (3.2.1), the coefficients $a_{\boldsymbol{\chi}}(n)$ should be in $\mathbb{Z}$. Since $\mathrm{Im}\boldsymbol{\chi} \subset \{\pm 1, \pm\sqrt{-1}\}$ by (3.2.6) and (3.2.10), and $a(C_i, n) \in \mathbb{Z}$, we have

$$\frac{1}{2} \sum_{i=0}^{h_k-1} \boldsymbol{\chi}({C_i}^{-1}) a(C_i, n) = \frac{1}{2} \sum_{i\in I} \boldsymbol{\chi}(C_i) a(C_i, n) = a_{\boldsymbol{\chi}}(n)$$

and hence

$$L(\boldsymbol{\chi}, s) = \sum_{n=1}^{\infty} a_{\boldsymbol{\chi}}(n) n^{-s}. \qquad \square$$

Here are some properties about the integer coefficients $a_{\boldsymbol{\chi}}(n)$ which will be used in the next section. Similar results were stated in [HM, 2.3].

Proposition 3.3.5. (1) *If $(m, n) = 1$, then $a_{\boldsymbol{\chi}}(mn) = a_{\boldsymbol{\chi}}(m) a_{\boldsymbol{\chi}}(n)$.*
(2) *If p is a prime number different from p_1 and p_2, then we have*

$$a_{\boldsymbol{\chi}}(p^{r+1}) - a_{\boldsymbol{\chi}}(p) a_{\boldsymbol{\chi}}(p^r) + \left(\frac{-p_1 p_2}{p} \right) a_{\boldsymbol{\chi}}(p^{r-1}) = 0 \ \text{ for } \ r \geq 1.$$

Here we mean $\left(\frac{-p_1p_2}{2}\right) = 1$ or -1 according as 2 is decomposed or inert in $k/\mathbb{Q}$, respectively.
(3) *Suppose $p = p_1$ or p_2. If the 2-class number $h_k(2) \geq 8$, then we have $a_{\boldsymbol{\chi}}(p^r) = 1$ for $r \geq 0$. If $h_k(2) = 4$, we have*

$$a_{\boldsymbol{\chi}}(p^r) = \begin{cases} 1 & \text{if } r \equiv 0 \bmod 2, \\ -1 & \text{if } r \equiv 1 \bmod 2. \end{cases}$$

Proof. (1) Let m, n be coprime positive integers. It is easy to set that the

map

$$\bigsqcup_{C_{i_1}C_{i_2}=C_i} (B(C_{i_1},m)\times B(C_{i_2},n)) \longrightarrow B(C_i,mn);\ \ (\mathfrak{a}_1,\mathfrak{a}_2)\mapsto \mathfrak{a}_1\mathfrak{a}_2$$

is bijective and so, by Lemma 3.3.2, we have

$$a(C_i,mn)=\frac{1}{2}\sum_{C_{i_1}C_{i_2}=C_i} a(C_{i_1},m)a(C_{i_2},n).$$

Therefore by (3.3.3) we have

$$\begin{aligned} a_{\boldsymbol{\chi}}(mn) &= \frac{1}{2}\sum_{i=0}^{h_k-1}\boldsymbol{\chi}(C_i)a(C_i,mn)\\ &= \left(\frac{1}{2}\sum_{i_1}\boldsymbol{\chi}(C_{i_1})a(C_{i_1},m)\right)\left(\frac{1}{2}\sum_{i_2}\boldsymbol{\chi}(C_{i_2})a(C_{i_2},n)\right)\\ &= a_{\boldsymbol{\chi}}(m)a_{\boldsymbol{\chi}}(n) \qquad \square \end{aligned}$$

(2) (i) The case p is inert in $k/\mathbb{Q}$, $(p)=\mathfrak{p}$: Then $(\frac{-p_1p_2}{p})=-1$ and so we have to prove

$$a_{\boldsymbol{\chi}}(p^{r+1})-a_{\boldsymbol{\chi}}(p)a_{\boldsymbol{\chi}}(p^r)-a_{\boldsymbol{\chi}}(p^{r-1})=0\ \ (r\geq 1). \tag{3.3.5.1}$$

First, since $\mathrm{N}\mathfrak{p}=p^2$, $a(C_i,p)=0$ for any i and so we have $a_{\boldsymbol{\chi}}(p)=0$. Next, since $[\mathfrak{p}]=C_0$, we note that the map

$$B(C_i,p^{r-1})\longrightarrow B(C_i,p^{r+1});\ \ \mathfrak{a}\mapsto \mathfrak{a}\mathfrak{p}$$

is a bijection for any i. By Lemma 3.3.2 and (3.3.3), we have $a_{\boldsymbol{\chi}}(p^{r+1})=a_{\boldsymbol{\chi}}(p^r)$. This proves (3.3.5.1).
(ii) The case p splits in $k/\mathbb{Q}$, $(p)=\mathfrak{p}\bar{\mathfrak{p}}$: Then $(\frac{-p_1p_2}{p})=1$ and so we need to prove

$$a_{\boldsymbol{\chi}}(p^{r+1})-a_{\boldsymbol{\chi}}(p)a_{\boldsymbol{\chi}}(p^r)+a_{\boldsymbol{\chi}}(p^{r-1})=0\ \ (r\geq 1). \tag{3.3.5.2}$$

$(\mathrm{ii})_1$. Suppose $[\mathfrak{p}]=[\bar{\mathfrak{p}}]$. By (3.3.1) and Lemma 3.3.2, we have

$$a(C_i,p)=\begin{cases} 4 & \text{if } C_i^{-1}=[\mathfrak{p}]=[\bar{\mathfrak{p}}],\\ 0 & \text{otherwise.}\end{cases}$$

Therefore we have

$$a_{\boldsymbol{\chi}}(p)=\frac{1}{2}\sum_{i=0}^{h_k-1}\boldsymbol{\chi}(C_i)a(C_i,p)=2\boldsymbol{\chi}([\mathfrak{p}]). \tag{3.3.5.3}$$

Note that the map

$$B(C_i[\mathfrak{p}], p^r) \longrightarrow B(C_i, p^{r+1}) \setminus \{\overline{\mathfrak{p}}^{r+1}\};\ \mathfrak{a} \mapsto \mathfrak{a}\mathfrak{p}$$

is a bijection for each i and so, by Lemma 3.3.2, we have

$$a(C_i[\mathfrak{p}], p^r) = \begin{cases} a(C_i, p^{r+1}) & \text{if } C_i \neq [\mathfrak{p}]^{r+1}, \\ a(C_i, p^{r+1}) - 2 & \text{if } C_i = [\mathfrak{p}]^{r+1}. \end{cases}$$

Therefore we have, for $r \geq 0$,

$$\begin{aligned} a_{\boldsymbol{\chi}}(p^{r+1}) &= \frac{1}{2}\sum_{i=0}^{h_k-1} \boldsymbol{\chi}(C_i) a(C_i, p^{r+1}) \\ &= \frac{1}{2}\sum_{i=0}^{h_k-1} \boldsymbol{\chi}(C_i) a(C_i[\mathfrak{p}], p^r) - \boldsymbol{\chi}([\mathfrak{p}])^{r+1} \\ &= \boldsymbol{\chi}([\mathfrak{p}]) a_{\boldsymbol{\chi}}(p^r) - \boldsymbol{\chi}([\mathfrak{p}])^{r+1} \quad ([\mathfrak{p}]^{-1} = [\mathfrak{p}]). \end{aligned} \tag{3.3.5.4}$$

By (3.3.5.3) and (3.3.5.4), we get

$$\begin{aligned} &a_{\boldsymbol{\chi}}(p^{r+1}) - a_{\boldsymbol{\chi}}(p) a_{\boldsymbol{\chi}}(p^r) + a_{\boldsymbol{\chi}}(p^{r-1}) \\ &= (\boldsymbol{\chi}([\mathfrak{p}]) a_{\boldsymbol{\chi}}(p^r) - \boldsymbol{\chi}([\mathfrak{p}])^{r+1}) - 2\boldsymbol{\chi}([\mathfrak{p}]) a_{\boldsymbol{\chi}}(p^r) + (\boldsymbol{\chi}([\mathfrak{p}]) a_{\boldsymbol{\chi}}(p^r) + \boldsymbol{\chi}([\mathfrak{p}])^{r+1}) \\ &= 0. \end{aligned}$$

(ii)$_2$. Suppose $[\mathfrak{p}] \neq [\overline{\mathfrak{p}}]$. By (3.3.1) and Lemma 3.3.2, we have

$$a(C_i, p) = \begin{cases} 2 & \text{if } C_i^{-1} = [\mathfrak{p}] \text{ or } [\overline{\mathfrak{p}}], \\ 0 & \text{otherwise.} \end{cases}$$

Therefore we have

$$a_{\boldsymbol{\chi}}(p) = \frac{1}{2}\sum_{i=0}^{h_k-1} \boldsymbol{\chi}(C_i) a(C_i, p) = \boldsymbol{\chi}([\mathfrak{p}]) + \boldsymbol{\chi}([\overline{\mathfrak{p}}]) \tag{3.3.5.5}$$

Note that the map

$$B(C_i[\mathfrak{p}], p^r) \longrightarrow B(C_i, p^{r+1}) \setminus \{\overline{\mathfrak{p}}^{r+1}\};\ \mathfrak{a} \mapsto \mathfrak{a}\mathfrak{p}$$

is a bijection for each i. Therefore, noting $[\mathfrak{p}]^{-1} = [\overline{\mathfrak{p}}]$, the argument similar to the case (ii)$_1$ shows

$$a_{\boldsymbol{\chi}}(p^{r+1}) = \boldsymbol{\chi}([\overline{\mathfrak{p}}]) a_{\boldsymbol{\chi}}(p^r) - \boldsymbol{\chi}([\mathfrak{p}])^{r+1} \quad (r \geq 0). \tag{3.3.5.6}$$

Since the map $B(C_i[\overline{\mathfrak{p}}], p^r) \to B(C_i, p^{r+1}) \setminus \{\mathfrak{p}^{r+1}\};\ \mathfrak{a} \mapsto \mathfrak{a}\overline{\mathfrak{p}}$ is also bijective for each i, we obtain similarly

$$a_{\boldsymbol{\chi}}(p^{r+1}) = \boldsymbol{\chi}([\mathfrak{p}]) a_{\boldsymbol{\chi}}(p^r) - \boldsymbol{\chi}([\overline{\mathfrak{p}}])^{r+1} \quad (r \geq 0). \tag{3.3.5.7}$$

By (3.3.5.5), (3.3.5.6) and (3.3.5.7), we get

$$\begin{aligned}
&a_{\boldsymbol{\chi}}(p^{r+1}) - a_{\boldsymbol{\chi}}(p)a_{\boldsymbol{\chi}}(p^r) + a_{\boldsymbol{\chi}}(p^{r-1}) \\
&= (\boldsymbol{\chi}([\mathfrak{p}])a_{\boldsymbol{\chi}}(p^r) - \boldsymbol{\chi}([\overline{\mathfrak{p}}])^{r+1}) - (\boldsymbol{\chi}([\mathfrak{p}]) + \boldsymbol{\chi}([\overline{\mathfrak{p}}]))a_{\boldsymbol{\chi}}(p^r) + (\boldsymbol{\chi}([\mathfrak{p}])a_{\boldsymbol{\chi}}(p^r) + \boldsymbol{\chi}([\mathfrak{p}])^{r+1}) \\
&= \boldsymbol{\chi}([\mathfrak{p}])a_{\boldsymbol{\chi}}(p^r) - \boldsymbol{\chi}([\overline{\mathfrak{p}}])^{r+1} - (\boldsymbol{\chi}([\overline{\mathfrak{p}}])a_{\boldsymbol{\chi}}(p^r) - \boldsymbol{\chi}([\mathfrak{p}])^{r+1}) \\
&= 0.
\end{aligned}$$

(3) Let $p = p_1$ or p_2 so that $(p) = \mathfrak{p}^2$, $\mathrm{N}\mathfrak{p} = p$. Since $[\mathfrak{p}]$ has order 2 in H_k by Corollary 3.1.7,(3), we have

$$a(C_i, p^r) = 2b(C_i, p^r) = 0 \quad \text{unless} \quad C_i = C_0 \text{ or } [\mathfrak{p}]$$

and

$$a(C_0, p^r) = 2b(C_i, p^r) = \begin{cases} 2 & \text{if } r \equiv 0 \bmod 2, \\ 0 & \text{if } r \equiv 1 \bmod 2, \end{cases}$$

$$a([\mathfrak{p}], p^r) = 2b(C_i, p^r) = \begin{cases} 0 & \text{if } r \equiv 0 \bmod 2, \\ 2 & \text{if } r \equiv 1 \bmod 2. \end{cases}$$

Further, $\boldsymbol{\chi}(C_0) = 1$, and by Corollary 3.1.7,(3),

$$\boldsymbol{\chi}([\mathfrak{p}]) = \begin{cases} 1 & \text{if } h_k(2) \geq 8, \\ -1 & \text{if } h_k(2) = 4. \end{cases}$$

Hence, if $h_k(2) \geq 8$, we have

$$a_{\boldsymbol{\chi}}(p^r) = \frac{1}{2}(a(C_0, p^r) + a([\mathfrak{p}], p^r)) = 1,$$

and if $h_k(2) = 4$,

$$a_{\boldsymbol{\chi}}(p^r) = \frac{1}{2}(a(C_0, p^r) - a([\mathfrak{p}], p^r)) = \begin{cases} 1 & \text{if } r \equiv 0 \bmod 2, \\ -1 & \text{if } r \equiv 1 \bmod 2. \end{cases} \qquad \square$$

3.4 Theta series and reciprocity laws

In this section, we express the Artin L-function in Section 3.2 as the L-function of a modular form associated to binary quadratic forms in Section 3.3. This may be seen as an explicit and constructive version of the theorem by Weil-Langlands and Deligne-Serre ([Se]) for the Rédei extension. In particular, the Rédei triple symbol is expressed as a Fourier coefficient of a modular form which is given in terms of the numbers of integral representations of binary quadratic forms. A reciprocity law for the triple symbol

yields certain reciprocal relations among Fourier coefficients.

Let $\mathfrak{H}$ be the upper half plane in $\mathbb{C}$. Let $M_w(\Gamma_0(N), \varepsilon)$ be the space of holomorphic modular forms on $\mathfrak{H}$ of weight w and character ε mod N with respect to $\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \bmod N\}$ on which the Hecke operators $T(m)$ $(m \in \mathbb{Z} > 0)$ act. Each modular form $f \in M_w(\Gamma_0(N), \varepsilon)$ has the Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n q^n, \quad q := \exp(2\pi\sqrt{-1}z) \quad (z \in \mathfrak{H}),$$

and the action of the Hecke operator $T(m)$ is defined by

$$(f|T(m))(z) = \sum_{n=0}^{\infty} b_n q^n, \qquad b_n = \sum_{0<d|(m,n)} \varepsilon(d) d^{\omega-1} a_{mn/d^2}, \tag{3.4.1}$$

where we understand that $b_n = a_{mn}$ if m divides N.

Let $S_w(\Gamma_0(N), \varepsilon)$ be the subspace of $M_w(\Gamma_0(N), \varepsilon)$ consisting of cusp forms $f(z)$ (i.e., $a_0 = 0$) which is stable under the action of Hecke operators $T(m)$ $(m \in \mathbb{Z} > 0)$. A cusp form in $S_w(\Gamma_0(N), \varepsilon)$ is called a Hecke eigenform if it is a common eigenfunction of all Hecke operators $T(m)$'s.

Now, let us be back in the situation of the previous sections. We consider the following theta series. For $z \in \mathfrak{H}$, we let

$$\begin{cases} \theta(C_i, z) := \dfrac{1}{2} \displaystyle\sum_{n=0}^{\infty} a(C_i, n) q^n = \frac{1}{2} \sum_{x,y \in \mathbb{Z}} q^{Q_i(x,y)} \quad (0 \le i \le h_k - 1), \\ \Theta_{\boldsymbol{\chi}}(z) := \displaystyle\sum_{n=0}^{\infty} a_{\boldsymbol{\chi}}(n) q^n = \sum_{i=0}^{h_k-1} \boldsymbol{\chi}(C_i) \theta(C_i, z). \end{cases} \tag{3.4.2}$$

Here we set $a(C_i, 0) = 1$ for all i and $a_{\boldsymbol{\chi}}(0) = \sum_{i=0}^{h_k-1} \boldsymbol{\chi}(C_i) = 0$. The following theorem is due to E. Hecke ([H]).

Theorem 3.4.3. (1) $\theta(C_i, z) \in M_1(\Gamma_0(p_1p_2), \left(\dfrac{-p_1p_2}{\cdot}\right))$.

(2) $\Theta_{\boldsymbol{\chi}}(z) \in S_1(\Gamma_0(p_1p_2), \left(\dfrac{-p_1p_2}{\cdot}\right))$ *and it is a Hecke eigenform.*

Proof. (1) We refer to [Mk, Corollary 4.9.5].
(2) Since $\boldsymbol{\chi}$ is not genus character (i.e., a character of order 2), $\Theta_{\boldsymbol{\chi}}(z)$ is a

cusp form ([Z, 4.3], [Mk, Theorem 4.8.2]). Further, by proposition 3.3.5, the Dirichlet series associated to $\Theta_{\boldsymbol{\chi}}(z)$ is written as

$$\sum_{n=1}^{\infty} a_{\boldsymbol{\chi}}(n)n^{-s} = \prod_{p}(1 - a_{\boldsymbol{\chi}}(p)p^{s} + \left(\frac{-p_1p_2}{p}\right)p^{-2s})^{-1} \tag{3.4.4}$$

where p runs over all prime numbers and we set $(\frac{-p_1p_2}{p}) = 0$ if $p = p_1$ or p_2. This implies that $\Theta_{\boldsymbol{\chi}}(z)$ is a Hecke eigenform ([Mk, Theorem 4.5.16]). □

Let $L(\Theta_{\boldsymbol{\chi}}, s)$ denote the L-function of the modular form $\Theta_{\boldsymbol{\chi}}(z)$, namely, the Dirichlet series

$$L(\Theta_{\boldsymbol{\chi}}, s) := \sum_{n=1}^{\infty} a_{\boldsymbol{\chi}}(n)n^{-s}. \tag{3.4.5}$$

By (3.4.4), we have

$$\begin{cases} L(\Theta_{\boldsymbol{\chi}}, s) = \prod_{p} L_p(\Theta_{\boldsymbol{\chi}}, s) \ \ (p \text{ runs over all prime numbers}), \\ L_p(\Theta_{\boldsymbol{\chi}}, s) = (1 - a_{\boldsymbol{\chi}}(p)p^{s} + \left(\frac{-p_1p_2}{p}\right)p^{-2s})^{-1}. \end{cases}$$

By Proposition 3.3.5, (3), we note

$$L_p(\Theta_{\boldsymbol{\chi}}, s) = \begin{cases} (1 - p^{-s})^{-1} & \text{if } p = p_1 \text{ or } p_2 \text{ and } h_k(2) \geq 8, \\ (1 + p^{-s})^{-1} & \text{if } p = p_1 \text{ or } p_2 \text{ and } h_k(2) = 4. \end{cases}$$

The following theorem may be regarded as an explicit and constructive version of the theorem of Weil-Langlands and Deligne-Serre ([Se]).

Theorem 3.4.6. *We have*

$$L(\rho, s) = L(\Theta_{\boldsymbol{\chi}}, s).$$

For a prime number $p \neq p_1, p_2$, we have

$$tr(\rho(\sigma_{\mathfrak{P}})) = a_{\boldsymbol{\chi}}(p)$$

where $\sigma_{\mathfrak{P}}$ is the Frobenius automorphism of a prime of K lying over p.

Proof. The first assertion follows from Propositions 3.2.12, 3.3.4 and (3.4.5). The second one follows from Lemma 3.2.4 and (3.4.4). □

Let p_1, p_2 and p_3 be prime numbers satisfying the condition (3.1.8). The following corollary gives a relation between the Rédei triple symbol and modular form.

Corollary 3.4.7. *We have*

$$[-p_1, p_2, p_3] = \frac{1}{2} a_{\boldsymbol{\chi}}(p_3).$$

In particular, p_3 is completely decomposed in the Rédei extension $K_{\{-p_1,p_2\}}/\mathbb{Q}$ if and only if $a_{\boldsymbol{\chi}}(p_3) = 2$.

Proof. This follows from Lemma 3.2.2 and Theorem 3.4.6. □

Now we write k_{12} and $\boldsymbol{\chi}_{12} : H_{k_{12}} \to \mathbb{C}^\times$ for $k = \mathbb{Q}(\sqrt{-p_1p_2})$ and $\boldsymbol{\chi}$ in the previous sections, and we let $k_{13} := \mathbb{Q}(\sqrt{-p_1p_2})$ and denote by $\boldsymbol{\chi}_{13}$ the Hecke character $H_{k_{13}} \to \mathbb{C}^\times$ defined in the similary manner to the case of $\boldsymbol{\chi}_{12}$. The reciprocity law for the triple symbol yields the following

Therorem 3.4.8. *Notations being as above, we have*

$$a_{\boldsymbol{\chi}_{12}}(p_3) = a_{\boldsymbol{\chi}_{13}}(p_2).$$

Proof. It follows from Theorem 3.1.12 and Corollary 3.4.7. □

3.5 Numerical examples

In this section, we discuss numerical examples. We keep the same notations as in the previous sections.

Example 3.5.1. Let $p_1 = 11$ and $p_2 = 5$. The associated Rédei extension is given by

$$K_{\{-11,5\}} = \mathbb{Q}(\sqrt{-p_1}, \sqrt{p_2}, \sqrt{\alpha}), \quad \alpha = 3 + 2\sqrt{5}.$$

Let $\rho : \mathrm{Gal}(K_{\{-11,5\}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ be the representation defined in (3.2.1). The ideal class group H_k of $k = \mathbb{Q}(\sqrt{-55})$ is a cyclic group of order 4:

$$H_k = \{C_0 = [\mathcal{O}_k],\ C_1 = [\mathfrak{p}_2],\ C_2 = C_1^2 = [\mathfrak{p}_5],\ C_3 = C_1^3 = [\overline{\mathfrak{p}_2}]\}$$

where $\mathcal{O}_k = [1,\ \omega]$, $\mathfrak{p}_2 = [2,\ \omega]$, $\mathfrak{p}_5 = [5,\ 2 + \omega]$, $\overline{\mathfrak{p}_2} = [2,\ 1 + \omega]$. ($\omega = (1 + \sqrt{-55})/2$), and the corresponding binary quadratic forms are

given respectively by

$$\begin{array}{ll} Q_0 = X^2 + XY + 14Y^2, & Q_1 = 2X^2 + XY + 7Y^2, \\ Q_2 = 5X^2 + 5XY + 4Y^2, & Q_3 = 2X^2 + 3XY + 8Y^2. \end{array}$$

Note that $K_{\{-11,5\}}$ is the Hilbert class field of k. For a positive integer n, $a(C_i, n) := \#\{(x, y) \in \mathbb{Z} \mid Q_i(x, y) = n\}$ $(0 \leq i \leq 3)$. Since the character $\boldsymbol{\chi} : H_k \to \mathbb{C}^\times$ in (3.2.10) is given by $\boldsymbol{\chi}(C_i) = (\pm\sqrt{-1})^i$ $(0 \leq i \leq 3)$, we have

$$a_{\boldsymbol{\chi}}(n) = \frac{1}{2}(a(C_0, n) - a(C_2, n))$$

and

$$\begin{aligned} \Theta_{\boldsymbol{\chi}}(z) &= \sum_{n=1}^{\infty} a_{\boldsymbol{\chi}}(n) q^n = \frac{1}{2}\left(\sum_{x,y\in\mathbb{Z}} q^{x^2+xy+14y^2} - \sum_{x,y\in\mathbb{Z}} q^{5x^2+5xy+4y^2}\right) \\ &= q - q^4 - q^5 + q^9 - q^{11} + q^{16} + \cdots \end{aligned}$$

Theorem 3.4.6 reads:

$$\begin{cases} L(\rho, s) = L(\Theta_{\boldsymbol{\chi}}, s), \\ \mathrm{tr}(\rho(\sigma_{\mathfrak{P}})) = a_{\boldsymbol{\chi}}(p) \ \text{ for a prime number } p \neq 5, 11. \end{cases}$$

By Corollary 3.4.7, for a prime number p_3 satisfying (3.1.8), i.e., $p_3 \equiv 1 \bmod 4$, $\left(\frac{11}{p_3}\right) = \left(\frac{5}{p_3}\right) = 1$, we have

$$[-11, 5, p_3] = \frac{1}{2} a_{\boldsymbol{\chi}}(p_3).$$

For example, let $p_3 = 89$ satisfying (3.1.8). To distinguish the notations, we write k_{12}, $Q_{12,i}$ and $\boldsymbol{\chi}_{12}$ for the above k, Q_i and $\boldsymbol{\chi}$, and let $k_{13} := \mathbb{Q}(\sqrt{-11 \cdot 89}) = \mathbb{Q}(\sqrt{-979})$. The ideal class group $H_{k_{13}}$ of k_{13} is a cyclic group of order 8 consisting of $C_{13,0}, C_{13,i} = (C_{13,1})^i$ $(1 \leq i \leq 7)$:

$$\begin{array}{ll} C_{13,0} = [X^2 + XY + 245Y^2], & C_{13,1} = [7X^2 + XY + 35Y^2], \\ C_{13,2} = [5X^2 + 9XY + 53Y^2], & C_{13,3} = [13X^2 + 23XY + 29Y^2], \\ C_{13,4} = [11X^2 + 11XY + 25Y^2], & C_{13,5} = [13X^2 + 35XY + 29Y^2], \\ C_{13,6} = [5X^2 + XY + 49Y^2], & C_{13,7} = [7X^2 + 13XY + 41Y^2]. \end{array}$$

We set $a(C_{13,i}, n) := \#\{(x, y) \in \mathbb{Z}^2 \mid Q_{13,i}(x, y) = n\}$. Since the character $\boldsymbol{\chi}_{13} : H_{k_{13}} \to \mathbb{C}^\times$ in (3.2.10) is given by $\boldsymbol{\chi}_{13}(C_{13,i}) = (\pm\sqrt{-1})^i$ $(0 \leq i \leq 7)$, we have

$$a_{\boldsymbol{\chi}_{13}}(n) = \frac{1}{2}(a(C_{13,0}, n) - a(C_{13,2}, n) + a(C_{13,4}, n) - a(C_{13,6}, n)).$$

The reciprocity law of Theorem 4.8 then reads

$$a_{\boldsymbol{\chi}_{12}}(89) = a_{\boldsymbol{\chi}_{13}}(5).$$

In fact, we can easily see $a_{\boldsymbol{\chi}_{13}}(5) = -2$. So the above reciprocity tells us $a_{\boldsymbol{\chi}_{12}}(89) = -2$. Therefore 89 is decomposed as $(89) = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4, \mathrm{N}\mathfrak{P}_i = 89^2$ in $K_{\{-11,5\}}$.

Example 3.5.2. Let $p_1 = 3$ and $p_2 = 73$. The associated Rédei extension is then given by

$$K_{\{-3,73\}} = \mathbb{Q}(\sqrt{-p_1}, \sqrt{p_2}, \sqrt{\alpha}), \quad \alpha = -17 + 2\sqrt{73}.$$

Let $\rho : \mathrm{Gal}(K_{\{-3,73\}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ be the representation defined in (3.2.1). The ideal class group H_k of $k = \mathbb{Q}(\sqrt{-219})$ is a cyclic group of order 4:

$$H_k = \{C_0 = [\mathcal{O}_k],\ C_1 = [\mathfrak{p}_5],\ C_2 = C_1^2 = [\mathfrak{p}_3],\ C_3 = C_1^3 = [\overline{\mathfrak{p}_5}]\}$$

where $\mathcal{O}_k = [1,\ \omega]$, $\mathfrak{p}_5 = [5,\ \omega]$, $\mathfrak{p}_3 = [3,\ 1+\omega]$, $\overline{\mathfrak{p}_5} = [1,\ 4+\omega]$. ($\omega = (1+\sqrt{-219})/2$), and the corresponding binary quadratic forms are given respectively by

$$\begin{aligned} Q_0 &= X^2 + XY + 55Y^2, & Q_1 &= 5X^2 + XY + 11Y^2, \\ Q_2 &= 3X^2 + 3XY + 19Y^2, & Q_3 &= 5X^2 + 9XY + 15Y^2. \end{aligned}$$

Note that $K_{\{-3,73\}}$ is the Hilbert class field of k. For a positive integer n, $a(C_i, n) := \#\{(x,y) \in \mathbb{Z}^2 \mid Q_i(x,y) = n\}$ $(0 \le i \le 3)$. Since the character $\boldsymbol{\chi} : H_k \to \mathbb{C}^\times$ in (3.2.10) is given by $\boldsymbol{\chi}(C_i) = (\pm\sqrt{-1})^i$ $(0 \le i \le 3)$, we have

$$a_{\boldsymbol{\chi}}(n) = \frac{1}{2}(a(C_0, n) - a(C_2, n))$$

and

$$\begin{aligned} \Theta_{\boldsymbol{\chi}}(z) &= \sum_{n=1}^{\infty} a_{\boldsymbol{\chi}}(n) q^n = \frac{1}{2}\left(\sum_{x,y\in\mathbb{Z}} q^{x^2+xy+55y^2} - \sum_{x,y\in\mathbb{Z}} q^{3x^2+3xy+19y^2}\right) \\ &= q - q^3 + q^4 + q^9 - q^{12} + q^{16} - \cdots \end{aligned}$$

Theorem 3.4.6 reads:

$$\begin{cases} L(\rho, s) = L(\Theta_{\boldsymbol{\chi}}, s), \\ \mathrm{tr}(\rho(\sigma_{\mathfrak{P}})) = a_{\boldsymbol{\chi}}(p) \ \text{ for a prime number } p \neq 3, 73. \end{cases}$$

By Corollary 3.4.7, for a prime number p_3 satisfying (3.1.8), i.e., $p_3 \equiv 1 \bmod 4$, $\left(\frac{3}{p_3}\right) = \left(\frac{73}{p_3}\right) = 1$, we have

$$[-3, 73, p_3] = \frac{1}{2} a_{\boldsymbol{\chi}}(p_3).$$

For example, let $p_3 = 97$. To distinguish the notations, we write k_{12}, $Q_{12,i}$ and $\boldsymbol{\chi}_{12}$ for the above k, Q_i and $\boldsymbol{\chi}$, and let $k_{13} := \mathbb{Q}(\sqrt{-3 \cdot 97}) = \mathbb{Q}(\sqrt{-291})$. According to the table of [WS], the triple of prime numbers $\{3, 73, 97\}$ is an example such that (3.1.8) is satisfied and the ideal class groups of k_{12} and k_{13} are both cyclic group of order 4. In fact, the ideal class group $H_{k_{13}}$ of k_{13} consists of $C_{13,0}, C_{13,i} = (C_{13,1})^i$ $(1 \leq i \leq 3)$:

$$\begin{array}{ll} C_{13,0} = [X^2 + XY + 73Y^2], & C_{13,1} = [5X^2 + 7XY + 17Y^2], \\ C_{13,2} = [3X^2 + 3XY + 25Y^2], & C_{13,3} = [5X^2 + 3XY + 15Y^2]. \end{array}$$

So $K_{\{-3,97\}}$ is also the Hilbert class field of k_{13}. We set $a(C_{13,i}, n) := \#\{(x, y) \in \mathbb{Z}^2 \mid Q_{13,i}(x, y) = n\}$. Since the Hecke character $\boldsymbol{\chi}_{13} : H_{k_{13}} \to \mathbb{C}^\times$ in (3.2.10) is given by $\boldsymbol{\chi}_{13}(C_{13,i}) = (\pm\sqrt{-1})^i$ $(0 \leq i \leq 3)$, we have

$$a_{\boldsymbol{\chi}_{13}}(n) = \frac{1}{2}(a(C_{13,0}, n) - a(C_{13,2}, n)).$$

The reciprocity law of Theorem 4.8 reads

$$a_{\boldsymbol{\chi}_{12}}(97) = a_{\boldsymbol{\chi}_{13}}(73).$$

In fact, we can easily see $a_{\boldsymbol{\chi}_{12}}(97) = a_{\boldsymbol{\chi}_{13}}(73) = 2$. So 97 (resp. 73) is completely decomposed in $K_{\{-3,73\}}/\mathbb{Q}$ (resp. $K_{\{-3,97\}}/\mathbb{Q}$).

Remark 3.5.3. We note that $k = \mathbb{Q}(\sqrt{-p_1 p_2})$ has the class number 4 if and only if the Rédei extension $K_{\{-p_1,p_2\}}$ is the Hilbert class field of k. According to the table of [WS], there are 21 pairs of (p_1, p_2) in the range $p_1 p_2 < 10000$ such that the condition (3.1.1) satisfied and the class number of k is 4, namely, $(p_1, p_2) = (3, 13)$, $(11, 5)$, $(31, 5)$, $(7, 29)$, $(3, 73)$, $(7, 37)$, $(3, 97)$, $(19, 17)$, $(71, 5)$, $(23, 29)$, $(3, 241)$, $(7, 109)$, $(191, 5)$, $(59, 17)$, $(79, 13)$, $(3, 409)$, $(11, 113)$, $(19, 73)$, $(83, 17)$, $(11, 137)$, $(311, 5)$. By [Ar] and [Wat], this list of 21 pairs is proved to be complete. Among these, the triples of (p_1, p_2, p_3) such that the condition (3.1.8) is satisfied are given by $(3, 73, 97), (3, 97, 241), (7, 29, 109)$.

Chapter 4

Certain $N_3(\mathbb{F}_3)$-extensions over $\mathbb{Q}(\sqrt{-3})$ and triple cubic residue symbols

In this chapter, we introduce a triple cubic residue symbol $[\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3]_3 \in \{1, \omega, \omega^2\}$, where $\mathfrak{p}_i$'s are certain prime ideals of $k := \mathbb{Q}(\sqrt{-3})$ and $\omega := \frac{-1+\sqrt{-3}}{2}$ is a cubic root of unit. For this, we construct concretely an $N_3(\mathbb{F}_3)$-extension E over k where ramified primes are only $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Our symbol $[\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3]_3$ describes the decomposition law of $\mathfrak{p}_3$ in E/k.

4.1 Construction of a certain $N_3(\mathbb{F}_3)$-extension

In this section, we construct a certain $N_3(\mathbb{F}_3)$-extension over $k := \mathbb{Q}(\sqrt{-3})$, which may be regarded as an analogue over k of the Rédei extension over $\mathbb{Q}$.

Let us recall the conditions on prime numbers for which the Rédei symbol is defined. The condition $p \equiv 1 \pmod 4$ means that only a prime number p is ramified in $\mathbb{Q}(\sqrt{p})$, and $\left(\frac{p_1}{p_2}\right) = 1$ means that p_2 is decomposed in $\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}$. These conditions correspond to the following conditions (2), (3) of Lemma 4.1.1. Therefore it may be suitable to consider primes $\mathfrak{p} = (p)$, $p \equiv 8 \pmod 9$ of k.

Lemma 4.1.1. *Let p be a prime number such that $p \equiv 8 \pmod 9$ and let $\mathfrak{p} = (p)$ be a prime of k. Then we have*
(1) *p is inert in $k/\mathbb{Q}$: $\mathrm{N}\mathfrak{p} = p^2$.*
(2) *Only $\mathfrak{p}$ is ramified in $k(\sqrt[3]{p})/k$.*

(3) *Let l be a prime number such that $l \neq p$, $l \equiv 8 \pmod 9$. Then the prime (l) is completely decomposed in $k(\sqrt[3]{p})/k$.*

Proof. (1) This follows immediately from the computation of the Legendre symbol:

$$\begin{aligned}\left(\tfrac{-3}{p}\right) &= (-1)^{(p-1)/2}\left(\tfrac{3}{p}\right)\\ &= (-1)^{(p-1)/2}(-1)^{\{(p-1)/2\}\{(3-1)/2\}}\left(\tfrac{p}{3}\right)\\ &= \left(\tfrac{2}{3}\right)\\ &= -1.\end{aligned}$$

(2) First we note that $\lambda := \sqrt{-3}(2-\sqrt[3]{p})/3 \in \mathcal{O}_{k(\sqrt[3]{p})}$, since λ satisfies $\lambda^3 - 2\sqrt{-3}\lambda^2 - 4\lambda + \sqrt{-3}(8-p)/9 = 0$ and $(8-p)/9 \in \mathbb{Z}$ by $p \equiv 8 \pmod 9$. Since the relative discriminant of λ in $k(\sqrt[3]{p})/k$ is

$$d(\lambda, k(\sqrt[3]{p})/k) = \begin{vmatrix} 1 & \lambda_1 & \lambda_1^2 \\ 1 & \lambda_2 & \lambda_2^2 \\ 1 & \lambda_3 & \lambda_3^2 \end{vmatrix}^2 = -\frac{p^2}{27}\begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix}^2 = p^2$$

where $\lambda_1 := \sqrt{-3}(2-\sqrt[3]{p})/3$, $\lambda_2 := \sqrt{-3}(2-\omega\sqrt[3]{p})/3$ and $\lambda_3 := \sqrt{-3}(2-\omega^2\sqrt[3]{p})/3$. Therefore only $\mathfrak{p}$ is ramified in $k(\sqrt[3]{p})/k$.
(3) Since $\mathbb{F}_l \ni a \mapsto a^3 \in \mathbb{F}_l$ is bijective, $X^3 \equiv p \pmod l$ has an integer solution b. Therefore $X^3 - p \equiv (X-b)(X^2+eX+d) \pmod l$. Here (l) is completely decomposed in $k(\sqrt[3]{p})/k$. □

In the following, let p_1, p_2, p_3 be distinct prime numbers such that $p_i \equiv 8 \pmod 9$ $(i = 1, 2, 3)$. We set

$$\mathfrak{p}_1 = (p_1), \quad \mathfrak{p}_2 = (p_2), \quad \mathfrak{p}_3 = (p_3).$$

We will find an equation which plays a role similar to $x^2 - p_1y^2 - p_2z^2 = 0$ in the case of Rédei's theory. Firstly we recall the following theorem by Iwasawa.

Theorem 4.1.2 ([Iw])**.** *Let K be a finite algebraic number field, L a finite Galois extension of K, and let h_K and h_L be class numbers of K and L respectively.*
(1) *If there exists a prime divisor $\mathfrak{p}$ of K which is fully ramified by the extension L/K, then $h_K \mid h_L$. In particular, for any prime number p,*

$$p \mid h_K \Rightarrow p \mid h_L \ \ (\text{or } p \nmid h_L \Rightarrow p \nmid h_K).$$

(2) *If, furthermore, L/K is a cyclic extension of p-power degree and has no ramified prime divisor other than $\mathfrak{p}$, then conversely*

$$p \mid h_L \Rightarrow p \mid h_K \quad (\text{or } p \nmid h_K \Rightarrow p \nmid h_L).$$

Corollary 4.1.3. *The class number of $k(\sqrt[3]{p_1})$ is not divisible by 3.*

Proof. Since the class number of k is 1, Lemma 4.1.1 (2) and Theorem 4.1.2 yield the assertion. □

By Lemma 4.1.1, $\mathfrak{p}_2$ has the following prime decomposition in $k(\sqrt[3]{p_1})$:

$$\mathfrak{p}_2 = \mathfrak{P}_{21}\mathfrak{P}_{22}\mathfrak{P}_{23}, \quad \mathrm{N}\mathfrak{P}_{2i} = p_2^2.$$

Let $\mathfrak{P}$ be one of primes $\mathfrak{P}_{2i}$'s which satisfies $\mathfrak{P}_{2i} = \mathfrak{P}_{2i}^{\tau}$ where $\tau : (\sqrt{-3}, \sqrt[3]{p_1}) \mapsto (-\sqrt{-3}, \sqrt[3]{p_1}) \in \mathrm{Gal}(k(\sqrt[3]{p_1})/\mathbb{Q})$.

Lemma 4.1.4. *There is an algebraic integer α in $k(\sqrt[3]{p_1})$ which satisfies the following properties.*
(1) $\mathrm{N}_{k(\sqrt[3]{p_1})/k}(\alpha) = p_2 s_1^3$ *for some* $s_1 \in k$.

$$\left(\begin{array}{l} For \ \ \alpha = x_1 + x_2\sqrt[3]{p_1} + x_3\sqrt[3]{p_1}^2 \ \ (x_i \in k), \\ \mathrm{N}_{k(\sqrt[3]{p_1})/k}(\alpha) = x_1^3 + p_1x_2^3 + p_1^2x_3^3 - 3p_1x_1x_2x_3. \end{array} \right)$$

(2) *The prime decomposition of (α) in $k(\sqrt[3]{p_1})$ has the following form:*

$$(\alpha) = \mathfrak{P}^m\mathfrak{q}_1^{3n_1}\cdots\mathfrak{q}_r^{3n_r} \quad , \quad (\alpha, 3) = 1,$$

where m and n_i's are positive integers, prime to 3.

Proof. Let h be the class number of $k(\sqrt[3]{p_1})$. There is $\beta \in \mathcal{O}_{k(\sqrt[3]{p_1})}$ such that $\mathfrak{P}^h = (\beta)$ and $\alpha := \beta\tau(\beta) \in \mathbb{Q}(\sqrt[3]{p_1})$. Since $\mathfrak{P} = \mathfrak{P}^{\tau}$, $(\alpha) = \mathfrak{P}^{2h}$ and so

$$\mathrm{N}_{\mathbb{Q}(\sqrt[3]{p_1})/\mathbb{Q}}((\alpha)) = \mathrm{N}_{\mathbb{Q}(\sqrt[3]{p_1})/\mathbb{Q}}\mathfrak{P}^{2h} = \mathrm{N}_{k(\sqrt[3]{p_1})/\mathbb{Q}}\mathfrak{P}^h = (p_2^{2h}).$$

Therefore $\mathrm{N}_{\mathbb{Q}(\sqrt[3]{p_1})/\mathbb{Q}}(\alpha) = \pm p_2^{2h} = (\pm 1)^3 p_2^{2h}$. By Corollary 4.1.3, we find that α satisfies the desired conditions (1) and (2). □

Let α be an element on $\mathcal{O}_{k(\sqrt[3]{p_1})}$ satisfying the properties of Lemma 4.1.4. Let σ be the element of $\mathrm{Gal}(k(\sqrt[3]{p_1})/k)$ defined by

$$\sigma : \sqrt[3]{p_1} \mapsto \omega\sqrt[3]{p_1}.$$

Then we have $\mathrm{Gal}(k(\sqrt[3]{p_1})/k) = \langle\sigma\rangle$. We let

$$\begin{cases} \alpha_1 := \alpha, \\ \alpha_2 := \sigma(\alpha), \\ \alpha_3 := \sigma^2(\alpha), \end{cases} \qquad \begin{cases} \mathfrak{P}_1 := \mathfrak{P}, \\ \mathfrak{P}_2 := \mathfrak{P}^{\sigma}, \\ \mathfrak{P}_3 := \mathfrak{P}^{\sigma^2}. \end{cases}$$

Here we note that $\mathfrak{P}_1, \mathfrak{P}_2$ and $\mathfrak{P}_3$ are distinct prime ideals of $\mathcal{O}_{k(\sqrt[3]{p_1})}$ lying over $\mathfrak{p}_2$. By Lemma 4.1.4, we easily see the following.

Corollary 4.1.5. *We let $\theta := \alpha_1^2\alpha_2 \in \mathcal{O}_{k(\sqrt[3]{p_1})}$. Then we have the followings*:
(1) $\mathrm{N}_{k(\sqrt[3]{p_1})/k}(\theta) = p_2^3 s_2^3$ *for some* $s_2 \in k$.
(2) $(\theta) = \mathfrak{P}_1^{2m}\mathfrak{P}_2^m\mathfrak{A}^3$ $(3 \nmid m,\ \mathfrak{A}$ *is an ideal of* $\mathcal{O}_{k(\sqrt[3]{p_1})})$, $(\theta, 3) = 1$.

In the following, we assume that θ satisfies the conditions (1), (2) of Corollary 4.1.5 and the following condition (4.1.6).

$$\exists\lambda \in \mathcal{O}_{k(\sqrt[3]{p_1})} \text{ s.t. } \lambda^3 \equiv \theta \mod (3\sqrt{-3}). \tag{4.1.6}$$

Definition 4.1.7. We let

$$E := k(\sqrt[3]{p_1}, \sqrt[3]{p_2}, \sqrt[3]{\theta})$$

and we call E the *A-extension* of k.

We let

$$\begin{cases} \theta_1 := \theta = \alpha_1^2\alpha_2, \\ \theta_2 := \sigma(\theta) = \alpha_2^2\alpha_3, \\ \theta_3 := \sigma^2(\theta) = \alpha_3^2\alpha_1. \end{cases}$$

Theorem 4.1.8. (1) *We have* $E = k(\sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3})$.
(2) *The extension E/k is a Galois extension. All prime numbers ramified in the extension E/k are $\mathfrak{p}_1$ and $\mathfrak{p}_2$ with ramification index* 3.

Proof. (1) We have $\theta_1\theta_2^2 = \alpha_1^2\alpha_2\alpha_2^4\alpha_3^2 = p_2^2(\alpha_2 s_1)^3$, $\theta_1\theta_2 = \alpha_1^2\alpha_2^3\alpha_3 = \theta_3^2(\alpha_2/\alpha_3)^3$. By $\sqrt[3]{p_2}, \sqrt[3]{\theta_1} \in E$, $\sqrt[3]{\theta_2}, \sqrt[3]{\theta_3} \in E$. Therefore $k(\sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3}) \subset E$.
Conversely, by $\omega\theta_1 + \theta_2 + \omega^2\theta_3 \in k(\sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3})$, $\sqrt[3]{p_1} \in k(\sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3})$. $\sqrt[3]{\theta_1}\sqrt[3]{\theta_2^2} = \sqrt[3]{p_2^2(\alpha_2 s_1)^3} \in k(\sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3})$. Therefore $\sqrt[3]{p_2} \in k(\sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3})$. Hence $E \subset k(\sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3})$.
(2) E/k is a Galois extension, because E is the splitting field of $\Pi_{i=1}^3(T^3 - \theta_i) = \Pi_{\sigma\in\mathrm{Gal}(k(\sqrt[3]{p_1})/k)}(T^3 - \sigma(\theta_1)) \in \mathbb{Z}[\omega][T]$. We shall show that only $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are ramified in E/k. By Corollary 4.1.5 (2), $\sqrt[3]{\theta_1} \notin k(\sqrt[3]{p_1})$ and so $[k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1}) : k(\sqrt[3]{p_1})] = 3$. Let $\gamma := \sqrt{-3}(\lambda - \sqrt[3]{\theta_1})/3$. Then $\gamma \in \mathcal{O}_{k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1})}$ since γ satisfies $\gamma^3 - \sqrt{-3}\lambda\gamma^2 - \lambda^2\gamma + \sqrt{-3}(\lambda - \theta_1)/9 = 0$ and $\sqrt{-3}(\lambda^3 - \theta_1)/9 \in \mathcal{O}_{k(\sqrt[3]{p_1})}$ by $\lambda^3 \equiv \theta_1 \pmod{3\sqrt{-3}}$((4.1.6)). Since the relative discriminant of γ in $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1})$ is

$$d(\gamma, k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1})/k(\sqrt[3]{p_1})) = \begin{vmatrix} 1 & \gamma_1 & \gamma_1^2 \\ 1 & \gamma_2 & \gamma_2^2 \\ 1 & \gamma_3 & \gamma_3^2 \end{vmatrix}^2 = -\frac{\theta_1^2}{27}\begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix}^2 = \theta_1^2$$

where $\gamma_1 := \gamma = \sqrt{-3}(\lambda - \sqrt[3]{\theta_1})/3$, $\gamma_2 := \sqrt{-3}(\lambda - \omega\sqrt[3]{\theta_1})/3$ and $\gamma_3 := \sqrt{-3}(\lambda - \omega^2\sqrt[3]{\theta_1})/3$. Therefore any prime over 3 is unramified in E/k. On the other hand, by Lemma 1.1.3 and Corollary 4.1.5 (2), only $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are ramified in $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1})/k(\sqrt[3]{p_1})$. Similarly, only $\mathfrak{P}_2$ and $\mathfrak{P}_3$ are ramified in $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_2})/k(\sqrt[3]{p_1})$. Here only $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are ramified in E/k and their ramification indices are 3. □

Theorem 4.1.9. *The extension E/k is a Galois extension whose Galois group is isomorphic to $N_3(\mathbb{F}_3)$.*

Proof. By Theorem 4.1.8, E/k is a Galois extension. We shall show that $[E : k(\sqrt[3]{p_1})] = 9$. Only $\mathfrak{P}_1$, $\mathfrak{P}_2$ and $\mathfrak{P}_3$ are ramified in $k(\sqrt[3]{p_1}, \sqrt[3]{p_2})/k(\sqrt[3]{p_1})$. By Theorem 4.1.8, only $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are ramified in $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1})/k(\sqrt[3]{p_1})$. Therefore $k(\sqrt[3]{p_1}, \sqrt[3]{p_2}) \neq k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1})$. $\mathrm{Gal}(E/k(\sqrt[3]{p_1}))$ is subgroup of $\mathrm{Gal}(k(\sqrt[3]{p_1}, \sqrt[3]{p_2})\,/k(\sqrt[3]{p_1})) \times \mathrm{Gal}(k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1})/k(\sqrt[3]{p_1})) \cong \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$. Hence $[E : k(\sqrt[3]{p_1})] = 9$. Therefore $[E : k] = [E : k(\sqrt[3]{p_1})][k(\sqrt[3]{p_1}) : k] = 27$.

By the computer calculation using GAP, we have the following presentation of the group $N_3(\mathbb{F}_3)$:

$$N_3(\mathbb{F}_3) = \left\langle g_1, g_2, g_3 \;\middle|\; \begin{array}{l} g_1^3 = g_2^3 = g_3^3 = 1 \\ g_1g_2 = g_2g_1g_3,\ g_3g_1 = g_1g_3,\ g_3g_2 = g_2g_3 \end{array} \right\rangle,$$

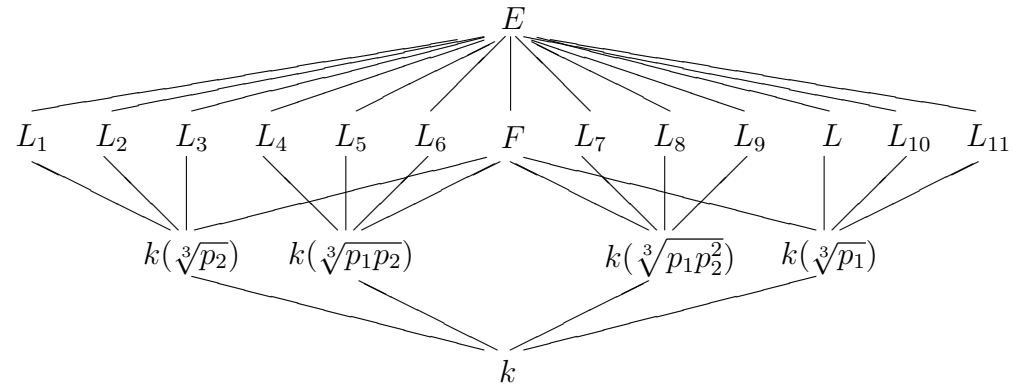
where g_1, g_2 and g_3 are words representing the following matrices respectively:

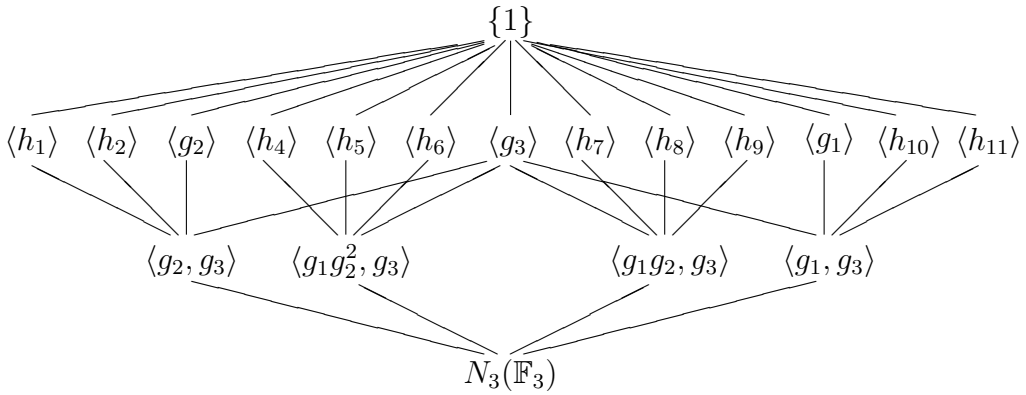
$$g_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We define $\tau_1, \tau_2, \tau_3 \in \mathrm{Gal}(E/\mathbb{Q})$ by

$$\begin{aligned}
\tau_1 :\ & (\sqrt[3]{p_1}, \sqrt[3]{p_2}, \sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3}) \\
& \mapsto (\sqrt[3]{p_1}, \omega\sqrt[3]{p_2}, \sqrt[3]{\theta_1}, \omega^2\sqrt[3]{\theta_2}, \omega\sqrt[3]{\theta_3}) \\
\tau_2 :\ & (\sqrt[3]{p_1}, \sqrt[3]{p_2}, \sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3}) \\
& \mapsto (\omega\sqrt[3]{p_1}, \sqrt[3]{p_2}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3}, \sqrt[3]{\theta_1}) \\
\tau_3 :\ & (\sqrt[3]{p_1}, \sqrt[3]{p_2}, \sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3}) \\
& \mapsto (\sqrt[3]{p_1}, \sqrt[3]{p_2}, \omega\sqrt[3]{\theta_1}, \omega\sqrt[3]{\theta_2}, \omega\sqrt[3]{\theta_3}).
\end{aligned}$$

Then we can easily check $\tau_1^3 = \tau_2^3 = \tau_3^3 = \mathrm{id}$, $\tau_1\tau_2 = \tau_2\tau_1\tau_3$, $\tau_3\tau_1 = \tau_1\tau_3$ and $\tau_3\tau_2 = \tau_2\tau_3$. Thus the correspondence $\tau_i \mapsto g_i$ $(i = 1, 2)$ gives an isomorphism $\mathrm{Gal}(E/k) \simeq N_3(\mathbb{F}_3)$.





where h_i are words representing the following matrices respectively:

$$h_1 = g_2g_3,\ \ h_2 = g_2g_3^2,\ \ h_4 = g_1g_2^2,\ \ h_5 = g_1g_2^2g_3,\ \ h_6 = g_1g_2^2g_3^2,$$
$$h_7 = g_1g_2,\ \ h_8 = g_1g_2g_3,\ \ h_9 = g_1g_2g_3^2,\ \ h_{10} = g_1g_3,\ \ h_{11} = g_1g_3^2.$$

□

We shall show that the field E is independent of the choice of θ_1, namely depends only on $\mathfrak{p}_1$ and $\mathfrak{p}_2$.

Theorem 4.1.10. *The field E is independent of the choice of θ_1.*

Proof. Let θ' be another integers satisfying the conditions (1), (2) in Corollary 4.1.5 and (4.1.6). Then, we have

$$(\theta') = \mathfrak{P}_1^{2m'}\mathfrak{P}_2^{m'}\mathfrak{A}'^3 \ \ (3 \nmid m',\ \ \mathfrak{A}'\text{is an ideal of } \mathcal{O}_{k(\sqrt[3]{p_1})}),\ \ (\theta', 3) = 1.$$

We shall show that $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1}) = k(\sqrt[3]{p_1}, \sqrt[3]{\theta'})$. By $3 \nmid m$ and $3 \nmid m'$, we have $m + m' \equiv 0 \pmod 3$ or we have $m + 2m' \equiv 0 \pmod 3$. If $m + m' \equiv 0 \pmod 3$, we have the following decomposition in $k(\sqrt[3]{p_1})$:

$$(\theta_1\theta') = \mathfrak{P}_1^{2(m+m')}\mathfrak{P}_2^{m+m'}\mathfrak{A}^3\mathfrak{A}'^3.$$

By Lemma 1.1.3, $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1\theta'})/k(\sqrt[3]{p_1})$ is an unramified extension. By class field theory and Corollary 4.1.3, $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1\theta'}) = k(\sqrt[3]{p_1})$. Hence $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1}) = k(\sqrt[3]{p_1}, \sqrt[3]{\theta'})$. If $m + 2m' \equiv 0 \pmod 3$, we have the following decomposition in $k(\sqrt[3]{p_1})$:

$$(\theta_1\theta'^2) = \mathfrak{P}_1^{2(m+2m')}\mathfrak{P}_2^{m+2m'}\mathfrak{A}^3\mathfrak{A}'^6.$$

By Lemma 1.1.3, $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1\theta'^2})/k(\sqrt[3]{p_1})$ is an unramified extension. By class field theory and Corollary 4.1.3, $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1\theta'^2}) = k(\sqrt[3]{p_1})$. Hence $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1}) = k(\sqrt[3]{p_1}, \sqrt[3]{\theta'})$. Hence E is independent of the choice of θ_1. □

Theorem 4.1.11. *Let K be a finite extension of $k(\sqrt[3]{p_1}, \sqrt[3]{p_2})$. Then the following conditions are equivalent.*
(1) *K/k is an A-extension.*
(2) *K/k is an $N_3(\mathbb{F}_3)$-extension such that prime ideal ramified in K/k are only $\mathfrak{p}_1$ and $\mathfrak{p}_2$ with ramification index 3.*

Proof. (1) $\Rightarrow$ (2) is nothing but Theorem 4.1.8 and Theorem 4.1.9. Therefore it suffices to show (2) $\Rightarrow$ (1). By the structure of the group $N_3(\mathbb{F}_3)$, we have four distinct quadratic subextensions of $K/k(\sqrt[3]{p_1})$. Let L be one of these three fields which is different from $k(\sqrt[3]{p_1}, \sqrt[3]{p_2})$. Then there is $\eta \in k(\sqrt[3]{p_1})$ such that $L = k(\sqrt[3]{p_1}, \sqrt[3]{\eta})$ and $K = k(\sqrt[3]{p_1}, \sqrt[3]{p_2}, \sqrt[3]{\eta})$. Then, by Lemma 1.1.3 and the assumption that all primes ramified in K/k are only $\mathfrak{p}_1$ and $\mathfrak{p}_2$ with ramification index 3, we have the following decomposition in $k(\sqrt[3]{p_1})$:

$$(\eta) = \mathfrak{P}_1^{a_1}\mathfrak{P}_2^{a_2}\mathfrak{P}_3^{a_3}\mathfrak{a}^3,$$

where a_1, a_2, a_3 are non-negative integers and $\mathfrak{a}$ is an integral ideal of $k(\sqrt[3]{p_1})$ prime to $\mathfrak{P}_1$, $\mathfrak{P}_2$ and $\mathfrak{P}_3$. We may assume that $a_3 = 0$. In fact, let $a = \min\{a_1, a_2, a_3\}$. Then $\sqrt[3]{\eta/p_2^a} \in K$ and we can take η to be a suitable conjugate of η/p_2^a over k so that $(\eta) = \mathfrak{P}_1^{a_1}\mathfrak{P}_2^{a_2}\mathfrak{a}^3$. We shall show that integers a_1, a_2 satisfies the following condition.

$$a_1 \not\equiv 0 \pmod 3, \quad a_2 \not\equiv 0 \pmod 3, \quad a_1 \not\equiv a_2 \pmod 3.$$

If $a_1 \equiv 0 \pmod 3$, by Lemma1.1.3 and Corollary 4.1.3, only $\mathfrak{P}_2$ are ramified in $L/k(\sqrt[3]{p_1})$ and only $\mathfrak{P}_3$ are ramified in $k(\sqrt[3]{p_1}, \sqrt[3]{\sigma(\eta)})/k(\sqrt[3]{p_1})$. By Lemma1.1.3, $\mathfrak{P}_1$ and $\mathfrak{P}_3$ are ramified in $k(\sqrt[3]{p_1}, \sqrt{p_2\eta})/k(\sqrt[3]{p_1})$ and $k(\sqrt[3]{p_1}, \sqrt{p_2^2\eta})/k(\sqrt[3]{p_1})$. By the structure of the group $N_3(\mathbb{F}_3)$, $k(\sqrt[3]{p_1}, \sqrt[3]{\sigma(\eta)})$ is $k(\sqrt[3]{p_1}, \sqrt{p_2\eta})$ or $k(\sqrt[3]{p_1}, \sqrt{p_2^2\eta})$, which is a contradiction. Therefore $a_1 \not\equiv 0 \pmod 3$. Similarly we can show that $a_2 \not\equiv 0 \pmod 3$, $a_1 \not\equiv a_2 \pmod 3$.

We let $E = k(\sqrt[3]{p_1}, \sqrt[3]{p_2}, \sqrt[3]{\theta_1})$ ($\theta_1 = \mathfrak{P}_1^{2m}\mathfrak{P}_2^m\mathfrak{A}^3,\ 3 \nmid m$) be an A-extension. We shall show that $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1}) = L$. By $a_1 \not\equiv 0 \pmod 3, a_2 \not\equiv 0 \pmod 3$, $a_1 \not\equiv a_2 \pmod 3$, we have $a_1 + 2m \equiv 0 \pmod 3, a_2 + m \equiv 0 \pmod 3$ or we have $2a_1 + 2m \equiv 0 \pmod 3, 2a_2 + m \equiv 0 \pmod 3$. If $a_1 + 2m \equiv 0 \pmod 3, a_2 + m \equiv 0 \pmod 3$, we have the following decomposition in $k(\sqrt[3]{p_1})$:

$$(\theta_1\eta) = \mathfrak{P}_1^{a_1+2m}\mathfrak{P}_2^{a_2+m}\mathfrak{a}^3\mathfrak{A}^3.$$

By Lemma 1.1.3, $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1\eta})/k(\sqrt[3]{p_1})$ is an unramified extension. By class field theory and Corollary 4.1.3, $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1\eta}) = k(\sqrt[3]{p_1})$. Hence $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1}) = L$ and so $E = K$. If $2a_1 + 2m \equiv 0 \pmod 3, 2a_2 + m \equiv 0 \pmod 3$, we have the following decomposition in $k(\sqrt[3]{p_1})$:

$$(\theta_1\eta^2) = \mathfrak{P}_1^{2a_1+2m}\mathfrak{P}_2^{2a_2+m}\mathfrak{a}^6\mathfrak{A}^3.$$

By Lemma 1.1.3, $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1\eta^2})/k(\sqrt[3]{p_1})$ is an unramified extension. By class field theory and Corollary 4.1.3, $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1\eta^2}) = k(\sqrt[3]{p_1})$. Hence $k(\sqrt[3]{p_1}, \sqrt[3]{\theta_1}) = L$ and so $E = K$. □

4.2 Triple cubic residue symbol

We note that the Rédei triple symbol may be defined as the Frobenius automorphism. Let $\mathfrak{Q}$ be a prime ideal of $\mathcal{O}_E$ over $\mathfrak{p}_3$. We have the Frobenius automorphism $\left(\frac{E/k}{\mathfrak{Q}}\right) \in \mathrm{Gal}(E/k)$. By Theorem 4.1.8, the inertia group T of $\mathfrak{Q}$ is $\langle \mathrm{id}_E \rangle$. By Lemma 4.1.1 (3), $\mathfrak{p}_3$ is completely decomposed $k(\sqrt[3]{p_1}, \sqrt[3]{p_2})$. Therefore the decomposition group Z of $\mathfrak{Q}$ is $\langle \mathrm{id}_E \rangle$ or $\langle e \rangle$, where $e : (\sqrt[3]{p_1}, \sqrt[3]{p_2}, \sqrt[3]{\theta_1}) \mapsto (\sqrt[3]{p_1}, \sqrt[3]{p_2}, \omega\sqrt[3]{\theta_1})$. Then we can easily check $Z \subset \{a \in \mathrm{Gal}(E/k) \mid ab = ba, \text{for all } b \in \mathrm{Gal}(E/k)\}$. Therefore the Frobenius automorphism $\left(\frac{E/k}{\mathfrak{Q}}\right) \in Z (\subset \mathrm{Gal}(E/k))$ is independent of the choice of a prime ideal of $\mathcal{O}_E$ over $\mathfrak{p}_3$. Therefore the following definition is well-defined.

Definition 4.2.1. We define the *triple cubic residue symbol* by

$$[\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3]_3 := \frac{\left(\frac{E/k}{\mathfrak{Q}}\right)(\sqrt[3]{\theta_1})}{\sqrt[3]{\theta_1}} \in \{1, \omega, \omega^2\}.$$

By Theorem 4.1.11, we easily see the following.

Theorem 4.2.2. *We have*

$$[\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3]_3 = [\mathfrak{p}_2, \mathfrak{p}_1, \mathfrak{p}_3]_3.$$

Example 4.2.3. Let $(p_1, p_2) := (17, 53)$. Then we have

$$\begin{cases} \alpha_1 = 8 - 3\sqrt[3]{17}, \\ \alpha_2 = 8 - 3\omega\sqrt[3]{17}, \\ \alpha_3 = 8 - 3\omega^2\sqrt[3]{17}, \end{cases} \quad \begin{cases} \theta_1 = \alpha_1^2\alpha_2, \\ \theta_2 = \alpha_2^2\alpha_3, \\ \theta_3 = \alpha_3^2\alpha_1. \end{cases}$$

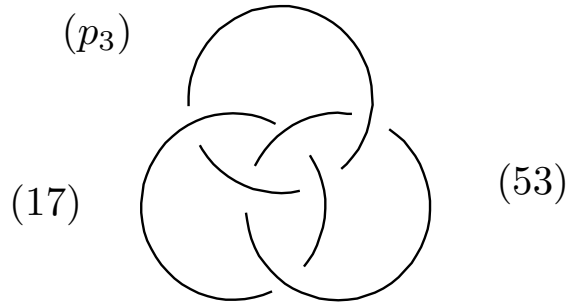
Then θ_1 satisfies the conditions (1), (2) in Corollary 4.1.5. Since $\alpha_1 \equiv \alpha_2 \mod (3\sqrt{-3})$, $\alpha_1^3 \equiv \theta_1 \mod (3\sqrt{-3})$ and so (4.1.6) is also satisfied. Hence

$$E = k(\sqrt[3]{p_1}, \sqrt[3]{p_2}, \sqrt[3]{\theta_1}).$$

Suppose $p_3 = 71, 89, 107, 179, 197$. Then we have

$[(17), (53), (71)]_3 = \omega^2$, $[(17), (53), (89)]_3 = \omega$, $[(17), (53), (107)]_3 = \omega^2$, $[(17), (53), (179)]_3 = \omega$, $[(17), (53), (197)]_3 = \omega$.

So there triples of primes $\{(17), (53), (p_3)\}$ are Borromean primes in $\mathrm{Spec}(\mathcal{O}_k)$.



Bibliography

[Am1] F. Amano, On Rédei's dihedral extension and triple reciprocity law, Proc. Japan Acad., **90**, Ser. A (2014) 1–5.

[Am2] F. Amano, On a certain nilpotent extension over $\mathbb{Q}$ of degree 64 and the 4-th multiple residue symbol, to appear in Tohoku Math. J.

[Am3] F. Amano, On a certain nilpotent extension over $\mathbb{Q}$ of degree 64 and the 4-th multiple residue symbol, RIMS kokyuroku Bessatsu B**44**, Algebraic Number Theory and Related Topics 2011, (edited by N. Suwa, A. Shiho and K. Sato), December, 2013 RIMS Kyoto University. 41–49.

[Am4] F. Amano, H. Kodani, M. Morishita, T. Sakamoto and T. Yoshida, Rédei's Triple Symbols and Modular Forms, wish Appendix by T. Ogasawara, Tokyo J. Math., **36**, No, 2, (2013). 405–427.

[Ar] S. Arno, The imaginary quadratic field of class number 4, Acta Arith. **60** (1992), no. 4, 321–334.

[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.

[Fu] G. Fujisaki, Introduction to Algebraic Number Theory (Japanese), Shokabo, 1975.

[FV] I. B. Fesenko, S. V. Vostokov, Local fields and their extensions. Second edition. Translations of Mathematical Monographs, **121**. American Mathematical Society, Providence, RI, 2002.

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

[H] E. Hecke, Zur Theorie der elliptischen Modulfunktionen, Math. Ann. **97** (1927), no. 1, 210–242.

[HM] T. Hiramatsu, Y. Mimura, The modular equation and modular forms of weight one, Nagoya Math. J. **100** (1985), 145–162.

[Ih] 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.

[Iw] K. Iwasawa, A note on class numbers of algebraic number fields, Abh. Math. Sem. Hamburg, **20** (1956), 257–258.

[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-extensions with given ramification, Appendix in: K. Haberland, Galois cohomology of algebraic number fields, VEB Deutscher Verlag der Wissenschaften, Berlin, (1978) 89–126.

[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.

[Mk] T. Miyake, Modular Forms, Springer Monographs in Mathematics, Springer, 2006.

[Mo1] M. Morishita, Milnor's link invariants attached to certain Galois groups over $\mathbf{Q}$, Proc. Japan Acad. Ser, A **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.

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

[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.

[Od] T. Oda, Note on meta-abelian quotients of pro-l free groups, (1985), preprint.

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

[Sa] S. Saito, Number Theory (Japanese), Kyoritsu, 1997.

[Se] J.-P. Serre, Modular forms of weight one and Galois representations, In: Algebraic number fields: L -functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 193–268.

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

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

[WS] H. Wada, M. Saito, A Table of Ideal Class Groups of Imaginary Quadratic Fields, Sophia Kôkyûroku in Mathematics, **28** (1988).

[Wat] M. Watkins, Class numbers of imaginary quadratic fields, Math. Comp. **73** (2004), no. 246, 907–938.

[Z] D. Zagier, Elliptic modular forms and their application, In: *The 1-2-3 of Modular Forms*, Universitext, Springer, 1-103.