

Arithmetic Milnor invariants and multiple power residue symbols in number fields: a précis

By

Masanori MORISHITA*

Abstract

This is a research announcement of my joint work with Fumiya Amano [AM] concerning a generalization of the Legendre, power residue symbols and the Rédei triple symbol. Such a generalization was firstly discussed by the author at the conference “Algebraic number theory and related topics (2000)” [Mo2]. Afterwards, a significant progress was made by Amano on the 4-tuple quadratic residue symbol over the rationals [A2], and now we are able to introduce n -tuple m -th power residue symbols for primes of a number field.

Introduction

Our work is motivated originally by the works of Gauss, about two hundred years ago, on arithmetic of quadratic residue and topology of linking numbers [G1], [G2].

For distinct odd rational primes p_1 and p_2 , the quadratic residue symbol is given by

$$\left(\frac{p_1}{p_2}\right) = \text{Frobenius over } p_2 \text{ in } \text{Gal}(\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}).$$

In view of the analogies between knots and primes [Mo5], it may be regarded as an arithmetic analogue of the mod 2 linking number, $\text{lk}_2(p_1, p_2) \in \mathbb{Z}/2\mathbb{Z}$:

$$\left(\frac{p_1}{p_2}\right) = (-1)^{\text{lk}_2(p_1, p_2)}.$$

In the 19th century, Kummer and Hilbert etc. generalized the quadratic residue symbol to higher power residue symbols in number fields. Let k be a number field

Received March 30, 2015. Revised July 15, 2015.

2010 Mathematics Subject Classification(s): 11R32, 57M05, 57M25.

Key Words: Pro- l Galois groups of link type, Arithmetic Milnor invariants, Multiple power residue symbols, Massey products.

Partly supported by Grants-in-Aids for Scientific Research (B) 24340005.

*Faculty of Mathematics, Kyushu University, 744, Motooka, Fukuoka 819-0395, Japan.

e-mail: morisita@math.kyushu-u.ac.jp

containing a primitive m -th root of unity ($m \geq 2$). For distinct principal prime ideals $\mathfrak{p}_1 = (\pi_1)$ and $\mathfrak{p}_2 = (\pi_2)$, prime to m , the m -th power residue symbol is given as

$$\left(\frac{\mathfrak{p}_1}{\mathfrak{p}_2}\right)_m = \text{Frobenius over } \mathfrak{p}_2 \text{ in } \text{Gal}(k(\sqrt[m]{\pi_1})/k).$$

Note that it is natural to assume \mathfrak{p}_i is principal, namely, “null-homologous” in $\text{Spec}(\mathcal{O}_k)$, in order to define the mod m linking number $\text{lk}_m(\mathfrak{p}_1, \mathfrak{p}_2) \in \mathbb{Z}/m\mathbb{Z}$. It may be noteworthy that Hilbert already discussed the power residue symbol for non-principal ideals in § 154 of his *Zahlbericht* [H].

In 1939, Rédei introduced the triple symbol aiming to generalize the arithmetic of quadratic fields such as Gauss’ theory of genera [R]. For distinct certain rational primes p_1, p_2 and p_3 , the Rédei symbol is defined well as

$$[p_1, p_2, p_3]_{\text{Rédei}} = \text{Frobenius over } p_3 \text{ in } \text{Gal}(\mathfrak{R}/\mathbb{Q}),$$

where \mathfrak{R} is determined by p_1, p_2 and given concretely by

$$\mathfrak{R} = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha}),$$

where $\alpha = x + y\sqrt{p_1}$, $x^2 - p_1y^2 - p_2z^2 = 0$ ($x, y, z \in \mathbb{Z}$). Note that \mathfrak{R}/\mathbb{Q} is a dihedral extension of degree 8, unramified outside p_1, p_2 and ∞ with ramification index for each p_i being 2. It might not be clear, however, why such a dihedral extension and triple symbol should be considered as a natural generalization of a quadratic field and the Legendre symbol, and it seemed that his work had been overlooked for a long time.

In the late 1990s, Kapranov and the author independently interpreted the Rédei symbol as an arithmetic analogue of a triple linking number for a link [Mi]. For example, the primes 13, 61 and 937 are linked like the Borromean ring [V].

Further the author introduced arithmetic analogues for rational primes of the Milnor invariants (higher order linking numbers) for a link in the 3-sphere [Mo1]-[Mo5]. For example, the mod 2 arithmetic Milnor invariant

$$\mu_2(12 \cdots n) \in \mathbb{Z}/2\mathbb{Z}$$

for certain rational primes p_1, p_2, \dots, p_n describes the decomposition law of p_n in a certain extension $K(n)/\mathbb{Q}$, determined by p_1, \dots, p_{n-1} , which has the following property:

- $K(n)/\mathbb{Q}$ is unramified outside p_1, \dots, p_{n-1} and ∞ with ramification index for each p_i being 2, and the Galois group $\text{Gal}(K(n)/\mathbb{Q}) \simeq N_n(\mathbb{F}_2)$,

where $N_n(R)$ stands for the group of n by n upper-triangular unipotent matrices over a commutative ring R . In particular, we have

$$(-1)^{\mu_2(12)} = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}, \quad (-1)^{\mu_2(123)} = [p_1, p_2, p_3]_{\text{R\'edei}},$$

and further

$$K(2) = \mathbb{Q}(\sqrt{p_1}), \quad K(3) = \mathfrak{K}$$

for $p_i \equiv 1 \pmod{4}$ ([A1], [Mo1]-[Mo4]). This unified interpretation may tell us that R\'edei's dihedral extension and triple symbol would be a natural generalization of a quadratic field and the Legendre symbol.

The idea is based on an analogy

$$\begin{array}{ccc} \pi_1^{\text{\'et}}(\text{Spec}(\mathbb{Z}) \setminus \{p_1, \dots, p_n\})(2) & \longleftrightarrow & \pi_1(\mathbb{R}^3 \setminus \{K_1, \dots, K_n\}) \\ \text{pro-2 Galois group} & & \text{link group,} \end{array}$$

where $\pi_1^{\text{\'et}}(\cdot)(l)$ means the maximal pro- l quotient for a prime number l of the \'etale fundamental group $\pi_1^{\text{\'et}}(\cdot)$. Using this analogy, we pursue the analogies in arithmetic of the theory of Milnor invariants in link theory.

Since the Milnor invariants are defined for a link in a homology 3-sphere [T], it would be natural to ask the following

Question: Can we extend mod 2 arithmetic Milnor invariants to mod m arithmetic Milnor invariants for a finite set S of finite primes in a number field k which contains a primitive m -th root of unity and whose class group $H_k = 1$?

However, we are faced immediately with the following difficulty: There is an obstruction B_S for the analogy

$$(\star) \quad \pi_1^{\text{\'et}}(\text{Spec}(\mathcal{O}_k) \setminus S)(l) \longleftrightarrow \pi_1(M \setminus \mathcal{L}),$$

where l is a certain prime number and \mathcal{L} is a link in a 3-manifold M . We note that the obstruction B_S is closely related to the group of units \mathcal{O}_k^\times .

Despite of this difficulty, we have the following

Result (rough form): Suppose that m is a power of l and that k contains a primitive m -th root of unity ζ_m and the l -class group $H_k(l) = 1$. Then we can introduce mod m arithmetic Milnor invariants $\mu_m(12 \cdots n) \in \mathbb{Z}/m\mathbb{Z}$ for a certain set $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ of finite primes of k and the n -tuple m -th power residue symbol in the manner

$$[\mathfrak{p}_1, \dots, \mathfrak{p}_n]_m = \zeta_m^{\mu_m(1 \dots n)}.$$

The idea is simple. Namely, we enlarge S so that the obstruction vanishes and we have the analogy (\star) , and then we show our invariants are independent of a choice of added auxiliary primes.

Throughout this article, we shall use the following

Notations: $l :=$ a fixed prime number, $m :=$ a fixed power of l .

$k =$ a finite algebraic number field such that k contains a fixed primitive m -th root of unity ζ_m and the l -class group $H_k(l) = 1$.

$S := \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} =$ a finite set of finite primes \mathfrak{p}_i of k with $(\mathfrak{p}_i, l) = 1$. Note that $N\mathfrak{p}_i \equiv 1 \pmod{m}$ ($1 \leq i \leq n$).

$k_{\mathfrak{p}_i} :=$ the \mathfrak{p}_i -adic completion of k .

$S_\infty :=$ the set of infinite primes of k .

$l_S := \max\{l^e \mid N\mathfrak{p}_i \equiv 1 \pmod{l^e} \text{ for } i = 1, \dots, n\}$.

$k_S(l) :=$ the maximal pro- l Galois extension of k , unramified outside $S \cup S_\infty$.

$G_{k,S}(l) := \text{Gal}(k_S(l)/k) = \pi_1^{\text{ét}}(\text{Spec}(\mathcal{O}_k) \setminus S)(l)$.

§ 1. Obstructions and pro- l Galois groups of link type

The *obstruction* B_S is defined by the \mathbb{F}_l -vector space

$$B_S := \{a \in k^\times \mid (a) = \mathfrak{a}^l, a \in (k_{\mathfrak{p}}^\times)^l \text{ for } \mathfrak{p} \in S \cup S_\infty\} / (k^\times)^l.$$

The following theorem is due to Koch.

Theorem 1.1 ([K, 11.4]). *Assume $B_S = 1$. Then we have*

$$G_{k,S}(l) = \langle x_1, \dots, x_n \mid x_i^{N\mathfrak{p}_i-1} [x_i, y_i] = 1 \ (i = 1, \dots, n) \rangle,$$

where x_i is a word representing a monodromy over \mathfrak{p}_i and y_i is a pro- l word of x_i 's representing a Frobenius automorphism over \mathfrak{p}_i .

The obstruction is closely related to the group of units \mathcal{O}_k^\times . We let

$$\mathcal{E}_k := \{\mathfrak{p} : \text{finite prime of } k \mid (\mathfrak{p}, l) = 1, \mathfrak{p} \text{ is inert in } k(\sqrt[l]{\mathcal{O}_k^\times})/k\},$$

which is an infinite set by the Chebotarev density theorem.

Proposition 1.2 ([AM]). *If S contains a prime in \mathcal{E}_k , then $B_S = 1$.*

Example 1.3. (1) Let $k = \mathbb{Q}$ and $l = 2$. Then we have $B_S = 1$ for any S .
 (2) Let $k = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ and $l = 3$. Then $B_S = 1$ if and only if S contains a prime \mathfrak{p} such that $N\mathfrak{p} \equiv 4$ or $7 \pmod{9}$.

§ 2. Arithmetic Milnor invariants and multiple power residue symbols

By Theorem 1.1 and Proposition 1.2, we can enlarge S to $T = S \cup \{\mathfrak{p}_{n+1}, \dots, \mathfrak{p}_t\}$ so that $B_T = 1$ and

$$G_{k,T}(l) = \langle x_1, \dots, x_t \mid x_i^{N\mathfrak{p}_i-1}[x_i, y_i] = 1 \ (i = 1, \dots, t) \rangle = F/N,$$

where F is the free pro- l group on the words x_1, \dots, x_t and N is the closed subgroup of F generated normally by $x_i^{N\mathfrak{p}_i-1}[x_i, y_i]$ ($i = 1, \dots, t$). We let

$$\Theta : F \longrightarrow \mathbb{Z}/m\mathbb{Z}\langle\langle X_1, \dots, X_t \rangle\rangle^\times$$

be the mod m Magnus expansion defined by $\Theta(x_i) := 1 + X_i$ for $1 \leq i \leq t$. We write, for $f \in F$,

$$\Theta(f) = 1 + \sum_{1 \leq i_1, \dots, i_r \leq t} \mu_m(i_1 \cdots i_r; f) X_{i_1} \cdots X_{i_r}$$

and set

$$\mu_m(i_1 \cdots i_a) := \mu_m(i_1 \cdots i_{a-1}; y_{i_a}) \quad (a > 1),$$

and $\mu_m(i) := 0$ ($1 \leq i \leq t$). Define $\Delta_m(1 \cdots n)$ by the ideal of $\mathbb{Z}/m\mathbb{Z}$ generated by $\mu_m(J)$ (multi-indices J running over all cyclic permutations of proper subsequence of $1 \cdots n$) and the binomial coefficients $\binom{l_S}{a}$ ($1 \leq a < n$), and we let

$$\bar{\mu}_m(1 \cdots n) := \mu_m(1 \cdots n) \pmod{\Delta_m(1 \cdots n)}.$$

Theorem 2.1 ([AM]). *Suppose $2 \leq n < l_S$. Then $\bar{\mu}_m(1 \cdots n)$ is an invariant of determined by the n -tuple $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ and m , more precisely, it is independent of choices of a monodromy and an extension of Frobenius over \mathfrak{p}_i ($1 \leq i \leq t$) and is independent of a choice of T .*

We call $\bar{\mu}_m(1 \cdots n)$ the mod m arithmetic Milnor invariant of the n -tuple $\mathfrak{p}_1, \dots, \mathfrak{p}_n$.

In the following, we assume for simplicity $\binom{l_S}{a} \equiv 0 \pmod{m}$ ($1 \leq a < n$) and $\mu_m(j_1 \cdots j_a) = 0$ for any proper subset $\{j_1, \dots, j_a\}$ of $\{1, \dots, n\}$.

We then define the n -tuple m -th power residue symbol by

$$[\mathfrak{p}_1, \dots, \mathfrak{p}_n]_m := \zeta_m^{\mu_m(1 \cdots n)}.$$

We will discuss some properties of our multiple power residue symbols. We define a homomorphism

$$\rho_{m,n} : F \longrightarrow N_n(\mathbb{Z}/m\mathbb{Z})$$

by

$$\rho_{m,n}(f) := \begin{pmatrix} 1 & \mu_m(1; f) & \mu_m(12; f) & \cdots & \mu_m(1 \cdots n - 1; f) \\ 0 & 1 & \mu_m(2; f) & \cdots & \mu_m(2 \cdots n - 1; f) \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & \mu_m(n - 1; f) \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}.$$

It is easily shown that $\rho_{m,n}$ factors through the Galois group $G_{k,T}(l)$.

Theorem 2.2 ([AM]). *Let $K_m(n)$ be the subfield of $k_T(l)$ fixed by $\text{Ker}(\rho_{m,n})$. Then the followings hold.*

- (1) $K_m(n)$ depends only on S .
- (2) $K_m(n)/k$ is unramified outside $\mathfrak{p}_1, \dots, \mathfrak{p}_{n-1}$ and S_∞ with ramification index for each \mathfrak{p}_i being m , and $\text{Gal}(K_m(n)/k) \simeq N_n(\mathbb{Z}/m\mathbb{Z})$.
- (3) \mathfrak{p}_n is completely decomposed in $K_m(n)/k$ if and only if $[\mathfrak{p}_1, \dots, \mathfrak{p}_n]_m = 1$.

In view of Theorem 2.2, the following problem is important in the arithmetic of multiple power residue symbols.

- Problem 2.3.** (i) Does the property (2) of Theorem 2.2 characterize $K_m(n)$ uniquely ?
- (ii) Can one construct $K_m(n)$ in a concrete manner ?

Example 2.4. (1) Let $n = 2$. The classical Kummer and Hilbert theory answers Problem 2.3 affirmatively and we have

$$[\mathfrak{p}_1, \mathfrak{p}_2]_m = \left(\frac{\pi_1}{\mathfrak{p}_2} \right)_m \text{ for } \mathfrak{p}_1 = (\pi_1).$$

(2) Let $k = \mathbb{Q}$, $l = m = 2$ and $n = 3$. Amano [A1] answers Problem 2.3 affirmatively so that $K_2(3)$ coincides with Rédei's dihedral extension \mathfrak{R} , and we have

$$[p_1, p_2, p_3]_2 = [p_1, p_2, p_3]_{\text{Rédei}}.$$

(3) (Triple cubic residue symbol) This is a new case where $k = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, $l = m = 3$ and $n = 3$. Let $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$ with $N\mathfrak{p}_i \equiv 1 \pmod{9}$. Then there is $\pi_i \in \mathbb{Z}[\zeta_3]$ uniquely such that $\mathfrak{p}_i = (\pi_i)$ and $\pi_i \equiv 1 \pmod{(1 - \zeta_3)^3}$. Assume that

$$\left(\frac{\pi_i}{\pi_j} \right)_3 = 1 \quad (i \neq j).$$

By Theorem 2.2, the extension $K_3(3)/k$ is a mod 3 Heisenberg extension of degree 27, unramified outside $\mathfrak{p}_1, \mathfrak{p}_2$ with ramification index for each prime \mathfrak{p}_i being 3. Then we have the following theorem.

Theorem 2.5 ([AM]). (1) *The property (2) of Theorem 2.2 with $m = n = 3$ characterizes $K_3(3)$ uniquely and we have*

$$K_3(3) = k(\sqrt[3]{\pi_1}, \sqrt[3]{\pi_2}, \sqrt[3]{\theta}),$$

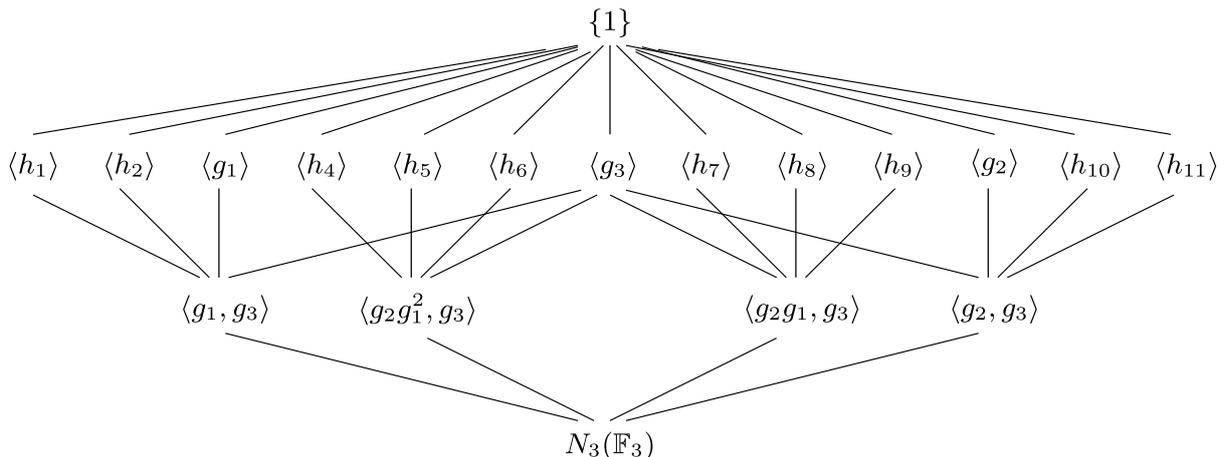
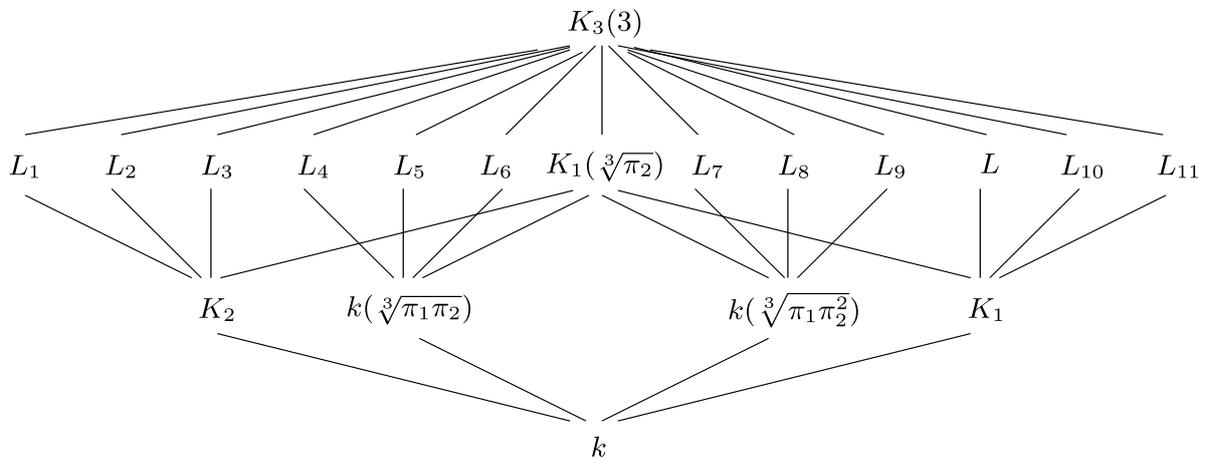
where $\theta = x + y\sqrt[3]{\pi_1} + z(\sqrt[3]{\pi_1})^2$ is an algebraic integer in $k(\sqrt[3]{\pi_1})$ satisfying $x^3 + \pi_1 y^3 + \pi_1^2 z^3 - 3\pi_1 xyz - \pi_2^3 w^2 = 0$ ($x, y, z, w \in \mathbb{Z}[\zeta_3]$). (For more detailed requirements of θ , refer to [AM; Section 4])

(2) *We have*

$$[\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3]_3 = \frac{\text{Frob}_{\mathfrak{p}_3}(\sqrt[3]{\theta})}{\sqrt[3]{\theta}},$$

where $\text{Frob}_{\mathfrak{p}_3}$ is an extension of Frobenius automorphism over \mathfrak{p}_3 in $K_3(3)/k$.

All subgroups of $\text{Gal}(K_3(3)/k)$ and the corresponding intermediate fields are illustrated as follows.



$$N_3(\mathbb{F}_3) = \left\langle g_1, g_2, g_3 \left| \begin{array}{l} g_1^3 = g_2^3 = g_3^3 = 1 \\ g_2g_1 = g_3g_2g_1, g_3g_1 = g_1g_3, g_3g_2 = g_2g_3 \end{array} \right. \right\rangle,$$

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

$$\begin{aligned} g_1 &: (\sqrt[3]{\pi_1}, \sqrt[3]{\pi_2}, \sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3}) \mapsto (\zeta_3 \sqrt[3]{\pi_1}, \sqrt[3]{\pi_2}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3}, \sqrt[3]{\theta_1}), \\ g_2 &: (\sqrt[3]{\pi_1}, \sqrt[3]{\pi_2}, \sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3}) \mapsto (\sqrt[3]{\pi_1}, \zeta_3 \sqrt[3]{\pi_2}, \sqrt[3]{\theta_1}, \zeta_3^2 \sqrt[3]{\theta_2}, \zeta_3 \sqrt[3]{\theta_3}), \\ g_3 &: (\sqrt[3]{\pi_1}, \sqrt[3]{\pi_2}, \sqrt[3]{\theta_1}, \sqrt[3]{\theta_2}, \sqrt[3]{\theta_3}) \mapsto (\sqrt[3]{\pi_1}, \sqrt[3]{\pi_2}, \zeta_3^2 \sqrt[3]{\theta_1}, \zeta_3^2 \sqrt[3]{\theta_2}, \zeta_3^2 \sqrt[3]{\theta_3}), \end{aligned}$$

where $\theta_1 := \theta, \theta_2 := g_1(\theta), \theta_3 := g_1^2(\theta)$.

$$\begin{aligned} h_1 &= g_1g_3, & h_2 &= g_1g_3^2, & h_4 &= g_2g_1^2, & h_5 &= g_2g_1^2g_3, & h_6 &= g_2g_1^2g_3^2, \\ h_7 &= g_2g_1, & h_8 &= g_2g_1g_3, & h_9 &= g_2g_1g_3^2, & h_{10} &= g_2g_3, & h_{11} &= g_2g_3^2. \end{aligned}$$

§ 3. Massey products

It is known that Milnor invariants of a link are interpreted as Massey products in the cohomology of the link complement [T]. Similarly, we can interpret our multiple power residue symbols as Massey products in the étale cohomology of the complement $\mathfrak{X} := \text{Spec}(\mathcal{O}_k) \setminus T$, where T is, as in §2, a finite set containing S such that $B_T = 1$. This is a generalization of the cup product interpretation of the power residue symbol [S]. We keep the same notations as in Section 2.

In order to define the Massey product structure in étale cohomology, we use Verdier's construction of étale cohomology presented in [AGV; Exposé V]. Let U_\bullet be a hypercovering on $\mathfrak{X}_{\text{ét}}$ and let $C^j := C^j(U_\bullet, \mathbb{Z}/m\mathbb{Z})$ be the Čech j -cochains ($j \geq 0$) associated to U_\bullet with coefficients in the constant sheaf $\mathbb{Z}/m\mathbb{Z}$. Consider the differential graded algebra $(C^\bullet := \bigoplus_{j \geq 0} C^j, d^\bullet)$ equipped with multiplication given by the Alexander-Whitney cup product \cup . Then, by the general procedure to define Massey products [Ma], we have the Massey product structure on the étale cohomology $H^\bullet(\mathfrak{X}_{\text{ét}}, \mathbb{Z}/m\mathbb{Z}) = \varinjlim H^*(C^\bullet(U_\bullet, \mathbb{Z}/m\mathbb{Z}))$, where the limit is taken over the homotopy category of hypercoverings U_\bullet .

Let us explain concretely the triple Massey product concerning Example 2.4 (3). For the general case, we refer to [AM; Section 5]. Let $\chi_i \in H^1(\mathfrak{X}_{\text{ét}}, \mathbb{Z}/m\mathbb{Z})$ be the Kronecker dual to the monodromies $x_j \in G_{k,T}(3)$, namely, $\chi_i(x_j) = \delta_{ij}$ for $1 \leq i, j \leq \#T$. By the

assumption $\left(\frac{\pi_i}{\pi_j}\right)_3 = 1$ ($i \neq j$), we have $\chi_{12}, \chi_{23} \in C^1$ such that

$$\chi_1 \cup \chi_2 = d\chi_{12}, \quad \chi_2 \cup \chi_3 = d\chi_{23}.$$

Then the triple Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle \in H^2(\mathfrak{X}_{\text{ét}}, \mathbb{Z}/m\mathbb{Z})$ is defined by the cohomology class of the 2-cocycle

$$\chi_1 \cup \chi_{23} + \chi_{12} \cup \chi_3.$$

On the other hand, let $\delta_3 \in H_2(\mathfrak{X}_{\text{ét}}, \mathbb{Z}/m\mathbb{Z})$ be the image of the canonical generator of $H_2(\text{Spec}(k_{\mathfrak{p}_3})_{\text{ét}}, \mathbb{Z}/m\mathbb{Z})$, which represents a “boundary of a tubular neighborhood” of $\text{Spec}(\mathcal{O}_k/\mathfrak{p}_3)$, under the natural homomorphism $H_2(\text{Spec}(k_{\mathfrak{p}_3})_{\text{ét}}, \mathbb{Z}/m\mathbb{Z}) \rightarrow H_2(\mathfrak{X}_{\text{ét}}, \mathbb{Z}/m\mathbb{Z})$.

Theorem 3.1 ([AM]). $[\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3]_3 = \zeta_3^{-\langle \chi_1, \chi_2, \chi_3 \rangle(\delta_3)}$.

Finally we present an important problem left unsolved:

Problem (reciprocity law). Study the behavior of $[\mathfrak{p}_1, \dots, \mathfrak{p}_n]_m$ under permutations of $\mathfrak{p}_1, \dots, \mathfrak{p}_n$.

References

- [A1] Amano, F., On Rédei’s dihedral extension and triple reciprocity law, Proc. Japan Acad., **90**, Ser. A (2014), 1–5.
- [A2] Amano, F., On a certain nilpotent extension over \mathbb{Q} of degree 64 and the 4-th multiple residue symbol, Tohoku Math. J. **66** No.4 (2014), 501–522.
- [A3] Amano, F., Arithmetic of nilpotent extensions and multiple residue symbols, Thesis, Kyushu University, 2014.
- [AGV] Artin, M., Grothendieck, A. and Verdier, J.-L., Théorie des topos et cohomologie étale des schémas, SGA4 Tome 2, Lecture Notes in Mathematics, vol. **270** Springer, Berlin-New York 1972.
- [AM] Amano, F., Morishita, M., Arithmetic Milnor invariants and multiple power residue symbols in number fields, arXiv:1412.6894.
- [G1] Gauss, C. F., Disquisitiones arithmeticae, Translated into English by A. Arthur, S. J. Clarke, Yale University Press, New Haven, Conn.-London 1966.
- [G2] Gauss, C. F., Zur mathematischen Theorie der electrodynamischen Wirkungen, Werke **V**, (1833), p 605.
- [H] Hilbert, D., Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Abhandlungen. Band I: Zahlentheorie. Zweite Auflage Springer, 1970.
- [K] Koch, H., Galoissche Theorie der p -Erweiterungen, Springer-Verlag, VEB Deutscher Verlag der Wissenschaften, Berlin, 1970.
- [Ma] May, J. P., Matric Massey products, J. Algebra **12** (1969), 533–568.

- [Mi] Milnor, J., Isotopy of links, in Algebraic Geometry and Topology, A symposium in honor of S. Lefschetz (edited by R.H. Fox, D.C. Spencer and A.W. Tucker), 280–306 Princeton University Press, Princeton, N.J., 1957.
- [Mo1] Morishita, M., Milnor’s link invariants attached to certain Galois groups over \mathbf{Q} , Proc. Japan Acad. Ser. A **76** (2000), 18–21.
- [Mo2] Morishita, M., Knots and primes, 3-manifolds and number fields (Japanese), Algebraic number theory and related topics (2000), RIMS Kôkyûroku **200** (2001), 103 – 115.
- [Mo3] Morishita, M., On certain analogies between knots and primes, J. Reine Angew. Math. **550** (2002), 141–167.
- [Mo4] Morishita, M., Milnor invariants and Massey products for prime numbers, Compos. Math., **140** (2004), 69–83.
- [Mo5] Morishita, M., Knots and Primes - An introduction to arithmetic topology, Universitext, Springer, London, 2012.
- [R] Rédei, L., Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper I, J. Reine Angew. Math., **180** (1939), 1-43.
- [S] Serre, J.-P., Corps locaux, Publications de l’Université de Nancago, Hermann, Paris, 1968.
- [T] Turaev, V., The Milnor invariants and Massey products, (Russian) Studies in topology, II. Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **66**, (1976), 189–203, 209–210.
- [V] Vogel, D., On the Galois group of 2-extensions with restricted ramification, J. Reine Angew. Math., **581** (2005), 117–150.