Arithmetic topology in Ihara theory II: Milnor invariants, dilogarithmic Heisenberg coverings and triple power residue symbols

Hikaru HIRANO and Masanori MORISHITA

Dedicated to Professor Yasutaka Ihara

Abstract: We introduce mod $l$ Milnor invariants of a Galois element associated to Ihara’s Galois representation on the pro-$l$ fundamental group of a punctured projective line ($l$ being a prime number), as arithmetic analogues of Milnor invariants of a pure braid. We then show that triple quadratic (resp. cubic) residue symbols of primes in the rational (resp. Eisenstein) number field are expressed by mod 2 (resp. mod 3) triple Milnor invariants of Frobenius elements. For this, we introduce dilogarithmic mod $l$ Heisenberg ramified covering $D^{(l)}$ of $\mathbb{P}^1$, which may be regarded as a higher analog of the dilogarithmic function, for the gerbe associated to the mod $l$ Heisenberg group, and we study the monodromy transformations of certain functions on $D^{(l)}$ along the pro-$l$ longitudes of Frobenius elements for $l = 2, 3$.

Introduction

In [KMT], following the analogy between the Artin representation of a pure braid group and the Ihara representation of the absolute Galois group $\text{Gal}_k := \text{Gal}(\overline{k}/k)$ of a number field $k$ on the pro-$l$ fundamental group of a punctured projective line ([I1],[I2]), $l$-adic Milnor invariants $\overline{\mu}^{(l)}(g; I) := \mu^{(l)}(g; I) \mod \Delta(g; I)$ of each Galois element $g \in \text{Gal}_k$ were introduced as arithmetic analogues of Milnor invariants of a pure braid ([MK; Chapter 6, 4],[Kd; 1.2]), where $l$ is a prime number, $I$ is a multi-index representing punctured points and $\Delta(g; I)$ is a certain indeterminacy (cf. Subsection 1.3). They were shown to enjoy some properties similar to those of Milnor invariants of pure braids. In principle, the information on the Ihara representation is encoded in $l$-adic Milnor numbers $\mu^{(l)}(g; I)$ for all $g$ and $I$.

2010 Mathematics Subject Classification: 11R, 57M
Key words: Ihara representation, mod $l$ Milnor invariants, dilogarithmic mod $l$ Heisenberg coverings, triple power residue symbols

1
On the other hand, based on the analogies between knots and primes ([Mo4]), we have mod 2 Milnor invariants $\mu_2(J)$ of certain rational primes ([Mo1]∼[Mo4]), as arithmetic analogues of Milnor invariants of a link ([Mi1], [Mi2], [T]), where a multi-index $J$ represents an ordered set of primes (cf. Subsection 3.2). For example, $(-1)^{\mu_2(12)}$ coincides with the Legendre symbol $(p_1/p_2)$. Assuming $\mu_2(ij) = 0$ $(1 \leq i, j \leq 3)$, $(-1)^{\mu_2(123)}$ is proved to equal the triple quadratic residue symbol $[p_1, p_2, p_3]$ introduced by Rédei ([R]), which describes the decomposition of $p_3$ in a certain dihedral extension, determined by $p_1$ and $p_2$, of degree 8 over $\mathbb{Q}$. Recently, mod 3 Milnor invariants $\mu_3(ij)$ and $\mu_3(123)$ were introduced for certain primes $p_i = (\pi_i)$ $(1 \leq i \leq 3)$ of the Eisenstein number field $\mathbb{Q}(\zeta_3)$, $\zeta_3 := \exp(2\pi\sqrt{-1}/3)$ ([AMM]). As in the mod 2 case, $\zeta_3^{\mu_3(12)}$ coincides with the cubic residue symbol $(\pi_1/\pi_2)_3$. Assuming $\mu_3(ij) = 0$ for $1 \leq i, j \leq 3$, $\zeta_3^{\mu_3(123)}$ is proved to equal the triple cubic residue symbol $[p_1, p_2, p_3]_3$, which describes the decomposition of $p_3$ in a certain mod 3 Heisenberg extension, determined by $p_1$ and $p_2$, of degree 27 over $\mathbb{Q}(\zeta_3)$ ([ibid]). We note that a key ingredient to introduce these Milnor invariants of primes is the theory of pro-$l$ extensions of number fields with restricted ramification due to Koch et al. (cf. [Kc]).

Since Milnor invariants of a braid $b$ coincide with those of the link obtained by closing $b$, the analogy with topology suggests to ask if there would be any relation between mod $l$ Milnor invariants $\mu_l(g; I) := \mu^{(l)}(g; I)$ mod $l$ of Galois elements and mod $l$ Milnor invariants $\mu_l(J)$ of primes. This question may be of arithmetic interest and importance, because such a relation would reveal a connection between Ihara theory and the classical arithmetic of pro-$l$ extensions of number fields. In this paper, we study this question. Let us describe our results in the following.

We firstly interpret the pro-$l$ longitudes of a Galois element ([KMT; §3.2) in terms of certain pro-$l$ paths and show that the $l$-th power residue symbol can be given by a mod $l$ Milnor invariant $\mu_l(\sigma; I)$ of a Frobenius element $\sigma$ with $|I| = 2$. Our main result is that triple quadratic (resp. cubic) residue symbols can be expressed by mod 2 (resp. mod 3) triple Milnor invariants of Frobenius elements (Theorem 4.1.10, Theorem 4.2.14), and hence answers the above question for triple Milnor invariants. For this, we introduce a certain mod $l$ Heisenberg ramified covering $D^{(l)}$ of $\mathbb{P}^1$, called the dilogarithmic mod $l$ Heisenberg ramified covering, which may be regarded as a higher analog of the dilogarithmic function, for the gerbe associated to the mod $l$ Heisenberg group. We then study the monodromy transformations of certain functions
on $D^{(l)}$ along the pro-$l$ longitudes of Frobenius elements for $l = 2, 3$, to obtain our main result. Our method is closely related with Wojtkowiak's work ([NW], [W1]~[W5]).

Here are the contents of this paper. In Section 1, we introduce the pro-$l$ longitudes of a Galois element in terms of pro-$l$ paths, and then introduce mod $l$ Milnor invariants of Galois elements. In Section 2, we introduce certain mod $l$ Heisenberg ramified coverings of $\mathbb{P}^1$, and explain the analogies with the dilogarithmic function. In Section 3, we recall mod 2 (resp. mod 3) Milnor invariants of primes of $\mathbb{Q}$ (resp. $\mathbb{Q}(\zeta_3)$). In Section 4, we interpret the Rédei symbol and the triple cubic residue symbol by mod $l$ Milnor invariants of Frobenius elements for $l = 2$ and 3, respectively, by computing the monodromy transformations of certain functions on the dilogarithmic mod $l$ Heisenberg coverings in Section 2 along the pro-$l$ longitudes, and deduce the relations between mod $l$ Milnor invariants of Galois elements in Ihara theory and mod $l$ Milnor invariants of primes for $l = 2, 3$.

Acknowledgement. We would like to thank Yasushi Mizusawa, Hiroaki Nakamura, Yuji Terashima, Hiroshi Tsunogai and Zdzisław Wojtkowiak for useful communications. Especially, we thank Terashima for discussions on the subsection 2.2. We would like to thank the referee for useful comments which improved the earlier version. The second author is partly supported by JSPS KAKENHI Grant Number JP17H02837, Grant-in-Aid for Scientific Research (B).

Notation. Throughout this paper, $l$ denotes a prime number.
For a number field $K$, $\mathcal{O}_K$ denotes the ring of integers of $K$.
For subgroups $A, B$ of a topological group $G$, $[A, B]$ stands for the closed subgroup of $G$ generated by commutators $[a, b] := aba^{-1}b^{-1}$ for $a \in A, b \in B$.

1. Mod $l$ Milnor invariants of Galois elements in Ihara theory

In [KMT; §3], following the analogy with Milnor invariants of braids associated to the Artin representation ([MK; Chapter 6, 4]), we introduced $l$-adic Milnor invariants of each Galois element, in a group theoretic manner, as the Magnus coefficients of the pro-$l$ longitudes of a Galois element associated to the Ihara representation. In this section, following [I3], [NW] and Wojtkowiak's series of papers [W1]~[W4], we interpret the pro-$l$ longitudes in
terms of pro-$l$ paths and then introduce mod $l$ Milnor invariants of a Galois element. We show that mod $l$ Milnor invariants for indices of length 2 are given by $l$-th power residue symbols.

1.1. The Ihara representation. Let $k$ be a fixed finite algebraic number field in the field $\mathbb{C}$ of complex numbers and $\overline{k}$ a fixed algebraic closure of $k$ in $\mathbb{C}$. Let $\mathbb{P}^1$ be the projective $t$-line over $k$. Let $a_1, \ldots, a_r$ be distinct $r$ numbers in $k$ ($r \geq 2$), identified with $k$-rational points on $\mathbb{P}^1$, and let $A := \{ a_0, a_1, \ldots, a_r \}$ with $a_0 = \infty$. We let $X := \mathbb{P}^1 \setminus A = \text{Spec} \ k[t, (t - a_j)^{-1}(1 \leq j \leq r)]$ and $X_\mathbb{C} := X \otimes_k \mathbb{C}$. For each $j$ $0 \leq j \leq r$, let $v_j$ be a $k$-rational tangential base point on $X$ at $a_j$ ([N; I]), which may be regarded as a tangential base point on the complex manifold $X(\mathbb{C})$ at $a_j$, a tangent vector on $X(\mathbb{C})$ at $a_i$. Following [W1; §2], the geometric generators of $\pi_1(X(\mathbb{C}); v_0)$ are defined as follows. Let $x_0$ be a small circle on $\mathbb{P}^1(\mathbb{C})$ around $a_0 = \infty$ starting from $v_0$ in the opposite clockwise way. Choose a point $v'_0 \in X(\mathbb{C})$ near $a_0 = \infty$ in the direction of $v_0$ and a path $\gamma$ in $X(\mathbb{C})$ from $v_0$ to $v'_0$. For $1 \leq j \leq r$, let $\gamma'_j$ be a path in $X(\mathbb{C})$ from $v'_0$ to $v_j$ and set $\gamma_i := \gamma'_i \cdot \gamma$, where paths are composed from the right. Let $x'_j$ be a small circle around $a_j$ starting from $v_j$ in the opposite clockwise way and set $x_j := \gamma^{-1}_j \cdot x'_j \cdot \gamma_j$. We may assume that paths $x'_1 \cdot \gamma'_1, \ldots, x'_r \cdot \gamma'_r$ are disjoint each other and that when we make a small circle around $v'_0$ in the opposite clockwise way starting from a point on $\gamma'_1$, we meet successively $\gamma'_2, \ldots, \gamma'_r$.

Then $\pi_1(X(\mathbb{C}); v_0)$ is generated by (the homotopy classes of) $x_0, x_1, \ldots, x_r$ subject to the relation $x_r \cdots x_1 x_0 = 1$. Hence $\pi_1(X(\mathbb{C}); v_0)$ is identified with the free group $F_r$ generated by $x_1, \ldots, x_r$ (the path $x_i$ and the word $x_i$ are identified). For $0 \leq j \leq r$, let $\widehat{\pi}_1^{(l)}(X(\mathbb{C}); v_0, v_j)$ denote the pro-$l$ completion of the set $\pi_1(X(\mathbb{C}); v_0, v_j)$ of homotopy classes of paths in $X(\mathbb{C})$ from $v_0$ to $v_j$. When $v_0 = v_j$, $\widehat{\pi}_1^{(l)}(X(\mathbb{C}); v_0, v_j)$ is denoted by $\widehat{\pi}_1^{(l)}(X(\mathbb{C}); v_0)$ which is the pro-$l$ completion $\widehat{F}_r^{(l)}$ of $F_r$. By ([G; XII, Corollaire 5.2]), $\pi_1^{(l)}(X(\mathbb{C}); v_0)$
is the maximal pro-$l$ quotient of the étale fundamental group of $X_{\overline{k}}$ based at $v_0$.

Let $\text{Gal}_k$ denote the absolute Galois group $\text{Gal}(\overline{k}/k)$ over $k$. The Ihara representation of $\text{Gal}_k$ on $\widehat{F}_r^{(l)} = \widehat{\pi}_1^{(l)}(X(\mathbb{C}); v_0)$ is given by the monodromy action as follows. Let $M_A$ be the maximal pro-$l$ extension of $\overline{k}(t)$ unramified outside $A$. Let $t_0 := 1/t$ and $t_j := t - a_j$ for $1 \leq j \leq r$. For each $j = 0, \ldots, r$, let $\overline{k}\{\{t_j\}\} := \bigcup_{n \geq 1} \overline{k}((t_j^{1/n}))$ be the field of Puiseux series in $t_j$ with coefficients in $\overline{k}$ and let $\iota_j : M_A \hookrightarrow \overline{k}\{\{t_j\}\}$ be the natural embedding. Let $M_j$ denote the image of $\iota_j$. For each path $p \in \pi_1(X(\mathbb{C}); v_0, v_j)$ ($0 \leq j \leq r$), we have a $\overline{k}(t)$-algebra isomorphism $[p] : M_0 \xrightarrow{\sim} M_j$ by the analytic continuation along $p$. Letting $\text{Isom}_{\overline{k}(t)}(M_0, M_j)$ denote the set of $\overline{k}(t)$-algebra isomorphisms from $M_0$ to $M_j$, the correspondence $p \mapsto [p]$ induces the bijection

\begin{equation}
\widehat{\pi}_1^{(l)}(X(\mathbb{C}); v_0, v_j) \xrightarrow{\sim} \text{Isom}_{\overline{k}(t)}(M_0, M_j).
\end{equation}

For the particular case that $v_j = v_0$, we have the isomorphism

\begin{equation}
\widehat{F}_r^{(l)} = \widehat{\pi}_1^{(l)}(X(\mathbb{C}); v_0) \xrightarrow{\sim} \text{Gal}(M_0/\overline{k}(t)) \simeq \text{Gal}(M_A/\overline{k}(t)),
\end{equation}

and hence a pro-$l$ word $f \in \widehat{F}_r^{(l)}$ acts on $M_0$ as the monodromy transformations of algebraic functions in $M_A$ along the pro-$l$ path $f$. The Galois group $\text{Gal}_k$ acts on $\overline{k}\{\{t_j\}\}$ via the action on Puiseux coefficients. This action stabilizes $M_j$ and so we have a homomorphism

\begin{equation}
s_j : \text{Gal}_k \longrightarrow \text{Gal}(M_j/\overline{k}(t)).
\end{equation}

Under the identification (1.1.1), we define the action of $\text{Gal}_k$ on $\widehat{\pi}_1^{(l)}(X(\mathbb{C}); v_0, v_j)$ by

\begin{equation}
g(p) := s_j(g) \cdot p \cdot s_0(g)^{-1}
\end{equation}

for $g \in \text{Gal}_k$ and $p \in \widehat{\pi}_1^{(l)}(X(\mathbb{C}); v_0, v_j)$. In particular, $\text{Gal}_k$ acts on $\widehat{F}_r^{(l)} = \widehat{\pi}_1^{(l)}(X(\mathbb{C}); v_0)$ by

\begin{equation}
g(f) := s_0(g)f s_0(g)^{-1}
\end{equation}

for $g \in \text{Gal}_k$ and $f \in \widehat{F}_r^{(l)}$ and thus we obtain the Ihara representation associated to $A$ and $v_0$

\begin{equation}
\text{Ih} = \text{Ih}_{(A, v_0)} : \text{Gal}_k \longrightarrow \text{Aut}(\widehat{F}_r^{(l)}),
\end{equation}
where $\text{Aut}(\hat{F}_r(l))$ is the group of (topological) automorphisms of $\hat{F}_r(l)$, which is virtually a pro-$l$ group ([DDMS; Theorem 5.6]).

For $1 \leq j \leq r$, we define the map $f_j : \text{Gal}_k \to \hat{F}_r(l) = \hat{\pi}_1(l)(X(\mathbb{C}); v_0)$ by

$$f_j(g) := g(\gamma_j)^{-1} \cdot \gamma_j = s_0(g) \cdot \gamma_j^{-1} \cdot s_j(g)^{-1} \cdot \gamma_j \quad (g \in \text{Gal}_k).$$

It is easy to see that $f_j$ is a 1-cocycle

$$f_j(gh) = \text{Ih}(g)(f_j(h))f_j(g) \quad (g, h \in \text{Gal}_k).$$

Then the action of $\text{Gal}_k$ on the generators $x_1, \ldots, x_r$ of $\hat{F}_r(l)$ is given as follows: Let $\chi_l : \text{Gal}_k \to \mathbb{Z}_l^\times$ be the $l$-cyclotomic character ($\mathbb{Z}_l$ : $l$-adic integers) defined by $g(\zeta_l^n) = \zeta_l^{\chi_l(g)n}$ for $g \in \text{Gal}_k$ and $\zeta_l := \exp(\frac{2\pi \sqrt{-1}}{l})$.

**Lemma 1.1.6** ([W1; Proposition 2.2.1]). Notations being as above, we have, for $g \in \text{Gal}_k$,

$$\text{Ih}(g)(x_0) = x_0^{\chi_l(g)}, \quad \text{Ih}(g)(x_j) = f_j(g)x_j^{\chi_l(g)}f_j(g)^{-1} \quad (1 \leq j \leq r).$$

By Lemma 1.1.6, the image of the Ihara representation (1.1.3) is in the following pro-$l$ analogue of the pure braid group ([I1])

$$\mathcal{P}(\hat{F}_r(l)) := \left\{ \varphi \in \text{Aut}(\hat{F}_r(l)) \mid \varphi(x_j) \sim x_j^{N(\varphi)} \quad (1 \leq j \leq r), \quad \varphi(x_1 \cdots x_r) = (x_1 \cdots x_r)^{N(\varphi)} \quad \text{for some } N(\varphi) \in \mathbb{Z}_l^\times \right\},$$

where $N \circ \text{Ih} = \chi_l$.

Let $\Omega_A$ be the subfield of $\overline{k}$ corresponding to the subgroup $\text{Ker(Ih)}$ of $\text{Gal}_k$:

$$\Omega_A := (\overline{k})^{\text{Ker(Ih)}},$$

which we call the **Ihara field of definition** for $A$. It is the smallest field of definition of all finite ramified coverings of $\mathbb{P}_C^1$ unramified outside $A$ whose Galois closures have degree $l$-power (cf. [AI; 3]). Since $\text{Aut}(\hat{F}_r(l))$ is virtually a pro-$l$ group, $\Omega_A$ is virtually a pro-$l$ extension of $k$. Moreover, since $\text{Ker(Ih)} \subset \text{Ker}(\chi_l)$, we have

$$k(\zeta_l^\infty) := \bigcup_{n \geq 1} k(\zeta_l^n) \subset \Omega_A.$$
The ramification in the extension $\Omega_A/k$ was studied by Wojtkowiak ([W4]). We also refer to [AI] for the case that $A$ contains $\{0, 1, \infty\}$. Define the finite set $S_A$ of primes of $k$ by

$$(1.1.8) \quad S_A := \left\{ p \in \text{Spm}(\mathcal{O}_k) \mid \begin{array}{l} v_p(l) > 0 \text{ or } v_p(a_i - a_j) > 0 \text{ for some } 1 \leq i \neq j \leq r \smallskip \text{ or } v_p(a_i) < 0 \text{ for some } 1 \leq i \leq r \end{array} \right\},$$

where $v_p$ denotes the $p$-adic valuation.

**Theorem 1.1.9** ([W4; Theorem 7.17]). *Notations being as above, the extension $\Omega_A/k$ is unramified outside $S_A$."

### 1.2. The pro-$l$ longitudes of a Galois element.

Let $H$ be the abelianization of $\widehat{\mathbb{F}_r}(l)$, $H := \widehat{\mathbb{F}_r}(l)/[\widehat{\mathbb{F}_r}(l), \widehat{\mathbb{F}_r}(l)]$, and let $[f]$ denote the image of $f \in \widehat{\mathbb{F}_r}(l)$ in $H$. We set $X_j := [x_j]$ for $1 \leq j \leq r$ so that $H$ is the free $\mathbb{Z}_l$-module with basis $X_1, \ldots, X_r$. For $1 \leq j \leq r$, the $j$-th (preferred) pro-$l$ longitude of $g \in \text{Gal}_k$ is defined to be a pro-$l$ word $y_j(g) \in \widehat{\mathbb{F}_r}(l)$ which satisfies the following conditions

$$(1.2.1) \quad \begin{cases} (1) \quad \text{Ih}(g)(x_j) = y_j(g)x_j^{\chi(g)}y_j(g)^{-1}, \\ (2) \quad [y_j(g)] = \prod_{i \neq j} e_iX_i \text{ for some } e_i \in \mathbb{Z}_l. \end{cases}$$

**Lemma 1.2.2** ([KMT; Lemma 3.2.1]). *For each $j$ ($1 \leq j \leq r$), the $j$-th pro-$l$ longitude of each Galois element in $\text{Gal}_k$ exists uniquely.*

The following proposition shows that the $j$-th pro-$l$ longitude of $g$ is given by $f_j(g)$ in (1.1.3). For $z \in k^\times$, let $\kappa_z : \text{Gal}_k \to \mathbb{Z}_l$ be the Kummer cocycle defined by

$$(1.2.3) \quad g(z^{1/l^n}) = \zeta_{l^n}^{\kappa_z(g)}z^{1/l^n} \quad (n \geq 1).$$

We easily see the formula $g^{-1}(z^{1/l^n}) = \zeta_{l^n}^{-\chi_i(g)^{-1}\kappa_z(g)}z^{1/l^n}$.

**Proposition 1.2.4.** For $1 \leq j \leq r$, the pro-$l$ word $f_j(g)$ is the $j$-th pro-$l$ longitude of $g \in \text{Gal}_k$ and we have

$$[f_j(g)] = -\sum_{i \neq j} \kappa_{a_j - a_i}(g)X_i.$$
Proof. Since the maximal abelian subextension of $M$ over $k(t)$ is generated by $t_i^{1/n}$ for $0 \leq i \leq r$ and $n \geq 1$, $[f_j(g)]$ is determined by its action on $t_i^{1/n}$. For $i \neq j$, the monodromy transformation of $t_i^{1/n} = (t-a_i)^{1/n}$ along $f_j(g) = s_0(g) \cdot \gamma_j^{-1} \cdot s_j(g)^{-1} \cdot \gamma_j$ is given as follows:

$$
\iota_0((t-a_i)^{1/n}) \xrightarrow{\gamma_j} (a_j-a_i)^{1/n} \sum_{m=0}^{\infty} \left(\frac{1}{m!}\right) (a_j-a_i)^m (t-a_j)^m
$$

$$
\xrightarrow{s_j(g)^{-1} \cdot \zeta_{\iota n}^{-1} \cdot \kappa_{x_j-a_i}(g)} \sum_{m=0}^{\infty} \left(\frac{1}{m!}\right) (a_j-a_i)^m (t-a_j)^m \quad \text{(by (1.2.3))}
$$

$$
\xrightarrow{\gamma_j^{-1} \cdot \zeta_{\iota n}^{-1} \cdot \kappa_{x_j-a_i}(g)} \iota_0((t-a_i)^{1/n})
$$

$$
\xrightarrow{s_0(g) \cdot \zeta_{\iota n}^{-1} \cdot \kappa_{x_j-a_i}(g)} \iota_0((t-a_i)^{1/n}) \quad \text{(by $\iota_0((t-a_i)^{1/n}) \in k\{1/t\}$)}.
$$

Similarly, we easily see that $f_j(g)$ acts trivially on $(t-a_i)^{1/n}$. Since the monodromy translation of $(t-a_i)^{1/n}$ along $x_j$ is the multiplication by $\zeta_{\iota n}$ if $i = j$ and the identity if $i \neq j$, we have

$$
[\gamma_j](t-a_i)^{1/n} = \sum_{i \neq j} \kappa_{a_j-a_i}(g) X_i.
$$

By Lemma 1.1.5, (1.2.1), (1.2.4.1) and the uniqueness of the $j$-th pro-$l$ longitude, $f_j(g)$ is the $j$-th pro-$l$ longitude of $g$. \square

Let $\Omega_{A}$ be as in (1.1.7) and let $\sigma \in \text{Gal}(\Omega_{A}/k)$. Choosing an extension $g$ of $\sigma$, we set

$$
f_j(\sigma) := f_j(g) \quad (1 \leq j \leq r).
$$

**Proposition 1.2.6.** The definition of $f_j(\sigma)$ in (1.2.5) is independent of the choice of an extension $g \in \text{Gal}_k$.

Proof. Let $g, g' \in \text{Gal}_k$ be extensions of $\sigma$. We can write $g' = gh$ for some $h \in \text{Gal}(k/\Omega_A)$. By (1.1.5), we have $f_j(g') = \iota(h) f_j(h) f_j(g)$. Since $\iota(h) = \text{id}$, the uniqueness of the pro-$l$ longitude in Lemma 1.2.2 yields $f_j(h) = 1$ and hence $f_j(g') = f_j(g)$. \square
1.3. Mod \( l \) Milnor invariants of a Galois element. Let \( \hat{T} \) be the complete tensor algebra of \( H \) over \( \mathbb{Z}_l \) defined by \( \hat{T} := \prod_{n \geq 0} H^\otimes n \), where \( H^\otimes 0 := \mathbb{Z}_l \) and \( H^\otimes n := H \otimes_{\mathbb{Z}_l} \cdots \otimes_{\mathbb{Z}_l} H \) (\( n \) times) for \( n \geq 1 \). It is nothing but the Magnus algebra \( \mathbb{Z}_l \langle\langle X_1, \ldots, X_r \rangle\rangle \) over \( \mathbb{Z}_l \), namely, the algebra of non-commutative formal power series (called Magnus power series) over \( \mathbb{Z}_l \) with variables \( X_1, \ldots, X_r \):

\[
\hat{T} = \prod_{n \geq 0} H^\otimes n = \mathbb{Z}_l \langle\langle X_1, \ldots, X_r \rangle\rangle.
\]

For \( n \geq 0 \), we set \( \hat{T}(n) := \prod_{m \geq n} H^\otimes m \). The degree of a Magnus power series \( \Phi \), denoted by \( \deg(\Phi) \), is defined to be the minimum \( n \) such that \( \Phi \in \hat{T}(n) \). We note that \( H^\otimes n \) is the free \( \mathbb{Z}_l \)-module on monomials \( X_{i_1} \cdots X_{i_n} \) (\( 1 \leq i_1, \ldots, i_n \leq r \)) of degree \( n \) and \( \hat{T}(n) \) consists of Magnus power series of degree \( \geq n \).

Let \( \mathbb{Z}_l[[\hat{F}_r^{(l)}]] \) be the complete group algebra of \( \hat{F}_r^{(l)} \) over \( \mathbb{Z}_l \) and let \( \epsilon_{\mathbb{Z}_l[[\hat{F}_r^{(l)}]]} : \mathbb{Z}_l[[\hat{F}_r^{(l)}]] \to \mathbb{Z}_l \) be the augmentation homomorphism with the augmentation ideal \( I_{\mathbb{Z}_l[[\hat{F}_r^{(l)}]]} := \text{Ker}(\epsilon_{\mathbb{Z}_l[[\hat{F}_r^{(l)}]]}) \). The correspondence \( x_i \mapsto 1 + X_i \) (\( 1 \leq i \leq r \)) gives rise to the pro-\( l \) Magnus isomorphism of topological \( \mathbb{Z}_l \)-algebras

\[
\Theta : \mathbb{Z}_l[[\hat{F}_r^{(l)}]] \overset{\sim}{\longrightarrow} \hat{T} = \mathbb{Z}_l \langle\langle X_1, \ldots, X_r \rangle\rangle.
\]

Here \( (I_{\mathbb{Z}_l[[\hat{F}_r^{(l)}]]})^n \) corresponds, under \( \Theta \), to \( \hat{T}(n) \) for \( n \geq 0 \). For \( \alpha \in \mathbb{Z}_l[[\hat{F}_r^{(l)}]] \), \( \Theta(\alpha) \) is called the pro-\( l \) Magnus expansion of \( \alpha \). In the following, for a multi-index \( I = (i_1 \cdots i_n) \), \( 1 \leq i_1, \ldots, i_n \leq r \), we set

\[
|I| := n \quad \text{and} \quad X_I := X_{i_1} \cdots X_{i_n}.
\]

We call the coefficient of \( X_I \) in \( \Theta(\alpha) \) the \( l \)-adic Magnus coefficient of \( \alpha \) for \( I \) and denote it by \( \mu^{(l)}(I; \alpha) \). So we have

\[
\Theta(\alpha) = \sum_{|I| \geq 1} \epsilon_{\mathbb{Z}_l[[\hat{F}_r^{(l)}]]}(\alpha) + \sum_{|I| \geq 1} \mu^{(l)}(I; \alpha)X_I.
\]

Taking mod \( l \) in (1.3.1), we have the mod \( l \) Magnus isomorphism

\[
\Theta : \mathbb{F}_l[[\hat{F}_r^{(l)}]] \overset{\sim}{\longrightarrow} \hat{T} \otimes_{\mathbb{Z}_l} \mathbb{F}_l = \mathbb{F}_l \langle\langle X_1, \ldots, X_r \rangle\rangle
\]
so that for $\alpha \in \mathbb{F}_l[[\hat{F}_r^{(l)}]]$, we have

$$\Theta_l(\alpha) = \epsilon_{\mathbb{F}_l[[\hat{F}_r^{(l)}]]}(\alpha) + \sum_{|I| \geq 1} \mu_l(I; \alpha) X_I,$$

where $\epsilon_{\mathbb{F}_l[[\hat{F}_r^{(l)}]]} : \mathbb{F}_l[[\hat{F}_r^{(l)}]] \to \mathbb{F}_l$ is the augmentation homomorphism and $\mu_l(I; \alpha) := \mu(I; \alpha) \mod l$. Let $\{\hat{F}_r^{(l)}(d)\}_{d \geq 1}$ be the Zassenhaus filtration of $\hat{F}_r^{(l)}$ defined by $\hat{F}_r^{(l)}(d) := \hat{F}_r^{(l)} \cap 1 + (I_{\mathbb{F}_l[[\hat{F}_r^{(l)}]]})^d$, where $I_{\mathbb{F}_l[[\hat{F}_r^{(l)}]]} := \text{Ker}(\epsilon_{\mathbb{F}_l[[\hat{F}_r^{(l)}]]})$. For $f \in \hat{F}_r^{(l)}$, we have

$$f \in \hat{F}_r^{(l)}(d) \iff \mu_l(I; f) = 0 \text{ for } |I| < d \text{ i.e., } \deg(\Theta_l(f - 1)) \geq d.$$

The following inductive formula for $\hat{F}_r^{(l)}(d)$ is known ([DDMS, 12.9]):

$$\hat{F}_r^{(l)}(d) = (\hat{F}_r^{(l)}([d/l])) \prod_{i+j=d} [\hat{F}_r^{(l)}(i), \hat{F}_r^{(l)}(j)],$$

where $[d/l]$ stands for the least integer $m$ such that $ml \geq d$.

Now, following the case for pure braids ([MK; Chapter 6, 4], [Kd; Chapter 1]), we will define the $l$-adic Milnor numbers of $g \in \text{Gal}_k$ by the $l$-adic Magnus coefficients of the $i$-th longitude $\gamma_i(g)$: Let $I = (i_1 \cdots i_n)$ be a multi-index, where $1 \leq i_1, \ldots, i_n \leq r$ and $|I| = n \geq 1$. The $l$-adic Milnor number of $g \in \text{Gal}_k$ for $I$, denoted by $\mu^{(l)}(g; I) = \mu^{(l)}(g; i_1 \cdots i_n)$, is defined by the $l$-adic Magnus coefficient of the pro-$l$ longitude $f_{i_n}(g)$ for $I' := (i_1 \cdots i_{n-1})$:

$$\mu^{(l)}(g; I) := \mu^{(l)}(I', f_{i_n}(g)).$$

Here we set $\mu^{(l)}(g; I) := 0$ if $|I| = 1$. In this paper, we shall use $mod \ l$ Milnor number $\mu_l(g; I)$ of $g \in \text{Gal}_k$ for $I$, which is defined by

$$\mu_l(g; I) := \mu_l(I'; f_{i_n}(g)) := \mu^{(l)}(g; I) \mod l.$$

By the proof of [KMT; Theorem 3.2.8], we have the following

**Theorem 1.3.5.** Let $g, h \in \text{Gal}_k$ satisfying $\chi_l(g) \equiv \chi_l(h) \equiv 1 \mod l$.
Let $I = (i_1 \cdots i_n)$ be a multi-index. We assume that $\mu_l(g; J) = 0$ for any $J = (j_1 \cdots j_m) \subseteq \{i_1, \ldots, i_n\}$. Then we have

$$\mu_l(hgh^{-1}; I) = \mu_l(g; I).$$

When the conditions in Theorem 1.3.5 are satisfied, we call $\mu_l(g; I)$ the mod $l$ Milnor invariant of $g$ for $I$.

Let $\Omega_A$ be the Ihara field of definition for $A$ in (1.1.7). By Proposition 1.2.6, mod $l$ Milnor number $\mu_l(\sigma; I)$ of $\sigma \in \text{Gal}(\Omega_A/k)$ for a multi-index $I$ is well defined by $\mu_l(g; I)$ for an extension $g \in \text{Gal}_k$ of $\sigma$. Let $\mathcal{S}_A$ be as in (1.1.8). Let $p \in \text{Spm}(\mathcal{O}_k) \setminus \mathcal{S}_A$ and let $p$ be an extension of $p$ to $\Omega_A$. Since $p$ is unramified in $\Omega_A/k$ by Theorem 1.1.9, we have the Frobenius automorphism $\sigma_p \in \text{Gal}(\Omega_A/k)$ of $p$ over $k$. We then have mod $l$ Milnor number $\mu_l(\sigma_p; I)$ for a multi-index $I$.

**Corollary 1.3.6.** Notations being as above, suppose $N_p \equiv 1 \mod l$. Let $I = (i_1 \cdots i_n)$ be a multi-index. We assume that $\mu_l(\sigma_p; J) = 0$ for any $J = (j_1 \cdots j_m) \subseteq \{i_1, \ldots, i_n\}$. Then $\mu_l(\sigma_p; I)$ is independent of the choice of an extension $p$ and hence it is denoted by $\mu_l(\sigma_p; I)$

**Proof.** This follows from Theorem 1.3.5 and $\chi_l(\sigma_p) = N_p \equiv 1 \mod l$. $\square$

**Theorem 1.3.7.** Notations being as above, for $1 \leq i \leq r$, we have

$$\mu_l(\sigma_p; ii) = 0.$$ 

For $1 \leq i \neq j \leq r$, we have

$$k((a_j - a_i)^{1/l^n}) \subset \Omega_A \quad (n \geq 1)$$

and

$$\zeta_l^{\mu(l(\sigma_p; ij))} = \left(\frac{a_j - a_i}{p}\right)_l^{-1}$$

for $p \notin \mathcal{S}_A$ with $N_p \equiv 1 \mod l$. Here $\left(\frac{\cdot}{p}\right)_l$ denotes the $l$-th power residue symbol in $k_p$.

**Proof.** The first assertion follows from Proposition 1.2.4. For the second assertion, it suffices to show that $g((a_j - a_i)^{1/l^n}) = (a_j - a_i)^{1/l^n}$ for any
$g \in \text{Gal}(\overline{k}/\Omega_A)$. Since $\text{Gal}(\overline{k}/\Omega_A) = \text{Ker}(Ih)$ by (1.1.7), we have $f_j(g) = 1$ for $1 \leq j \leq r$ by (1.2.1), Lemma 1.2.2 and Proposition 1.2.4. By Proposition 1.2.4 again, we have $\kappa_{a_j-a_i}(g) = 0$ for $i \neq j$. By (1.2.3), $g((a_j - a_i)^{1/l^n}) = (a_j - a_i)^{1/l^n}$.

We note by the second assertion and Theorem 1.1.9 that $k_p((a_i - a_j)^{1/l})$ is an unramified extension of $k_p$ for $p \notin S_A$. By (1.2.3), Proposition 1.2.4 and (1.3.4), the third assertion is obtained as follows:

\[
\zeta_l^{-\mu_l(i; f_j(\sigma_p))} = \zeta_l^{-\kappa_{a_j-a_i}(\sigma_p)} = \left(\frac{\sigma_p((a_j - a_i)^{1/l})}{(a_j - a_i)^{1/l}}\right)^{-1} = \left(\frac{a_j - a_i}{p}\right)_l \quad \square
\]

Remark 1.3.8. (1) By the relation between Magnus coefficients and Massey products ([Dw],[St]), it was shown in [KMT; §3.3] that the mod $l$ Milnor invariants of a Galois element $g$ are expressed by Massey products in the mod $l$ cohomology of the pro-$l$ link group of $g$ defined by

\[
\Pi_A(g) := \langle x_1, \ldots, x_r \mid x_1^{-\chi_l(g)}[x_1^{-1}, f_1(g)^{-1}] = \cdots = x_r^{-\chi_l(g)}[x_r^{-1}, f_r(g)^{-1}] = 1 \rangle.
\]

(2) Let $E : \hat{F}_r^{(l)} \to \mathbb{Q}_l\langle X_1, \ldots, X_r \rangle$ be the embedding defined by $E(x_i) := \exp(X_i) = 1 + X_i + \frac{1}{2}X_i^2 + \cdots + \frac{1}{m!}X_i^m + \cdots$. In a series of papers [NW], [W1] $\sim$ [W4], Wojtkowiak has studied the coefficients of Lie elements in the series $\log E(f_j(g)^{-1})$, called the $l$-adic iterated integrals. Our $l$-adic Milnor numbers are expressed by $l$-adic iterated integrals, and $l$-adic iterated integrals, vice versa.

2. Dilogarithmic mod $l$ Heisenberg ramified coverings of $\mathbb{P}^1$

In this section, we introduce certain mod $l$ Heisenberg extensions of $k(t)$, called the dilogarithmic mod $l$ Heisenberg extensions, which will be used later in the section 4. We explain the analogies between our mod $l$ Heisenberg coverings and the dilogarithmic function from cohomological viewpoint. We assume that the number field $k$ contains $\zeta_l = \exp(\frac{2\pi i}{l})$. 

12
2.1. Mod l Heisenberg branched coverings of \( \mathbb{P}^1 \). Let \( k(t) \) be the function field of the projective \( t \)-line \( \mathbb{P}^1 \) over \( k \). For \( c \in k^\times \), let \( K^{(l)} := K_{\{c,t\}}^{(l)} \) be the extension of \( k(t) \) defined by

\[
K^{(l)} := K_{\{c,t\}}^{(l)} := k(t)(t^{1/l}, (c^l - t)^{1/l}).
\]

It is a Kummer extension of \( k(t) \) such that the Galois group \( \text{Gal}(K^{(l)}/k(t)) \) is isomorphic to \( \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z} \) generated by \( \alpha, \beta \) defined by

\[
\alpha(t^{1/l}) := \zeta l t^{1/l}, \quad \alpha((c^l - t)^{1/l}) := (c^l - t)^{1/l},
\]
\[
\beta(t^{1/l}) := t^{1/l}, \quad \beta((c^l - t)^{1/l}) := \zeta_l (c^l - t)^{1/l},
\]

and it is unramified outside \( \infty, 0 \) and \( c^l \). The ramification index of these points are \( l \). A non-singular projective curve \( C^{(l)} \) over \( k \) with function field \( K^{(l)} \) is given by the Fermat plane curve

\[
X^l + Y^l = (cZ)^l
\]

in \( \mathbb{P}^2 \) and the covering map \( C^{(l)} \rightarrow \mathbb{P}^1 \) is given by

\[
(X : Y : Z) \mapsto (X^l : Z^l).
\]

We set

\[
\varepsilon_l(t) := \prod_{i=1}^{l-1} (c - \zeta_i t^{1/l})^i
\]

and define the extension \( R^{(l)} := R_{\{c,t\}}^{(l)} \) of \( K^{(l)} \) by

\[
R^{(l)} := R_{\{c,t\}}^{(l)} := K^{(l)}(\varepsilon_l(t)^{1/l}) = k(t)(t^{1/l}, (c^l - t)^{1/l}, \varepsilon_l(t)^{1/l}).
\]

It is a cyclic Kummer extension of \( K^{(l)} \) of degree \( l \) whose Galois group \( \text{Gal}(R^{(l)}/K^{(l)}) \) is generated by \( \delta \) defined by

\[
\delta(\varepsilon_l(t)^{1/l}) := \zeta_l \varepsilon_l(t)^{1/l},
\]

and in which only primes \( (c - \zeta_i t^{1/l}) (0 \leq i \leq l - 1) \) of \( K^{(l)} \), which are all lying over \( t = c^l \), can be ramified in \( R^{(l)} \). Let \( D^{(l)} \) be a non-singular projective curve whose function field is \( R^{(l)} \). For \( l = 2 \) and \( 3 \), concrete defining equations for \( D^{(l)} \) are given as follows.
Example 2.1.3. Let \( l = 2 \). By setting \( U/W = \sqrt{c - \sqrt{t}} \) and \( V/W = \sqrt{c + \sqrt{t}} \), we can take a non-singular projective model \( D^{(2)} \) of \( R^{(2)} \) by the plane curve

\[ U^2 + V^2 = 2cW^2 \]

and hence the genus of \( D^{(2)} \) is 0. The covering map \( D^{(2)} \rightarrow C^{(2)} \) is given by

\[ (U : V : W) \mapsto (cW^2 - U^2 : UV : W^2), \]

which is ramified at \( (0 : \pm \sqrt{2c} : 1) \in C^{(2)} \).

Let \( l = 3 \). By setting \( U = \sqrt[3]{c - \zeta_3 \sqrt{t}}, V = \sqrt[3]{c - \zeta_3^2 \sqrt{t}} \) and \( W = \sqrt[3]{c - \sqrt{t}} \), we can take a non-singular projective model \( D^{(3)} \) of \( R^{(3)} \) by the plane curve

\[ \zeta_3^2 U^3 + V^3 = -\zeta_3 W^3 \]

and hence the genus of \( D^{(3)} \) is 1. The covering map \( D^{(3)} \rightarrow C^{(3)} \) is given by

\[ (U : V : W) \mapsto (c(U^3 - W^3) : c(1 - \zeta_3)UVW : U^3 - \zeta_3 W^3), \]

which is unramified.

Theorem 2.1.4. Notations being as above, \( R^{(l)} \) is a Galois extension of \( k(t) \) such that Galois group \( \text{Gal}(R^{(l)}/k(t)) \) is isomorphic to the mod \( l \) Heisenberg group

\[ H(\mathbb{F}_l) := \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \mid * \in \mathbb{F}_l \right\}, \]

and it is unramified outside \( \infty, 0 \) and \( c^j \).

Proof. The assertion about the ramification in \( R^{(l)}/k(t) \) follows immediately from those in \( K^{(l)}/k(t) \) and \( R^{(l)}/K^{(l)} \). For \( 0 \leq j < l \), we see that

\[ \alpha^j(\varepsilon_t(t)) = \frac{(c - t^{1/l}) \cdots (c - \zeta^{j-1} t^{1/l})}{(c^j - t)^j} \varepsilon_t(t), \quad \beta^j(\varepsilon_t(t)) = \varepsilon_t(t), \]

from which any conjugate of \( \varepsilon(t)^{1/l} \) over \( k(t) \) lies in \( R^{(l)} \) and so \( R^{(l)} \) is a Galois extension of \( k(t) \). We define the extensions \( \alpha, \beta \in \text{Gal}(R^{(l)}/k(t)) \) of
\(\alpha, \beta \in \text{Gal}(K^{(l)}/k(t))\), respectively, by
\[(2.1.4.1)\]
\[
\begin{align*}
\tilde{\alpha}(t^{1/l}) &:= \zeta t^{1/l}, \quad \tilde{\alpha}((c' - t)^{1/l}) := (c' - t)^{1/l}, \quad \tilde{\alpha}(\varepsilon_l(t)^{1/l}) := \frac{c - t^{1/l}}{(c' - t)^{1/l}} \varepsilon_l(t)^{1/l}, \\
\tilde{\beta}(t^{1/l}) &:= t^{1/l}, \quad \tilde{\beta}((c' - t)^{1/l}) := \zeta_l (c' - t)^{1/l}, \quad \tilde{\beta}(\varepsilon_l(t)^{1/l}) := \varepsilon_l(t)^{1/l}, 
\end{align*}
\]
where we easily verify that \(\tilde{\alpha}l = \tilde{\beta}l = 1\). By the straightforward computation, we have
\[(2.1.4.2)\]
\[
\begin{align*}
[\tilde{\alpha}, \tilde{\beta}](t^{1/l}) &= t^{1/l}, \quad [\tilde{\alpha}, \tilde{\beta}](c' - t)^{1/l} = (c' - t)^{1/l}, \quad [\tilde{\alpha}, \tilde{\beta}](\varepsilon_l(t)^{1/l}) &= \zeta_l \varepsilon_l(t)^{1/l}
\end{align*}
\]
and so \([\tilde{\alpha}, \tilde{\beta}] = \delta\). Therefore the correspondence
\[
\tilde{\alpha} \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \tilde{\beta} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},
\]
induces the isomorphism
\[
\text{Gal}(R^{(l)}/k(t)) \simrightarrow H(F_l). \quad \Box
\]

We call the extension \(R^{(l)}/k(t)\) the \textit{dilogarithmic mod l Heisenberg extension}, and call the ramified covering \(D^{(l)} \to \mathbb{P}^1_k\) (resp. the (unramified) covering \(D^{(l)}|_X \to X\) for \(X := \mathbb{P}^1 \setminus \{\infty, 0, c'\}\)) the \textit{dilogarithmic mod l Heisenberg ramified covering} (resp. the \textit{dilogarithmic mod l Heisenberg covering}). A mod \(l\) Heisenberg extension (resp. (ramified) covering) will also be called simply an \(H(F_l)\)-extension (resp. \(H(F_l)\)-(ramified) covering). The reason why we call “dilogarithmic” will be explained in the next subsection 2.2.

By Theorem 2.1.4, we have the surjective homomorphism
\[
\text{Gal}(M_A/k(t)) \to \text{Gal}(R^{(l)}/k(t)),
\]
when \(A\) contains \(\infty, 0\) and \(c'\). Composing with it the natural homomorphism \(\tilde{\pi}_1^{(l)}(\mathbb{P}^1(\mathbb{C}) \setminus A) \to \text{Gal}(M_A/k(t))\) obtained by the isomorphism (1.1.2) and the inclusion \(\text{Gal}(M_A/\overline{k(t)}) \subset \text{Gal}(M_A/k(t))\), we have the homomorphism
\[
\rho : \tilde{\pi}_1^{(l)}(\mathbb{P}^1(\mathbb{C}) \setminus A; v_0) \longrightarrow \text{Gal}(R^{(l)}/k(t)).
\]
Let $a_0 := \infty$, $a_1 := 0$ and $a_2 := c'$ and let $x_1$ and $x_2$ be the loops around 0 and $c'$, respectively, as in Subsection 1.1. Then we have

$$(2.1.5) \quad \rho(x_1) = \tilde{\alpha}, \; \rho(x_2) = \tilde{\beta}.$$ 

**Corollary 2.1.6.** The monodromy transformation of $\varepsilon_i(t)^{1/l}$ along the pro-$l$ path $[x_i, x_j]$ (resp. $x_i'$) $(1 \leq i < j \leq r)$ is given by

$$\varepsilon_i(t)^{1/l} \mapsto \begin{cases} \zeta \varepsilon_i(t)^{1/l} & (i, j) = (1, 2), \\ \varepsilon_i(t)^{1/l} & \text{otherwise}, \end{cases} \quad \text{(resp. } \varepsilon_i(t)^{1/l} \mapsto \varepsilon_i(t)^{1/l}).$$

**Proof.** The assertion for the monodromy along $[x_i, x_j]$ follows from (2.1.4.2) and (2.1.5) when $(i, j) = (1, 2)$, and from $\rho([x_i, x_j]) = \text{id}$ when $(i, j) \neq (1, 2)$. The assertion for the monodromy along $x_i'$ follows from (2.1.4.1) and $\rho(x_i) = \text{id}$ when $i \neq 1, 2$. \qed

**Theorem 2.1.7.** Let $a \in k \setminus \{0, c\}$ and let $A := \{a_0 := \infty, a_1 := 0, a_2 := c', a_3 := a\}$. Let $\Omega_A$ be the Ihara field of definition for $A$ in (1.1.7). Then we have

$${\mathcal{R}}_{\{e, a\}}^{(l)} \subset \Omega_A.$$ 

**Proof.** It suffices to show that

$$(2.1.7.1) \quad g(a^{1/l}) = a', \; g((c' - a)^{1/l}) = (c' - a)^{1/l} \quad \text{and} \quad g(\varepsilon_i(a)^{1/l}) = \varepsilon_i(a)^{1/l}$$

for any $g \in \text{Gal}(\overline{k}/\Omega_A)$. Since $\text{Gal}(\overline{k}/\Omega_A) = \text{Ker}(\text{Ih})$, we have $f_j(g) = 1$ for $1 \leq j \leq 3$ by (1.2.1), Lemma 1.2.2 and Proposition 1.2.4. By Proposition 1.2.4, noting $a_3 - a_1 = a$ and $a_2 - a_3 = c' - a$, we have $\kappa_a(g) = \kappa_{c' - a}(g) = 1$, which yields the first 2 equalities in (2.1.7.1). To prove the 3rd equality in (2.1.7.1), we first note that for each $n \geq 0$, there is $\Phi_n(X_1, X_2) \in k(X_1, X_2)$ such that

$$\left.\frac{d^n}{dt^n}\varepsilon_i(t)^{1/l}\right|_{t=a} = \varepsilon_i(a)^{1/l}\Phi_n(\varepsilon_i(a), a^{1/l}).$$

Using this and the 1st equality in (2.1.7.1), the monodromy transformation
of $\varepsilon_l(t)^{1/l}$ along $f_3(g) = s_0(g) \cdot \gamma_3^{-1} \cdot s_3(g)^{-1} \cdot \gamma_3$ is computed as follows:

$$
\iota_0(\varepsilon_l(t)^{1/l}) \xrightarrow{\gamma_3^{-1}} \varepsilon_l(a)^{1/l} \sum_{n=0}^{\infty} \Phi_n(\varepsilon_l(a), a^{1/l})(t - a)^n
$$

$$
\xrightarrow{g^{-1}} \frac{g^{-1}(\varepsilon_l(a)^{1/l})}{\varepsilon_l(a)^{1/l}} \varepsilon_l(a)^{1/l} \sum_{n=0}^{\infty} \Phi_n(\varepsilon_l(a), a^{1/l})(t - a)^n
$$

$$
\xrightarrow{\gamma_3^{-1}} \frac{g^{-1}(\varepsilon_l(a)^{1/l})}{\varepsilon_l(a)^{1/l}} \iota_0(\varepsilon_l(t)^{1/l})
$$

$$
\xrightarrow{s_0(g)} \frac{\varepsilon_l(a)^{1/l}}{g(\varepsilon_l(a)^{1/l})} \iota_0(\varepsilon_l(t)^{1/l}). \quad \square
$$

Since $f_3(g) = 1$, we have $g(\varepsilon_l(a)^{1/l}) = \varepsilon_l(a)^{1/l}$ for any $g \in \text{Gal}(\overline{k}/\Omega_A)$. \quad \square

**Remark 2.1.8.** (1) The dilogarithmic $H(F_l)$-extension $R(l)$ of $k(t)$ is a special case of Anderson-Ihara’s elementary extensions ([AI]) and Wojtkowiak’s polylogarithmic extensions ([W5; 3]).

(2) For the case that $A$ contains $\infty, 0$ and $1$, it was shown in [AI] that $\Omega_A$ is generated over $k$ by algebraic numbers generalizing higher circular $l$-units.

2.2. Gerbes and analogies with the dilogarithmic function. In this subsection, we explain the reason why we call $D^{(l)}|_X \to X$ the *dilogarithmic* $H(F_l)$-covering. It comes from some analogies with the dilogarithmic function, which also explain a geometric meaning of our $H(F_l)$-coverings. The analogies we discuss in this subsection were suggested by Brylinski’s work ([Br1], [Br2]), and we refer to [Br1] for materials on Deligne cohomology and gerbes.

First, let us recall the dilogarithmic function side. Let $f_1$ and $f_2$ be invertible holomorphic functions on $X := \mathbb{P}^1(\mathbb{C}) \setminus A$. Let $H^0_D(X, \mathbb{Z}(n)) (n \geq 1)$ denote the holomorphic Deligne cohomology, the $n$-th hypercohomology of the Deligne complex $(2\pi \sqrt{-1})^n \mathbb{Z} \to \mathcal{O}_X \xrightarrow{d_2} \cdots \xrightarrow{d_2} \Omega^{n-1}_X ([\text{Br1}; \text{Definition 1.5.9}])$. Since $H^0(X, \mathcal{O}_X^*) \simeq H^1_D(X, \mathbb{Z}(1))$ ([ibid; Proposition 1.5.10]), each $f_i$ defines a class $c(f_i) \in H^1_D(X, \mathbb{Z}(1))$. Recall that $H^2_D(X, \mathbb{Z}(2))$ classifies isomorphism classes of holomorphic line bundles over $X$ with holomorphic connection ([ibid; Theorem 2.2.20])

$$
H^2_D(X, \mathbb{Z}(2)) \simeq \left\{ \text{isom. classes of holomorphic line bundles over } X \text{ with holomorphic connection} \right\}.
$$
Hence the cup product \( c(f_1) \cup c(f_2) \) defines an isomorphism class of holomorphic line bundle with holomorphic connection, denoted by \((f_1, f_2)\), which we call the Deligne line bundle. In more concrete terms, the transition function of \((f_1, f_2)\) is given by \( f_2^{\log, f_1 - \log, f_1} \) on \( U_i \cap U_j \) and the connection 1-form is given by \( \log, f d \log f_2 \) on \( U_i \), where \( X = \bigcup_i U_i \) is an open cover and \( \log, f \) is a chosen branch of \( \log f \) on \( U_i \). The map \( \{f_1, f_2\} \to (f_1, f_2) \) is known to be the Bloch-Beilinson regulator ([Be], [Bl, §1])

\[
K_2(X) \longrightarrow H^2_{\mathbb{D}}(X, \mathbb{Z}(2)).
\]

We note that \((f_1, f_2) = 1\) if and only if there is a trivialization of \((f_1, f_2)\), namely, a horizontal section. In particular, let \( A = \{\infty, 0, 1\} \) and \( f_1 = 1 - t, f_2 = t \). Then the dilogarithmic function

\[
\text{Li}_2(t) = -\int_0^t \log(1 - t) d \log t = \sum_{n=1}^{\infty} \frac{t^n}{n^2}
\]

gives a horizontal section of \((1 - t, t)\) ([Bl, §1], [De; Example 3.5]). The triviality \((1 - t, t) = 1\) reflects the Steinberg relation in \( K_2(X) \).

Next, let us see the Heisenberg covering side. Let \( f_1 \) and \( f_2 \) be invertible regular functions on \( X = \mathbb{P}^1_k \setminus A \). Let \( H^n_{\text{ét}}(X, \mathbb{F}_l) \) denote the \( n \)-th étale cohomology group. Since \( k \) contains \( \zeta_l \), we note \( H^0_{\text{ét}}(X, \mu_l^{\otimes i}) = H^0_{\text{ét}}(X, \mathbb{F}_l) \), where \( \mu_l \) is the étale sheaf of \( l \)-th roots of unity on \( X \). By Kummer class map \( H^0_{\text{ét}}(X, \mathbb{G}_m) \to H^1_{\text{ét}}(X, \mathbb{F}_l) \), each \( f_i \) defines a class \( c(f_i) \in H^1_{\text{ét}}(X, \mathbb{F}_l) \). Recall that \( H^2_{\text{ét}}(X, \mathbb{F}_l) \) classifies equivalence classes of gerbes over \( X \) with band \( \mathbb{F}_l \) ([Br1; Theorem 5.2.8], [Gi])

\[
H^2_{\text{ét}}(X, \mathbb{F}_l) \simeq \{ \text{equiv. classes of gerbes over } X \text{ with band } \mathbb{F}_l \}.
\]

Hence the cup product \( c(f_1) \cup c(f_2) \) defines an isomorphism class of gerbes with band \( \mathbb{F}_l \), denoted by \((f_1, f_2)_t\). In more concrete terms, \((f_1, f_2)_t\) is the gerbe associated to the central extension of group schemes over \( X \)

\[
1 \longrightarrow \mathbb{F}_l \longrightarrow H(\mathbb{F}_l) \longrightarrow \mathbb{F}_l^{\oplus 2} \longrightarrow 1
\]

and the \( \mathbb{F}_l^{\oplus 2} \)-covering \( \mathcal{C}^{(t)}(f_1, f_2) := \text{Spec}(k[t, (t-a_i)^{-1}(1 \leq i \leq r); f_1^{1/t}, f_2^{1/t}]) \to X \). So the gerbe \((f_1, f_2)_t\) is the obstruction to lifting of the \( \mathbb{F}_l^{\oplus 2} \)-covering \( \mathcal{C}^{(t)}(f_1, f_2) \to X \) to an \( H(\mathbb{F}_l) \)-covering ([Br1; 5.2], [Br2; 5]). The map \( \{f_1, f_2\} \to (f_1, f_2)_t \) is known to be the Soulé regulator ([So])

\[
K_2(X) \otimes \mathbb{F}_l \longrightarrow H^2_{\text{ét}}(X, \mathbb{F}_l).
\]
We note that \((f_1, f_2) = 1\) if and only if there is a trivialization of \((f_1, f_2)_l\), namely, an \(H(\mathbb{F}_l)\)-covering over \(X\), which lifts \(C(l)(f_1, f_2) \to X\). Without loss of generality, we may assume \(c = 1\) for \(C(l)\) and \(D(l)\), and let \(A = \{\infty, 0, 1\}\) and \(f_1 = 1 - t, f_2 = t\). Then \(C(l)(1 - t, t) = C(l)\) and so the \(H(\mathbb{F}_l)\)-covering \(D(l)|_X \to X\) gives a trivialization of \((1 - t, t)_l\).

Summing up, we have the following comparison. So our \(H(\mathbb{F}_l)\)-covering \(D(l)|_X \to X\) may be regarded as a categorical higher analog of the dilogarithmic function.

| Deligne line bundle \((f_1, f_2) \in H^2_B(X, \mathbb{Z}(2))\) | Gerbe associated to \(H_3(\mathbb{F}_l)\) \((f_1, f_2)_l \in H^2_{\text{et}}(X, \mathbb{F}_l)\) |
|-------------------------|-------------------------|
| Bloch-Beilinson regulator \(K_2(X) \to H^2_B(X, \mathbb{Z}(2))\) | Soulé regulator \(K_2(X) \to H^2_{\text{et}}(X, \mathbb{F}_l)\) |
| Trivialization of \((1 - t, t)_l\): Dilogarithmic function \(Li_2(t) = -\int_0^t \log(1 - t)\frac{dt}{t}\) | Trivialization of \((1 - t, t)_l\): Mod \(l\) Heisenberg covering \(D(l)|_X \to X\) |

3. Mod \(l\) Milnor invariants of primes for \(l = 2, 3\)

In this section, we review the arithmetic of mod 2 (resp. mod 3) Milnor invariants of rational primes (resp. primes of \(\mathbb{Q}(\zeta_3)\)), which has been studied in [AMM] and [Mo1] \(\sim\) [Mo4].

3.1. Maximal pro-\(l\) Galois groups with restricted ramification for \(l = 2, 3\). Let \(k\) be a finite algebraic number field such that \(k\) contains \(\zeta_l := \exp\left(\frac{2\pi i}{l}\right)\) and the class number of \(k\) is one. Let \(S\) be a finite subset of \(s\) distinct finite primes which are not lying over \(l\), \(S := \{p_1, \ldots, p_s\}\). Note that \(Np_i \equiv 1\) mod \(l\) \((1 \leq i \leq s)\). Let \(k_S(l)\) denote the maximal pro-\(l\) extension of \(k\), unramified outside \(S \cup S_k^\infty\), in a fixed algebraic closure \(\bar{k}\), where \(S_k^\infty\) denotes the set of infinite primes of \(k\). Let \(G_{k,S}(l)\) denote the Galois group of \(k_S(l)\) over \(k\). We describe the structure of the pro-\(l\) group \(G_{k,S}(l)\) in a certain unobstructed case.

We firstly recall Iwasawa’s result on the local Galois group ([Iw]). For each \(i\) \((1 \leq i \leq s)\), let \(k_{p_i}\) be the \(p_i\)-adic field with a prime element \(\pi_i\). We fix an algebraic closure \(\overline{k}_{p_i}\) of \(k_{p_i}\) and an embedding \(\bar{k} \hookrightarrow \overline{k}_{p_i}\). Let \(k_{p_i}(l)\) denote
the maximal pro-$l$ extension of $k_{p_i}$ in $\overline{k_{p_i}}$ and $G_{k_{p_i}}(l)$ denote the Galois group of $k_{p_i}(l)$ over $k_{p_i}$. Then we have

$$k_{p_i}(l) = k_{p_i}(\zeta_{l^n}, \sqrt[l]{\pi_i} \mid a \geq 1),$$

where $\zeta_{l^n}$ denotes a primitive $l^n$-th root of unity in $\bar{k}$ such that $(\zeta_{l^n})^{l^c} = \zeta_{l^{b-c}}$ for all $b \geq c$. The local Galois group $G_{k_{p_i}}(l)$ is then topologically generated by the monodromy $\tau_i$ and (an extension of) the Frobenius automorphism $\sigma_i$ which are defined by

$$\tau_i(\zeta_{l^n}) := \zeta_{l^n}, \quad \tau_i(\sqrt[l]{\pi_i}) := \zeta_{l^{n\sqrt[l]{\pi_i}}},$$

$$\sigma_i(\zeta_{l^n}) := \zeta_{l^{n\pi_i}}, \quad \sigma_i(\sqrt[l]{\pi_i}) := \sqrt[l]{\pi_i}$$

and subject to the relation

$$(3.1.1) \quad \tau_i^{-1}[\tau_i, \sigma_i] = 1.$$

For each $i$ ($1 \leq i \leq s$), the fixed embedding $\bar{k} \hookrightarrow \overline{k_{p_i}}$ gives an embedding $k_S(l) \hookrightarrow k_{p_i}(l)$, hence a prime $\mathfrak{P}_i$ of $k_S(l)$ lying over $p_i$. We denote by the same letters $\tau_i$ and $\sigma_i$ the images of $\tau_i$ and $\sigma_i$, respectively, under the homomorphism

$$G_{k_{p_i}}(l) \longrightarrow G_{k,S}(l)$$

induced by the embedding $k_S(l) \hookrightarrow k_{p_i}(l)$. Then $\tau_i$ is a topological generator of the inertia group of the prime $\mathfrak{P}_i$ and $\sigma_i$ is an extension of the Frobenius automorphism of the maximal subextension of $k_S(l)/k$ for which $\mathfrak{P}_i$ is unramified. We call simply $\tau_i$ and $\sigma_i$ a monodromy over $p_i$ in $k_S(l)/k$ and a Frobenius automorphism over $p_i$ in $k_S(l)/k$, respectively.

Since the ideal class group of $k$ is trivial, class field theory tells us that the monodromies $\tau_1, \ldots, \tau_s$ generate topologically the global Galois group $G_{k,S}(l)$. However, they may not be a minimal set of generators in general. In fact, noting that $k$ contains $\zeta_l$, Shafarevich’s theorem ([Kc; Satz 11.8]) tells us that the minimal number $d(G_{k,S}(l))$ of generators of $G_{k,S}(l)$ is given by

$$(3.1.2) \quad d(G_{k,S}(l)) = s - r_C(k) + \dim_{\mathbb{F}_l} B^{(l)}_{k,S}.$$

Here $r_C(k)$ denotes the number of complex primes (up to conjugation) of $k$ and the obstruction $B^{(l)}_{k,S}$ is defined by

$$B^{(l)}_{k,S} := \{ a \in k^\times \mid (a) = a', a \in (k^\times_p)^l \text{ for all } p \in S \cup S_k^\infty \}/(k^\times)^l,$$
where \( \mathfrak{a} \) is a fractional ideal of \( \mathcal{O}_k \).

In the following, we deal with the case that \( l = 2 \) and \( k = \mathbb{Q} \) or the case that \( l = 3 \) and \( k = \mathbb{Q}(\zeta_3) \). For these cases, we can determine \( B_{k,S}^{(l)} \) and, moreover, we can show that the relations for minimal generators of \( G_{k,S}(l) \) are given by the local relations (3.1.1).

- The case that \( l = 2 \) and \( k = \mathbb{Q} \). We have \( r_C(\mathbb{Q}) = 0 \) and we can easily verify \( B_{(2)Q,S}^{(2)} = \{1\} \) for any \( S = \{(p_1), \ldots, (p_s)\} \), where \( p_i \)'s are odd prime numbers. Therefore, by (3.1.2), we have \( d(G_{Q,S}(2)) = s \), namely, \( \tau_1, \ldots, \tau_s \) are minimal generators of \( G_{Q,S}(2) \). By Koch’s theorems [Kc; Satz 6.11] ([Kc; Satz 6.14]) and [Kc; Satz 11.3], the relations for these minimal generators are given by the local relations (3.1.1). Hence, we have the following

**Theorem 3.1.3** ([Mo4; Theorem 7.4]). *The pro-2 group \( G_{Q,S}(2) \) has the following minimal presentation*

\[
G_{Q,S}(2) = \langle x_1, \ldots, x_s \mid x_1^{p_1-1}[x_1, y_1] = \cdots = x_s^{p_s-1}[x_s, y_s] = 1 \rangle
= \widehat{F}_s^{(2)}/N_S^{(2)}.
\]

*Here \( \widehat{F}_s^{(2)} \) is the free pro-2 group generated by letters \( x_1, \ldots, x_s \) where \( x_i \) denotes a monodromy \( \tau_i \) over \( p_i \) in \( \mathbb{Q}_S(2)/\mathbb{Q} \), and \( N_S^{(2)} \) is the closed subgroup of \( \widehat{F}_s^{(2)} \) normally generated by \( x_1^{p_1-1}[x_1, y_1], \ldots, x_s^{p_s-1}[x_s, y_s] \) where \( y_i \) is the free pro-2 word in \( \widehat{F}_s^{(2)} \) which represents a Frobenius automorphism over \( p_i \) in \( \mathbb{Q}_S(2)/\mathbb{Q} \).*

- The case that \( l = 3 \) and \( k = \mathbb{Q}(\zeta_3) \). We have \( r_C(\mathbb{Q}(\zeta_3)) = 1 \) and, by [AMM; Proposition 1.8], \( B_{(3)Q(S)}^{(3)} = \{1\} \) if and only if \( S \) contains a prime \( p \) satisfying \( Np \equiv 4 \text{ or } 7 \mod 9 \). We let \( S_0 := \{p_1, \ldots, p_{s-1}\} \) with \( s \geq 2 \) and \( N_{p_i} \equiv 1 \mod 9 \) \( (1 \leq i \leq s) \) and let \( S := S \cup \{p_s\} \) with \( N_{p_s} \equiv 4 \text{ or } 7 \mod 9 \). By (3.1.2), we have \( d(G_{Q(S)}(3)) = s - 1 \), namely, one of \( \tau_1, \ldots, \tau_s \) is redundant for minimal generators of \( G_{Q(S)}(3) \). It is shown in [AMM; Proposition 1.9] that we can exclude the monodromy over \( p_s \) to obtain minimal generator of \( G_{Q(S)}(3) \). By [Kc; Satz 6.11] ([Kc; Satz 6.14]), [Kc; Satz 11.3] and [Kc; Satz 11.4], we have the following

**Theorem 3.1.4** ([AMM; Theorem 1.10]). *The pro-3 group \( G_{Q(S)}(3) \) has*
the following minimal presentation
\[
G_{\mathbb{Q}(\zeta_3), S}(3) = \langle x_1, \ldots, x_{s-1} \mid x_1^{N_{p_1}-1}[x_1, y_1] = \cdots = x_s^{N_{p_{s-1}}-1}[x_{s-1}, y_{s-1}] = 1 \rangle = \hat{F}_{s-1}(3)/N_S^{(3)}.
\]

Here \(\hat{F}_{s-1}(3)\) is the free pro-3 group generated by letters \(x_1, \ldots, x_{s-1}\) where \(x_i\) represents a monodromy \(\tau_i\) over \(p_i\) in \(\mathbb{Q}(\zeta_3)S/(\zeta_3)\), and \(N_S^{(3)}\) is the closed subgroup of \(\hat{F}_{s-1}(3)\) normally generated by \(x_1^{N_{p_1}-1}[x_1, y_1], \ldots, x_{s-1}^{N_{p_{s-1}}-1}[x_{s-1}, y_{s-1}]\) where \(y_i\) is the free pro-2 word in \(\hat{F}_{s-1}(3)\) which represents a Frobenius automorphism over \(p_i\) in \(\mathbb{Q}(\zeta_3)S/(\zeta_3)\).

3.2. Mod l Milnor invariants of primes for \(l = 2, 3\). In this subsection, we recall mod 2 Milnor invariants of rational primes and mod 3 Milnor invariants of primes in \(\mathbb{Q}(\zeta_3)\). We keep the same notations as in Subsection 3.1.

• Mod 2 Milnor invariants of rational primes. Let \(\hat{F}_s^{(2)}\) be the free pro-2 group generated by \(x_1, \ldots, x_s\) where each \(x_i\) represents a monodromy over \(p_i\), as in Theorem 3.1.3. Let \(\Theta_2 : F_2[[\hat{F}_s^{(2)}]] \xrightarrow{\sim} F_2\langle X_1, \ldots, X_s \rangle\) be the mod 2 Magnus isomorphism in (1.3.2). For a multi-index \(I\) and \(1 \leq j \leq s\), we let \(\mu_2(Ij) := \mu_2(I; y_j)\), where the pro-2 word \(y_j\) represents a Frobenius automorphism over \(p_j\), so that we have

\[
\Theta_2(y_j) = 1 + \sum_{|I| \geq 1} \mu_2(Ij)X_I.
\]

We set \(\mu_2(I) := 0\) if \(|I| = 1\). Let \(e_S := \max\{e | p_1 \equiv 1 \mod 2^e (1 \leq i \leq s)\}\).

**Theorem 3.2.1** ([Mo4; 8.4]). (1) For \(i \neq j\), we have

\[
(-1)^{\mu_2(ij)} = \left(\frac{p_i}{p_j}\right),
\]

where \(\left(\frac{p_i}{p_j}\right)\) stands for the Legendre symbol.

(2) Let \(I = (i_1 \cdots i_n)\) be a multi-index with \(2 \leq n \leq 2^{e_S}\). If \(\mu_2(j_1 \cdots j_m) = 0\) for any proper subset \(\{j_1, \ldots, j_m\}\) of \(\{i_1, \ldots, i_n\}\), then \(\mu_2(I)\) is an invariant, called mod 2 Milnor invariants, of an ordered set \(\{i_1, \ldots, i_n\}\).
• Mod 3 Milnor invariants of primes in $\mathbb{Q}(\zeta_3)$. Let $\hat{F}_{s-1}^{(3)}$ be the free pro-3 group generated by $x_1, \ldots, x_{s-1}$, where each $x_i$ represents a monodromy over $p_i$, as in Theorem 3.1.4. Let $\Theta_3 : \mathbb{F}_3[[\hat{F}_{s-1}^{(3)}]] \rightarrow \mathbb{F}_3\langle\langle X_1, \ldots, X_{s-1}\rangle\rangle$ be the mod 3 Magnus isomorphism in (1.3.2). For a multi-index $I$ and $1 \leq j \leq s$, we let $\mu_3(\iota^j) := \mu_3(I; y_j)$, where the pro-3 word $y_j$ represents a Frobenius automorphism over $p_j$, so that we have

$$\Theta_3(y_j) = 1 + \sum_{|I| \geq 1} \mu_3(\iota^j)X_I.$$  

We set $\mu_3(I) := 0$ if $|I| = 1$. We choose the unique prime element $\pi_i$ ($1 \leq i \leq s - 1$) such that $\pi_i \equiv 1 \mod (3\sqrt{3}-3)$.

**Theorem 3.2.2.** (1) ([AMM; Theorem 3.6]). For $i \neq j$, we have

$$\zeta_3^{\mu_3(\iota^j)} = \left(\frac{\pi_i}{\pi_j}\right)_3,$$

where $\left(\frac{\pi_i}{\pi_j}\right)_3$ stands for the cubic residue symbol.

(2) ([AMM; Proposition 4.3, Theorem 4.4]). Let $i, j, k$ be distinct indices, $1 \leq i, j, k \leq s - 1$. Assume that $p_i$ and $p_j$ are generated by rational prime numbers and that $\mu_3(ab) = 0$ for $a, b \in \{i, j, k\}$. Then $\mu_3(\iota^{ijk})$ is independent of a choice of $p_s$ and an invariant, called the mod 3 Milnor invariant, of an ordered set $\{i, j, k\}$.

**Remark 3.2.3.** As in Remark 1.3.8 (1), by using the relation between Magnus coefficients and Massey products ([Dw],[St]), it was shown in [Mo 3] and [AMM; 7] that the mod $l$ Milnor invariants of primes are expressed by Massey products of the mod $l$ cohomology of the Galois group $G_{k,S}(l)$ for $l = 2, k = \mathbb{Q}$ or $l = 3, k = \mathbb{Q}(\zeta_3)$.

4. Triple quadratic and cubic residue symbols in Ihara theory

In this section, we interpret quadratic (resp. cubic) residue symbols as mod 2 (resp. mod 3) Milnor invariants of Galois elements in Ihara theory.
4.1. Triple quadratic residue symbols (Rédei symbols). Let \( p_1 \) and \( p_2 \) be distinct prime numbers satisfying

\[
p_i \equiv 1 \mod 4 \ (i = 1, 2), \quad \left( \frac{p_i}{p_j} \right) = 1 \ (1 \leq i \neq j \leq 2).
\]

By the assumption (4.1.1), there are integers \( x, y \) and \( z \) such that

\[
x^2 - p_1 y^2 - p_2 z^2 = 0, \ (x, y, z) = 1, \ x - y \equiv 1 \mod 4.
\]

We set

\[
R^{(2)} := R^{(2)}_{\{p_1, p_2\}} := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha}), \ \alpha := x + \sqrt{p_1}y.
\]

It is the unique Galois extension of \( \mathbb{Q} \), determined by the set \( \{p_1, p_2\} \), having the following properties: its Galois group is the dihedral group \( H(\mathbb{F}_2) \) of order 8 and it is unramified outside \( p_1, p_2 \) and the infinite prime ([A], [R]). Let \( p_3 \) be a prime number satisfying

\[
p_3 \equiv 1 \mod 4, \quad \left( \frac{p_i}{p_j} \right) = 1 \ (1 \leq i \neq j \leq 3).
\]

Let \( K^{(2)} := K^{(2)}_{\{p_1, p_2, p_3\}} := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}) \). For a prime \( \tilde{p} \) of \( K^{(2)} \) lying over \( p_3 \), the Rédei symbol is defined by

\[
[p_1, p_2, p_3] := \frac{(R^{(2)}/K^{(2)})_{\tilde{p}}(\sqrt{\alpha})}{\sqrt{\alpha}},
\]

which is independent of a choice of \( \tilde{p} \) ([A], [R]).

By Theorems 3.2.1 applied to the case \( S := \{p_1, p_2, p_3\} \) with the assumptions (4.1.1) and (4.1.4) satisfied, the mod 2 triple Milnor invariant \( \mu_2(123) \) of rational primes \( \{p_1, p_2, p_3\} \) is well defined. The following theorem gives an interpretation of the Rédei symbol in terms of a mod 2 triple Milnor invariant.

**Theorem 4.1.6 ([Mo4; 8.4]).** We have

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

Now we shall interpret the Rédei symbol as a mod 2 Milnor invariant of a Galois element in Ihara theory. Following the notations in the sections 1 and 2, we consider the case where \( l = 2, k = \mathbb{Q} \) and \( A = \{a_0, a_1, a_2, a_3\} \) with

\[
a_0 := \infty, a_1 := 0, a_2 := x^2, a_3 := p_1 y^2.
\]
Let $K^{(2)}_{\{x,t\}}$ be the $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$-extension of $\mathbb{Q}(t)$ in (2.1.1) and let $R^{(2)}_{\{x,t\}}$ be the dilogarithmic $H(\mathbb{F}_2)$-extension of $\mathbb{Q}(t)$ in (2.1.2), with $l = 2$ and $c = x$:

$$R^{(2)}_{\{x,t\}} := K^{(2)}_{\{x,t\}}(\sqrt{\varepsilon_2(t)}) = \mathbb{Q}(t)(\sqrt{t}, \sqrt{x^2 - t}, \sqrt{\varepsilon_2(t)}), \quad \varepsilon_2(t) := x + \sqrt{t}.$$  

(4.1.7)

We note by (4.1.2), (4.1.3) and (4.1.7) that $K^{(2)}_{\{x,t\}}$ and $R^{(2)}_{\{x,t\}}$ are specialized to $K^{(2)}_{\{p_1,p_2\}}$ and $R^{(2)}_{\{p_1,p_2\}}$, respectively, by the evaluation $c = x, t = p_1 y^2$:

$$K^{(2)}_{\{x,p_1 y^2\}} = K^{(2)}_{\{p_1,p_2\}}, \quad R^{(2)}_{\{x,p_1 y^2\}} = R^{(2)}_{\{p_1,p_2\}}, \quad \varepsilon_2(p_1 y^2) = \alpha.$$

Let $\Omega_A$ be the Ihara field of definition for $A$ in (1.1.7). By Theorem 2.6, we have

$$R^{(2)}_{\{p_1,p_2\}} \subset \Omega_A.$$

Let $S_A$ be as in (1.1.8). We suppose that $p_3$ satisfies $(p_3) / \in S_A$ as well as (4.1.4). Let $\mathfrak{P}$ be an extension of $p_3$ to $\Omega_A$ and let $\sigma_{\mathfrak{P}}$ be the Frobenius automorphism of $\mathfrak{P}$ over $\mathbb{Q}$.

**Proposition 4.1.8.** Let the notations and assumptions be as above. For any $i, j \in \{1, 2, 3\}$, we have

$$\mu_2(\sigma_{\mathfrak{P}}; ij) = 0.$$  

Hence $\mu_2(\sigma_{\mathfrak{P}}; ij3)$ is independent of a choice of $\mathfrak{P}$ by Collorary 1.3.6 and so it is denoted by $\mu_2(\sigma_{p_3}; ij3)$. Then we have

$$f_3(\sigma_{\mathfrak{P}}) \equiv \prod_{i=1}^3 x_i^{2\mu_2(\sigma_{p_3}; ij3)} \prod_{1 \leq i < j \leq 3} [x_i, x_j]^{\mu_2(\sigma_{p_3}; ij3)} \mod \hat{F}_3^{(2)}(3),$$

where $\hat{F}_3^{(2)}(3) = (\hat{F}_3^{(2)}(2))^2[\hat{F}_3^{(2)}, [\hat{F}_3^{(2)}, \hat{F}_3^{(2)}]]$ is the 3rd term of the mod 2 Zassenhaus filtration of $\hat{F}_3^{(2)}$ (cf. (1.3.3)).

**Proof.** For $i \neq j$, we have $a_i - a_j = \pm x^2, \pm p_1 y^2, \pm p_2 z^2$ by (4.1.2). So the first assertion follows from Theorem 1.3.7 and the assumptions (4.1.1) and (4.1.4), and so we have $f_3(\sigma_{\mathfrak{P}}) \in \hat{F}_3^{(2)}(2)$. Note by (1.3.3) that $\hat{F}_3^{(2)}(2) / \hat{F}_3^{(2)}(3)$ has a basis $x_1^2, x_2^2, x_3^2, [x_1, x_2], [x_2, x_3], [x_1, x_3]$ over $\mathbb{F}_2$. Then the second assertion
follows from the definition of mod 2 Milnor invariants. □

**Proposition 4.1.9.** The monodromy transformation of $\sqrt{\varepsilon_2(t)}$ along the pro-2 longitude $f_3(\sigma_\Psi)$ is given by

$$\sqrt{\varepsilon_2(t)} \mapsto [p_1, p_2, p_3] \sqrt{\varepsilon_2(t)}.$$  

*Proof.* First, we note the followings.

(i) By induction on $n \geq 0$, we easily see

$$\frac{d^n}{dt^n} \sqrt{\varepsilon_2(t)} \bigg|_{t = p_1y^2} = \sqrt{\alpha} \cdot \Phi_n(\alpha, y\sqrt{p_1})$$

for some $\Phi_n(X_1, X_2) \in \mathbb{Q}(X_1, X_2)$.

(ii) By (4.1.4) and (4.1.5), we have

$$\chi_2(\sigma_\Psi) \equiv 1 \mod 4, \sigma_\Psi(\sqrt{p_1}) = \sqrt{p_1}, \text{ and } \sigma_\Psi(\sqrt{\alpha}) = [p_1, p_2, p_3] \sqrt{\alpha}.$$

(iii) We easily see $\iota_0(\sqrt{\varepsilon_2(t)}) \in \mathbb{Q}\{1/t\}$.

Then the monodromy transformation of $\sqrt{\varepsilon_2(t)}$ along the pro-2 longitude $f_3(\sigma_\Psi) = s_0(\sigma_\Psi) \cdot \gamma_3^{-1} \cdot s_3(\sigma_\Psi)^{-1} \cdot \gamma_3$ is given as follows:

$$\iota_0(\sqrt{\varepsilon_2(t)}) \xrightarrow{\gamma_3} \sqrt{\alpha} \sum_{n=0}^{\infty} \Phi_n(\alpha, y\sqrt{p_1})(t - p_1y^2)^n \text{ (by (i))}$$

$$\xrightarrow{s_3(\sigma_\Psi)^{-1}} [p_1, p_2, p_3] \sqrt{\alpha} \sum_{n=0}^{\infty} \Phi_n(\alpha, y\sqrt{p_1})(t - p_1y^2)^n \text{ (by (ii))}$$

$$\xrightarrow{\gamma_3^{-1}} [p_1, p_2, p_3] \iota_0(\sqrt{\varepsilon_2(t)})$$

$$\xrightarrow{s_0(\sigma_\Psi)} [p_1, p_2, p_3] \iota_0(\sqrt{\varepsilon_2(t)}) \text{ (by (iii))}. \ □$$

**Theorem 4.1.10.** We have

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

and hence

$$\mu_2(123) = \mu_2(\sigma_{p_3}; 123).$$

*Proof.* Since $\mathcal{K}_{(x,t)}^{(2)}$ is a metabelian extension of $k(t)$, any element of $\hat{F}_3^{(2)}(3)$
acts on $\sqrt{\varepsilon_2(t)}$ trivially. Then the assertion follows from Proposition 4.1.8, Corollary 2.1.6 and Proposition 4.1.9. □

4.2. Triple cubic residue symbols. Let $p_1$ and $p_2$ be distinct primes of $\mathbb{Q}(\zeta_3)$ with $Np_i \equiv 1 \pmod{9}$. We assume that each $p_i$ is generated by a rational prime number. Let $\pi_i$ be the unique prime element of $p_i$ such that $\pi_i \equiv 1 \pmod{(3\sqrt{-3})}$. We assume that

$$\left(\frac{\pi_i}{\pi_j}\right)_3 = 1 \quad (1 \leq i \neq j \leq 2).$$

Let $K_1 := k(\sqrt[3]{\pi})$ and let $\tau$ be the generator of the Galois group of $k(\sqrt[3]{\pi})$ defined by $\tau(\sqrt[3]{\pi}) = \zeta_3 \sqrt[3]{\pi}$. By (4.2.1), there is $\alpha$ in $O_{K_1}$ such that

$$N_{K_1/k}(\alpha) = \pi_2 z^3, \quad (\alpha) = \mathfrak{P}^e \mathfrak{B}^f$$

with $(e, 3) = 1$, $(\mathfrak{B}, 3) = 1$, $f \equiv 0 \pmod{3}$, where $z \in \mathbb{Z}[\zeta_3]$ and $\mathfrak{P}, \mathfrak{B}$ are ideals of $\mathbb{Z}[\zeta_3]$. We let

$$\theta := \tau(\alpha)(\tau^2(\alpha))^2$$

and set

$$R^{(3)} := R^{(3)}_{\{p_1, p_2\}} := \mathbb{Q}(\zeta_3)(\sqrt[3]{\pi_1}, \sqrt[3]{\pi_2}, \sqrt[3]{\theta}).$$

It is the unique Galois extension of $\mathbb{Q}(\zeta_3)$, determined by the set $\{p_1, p_2\}$, having the following properties: its Galois group is isomorphic to $H(\mathbb{F}_3)$ and only $p_1$ and $p_2$ are ramified with ramification indices being 3 ([AMM; Theorem 5.11, Corollary 5.12]). Let $p_3$ be a prime of $\mathbb{Q}(\zeta_3)$ such that $Np_3 \equiv 1 \pmod{9}$ and let $\pi_3$ be the unique prime element in $p_3$ such that $\pi_3 \equiv 1 \pmod{(3\sqrt{-3})}$. We assume that

$$\left(\frac{\pi_i}{\pi_j}\right)_3 = 1 \quad (1 \leq i \neq j \leq 3).$$

Let $K^{(3)} := K^{(3)}_{\{p_1, p_2\}} := \mathbb{Q}(\zeta_3)(\sqrt[3]{\pi_1}, \sqrt[3]{\pi_2})$. For a prime $\tilde{p}$ of $K^{(3)}$ lying over $p_3$, we define the triple cubic residue symbol by

$$[p_1, p_2, p_3]_3 := \left(\frac{R^{(3)/K^{(3)}}}{\tilde{p}}\right)(\sqrt[3]{\theta}).$$
which is independent of the choice of a prime $\tilde{p}$.

By Theorems 3.2.2 applied to the case $S := \{p_1, p_2, p_3\}$ with the assumptions (4.2.1) and (4.2.5) satisfied, the mod 3 triple Milnor invariant $\mu_3(123)$ of primes $\{p_1, p_2, p_3\}$ is well defined. The following theorem gives an interpretation of the Rédei symbol in terms of a mod 3 triple Milnor invariant.

**Theorem 4.2.7** ([AMM; Definition 6.2, Theorem 6.3]). We have

$$\zeta_3^{\mu_3(123)} = [p_1, p_2, p_3]_3.$$ 

Now we shall interpret the triple cubic residue symbol as a mod 3 Milnor invariant of a Galois element in Ihara theory. In the following, we assume that $\alpha \in \mathcal{O}_{K_1}$ in (4.2.2) is of the form

$$(4.2.8) \quad \alpha = x + y\sqrt[3]{\pi_1}$$

for some $x, y \in \mathbb{Q}(\zeta_3)$ and so $N_{K_1/k}(\alpha) = \pi_2 z^2$ in (4.2.2) and $\theta$ in (4.2.3) are written as

$$(4.2.9) \quad x^3 + \pi_1 y^3 = \pi_2 z^3.$$ 

and

$$(4.2.10) \quad \theta = (x + \zeta_3 y \sqrt[3]{\pi_1})(x + \zeta_2 y \sqrt[3]{\pi_1})^2.$$ 

Following the notations in the sections 1 and 2, we consider the case where $l = 3$, $k = \mathbb{Q}(\zeta_3)$ and $A = \{a_0, a_1, a_2, a_3\}$ with

$$a_0 := \infty, a_1 := 0, a_2 := x^3, a_3 := -\pi_1 y^3.$$ 

Let $\mathcal{K}_{\{x,t\}}^{(3)}$ be the $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$-extension of $\mathbb{Q}(\zeta_3)(t)$ in (2.1.1) and let $\mathcal{R}_{\{x,t\}}^{(3)}$ be the dilogarithmic $H(\mathbb{F}_3)$-extension of $\mathbb{Q}(\zeta_3)(t)$ in (2.1.2), with $l = 3$ and $c = x$:

$$(4.2.11) \quad \mathcal{R}_{\{x,t\}}^{(3)} := \mathcal{K}_{\{x,t\}}^{(3)}(\sqrt[3]{\varepsilon_3(t)}), \quad \varepsilon_3(t) := (x - \zeta_3 \sqrt[3]{\pi_1})(x - \zeta_2 \sqrt[3]{\pi_1})^2.$$ 

We note by (4.2.4), (4.2.9), (4.2.10) and (4.2.11) that $\mathcal{K}_{\{x,t\}}^{(3)}$ and $\mathcal{R}_{\{x,t\}}^{(3)}$ are specialized to $K_{\{p_1,p_2\}}^{(3)}$ and $R_{\{p_1,p_2\}}^{(3)}$, respectively, by the evaluation $c = x, t = -\pi_1 y^3$:

$$\mathcal{K}_{\{x,-\pi_1 y^3\}}^{(3)} = K_{\{p_1,p_2\}}^{(3)}, \quad \mathcal{R}_{\{x,-\pi_1 y^3\}}^{(3)} = R_{\{p_1,p_2\}}^{(3)}, \quad \varepsilon_3(-\pi_1 y^3) = \theta.$$ 

28
Let $\Omega_A$ be the Ihara field of definition in (1.1.7). By Theorem 2.6, we have

$$R_{\{p_1, p_2\}}^{(3)} \subset \Omega_A.$$ 

Let $S_A$ be as in (1.1.8). We suppose that $p_3$ satisfies $p_3 \notin S_A$ as well as (4.2.5). Let $\mathfrak{P}$ be an extension of $p_3$ to $\Omega_A$ and let $\sigma_p$ be the Frobenius element of $\mathfrak{P}$ over $\mathbb{Q}(\zeta_3)$.

**Proposition 4.2.12.** Let the notations and assumptions be as above. For any $i, j \in \{1, 2, 3\}$, we have

$$\mu_3(\sigma_p; ij) = 0.$$ 

Hence $\mu_3(\sigma_p; ij3)$ is independent of a choice of $\mathfrak{P}$ by Corollary 1.3.6 and so it is denoted by $\mu_3(\sigma_{p_3}; ij3)$. Then we have

$$f_3(\sigma_p) \equiv \prod_{1 \leq i < j \leq 3} [x_i, x_j]^{\mu_3(\sigma_{p_3}; ij3)} \mod \hat{F}_3^{(3)}(3),$$

where $\hat{F}_3^{(3)}(3) = (\hat{F}_3^{(3)})^3(\hat{F}_3^{(3)}, [\hat{F}_3^{(3)}, \hat{F}_3^{(3)}])$ is the 3rd term of the mod 3 Zassenhaus filtration of $\hat{F}_3^{(3)}$ (cf. (1.3.3)).

**Proof.** For $i \neq j$, we have $a_i - a_j = \pm x^3, \pm \pi_1 y^3, \pm \pi_2 z^3$ by (4.2.9). So the first assertion follows from Theorem 1.3.7 and the assumptions (4.2.1) and (4.2.5), and so $f_3(\sigma_p) \in \hat{F}_3^{(3)}(2)$. Note by (1.3.3) that $\hat{F}_3^{(3)}(2)/\hat{F}_3^{(3)}(3)$ has a basis $[x_1, x_2], [x_2, x_3], [x_1, x_3]$ over $\mathbb{F}_3$. Then the second assertion follows from the definition of mod 3 Milnor invariants. $\square$

**Proposition 4.2.13.** The monodromy transformation of $\sqrt[3]{\varepsilon_3(t)}$ along the pro-3 longitude $f_3(\sigma_p)$ is given by

$$\sqrt[3]{\varepsilon_3(t)} \mapsto [p_1, p_2, p_3]^{-1} \sqrt[3]{\varepsilon_3(t)}.$$

**Proof.** The proof goes in a way similar to that of Proposition 4.1.9. First, we note the followings.

(i) By induction on $n \geq 0$, we easily see

$$\frac{d^n}{dt^n} \sqrt[3]{\varepsilon_3(t)} \bigg|_{t = -\pi_1 y^3} = \sqrt[3]{\theta} \cdot \Phi_n(\theta, y \sqrt[3]{\pi_1}).$$
for some $\Phi_n(X_1, X_2) \in \mathbb{Q}(X_1, X_2)$.

(ii) By (4.2.5) and (4.2.6), we have

$$\chi_3(\sigma_\Phi) \equiv 1 \mod 9, \quad \sigma_\Phi(\sqrt[3]{\pi_1}) = \sqrt[3]{\pi_1}, \text{ and } \sigma_\Phi(\sqrt[3]{\theta}) = [p_1, p_2, p_3]_3 \sqrt[3]{\theta}.$$ 

(iii) We easily see $\nu_0(\sqrt[3]{\varepsilon_3(t)}) \in \mathbb{Q}(\zeta_3)\{\{1/t\}\}$. Then the monodromy transformation of $\sqrt[3]{\varepsilon_3(t)}$ along the pro-3 longitude $f_3(\sigma_\Phi) = s_0(\sigma_\Phi) \cdot \gamma_3^{-1} \cdot s_3(\sigma_\Phi)^{-1} \cdot \gamma_3$ is given as follows:

$$\nu_0(\sqrt[3]{\varepsilon_3(t)}) \xrightarrow{\gamma_3} 3\sqrt[3]{\theta} \sum_{n=0}^\infty \Phi_n(\theta, y \sqrt[3]{\pi_1})(t + \pi_1 y^3)^n \ (\text{by (i)})$$

$$\xrightarrow{s_3(\sigma_\Phi)^{-1}} [p_1, p_2, p_3]_3^{-1} 3\sqrt[3]{\theta} \sum_{n=0}^\infty \Phi_n(\theta, y \sqrt[3]{\pi_1})(t + \pi_1 y^3)^n \ (\text{by (ii)})$$

$$\xrightarrow{\gamma_3^{-1}} [p_1, p_2, p_3]_3^{-1} \nu_0(\sqrt[3]{\varepsilon_3(t)})$$

$$\xrightarrow{s_0(\sigma_\Phi)} [p_1, p_2, p_3]_3^{-1} \nu_0(\sqrt[3]{\varepsilon_3(t)}) \ (\text{by (iii)}).$$

\textbf{Theorem 4.2.14.} We have

$$[p_1, p_2, p_3]_3^{-1} = \zeta_3^{\mu_3(\sigma_\Phi; 123)}$$

and hence

$$-\mu_3(123) = \mu_3(\sigma_\Phi; 123).$$

\textit{Proof.} Since $\mathcal{K}_{(x,t)}^{(3)}$ is a metabelian extension of $k(t)$, any element of $\hat{F}_3^{(3)}(3)$ acts on $\sqrt[3]{\varepsilon_3(t)}$ trivially. Then the assertion follows from Proposition 4.2.12, Corollary 2.1.6 and Proposition 4.2.13. \hfill \Box

\textbf{Example 4.2.15.} The assumptions (4.2.1) and (4.2.8) are satisfied for the cases $(-\pi_1, -\pi_2) = (17,53), (17,467), (107,449), (431, 233)$ etc. (This computation is due to Y. Mizusawa.)

Let $(-\pi_1, -\pi_2) = (17,53)$. Then we can take $x = 8, y = 3, z = -1$ and so

$$\alpha = 8 - 3\sqrt[3]{17}, \ \theta = (8 - 3\zeta_3\sqrt[3]{17})(8 - 3\zeta_3^2\sqrt[3]{17})^2$$

and

$$\mathcal{R}_{(8,3^3,17)}^{(3)} = R_{(17),(53)}^{(3)} = \mathbb{Q}(\zeta_3)(\sqrt[3]{17}, \sqrt[3]{53}, \sqrt[3]{\theta}).$$
By [AMM; Example 6.4], for $-\pi = 71, 89, 107, 179, 197$, we have

$$\mu_3(\sigma(71); 123) = -\mu_3(123) = 1, \quad \mu_3(\sigma(89); 123) = -\mu_3(123) = 2,$$
$$\mu_3(\sigma(107); 123) = -\mu_3(123) = 1, \quad \mu_3(\sigma(179); 123) = -\mu_3(123) = 2,$$
$$\mu_3(\sigma(197); 123) = -\mu_3(123) = 2.$$
Soc., Providence, RI, 1988.

[I3] Y. Ihara, Braids, Galois groups, and some arithmetic functions, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), 99–120, Math. Soc. Japan, Tokyo, 1991.

[Iw] K. Iwasawa, On Galois groups of local fields, Trans. Amer. Math. Soc. 80 (1955), 448–469.

[Kc] H. Koch, Galoissche Theorie der p-Erweiterungen, Springer-Verlag, Berlin-New York; VEB Deutscher Verlag der Wissenschaften, Berlin, 1970.

[Kd] H. Kodani, Arithmetic topology on braid and absolute Galois groups, Doctoral Thesis, Kyushu University, 2017.

[KMT] H. Kodani, M. Morishita, Y. Terashima, Arithmetic topology in Ihara theory, Publ. Res. Inst. Math. Sci., Kyoto Univ., 53, No.4. (2017), 629–688.

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

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

[Mo1] M. Morishita, Milnor’s link invariants attached to certain Galois groups over $\mathbb{Q}$, 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, 2011.

[MK] K. Murasugi, B.I. Kurpita, A study of braids, Mathematics and its Applications, 484, Kluwer Academic Publishers, Dordrecht, 1999.

[N] H. Nakamura, Tangential base points and Eisenstein power series, Aspects of Galois theory (Gainesville, FL, 1996), 202–217, London Math. Soc. Lecture Note Ser., 256, Cambridge Univ. Press, Cambridge, 1999.

[NW] H. Nakamura, Z. Wojtkowiak, On explicit formulae for $l$-adic polylogarithms, In: Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), 285–294, Proc. Sympos. Pure Math., 70, Amer. Math. Soc., Providence, RI, 2002.

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

[So] C. Soulé, $K$-théorie des anneaux d’entiers de corps de nombres et cohomologie étale, Invent. Math. 55 (1979), no. 3, 251–295.

[St] D. Stein, Massey products in the cohomology of groups with applications to link theory, Trans. Amer. Math. Soc. 318 (1990), 301–325.
[T] V. Turaev, 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.

[W1] Z. Wojtkowiak, On $l$-adic iterated integrals, I. Analog of Zagier conjecture, Nagoya Math. J. 176 (2004), 113–158.

[W2] Z. Wojtkowiak, On $l$-adic iterated integrals, II. Functional equations and $l$-adic polylogarithms, Nagoya Math. J. 177 (2005), 117–153.

[W3] Z. Wojtkowiak, On $l$-adic iterated integrals, III. Galois actions on fundamental groups. Nagoya Math. J. 178 (2005), 1–36.

[W4] Z. Wojtkowiak, On $l$-adic iterated integrals, IV. Ramification and generators of Galois actions on fundamental groups and torsors of paths, Math. J. Okayama Univ. 51 (2009), 47–69.

[W5] Z. Wojtkowiak, A remark on nilpotent polylogarithmic extensions of the field of rational functions of one variable over $\mathbb{C}$, Tokyo J. Math. 30 (2007), no. 2, 373–382.

Hikaru Hirano
Faculty of Mathematics, Kyushu University
744, Motooka, Nishi-ku, Fukuoka, 819-0395, JAPAN
e-mail: ma218019@math.kyushu-u.ac.jp

Masanori Morishita
Faculty of Mathematics, Kyushu University
744, Motooka, Nishi-ku, Fukuoka, 819-0395, JAPAN
e-mail: morisita@math.kyushu-u.ac.jp