Arithmetic topology in Ihara theory

To the memory of Professor Akito Nomura

Hisatoshi Kodani, Masanori Morishita and Yuji Terashima

Abstract. Ihara initiated to study a certain Galois representation which may be seen as an arithmetic analogue of the Artin representation of a pure braid group. We pursue the analogies in Ihara theory further and give foundational results, following after some issues and their inter-relations in the theory of braids and links such as Milnor invariants, Johnson homomorphisms, Magnus-Gassner cocycles and Alexander invariants, and study relations with arithmetic in Ihara theory.

Introduction

Let $l$ be a prime number. Let $S$ be a set of ordered $r + 1$ ($r \geq 2$) distinct $\overline{\mathbb{Q}}$-rational points on the projective line $\mathbb{P}^1$ over the rational number field $\mathbb{Q}$, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. Let $k := \mathbb{Q}(S \setminus \{\infty\})$, the finite algebraic number field generated by coordinates of points in $S \setminus \{\infty\}$. Note that the absolute Galois group $\text{Gal}_k := \text{Gal}(\overline{\mathbb{Q}}/k)$ is the étale fundamental group of $\text{Spec} \ k$ so that it acts on the geometric fiber $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus S$ of the fibration $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus S \to \text{Spec} \ k$ and hence on the pro-$l$ étale fundamental group $\pi_1^{\text{pro-}l}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus S) \simeq \tilde{\mathfrak{S}}_r$, where $\tilde{\mathfrak{S}}_r$ denotes the free pro-$l$ group on $r$ generators $x_1, \ldots, x_r$. In [Ih1], Ihara initiated to study this monodromy Galois representation

\begin{equation}
\text{Ih}_S : \text{Gal}_k \to \text{Aut}(\tilde{\mathfrak{S}}_r),
\end{equation}

particularly for the case $S = \{0, 1, \infty\}$ and $k = \mathbb{Q}$, in connection with deep arithmetic such as Iwasawa theory on cyclotomy and complex multiplications.

2010 Mathematics Subject Classification: 11R, 57M

Key words: Ihara representation, $l$-adic Milnor invariants, Pro-$l$ Johnson homomorphisms, Pro-$l$ Magnus-Gassner cocycles, $l$-adic Alexander invariants, Ihara power seires

H.K. is partly supported by Grants-in-Aid for JSPS Fellows 14J12303.

Y.T. is partly supported by Grants-in-Aid for Scientific Research (C) 25400083 and by CREST, JST.
of Fermat Jacobians. We note that the image of $\text{Ih}_S$ is contained in the subgroup consisting of $\varphi \in \text{Aut}(\mathcal{F}_r)$ such that $\varphi(x_i) \sim x_i^\alpha$ (conjugate) for $1 \leq i \leq r$ and $\varphi(x_1 \cdots x_r) = (x_1 \cdots x_r)^\alpha$ for some $\alpha \in \mathbb{Z}_l^\times$.

As explained in [Ih3], the Ihara representation (0.1) may be regarded as an arithmetic analogue of the Artin representation of a pure braid group ([Ar]). Let $P_r$ be the pure braid group with $r$ strings ($r \geq 2$). Note that $P_r$ is the topological fundamental group of the configuration space $D^r \setminus \Delta$ of ordered $r$ points on a 2-dimensional disk $D$, where $\Delta$ denotes the hyperdiagonal of $D^r$. For $Q = (z_1, \ldots, z_r) \in D^r \setminus \Delta$, we also write the same $Q$ for the subset $\{z_1, \ldots, z_r\}$ of $D$. Then $P_r$ acts, as the monodoromy, on the fiber $D \setminus Q$ of the universal bundle over a point $Q \in D^r \setminus \Delta$ and hence on the topological fundamental group $\pi_1(D \setminus Q) \simeq F_r$, where $F_r$ denotes the free group on $r$ generators $x_1, \ldots, x_r$. Thus we have the Artin representation

\begin{equation}
\text{Ar}_Q : P_r \longrightarrow \text{Aut}(F_r),
\end{equation}

which is in fact isomorphic onto the subgroup $\varphi \in \text{Aut}(F_r)$ such that $\varphi(x_i) \sim x_i$ for $1 \leq i \leq r$ and $\varphi(x_1 \cdots x_r) = x_1 \cdots x_r$.

We may see the following analogy between the Ihara representation (0.1) and the Artin representation (0.2):

\begin{equation}
\begin{array}{|c|c|}
\hline
\text{absolute Galois group} & \text{pure braid group} \\
\text{Gal}_{k} & P_r \\
\hline
\mathbb{P}^1_k \setminus S \rightarrow \text{Spec} k & \text{universal bundle over } D^r \setminus \Delta \\
\text{with geometric fiber } \mathbb{P}^1_k \setminus S & \text{with fibers } D \setminus Q \\
\hline
\text{Ihara representation of } \text{Gal}_{k} & \text{Artin representation of } P_r \\
on \pi^\text{pro-l}(\mathbb{P}^1_k \setminus S) = \mathcal{F}_r & \text{on } \pi_1(D \setminus Q) = F_r \\
\hline
\end{array}
\end{equation}

The aim of this paper is, based on the above analogy (0.3), to give foundational results obtained by pursuing pro-$l$ analogues for the Ihara representation of various objects derived from the Artin representation. To be precise, we shall investigate arithmetic (pro-$l$) analogues in Ihara theory of the following issues (I) $\sim$ (IV) and their inter-relations in the theory of braids and links:

(I) Milnor invariants of links,
(II) Johnson homomorphisms for the pure braid group $P_r$,
(III) Magnus-Gassner representations of $P_r$,
(IV) Alexander invariants of links.

2
Milnor invariants are higher order linking numbers of a link introduced by Milnor in [Mi]. For a pure braid link, they are defined as follows. For \( b \in P_r \) and each \( i \) \((1 \leq i \leq r)\), we can write \( \text{Art}_Q(b)(x_i) = y_i(b)x_iy_i(b)^{-1} \) for the unique \( y_i(b) \in F_r \), where the sum of exponents of \( x_i \) in the word \( y_i(b) \) is 0. The Milnor number \( \mu(b; i_1 \cdots i_n i) \in \mathbb{Z} \) is then defined to be the coefficient of \( X_{i_1} \cdots X_{i_n} \) in the Magnus expansion of \( y_i(b) \):

\[
y_i(b) = \sum_{1 \leq i_1, \ldots, i_n \leq r} \mu(b; i_1 \cdots i_n i)X_{i_1} \cdots X_{i_n} \quad (x_j = 1 + X_j).
\]

The Milnor invariant \( \overline{\mu}(\tilde{b}; i_1 \cdots i_n i) \) is defined by taking modulo a certain indeterminacy \( \Delta(b; i_1 \cdots i_n i) \):

\[
\overline{\mu}(\tilde{b}; i_1 \cdots i_n i) := \mu(b; i_1 \cdots i_n i) \mod \Delta(b; i_1 \cdots i_n i).
\]

It turns out that it is an invariant of the link \( \tilde{b} \) obtained by closing \( b \). The Milnor invariants are also interpreted in terms of Massey products in the cohomology of the link group ([Ki], [T]). Johnson homomorphisms are useful means to study the structure of the mapping class group of a surface ([J1], [J2], [Mt1], [Mt2]). The main tools are algebraic and applicable to the study of the automorphism group \( \text{Aut}(F_r) \) of a free group \( F_r \) ([Ka], [Sa]). Johnson homomorphisms describe the action of a certain filtration of \( \text{Aut}(F_r) \) on the nilpotent quotients \( F_r/F_r(n) \) for \( n \geq 1 \), where \( F_r(n) \) is the \( n \)-th term of the lower central series of \( F_r \). Since the pure braid group \( P_r \) is a subgroup of the mapping class group of \( r \) punctured disk, the theory of Johnson homomorphisms can also be applied to \( P_r \). It was shown in [Ko1], [Ko3; Chapter 1] that the Johnson homomorphisms are described by Milnor invariants of pure braid links. Magnus cocycles are crossed homomorphisms of \( P_r \) defined by using the Fox free derivation ([B; 3.1, 3.2], [F]). The Gassner representation Gass of \( P_r \) is a particular case of Magnus cocycles over the Laurent polynomial ring of \( r \) variables and the determinant \( \det(\text{Gass}(b) - I) \) gives the Alexander invariant which is a polynomial invariant of the link \( \tilde{b} \) ([B; 3.3]). The relations of the Gassner representations with Johnson homomorphisms and Milnor invariants were studied in [Ko2], [Ko3; Chapter 2].

In this paper, based on the analogy (0.3), we shall study arithmetic analogues in Ihara theory of these issues (I) \( \sim \) (IV). The contents of this paper are organized as follows. In Section 1, we recall the construction of the Ihara representations and some basic results. In Section 2, we define \( l \)-adic Milnor numbers for each element in \( \text{Gal}_k \) and \( l \)-adic Milnor invariants for certain primes of \( k(\zeta_{l^\infty}) \), the field obtained by adjoining all \( l \)-powerth roots of unity.
to $k$. We introduce the pro-$l$ link group of each element of $\text{Gal}_k$ and give a cohomological interpretation of $l$-adic Milnor invariants in terms of Massey products in the cohomology of the pro-$l$ link group. In Section 3, we present a general theory of the pro-$l$ Johnson map and pro-$l$ Johnson homomorphisms for the absolute Galois group $\text{Gal}_k$. A similar theory has been developed in the context of non-abelian Iwasawa theory ([MT]). Among other things, we describe the pro-$l$ Johnson homomorphisms in terms of $l$-adic Milnor numbers. Sections 2 and 3 may be regarded as an arithmetic counterpart of [Ko1], [Ko3; Chapter 1]. In Section 4, we introduce the pro-$l$ Magnus cocycles of $\text{Gal}_k$ by using the pro-$l$ Fox free calculus, and give a relation with pro-$l$ Johnson homomorphisms. We consider the pro-$l$ (reduced) Gassner cocycle of $\text{Gal}_k$ as a special case and express it by $l$-adic Milnor numbers. Section 4 may be regarded as an arithmetic counterpart of [Ko2], [Ko3; Chapter 2]. We note that Oda’s unpublished notes ([O1], [O2]) also concern some issues related to Sections 3, 4. In Section 5, we introduce the pro-$l$ link module and $l$-adic Alexander invariants. In Section 6, we consider the case that $S = \{0, 1, \infty\}$. We show that the Ihara power series $F_g(u_1, u_2) \ (g \in \text{Gal}_\mathbb{Q})$ introduced in [Ih1] coincides with our pro-$l$ reduced Gassner cocycle, and give a formula which expresses $F_g(u_1, u_2)$ in terms of $l$-adic Milnor numbers. Accordingly, using our formula and Ihara’s formula, we express the Jacobi sum in $\mathbb{Q}(\zeta_{p^n})$ as a $(\zeta_{p^n} - 1)$-adic expansion with coefficients $l$-adic Milnor numbers. Finally, combining our formula and the result by Ihara, Kaneko and Yukinari ([IKY]), we give some formula relating Soulé characters ([So]) with $l$-adic Milnor numbers.

This paper forms a (part of) elementary and group-theoretical foundation of arithmetic topology in Ihara theory. In the forthcoming papers, we shall study some connections of $l$-adic Milnor invariants and pro-$l$ Johnson homomorphisms in this paper with arithmetic of multiple power residue symbols in [Am], [Ms1], [Ms2; Chapter 8] and the works of Wojtkowiak on $l$-adic iterated integrals and $l$-adic polylogarithms ([NW], [W1] ~ [W4] etc). See Remark 2.2.12. We shall also study arithmetic analogues of some issues in quantum topology such as Habegger-Masbaum’s theorem on the relation between Milnor invariants and Kontsevich integrals ([HM]).

Notation. We denote by $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{C}$ the ring of rational integers, the field of rational numbers and the field of complex numbers, respectively. Throughout this paper, $l$ denotes a fixed prime number. We denote by $\mathbb{Z}_l$
and \( \mathbb{Q} \) the ring of \( l \)-adic integers and the field of \( l \)-adic numbers, respectively.

For \( a, b \) in a group \( G \), \( a \sim b \) means that \( a \) is conjugate to \( b \) in \( G \). 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 all \( a \in A, b \in B \).

For a positive integer \( n \) and a ring \( R \) with identity, \( M(n; R) \) denotes the ring of \( n \times n \) matrices whose entries are in \( R \) and \( \text{GL}(n; R) \) denotes the group of invertible elements of \( M(n; R) \).

1. The Ihara representation

In this section, we recall the set-up and some results on the Galois representation introduced by Ihara in [Ih1].

1.1. The outer Galois representation. Let \( x_1, \ldots, x_r \) be \( r \) letters \((r \geq 2)\) and let \( F_r \) denote the free group of rank \( r \) on \( x_1, \ldots, x_r \). Let \( x_{r+1} \) be the element of \( F_r \) defined by \( x_1 \cdots x_r x_{r+1} = 1 \) so that \( F_r \) has the presentation \( F_r = \langle x_1, \ldots, x_r, x_{r+1} | x_1 \cdots x_r x_{r+1} = 1 \rangle \). Let \( \mathfrak{F}_r \) denote the pro-\( l \) completion of \( F_r \). Let \( \text{Aut}(\mathfrak{F}_r) \) (resp. \( \text{Int}(\mathfrak{F}_r) \)) denote the group of topological automorphisms (resp. inner-automorphisms) of \( \mathfrak{F}_r \) with compact-open topology.

We note that any abstract automorphism of \( \mathfrak{F}_r \) is bicontinuous ([DDMS; Corollary 1.22]) and that \( \text{Aut}(\mathfrak{F}_r) \) is virtually a pro-\( l \) group ([DDMS; Theorem 5.6]). Let \( H \) be the abelianization of \( \mathfrak{F}_r \), \( H := \mathfrak{F}_r/[\mathfrak{F}_r, \mathfrak{F}_r] \), and let \( \pi : \mathfrak{F}_r \to H \) be the abelianization homomorphism. For \( f \in \mathfrak{F}_r \), we let \([f] := \pi(f)\). We set \( X_i := [x_i] \) \((1 \leq i \leq r+1)\) for simplicity so that \( H \) is the free \( \mathbb{Z}_l \)-module with basis \( X_1, \ldots, X_r \) and we have \( X_1 + \cdots + X_r + X_{r+1} = 0 \). Each \( \varphi \in \text{Aut}(\mathfrak{F}_r) \) induces an automorphism of the \( \mathbb{Z}_l \)-module \( H \) which is denoted by \([\varphi] \in \text{GL}(H)\).

Let \( \overline{\mathbb{Q}} \) be the field of algebraic numbers in \( \mathbb{C} \). Let \( S \) be a given set of ordered \( r+1 \) \( \overline{\mathbb{Q}} \)-rational points \( P_1, \ldots, P_{r+1} \) on the projective line \( \mathbb{P}^1_{\overline{\mathbb{Q}}} \) and we suppose that \( P_1 = 0, P_2 = 1 \) and \( P_{r+1} = \infty \). Let \( k := \mathbb{Q}(S \setminus \{ \infty \}) \), the finite algebraic number field generated over \( \mathbb{Q} \) by coordinates of \( P_1, \ldots, P_r \), so that all \( P_i \)'s are \( k \)-rational points of \( \mathbb{P}^1 \). Let \( \text{Gal}_k := \text{Gal}(\overline{\mathbb{Q}}/k) \) be the absolute Galois group of \( k \) equipped with the Krull topology. Note that \( \text{Gal}_k \) is the étale fundamental group \( \pi_1^{\text{ét}}(\text{Spec} \ k) \) with the base point \( \text{Spec} \overline{\mathbb{Q}} \to \text{Spec} \ k \).

Let \( \pi_1^{\text{pro-}l}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus S) \) denote the maximal pro-\( l \) quotient of the étale fundamental group of \( \mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus S \) with a base point \( \text{Spec} \overline{\mathbb{Q}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus S \) which lifts \( \text{Spec} \overline{\mathbb{Q}} \to \text{Spec} \ k \). By [G; XII, Corollaire 5.2], \( \pi_1^{\text{pro-}l}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus S) \) is the pro-\( l \) completion
of the topological fundamental group $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S)$. We fix once and for all
an identification of $F_r/\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus S)$ obtained by associating to each $x_i$
the homotopy class of a small loop around $P_i$ and hence an identification of
$\pi_1^{\text{pro-}l}(\mathbb{P}^1_{\mathbf{Q}} \setminus S)$ with $\mathfrak{F}_r$.

The absolute Galois group $\text{Gal}_k = \pi_1^{\text{et}}(\text{Spec } k)$ acts, as the monodromy,
on the geometric fiber $\mathbb{P}^1_{\mathbf{Q}} \setminus S$ of the fibration $\mathbb{P}^1_{\mathbf{Q}} \setminus S \to \text{Spec } k$ and hence
acts continuously on the pro-$l$ fundamental group $\pi_1^{\text{pro-}l}(\mathbb{P}^1_{\mathbf{Q}} \setminus S) \simeq \mathfrak{F}_r$. The
effect of changing a base point of $\mathbb{P}^1_{\mathbf{Q}} \setminus S$ is given as an inner automorphism
of $\mathfrak{F}_r$. Thus we have the continuous outer Galois representation

\[(1.1.1) \quad \Phi_S : \text{Gal}_k \longrightarrow \text{Out}(\mathfrak{F}_r) := \text{Aut}(\mathfrak{F}_r)/\text{Int}(\mathfrak{F}_r).\]

In terms of the field extensions, the representation $\Phi_S$ is described as follows. Let $t$ be a variable over $k$. We regard $\mathbb{P}^1$ as the $t$-line and so the
function field $K$ of $\mathbb{P}^1_{\mathbf{Q}}$ is the rational function field $\mathbf{Q}(t)$. The $k$-rational
points $P_i$ are identified with places of $K/\mathbf{Q}$. Let $M$ be the maximal pro-$l$
extension of $K$ unramified outside $P_i$ ($1 \leq i \leq r + 1$). We fix once and for
all an identification of $\mathfrak{F}_r$, with $\text{Gal}(M/K)$ obtained by associating to each $x_i$ a topological generator of the inertia group of an extension $P_i^M$ of $P_i$ to
a place of $M$. Since $P_i$'s are $k$-rational, $M/k(t)$ is a Galois extension and so
we have the exact sequence

\[1 \to \mathfrak{F}_r = \text{Gal}(M/K) \to \text{Gal}(M/k(t)) \to \text{Gal}(K/k(t)) = \text{Gal}_k \to 1.\]

For $g \in \text{Gal}_k$, choose $\tilde{g} \in \text{Gal}(M/k(t))$ which lifts $g$. Consider the action of $\text{Gal}_k$ on $\text{Gal}(M/K)$ defined by $f \mapsto \tilde{g}f\tilde{g}^{-1}$ and regard it as an automorphism
of $\mathfrak{F}_r$ via the isomorphism $\iota$. The effect of changing a lift $\tilde{g}$ is given as an inner automorphism of $\mathfrak{F}_r$. Thus we obtain the representation $\Phi_S$. Note further
that $g \circ P_i^M \circ \tilde{g}^{-1}$ is a place of $M$ which coincides with $P_i^M$ on $K$ ($1 \leq i \leq r + 1$).
So we have $g \circ P_i^M \circ \tilde{g}^{-1} \circ h = P_i^M$ for some $h \in \text{Gal}(M/K)$ so that $h^{-1}\tilde{g}x_i\tilde{g}^{-1}h$ is a topological generator of $P_i^M$. Hence $\tilde{g}x_i\tilde{g}^{-1} \sim x_i^{c_i}$ for
some $c_i$ in $\mathbb{Z}_l$, the ring of $l$-adic integers. We pass to the abelianization $H$.
Applying the conjugate by $\tilde{g}$ on the equality $X_1 + \cdots + X_{r+1} = 0$ in $H$, we have
$c_1X_1 + \cdots + c_{r+1}X_{r+1} = 0$. From these equations, we have $c_1 = \cdots = c_{r+1}$.
Therefore the action of $\text{Gal}_k$ on $\mathfrak{F}_r$ gives an element of the subgroup $\bar{P}(\mathfrak{F}_r)$
of $\text{Aut}(\mathfrak{F}_r)$ defined by

$\bar{P}(\mathfrak{F}_r) := \{ \varphi \in \text{Aut}(\mathfrak{F}_r) \mid \varphi(x_i) \sim x_i^{N(\varphi)} \ (1 \leq i \leq r + 1) \text{ for some } N(\varphi) \in \mathbb{Z}_l^+ \}$. 

6
Here the exponent $N(\varphi)$, called the norm of $\varphi$, gives a homomorphism $N : Aut(\mathfrak{F}_r) \to \mathbb{Z}_r^\times$. So each $\varphi \in \hat{P}(\mathfrak{F}_r)$ acts on the abelianization $H$ by the multiplication by $N(\varphi)$, $[\varphi](X_i) = N(\varphi)X_i$ for $1 \leq i \leq r$. It is easy to see $Int(\mathfrak{F}_r) \subset \hat{P}(\mathfrak{F}_r)$. Thus we have the outer Galois representation (1.1.1)

\begin{equation}
\Phi_S : \text{Gal}_k \to \hat{P}(\mathfrak{F}_r) / \text{Int}(\mathfrak{F}_r).
\end{equation}

1.2. The Ihara representation. We will lift $\Phi_S$ to a representation in $Aut(\mathfrak{F}_r)$. For this, consider the subgroup $P(\mathfrak{F}_r)$ of $\hat{P}(\mathfrak{F}_r)$ defined by (1.2.1)

\[ P(\mathfrak{F}_r) := \left\{ \varphi \in Aut(\mathfrak{F}_r) \mid \begin{array}{l}
\varphi(x_i) \sim x_i^{N(\varphi)} (1 \leq i \leq r-1) \varphi(x_r) \sim x_r^{N(\varphi)}, \\
\varphi(x_{r+1}) = x_{r+1}^{N(\varphi)} \text{ for some } N(\varphi) \in \mathbb{Z}_r^\times
\end{array} \right\}, \]

where $\sim$ denotes conjugacy by an element of the subgroup $\mathfrak{R}$ of $\mathfrak{F}_r$ generated by $[\mathfrak{F}_r, \mathfrak{F}_r]$ and $x_1, \ldots, x_{r-2}$. We denote by $P^1(\mathfrak{F}_r)$ the kernel of $N|_{P(\mathfrak{F}_r)}$:

\[ P^1(\mathfrak{F}_r) := \left\{ \varphi \in Aut(\mathfrak{F}_r) \mid \begin{array}{l}
\varphi(x_i) \sim x_i (1 \leq i \leq r-1) \varphi(x_r) \sim x_r, \\
\varphi(x_{r+1}) = x_{r+1}
\end{array} \right\}. \]

The following proposition was proved in [Ih1; Proposition 3, page 55] for the case $r = 2$ and stated in [Ih3; page 252] for the general case.

**Proposition 1.2.2.** The natural homomorphism $Aut(\mathfrak{F}_r) \to Aut(\mathfrak{F}_r) / \text{Int}(\mathfrak{F}_r)$ induces the isomorphism $P(\mathfrak{F}_r) \simeq \hat{P}(\mathfrak{F}_r) / \text{Int}(\mathfrak{F}_r)$. The representatives in $P(\mathfrak{F}_r)$ of $\hat{P}(\mathfrak{F}_r) / \text{Int}(\mathfrak{F}_r)$ are called Belyi’s lifts.

**Proof.** Although the proof is similar to that for $r = 2$, we give a concise proof for the sake of readers. First, we note that the centralizer of $x_i$ in $\mathfrak{F}_r$ is $\langle x_i \rangle = x_i^{\mathbb{Z}_r}$ for $1 \leq i \leq r+1$.

**Injectivity:** Suppose $\varphi \in P(\mathfrak{F}_r)$ and $\varphi = \text{Int}(f)$ with $f \in \mathfrak{F}_r$. Then $fx_{r+1}f^{-1} = x_{r+1}^{N(\varphi)}$. Passing to $H$, we see $N(\varphi) = 1$ and so $f$ is in the centralizer of $x_{r+1}$. Hence $f = x_{r+1}^a$ for some $a \in \mathbb{Z}_r$. Since $\varphi \in P(\mathfrak{F}_r)$, $fx_rf^{-1} = \varphi(x_r) = gx_rg^{-1}$ for some $g \in \mathfrak{R}$ and hence $g^{-1}f = x_r^b$ for some $b \in \mathbb{Z}_r$. Passing to the abelianization $H$, we find $a = b = 0$. Hence $f = 1$ and $\varphi = 1$.

**Surjectivity:** Take $\varphi \in \hat{P}(\mathfrak{F}_r)$. Multiplying $\varphi$ by an element of $\text{Int}(\mathfrak{F}_r)$, we may assume $\varphi(x_{r+1}) = x_{r+1}^{N(\varphi)}$. Set $\varphi(x_r) = gx_rg^{-1}$ with $g \in \mathfrak{F}_r$. Write
\[ [g] = \sum_{i=1}^{r} c_i X_i \text{ in } H \ (c_i \in \mathbb{Z}) \] and let \( \varphi_1 := \text{Int}(x_{r-1}^{-c_{r-1}}x_{r-1}^{-c_r}) \circ \varphi \). Then \( \varphi_1(x_r) = g_1 x_r g_1^{-1} \) and \( g_1 := x_{r-1}^{-c_{r-1}}x_{r-1}^{-c_r} g \in \mathfrak{F} \). Hence \( \varphi_1 \in P(\mathfrak{F}_r) \) and \( \varphi \equiv \varphi_1 \pmod{\text{Int}(\mathfrak{F}_r)} \). □

By Proposition 1.2.2, we can lift \( \Phi_S \) of (1.1.2) to the representation in \( P(\mathfrak{F}_r) \), denoted by \( \text{Ih}_S \):

(1.2.3) \[
\text{Ih}_S : \text{Gal}_k \longrightarrow P(\mathfrak{F}_r),
\]
which we call the Ihara representation associated to \( S \). Let \( \Omega_S \) denote the subfield of \( \mathbb{Q} \) corresponding to the kernel of \( \text{Ih}_S \) so that \( \text{Ih}_S \) factors through the Galois group \( \text{Gal}(\Omega_S/k) \):

(1.2.4) \[
\text{Ih}_S : \text{Gal}(\Omega_S/k) \longrightarrow P(\mathfrak{F}_r).
\]

We recall some arithmetic properties on the ramification in the Galois extension \( \Omega_S/k \). For this, let us prepare some notations. Let \( \zeta_{l^n} \) be a primitive \( l^n \)-th root of unity for a positive integer \( n \) such that \( (\zeta_{l^{n+1}})^l = \zeta_{l^n} \) for \( n \geq 1 \). We set \( k(\zeta_{l^n}) := \bigcup_{n \geq 1} k(\zeta_{l^n}) \). The \( l \)-cyclotomic character \( \chi_l : \text{Gal}_k \rightarrow \mathbb{Z}_l^\times \) is defined by \( g(\zeta_{l^n}) = \zeta_{l^n}^{\chi_l(g)} \) for \( g \in \text{Gal}_k \). Finally we define the set \( R_S \) of finite primes of \( k \) associated to \( S \) as follows: Let \( s_i \) be the coordinate of \( P_i \) for \( 1 \leq i \leq r \), and let \( \mathcal{O}_S \) be the integral closure of \( \mathbb{Z}[l^{-1}, (s_i - s_j)^{-1} | 1 \leq i \neq j \leq r] \) in \( k \). We then define \( R_S \) by the maximal spectrum

(1.2.5) \[
R_S := \text{Spm} \mathcal{O}_S.
\]

**Theorem 1.2.6.** Notations being as above, the following assertions hold:

(1) ([Ih1; Proposition 2, page 53]). \( N \circ \text{Ih}_S : \text{Gal}_k \rightarrow \mathbb{Z}_l^\times \) coincides with \( \chi_l \). In particular, the restriction of \( \varphi_S \) to \( \text{Gal}_{k(\zeta_{l^n})} := \text{Gal}(\mathbb{Q}/k(\zeta_{l^n})) \), denoted by \( \text{Ih}_S^1 \), gives the representation

\[
\text{Ih}_S^1 : \text{Gal}_{k(\zeta_{l^n})} \longrightarrow P^1(\mathfrak{F}_r)
\]
and we have \( k(\zeta_{l^n}) \subset \Omega_S \).

(2) ([AI; Proposition 2.5.2, Theorem 3]). The Galois extension \( \Omega_S/k \) is unramified over \( R_S \) and \( \Omega_S/k(\zeta_l) \) is a pro-\( l \) extension.

**Remark 1.2.7** (cf. [Ih2]). By Artin’s theorem ([Ar], [B; Theorem 1.9]),
the Artin representation $\text{Ar}_Q$ of the pure braid group $P_r$ in Introduction induces the isomorphism

$$\text{Ar}_Q : P_r \xrightarrow{\sim} \{ \varphi \in \text{Aut}(F_r) \mid \varphi(x_i) \sim x_i \ (1 \leq i \leq r), \ \varphi(x_1 \cdots x_r) = x_1 \cdots x_r \}.$$ 

So the representation $\text{Ih} : \text{Gal}_k(\zeta_{l\infty}) \to P^1(\mathfrak{H}_r)$ (resp. $\text{Ih}_S : \text{Gal}_k \to P(\mathfrak{H}_r)$) may be seen as an (resp. extended) arithmetic analogue of the Artin representation $\text{Ar}_Q$.

## 2. $l$-adic Milnor invariants and pro-$l$ link groups

### 2.1. Pro-$l$ Magnus expansions

Let $\{\mathfrak{H}_r(n)\}_{n \geq 1}$ be the lower central series of $\mathfrak{H}_r$ defined by

$$\mathfrak{H}_r(1) := \mathfrak{H}_r, \quad \mathfrak{H}_r(n + 1) := [\mathfrak{H}_r(n), \mathfrak{H}_r] \quad (n \geq 1).$$

Note that each $\mathfrak{H}_r(n)$ is a closed normal subgroup of $\mathfrak{H}_r$, so that $\mathfrak{H}_r(n)/\mathfrak{H}_r(n + 1)$ is central in $\mathfrak{H}_r/\mathfrak{H}_r(n + 1)$, and that each $\mathfrak{H}_r(n)$ is a finitely generated pro-$l$ group ([DDMS; 1.7, 1.14]). As in Section 1, let $H$ denote the abelianization of $\mathfrak{H}_r$:

$$H := \text{gr}_1(\mathfrak{H}_r) = H_1(\mathfrak{H}_r, \mathbb{Z}_l),$$

which is the free $\mathbb{Z}_l$-module with basis $X_1, \ldots, X_r$, where $X_i$ is the image of $x_i$ in $H$. Let $T(H)$ be the tensor algebra of $H$ over $\mathbb{Z}_l$ defined by $\bigoplus_{n \geq 0} H^\otimes n$, 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 non-commutative polynomial algebra $\mathbb{Z}_l\langle X_1, \ldots, X_r \rangle$ over $\mathbb{Z}_l$ with variables $X_1, \ldots, X_r$:

$$T(H) = \bigoplus_{n \geq 0} H^\otimes n = \mathbb{Z}_l\langle X_1, \ldots, X_r \rangle.$$ 

Let $\hat{T}(H)$ be the completion of $T(H)$ with respect to the $\mathfrak{m}_T$-adic topology, where $\mathfrak{m}_T$ is the maximal two-sided ideal of $T(H)$ generated by $X_1, \ldots, X_r$ and $l$. It is the infinite product $\prod_{n \geq 0} H^\otimes n$, which 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 $X_1, \ldots, X_r$:

$$\hat{T}(H) = \prod_{n \geq 0} H^\otimes n = \mathbb{Z}_l\langle\langle X_1, \ldots, X_r \rangle\rangle.$$
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 \( H^\otimes \) 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 \( \mathbb{Z}_l[[\hat{\mathfrak{g}}]] \) be the complete group algebra of \( \hat{\mathfrak{g}} \) over \( \mathbb{Z}_l \) and let \( \epsilon_{\mathbb{Z}_l[[\hat{\mathfrak{g}}]]} : \mathbb{Z}_l[[\hat{\mathfrak{g}}]] \to \mathbb{Z}_l \) be the augmentation homomorphism with the augmentation ideal \( I_{\mathbb{Z}_l[[\hat{\mathfrak{g}}]]} := \text{Ker}(\epsilon_{\mathbb{Z}_l[[\hat{\mathfrak{g}}]]}) \). The correspondence \( x_i \mapsto 1 + X_i \) \((1 \leq i \leq r)\) gives rise to the isomorphism of topological \( \mathbb{Z}_l \)-algebras

\[
\Theta : \mathbb{Z}_l[[\hat{\mathfrak{g}}]] \xrightarrow{\sim} \hat{T}(H),
\]

which we call the pro-\( l \) Magnus isomorphism. Here \( I_{\mathbb{Z}_l[[\hat{\mathfrak{g}}]]} \) corresponds, under \( \Theta \), to \( \hat{T}(n) \) for \( n \geq 0 \). For \( \alpha \in \mathbb{Z}_l[[\hat{\mathfrak{g}}]] \), \( \Theta(\alpha) \) 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

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

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

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

Restricting \( \Theta \) to \( \hat{\mathfrak{g}} \), we have an injective group homomorphism, denoted by the same \( \Theta \),

\[
\Theta : \hat{\mathfrak{g}} \hookrightarrow 1 + \hat{T}(1),
\]

which we call the pro-\( l \) Magnus embedding of \( \hat{\mathfrak{g}} \) into \( 1 + \hat{T}(1) \).

Here are some basic properties of \( l \)-adic Magnus coefficients:

(2.1.4) For \( \alpha, \beta \in \mathbb{Z}_l[[\hat{\mathfrak{g}}]] \) and a multi-index \( I \), we have

\[
\mu(I; \alpha \beta) = \sum_{I = AB} \mu(A; \alpha) \mu(B; \beta),
\]

where the sum ranges over all pairs \( (A, B) \) of multi-indices such that \( AB = I \), and we understand that \( \mu(A; \alpha) = \epsilon_{\mathbb{Z}_l[[\hat{\mathfrak{g}}]]}(\alpha) \) (resp. \( \mu(B; \beta) = \epsilon_{\mathbb{Z}_l[[\hat{\mathfrak{g}}]]}(\beta) \)) if \(|A| = 0\) (resp. \(|B| = 0\) ).
(2.1.5) **(Shuffle relation)** For \( f \in \mathfrak{F}_r \) and multi-indices \( I, J \) with \(|I|, |J| \geq 1\), we have
\[
\mu(I; f)\mu(J; f) = \sum_{A \in \text{Sh}(I, J)} \mu(A; f),
\]
where \( \text{Sh}(I, J) \) denotes the set of the results of all shuffles of \( I \) and \( J \) ([CFL]).

(2.1.6) For \( f \in \mathfrak{F}_r \) and \( d \geq 2 \), we have
\[
\mu(I; f) = 0 \text{ for } |I| < d \quad \text{i.e., } \deg(\Theta(f - 1)) \geq d \iff f \in \mathfrak{F}_r(d) \iff f - 1 \in I_d^{\mathfrak{F}_r}.
\]

An automorphism \( \varphi \) of the topological \( \mathbb{Z}_l \)-algebra \( \mathbb{Z}_l[[\mathfrak{F}_r]] \) (resp. \( \hat{T}(H) \)) is said to be **filtration-preserving** if \( \varphi(I^n_{\mathbb{Z}_l[[\mathfrak{F}_r]]}) = I^n_{\mathbb{Z}_l[[\mathfrak{F}_r]]} \) (resp. \( \varphi(\hat{T}(n)) = \hat{T}(n) \)) for all \( n \geq 1 \). Let \( \text{Aut}^\text{fil}(\mathbb{Z}_l[[\mathfrak{F}_r]]) \) (resp. \( \text{Aut}^\text{fil}(\hat{T}(H)) \)) be the group of filtration-preserving automorphisms of the topological \( \mathbb{Z}_l \)-algebras \( \mathbb{Z}_l[[\mathfrak{F}_r]] \) (resp. \( \hat{T}(H) \)). The pro-\( l \) Magnus isomorphism \( \Theta \) in (2.1.1) induces the isomorphism
\[
(2.1.7) \quad \text{Aut}^\text{fil}(\mathbb{Z}_l[[\mathfrak{F}_r]]) \xrightarrow{\sim} \text{Aut}^\text{fil}(\hat{T}(H)); \quad \varphi \mapsto \Theta \circ \varphi \circ \Theta^{-1}.
\]

In the following we set
\[
(2.1.8) \quad \varphi^* := \Theta \circ \varphi \circ \Theta^{-1}.
\]

We note by (2.1.6) that any automorphism \( \varphi \) of \( \mathfrak{F}_r \) can be extended uniquely to a filtration-preserving topological automorphism of \( \mathbb{Z}_l[[\mathfrak{F}_r]] \), which is also denoted by \( \varphi \). It is easy to see by (2.1.8) that for \( \varphi \in \text{Aut}^\text{fil}(\mathbb{Z}_l[[\mathfrak{F}_r]]), \alpha \in \mathbb{Z}_l[[\mathfrak{F}_r]] \), we have
\[
(2.1.9) \quad \Theta(\varphi(\alpha)) = \varphi^*(\Theta(\alpha)).
\]

### 2.2. \( l \)-adic Milnor invariants

Let \( \text{Ih}_S : \text{Gal}_k \to P(\mathfrak{F}_r) \) be the Ihara representation associated to \( S \) in (1.2.3).

**Lemma 2.2.1.** Let \( g \in \text{Gal}_k \). For each \( 1 \leq i \leq r \), there exists uniquely \( y_i(g) \in \mathfrak{F}_r \) satisfying the following properties:

1. \( \text{Ih}_S(g)(x_i) = y_i(g)x_i^{\chi_l(g)}y_i(g)^{-1} \), where \( \chi_l \) is the \( l \)-cyclotomic character,
2. In the expression \( [y_i(g)] = c_1^{(i)}X_1 + \cdots + c_r^{(i)}X_r \) \((c_j^{(i)} \in \mathbb{Z}_l), c_i^{(i)} = 0\).
We call \( \chi(g) \) the Magnus coefficient of \( g \). We also write \( \Delta(g) \) to be the ideal of \( \mathbb{Z}_l \) generated by \( \chi(g) - 1 \). Note that \( \Delta(g) = 0 \) when \( g \in \text{Gal}_{k(\zeta_l)} \). We then define the indeterminacy \( \Delta(g; I) \) by
\[
\Delta(g; I) := \text{the ideal of } \mathbb{Z}_l \text{ generated by } \Delta(g) \text{ and } \mu(I; y_j(g)), \quad \text{where } J \text{ ranges over proper subsequence of } I \text{ and } j = i_n \text{ or } j \text{ is in } J.
\]
We also write \( \Delta(I'; y_{i_n}(g)) \) for \( \Delta(g; I) \) for the convenience later. We then set
\[
\overline{\mu}(g; I) := \mu(g; I) \mod \Delta(g; I),
\]
which we call the l-adic Milnor invariant of \( g \in \text{Gal}_k \) for \( I \).

We will show that the l-adic Milnor invariant \( \overline{\mu}(g; I) \) for \( g \in \text{Gal}_k \) is unchanged when \( g \) is replaced by its conjugate \( hgh^{-1} \) for \( h \in \text{Gal}_{k(\zeta_{\infty})} \). To prove this, we prepare some lemmas. The formulas (1) and (2) of the next lemma was proved by Wojtkowiak in terms of torsors of paths. See [W1; Proposition 1.0.7, Corollary 1.0.8 and Proposition 2.2.1].

**Lemma 2.2.5.** For \( g, h \in \text{Gal}_k \) and \( 1 \leq i \leq r \), we have

1. \( \@y_i(h^{-1}) = \text{Ih}_S(h^{-1})(y_i(h)^{-1}) \),
2. \( \@y_i(hg) = \text{Ih}_S(h)(y_i(g))y_i(h) \) (cocyycle property),
3. \( \@y_i(hgh^{-1}) = \text{Ih}_S(hg)(y_i(h^{-1}))\text{Ih}_S(h)(y_i(g))y_i(h) \).

**Proof.** (1) By Lemma 2.2.1, we have

\[
x_i = \text{Ih}_S(h^{-1})\text{Ih}_S(h)(x_i) \\
= \text{Ih}_S(h^{-1})(y_i(h)x_i^{y_i(h)}y_i(h)^{-1}) \\
= \text{Ih}_S(h^{-1})(y_i(h))y_i(h^{-1})x_i\text{Ih}_S(h^{-1})(y_i(h)^{-1}),
\]

from which we find \( \text{Ih}_S(h^{-1})(y_i(h))y_i(h^{-1}) = x_i^{a_i} \) for some \( a_i \in \mathbb{Z}_l \). Passing to the abelianization \( H \) of \( \mathfrak{F}_r \) and comparing the coefficients of \( X_i \), we find \( a_i = 0 \) and hence we obtain (1).

(2) By Lemma 2.2.1, we have

\[
(2.2.5.1) \hspace{1cm} \text{Ih}_S(hg)(x_i) = y_i(hg)x_i^{y_i(hg)}y_i(hg)^{-1}.
\]

On the other hand, we have

\[
\text{Ih}_S(hg)(x_i) = \text{Ih}_S(h)\text{Ih}_S(g)(x_i) \\
= \text{Ih}_S(h)(y_i(g)x_i^{y_i(g)}y_i(g)^{-1}) \\
= \text{Ih}_S(h)(y_i(g))\text{Ih}_S(h)(x_i^{y_i(g)})\text{Ih}_S(h)(y_i(g)^{-1}) \\
= \text{Ih}_S(h)(y_i(g))y_i(h)x_i^{y_i(hg)}y_i(h)^{-1}\text{Ih}_S(h)(y_i(g)^{-1}).
\]

Comparing (2.2.5.1) and (2.2.5.2), we have \( y_i(hg)^{-1}\text{Ih}_S(h)(y_i(g))y_i(h) = x_i^{b_i} \) for some \( b_i \in \mathbb{Z}_l \). Passing to the abelianization and comparing the coefficients of \( X_i \), we find \( b_i = 0 \) and hence we obtain (2).

(3) By (2), we have

\[
y_i(hgh^{-1}) = \text{Ih}_S(hg)(y_i(h^{-1}))y_i(hg) = \text{Ih}_S(hg)(y_i(h^{-1}))\text{Ih}_S(h)(y_i(g))y_i(h). \quad \Box
\]
For $\rho \in \text{Gal}_k$ and a multi-index $J$ with $|J| \geq 1$, we define $\Theta_J(\rho)$ by

\begin{equation}
\Theta_J(\rho) := \text{Ih}_S(\rho)^*(X_J) - \chi_i(\rho)^{|J|}X_J.
\end{equation}

Since $\text{Ih}_S(\rho)^*$ is filtration-preserving, we note $\deg(\Theta_J(\rho)) \geq |J|$.

**Lemma 2.2.7.** Notations being as above, the following assertions hold.

1. $\Theta_J(\rho)$ is a Magnus power series $\sum_{|A| \geq |J|} m_A(J; \rho)X_A$ satisfying the following properties:
   a. if $m_A(J; \rho) \neq 0$, then $A$ contains $J$ as a proper subsequence. So we may write $\Theta_J(\rho) = \sum_{J \subseteq A} m_A(J; \rho)X_A$.
   b. any coefficient $m_A(J; \rho)$ is a multiple of $\mu(B; y_j(\rho))$ by an $l$-adic integer, where $B$ is some proper subsequence of $A$ and $j$ is in $J$.

2. For $y \in \mathfrak{F}_r$, we have

\begin{align*}
\Theta(\text{Ih}_S(\rho)(y)) &= 1 + \sum_{|J| \geq 1} \chi_i(\rho)^{|J|}\mu(J; y)X_J + \sum_{|J| \geq 1} \mu(J; y)\Theta_J(\rho) \\
&= \Theta(y) + \sum_{|J| \geq 1} \mu(J; y)\Theta_J(\rho) \mod a(\rho).
\end{align*}

**Proof.** (1) Let $1 \leq j \leq r$ and write $\Theta(y_j(\rho)) = 1 + Y_j(\rho)$. By (2.1.9) and Lemma 2.2.1, we have

\begin{equation}
\text{Ih}_S(\rho)^*(X_j) = \text{Ih}_S(\rho)^*(\Theta(x_j - 1)) = \Theta(\text{Ih}_S(\rho)(x_j - 1)) = \Theta(y_j(\rho)x_j^{\chi_i(\rho)}y_j(\rho)^{-1}) - 1 = \Theta(y_j(\rho))\Theta(x_j)^{\chi_i(\rho)}\Theta(y_j(\rho)^{-1}) - 1 = (1 + Y_j(\rho))(1 + X_j)^{\chi_i(\rho)}(1 - Y_j(\rho) + Y_j(\rho)^2 - \cdots) - 1 = \chi_i(\rho)X_j + \Theta_j(\rho),
\end{equation}

where $\Theta_j(\rho)$ is the sum of terms of the form $uY_j(\rho)^aX_bY_j(\rho)^c$ for some $a, c \geq 0$ with $a + c \geq 1, b \geq 1$ and $u \in \mathbb{Z}_l$. Write $\Theta_J(\rho) = \sum_{|A| \geq 2} m_A(J; \rho)X_A$. Then it is easy to see that if $m_A(J; \rho) \neq 0$, then $A$ must contain $j$. Moreover, since $Y_j(\rho) = \sum_{|B| \geq 1} \mu(B; y_j(\rho))X_B$, $m_A(J; \rho)$ is a multiple of $\mu(B; y_j(\rho))$ by an $l$-adic integer, where $B$ is some proper subsequence of $A$. Let $J = (j_1 \cdots j_n)$. 

\[14\]
By (2.2.7.1), we have
\[ \sum_{|A| \geq |J|} m_A(J; \rho) X_A := \Theta_J(\rho) \]
\[ := \text{Ih}_S(\rho)^* (X_J) - \chi_J(\rho)^{|J|} X_J \]
\[ = \text{Ih}_S(\rho)^* (X_{J_1}) \cdots \text{Ih}_S(\rho)^* (X_{J_n}) - \chi_J(\rho)^{|J|} X_J \]
\[ = (\chi_J(\rho) X_{J_1} + \Theta_{J_1}(\rho)) \cdots (\chi_J(\rho) X_{J_n} + \Theta_{J_n}(\rho)) - \chi_J(\rho)^{|J|} X_J \]
\[ = \Phi_{J_1}(\rho) \cdots \Phi_{J_n}(\rho), \]
where \( \Phi_j(\rho) \) is \( \chi_J(\rho) X_J \) or \( \Theta_J(\rho) \) and at least one \( \Theta_J(\rho) \) is involved for some \( j \).
Hence, by the properties of coefficients of \( \Theta_J(\rho) = \sum_{|A| \geq 2} m_A(j; \rho) X_A \) proved above, we obtain the properties (i) and (ii).

(2) By (2.1.9) and (2.2.6), we have
\[ \Theta(\text{Ih}_S(\rho)(y)) = \text{Ih}_S(\rho)^* (\Theta(y)) \]
\[ = \text{Ih}_S(\rho)^* (1 + \sum_{|J| \geq 1} \mu(J; y) X_J) \]
\[ = 1 + \sum_{|J| \geq 1} \mu(J; y) \text{Ih}_S(\rho)^* (X_J) \]
\[ = 1 + \sum_{|J| \geq 1} \mu(J; y) (\chi_J(\rho)^{|J|} X_J + \Theta_J(\rho)) \]
\[ = 1 + \sum_{|J| \geq 1} \chi_J(\rho)^{|J|} \mu(J; y) X_J + \sum_{|J| \geq 1} \mu(J; y) \Theta_J(\rho) \]
\[ \equiv \Theta(y) + \sum_{|J| \geq 1} \mu(J; y) \Theta_J(\rho) \mod \text{Ih}_S(\rho). \square \]

We are ready to prove the following

**Theorem 2.2.8.** For a multi-index \( I \), the \( l \)-adic Milnor invariant \( \overline{\tau}(g; I) \) for \( g \in \text{Gal}_k \) is unchanged when \( g \) is replaced with its conjugate by an element of \( \text{Gal}_{k(\zeta_\infty)} \). To be precise, let \( I \) be a multi-index with \( |I| \geq 1 \). Let \( g \in \text{Gal}_k \) and \( h \in \text{Gal}_{k(\zeta_\infty)} \). Then we have \( \Delta(hg^{-1}; I) = \Delta(g; I) \) and
\[ \overline{\tau}(hg^{-1}; I) = \overline{\tau}(g; I). \]

**Proof.** Let \( I \) be a multi-index with \( |I| \geq 1 \) and \( 1 \leq i \leq r \). For \( g, h \in \text{Gal}_k \), we will show

(2.2.8.1) \[ \mu(I; y_i(hg^{-1})) \equiv \mu(I; y_i(g)) \mod \Delta(I; y_i(g)). \]
By Lemma 2.2.5 (3), we have

\[(2.2.8.2) \quad \Theta(y_i(hg^{h^{-1}})) = \Theta(Ih_S(hg)(y_i(h^{-1})))\Theta(Ih_S(h)(y_i(g)))\Theta(y_i(h)).\]

For simplicity, we set, for a multi-index \(J\) with \(|J| \geq 1\),

\[a_J := \mu(J; Ih_S(hg)(y_i(h^{-1}))), b_J := \mu(J; Ih_S(h)(y_i(g))), c_J := \mu(J; y_i(h)).\]

Then, from (2.2.8.2) or (2.1.4), we have

\[(2.2.8.3) \quad \mu(I; y_i(hg^{h^{-1}})) = a_I + b_I + c_I + \sum_{AB=I} a_A b_B + \sum_{BC=I} b_B c_C + \sum_{AC=I} a_A c_C + \sum_{ABC=I} a_A b_B c_C,\]

where \(A, B, C\) are multi-indices with \(|A|, |B|, |C| \geq 1\).

First, we look at \(b_B\) for a subsequence \(B\) of \(I\). By Lemma 2.2.7 (1), (2) and as \(h \in \text{Gal}_{k(\zeta)}\), we have

\[b_B = \mu(B; y_i(g)) + \mu(J; y_i(g))\text{(an } l\text{-adic integer)}\]

for some proper subsequence \(J\) of \(B\). Therefore, by (2.2.8.3) and the definition of \(\Delta(I; y_i(g))\), we have

\[(2.2.8.4) \quad \mu(I; y_i(hg^{h^{-1}})) - \mu(I; y_i(g)) \equiv a_I + c_I + \sum_{AC=I} a_A c_C \mod \Delta(I; y_i(g)).\]

Here we note that the right hand side of (2.2.8.4) is the coefficient of \(X_I\) of

\[\Theta(Ih_S(hg)(y_i(h^{-1})))\Theta(y_i(h)).\]

So, next, we look at \(\Theta(Ih_S(hg)(y_i(h^{-1})))\Theta(y_i(h))\). By (2.1.9), Lemma

2.2.5 (1) and Lemma 2.2.7 (2), we have

\[(2.2.8.5) \quad \Theta(Ih_S(hg)(y_i(h^{-1}))) = Ih_S(hg)^*(\Theta(y_i(h^{-1}))) = Ih_S(h)^*Ih_S(g)^*(\Theta(y_i(h^{-1}))) \equiv Ih_S(h)^*(\Theta(y_i(h^{-1}))) + \sum_{|J| \geq 1} \mu(J; y_i(h^{-1}))\Theta_J(g) (\text{mod } a(g)) = \Theta(Ih_S(h)(y_i(h^{-1}))) + \sum_{|J| \geq 1} \mu(J; y_i(h^{-1}))Ih_S(h)^*(\Theta_J(g)) = \Theta(y_i(h^{-1})) + \sum_{|J| \geq 1} \mu(J; y_i(h^{-1}))Ih_S(h)^*(\Theta_J(g)).\]
Here let us write $\Theta_I(g) = \sum_{J \subseteq A} m_A(J; g) X_A$ as in Lemma 2.2.7 (1). Then we have, as $h \in \text{Gal}_{k(\zeta)}$,

$$Ih_S(h)^*(\Theta_I(g)) = \sum_{J \subseteq A} m_A(J; g) Ih_S(h)^*(X_A)$$

(2.2.8.6)

$$= \sum_{J \subseteq A} m_A(J; g)(X_A + \Theta_A(h)) \pmod{a(g)}$$

$$= \sum_{J \subseteq A} m_A(J; g)(X_A + \sum_{A \not\subseteq A'} m_{A'}(A; h)X_{A'}).$$

By (2.2.8.5) and (2.2.8.6), we have

$$\Theta(Ih_S(hg)(y_i(h^{-1}))) \equiv \Theta(y_i(h^{-1}) + \sum_{|J| \geq 1} \sum_{J \subseteq A} \mu(J; y_i(h^{-1})) m_A(J; g)(X_A + \sum_{A \not\subseteq A'} m_{A'}(A; h)X_{A'}) \pmod{a(g)}$$

and hence

(2.2.8.7)

$$\Theta(Ih_S(hg)(y_i(h^{-1}))) \Theta(y_i(h)) \equiv 1 + \sum_{|J| \geq 1} \sum_{J \subseteq A} \mu(J; y_i(h^{-1})) m_A(J; g)(X_A + \sum_{A \not\subseteq A'} m_{A'}(A; h)X_{A'}) \Theta(y_i(h)) \pmod{a(g)}.$$

Here we note by Lemma 2.2.7 (2) that $m_A(J; g)$ is a multiple of $\mu(B; y_j(g))$ by an $l$-adic integer for some proper subsequence $B$ of $A$ and $j$ in $J$. By the definition (2.2.3) of $\Delta(I; y_i(g))$, the coefficient of $X_I$ in the right hand side of (2.2.8.7) must be congruent to 0 mod $\Delta(I; y_i(g))$. By (2.2.8.4), we obtain (2.2.8.1).

Finally, we show that $\Delta(I; y_i(hgh^{-1})) = \Delta(I; y_i(g))$ by induction on $|I|$. When $|I| = 1$, this is obviously true (both sides are $a(g) = a(hgh^{-1})$) by the definition. Assume that $\Delta(I; y_i(hgh^{-1})) = \Delta(I; y_i(g))$ for all $I$ with $|I| \leq n$ ($n \geq 1$). Then, by (2.2.8.1), we have, for all $I$ with $|I| \leq n$ and $1 \leq i \leq r$,

(2.2.8.8) $\mu(I; y_i(hgh^{-1})) \equiv \mu(I; y_i(g)) \pmod{\Delta(I; y_i(g))} = \Delta(I; y_i(hgh^{-1}))$

Using (2.2.8.8) and the definition (2.2.3) of $\Delta(I; y_i(\rho))$ for $\rho = hgh^{-1}, g$, we have $\Delta(I; y_i(hgh^{-1})) = \Delta(I; y_i(g))$ for $I$ with $|I| = n + 1$. \qed
Remark 2.2.9. It is known that a braid $\beta$ and its conjugate $\gamma \beta \gamma^{-1}$ give rise to the same link as their closures ($\beta \mapsto \gamma \beta \gamma^{-1}$ is one of Markov's transforms. cf. [B; 2.2], [MK; Chapter 9]). In particular, they have the same Milnor invariants. So Theorem 2.2.8 may be seen as an arithmetic analogue of this known fact for braids.

As a property of $l$-adic Milnor invariants, we have the following shuffle relation.

Proposition 2.2.10. Let $g \in \text{Gal}_k$. For multi-indices $I, J$ with $|I|, |J| \geq 1$ and $1 \leq i \leq r$, we have

$$\sum_{H \in \text{PSh}(I,J)} \overline{\pi}(g; Hi) \equiv 0 \mod \gcd\{\Delta(Hi) \mid H \in \text{PSh}(I,J)\},$$

where $\text{PSh}(I,J)$ denotes the set of results of all proper shuffles of $I$ and $J$ ([CFL]).

Proof. By (2.1.5), we have

$$\mu(g; I_i)\mu(g; J_i) = \sum_{A \in \text{Sh}(I,J)} \mu(g; Ai).$$

Taking mod $\gcd\{\Delta(Hi) \mid H \in \text{PSh}(I,J)\}$, the left hand side is congruent to 0 and any term $\mu(g; Ai)$ with $A \notin \text{PSh}(I,J)$ is also congruent to 0. So the assertion follows. □

Let $R_S^\infty$ be the set of primes of $k(\zeta_i)$ lying over $R_S$ in (1.2.5). For $p\in R_S^\infty$, choose a prime $\mathfrak{p}$ of $\Omega_S$ lying over $p\infty$. Since $\mathfrak{p}$ is unramified in the Galois extension $\Omega_S/k$ by Theorem 1.2.6 (2), we have the Frobenius automorphism $\sigma_{\mathfrak{p}} \in \text{Gal}(\Omega_S/k)$ of $\mathfrak{p}$. By Theorem 2.2.8, $\overline{\pi}(\sigma_{\mathfrak{p}}; I)$ is independent of the choice of $\mathfrak{p}$ lying over $p\infty$. So we define the $l$-adic Milnor invariant of $p\infty$ for a multi-index $I$ by

$$(2.2.11) \quad \overline{\pi}(p\infty; I) := \overline{\pi}(\sigma_{\mathfrak{p}}; I).$$

We also set $\Delta(p\infty; I) := \Delta(\sigma_{\mathfrak{p}}; I)$ so that $\overline{\pi}(p\infty; I) \in \mathbb{Z}_l/\Delta(p\infty; I)$. Let $p$ be the prime of $k$ lying below $p\infty$. Since $\chi_l(\sigma_{\mathfrak{p}}) = Np$ (the norm of $p$), in order to have $\mathbb{Z}_l/\Delta(p\infty; I) \neq 0$, it is necessary that primes $p\infty$ in $R_S^\infty$ lie over

$$R_S^1 := \{p \in R_S \mid Np \equiv 1 \mod l\}.$$
For $p \in R^1_S$, let $e(p)$ denote the maximal integer such that 
\[ Np \equiv 1 \mod l^{e(p)}. \]

It means that $p$ is completely decomposed in $k(\zeta_{l^{e(p)}})/k$ and any prime of $k(\zeta_{l^{e(p)}})$ lying over $p$ is inert in $k(\zeta_{l^{\infty}})/k(\zeta_{l^{e(p)}})$. Hence $\sigma_p \in \text{Gal}(\Omega_S/k(\zeta_{l^{e(p)}}))$. Then the indeterminacy $\Delta(p_{\infty}; I)$ is an ideal of $\mathbb{Z}/l^{e(p)}\mathbb{Z}$. We note that if $\mu(\sigma_p; I) \equiv 0 \mod l^{e(p)}$ for all $|I| \leq n$, then $\overline{\mu}(p_{\infty}; I)$ is well defined in $\mathbb{Z}/l^{e(p)}\mathbb{Z}$ for $|I| = n + 1$.

**Remark 2.2.12.** In [Ms1] and [Ms2; Chapter 8], the arithmetic Milnor invariants for certain primes of a number field were introduced as multiple generalizations of power residue symbols and the Rédei triple symbol ([R]). See also [Am]. They are arithmetic analogues for primes of Milnor invariants of links. It is known ([Ko1], [Ko3; Chaper 1]) that Milnor invariants for a pure braid coincide with those for the link obtained by closing the pure braid. Recently, we found a relation between $l$-adic Milnor invariants, Wojtkowiak’s $l$-adic iterated integrals and $l$-adic polylogarithms ([NW], [W1]∼[W4]) and multiple power residue symbols (in particular, Rédei symbols), which will be discussed in the forthcoming paper.

We then have the descending series
\[ \text{Gal}_k = \text{Gal}_k^{\text{Mil}}[0] \supset \text{Gal}_k^{\text{Mil}}[1] \supset \cdots \supset \text{Gal}_k^{\text{Mil}}[n] \supset \cdots \]
and we call it the Milnor filtration of $\text{Gal}_k$.

**Proposition 2.2.14.** For $n \geq 0$, $\text{Gal}_k^{\text{Mil}}[n]$ is a closed normal subgroup of $\text{Gal}_k$.

**Proof.** This proposition is an immediate consequence of the coincidence of the Milnor filtration and the Johnson filtration which will be proved in Proposition 3.3.3 in Section 3. So we give herewith a direct and brief proof.
We may assume \( n \geq 1 \). Since \( \mu(\cdot ; I) : \text{Gal}_k \to \mathbb{Z}_l \) is continuous for each \( I \) and \( \text{Gal}^{\text{Mil}}_k[n] = \bigcap_{|I| \leq n} \mu(\cdot ; I)^{-1}(0) \), \( \text{Gal}^{\text{Mil}}_k[n] \) is closed in \( \text{Gal}_k \). Let \( g, h \in \text{Gal}^{\text{Mil}}_k[n] \) and so \( \deg(\Theta(y_i(\rho)) - 1) \geq n \) for \( \rho = g, h \) and each \( 1 \leq i \leq r \). Then we can show easily \( \deg(\Theta(y_i(g^{-1})) - 1) \geq n \), \( \deg(\Theta(y_i(gh)) - 1) \geq n \) and \( \deg(\Theta(y_i(hgh^{-1})) - 1) \geq n \) by using Lemma 2.2.5 (1), (2) and (3), respectively. □

2.3. Pro-\( l \) link groups and Massey products. Following the analogy with the link group of a pure braid link ([Ar], [B; Theorem 2.2]), we define the pro-\( l \) link group of each Galois element \( g \in \text{Gal}_k \) associated to \( \text{Ih}_S \) by (2.3.1)

\[
\Pi_S(g) := \langle x_1, \ldots, x_r \mid y_1(g)x_1^{\chi_1(g)}y_1(g)^{-1} = x_1, \ldots, y_r(g)x_r^{\chi_r(g)}y_r(g)^{-1} = x_r \rangle = \langle x_1, \ldots, x_r \mid x_1^{\chi_1(g)}[x_1^{-1}, y_1(g)^{-1}] = \cdots = x_r^{\chi_r(g)}[x_r^{-1}, y_r(g)^{-1}] \rangle = \mathfrak{g}_r/\mathfrak{n}_S(g),
\]

where \( \mathfrak{n}_S(g) \) denotes the closed subgroup of \( \mathfrak{g}_r \) generated normally by the pro-\( l \) words \( x_1^{\chi_1(g)}[x_1^{-1}, y_1(g)^{-1}], \ldots, x_r^{\chi_r(g)}[x_r^{-1}, y_r(g)^{-1}] \). We will give a cohomological interpretation of \( l \)-adic Milnor invariants of \( g \in \text{Gal}_k \) by Massey products in the cohomology of the pro-\( l \) link group \( \Pi_S(g) \). In the following, we let \( g \in \text{Gal}_k \) and \( a \) an ideal of \( \mathbb{Z}_l \) such that \( a \neq \mathbb{Z}_l \) and \( \chi_l(g) \equiv 1 \mod a \). We may write \( a = l^a \mathbb{Z}_l \) for some \( 1 \leq a \leq \infty \) (\( l^0 := 0 \) if \( a = \infty \)). When \( g \in \text{Gal}_k(\frac{\mathbb{Q}_l \cdot i}{i}) \), we have \( a = \infty \) and \( a = 0 \).

Let \( C^i(\Pi_S(g), \mathbb{Z}_l/a) \) be the \( \mathbb{Z}_l/a \)-module of continuous \( i \)-cochains \( (i \geq 0) \) of \( \Pi_S(g) \) with coefficients in \( \mathbb{Z}_l/a \), where \( \Pi_S(g) \) acts on \( \mathbb{Z}_l/a \) trivially. We consider the differential graded algebra \( (C^\bullet(\Pi_S(g), \mathbb{Z}_l/a), d) \), where the product on \( C^\bullet(\Pi_S(g), \mathbb{Z}_l/a) = \bigoplus_{i \geq 0} C^i(\Pi_S(g), \mathbb{Z}_l/a) \) is given by the cup product and the differential \( d \) is the coboundary operator. Then we have the cohomology ring \( H^\bullet(\Pi_S(g), \mathbb{Z}_l/a) := \bigoplus_{i \geq 0} H^i(C^\bullet(\Pi_S(g), \mathbb{Z}_l/a)) \) of the pro-\( l \) group \( \Pi_S(g) \) with coefficients in \( \mathbb{Z}_l/a \). In the following, we deal with only one and two dimensional cohomology groups. For the sign convention, we follow [Dw]. For \( c_1, \ldots, c_n \in H^1(\Pi_S(g), \mathbb{Z}_l/a) \), an \( n \)-th Massey product \( \langle c_1, \ldots, c_n \rangle \) is said to be defined if there is an array

\[
W = \{ w_{ij} \in C^1(\Pi_S(g), \mathbb{Z}_l/a) \mid 1 \leq i < j \leq n + 1, (i, j) \neq (1, n + 1) \}
\]

such that

\[
\begin{cases}
[\omega_{i,i+1}] = c_i & (1 \leq i \leq n), \\
\sum_{a = i + 1}^{j-1} w_{ai} \cup w_{aj} & (j \neq i + 1).
\end{cases}
\]
Such an array $W$ is called a defining system for $\langle c_1, \ldots, c_n \rangle$. The value of $\langle c_1, \ldots, c_n \rangle$ relative to $W$ is defined by the cohomology class represented by the 2-cocycle

$$\sum_{a=2}^{n} w_{1a} \cup w_{a,n+1},$$

and denoted by $\langle c_1, \ldots, c_n \rangle_W$. A Massey product $\langle c_1, \ldots, c_n \rangle$ itself is taken to be the subset of $H^2(\Pi_S(g), \mathbb{Z}_d/a)$ consisting of elements $\langle c_1, \ldots, c_n \rangle_W$ for some defining system $W$. By convention, $\langle c \rangle = 0$. The following lemma is a basic fact ([Kr]).

**Lemma 2.3.2.** We have $\langle c_1, c_2 \rangle = c_1 \cup c_2$. For $n \geq 3$, $\langle c_1, \ldots, c_n \rangle$ is defined and consists of a single element if $\langle c_{j_1}, \ldots, c_{j_a} \rangle = 0$ for all proper subsets $\{j_1, \ldots, j_a\}$ ($a \geq 2$) of $\{1, \ldots, n\}$.

Next, we recall a relation between Massey products and the Magnus coefficients for our situation. Let $\psi : \mathfrak{F}_r \to \Pi_S(g) = \mathfrak{F}_r / \mathfrak{N}_S(g)$ be the natural homomorphism. We denote by $\gamma_i$ the image of $x_i$ under $\psi$, $\gamma_i := x_i \bmod \mathfrak{N}_S(g)$, for $1 \leq i \leq r$. By the definition (2.3.1) of $\Pi_S(g)$ and our assumption, $\pi$ induces the isomorphism $\mathfrak{F}_r \cong \mathfrak{F}_r(2) \cong \Pi_S(g) / \Pi_S(g)[\Pi_S(g), \Pi_S(g)] \cong (\mathbb{Z}_d/a)^{\oplus r}$ and so we have the isomorphism $H^1(\Pi_S(g), \mathbb{Z}_d/a) \simeq H^1(\mathfrak{F}_r, \mathbb{Z}_d/a)$. Therefore the Hochschild-Serre spectral sequence yields the isomorphism

$$\text{tg} : H^1(\mathfrak{N}_S(g), \mathbb{Z}_d/a)^{\Pi_S(g)} \to H^2(\Pi_S(g), \mathbb{Z}_d/a).$$

Here $\text{tg}$ is the transgression defined as follows. For $a \in H^1(\mathfrak{N}_S(g), \mathbb{Z}_d/a)^{\Pi_S(g)}$, choose a 1-cochain $b \in C^1(\mathfrak{F}_r, \mathbb{Z}_d/a)$ such that $b|_{\mathfrak{N}_S(g)} = a$. Since the value $db(f_1, f_2)$, $f_i \in \mathfrak{F}_r$, depends only on the cosets $f_i \bmod \mathfrak{N}_S(g)$, there is a 2-cocycle $c \in Z^2(\Pi_S(g), \mathbb{Z}_d/a)$ such that $\psi^*(c) = db$. Then $\text{tg}(a)$ is defined to be the class of $c$. The dual to $\text{tg}$ is called the Hopf isomorphism:

$$\text{tg}^\vee : H_2(\Pi_S(g), \mathbb{Z}_d/a) \cong H_1(\mathfrak{N}_S(g), \mathbb{Z}_d/a)^{\Pi_S(g)} = \mathfrak{N}_S(g)^{\Pi_S(g)}[\mathfrak{N}_S(g), \mathfrak{F}_r].$$

Then we have the following proposition (cf. [St; Lemma 1.5], [Ms1, Theorem 2.2.2]).

**Proposition 2.3.3.** Notations being as above, let $c, \ldots, c_n \in H^1(\Pi_S(g), \mathbb{Z}_d/a)$ and $W = (w_{ij})$ a defining system for the Massey product $\langle c_1, \ldots, c_n \rangle$. Let
\[ f \in \mathfrak{M}(g) \] and set \( r := (tg^N)^{-1}(f \mod \mathfrak{M}(g)^e[\mathfrak{M}(g), \mathfrak{F}]) \). Then we have
\[
\langle c_1, \ldots, c_n \rangle w(r) = \sum_{j=1}^{n} (-1)^{j+1} \sum_{e_1 + \cdots + e_j = n} \sum_{i=(i_1 \cdots i_j)} w_{1,1+e_1}(\gamma_{i_1}) \cdots w_{n+1-e_j,n+1}(\gamma_{i_j}) \mu(I; f)_a,
\]
where \( e_1, \ldots, e_j \) run over positive integers satisfying \( e_1 + \cdots + e_j = n \) and \( \mu(I; f)_a := \mu(I; f) \mod a \).

Now, let \( \gamma_1, \ldots, \gamma_r \in H^1(\Pi_S(g), \mathbb{Z}/a) \) be the Kronecker dual to \( \gamma_1, \ldots, \gamma_r \), namely, \( \gamma^*_i(\gamma_j) = \delta_{ij} \) for \( 1 \leq i, j \leq r \). Let \( r_i := (tg^N)^{-1}(x_i^{1-\chi(g)}[x_i^{-1}, y_i(g)^{-1}]) \mod [\mathfrak{M}(g), \mathfrak{F}] \) for \( 1 \leq i \leq r \). Let \( I = (i_1 \cdots i_n) \) be a multi-index such that \( |I| = n \geq 2 \). Let \( g \in \text{Gal}_k \). We assume the following conditions:

\[
\begin{align*}
(1) \quad & \mu((j_1 \cdots j_a); x_i^{1-\chi(g)}) \equiv 0 \mod a \text{ for any subset } \\
& \{j_1, \ldots, j_a\} \text{ of } \{i_1, \ldots, i_n\} \text{ and } 1 \leq i \leq r, \\
(2) \quad & i_1, \ldots, i_n \text{ are distinct each other, and } \\
& \mu(g; (j_1 \cdots j_a)) \equiv 0 \mod a \text{ for any proper subset } \\
& \{j_1, \ldots, j_a\} \text{ of } \{i_1, \ldots, i_n\}.
\end{align*}
\]

(2.3.4)

We note that the condition (1) is unnecessary when \( g \in \text{Gal}_k(\xi^n) \). The following theorem gives a cohomological interpretation of \( \mu(g; I)_a := \mu(g; I) \mod a \) by the Massey product in the cohomology of \( \Pi_S(g) \).

**Theorem 2.3.5.** Notations and assumptions being as above, the Massey product \( \langle \gamma^*_1, \ldots, \gamma^*_n \rangle \) in \( H^2(\Pi_S(g), \mathbb{Z}/a) \) is uniquely defined and we have
\[
\mu(g; I)_a = (-1)^n \langle \gamma^*_1, \ldots, \gamma^*_n \rangle (r_m).
\]

Proof. First, we compute \( \mu(J; x_i^{1-\chi(g)}[x_i^{-1}, y_i(g)^{-1}]) \) for a multi-index \( J = (j_1 \cdots j_a) \), where \( \{j_1, \ldots, j_a\} \) is a subset of \( \{i_1, \ldots, i_n\} \). We note that
\[
\Theta(x_i^{1-\chi(g)}[x_i^{-1}, y_i(g)^{-1}]) = \Theta(x_i^{1-\chi(g)})(1 + \Theta(x_i^{1})\Theta(y_i(g)^{-1})(\Theta(x_iy_i(g)) - \Theta(y_i(g)x_i))).
\]

By our assumption (2.3.4) (1), we have
(2.3.5.1)
\[
\mu(J; x_i^{1-\chi(g)}[x_i^{-1}, y_i(g)^{-1}]) \equiv \mu(J; x_iy_i(g)) - \mu(J; y_i(g)x_i) \\
+ \sum_A (\mu(A; x_iy_i(g)) - \mu(A; y_i(g)x_i)) \nu_A \mod a,
\]
where $A$ runs over some proper subsequences of $J$ and $\nu_A \in \mathbb{Z}_l$. By the straightforward computation, we have
\[
\mu(J; x_i y_i(g)) = \begin{cases} 
\mu(g; (Ji)) & (i \neq j_1), \\
\mu(g; (Jj_1)) + \mu(g; (j_2 \cdots j_a j_1)) & (i = j_1), 
\end{cases}
\]
and
\[
\mu(J; y_i(g)x_i) = \begin{cases} 
\mu(g; (Ji)) & (i \neq j_a), \\
\mu(g; (Jj_a)) + \mu(g; J) & (i = j_a).
\end{cases}
\]
Hence we have
(2.3.5.2)
\[
\mu(J; x_i y_i(g)) - \mu(J; y_i(g)x_i) = \begin{cases} 
\mu(g; (j_2 \cdots j_a j_1)) - \delta_{j_1, j_a} \mu(g; J) & (i = j_1), \\
\mu(g; (j_2 \cdots j_a j_1))\delta_{j_1, j_a} - \mu(g; J) & (i = j_a), \\
0 & (\text{otherwise}).
\end{cases}
\]
Now, let $n = 2$. Then we have $\langle \gamma^*_i^1, \gamma^*_i^2 \rangle = \gamma^*_i^1 \cup \gamma^*_i^2$. By Proposition 2.3.3, (2.3.4) (2), (2.3.5.1) and (2.3.5.2), we have
\[
\langle \gamma^*_i^1, \gamma^*_i^2 \rangle(r_{i_2}) = -\mu(I; [x_{i_2}, y_{i_2}(g)])_a = \mu(g; I)_a.
\]
Suppose $n \geq 3$ and let $\{j_1, \ldots, j_a\}$ be a proper subset of $\{i_1, \ldots, i_n\}$. Then, by our assumption (2.3.4) (2), (2.3.5.1) and (2.3.5.2), we have
\[
\mu(J; x_i^{-1-x_i(g)}[x_i^{-1}, y_i(g)^{-1}]) \equiv 0 \mod a
\]
for $J = (j_1 \cdots j_a)$ and $1 \leq i \leq r$. So, by Proposition 2.3.4, we have
\[
\langle \gamma^*_j^1, \ldots, \gamma^*_j^a \rangle(r_i) = 0
\]
for $1 \leq i \leq r$. Since $H_2(\Pi(g), \mathbb{Z}/a)$ is generated by $x_i^{-1-x_i(g)}[x_i, y_i(g)]$ for $1 \leq i \leq r$, we have
\[
\langle c_{j_1}, \ldots, c_{j_a} \rangle = 0.
\]
Therefore, by Lemma 2.3.2, the Massey product $\langle c_{i_1}, \ldots, c_{i_n} \rangle$ is uniquely defined. By Proposition 2.3.3, (2.3.4) (2), (2.3.5.1) and (2.3.5.2) again, we have
\[
\langle \gamma^*_i^1, \ldots, \gamma^*_i^n \rangle(r_{i_2}) = (-1)^{n+1} \mu(I; x_i^{-1-x_i(g)}[x_i, y_i(g)])_a = (-1)^n \mu(g; I)_a. \quad \Box
\]
3. Pro-$l$ Johnson homomorphisms

3.1. Some algebras associated to lower central series. For each integer $n \geq 1$, we let

$$\text{gr}_n(\mathfrak{F}_r) := \mathfrak{F}_r(n) / \mathfrak{F}_r(n + 1),$$

which is a free $\mathbb{Z}_l$-module whose rank $\ell_r(n)$ is given by the Witt formula ([MKS; 5.6, Theorem 5.11], [Se; Ch. IV, 4, 6]):

$$\ell_r(n) = \frac{1}{n} \sum_{d | n} \mu(d) r^{n/d},$$

where $\mu(d)$ is the Möbius function. The graded $\mathbb{Z}_l$-module

$$\text{gr}(\mathfrak{F}_r) := \bigoplus_{n \geq 1} \text{gr}_n(\mathfrak{F}_r)$$

has the structure of a graded free Lie algebra over $\mathbb{Z}_l$: For $a = s \bmod \mathfrak{F}_r(m + 1) \in \text{gr}_m(\mathfrak{F}_r)$ and $b = t \bmod \mathfrak{F}_r(n + 1) \in \text{gr}_n(\mathfrak{F}_r)$ ($s \in \mathfrak{F}_r(m), t \in \mathfrak{F}_r(n)$), the Lie bracket on $\text{gr}(\mathfrak{F}_r)$ is defined by

$$[a, b] := [s, t] \bmod \mathfrak{F}_r(m + n + 1).$$

We consider the graded associative algebra over $\mathbb{Z}_l$ defined by

$$\text{gr}(\mathbb{Z}_l[[\mathfrak{F}_r]]) := \bigoplus_{n \geq 0} \text{gr}_n(\mathbb{Z}_l[[\mathfrak{F}_r]]), \quad \text{gr}_n(\mathbb{Z}_l[[\mathfrak{F}_r]]) := I^n_{\mathbb{Z}_l[[\mathfrak{F}_r]]} / I^{n+1}_{\mathbb{Z}_l[[\mathfrak{F}_r]]}.$$  

The map $f \mapsto f - 1$ ($f \in \mathfrak{F}_r(n)$) defines an injective $\mathbb{Z}_l$-linear map

(3.1.1)  $$\text{gr}_n(\mathfrak{F}_r) \hookrightarrow \text{gr}_n(\mathbb{Z}_l[[\mathfrak{F}_r]])$$

for $n \geq 1$ and the injective Lie algebra homomorphism over $\mathbb{Z}_l$

$$\text{gr}(\mathfrak{F}_r) \hookrightarrow \text{gr}(\mathbb{Z}_l[[\mathfrak{F}_r]]),$$

where $\text{gr}(\mathbb{Z}_l[[\mathfrak{F}_r]])$ is shown to be the universal enveloping algebra of the Lie algebra $\text{gr}(\mathfrak{F}_r)$. Moreover, by the correspondence $x_i - 1 \bmod I^2_{\mathbb{Z}_l[[\mathfrak{F}_r]]} \in \text{gr}_1(\mathbb{Z}_l[[\mathfrak{F}_r]]) \leftrightarrow X_i \in H$, we have the isomorphism of $\mathbb{Z}_l$-modules

(3.1.2)  $$\Theta_n : \text{gr}_n(\mathbb{Z}_l[[\mathfrak{F}_r]]) \simeq H^\otimes n$$
for each $n \geq 0$ and so $\text{gr}(\mathbb{Z}[\mathfrak{g}_r])$ is identified with the tensor algebra $T(H)$:

$$\text{gr}(\mathbb{Z}[\mathfrak{g}_r]) = T(H) = \mathbb{Z}\langle X_1, \ldots, X_r \rangle.$$ 

The composition of the map of (3.1.1) with $\Theta_n$ in (3.1.2), denoted also by $\Theta_n : \text{gr}_n(\mathfrak{g}_r) \hookrightarrow H^{\otimes n}$, is the degree $n$ part of the pro-$l$ Magnus embedding in (2.1.3):

$$(3.1.3) \quad \Theta_n = (\Theta - 1)|_{\mathfrak{g}_r(n)} \pmod{\hat{T}(n + 1)}.$$ 

Here we may note that $\Theta$ is multiplicative, $\Theta(f_1 f_2) = \Theta(f_1)\Theta(f_2)$ for $f_1, f_2 \in \mathfrak{g}_r$, while $\Theta_n$ is additive, $\Theta_n([f_1 f_2]) = \Theta_n([f_1] + [f_2]) = \Theta_n([f_1]) + \Theta_n([f_2])$, where $[\cdot]$ stands for the class mod $\mathfrak{g}_r(n + 1)$.

3.2. The pro-$l$ Johnson map. This subsection concerns the pro-$l$ Johnson map associated to the Ihara representation, which is a pro-$l$ analogue of the Johnson map introduced by Kawazumi ([Ka]). Overall, we follow Kazazumi’s arguments in [ibid] in our pro-$l$ setting.

For $\varphi \in \text{Aut}^{\text{fil}}(\hat{T}(H))$, we denote by $[\varphi]$ the induced $\mathbb{Z}_l$-endomorphism of $H = \hat{T}(1)/\hat{T}(2) = \mathbb{Z}_l^{\otimes r}$.

**Lemma 3.2.1.** A $\mathbb{Z}_l$-algebra endomorphism $\varphi$ of $\hat{T}(H)$ is a filtration-preserving automorphism of $\hat{T}(H)$, $\varphi \in \text{Aut}^{\text{fil}}(\hat{T}(H))$, if and only if the following conditions are satisfied:

1. $\varphi(\hat{T}(n)) \subset \hat{T}(n)$ for all $n \geq 0$.
2. the induced $\mathbb{Z}_l$-endomorphism $[\varphi]$ on $\hat{T}(1)/\hat{T}(2) = H$ is an isomorphism.

**Proof.** Suppose $\varphi \in \text{Aut}^{\text{fil}}(\hat{T}(H))$. Since $\varphi$ is filtration-preserving, the condition (1) holds. To show the condition (2), consider the following commutative diagram for vector spaces over $\mathbb{Z}_l$ with exact rows:

$$
\begin{array}{cccccc}
0 & \rightarrow & \hat{T}(2) & \rightarrow & \hat{T}(1) & \rightarrow & H & \rightarrow & 0 \\
\downarrow \varphi|_{\hat{T}(2)} & & \downarrow \varphi|_{\hat{T}(1)} & & \downarrow [\varphi] \\
0 & \rightarrow & \hat{T}(2) & \rightarrow & \hat{T}(1) & \rightarrow & H & \rightarrow & 0.
\end{array}
$$
Since $\varphi(\hat{T}(n)) = \hat{T}(n)$ for all $n \geq 0$, we have $\text{Coker}(\varphi|_{\hat{T}(i)}) = 0$ for $i = 1, 2$, in particular. Since $\varphi$ is an automorphism, we have $\text{Ker}(\varphi) = 0$, in particular, $\text{Ker}(\varphi|_{\hat{T}(i)}) = 0$ for $i = 1, 2$. By snake lemma applied to the above diagram, we obtain $\text{Ker}(\varphi) = 0$ and $\text{Coker}(\varphi) = 0$, hence the condition (2).

Suppose that a $\mathbb{Z}_l$-algebra endomorphism $\varphi$ of $\hat{T}$ satisfies the conditions (1) and (2). Let $z = (z_m)$ be any element of $\hat{T}$ with $z_m \in H^{\otimes m}$ for $m \geq 0$. To show that $\varphi$ is an automorphism, we have only to prove that there exists uniquely $y = (y_m) \in \hat{T}$ such that

$$z = \varphi(y).$$

Note by the condition (1) and (2) that $\varphi$ induces a $\mathbb{Z}_l$-linear automorphism of $\hat{T}/\hat{T}(m+1) = H^{\otimes m}$, which is nothing but $[\varphi]^{\otimes m}$. Then, writing $\varphi(y_i)_j$ for the component of $\varphi(y_i)$ in $H^{\otimes j}$ for $i < j$, the equation (3.2.1.1) is equivalent to the following system of equations:

$$
\begin{cases}
  z_0 = \varphi(y_0) = y_0, \\
  z_1 = [\varphi](y_1), \\
  z_2 = [\varphi]^{\otimes 2}(y_2) + \varphi(y_1)_2, \\
  \quad \vdots \\
  z_m = [\varphi]^{\otimes m}(y_m) + \varphi(y_1)_m + \cdots + \varphi(y_{m-1})_m, \\
  \quad \vdots
\end{cases}
$$

Since $[\varphi]^{\otimes m}$ is an automorphism, we can find the unique solution $y = (y_m)$ of (3.2.1.2) from the lower degree. Therefore $\varphi$ is an $\mathbb{Z}_l$-algebra automorphism. Furthermore, we can see easily that if $z_0 = \cdots = z_{n-1} = 0$, then $y_0 = \cdots = y_{n-1} = 0$ for $n \geq 1$. This means that $\varphi^{-1}(\hat{T}(n)) \subset \hat{T}(n)$ and so $\varphi$ is filtration-preserving.

By Lemma 3.2.1, each $\varphi \in \text{Aut}^\text{fil}(\hat{T}(H))$ induces a $\mathbb{Z}_l$-linear automorphism $[\varphi]$ of $H = \hat{T}(1)/\hat{T}(2)$ and so we have a group homomorphism

$$[\ ] : \text{Aut}^\text{fil}(\hat{T}(H)) \longrightarrow \text{GL}(H),$$

where $\text{GL}(H)$ denotes the group of $\mathbb{Z}_l$-linear automorphisms of $H$. We then define the induced automorphism group of $\hat{T}$ by

$$\text{IA}(\hat{T}(H)) := \text{Ker}([\ ])
= \{ \varphi \in \text{Aut}(\hat{T}(H)) \mid \varphi(h) \equiv h \text{ mod } \hat{T}(2) \text{ for any } h \in H \}.$$
We note that there is a natural splitting $s : \text{GL}(H) \to \text{Aut}^\text{fil}(\hat{T}(H))$ of $\lbrack ~ \rbrack$, which is defined by

$$s(P)((z_n)) := (P \otimes^n(z_n)) \text{ for } P \in \text{GL}(H).$$

In the following, we also regard $[P] \in \text{GL}(H)$ as an element of $\text{Aut}^\text{fil}(\hat{T})$ through the splitting $s$. Thus we have the following

**Lemma 3.2.2.** We have a semi-direct decomposition

$$\text{Aut}^\text{fil}(\hat{T}(H)) = \text{IA}(\widehat{\text{T}}(H)) \rtimes \text{GL}(H); \ \varphi = (\varphi \circ [\varphi]^{-1}, [\varphi]).$$

Let $\varphi \in \text{IA}(\hat{T}(H))$. Then we have $\varphi(h) - h \in \hat{T}(2)$ for any $h \in H$, and so we have a map

$$(3.2.3) \quad E : \text{IA}(\hat{T}) \to \text{Hom}_{\mathbb{Z}_l}(H, \hat{T}(2)); \ \varphi \mapsto \varphi|_H - \text{id}_H,$$

where $\text{Hom}_{\mathbb{Z}_l}(H, \hat{T}(2))$ denotes the $\mathbb{Z}_l$-module of $\mathbb{Z}_l$-homomorphisms $H \to \hat{T}(2)$. The following Proposition will play a key role in our discussion.

**Proposition 3.2.4.** The map $E$ is bijective.

**Proof.** Injectivity: Suppose $E(\varphi) = E(\varphi')$ for $\varphi, \varphi' \in \text{IA}(\hat{T}(H))$. Then we have $\varphi|_H = \varphi'|_H$. Since an $\mathbb{Z}_l$-algebra endomorphism of $\hat{T}(H)$ is determined by its restriction on $H$, we have $\varphi = \varphi'$.

Surjectivity: Take any $\phi \in \text{Hom}_{\mathbb{Z}_l}(H, \hat{T}(2))$. We can extend $\phi + \text{id}_H : H \to \hat{T}(2)$ uniquely to a $\mathbb{Z}_l$-algebra endomorphism $\varphi$ of $\hat{T}(H)$. Then we have obviously $\varphi(\hat{T}(n)) \subset \hat{T}(n)$ for all $n \geq 0$. Since $\hat{T}(1)/\hat{T}(2) = H$ and we see that

$$[\varphi](h \text{ mod } \hat{T}(2)) = \varphi(h) \text{ mod } \hat{T}(2) = h + \phi(h) \text{ mod } \hat{T}(2) = h \text{ mod } \hat{T}(2),$$

we have $[\varphi] = \text{id}_H$. By Lemma 3.2.1, we have $\varphi \in \text{IA}(\hat{T})$ and $E(\varphi) = \phi$. □

By Lemma 3.2.2 and Proposition 3.2.4, we have the following

**Corollary 3.2.5.** We have a bijection

$$\hat{E} : \text{Aut}^\text{fil}(\hat{T}(H)) \simeq \text{Hom}_{\mathbb{Z}_l}(H, \hat{T}(2)) \times \text{GL}(H)$$
defined by $\hat{E}(\varphi) = (E(\varphi \circ [\varphi]^{-1}), [\varphi])$.

Now, let $Ih_S : \text{Gal}_k \to P(\mathfrak{F}_r)$ be the Ihara representation associated to $S$ in (1.2.3). We recall that the correspondence $\varphi \mapsto \varphi^* := \Theta \circ \varphi \circ \Theta^{-1}$ in (2.1.8) gives the injective homomorphism $\text{Aut}(\mathfrak{F}_r) \to \text{Aut}^\text{fil}(\hat{T}(H))$ and hence the inclusion $P(\mathfrak{F}_r) \hookrightarrow \text{Aut}^\text{fil}(\hat{T}(H))$ which satisfies $[\varphi] = [\varphi^*]$ in $\text{GL}(H)$. Composing $Ih_S$ with this inclusion, we have the homomorphism $\hat{\eta}_S : \text{Gal}_k \to \text{Aut}^\text{fil}(\hat{T}(H))$ defined by

$$\hat{\eta}_S(g) := Ih_S(g)^* = \Theta \circ Ih_S(g) \circ \Theta^{-1}.$$  

We then define the map $\eta_S : \text{Gal}_k \to \text{IA}(\hat{T}(H))$ by composing $\hat{\eta}_S$ with the projection on $\text{IA}(\hat{T}(H))$:

$$(3.6) \quad \eta_S(g) := \hat{\eta}_S(g) \circ [Ih_S(g)]^{-1} = Ih_S(g)^* \circ [Ih_S(g)]^{-1} = \Theta \circ Ih_S(g) \circ \Theta^{-1} \circ [Ih_S(g)]^{-1}.$$  

Thus, we have $\hat{\eta}_S(g) = (\eta_S(g), [Ih_S(g)])$ for $g \in \text{Gal}_k$ under the semi-direct decomposition $\text{Aut}^\text{fil}(\hat{T}(H)) = \text{IA}(\hat{T}(H)) \rtimes \text{GL}(H)$ of Lemma 3.2.2.

Now, we define the pro-$l$ Johnson map

$$\tau_S : \text{Gal}_k \to \text{Hom}_{\mathbb{Z}_l}(H, \hat{T}(2))$$

by the composing $\eta_S$ with $E$ in (3.2.3), and define the extended pro-$l$ Johnson map

$$\hat{\tau}_S : \text{Gal}_k \to \text{Hom}_{\mathbb{Z}_l}(H, \hat{T}(2)) \rtimes \text{GL}(H)$$

by composing $\hat{\eta}_S$ with $\hat{E}$ of Corollary 3.2.5. So we have, for $g \in \text{Gal}_k$,

$$(3.7) \quad \tau_S(g) := E(\eta_S(g)) = \eta_S(g)|_H - \text{id}_H = Ih_S(g)^* \circ [Ih_S(g)]^{-1}|_H - \text{id}|_H = \Theta \circ Ih_S(g) \circ \Theta^{-1} \circ [Ih_S(g)]^{-1}|_H - \text{id}|_H, \quad \hat{\tau}_S(g) := (\tau_S(g), [Ih_S(g)]).$$

For $m \geq 1$, let $\text{Hom}_{\mathbb{Z}_l}(H, H^\otimes (m+1))$ denote the $\mathbb{Z}_l$-module of $\mathbb{Z}_l$-homomorphisms $H \to H^\otimes (m+1)$, and we define the $m$-th pro-$l$ Johnson map

$$\tau^{(m)}_S : \text{Gal}_k \to \text{Hom}_{\mathbb{Z}_l}(H, H^\otimes (m+1))$$

by the $m$-th component of $\tau_S$:

$$(3.8) \quad \tau_S(g) := \sum_{m \geq 1} \tau^{(m)}_S(g) \quad (g \in \text{Gal}_k).$$
We note that the pro-$l$ Johnson map $\tau_S$ is no longer a homomorphism. In fact, we have the following

**Proposition 3.2.9.** For $g_1, g_2 \in \text{Gal}_k$, we have

$$\eta_S(g_1 g_2) = \eta_S(g_1) \circ [\text{Ih}_S(g_1)] \circ \eta_S(g_2) \circ [\text{Ih}_S(g_1)]^{-1}.$$ 

**Proof.** By (3.2.6), we have

$$\eta_S(g_1 g_2) = \text{Ih}_S(g_1 g_2)^* \circ [\text{Ih}_S(g_1 g_2)]^{-1}$$
$$= \Theta \circ (\text{Ih}_S(g_1 g_2) \circ \Theta^{-1} \circ [\text{Ih}_S(g_1 g_2)]^{-1}$$
$$= \Theta \circ \text{Ih}_S(g_1) \circ \text{Ih}_S(g_2) \circ \Theta^{-1} \circ [\text{Ih}_S(g_2)]^{-1} \circ [\text{Ih}_S(g_1)]^{-1}$$
$$= \Theta \circ \text{Ih}_S(g_1) \circ \Theta^{-1} \circ [\text{Ih}_S(g_1)]^{-1} \circ [\text{Ih}_S(g_2)]^{-1} \circ [\text{Ih}_S(g_1)]$$
$$= \eta_S(g_1) \circ [\text{Ih}_S(g_1)] \circ \eta_S(g_2) \circ [\text{Ih}_S(g_1)]^{-1}. \quad \square$$

Proposition 3.2.9 yields coboundary relations among $\tau_S^{(m)}$. Here we give the formulas only for $\tau_S^{(1)}$ and $\tau_S^{(2)}$.

**Proposition 3.2.10.** For $g_1, g_2 \in \text{Gal}_k$, we have

$$\tau_S^{(1)}(g_1 g_2) = \tau_S^{(1)}(g_1) + [\text{Ih}_S(g_1)] \otimes \tau_S^{(1)}(g_2) \circ [\text{Ih}_S(g_1)]^{-1},$$
$$\tau_S^{(2)}(g_1 g_2) = \tau_S^{(2)}(g_1) + (\tau_S^{(1)}(g_1) \otimes \text{id}_H + \text{id}_H \otimes \tau_S^{(1)}(g_1)) \circ [\text{Ih}_S(g_1)] \otimes \tau_S^{(2)}(g_2) \circ [\text{Ih}_S(g_1)]^{-1}.$$ 

**Proof.** By definition (3.2.8), we have

$$\tau_S(g_1 g_2) = \sum_{m \geq 1} \tau_S^{(m)}(g_1 g_2).$$
On the other hand, by Proposition 3.2.9 and (3.2.7), we have, for $h \in H$,
\[
\tau_S(g_1 g_2)(h) = -h + \eta_S(g_1 g_2)(h)
\]
\[
= -h + (\eta_S(g_1) \circ [\text{Ih}_S(g_1)] \circ \eta_S(g_2) \circ [\text{Ih}_S(g_1)]^{-1})(h)
\]
\[
= -h + (\eta_S(g_1) \circ [\text{Ih}_S(g_1)] \circ (\text{id}_H + \tau_S(g_2))(\text{Ih}_S(g_1)]^{-1})(h))
\]
\[
= -h + (\eta_S(g_1) \circ [\text{Ih}_S(g_1)] \left( [\text{Ih}_S(g_1)]^{-1}(h) + \sum_{m \geq 1} (\tau_S^m(g_2) \circ [\text{Ih}_S(g_1)]^{-1})(h) \right)
\]
\[
= -h + \eta_S(g_1) \left( h + \sum_{m \geq 1} ([\text{Ih}_S(g_1)] \circ \tau_S^m(g_2) \circ [\text{Ih}_S(g_1)]^{-1})(h) \right)
\]
\[
= -h + \eta_S(g_1) \left( h + \sum_{m \geq 1} (\text{id}_H + \tau_S^m(g_2))(\text{Ih}_S(g_1)]^{-1})(h) \right)
\]

We note that
\[
\eta_S(g)|_{H^\otimes m} = (\text{id}_H + \tau_S(g))|_{H^\otimes m} : H^\otimes m \to H \times \hat{T}(2m)
\]

for any $g \in \text{Gal}_k$ and so we have the following congruences mod $\hat{T}(4)$:
\[
\eta_S(g_1)(h) \equiv h + \tau_S^1(g_1)(h) + \tau_S^2(g_1)(h),
\]
\[
\eta_S(g_1)([\text{Ih}_S(g_1)] \circ \tau_S^1(g_2) \circ [\text{Ih}_S(g_1)]^{-1})(h)
\]
\[
\equiv ([\text{Ih}_S(g_1)] \circ \tau_S^1(g_2) \circ [\text{Ih}_S(g_1)]^{-1})(h)
\]
\[
+ (\tau_S^1(g_1) \otimes \text{id}_H + \text{id}_H \otimes \tau_S^1(g_1)) \circ [\text{Ih}_S(g_1)] \circ \tau_S^1(g_2) \circ [\text{Ih}_S(g_1)]^{-1})(h),
\]
\[
\eta_S(g_1)([\text{Ih}_S(g_1)] \circ \tau_S^1(g_2) \circ [\text{Ih}_S(g_1)]^{-1})(h)
\]
\[
\equiv ([\text{Ih}_S(g_1)] \circ \tau_S^1(g_2) \circ [\text{Ih}_S(g_1)]^{-1})(h).
\]

Therefore we have
(3.2.10.2)
\[
\tau_S(g_1 g_2)(h)
\]
\[
\equiv \tau_S^1(g_1)(h) + \tau_S^2(g_1)(h)
\]
\[
+ ([\text{Ih}_S(g_1)] \circ \tau_S^1(g_2) \circ [\text{Ih}_S(g_1)]^{-1})(h)
\]
\[
+ (\tau_S^1(g_1) \otimes \text{id}_H + \text{id}_H \otimes \tau_S^1(g_1)) \circ [\text{Ih}_S(g_1)] \circ \tau_S^1(g_2) \circ [\text{Ih}_S(g_1)]^{-1})(h)
\]
\[
+ ([\text{Ih}_S(g_1)] \circ \tau_S^1(g_2) \circ [\text{Ih}_S(g_1)]^{-1})(h) \quad \text{mod } \hat{T}(4).
\]

Comparing (3.2.10.1) and (3.2.10.2), we obtain the assertions. □

### 3.3. Pro-$l$ Johnson homomorphisms.

For $n \geq 0$, let $\pi_n : \mathfrak{F}_r \to \mathfrak{F}_r/(n + 1)$ be the natural homomorphism. Since each $\mathfrak{F}_r/(n)$ is a characteristic subgroup of $\mathfrak{F}_r$, $\pi_n$ induces the natural homomorphism $\pi_n : P(\mathfrak{F}_r) \to$
Let $\text{Aut}(\mathfrak{F}_r) \to \text{Aut}(\mathfrak{F}_r/\mathfrak{F}_r(n + 1))$. Let $I_{h_{S}}^{(n)}$ denote the composite of $I_{h_{S}}$ with $\pi_{n}$:

$$I_{h_{S}}^{(n)} : \text{Gal}_{k} \longrightarrow \text{Aut}(\mathfrak{F}_r/\mathfrak{F}_r(n + 1)).$$

In particular, $I_{h_{S}}^{(1)}(g) = [I_{h_{S}}(g)]$ for $g \in \text{Gal}_{k}$. Let $\text{Gal}_{k}^{\text{Joh}}[n]$ denote the kernel of $I_{h_{S}}^{(n)}$:

$$\text{Gal}_{k}^{\text{Joh}}[n] := \text{Ker}(I_{h_{S}}^{(n)}) = \{g \in \text{Gal}_{k} | I_{h_{S}}(g)(f)f^{-1} \in \mathfrak{F}_r(n + 1) \text{ for all } f \in \mathfrak{F}_r\}.$$  

We then have the descending series of closed normal subgroups of $\text{Gal}_{k}$:

$$\text{Gal}_{k} = \text{Gal}_{k}^{\text{Joh}}[0] \supset \text{Gal}_{k}^{\text{Joh}}[1] \supset \cdots \supset \text{Gal}_{k}^{\text{Joh}}[n] \supset \cdots$$

and we call it the Johnson filtration of $\text{Gal}_{k}$ associated to the Ihara representation $\varphi_{S}$ (cf. [Aa], [J1], [J2]). We note by Theorem 1.2.6 (1)

$$\text{Gal}_{k}^{\text{Joh}}[1] = \text{Ker}(I_{h_{S}}^{(1)} : \text{Gal}_{k} \to \text{GL}(H)) = \text{Gal}_{k}(\zeta_{l^{\infty}}).$$

The relation with the Milnor filtration defined in (2.2.13) is given as follows.

**Proposition 3.3.3.** The Johnson filtration coincides with the Milnor filtration, namely, for each $n \geq 0$, we have

$$\text{Gal}_{k}^{\text{Joh}}[n] = \text{Gal}_{k}^{\text{Mil}}[n].$$

**Proof.** We may assume $n \geq 1$ and hence $g \in \text{Gal}_{k}(\zeta_{l^{\infty}})$. Then we have

$$g \in \text{Gal}_{k}^{\text{Joh}}[n] \iff I_{h_{S}}(g)(x_{i})x_{i}^{-1} \in \mathfrak{F}_r(n + 1) \text{ for all } 1 \leq i \leq r$$

$$\iff y_{i}(g)x_{i}y_{i}(g)^{-1}x_{i}^{-1} \in \mathfrak{F}_r(n + 1) \text{ for all } 1 \leq i \leq r$$

$$\iff y_{i}(g) \in \mathfrak{F}_r(n) \text{ for all } 1 \leq i \leq r$$

$$\iff \deg(\Theta(y_{i}(g) - 1)) \geq n \text{ for all } 1 \leq i \leq r$$

$$\iff g \in \text{Gal}_{k}^{\text{Mil}}[n].$$

Note that Proposition 3.3.3 yields Proposition 2.2.14. In the following, we simply write $\text{Gal}_{k}[n]$ for the $n$-th term of the Johnson (or Milnor) filtration for $n \geq 0$ and we denote by $k[n]$ the Galois subextension of $k$ in $\overline{\mathbb{Q}}$ corresponding to $\text{Gal}_{k}[n]$. By (3.3.2), we have $k[1] = k(\zeta_{l^{\infty}})$. We give some basic properties of the Johnson filtration. The following Lemma
3.3.4, Proposition 3.3.5 and Theorem 3.3.6 (2) were shown by Ihara for the case \( r = 2 \). See [Ih1; Proposition 7, page 59] and also [O1]. We give herewith concise proofs for the sake of readers.

**Lemma 3.3.4.** For \( g \in \text{Gal}_k[m] \) (\( m \geq 0 \)) and \( f \in \mathcal{F}_r(n) \) (\( n \geq 1 \)), we have

\[
I_{h_S}(g)(f^{-1}) \in \mathcal{F}_r(m + n).
\]

**Proof.** We fix \( m \geq 0 \) and \( g \in \text{Gal}_k[m] \). We prove the assertion by induction on \( n \). For \( n = 1 \), the assertion \( I_{h_S}(g)(f^{-1}) \in \mathcal{F}_r(m + 1) \) is true by the definition (3.3.1). Assume that

(3.3.4.1) \( I_{h_S}(g)(f^{-1}) \in \mathcal{F}_r(m + i) \) if \( f \in \mathcal{F}_r(i) \) and \( 1 \leq i \leq n \).

Let \( [\mathcal{F}_r(n), \mathcal{F}_r]_{\text{abst}} \) denote the abstract group generated by \([a, b] \) (\( a \in \mathcal{F}_r(n), b \in \mathcal{F}_r \)). Since \( I_{h_S}(g) \) is continuous and \( [\mathcal{F}_r(n), \mathcal{F}_r]_{\text{abst}} \) is dense in \( \mathcal{F}_r(n + 1) \), it suffices to show that

\[
I_{h_S}(g)(f^{-1}) \in \mathcal{F}_r(m + n + 1) \quad \text{for} \quad f \in [\mathcal{F}_r(n), \mathcal{F}_r]_{\text{abst}}.
\]

For this, we have only to show

(3.3.4.2) \( I_{h_S}(g)([b, c])^{-1} \in \mathcal{F}_r(m + n + 1) \) if \( b \in \mathcal{F}_r(n), c \in \mathcal{F}_r \).

For simplicity, we shall use the notation: \([\varphi, x] := \psi(x)x^{-1} \) and \([x, \varphi] := x\varphi(x)^{-1} \) for \( x \in \mathcal{F}_r \) and \( \varphi \in \text{Aut}(\mathcal{F}_r) \). By the “three subgroup lemma” and the induction hypothesis (3.3.4.1), we have

\[
I_{h_S}(g)([b, c])^{-1} = [I_{h_S}(g), [b, c]]
\in [I_{h_S}(g), [\mathcal{F}_r(n), \mathcal{F}_r]]
\subset [[I_{h_S}(g), \mathcal{F}_r(n)], \mathcal{F}_r][[\mathcal{F}_r, I_{h_S}(g)], \mathcal{F}_r(n)]
\subset [\mathcal{F}_r(m + n), \mathcal{F}_r][\mathcal{F}_r(m + 1), \mathcal{F}_r(n)]
= \mathcal{F}_r(m + n + 1)
\]

and our claim (3.3.4.2) follows. \( \square \)

Lemma 3.3.4 yields the following

**Proposition 3.3.5.** For \( m, n \geq 0 \), we have

\[
[\text{Gal}_k[m], \text{Gal}_k[n]] \subset \text{Gal}_k[m + n] \quad \text{for} \quad m, n \geq 0.
\]
In particular, the Johnson (or Milnor) filtration is a central series.

Proof. Using the same notation as in the proof of (3.3.4.2) and Lemma 3.3.4, we have

\[
[[\text{Gal}_{k[n]}, \mathfrak{F}_r], \text{Gal}_{k[m]}] \subset [\mathfrak{F}_r[n+1], \text{Gal}_{k[m]}] \subset \mathfrak{F}_r[m+n+1],
[[\mathfrak{F}_r, \text{Gal}_{k[m]}], \text{Gal}_{k[n]}] \subset [\mathfrak{F}_r(m+1), \text{Gal}_{k[n]}] \subset \mathfrak{F}_r(m+n+1).
\]

By the three subgroup lemma, we have

\[
[[\text{Gal}_{k[m]}, \text{Gal}_{k[n]}], \mathfrak{F}_r] \subset [\text{Gal}_{k[n]}, \mathfrak{F}_r], [\text{Gal}_{k[m]}, \mathfrak{F}_r, \text{Gal}_{k[n]}] \subset [\text{Gal}_{k[n+1]}, \mathfrak{F}_r(n+1), \mathfrak{F}_r(m+n+1)],
\]

which yields the assertion by the definition (3.3.1). □

For \(n \geq 0\), let

\[
\text{gr}_n(\text{Gal}_k) := \text{Gal}_{k[n]}/\text{Gal}_{k[n+1]},
\]

which is a \(\mathbb{Z}_l\)-module. Then, by Proposition 3.3.5, the graded \(\mathbb{Z}_l\)-module

\[
\text{gr}(\text{Gal}_k) := \bigoplus_{n \geq 0} \text{gr}_n(\text{Gal}_k)
\]

has the structure of a graded Lie algebra over \(\mathbb{Z}_l\), where the Lie bracket is defined by the commutator: For \(a = g \text{ mod } \text{Gal}_{k[m+1]}, b = h \text{ mod } \text{Gal}_{k[n+1]}\) \((g \in \text{Gal}_{k[m]}, h \in \text{Gal}_{k[n]}),\)

\[
[a, b] := [g, h] \text{ mod } \text{Gal}_{k[m+n+1]}.
\]

Now, for \(m \geq 1\), we let \(\tau^{[m]}_S\) denote the restriction of the \(m\)-th \(l\)-adic Johnson map \(\tau^{(m)}_S\) in (3.2.8) to \(\text{Gal}_{k[m]}\):

\[
\tau^{[m]}_S := \tau^{(m)}_S|_{\text{Gal}_k[m]} : \text{Gal}_k[m] \rightarrow \text{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)}).
\]

The following theorem asserts that \(\tau^{[m]}_S\) describes the action of \(\text{Gal}_{k[m]}\) on \(\mathfrak{F}_r/\mathfrak{F}_r(m+2)\).

**Theorem 3.3.6.** Notations being as above, the following assertions hold.

(1) For \(g \in \text{Gal}_k[m]\) and \(f \in \mathfrak{F}_r\), we have

\[
\tau^{[m]}_S(g)([f]) = \Theta_{m+1}(\text{Ih}_S(g)(f)f^{-1}),
\]

33
where \( \Theta_{m+1} : \text{gr}_{m+1}(\mathfrak{F}_r) \hookrightarrow H^{\otimes(m+1)} \) is the degree \((m + 1)\)-part of the Magnus embedding in (3.1.3).

(2) The map \( \tau_S^{[m]} \) is a \( \mathbb{Z}_l \)-homomorphism and \( \text{Ker}(\tau_S^{[m]}) = \text{Gal}_k[m+1] \). Hence \( \tau_S^{[m]} \) induces the injective \( \mathbb{Z}_l \)-homomorphism \( \text{gr}_m(\text{Gal}_k) \hookrightarrow \text{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)}) \).

In particular, we have
\[
\text{gr}_m(\text{Gal}_k) \cong \mathbb{Z}_l^{\oplus r_m}
\]
for some integer \( r_m \geq 0 \).

**Proof.** (1) We need to show that for \( g \in \text{Gal}_k[m] \),
\[
(3.3.6.1) \quad \tau_S^{(m)}(g)(X_i) = \Theta_{m+1}(\text{Ih}_S(g)(x_i)x_i^{-1}) \quad 1 \leq i \leq r.
\]

By (3.2.7) and \( [\text{Ih}_S(g)] = \text{id}_H \), we have
\[
\tau_S(g)(X_i) = (\Theta \circ \text{Ih}_S(g) \circ \Theta^{-1})(\Theta(x_i) - 1) - (\Theta(x_i) - 1) = \Theta(\text{Ih}_S(g)(x_i)) - \Theta(x_i).
\]

Therefore, by (3.2.8), we have
\[
(3.3.6.2) \quad \tau_S^{(m)}(g)(X_i) = \text{the component in } H^{\otimes(m+1)} \text{ of } \Theta(\text{Ih}_S(g)(x_i)) - \Theta(x_i).
\]

On the other hand, since \( \text{Ih}_S(g)(x_i)x_i^{-1} \in \mathfrak{F}_r(m + 1) \), we have
\[
\Theta(\text{Ih}_S(g)(x_i)x_i^{-1}) \equiv 1 + \Theta_{m+1}(\text{Ih}_S(g)(x_i)x_i^{-1}) \mod \hat{T}(m + 2).
\]

Multiplying the above equation by \( \Theta(x_i) \) from right, we have
\[
(3.3.6.3) \quad \Theta(\text{Ih}_S(g)(x_i)) \equiv \Theta(x_i) + \Theta_{m+1}(\text{Ih}_S(g)(x_i)x_i^{-1}) \mod \hat{T}(m + 2).
\]

By (3.3.6.2) and (3.3.6.3), we obtain (3.3.6.1).

(2) By (1), for \( g, h \in \text{Gal}_k[m] \) and \( f \in \mathfrak{F}_r \), we have
\[
\tau_S^{[m]}(gh)([f]) = \Theta_{m+1}(\text{Ih}_S(gh)(f)f^{-1}) = \Theta_{m+1}(\text{Ih}_S(g)(\text{Ih}_S(h)(f))f^{-1}) = \Theta_{m+1}(\text{Ih}_S(g)(\text{Ih}_S(h)(f)f^{-1})\text{Ih}_S(g)(f)f^{-1}).
\]

Since \( \text{Ih}_S(h)(f)f^{-1} \in \mathfrak{F}_r(m+1) \), we have \( \text{Ih}_S(g)(\text{Ih}_S(h)(f)f^{-1}) \equiv \text{Ih}_S(h)(f)f^{-1} \mod \mathfrak{F}_r(2m + 1)(\subset \mathfrak{F}_r(m + 2)) \) by Lemma 3.3.4, and hence
\[
\tau_S^{[m]}(gh)([f]) = \Theta_{m+1}(\text{Ih}_S(g)(f)f^{-1}) + \Theta_{m+1}(\text{Ih}_S(h)(f)f^{-1}) = (\tau_S^{[m]}(g) + \tau_S^{[m]}(h))(f).
\]

34
for any \( f \in \xi_r \). Since \( \text{Ih}_S \) is continuous, we see that \( \tau_S^{[m]} \) is a \( \mathbb{Z}_l \)-homomorphism. By (1) and (3.3.1), \( \text{Ker}(\tau_S^{[m]}) = \text{Gal}_k[m+1] \), and hence \( \tau_S^{[m]} \) induces the injective \( \mathbb{Z}_l \)-homomorphism \( \text{gr}_m(\text{Gal}_k) \hookrightarrow \text{Hom}_{\mathbb{Z}_l}(H,H^{\otimes (m+1)}) \). Since \( \text{Hom}_{\mathbb{Z}_l}(H,H^{\otimes (m+1)}) \) is a free \( \mathbb{Z}_l \)-module of finite rank, the last assertion follows. \( \square \)

By Theorem 3.3.6 (1), \( \tau_S^{[m]} \) factors through \( \text{Hom}_{\mathbb{Z}_l}(H,\text{gr}_{m+1}(\xi_r)) \)

\[
\tau_S^{[m]} : \text{Gal}_k[m] \rightarrow \text{Hom}_{\mathbb{Z}_l}(H,\text{gr}_{m+1}(\xi_r)); \ g \mapsto ([f] \mapsto \text{Ih}_S(g)(f)f^{-1})
\]

followed by the map \( \text{Hom}_{\mathbb{Z}_l}(H,\text{gr}_{m+1}(\xi_r)) \rightarrow \text{Hom}_{\mathbb{Z}_l}(H,H^{\otimes (m+1)}) \) induced by \( \Theta_{m+1} \). We call \( \tau_S^{[m]} : \text{Gal}_k[m] \rightarrow \text{Hom}_{\mathbb{Z}_l}(H,H^{\otimes (m+1)}) \) \( (m \geq 1) \) or the induced injective \( \mathbb{Z}_l \)-homomorphism \( \text{gr}_m(\text{Gal}_k) \hookrightarrow \text{Hom}_{\mathbb{Z}_l}(H,H^{\otimes (m+1)}) \), denoted by the same \( \tau_S^{[m]} \), the \( m \)-th pro-\( l \) Johnson homomorphism.

A relation between the \( m \)-th pro-\( l \) Johnson homomorphisms and \( l \)-adic Milnor numbers in Section 2 is given as follows.

**Theorem 3.3.7.** For \( g \in \text{Gal}_k[m] \) \( (m \geq 1) \), we have

\[
\tau_S^{[m]}(g)(X_i) = - \sum_{|J|=m+1} \mu(J)X_J,
\]

where for \( J = (j_1 \cdots j_{m+1}) \),

\[
\mu(J) = \begin{cases} 
\mu(g; j_2 \cdots j_{m+1}j_1) - \delta_{j_1,j_{m+1}}\mu(g; J) & (i = j_1), \\
\mu(g; j_2 \cdots j_{m+1}j_1j) - \mu(g; J) & (i = j_{m+1}), \\
0 & (\text{otherwise}).
\end{cases}
\]

**Proof.** By Theorem 3.3.6 (1), we have

\[
\tau_S^{[m]}(g)(X_i) = \Theta_{m+1}(\text{Ih}_S(g)(x_i)x_i^{-1})
= \Theta_{m+1}(y_i(g)x_iy_i(g)^{-1}x_i^{-1})
= -\Theta_{m+1}([x_i, y_i(g)])
= - \sum_{|J|=m+1} \mu(J; [x_i, y_i(g)])X_J.
\]

(3.3.7.1)

By the computation in the proof of Theorem 2.3.3, we have, for \( |J| = \)
\((j_1 \cdots j_{m+1})\),
\[(3.3.7.2)\]
\[
\mu(J;[x_i,y_i(g)]) = \mu(J;x_i y_i(g)) - \mu(J;y_i(g)x_i)
\]
\[
= \left\{
\begin{array}{ll}
\mu(g;j_2 \cdots j_{m+1} J_{j_1}) - \delta_{j_1} \delta_{j_{m+1}} \mu(g; J) & (i = j_1), \\
\mu(g;j_2 \cdots j_{m+1} J_{j_1}) \delta_{j_1} \delta_{j_{m+1}} - \mu(g; J) & (i = j_{m+1}). \\
0 & \text{(otherwise)}.
\end{array}
\right.
\]

By (3.3.7.1) and (3.3.7.2), the assertion follows. \(\square\)

**Remark 3.3.8.** A correspondence between Johnson invariants and Milnor invariants was given by Habegger in a topological framework ([Ha]). Our treatment in this paper is group-theoretical and similar to that given in [Ko1], [Ko3; Chapter 1] for pure braids.

We compute the pro-\(l\) Johnson homomorphisms on commutators.

**Proposition 3.3.9.** For \(g \in \text{Gal}_k[m]\), \(h \in \text{Gal}_k[n]\) \((m, n \geq 0)\) and \(f \in \frak{F}_r\), we have
\[
\tau_{\frak{S}}^{[m+n]}([g,h])([f]) = \Theta_{m+n+1}(\text{Ih}_s(g)(\text{Ih}_s(h)(f))^{-1})(\text{Ih}_s(h)(f))^{-1} - \text{Ih}_s(h)(\text{Ih}_s(g)(f))^{-1}(\text{Ih}_s(g)(f))^{-1}.
\]

**Proof.** For simplicity, we set \(\psi := \text{Ih}_s(g), \phi := \text{Ih}_s(h)\). By a straightforward computation using \([g,h] \in \text{Gal}_k[m+n]\) (Proposition 3.3.5) and \(\psi(f)^{-1} \in \frak{F}_r(m+1)\) (Lemma 3.3.4), we obtain
\[
[\psi, \phi](f)^{-1} = [\psi, \phi]((\phi(f)^{-1})^{-1}) \cdot (\psi \phi \psi^{-1}((\psi(f)^{-1})^{-1}) \cdot \psi(\phi(f)^{-1}) \cdot \psi(f)^{-1}
\]
\[
= (\phi(f)^{-1})^{-1} \cdot \phi((\psi(f)^{-1})^{-1}) \cdot \psi(\phi(f)^{-1}) \cdot \psi(f)^{-1} \text{ mod } \frak{F}_r(m+n+2).
\]

Since \(\psi(f)^{-1} \in \frak{F}_r(m+1), \phi(f)^{-1} \in \frak{F}_r(n+1)\) and \([\frak{F}_r(m+1), \frak{F}_r(n+1)] \subset \frak{F}(m+n+2)\), we have
\[
[\psi, \phi](f)^{-1} \equiv (\phi(f)^{-1})^{-1} \cdot \psi(\phi(f)^{-1}) \cdot \phi((\psi(f)^{-1})^{-1}) \cdot \psi(f)^{-1} \text{ mod } \frak{F}_r(m+n+2).
\]

Since we easily see that
\[
\left\{
\begin{array}{ll}
(\phi(f)^{-1})^{-1} \psi(\phi(f)^{-1}) \equiv \psi(\phi(f)^{-1})(\phi(f)^{-1})^{-1} \mod \frak{F}_r(m+n+2), \\
\phi((\psi(f)^{-1})^{-1}) \cdot \psi(f)^{-1} \equiv (\phi(\psi(f)^{-1}) \cdot (\psi(f)^{-1})^{-1})^{-1} \mod \frak{F}_r(m+n+2),
\end{array}
\right.
\]

36
we obtain the assertion. □

By Proposition 3.3.9, the direct sum of Johnson homomorphisms $\tau^m_S$ over all $m \geq 1$ defines a graded Lie algebra homomorphism from $\text{gr}(\text{Gal}_k)$ to the derivation algebra of $\text{gr}(\frak{F}_r)$ as follows. Recall that a $\mathbb{Z}_r$-linear endomorphism $\delta$ of $\text{gr}(\frak{F}_r)$ is called a derivation on $\text{gr}(\frak{F}_r)$ if it satisfies

$$\delta([x, y]) = [\delta(x), y] + [x, \delta(y)] \quad (x, y \in \text{gr}(\frak{F}_r)).$$

Let $\text{Der}(\text{gr}(\frak{F}_r))$ denote the associative $\mathbb{Z}_l$-algebra of all derivations on $\text{gr}(\frak{F}_r)$ which has a Lie algebra structure over $\mathbb{Z}_l$ with the Lie bracket defined by $[\delta, \delta'] := \delta \circ \delta' - \delta' \circ \delta$ for $\delta, \delta' \in \text{Der}(\text{gr}(\frak{F}_r))$. For $m \geq 0$, we define the subspace $\text{Der}_m(\text{gr}(\frak{F}_r))$ of $\text{Der}(\text{gr}(\frak{F}_r))$, the degree $m$ part, by

$$\text{Der}_m(\text{gr}(\frak{F}_r)) := \{ \delta \in \text{Der}(\text{gr}(\frak{F}_r)) | \delta(\text{gr}_n(\frak{F}_r)) \subset \text{gr}_{m+n}(\frak{F}_r) \text{ for } n \geq 1 \}$$

so that $\text{Der}(\text{gr}(\frak{F}_r))$ is a graded Lie algebra over $\mathbb{Z}_l$:

$$\text{Der}(\text{gr}(\frak{F}_r)) = \bigoplus_{m \geq 0} \text{Der}_m(\text{gr}(\frak{F}_r)).$$

A derivation $\delta \in \text{Der}_m(\text{gr}(\frak{F}_r))$ is called a special derivation if there are $Y_i \in \text{gr}_m(\frak{F}_r)$ such that $\delta(X_i) = [Y_i, X_i]$ (1 \leq i \leq r) and moreover if the condition $\sum_{i=1}^r [Y_i, X_i] = 0$ is satisfied, a special derivation is said to be normalized ([Ilh4; §2]). It is easy to see that normalized special derivations form a graded Lie subalgebra

$$\text{Der}^{n,s}(\text{gr}(\frak{F}_r)) = \bigoplus_{m \geq 0} \text{Der}_m^{n,s}(\text{gr}(\frak{F}_r))$$

of $\text{Der}(\text{gr}(\frak{F}_r))$. Since a derivation on $\text{gr}(\frak{F}_r)$ is determined by its restriction on $H = \text{gr}_1(\frak{F}_r)$, we have a natural inclusion, for each $m \geq 1$,

$$\text{Der}_m(\text{gr}(\frak{F}_r)) \subset \text{Hom}_{\mathbb{Z}_l}(H, \text{gr}_{m+1}(\frak{F}_r)); \ \delta \mapsto \delta|_H.$$

Hence we have the inclusions

$$\text{Der}^{n,s}_+(\text{gr}(\frak{F}_r)) \subset \text{Der}_+(\text{gr}(\frak{F}_r)) \subset \bigoplus_{m \geq 1} \text{Hom}_{\mathbb{Z}_p}(H, \text{gr}_{m+1}(\frak{F}_r)),$$

where $\text{Der}_+(\text{gr}(\frak{F}_r))$ (resp. $\text{Der}^{n,s}_+(\text{gr}(\frak{F}_r))$) is the Lie subalgebra of $\text{Der}(\text{gr}(\frak{F}_r))$ (resp. $\text{Der}^{n,s}_+(\text{gr}(\frak{F}_r))$) consisting of positive degree part. Although we make
use of the arithmetic pro-l Johnson homomorphisms, the following proposition was essentially proved by Ihara in [Ih4; §2].

**Proposition 3.3.10.** The direct sum of $\tau_{S}^{[m]}$ over $m \geq 1$ defines the Lie algebra homomorphism

$$\text{gr}(\tau) := \bigoplus_{m \geq 1} \tau_{S}^{[m]} : \text{gr}(\text{Gal}_k) \longrightarrow \text{Der}_{s}^{n_{s}}(\text{gr}(\mathfrak{f}_{r})).$$

**Proof.** (cf. [Da; Proposition 3.18]) By Theorem 3.3.6 (1), it suffices to show that for $g \in \text{Gal}_k[m]$, the map $f \mapsto \text{Ih}_S(g)(f)f^{-1}$ is indeed a special derivation on $\text{gr}(\mathfrak{f}_{r})$. This was shown in [Ih4; §2] for the case $r = 2$. We give herewith a proof for the sake of readers. Let $g \in \text{Gal}_k[m] (m \geq 1)$ and $s \in \mathfrak{f}_{r}(i), h \in \mathfrak{f}_{r}(j)$. By using the commutator formulas

$$[ab, c] = a[b, c]a^{-1} \cdot [a, c], \quad [a, bc] = [a, b] \cdot [a, c]b^{-1} \quad (a, b, c \in G),$$

we have

$$\text{Ih}_S(g)([s, t])[s, t]^{-1} = [\text{Ih}_S(g)(s), \text{Ih}_S(g)(t)][s, t]^{-1}$$

$$= [s^{-1}\text{Ih}_S(g)(s), \text{Ih}_S(g)(t)t^{-1}][s, t]^{-1}$$

$$= s[s^{-1}\text{Ih}_S(g)(s), \text{Ih}_S(g)(t)t^{-1}][s^{-1}\text{Ih}_S(g)(s), t](\text{Ih}_S(g)(t)t^{-1})^{-1}s^{-1}$$

$$\cdot [s, \text{Ih}_S(g)(t)t^{-1}][\text{Ih}_S(g)(t)t^{-1}][s, t](\text{Ih}_S(g)(t)t^{-1})^{-1}[s, t]^{-1}$$

$$= s[s^{-1}\text{Ih}_S(g)(s), \text{Ih}_S(g)(t)t^{-1}][s^{-1}\text{Ih}_S(g)(s), t][\text{Ih}_S(g)(t)t^{-1}]^{-1}s^{-1}$$

$$\cdot [s, \text{Ih}_S(g)(t)t^{-1}][\text{Ih}_S(g)(t)t^{-1}, [s, t]].$$

Since $s^{-1}\text{Ih}_S(g)(s) \in \mathfrak{f}_{r}(i + m), \text{Ih}_S(g)(t)t^{-1} \in \mathfrak{f}_{r}(j + m)$ by Lemma 3.3.4, we have

$$[s^{-1}\text{Ih}_S(g)(s), \text{Ih}_S(g)(t)t^{-1}] \in \mathfrak{f}_{r}(i + j + 2m), \quad [\text{Ih}_S(g)(t)t^{-1}, [s, t]] \in \mathfrak{f}_{r}(i + 2j + m).$$

By these claims together, we obtain

$$\text{Ih}_S(g)([s, t])[s, t]^{-1}$$

$$\equiv s\text{Ih}_S(g)(t)t^{-1}[s^{-1}\text{Ih}_S(g)(s), t](s\text{Ih}_S(g)(t)t^{-1})^{-1}[s, \text{Ih}_S(g)(t)t^{-1}] \mod \mathfrak{f}_{r}(i + j + m + 1).$$

Noting $x[s^{-1}\text{Ih}_S(g)(s), t]x^{-1} \equiv [s^{-1}\text{Ih}_S(g)(s), t] \mod \mathfrak{f}_{r}(i + j + m + 1)$ for $x \in \mathfrak{f}_{r}$, we proved that $f \mapsto \text{Ih}_S(g)(f)f^{-1}$ is a derivation. That it is special and normalized follows from $\text{Ih}_S(g)(x_i) = y_i(g)x_iy_i(g)^{-1} (1 \leq i \leq r)$ and

38
Ih$_S(g)(x_1 \cdots x_r) = x_1 \cdots x_r$ for $g \in \text{Gal}_k[m]$ ($m \geq 1$). \hfill \Box

Finally we introduce an analogue of the Morita trace map ([Mt1; 6]). For each $m \geq 1$, we identify $\text{Hom}_{Z_l}(H, H^\otimes(m+1))$ with $H^* \otimes_{Z_l} H^\otimes(m+1)$, where $H^* := \text{Hom}_{Z_l}(H, Z_l)$ is the dual $Z_l$-module, and let
\[
c_{m+1} : \text{Hom}_{Z_l}(H, H^\otimes(m+1)) = H^* \otimes_{Z_l} H^\otimes(m+1) \longrightarrow H^\otimes m
\]
be the contraction at $(m+1)$-component defined by
\[
c_{m+1}(\phi \otimes h_1 \otimes \cdots \otimes h_{m+1}) := \phi(h_{m+1})h_1 \otimes \cdots \otimes h_m
\]
for $\phi \in H^*$, $h_i \in H$. We then define the $m$-th pro-$l$ Morita trace map
\[
\text{Tr}^{[m]} : \text{Hom}_{Z_l}(H, H^\otimes(m+1)) \rightarrow S^m(H)
\]
by the composite map $q \circ c_{m+1}.$

4. Pro-$l$ Magnus-Gassner cocycles

4.1. Pro-$l$ Fox free derivation. The pro-$l$ Fox free derivative $\frac{\partial}{\partial x_j}$: $\mathbb{Z}_l[[\mathcal{F}_r]] \rightarrow \mathbb{Z}_l[[\mathcal{F}_r]]$ ($1 \leq j \leq r$) is a continuous $\mathbb{Z}_l$-linear map satisfying the following property: For any $\alpha \in \mathbb{Z}_l[[\mathcal{F}_r]],$
\[
\alpha = \epsilon_{\mathbb{Z}_l[[\mathcal{F}_r]]}(\alpha) + \sum_{j=1}^r \frac{\partial \alpha}{\partial x_j}(x_j - 1).
\]
We note by (4.1.1) that $\frac{\partial \alpha}{\partial x_j} \in I_{\mathbb{Z}_l[[\mathcal{F}_r]]}^{n-1}$ if $\alpha - \epsilon_{\mathbb{Z}_l[[\mathcal{F}_r]]}(\alpha) \in I_{\mathbb{Z}_l[[\mathcal{F}_r]]}^n$ for $n \geq 1$.

Here are some basic rules for the pro-$l$ free calculus:

(i) $\frac{\partial x_i}{\partial x_j} = \delta_{ij}$.

(ii) $\frac{\partial \alpha \beta}{\partial x_j} = \frac{\partial \alpha}{\partial x_j}\epsilon_{\mathbb{Z}_l[[\mathcal{F}_r]]}(\beta) + \alpha \frac{\partial \beta}{\partial x_j}$ ($\alpha, \beta \in \mathbb{Z}_l[[\mathcal{F}_r]]$).

(iii) $\frac{\partial f^{-1}}{\partial x_j} = -f^{-1} \frac{\partial f}{\partial x_j}$ ($f \in \mathcal{F}_r$).

(iv) $\frac{\partial f^\alpha}{\partial x_j} = \beta \frac{\partial f}{\partial x_j}$ ($f \in \mathcal{F}_r, \alpha \in \mathbb{Z}_l$), where $\beta$ is any element of $\mathbb{Z}_l[[\mathcal{F}_r]]$. 

39
such that \( \beta(f - 1) = f^\alpha - 1 \) if exists.

(v) \( \frac{\partial \varphi(\alpha)}{\partial \varphi(x_j)} = \varphi \left( \frac{\partial \alpha}{\partial x_j} \right) \) (\( \varphi \in \text{Aut}(\mathfrak{F}_r), \alpha \in \mathbb{Z}_l[[\mathfrak{F}_r]] \)). (Note that \( \varphi(x_1), \ldots, \varphi(x_r) \) are free generators of \( \mathfrak{F}_r \).

(vi) If \( \mathfrak{F}' \) is an open free subgroup of \( \mathfrak{F}_r \) with free generators \( y_1, \ldots, y_s \), we have the chain rule:

\[
\frac{\partial \alpha}{\partial x_j} = \sum_{i=1}^{s} \frac{\partial \alpha}{\partial y_i} \frac{\partial y_i}{\partial x_j} \quad (\alpha \in \mathbb{Z}_l[[\mathfrak{F}']]).
\]

The higher derivatives are defined inductively and the \( l \)-adic Magnus coefficient \( \mu(I; \alpha) \) of \( \alpha \in \mathbb{Z}_l[[\mathfrak{F}_r]] \) for \( I = (i_1 \cdots i_n) \) is expressed by

\[
\mu(I; \alpha) = \epsilon_{\mathbb{Z}_l[[\mathfrak{F}_r]]} \left( \frac{\partial^n \alpha}{\partial x_{i_1} \cdots \partial x_{i_n}} \right)
\]

so that the pro-\( l \) Magnus expansion (2.1.4) is written as

\[
\Theta(\alpha) = \epsilon_{\mathbb{Z}_l[[\mathfrak{F}_r]]}(\alpha) + \sum_{1 \leq i_1, \ldots, i_n \leq r} \epsilon_{\mathbb{Z}_l[[\mathfrak{F}_r]]} \left( \frac{\partial^n \alpha}{\partial x_{i_1} \cdots \partial x_{i_n}} \right) X_{i_1} \cdots X_{i_n}.
\]

### 4.2. Pro-\( l \) Magnus cocycles.

Let \( \text{Ih}_S : \text{Gal}_k \to P(\mathfrak{F}_r) \subset \text{Aut}(\mathfrak{F}_r) \) be the Ihara representation associated to \( S \) in (1.2.3). Let \( \bar{\cdot} : \mathbb{Z}_l[[\mathfrak{F}_r]] \to \mathbb{Z}_l[[\mathfrak{F}_r]] \) denote the anti-automorphism induced by the involution \( \mathfrak{F}_r \ni f \mapsto f^{-1} \in \mathfrak{F}_r \).

We define the pro-\( l \) Magnus cocycle \( M_S : \text{Gal}_k \to M(r; \mathbb{Z}_l[[\mathfrak{F}_r]]) \) associated to \( \text{Ih}_S \) by

\[
M_S(g) := \left( \frac{\partial \text{Ih}_S(g)(x_j)}{\partial x_i} \right)
\]

for \( g \in \text{Gal}_k \). In fact, we have the following

**Lemma 4.2.2.** The map \( M_S \) is a 1-cocycle of \( \text{Gal}_k \) with coefficients in \( \text{GL}(r; \mathbb{Z}_l[[\mathfrak{F}_r]]) \) with respect to the action \( \text{Ih}_S \). To be precise, for \( g, h \in \text{Gal}_k \), we have

\[
M_S(gh) = M_S(g) \text{Ih}_S(g)(M_S(h)),
\]

where \( \text{Ih}_S(g)(M_S(h)) \) is the matrix obtained by applying \( \text{Ih}_S(g) \) to each entry of \( M_S(h) \).

**Proof.** Let \( y_j := \text{Ih}_S(h)(x_j) \) for \( 1 \leq j \leq r \). Then we have

\[
\frac{\partial \text{Ih}_S(gh)(x_j)}{\partial x_i} = \frac{\partial \text{Ih}_S(g)(y_j)}{\partial x_i}.
\]
Using the basic rules (v), (vi) of the pro-

Fox derivatives, we have

\[ \frac{\partial \mathrm{I}_S(g)(y_j)}{\partial x_i} = \sum_{a=1}^{r} \frac{\partial \mathrm{I}_S(g)(y_j)}{\partial x_a} \frac{\partial \mathrm{I}_S(g)(x_a)}{\partial x_i} \]

(4.2.2.2)

By (4.2.2.1) and (4.2.2.2), we have

\[ \frac{\partial \mathrm{I}_S(gh)(x_j)}{\partial x_i} = \sum_{a=1}^{r} \frac{\partial \mathrm{I}_S(g)(x_a)}{\partial x_i} \cdot \mathrm{I}_S(g) \left( \frac{\partial y_j}{\partial x_a} \right) \frac{\partial \mathrm{I}_S(g)(x_a)}{\partial x_i} \]

Since \( \mathrm{I}_S(g) \) and \( - \) are commutative operators, we obtain the desired equality of the matrices. Taking \( h = g^{-1} \), we see that \( M_S(g) \in \text{GL}(r; \mathbb{Z}_l[[\mathfrak{F}_r]]) \) for \( g \in \text{Gal}_k \). \( \square \).

For \( m \geq 1 \), we let \( M_S^{[m]} \) be the composite of \( M_S \) restricted to \( \text{Gal}_k[m] \) with the natural homomorphism \( \text{GL}(r; \mathbb{Z}_l[[\mathfrak{F}_r]]) \to \text{GL}(r; \mathbb{Z}_l[[\mathfrak{F}_r]])/I_{Z_l[[\mathfrak{F}_r]]}^{m+1} \)

\[ M_S^{[m]} : \text{Gal}_k[m] \to \text{GL}(r; \mathbb{Z}_l[[\mathfrak{F}_r]])/I_{Z_l[[\mathfrak{F}_r]]}^{m+1}. \]

A relation between \( M_S^{[m]} \) and the \( m \)-th pro-\( l \) Johnson homomorphism is given as follows. First, recall the identification \( \Theta_n : \text{gr}_n(\mathfrak{F}_r) \simeq H^\otimes n \) by the degree \( n \) part of the Magnus isomorphism in (3.1.2). We then have a matrix representation of \( \text{Hom}_{\mathbb{Z}_l}(H, H^\otimes (m+1)) \) for \( m \geq 1 \)

\[ || \tau || : \text{Hom}_{\mathbb{Z}_l}(H, H^\otimes (m+1)) \to M(r; \text{gr}_m(\mathbb{Z}_l[[\mathfrak{F}_r]])) \]

by associating to each element \( \tau \in \text{Hom}_{\mathbb{Z}_l}(H, H^\otimes (m+1)) \) the matrix

(4.2.3) \[ ||\tau|| := \left( \frac{\partial (\Theta_{m+1}^{-1} \circ \tau)(X_j)}{\partial x_i} \right) \in M(r; \text{gr}_m(\mathbb{Z}_l[[\mathfrak{F}_r]])). \]

**Proposition 4.2.4.** For \( g \in \text{Gal}_k[m] \), we have

\[ M_S^{[m]}(g) = I + ||\tau_S^{[m]}(g)||. \]

**Proof.** By Theorem 3.3.6, we have

\[ (\Theta_{m+1}^{-1} \circ \tau_S^{[m]}(g))(X_j) = \mathrm{I}_S(g)(x_j)x_j^{-1} \]
and so
\[
\frac{\partial (\Theta_{m+1}^{-1} \circ \tau^{[m]}_S)(X_j)}{\partial x_i} = \frac{\partial \text{Ih}_S(g)(x_j)x_j^{-1}}{\partial x_i} = \frac{\partial \text{Ih}_S(g)(x_j)}{\partial x_i} - \text{Ih}_S(g)(x_j)x_j^{-1}\delta_{ij}.
\]
Since \(\text{Ih}_S(g)(x_j)x_j^{-1} \in \mathfrak{F}_r(m + 1)\), we have \(\text{Ih}_S(g)(x_j)x_j^{-1}\delta_{ij} \equiv \delta_{ij} \mod \mathfrak{F}_r\) and hence the assertion is proved. □

In terms of \(\| \cdot \|\), the \(m\)-th pro-l Morita trace \(\text{Tr}^{[m]}(\tau)\) in (3.3.12) is, in fact, written as the trace of the matrix \(\|\tau\|\).

**Proposition 4.2.5.** For \(m \geq 1\) and \(\tau \in \text{Hom}_{\mathbb{Z}_l}(H, H^\otimes (m+1))\), we have
\[
\text{Tr}^{[m]}(\tau) = q_m(\text{tr}(\Theta_m(\|\tau\|))),
\]
where \(q_m : H^\otimes m \rightarrow S^m(H)\) is the natural map.

**Proof.** We identify \(\text{Hom}_{\mathbb{Z}_l}(H, H^\otimes (m+1))\) with \(H^* \otimes H^\otimes m\). Let \(\tau = \phi \otimes X_{i_1} \otimes \cdots \otimes X_{i_{m+1}}\) (\(\phi \in H^*\)). By (4.2.3), we have
\[
(4.2.5.1) \quad \text{tr}(\|\tau\|) = \sum_{i=1}^{r} \frac{\partial (\Theta_{m+1}^{-1} \circ \tau)(X_i)}{\partial x_i} = \sum_{i=1}^{r} \phi(X_i) \frac{\partial \Theta_{m+1}^{-1}(X_{i_1} \otimes \cdots \otimes X_{i_{m+1}})}{\partial x_i}.
\]
We note that any element \(Y\) of \(H^\otimes (m+1)\) can be written uniquely as
\[
Y = Y_1 \otimes X_1 + \cdots + Y_r \otimes X_r, \quad Y_i \in H^\otimes m
\]
and then we have, by (4.1.1),
\[
\frac{\partial \Theta_{m+1}^{-1}(Y)}{\partial x_i} = \Theta_m^{-1}(Y_i).
\]
Therefore we have
\[
\frac{\partial \Theta_{m+1}^{-1}(X_{i_1} \otimes \cdots \otimes X_{i_{m+1}})}{\partial x_i} = \delta_{i,i_{m+1}} X_{i_1} \otimes \cdots \otimes X_{i_m}
\]
and hence, by (4.2.5.1),
\[
\text{tr}(\Theta_m(\|\tau\|)) = \phi(X_{i_{m+1}})X_{i_1} \otimes \cdots \otimes X_{i_m}.
\]

42
where the right hand side is $c_{m+1}(\tau)$ by (3.3.11). By the definition (3.3.12), the assertion is proved. □

Now, for some application later on, we extend the construction of the pro-$l$ Magnus cocycle to a relative situation. Let $\mathfrak{G}$ be a pro-$l$ group and let $\psi : \mathfrak{F}_r \to \mathfrak{G}$ be a continuous surjective homomorphism. We also denote by $\psi$ the induced surjective homomorphism $\mathbb{Z}_l[[\mathfrak{F}_r]] \to \mathbb{Z}_l[[\mathfrak{G}]]$ of complete group algebras over $\mathbb{Z}_l$. Let $\mathfrak{N} := \text{Ker}(\psi)$ so that $\mathfrak{F}_r/\mathfrak{N} \simeq \mathfrak{G}$. We assume that $\mathfrak{N}$ is stable under the action of $\text{Gal}_k$ through $\text{Ih}_S$, namely $\text{Ih}_S(g)(\mathfrak{N}) \subset \mathfrak{N}$ for all $g \in \text{Gal}_k$ (This is certainly satisfied if $\mathfrak{N}$ is a characteristic subgroup of $\mathfrak{F}_r$).

Then we have a homomorphism $\text{Ih}_{S,\psi} : \text{Gal}_k \to \text{Aut}(\mathbb{Z}_l[[\mathfrak{G}]])$ defined by

\begin{equation}
(4.2.6) \quad \text{Ih}_{S,\psi}(g)(\psi(\alpha)) := \psi(\text{Ih}_S(g)(\alpha)) \quad (\alpha \in \mathbb{Z}_l[[\mathfrak{F}_r]]).
\end{equation}

Let $\text{Gal}_k[\psi]$ be the subgroup of $\text{Gal}_k$ defined by

\begin{equation}
(4.2.7) \quad \text{Gal}_k[\psi] := \text{Ker}(\text{Ih}_{S,\psi}) = \{g \in \text{Gal}_k \mid \psi \circ \text{Ih}_S(g) = \psi\}
\end{equation}

and let $k[\psi]$ denote the subfield of $\overline{\mathbb{Q}}/k$ corresponding to $\text{Gal}_k[\psi]$. Now we define the pro-$l$ Magnus cocycle $M_{S,\psi} : \text{Gal}_k \to \text{GL}(r;\mathbb{Z}_l[[\mathfrak{G}]])$ associated to $\text{Ih}_S$ and $\psi$ by

\[ M_{S,\psi}(g) := \psi(M_S(g)) \quad (g \in \text{Gal}_k), \]

where the right hand side is the matrix obtained by applying $\psi$ to each entry of $M_S(g)$. For $m \geq 1$, let $M_{S,\psi}^{[m]}$ be the composite of $M_{S,\psi}$ with the natural homomorphism $\text{GL}(r;\mathbb{Z}_l[[\mathfrak{F}_r]])/I_{\mathbb{Z}_l[[\mathfrak{F}_r]]}^{m+1} \to \text{GL}(r;\mathbb{Z}_l[[\mathfrak{G}]])/I_{\mathbb{Z}_l[[\mathfrak{G}]]}^{m+1}$ induced by $\psi$.

Lemma 4.2.2 and Proposition 4.2.4 are extended to the following

**Proposition 4.2.8.** Notations being as above, the following assertions hold.

1. For $g, h \in \text{Gal}_k$, we have

\[ M_{S,\psi}(gh) = M_{S,\psi}(g)\text{Ih}_{S,\psi}(g)(M_{S,\psi}(h)). \]

2. For $g \in \text{Gal}_k$, we have

\[ M_{S,\psi}^{[m]}(g) = I + \psi(||_{\mathfrak{F}_r}^{[m]}(g)||). \]

3. The restriction of $M_{S,\psi}$ to $\text{Gal}_k[\psi]$, denoted by the same $M_{S,\psi}$,

\[ M_{S,\psi} : \text{Gal}_k[\psi] \to \text{GL}(r;\mathbb{Z}_l[[\mathfrak{G}]])/I_{\mathbb{Z}_l[[\mathfrak{G}]]}^{m+1} \]

43
is a homomorphism and factors through the Galois group $\text{Gal}(\Omega_S/k[\psi])$, where $\Omega_S$ is the subfield of $\overline{\mathbb{Q}}$ corresponding to $\text{Ker}(\text{Ih}_S)$ as in (1.2.4). We call it the pro-$l$ Magnus representation of $\text{Gal}_k[\psi]$ associated to $\text{Ih}_S$ and $\psi$.

Proof. (1) The formula is obtained by applying $\psi$ to the both sides of the formula in Lemma 4.2.2. (2) This is also obtained by applying $\psi$ to the matrices of the both sides of the formula in Proposition 4.2.4. (3) Suppose $g, h \in \text{Gal}_k$. Since $\psi \circ \text{Ih}_S(g) = \psi$, we have $\text{Ih}_{S,\psi}(g)(M_{S,\psi}(h)) = M_{S,\psi}(h)$ and so $M_{S,\psi}(gh) = M_{S,\psi}(g)M_{S,\psi}(h)$. Since $M_{S,\psi}(g) = I$ for $g \in \text{Ker}(\text{Ih}_S)$, we have $\text{Ker}(M_{S,\psi}) \supset \text{Ker}(\text{Ih}_S)$ and hence $M_{S,\psi}$ factors through $\text{Gal}(\Omega_S/k[\psi])$. □

For $n \geq 0$, let $\pi_n : \mathfrak{g}_r \to \mathfrak{g}_r/\mathfrak{g}_r(n+1)$ be the natural homomorphism. We consider the case that $\psi = \pi_n$ and so $\text{Ih}_{S,\psi} = \text{Ih}_S(n)$. By (3.3.1) and Lemma 3.3.3, we have

$$\text{Gal}_k[\pi_n] = \{g \in \text{Gal}_k \mid \pi_n \circ \text{Ih}_S(g) = \pi_n\} = \{g \in \text{Gal}_k \mid \text{Ih}_S(g)(f) \equiv f \mod \mathfrak{g}_r(n+1) \text{ for all } f \in \mathfrak{g}_r\} = \text{Gal}_k[n].$$

Then we have a family of pro-$l$ Magnus cocycles

$$(4.2.9) \quad M_{S,\pi_n} : \text{Gal}_k \to \text{GL}(r; \mathbb{Z}_l[[\mathfrak{g}_r/\mathfrak{g}_r(n+1)]]),$$

and the pro-$l$ Magnus representation

$$(4.2.10) \quad M_{S,\pi_n} : \text{Gal}_k[n] \to \text{GL}(r; \mathbb{Z}_l[[\mathfrak{g}_r/\mathfrak{g}_r(n+1)]]),$$

associated to $\text{Ih}_S$ and $\pi_n$ for $n \geq 0$.

4.3. Pro-$l$ Gassner cocycles. This subsection concerns the pro-$l$ (reduced) Gassner cocycles as special cases of the Magnus cocycles. For the construction of the pro-$l$ reduced Gassner cocycles, we follow Oda’s arguments [O2]. We also refer to [N; II] for Magnus-Gassner matrices.

The pro-$l$ Gassner cocycle is defined by $M_{S,\pi_1}$ in (4.2.9). To be precise, let $\Lambda_r := \mathbb{Z}_l[[u_1, \ldots, u_r]]$ denote the algebra of commutative formal power series over $\mathbb{Z}_l$ of variables $u_1, \ldots, u_r$, called the Iwasawa algebra of $r$ variables. The correspondence $x_i \mod \mathfrak{g}_r(2) \mapsto 1 + u_i (1 \leq i \leq r)$ gives the abelianized pro-$l$ Magnus isomorphism

$$\theta : \mathbb{Z}_l[[\mathfrak{g}_r/\mathfrak{g}_r(2)]] \xrightarrow{\sim} \Lambda_r.$$
We let $\pi := \pi_1$ and

\[(4.3.1) \quad \chi_{\Lambda_r} := \text{Ih}_S \circ \theta \circ \pi : \text{Gal}_k \to \text{Aut}(\Lambda_r),\]

which is defined by (4.2.4) with $\psi = \theta \circ \pi$. In fact, by Lemma 2.2.1, $\chi_{\Lambda_r}$ is given by

\[(4.3.2) \quad \chi_{\Lambda_r}(g)(u_i) = (\theta \circ \pi)(\text{Ih}_S(g)(x_i - 1)) = (1 + u_i)x_i(g) - 1 \quad (1 \leq i \leq r).\]

Then the pro-$l$ Gassner cocycle of $\text{Gal}_k$ associated to $\text{Ih}_S$ is defined by

\[(4.3.3) \quad \text{Gass}_S : \text{Gal}_k \to \text{GL}(r; \Lambda_r),\]

where we note that we do not need to take the anti-automorphism $-\bar{\chi}$ in (4.3.3) to obtain the 1-cocycle relation

$$\text{Gass}_S(gh) = \text{Gass}_S(g)\chi_{\Lambda_r}(g)(\text{Gass}_S(h)) \quad (g, h \in \text{Gal}_k),$$

since $\Lambda_r$ is commutative. Here $\chi_{\Lambda_r}(g)(\text{Gass}_S(h))$ is the matrix obtained by applying $\chi_{\Lambda_r}(g)$ to each entry of $\text{Gass}_S(h)$. We can express $\text{Gass}_S(g)$ in terms of $l$-adic Milnor numbers as follows.

**Proposition 4.3.4.** The $(i, j)$-entry of $\text{Gass}_S(g)$ ($g \in \text{Gal}_k$) is expressed by

$$\text{Gass}_S(g)_{ij} = \begin{cases} \frac{\chi_{\Lambda_r}(g)(u_i)}{u_i} \left(1 + \sum_{n \geq 1} \sum_{1 \leq i_1, \ldots, i_n \leq r} \mu(g; i_1 \cdot \cdot \cdot i_n i)u_{i_1} \cdot \cdot \cdot u_{i_n}\right) & (i = j), \\
-\chi_{\Lambda_r}(g)(u_j) \left(\mu(g; ij) + \sum_{n \geq 1} \sum_{1 \leq i_1, \ldots, i_n \leq r} \mu(g; i_1 \cdot \cdot \cdot i_n ij)u_{i_1} \cdot \cdot \cdot u_{i_n}\right) & (i \neq j). \end{cases}$$

**Proof.** By Lemma 2.2.1 and a straightforward computation, we have

$$\frac{\partial \text{Ih}_S(g)(x_j)}{\partial x_i} = \frac{\partial y_j(g)x_j^{\chi(g)}y_j(g)^{-1}}{y_j(g)x_j^{\chi(g)}y_j(g)^{-1}} \frac{\partial x_j}{\partial x_i},$$

$$= y_j(g)x_j^{\chi(g)}\frac{1}{x_j - 1}\delta_{ij} + (1 - y_j(g)x_j^{\chi(g)}y_j(g)^{-1}) \frac{\partial y_j(g)}{\partial x_i}.$$
and hence, by (4.3.2),

\[(4.3.4.1)\]

\[
(\theta \circ \pi) \left( \frac{\partial I_{S}(g)(x_j)}{\partial x_i} \right) = (\theta \circ \pi)(y_j(g)) \frac{(1 + u_j)\chi_{I}(g) - 1}{u_j} \delta_{ij} + (1 - (1 + u_j)\chi_{I}(g))(\theta \circ \pi) \left( \frac{\partial y_j(g)}{\partial x_i} \right)
\]

\[
= \frac{\chi_{\Lambda_{r}}(g)(u_j)}{u_j} (\theta \circ \pi)(y_j(g))\delta_{ij} - \chi_{\Lambda_{r}}(g)(u_j)(\theta \circ \pi) \left( \frac{\partial y_j(g)}{\partial x_i} \right).
\]

Here we have

\[(4.3.4.2)\]

\[
(\theta \circ \pi)(y_j(g)) = 1 + \sum_{|I| \geq 1} \mu(g; I)u_I,
\]

where we set \(u_I := u_{i_1} \cdots u_{i_n}\) for \(I = (i_1 \cdots i_n)\), and (4.1.1) yields

\[(4.3.4.3)\]

\[
(\theta \circ \pi) \left( \frac{\partial y_j(g)}{\partial x_i} \right) = \sum_{|I| \geq 0} \mu(g; I)u_I.
\]

By (4.3.3), (4.3.4.1), (4.3.4.2) and (4.3.4.3), we have

\[
G_{S}(g) = (\theta \circ \pi) \left( \frac{\partial I_{S}(g)(x_j)}{\partial x_i} \right) = \delta_{ij} \frac{\chi_{\Lambda_{r}}(g)(u_j)}{u_j} \left( 1 + \sum_{|I| \geq 1} \mu(g; I)u_I \right) - \chi_{\Lambda_{r}}(g)(u_j) \sum_{|I| \geq 0} \mu(g; I)u_I.
\]

By \(\mu(g; ii) = 0\) and a simple observation, we obtain the assertion. \(\square\)

By (4.2.10), when \(G_{S}\) is restricted to \(\text{Gal}_{k}[1]\), we have a representation

\[
G_{S} : \text{Gal}_{k}[1] \rightarrow \text{GL}_{r}(\Lambda_{r}),
\]

which we call the \textit{pro-l Gassner representation} of \(\text{Gal}_{k}[1]\) associated to \(I_{S}\).

It factors through the Galois group \(\text{Gal}(\Omega_{S}/k[1])\) by Theorem 4.2.8 (3).

In the following, for simplicity, we let

\[
\mathfrak{z}'_{r} := \mathfrak{z}_{r}(2), \mathfrak{z}''_{r} := [\mathfrak{z}'_{r}, \mathfrak{z}'_{r}], \text{ and } \mathcal{L}_{r} := \mathfrak{z}'_{r}/\mathfrak{z}''_{r} = H_{1}(\mathfrak{z}'_{r}, \mathbb{Z}_{4}).
\]
We consider $\mathcal{L}$ as a $\Lambda_r$-module by conjugation: For $f \in \mathfrak{F}_r$ and $f' \in \mathfrak{F}'_r$, we set 
\[ [f].(f' \mod \mathfrak{F}'') := ff'f^{-1} \mod \mathfrak{F}''. \]
and extend it by the $\mathbb{Z}_l$-linearity and continuity. The structure of the $\Lambda_r$-module $\mathcal{L}_r$ can be described by means of the pro-$l$ Crowell exact sequence ([Ms2: Chapter 9]). Attached to the surjective homomorphism $\pi : \mathfrak{F}_r \twoheadrightarrow \mathfrak{F}_r/\mathfrak{F}'_r$, the pro-$l$ Crowell exact sequence reads as the exact sequence of $\Lambda_r$-modules:
\[ 0 \longrightarrow \mathcal{L}_r \overset{\nu_1}{\longrightarrow} \Lambda^\oplus_r \overset{\nu_2}{\longrightarrow} I_{\Lambda_r} \longrightarrow 0, \]
where $I_{\Lambda_r}$ is the (augmentation) ideal of $\Lambda_r$ generated by $u_1, \ldots, u_r$ and $\nu_1, \nu_2$ are $\Lambda_r$-homomorphisms defined by
\[ (4.3.5) \quad \nu_1(f' \mod \mathfrak{F}'') := ((\theta \circ \pi) \left( \frac{\partial f'}{\partial x_i} \right)) \quad (f' \in \mathfrak{F}'_r); \quad \nu_2((\lambda_i)) := \sum_{i=1}^r \lambda_i u_i. \]
(Convention: An element $(\lambda_i)$ of $\Lambda^\oplus_r$ is understood as a column vector.) Hence we have the isomorphism of $\Lambda_r$-modules induced by $\nu_1$, called the Blanchfield-Lyndon isomorphism:
\[ (4.3.6) \quad \nu_1 : \mathcal{L}_r \overset{\sim}{\longrightarrow} \{ (\lambda_i) \in \Lambda^\oplus_r \mid \sum_{i=1}^r \lambda_i u_i = 0 \}. \]

We define the action $\text{Meta}_S$ of $\text{Gal}_k$ on $\mathcal{L}_r$ through the Ihara representation $\text{Ih}_S$: For $g \in \text{Gal}_k$ and $f' \in \mathfrak{F}'_r$,
\[ \text{Meta}_S(g)(f' \mod \mathfrak{F}'') := \text{Ih}_S(g)(f') \mod \mathfrak{F}''. \]
It is easy to see that $\text{Meta}_S(g)$ is a $\chi_{\Lambda_r}$-linear automorphism of $\mathcal{L}_r$, namely, a $\mathbb{Z}_l$-linear automorphism and satisfies
\[ \text{Meta}_S(g)(\lambda(f' \mod \mathfrak{F}'')) = \chi_{\Lambda_r}(g)(\lambda)(f' \mod \mathfrak{F}'') \]
for $\lambda \in \Lambda_r$ and $f' \in \mathfrak{F}'_r$. When $\text{Meta}_S$ is restricted to $\text{Gal}_k[1]$, we have the representation, which we call the pro-$l$ meta-abelian representation of $\text{Gal}_k[1]$ associated to $\text{Ih}_S$,
\[ \text{Meta}_S : \text{Gal}_k[1] \longrightarrow \text{GL}_{\Lambda_r}(\mathcal{L}_r), \]
where $\text{GL}_{\Lambda_r}(\mathcal{L}_r)$ is the group of $\Lambda_r$-module automorphisms of $\mathcal{L}_r$. Regarding $\mathcal{L}_r$ as a $\Lambda_r$-submodule of $\Lambda^\oplus_r$ by the isomorphism (4.3.6), $\text{Meta}_S$ and $\text{Gass}_S$
Proposition 4.3.7. For \( g \in \text{Gal}_k \) and \( f' \in \mathfrak{F}'_r \), we have

\[
(\nu_1 \circ \text{Meta}_S(g))(f' \mod \mathfrak{F}'_r) = \text{Gass}_S(g)(\chi_{\Lambda_r}(g) \circ \nu_1)(f' \mod \mathfrak{F}'_r).
\]

When \( \text{Meta}_S \) and \( \text{Gass}_S|_{\mathfrak{L}_r} \) are restricted to \( \text{Gal}_k[1] \), they are equivalent representations over \( \Lambda_r \).

Proof. The first assertion follows from the direct computation: By (4.3.1), (4.3.3) and (4.3.5), we have, for any \( g \in \text{Gal}_k \) and \( f' \in \mathfrak{F}'_r \),

\[
(\nu_1 \circ \text{Meta}_S(g))(f' \mod \mathfrak{F}'_r) = \nu_1(\text{Ih}_S(g)(f') \mod \mathfrak{F}'_r) \\
= ((\theta \circ \pi) \left( \frac{\partial \text{Ih}_S(g)(f')}{\partial x_i} \right)) \\
= ((\theta \circ \pi) \left( \sum_{a=1}^{r} \frac{\partial \text{Ih}_S(g)(f') \partial \text{Ih}_S(g)(x_a)}{\partial x_i} \right)) \\
= \left( \sum_{a=1}^{r} (\theta \circ \pi) \left( \frac{\partial \text{Ih}_S(g)(x_a)}{\partial x_i} \right) \right) (\theta \circ \pi \circ \text{Ih}_S(g))(\frac{\partial f'}{\partial x_a}) \\
= \text{Gass}_S(g)\chi_{\Lambda_r}(g)(\nu_1(f' \mod \mathfrak{F}'_r)).
\]

When \( \text{Meta}_S \) and \( \text{Gass}_S \) are restricted to \( \text{Gal}_k[1] \), by the first assertion, we have the commutative diagram of \( \Lambda_r \)-modules for any \( g \in \text{Gal}_k[1] \):

\[
\begin{array}{ccc}
\mathfrak{L}_r & \xrightarrow{\nu_1} & \Lambda_r^{\oplus r} \\
\text{Meta}_S(g) \downarrow & & \downarrow \text{Gass}_S(g) \\
\mathfrak{L}_r & \xrightarrow{\nu_1} & \Lambda_r^{\oplus r},
\end{array}
\]

from which the latter assertion follows. \( \Box \)

Next, we introduce the pro-\( l \) reduced Gassner cocycle associated to the Ihara representation \( \text{Ih}_S \). For this, we follow Oda’s arguments ([O2]). We first define a certain \( \Lambda_r \)-submodule \( \mathfrak{L}_r^{\text{prim}} \) of \( \mathfrak{L}_r \), which Oda calls the primitive part of \( \mathfrak{L}_r \), as follows. For \( 1 \leq i \leq r \), let \( \mathfrak{N}_i \) be the closed subgroup generated normally by \( x_i \) and let \( \mathfrak{F}^{(i)}_r := \mathfrak{F}_r/\mathfrak{N}_i \). Let \( \Lambda_r^{(i)} := \mathbb{Z}[[u_1, \ldots, \hat{u}_i, \ldots, u_r]] \simeq \mathbb{Z}[[\mathfrak{F}^{(i)}_r/(\mathfrak{F}^{(i)}_r)]] \) (\( \hat{u}_i \) means deleting \( u_i \)) with augmentation ideal \( I_{\Lambda_r^{(i)}} \), and let \( \delta_i : \Lambda_r \to \Lambda_r^{(i)} \) be the \( \mathbb{Z}_l \)-algebra homomorphism defined by \( \delta_i(u_j) := u_j \).
if $j \neq i$ and $\delta_i(u_i) := 0$. Note that any $\Lambda_r^{(i)}$-module is regarded as a $\Lambda_r$-module via $\delta_i$. Let $L_r^{(i)} := (\mathfrak{g}_r^{(i)})'/(\mathfrak{g}_r^{(i)})''$ and let $\xi_i : L_r \to L_r^{(i)}$ be the $\Lambda_r$-homomorphism induced by the natural homomorphism $\mathfrak{g}_r \to \mathfrak{g}_r^{(i)}$. Then the primitive part $L_r^{\text{prim}}$ of $L_r$ is defined by

\[(4.3.8) \quad L_r^{\text{prim}} := \bigcap_{i=1}^r \ker(\xi_i).\]

We set $w := u_1 \cdots u_r$. The following theorem and the proof are due to Oda.

**Theorem 4.3.9 ([O2]).** Notations being as above, the following assertions hold.

(1) The Blanchfield-Lyndon isomorphism $\nu_1$ in (4.3.6) restricted to $L_r^{\text{prim}}$ induces the following isomorphism of $\Lambda_r$-modules

$$L_r^{\text{prim}} \simeq \{ (\lambda_j w) \in \Lambda_r^{\oplus r} \mid \lambda_j \in \Lambda_r, \sum_{j=1}^r \lambda_j = 0 \}.$$ 

In particular, $L_r^{\text{prim}}$ is the free $\Lambda_r$-module of rank $r - 1$ on the basis

$$v_1 := t\left(\frac{w}{u_1}, \frac{w}{u_2}, 0, \ldots, 0\right), \ldots, v_{r-1} := t(0, \ldots, 0, -\frac{w}{u_{r-1}}, \frac{w}{u_r}).$$

(2) $L_r^{\text{prim}}$ is stable under the action of $\text{Gal}_k$ through $\text{Meta}_S$ and defines 1-cocycle $\text{Gass}_S^{\text{red}} : \text{Gal}_k \to \text{GL}_{r-1}(\Lambda_r)$ with respect to the basis $v_1, \ldots, v_{r-1}$ and the action $\chi_{\Lambda_r}$ in (4.3.1). We call $\text{Gass}_S^{\text{red}}$ the pro-$l$ reduced Gassner cocycle of $\text{Gal}_k$ associated to $\text{Ih}_S$.

**Proof.** (1) We define the $\Lambda_r$-homomorphism $\tilde{\xi}_i : \Lambda_r^{\oplus r} \to (\Lambda_r^{(i)})^{\oplus (r-1)}$ by

$$\tilde{\xi}_i(t(\lambda_1, \ldots, \lambda_r)) := t(\delta_i(\lambda_1), \ldots, \delta_i(\lambda_{i-1}), \delta_i(\lambda_{i+1}), \ldots, \delta_i(\lambda_r)).$$

Then we have $\xi_i = \tilde{\xi}_i|_{L_r}$ for $1 \leq i \leq r$ and the commutative diagram of $\Lambda_r$-modules:

$$
\begin{array}{cccccc}
0 & \longrightarrow & L_r & \longrightarrow & \Lambda_r^{\oplus r} & \longrightarrow & I_{\Lambda_r} & \longrightarrow & 0 \\
\downarrow \xi_i & & \downarrow \tilde{\xi}_i & & \downarrow \delta_i & & \downarrow \delta_i & & \\
0 & \longrightarrow & L_r^{(i)} & \longrightarrow & (\Lambda_r^{(i)})^{\oplus (r-1)} & \longrightarrow & I_{\Lambda_r^{(i)}} & \longrightarrow & 0,
\end{array}
$$

49
where two rows are the pro-\(l\) Crowell exact sequences. It is easy to see that \(\text{Ker}(\tilde{\xi}_i)\) is given by

\[
\text{Ker}(\tilde{\xi}_i) = \{ (\lambda_1 u_i, \ldots, \lambda_{i-1} u_i, \lambda_i, \lambda_{i+1} u_i, \ldots, \lambda_r u_i) \mid \lambda_j \in \Lambda_r \ (1 \leq j \leq r) \}
\]

and hence, by (4.3.6) and (4.3.8), we have

\[
\mathfrak{L}_r^{\text{prim}} = \{ (\lambda_j) \in \Lambda_r^{\oplus r} \mid \sum_{j=1}^{r} \lambda_j u_j = 0, \lambda_j \equiv 0 \mod u_i \text{ if } i \neq j \}.
\]

Since \(\Lambda_r\) is a regular local ring, it is factorial. Therefore we have the first assertion

\[
\mathfrak{L}_r^{\text{prim}} = \{ (\lambda_j) \in \Lambda_r^{\oplus r} \mid \sum_{j=1}^{r} \lambda_j u_j = 0, \lambda_j \equiv 0 \mod \frac{w}{u_j} (1 \leq j \leq r) \}.
\]

The assertion for a basis of \(\mathfrak{L}_r^{\text{prim}}\) is clear.

(2) Since \(\text{Ih}_S(g)(x_i)\) is conjugate to \(x_i^{\chi(g)}\) for \(g \in \text{Gal}_k\) and \(1 \leq i \leq r\), the definition (4.3.8) implies that \(\mathfrak{L}_r^{\text{prim}}\) is \(\text{Gal}_k\)-stable under the action \(\text{Meta}_S\).

So we may write, for \(1 \leq j \leq r - 1\),

\[
(4.3.9.1) \quad \text{Ih}_S(g)(v_j) = \sum_{i=1}^{r-1} \text{Gass}_S^{\text{red}}(g)_{ij} v_i,
\]

where \(\text{Gass}_S^{\text{red}}(g)_{ij} \in \Lambda_r\) is the \((i, j)\)-entry of the representation matrix of \(\text{Ih}_S(g)\) with respect to \(v_1, \ldots, v_{r-1}\). Then we have, for \(g, h \in \text{Gal}_k\),

\[
\text{Ih}_S(gh)(v_j) = \text{Ih}_S(g)(\text{Ih}_S(h)(v_j))
\]

\[
= \text{Ih}_S(g) \left( \sum_{i=1}^{r-1} \text{Gass}_S^{\text{red}}(h)_{ij} v_i \right)
\]

\[
= \sum_{i=1}^{r-1} \chi_{\Lambda_r}(\text{Gass}_S^{\text{red}}(h)_{ij}) \text{Ih}_S(g)(v_i) \quad \text{(by (4.3.1))}
\]

\[
= \sum_{t=1}^{r-1} \left( \sum_{i=1}^{r-1} \text{Gass}_S^{\text{red}}(g)_{ti} \chi_{\Lambda_r}(g)(\text{Gass}_S^{\text{red}}(h)_{ij}) \right) v_t,
\]

which means the cocycle relation

\[
\text{Gass}_S^{\text{red}}(gh) = \text{Gass}_S^{\text{red}}(g) \chi_{\Lambda_r}(g)(\text{Gass}_S^{\text{red}}(h)).
\]
Hence the assertion is proved. □

When we restrict $\text{Gass}_S^{\text{red}}$ to $\text{Gal}_k[1]$, we have a representation

$$\text{Gass}_S^{\text{red}} : \text{Gal}_k[1] \rightarrow \text{GL}(r - 1; \Lambda),$$

which we call the *pro-$l$ reduced Gassner representation* of $\text{Gal}[1]$ associated to $\text{Ih}_S$.

Let $\Gamma$ be a free pro-$l$ group of rank 1 generated by $x$ so that $\mathbb{Z}_l[[\Gamma]]$ is identified with the Iwasawa algebra $\Lambda := \mathbb{Z}_l[[u]]$ ($x \leftrightarrow 1 + u$). Let $\hat{\mathfrak{g}} : \mathbb{F}_r \rightarrow \Gamma$ be the homomorphism defined by $\hat{\mathfrak{g}}(x_i) := x$ for $1 \leq i \leq r$. Let $\chi_{\Lambda}$ be the action of $\text{Gal}_k$ on $\Lambda$ defined by $\chi_{\Lambda}(g)(u) := (1 + u)^{\chi_l(g)} - 1$ for $g \in \text{Gal}_k$ Then we have the pro-$l$ Magnus cocycle associated to $\text{Ih}_S$ and $\hat{\mathfrak{g}}$

$$\text{Bur}_S : \text{Gal}_k \rightarrow \text{GL}(r; \Lambda),$$

which we call the *pro-$l$ Burau cocycle* of $\text{Gal}_k$ associated to $\text{Ih}_S$. It is the 1-cocycle of $\text{Gal}_k$ with coefficients in $\text{GL}(r; \Lambda)$ with respect to the action $\chi_{\Lambda}$. By definition, we have

$$\text{Bur}_S(g) = \text{Gass}_S(g)|_{u_1 = \cdots = u_r = u}.$$  

Similarly, we have the *pro-$l$ reduced Burau cocycle* associated to $\text{Ih}_S$

$$\text{Bur}_S^{\text{red}} : \text{Gal}_k \rightarrow \text{GL}(r - 1; \Lambda)$$

defined by

$$\text{Bur}_S^{\text{red}}(g) := \text{Gass}_S^{\text{red}}(g)|_{u_1 = \cdots = u_r = u}.$$  

Since $(\hat{\mathfrak{g}} \circ \text{Ih}_S(g))(x_i) = \hat{\mathfrak{g}}(y_i(g)x_iy_i(g)^{-1}) = \hat{\mathfrak{g}}(x_i)$ for $g \in \text{Gal}_k[1]$, we have

$$\hat{\mathfrak{g}} \circ \text{Ih}_S(g) = \hat{\mathfrak{g}} (g \in \text{Gal}_k[1]).$$

So, when we restrict $\text{Bur}_S$ and $\text{Bur}_S^{\text{red}}$ to $\text{Gal}_k[1]$, we have representations

$$\text{Bur}_S : \text{Gal}_k[1] \rightarrow \text{GL}_r(\Lambda), \quad \text{Bur}_S^{\text{red}} : \text{Gal}_k[1] \rightarrow \text{GL}_{r-1}(\Lambda),$$

which are called the *pro-$l$ Burau representation* and the *pro-$l$ reduced Burau representation* of $\text{Gal}_k[1]$ associated to $\text{Ih}_S$, respectively.
5. \textit{l}-adic Alexander invariants

5.1. \textit{Pro-}l link modules. Let $g \in \text{Gal}_k$. As in (2.3.1), let $\Pi_S(g)$ be the pro-$l$ link group of $g$ associated to the Ihara representation $Ih_S$:

$$\Pi_S(g) = \langle x_1, \ldots, x_r \mid y_1(g)x_1^{\chi(g)}y_1(g)^{-1}x_1^{-1} = \cdots = y_r(g)x_r^{\chi(g)}y_r(g)^{-1}x_r^{-1} = 1 \rangle = \mathfrak{H}/\mathfrak{N}_S(g),$$

where $\mathfrak{N}_S(g)$ is the closed subgroup of $\mathfrak{H}$ generated normally by the pro-$l$ words $y_1(g)x_1^{\chi(g)}y_1(g)^{-1}x_1^{-1}, \ldots, y_r(g)x_r^{\chi(g)}y_r(g)^{-1}x_r^{-1}$. Let $\psi : \mathfrak{H} \to \Pi_S(g)$ be the natural homomorphism and let $\gamma_i := \psi(x_i) (1 \leq i \leq r)$. Recall that $a(g)$ denotes the ideal of $\mathbb{Z}_l$ generated by $\chi_i(g) - 1$. Then we have

$$\Pi_S(g)/\Pi_S(g)' = \mathbb{Z}_l/a(g)[\gamma_1] \oplus \cdots \oplus \mathbb{Z}_l/a(g)[\gamma_r] \approx (\mathbb{Z}_l/a(g))^\oplus r,$$

where $[\gamma_i] := \gamma_i \bmod \Pi_S(g)' (1 \leq i \leq r)$. The correspondence $\gamma_i \mapsto u_i$ induces the $\mathbb{Z}_l$-algebra isomorphism

$$\theta(g) : \mathbb{Z}_l[[(\Pi_S(g)/\Pi_S(g)')]] \approx \Lambda_r/((1 + u_1)^{\chi(g)-1} - 1, \ldots, (1 + u_r)^{\chi(g)-1} - 1).$$

We denote the right hand side by $\Lambda_r(g)$:

$$\Lambda_r(g) := \Lambda_r/((1 + u_1)^{\chi(g)-1} - 1, \ldots, (1 + u_r)^{\chi(g)-1} - 1),$$

and by $I_{\Lambda_r(g)}$ the augmentation ideal of $\Lambda_r(g)$.

We define the \textit{pro-$l$ link module} $\mathcal{L}_S(g)$ of $g$ associated to $Ih_S$ by

$$\mathcal{L}_S(g) := \Pi_S(g)''/\Pi_S(g)'', $$

which is considered as a $\Lambda_r(g) = \mathbb{Z}_l[[(\Pi_S(g)/\Pi_S(g)')]]$-module. It may be seen as an analogue of the classical link module in link theory (cf. [Hi], [Ms2, Chapter 9]).

Let $\varpi : \Pi_S(g) \to \Pi_S(g)/\Pi_S(g)'$ be the abelianization map. We define the \textit{pro-$l$ Alexander module} $\mathfrak{A}_S(g)$ of $g$ associated to $Ih_S$ by the \textit{pro-$l$ differential module} associated to $\varpi$, namely the quotient module of the free $\Lambda_r(g)$-module on symbols $d\gamma$ for $\gamma \in \Pi_S(g)$ by the $\Lambda_r(g)$-submodule generated by $d(\gamma_1\gamma_2) - d\gamma_1 - \varpi(\gamma_1)d\gamma_2$ for $\gamma_1, \gamma_2 \in \Pi_S(g)$ ([Ms; 9.3]):

$$\mathfrak{A}_S(g) := \bigoplus_{\gamma \in \Pi_S(g)} \Lambda_r(g)d\gamma/\langle d(\gamma_1\gamma_2) - d\gamma_1 - \varpi(\gamma_1)d\gamma_2 \mid \gamma_1, \gamma_2 \in \Pi_S(g) \rangle_{\Lambda_r(g)}.$$
We define the $l$-adic Alexander matrix $Q_S(g)$ by the Jacobian matrix of the relators of $\Pi_S(g)$:

\[(5.1.1) \quad Q_S(g) := \left( (\theta(g) \circ \varpi \circ \psi) \left( \frac{\partial y_j(g)x_j^{\chi_i(g)}y_j(g)x_j^{-1}}{\partial x_i} \right) \right). \]

**Proposition 5.1.2.** Notations being as above, the following assertions hold.

1. The correspondence $d\gamma \mapsto (\theta(g) \circ \varpi \circ \psi) \left( \frac{\partial f}{\partial x_i} \right)$ gives the isomorphism

\[\mathfrak{A}_S(g) \cong \text{Coker}(Q_S(g) : \Lambda_r(g) \to \Lambda_r(g)),\]

where $f$ is any element of $\mathfrak{g}_r$ such that $\gamma = \varpi(f)$.

2. (Pro-$l$ Crowell exact sequence) We have the following exact sequence of $\Lambda_r(g)$-modules:

\[0 \to \mathfrak{L}_S(g) \xrightarrow{\nu_1} \mathfrak{A}_S(g) \xrightarrow{\nu_2} I_{\Lambda_r(g)} \to 0,\]

where $\nu_1, \nu_2$ are given by

\[\nu_1(\gamma' \mod \Pi_S(g)) := d\gamma (\gamma' \in \Pi_S(g)); \quad \nu_2(d\gamma) := (\theta(g) \circ \varpi)(\gamma) - 1 (\gamma \in \Pi_S(g)).\]

**Proof.** We refer to [Ms2; Theorems 9.3.6, 9.4.2].

Let $\phi_g : \Lambda_r \to \Lambda_r(g)$ be the natural $\mathbb{Z}_l$-algebra homomorphism.

**Proposition 5.1.3.** We have

\[Q_S(g) = \phi_g(Gass_S(g) - I)\]

and its $(i,j)$-entry is given by

\[Q_S(g)_{ij} = \begin{cases} 
\phi_g \left( \sum_{n \geq 1} \sum_{1 \leq i_1, \ldots, i_n \leq r} \mu(g; i_1 \cdots i_n)u_{i_1} \cdots u_{i_n} \right) & (i = j), \\
\phi_g \left( -u_j \left( \mu(g; ij) + \sum_{n \geq 1} \sum_{1 \leq i_1, \ldots, i_n \leq r} \mu(g; i_1 \cdots i_n u_j)u_{i_1} \cdots u_{i_n} \right) \right) & (i \neq j). 
\end{cases} \]
Proof. By the definition (5.1.1), we have

$$Q_S(g)_{ij} := (\theta(g) \circ \varpi \circ \psi) \left( \frac{\partial y_j(g)x_j^x(g)y_j(g)^{-1}x_j^{-1}}{\partial x_i} \right).$$

By the basic rules of pro-$l$ Fox free derivatives, we have

$$\frac{\partial y_j(g)x_j^x(g)y_j(g)^{-1}x_j^{-1}}{\partial x_i} = \frac{\partial y_j(g)x_j^x(g)y_j(g)^{-1}}{\partial x_i} - \delta_{ij} y_j(g)x_j^x(g)y_j(g)^{-1}x_j^{-1}.$$ 

By (4.3.3) and $\theta(g) \circ \varpi \circ \psi = \phi g \circ \theta \circ \pi$, we have

$$(\theta(g) \circ \varpi \circ \psi) \left( \frac{\partial y_j(g)x_j^x(g)y_j(g)^{-1}x_j^{-1}}{\partial x_i} \right) = \phi g(\text{Gass}_S(g)_{ij}),$$

and we also have

$$(\theta(g) \circ \varpi \circ \psi)(y_j(g)x_j^x(g)y_j(g)^{-1}x_j^{-1}) = \theta(g)(\gamma_j^x(g)^{-1}) = (1 + u_j)^{\chi_j(g)} = 1.$$ 

Therefore we have

$$Q_S(g)_{ij} = \phi g(\text{Gass}_S(g)_{ij} - \delta_{ij}).$$

The second assertion follows from Proposition 4.3.4 and

$$\phi g(\chi_{\Lambda_r}(g)(u_j)) = \phi g((1 + u_j)^{\chi_j(g)} - 1) = \phi g(u_j).$$ 

\square

Corollary 5.1.4. For $g, h \in \text{Gal}_k[1]$, we have the following isomorphisms of $\Lambda_r$-modules

$$\mathfrak{A}_S(ghh^{-1}) \simeq \mathfrak{A}_S(g), \quad \mathfrak{L}_S(ghh^{-1}) \simeq \mathfrak{L}_S(h).$$

Proof. Since $\text{Gass}_S : \text{Gal}_k \rightarrow \text{GL}(r; \Lambda_r)$ is a representation, we have

$$Q_S(ghh^{-1}) = \phi g(\text{Gass}_S(ghh^{-1}) - I) = \phi g(\text{Gass}_S(h))Q_S(g)\phi g(\text{Gass}_S(h))^{-1}$$

by Proposition 5.1.3. Then the first assertion follows from Proposition 5.1.2 (1). The second assertion follows from Proposition 5.1.2 (2). \square

5.2. $l$-adic Alexander invariants. For $n \geq 0$, we define the $n$-th $l$-adic Alexander ideal $\mathfrak{C}_S(g)^{(n)}$ of $g \in \text{Gal}_k$ associated to $\text{Ih}_S$ by the $n$-th Fitting ideal of the pro-$l$ Alexander module $\mathfrak{A}_S(g)$ over $\Lambda_r(g)$. The $n$-th $l$-adic
Alexander invariant $A_S(g) \langle n \rangle$ is then defined by a generator of the divisorial hull of $E_S(g) \langle n \rangle$. By Proposition 5.1.2 (1), $E_S(g) \langle n \rangle$ is the ideal generated by all $(r - n)$-minors of $Q_S(g)$ if $r - n > 0$ and $E_S(g) \langle n \rangle := \Lambda_r(g)$ if $r - n \leq 0$, and $A_S(g) \langle n \rangle$ is the greatest common divisor of all $(r - n)$-minors of $Q_S(g)$ if $r - n > 0$ and $A_S(g) \langle n \rangle := 1$ if $r - n \leq 0$:

$$A_S(g) \langle n \rangle := \begin{cases} \text{g.c.d of all $(r - n)$-minors of } Q_S(g) & (r - n > 0), \\ 1 & (r - n \leq 0). \end{cases}$$

We note that $A_S(g) \langle n \rangle$ is defined up to multiplication of a unit of $\Lambda_r(g)$. We write $E_S(g)$ (resp. $A_S(g)$) for $E_S(g) \langle 0 \rangle$ (resp. $A_S(g) \langle 0 \rangle$) and call $E_S(g)$ (resp. $A_S(g)$) the $l$-adic Alexander ideal (resp. $l$-adic Alexander invariant) of $g$ associated to $Ih_S$. From Proposition 5.1.3, the following proposition is immediate.

**Proposition 5.2.1.** For $g \in \text{Gal}_k$, we have

$$A_S(g) = \phi_g(\det(Gass_S(g) - I)).$$

When $g \in \text{Gal}_k[1]$, $A_S(g) = 0$ if and only if $Gass_S(g)$ has the eigenvalue 1.

Moreover, since the $l$-adic Alexander matrix $Q_S(g)$ is described by $l$-adic Milnor numbers as in Proposition 5.1.3, $n$-th $l$-adic Alexander invariants are also described by $l$-adic Milnor numbers (cf. [Ms2; Chapter 10], [Mu]).

### 6. The Ihara power series

In this section, we suppose that $S = \{0, 1, \infty\}$ and so $k = \mathbb{Q}$. In the following, we will omit $S$ in the notations. The Ihara representation in this case is

$$Ih : \text{Gal}_\mathbb{Q} \rightarrow P(\mathfrak{S}_2),$$

which factors through the Galois group $\text{Gal}(\Omega_l/\mathbb{Q})$ by Theorem 1.2.6 (2), where $\Omega_l$ denotes the maximal pro-$l$ extension of $\mathbb{Q}[1] = \mathbb{Q}(\zeta_{\infty})$ unramified outside $l$.

**6.1. The Ihara power series.** The following lemma is a restatement of [Ih1; Theorem 2 (i)]. See also [Ih2; §1 (D) Example 2]. For the sake of readers, we give a proof using Theorem 4.3.9.
Lemma 6.1.1. We have $\mathcal{L}_2 = \mathcal{L}_2^\text{prim}$ with basis $t(-u_2, u_1)$ over $\Lambda_2$, and $t(-u_2, u_1) = \nu_1([x_1, x_2])$.

Proof. By Theorem 4.3.9 (1), $\mathcal{L}_2^\text{prim}$ is the free $\Lambda_2$-module with basis $t(-u_2, u_1)$. On the other hand, we note that $\lambda_1 u_1 + \lambda_2 u_2 = 0$ implies $\lambda_1 = -a u_2, \lambda_2 = a u_1$ for some $a \in \Lambda_2$, because $\Lambda_2$ is U.F.D. Therefore $\mathcal{L}_2$ is also the free $\Lambda_2$-module with basis $t(-u_2, u_1)$ by (4.3.6). Hence $\mathcal{L}_2 = \mathcal{L}_2^\text{prim}$. The second assertion follows from

$$(\theta \circ \pi) \left( \frac{\partial [x_1, x_2]}{\partial x_1} \right) = -u_2, \ (\theta \circ \pi) \left( \frac{\partial [x_1, x_2]}{\partial x_2} \right) = u_1. \ \Box$$

Thanks to Lemma 6.1.1, Ihara introduced a power series $F_g(u_1, u_2) \in \Lambda_2$, called the Ihara power series, by the following equality in $\mathcal{L}_2$

\begin{equation}
\text{Ih}_2(g)([x_1, x_2]) \equiv F_g(u_1, u_2)[x_1, x_2] \mod \mathfrak{F}_2''.
\end{equation}

The following theorem gives an arithmetic topological interpretation of the Ihara power series $F_g(u_1, u_2)$. For a multi-index $I = (i_1 \cdots i_n)$ with $i_j = 1$ or 2, we denote by $|I|_1$ (resp. $|I|_2$) the number of $j$'s ($1 \leq j \leq n$) such that $i_j = 1$ (resp. $i_j = 2$). For integers $n_1, n_2 \geq 0$ with $n_1 + n_2 \geq 1$ and $g \in \text{Gal}_Q$, we let

$$\mu(g; n_1, n_2) := \sum_{|I|_1 = n_1 - 1, |I|_2 = n_2} \mu(g; I12) + \sum_{|I|_1 = n_1, |I|_2 = n_2 - 1} \mu(g; I21).$$

We recall the pro-$l$ Gassner and the pro-$l$ reduced Gassner cocycles in (4.3.3) and (4.3.9.1):

\[\text{Gass}: \text{Gal}_Q \rightarrow \text{GL}(2; \Lambda_2); \ \text{Gass}^\text{red}: \text{Gal}_Q \rightarrow \Lambda_2^\times.\]

Theorem 6.1.3. Notations being as above, we have, for $g \in \text{Gal}_Q$,

$$F_g(u_1, u_2) = \text{Gass}^\text{red}(g) \frac{\chi_{\Lambda_2}(g)(u_1 u_2)}{u_1 u_2} \left( 1 + \sum_{n \geq 1} \sum_{1 \leq i_1, \ldots, i_n \leq 2 \atop i_n \neq i_{n+1}} \mu(g; i_1 \cdots i_n i_{n+1}) u_{i_1} \cdots u_{i_n} \right)$$

$$= \chi_{\Lambda_2}(g)(u_1 u_2) \frac{1 + \sum_{n_1, n_2 \geq 0 \atop n_1 + n_2 \geq 1} \mu(g; n_1, n_2) u_1^{n_1} u_2^{n_2}}{u_1 u_2}.$$
Proof. Applying the $\Lambda_2$-homomorphism $\nu_1$ to (6.1.2), we have, for $g \in \text{Gal}_k$,

$$\nu_1(\text{Ih}(g)([x_1, x_2])) = F_g(u_1, u_2)\nu_1([x_1, x_2]) = F_g(u_1, u_2) \left( \frac{-u_2}{u_1} \right).$$

On the other hand, by the definition of $\text{Gass}^{\text{red}}(g)$ (cf. (4.3.9.1)), we have

$$\nu_1(\text{Ih}(g)([x_1, x_2])) = \text{Gass}^{\text{red}}(g)\left( \frac{-u_2}{u_1} \right).$$

Hence we have

$$F_g(u_1, u_2) = \text{Gass}^{\text{red}}(g).$$

By Proposition 4.3.7 and Lemma 6.1.1, we have

$$\nu_1(\text{Ih}(g)([x_1, x_2])) = \text{Gass}(g)\chi_{\Lambda_2}(g)\nu_1([x_1, x_2]) = \text{Gass}(g)\left( \frac{-\chi_{\Lambda_2}(g)(u_2)}{\chi_{\Lambda_2}(g)(u_1)} \right).$$

A straightforward calculation using Proposition 4.3.4 yields

$$\text{Gass}(g)\left( \frac{-\chi_{\Lambda_2}(g)(u_2)}{\chi_{\Lambda_2}(g)(u_1)} \right) = \chi_{\Lambda_2}(g)\left( \frac{u_1}{u_2} \right) \left( 1 + \sum_{n \geq 1} \sum_{1 \leq i_1, \ldots, i_n \leq 2, i_n \neq i_{n+1}} \mu(g; i_1, \ldots, i_n, u_{i_1}, \ldots, u_{i_n}) \right) \left( \frac{-u_2}{u_1} \right).$$

Getting these together, we obtain the assertion. □

Ihara also interpreted $\mathfrak{L}_2$ in terms of Fermat Jacobians. For a positive integer $n$, let $C_n$ be the non-singular, projective curve over $\mathbb{Q}$ defined by

$$X^{l^n} + Y^{l^n} = Z^{l^n}$$

and let $\text{Jac}_n$ be the Jacobian variety of $C_n$. Let $T(\text{Jac}_n)$ be the $l$-adic Tate module of $\text{Jac}_n$:

$$T(\text{Jac}_n) := \text{Hom}(\mathbb{Q}_l/\mathbb{Z}_l, \text{Jac}_n(\overline{\mathbb{Q}})) \simeq H_1^{\text{sing}}(C_n(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_l,$$
and let
\[ T := \lim_{\leftarrow} T(\text{Jac}_n), \]
where the inverse limit is taken with respect to the maps \( T(\text{Jac}_{n+1}) \to T(\text{Jac}_n) \) induced by the morphisms \( C_{n+1} \to C_n \): \((X, Y, Z) \mapsto (X^l, Y^l, Z^l)\). Let \( g_{X,n}, g_{Y,n} \) be the automorphisms of \( \overline{C_n} := C_n \times_{\text{Spec} \mathbb{Q}} \text{Spec} \mathbb{Q} \) over \( \mathbb{P}^1 \) defined by
\[
g_{X,n} : (X, Y, Z) \mapsto (\zeta_n X, Y, Z), \quad g_{Y,n} : (X, Y, Z) \mapsto (X, \zeta_n Y, Z)\]
and set \( g_X := \lim g_{X,n}, g_Y := \lim g_{Y,n} \). Then \( \text{Gal}(\overline{C_n}/\mathbb{P}^1_{\mathbb{Q}}) = (\mathbb{Z}/\mathbb{Z}_l) g_{X,n} \oplus (\mathbb{Z}/\mathbb{Z}_l) g_{Y,n} \) and so \( \text{lim} \mathbb{Z}[\text{Gal}(\overline{C_n}/\mathbb{P}^1_{\mathbb{Q}})] \simeq \Lambda_2 \) by the correspondence \( g_X \mapsto 1 + u_1, g_Y \mapsto 1 + u_2 \). Thus \( T \) is regarded as a \( \Lambda_2 \)-module. Then we have the isomorphism of \( \Lambda_2 \)-modules
\[ \mathcal{L}_2 \simeq T. \]
For an explicit construction of the basis of \( T \) corresponding to \([x_1, x_2]\), we consult [Ae; §13].

Now, the main results in [Ih1] are arithmetic descriptions of
• values of \( F_g(u_1, u_2) \) at \( l \)-powerth roots of unity in terms of the Jacobi sums which arise from the Galois action on \( T(\text{Jac}_n) \), and
• coefficients of \( F_g(u_1, u_2) \) in terms of \( l \)-adic Soulé cocycles which are defined by the Galois action on higher cyclotomic \( l \)-units.

We will describe these, using Theorem 6.1.3, from the view point of arithmetic topology.

### 6.2. Values of the Ihara power series.

Let \( p \) be a rational prime which is in \( R_S \) of (1.2.5) and let \( \overline{\mathfrak{p}} \) be a prime of \( \overline{\mathbb{Q}} \) lying over \( p \). By Theorem 1.2.6 (2), \( \overline{\mathfrak{p}} \) is unramified in \( \Omega_S/\mathbb{Q} \) and so we have the Frobenius automorphism \( \sigma_{\overline{\mathfrak{p}}} \in \text{Gal}(\Omega_S/\mathbb{Q}) \). Let \( n \) be a fixed positive integer. Let \( \mathfrak{p}_n \) be the prime of \( \mathbb{Q}(\zeta_n) \) lying below \( \overline{\mathfrak{p}} \) and let \( \left( \frac{x}{\mathfrak{p}_n} \right)_{l^n} \) denote the \( l^n \)-th power residue symbol at \( \mathfrak{p}_n \) for \( x \in (\mathbb{Z}[\zeta_n]/\mathfrak{p}_n)^{\times} \). For \( a, b \in \mathbb{Z}/l^n \mathbb{Z} \setminus \{0\} \) with \((a, b, l) = 1\), we define the Jacobi sum by
\[
J_{l^n}(\mathfrak{p}_n)^{(a,b)} = \sum_{x,y \in (\mathbb{Z}[\zeta_n]/\mathfrak{p}_n)^{\times}, x+y=-1} \left( \frac{x}{\mathfrak{p}_n} \right)_{l^n}^a \left( \frac{y}{\mathfrak{p}_n} \right)_{l^n}^b.
\]
58
For \( l = 2 \), \( J_l(n)(a,b) \) must be multiplied by \( \left( \frac{-1}{p_n} \right)^a \). Let \( f \) be the order of \( p \) in \((\mathbb{Z}/l^n\mathbb{Z})^\times\). We note that \( \sigma_p^f \in \text{Gal}(\Omega_S/\mathbb{Q}(\zeta_{l^n})) \). By using Weil’s theorem, Ihara showed the following

**Theorem 6.2.1** ([Ih1; Theorem 7]). Let \( a, b \in \mathbb{Z}/l^n\mathbb{Z}\setminus\{0\} \) such that \( a+b \neq 0 \) and \( (a, b, a+b, l) = 1 \). Then we have

\[
F_\sigma^f(\zeta_{l^n}^a, \zeta_{l^n}^b - 1) = J_l(n)(a,b).
\]

Combining Theorem 6.1.3 and Theorem 6.2.1, we obtain the following \( l \)-adic expansion of the Jacobi sum \( J_l(n)(a,b) \) with coefficients \( l \)-adic Milnor numbers.

**Theorem 6.2.2.** Notations being as above, we have

\[
J_l(n)(a,b) = 1 + \sum_{n_1, n_2 \geq 0 \atop n_1 + n_2 \geq 1} \mu(\sigma_p^f; n_1, n_2)(\zeta_{l^n}^a - 1)^{n_1}(\zeta_{l^n}^b - 1)^{n_2}.
\]

**Proof.** Since we have \( \zeta_{l^n}^{\chi_m(\sigma_p^f)} = \zeta_{l^n}^{p^f} = \zeta_{l^n} \) by \( p^f \equiv 1 \mod l^n \), the formula follows from Theorem 6.1.3 and Theorem 6.2.1. □

### 6.3. Coefficients of the Ihara power series.

We will combine Theorem 6.1.3 with the result of Ihara, Kaneko and Yukinari on the Ihara power series ([IKY]) and deduce some formulas relating our \( l \)-adic Milnor numbers with the Soulé cocycles ([So]). As in 1.2, let \( \zeta_{l^n} \) be a primitive \( l^n \)-th root of unity for a positive integer \( n \) such that \( (\zeta_{l^{n+1}})^l = \zeta_{l^n} \) for \( n \geq 1 \). For \( a \in \mathbb{Z}/l^n\mathbb{Z} \), let \( \langle a \rangle_{l^n} \) denote the integer such that \( 0 \leq \langle a \rangle_{l^n} < l^n \) and \( a = \langle a \rangle_{l^n} \mod l^n \). For a positive integer \( m \), we let

\[
\varepsilon_{l^n}^{(m)} := \prod_{a \in (\mathbb{Z}/l^n\mathbb{Z})^\times} (\zeta_{l^n} - 1)^{\langle a^{m-1} \rangle_{l^n}},
\]

which is an \( l \)-unit in \( \mathbb{Q}(\zeta_{l^n}) \), called a **cyclotomic \( l \)-unit**. Then we define the \( m \)-th \( l \)-adic Soulé cocycle \( \chi_{l^n}^{(m)} : \text{Gal}_l \to \mathbb{Z}_l \) by the Kummer cocycle attached to the system of cyclotomic \( l \)-units \( \{\varepsilon_{l^n}^{(m)}\}_{n \geq 1} \)

\[
\zeta_{l^n}^{\chi_{l^n}^{(m)}(g)} = \left( (\varepsilon_{l^n}^{(m)})^{1/l^n} \right)^{g-1} \quad (n \geq 1, g \in \text{Gal}_l).
\]
It is easy to see the cocycle relation
\[
\chi^{(m)}(gh) = \chi^{(m)}(g) + \chi_l(g)\chi^{(m)}(h) \quad (g, h \in \text{Gal}_Q)
\]
and hence the restriction of \(\chi^{(m)}|_{\text{Gal}_Q[1]}\) is a character. Let \(\Omega^{ab}_l\) be the maximal abelian subextension of \(\Omega_l/Q[1]\). Since \(\mathbb{Q}(\zeta_l, (\zeta^{(m)}_l)^{1/l^n})\) is a cyclic extension of \(\mathbb{Q}(\zeta_l)\) unramified outside \(l\), we have \((\zeta^{(m)}_l)^{1/l^n} \in \Omega^{ab}_l\) and so the Soulé character \(\chi^{(m)}|_{\text{Gal}_Q[1]}\) factors through the Galois group \(\text{Gal}(\Omega^{ab}_l/Q[1])\). We note by Theorem 4.2.8 (3) that the pro-\(l\) reduced Gassner representation \(\text{Gass}^{\text{red}}\) also factors through \(\text{Gal}(\Omega^{ab}_l/Q[1])\).

We set
\[
\kappa_m(g) := \frac{\chi^{(m)}(g)}{1 - l^{m-1}} \quad (g \in \text{Gal}_Q),
\]
and introduce new variables \(U_1, U_2\) defined by
\[
1 + u_i = \exp(U_i) = \sum_{n=0}^{\infty} \frac{U_i^n}{n!} \in \mathbb{Q}_l[[U_i]] \quad (i = 1, 2)
\]
and set
\[
F_g(U_1, U_2) := F_g(u_1, u_2)|_{u_i=\exp(U_i)-1}.
\]

**Theorem 6.3.1.** ([IKY; Theorem A_2]). Notations being as above, we have, for \(g \in \text{Gal}(\Omega^{ab}_l/Q[1])\),
\[
F_g(U_1, U_2) = \exp \left\{ - \sum_{\substack{m \geq 3 \\
odd}} \kappa_m(g) \left( \sum_{m_1, m_2 \geq 1 \atop m_1 + m_2 = m} \frac{U_{1}^{m_1} U_{2}^{m_2}}{m_1! m_2!} \right) \right\}.
\]
Combining Theorem 6.1.3 and Theorem 6.3.1, we can deduce relations between \(l\)-adic Milnor numbers and \(l\)-adic Soulé characters. For this, we prepare the following

**Lemma 6.3.2.** Let \(a(n_1, n_2)\) and \(c(m_1, m_2)\) be given \(l\)-adic numbers for integers \(m_1, m_2, n_1, n_2 \geq 0\) with \(m_1 + m_2, n_1 + n_2 \geq 1\). Let
\[
A(u_1, u_2) := 1 + \sum_{n_1, n_2 \geq 0 \atop n_1 + n_2 \geq 1} a(n_1, n_2) u_1^{n_1} u_2^{n_2} \in \mathbb{Q}_l[[u_1, u_2]]
\]
and set

\[ B(U_1, U_2) := A(u_1, u_2)|_{u_i = \exp(u_i) - 1} = 1 + \sum_{N_1, N_2 \geq 0 \atop N_1 + N_2 \geq 1} b(N_1, N_2) U_1^{N_1} U_2^{N_2} \in \mathbb{Q}_l[[U_1, U_2]]. \]

Then we have

\[ b(N_1, N_2) = \sum_{n_1, n_2 \geq 1 \atop 0 \leq n_1 \leq N_1, 0 \leq n_2 \leq N_2} a(n_1, n_2) a_{n_1}(N_1) a_{n_2}(N_2), \]

where for \( j = 1, 2 \),

\[ a_{n_j}(N_j) := \begin{cases} 1 & (n_j = 0), \\ \sum_{e_1, \ldots, e_{n_j} \geq 1 \atop e_1 + \cdots + e_{n_j} = N_j} \frac{1}{e_1! \cdots e_{n_j}!} & (n_j \geq 1). \end{cases} \]

Let

\[ C(U_1, U_2) := \sum_{m_1, m_2 \geq 0 \atop m_1 + m_2 \geq 1} c(m_1, m_2) U_1^{m_1} U_2^{m_2} \in \mathbb{Q}_l[[U_1, U_2]] \]

and set

\[ D(U_1, U_2) := \exp(C(U_1, U_2)) = 1 + \sum_{N_1, N_2 \geq 0 \atop N_1 + N_2 \geq 1} d(N_1, N_2) U_1^{N_1} U_2^{N_2} \in \mathbb{Q}_l[[U_1, U_2]]. \]

Then we have

\[ d(N_1, N_2) = \sum_{1 \leq n \leq N_1 + N_2} \frac{1}{n!} \sum_{c(m_1^{(1)}, m_2^{(1)}) \cdots c(m_1^{(n)}, m_2^{(n)})} c(m_1^{(1)}, m_2^{(1)}) \cdots c(m_1^{(n)}, m_2^{(n)}), \]

where the second sum ranges over integers \( m_1^{(i)}, \ldots, m_1^{(n)}, m_2^{(1)}, \ldots, m_2^{(n)} \geq 0 \) satisfying \( m_1^{(i)} + m_2^{(i)} \geq 1 \) \( (1 \leq i \leq n) \), \( m_1^{(1)} + \cdots + m_1^{(n)} = N_1 \) and \( m_2^{(1)} + \cdots + m_2^{(n)} = N_2 \).

**Proof.** Both formulas for \( b(N_1, N_2) \) and \( d(N_1, N_2) \) follow from straightforward computations. \( \square \)
We apply Lemma 6.3.2 to the case that
$$A(u_1, u_2) = \text{Gass}^{\text{red}}(g),$$
where
$$a(n_1, n_2) = \mu(g; n_1, n_2)$$
and
$$C(U_1, U_2) = \log(\mathcal{F}_g(U_1, U_2)),$$
where
$$c(m_1, m_2) = \begin{cases} \frac{-\kappa_{m_1+m_2}(g)}{m_1!m_2!}, & (m_1 + m_2 \geq 3, \text{ odd}), \\ 0, & \text{otherwise.} \end{cases}$$
Then, by comparing coefficients of $U_1^{N_1}U_2^{N_2}$ in $\text{Gass}^{\text{red}}(g)|_{U_i = \exp(U_i) - 1} = \mathcal{F}_g(U_1, U_2)$, we obtain the following

**Theorem 6.3.3.** Notations being as above, we have the following equality for $g \in \text{Gal}_{\mathbb{Q}[1]}$:

$$\sum_{0 \leq n_1 \leq N_1, 0 \leq n_2 \leq N_2} \mu(g; n_1, n_2)a_{n_1}(N_1)a_{n_2}(N_2)$$

$$= \sum_{1 \leq n \leq N_1+N_2} \frac{(-1)^n}{n!} \sum_{m_1^{(i)} + m_2^{(i)} \geq 3} \frac{\kappa_{m_1^{(i)}+m_2^{(i)}}(g)}{m_1^{(i)}!m_2^{(i)}!} \cdots \frac{\kappa_{m_1^{(n)}+m_2^{(n)}}(g)}{m_1^{(n)}!m_2^{(n)}!},$$

where the last sum ranges over integers $m_1^{(1)}, \ldots, m_1^{(n)}, m_2^{(1)}, \ldots, m_2^{(n)} \geq 0$ satisfying $m_1^{(i)} + m_2^{(i)} \geq 3$; odd $(1 \leq i \leq n)$, $m_1^{(1)} + \cdots + m_1^{(n)} = N_1$ and $m_2^{(1)} + \cdots + m_2^{(n)} = N_2$.

For example, lower terms are given by

$$\mu(g; (12)) = \mu(g; (21)) = 0, \quad \mu(g; (212)) + \mu(g; (121)) = 0,$$

$$\mu(g; (221)) + \mu(g; (2212)) + \mu(g; (1221)) + \mu(g; (2121)) = -\frac{\kappa_3(g)}{2},$$

$$\mu(g; (112)) + \mu(g; (1121)) + \mu(g; (2112)) + \mu(g; (1212)) = -\frac{\kappa_3(g)}{2}.$$
References

[Am] F. Amano, On a certain nilpotent extension over \(\mathbb{Q}\) of degree 64 and the 4-th multiple residue symbol, Tohoku Math. J. (2) 66 (2014), no. 4, 501–522.

[Ae] G. Anderson, The hyperadelic gamma function, Invent. Math. 95, (1989), no. 1, 63–131.

[AI] G. Anderson, Y. Ihara, Pro-\(l\) branched coverings of \(\mathbb{P}^1\) and higher circular \(l\)-units, Ann. of Math. (2) 128 (1988), no. 2, 271–293.

[Aa] S. Andreadakis, On the automorphisms of free groups and free nilpotent groups, Proc. London Math. Soc. 15 (1965), 239-268.

[Ar] E. Artin, Theorie der Zöpfe, Abh. Math. Sem. Univ. Hamburg, 4 (1925), no. 1, 47–72.

[B] J. S. Birman, Braids, links, and mapping class groups, Annals of Mathematics Studies, 82. Princeton Univ. Press, Princeton, N.J.; Univ. of Tokyo Press, Tokyo, 1974.

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

[Da] M. Day, Nilpotence invariants of automorphism groups, Lecture note. Available at http://www.math.caltech.edu/~2010-11/1term/ma191a/

[DDMS] J. D. Dixon, M. P. F. du Sautoy, A. Mann, D. Segal, Analytic pro-\(p\) groups, Second edition. Cambridge Studies in Advanced Mathematics, 61, Cambridge University Press, Cambridge, 1999.

[Dw] W. G. Dwyer, Homology, Massey products and maps between groups, J. Pure Appl. Algebra 6 (1975), no. 2, 177–190.

[F] R. H. Fox, Free differential calculus. I. Derivation in the free group ring, Ann. of Math. (2) 57 (1953). 547–560.

[G] A. Grothendieck, Revêtements Étales et Groupe Fondamental, Lecture Notes in Mathematics, 224, Springer-Verlag, 1971.

[Ha] N. Habegger, Milnor, Johnson, and Tree Level Perturbative Invariants, preprint, 2000.

[HM] N. Habegger, G. Masbaum, The Kontsevich integral and Milnor’s invariants, Topology 39 (2000), no. 6, 1253–1289.

[Hi] J. Hillman, Algebraic invariants of links, Second edition. Series on Knots and Everything, 52. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.

[Ih1] Y. Ihara, Profinite braid groups, Galois representations and complex multiplications, Ann. of Math. (2) 123 (1986), no. 1, 43–106.
[Ih2] Y. Ihara, On Galois representations arising from towers of coverings of \( \mathbb{P}^1 \setminus \{0, 1, \infty\} \), Invent. Math. 86 (1986), no. 3, 427–459.

[Ih3] Y. Ihara, Arithmetic analogues of braid groups and Galois representations, Braids (Santa Cruz, CA, 1986), 245–257, Contemp. Math., 78, Amer. Math. Soc., Providence, RI, 1988.

[Ih4] Y. Ihara, The Galois representation arising from \( \mathbb{P}^1 \setminus \{0, 1, \infty\} \) and Tate twists of even degree, Galois groups over \( \mathbb{Q} \) (Berkeley, CA, 1987), 299–313, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.

[IKY] Y. Ihara, M. Kaneko, A. Yukinari, On some properties of the universal power series for Jacobi sums, in Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986), Adv. Stud. Pure Math., 12 North-Holland, Amsterdam, (1987), 65–86.

[J1] D. Johnson, An abelian quotient of the mapping class group \( T_g \), Math. Ann. 249 (1980), 225–242.

[J2] D. Johnson, A survey of Torelli group, Low-dimensional topology (San Francisco, Calif., 1981), 165–179, Contemp. Math., 20, Amer. Math. Soc., Providence, RI, 1983.

[Ka] N. Kawazumi, Cohomological aspects of Magnus expansions, arXiv:0505497, 2006.

[Ki] T. Kitano, Johnson’s homomorphisms of subgroups of the mapping class group, the Magnus expansion and Massey higher products of mapping tori. Topology and its application, 69 1996, 165–172.

[Ko1] H. Kodani, On Johnson homomorphisms and Milnor invariants for pure braids, preprint, 2015.

[Ko2] H. Kodani, On Gassner representation, the Johnson homomorphisms and the Milnor invariants for pure braids, preprint, 2016.

[Ko3] H. Kodani, Arithmetic topology on braid and absolute Galois groups, Ph.D Thesis, Kyushu University, 2017.

[Kr] D. Kraines, Massey higher products, Trans. Amer. Math. Soc. 124 (1966), 431–449.

[MKS] W. Magnus, A. Karrass, D. Solitar, Combinatorial group theory. Presentations of groups in terms of generators and relations, Reprint of the 1976 second edition. Dover Publications, Inc., Mineola, NY, 2004.

[Ma] J. P. May, Matric Massey products, J. Algebra 12 (1969), 533–568.

[Mi] 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.

[Ms1] M. Morishita, Milnor invariants and Massey products for prime
numbers, Compos. Math. 140 (2004), no. 1, 69–83.
[Ms2] M. Morishita, Knots and Primes – An Introduction to Arithmetic Topology, Universitext, Springer, 2011.
[MT] M. Morishita, Y. Terashima, $p$-Johnson homomorphisms and pro-$p$ groups, J. of Algebra. 479 (2017), 102–136.
[Mt1] S. Morita, Abelian quotients of subgroups of the mapping class group of surfaces, Duke Math. J. 70 (1993), 699–726.
[Mt2] S. Morita, The extension of Johnson’s homomorphism from the Torelli group to the mapping class group, Invent. Math. 111 (1993), no. 1, 197–224.
[Mu] K. Murasugi, On Milnor’s invariant for links, Trans. Amer. Math. Soc. 124 (1966), 94–110.
[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.
[O1] T. Oda, Two propositions on pro-$l$ braid groups, unpublished note, 1985.
[O2] T. Oda, Note on meta-abelian quotients of pro-$l$ free groups, unpublished note, 1985.
[R] L. Rédei, Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper I, J. Reine Angew. Math., 180 (1939), 1–43.
[Sa] T. Satoh, A survey of the Johnson homomorphisms of the automorphism groups of free groups and related topics, Handbook of Teichmüller theory, volume V. (editor: A. Papadopoulos), 2016, 167–209.
[Se] J.-P. Serre, Lie algebras and Lie groups, Lecture Notes in Mathematics, 1500, Springer-Verlag, Berlin, 2006.
[So] C. Soulé, On higher $p$-adic regulators, Lecture Notes in Mathematics, 854, Springer-Verlag, 1981, 372–401.
[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, 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.

H. Kodani:
Graduate School of Mathematics, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, 819-0395, Japan.
e-mail: h-kodani@math.kyushu-u.ac.jp

M. Morishita:
Graduate School of Mathematics, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, 819-0395, Japan.
e-mail: morisita@math.kyushu-u.ac.jp

Y. Terashima:
Department of Mathematical and Computing Sciences, Tokyo Institute of Technology, 2-12-1 Oh-okayama, Meguro-ku, Tokyo 152-8551, Japan.
e-mail: tera@is.titech.ac.jp