Publ. RIMS Kyoto Univ. **53** (2017), 629–688
DOI 10.4171/PRIMS/53-4-6

Arithmetic Topology in Ihara Theory

To the memory of Professor Akito Nomura

by

Hisatoshi Kodani, Masanori Morishita and Yuji Terashima

Abstract

Ihara initiated the study of a certain Galois representation that 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 some issues and their interrelations 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.

2010 Mathematics Subject Classification: Primary 11R, 57M.
Keywords: Ihara representation, l-adic Milnor invariants, Pro-l Johnson homomorphisms, Pro-l Magnus–Gassner cocycles, l-adic Alexander invariants, Ihara power series.

§1. 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 $\mathrm{Gal}_k := \mathrm{Gal}(\overline{\mathbb{Q}}/k)$ is the étale fundamental group of $\mathrm{Spec}\, k$ so that it acts on the geometric fiber $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus S$ of the fibration $\mathbb{P}^1_k \setminus S \to \mathrm{Spec}\, k$ and hence on the pro-l étale fundamental group $\pi_1^{\text{pro-}l}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus S) \simeq \mathfrak{F}_r$, where $\mathfrak{F}_r$ denotes the free pro-l

Communicated by S. Mochizuki. Received December 20, 2016. Revised March 2, 2017; April 3, 2017; May 2, 2017.

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

group on r generators $x_1, \ldots, x_r$. In [Ih1], Ihara began to study this monodromy Galois representation

$$\mathrm{Ih}_S : \mathrm{Gal}_k \longrightarrow \mathrm{Aut}(\mathfrak{F}_r), \tag{1.1}$$

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 of Fermat Jacobians. We note that the image of Ih_S is contained in the subgroup consisting of $\varphi \in \mathrm{Aut}(\mathfrak{F}_r)$ such that $\varphi(x_i) \sim x_i^\alpha$ (conjugate) for $1 \le i \le r$ 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 (1.1) 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 ($r \ge 2$). Note that P_r is the topological fundamental group of the configuration space $D^r \setminus \Delta$ of ordered r points on a two-dimensional disk D, where Δ 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 monodromy, 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

$$\mathrm{Ar}_Q : P_r \longrightarrow \mathrm{Aut}(F_r), \tag{1.2}$$

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

We may see the following analogy between the Ihara representation (1.1) and the Artin representation (1.2):

(1.3)

Absolute Galois group Gal_k	Pure braid group P_r
$\mathbb{P}^1_k \setminus S \to \mathrm{Spec}\, k$ with geometric fiber $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus S$	Universal bundle over $D^r \setminus \Delta$ with fibers $D \setminus Q$
Ihara representation of Gal_k on $\pi_1^{\text{pro-}l}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus S) = \mathfrak{F}_r$	Artin representation of P_r on $\pi_1(D \setminus Q) = F_r$

The aim of this paper is, based on the above analogy (1.3), 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)∼(IV) and their interrelations 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.

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 $\mathrm{Ar}_Q(b)(x_i) = y_i(b) x_i y_i(b)^{-1}$ 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 $\overline{\mu}(\hat{b}; i_1 \cdots i_n i)$ is defined by taking modulo a certain indeterminacy $\Delta(b; i_1 \cdots i_n i)$: $\overline{\mu}(\hat{b}; i_1 \cdots i_n i) := \mu(b; i_1 \cdots i_n i) \bmod \Delta(b; i_1 \cdots i_n i)$. It turns out that it is an invariant of the link $\hat{b}$ 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 a 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 $\mathrm{Aut}(F_r)$ of a free group F_r ([Ka], [Sa]). Johnson homomorphisms describe the action of a certain filtration of $\mathrm{Aut}(F_r)$ on the nilpotent quotients $F_r/F_r(n)$ for $n \geq 1$, where $F_r(n)$ is the nth 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 the r punctured disk, the theory of Johnson homomorphisms can also be applied to P_r. It was shown in [Ko1], [Ko3, Chap. 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 $\det(\mathrm{Gass}(b) - I)$ gives the Alexander invariant which is a polynomial invariant of the link $\hat{b}$ ([B, 3.3]). The relations of the Gassner representations with Johnson homomorphisms and Milnor invariants were studied in [Ko2], [Ko3, Chap. 2].

In this paper, based on the analogy (1.3), we shall study arithmetic analogues in Ihara theory of issues (I)∼(IV). The contents of this paper are organized as follows. In Section 2, we recall the construction of Ihara representations and some basic results. In Section 3, we define l-adic Milnor numbers for each element in Gal_k and l-adic Milnor invariants for certain primes of $k(\zeta_{l^\infty})$, the field obtained by adjoining all lth-power roots of unity to k. We introduce the pro-l link group of each element of 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 4, we present a general theory of the pro-l Johnson map and pro-l Johnson homomorphisms for the absolute Galois group Gal_k. A similar theory has been developed in the context of non-abelian Iwasawa theory ([MT]). Among other things, we describe pro-l Johnson homomorphisms in terms of l-adic Milnor numbers. Sections 3 and 4 may be regarded as an arithmetic counterpart of [Ko1] and [Ko3, Chap. 1]. In Section 5, we introduce pro-l Magnus cocycles of Gal_k by using pro-l Fox free calculus, and give a relation with pro-l Johnson homomorphisms. We consider the pro-l (reduced) Gassner cocycle of Gal_k as a special case and express it by l-adic Milnor numbers. Section 5 may be regarded as an arithmetic counterpart of [Ko2] and [Ko3, Chap. 2]. We note that Oda's unpublished notes ([O1], [O2]) also concern some issues related to Sections 4 and 5. In Section 6, we introduce the pro-l link module and l-adic Alexander invariants. In Section 7, we consider the case that $S = \{0, 1, \infty\}$. We show that the Ihara power series $F_g(u_1, u_2)$ ($g \in \mathrm{Gal}_{\mathbb{Q}}$) introduced in [Ih1] coincides with our pro-l reduced Gassner cocycle, and give a formula that 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 $\mathbb{Q}(\zeta_{l^n})$ as a $(\zeta_{l^n} - 1)$-adic expansion with coefficients l-adic Milnor numbers. Finally, combining our formula and the result by Ihara, Kaneko and Yukinari [IKY], we give some formulas relating Soulé characters ([So]) with l-adic Milnor numbers.

This paper forms (part of) an elementary and group-theoretical foundation of *arithmetic topology* in Ihara theory. In 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, Chap. 8] and the works of Wojtkowiak on l-adic iterated integrals and l-adic polylogarithms ([NW], [W1], [W2], [W3], [W4], etc). See Remark 3.2.12. 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 $\mathbb{Q}_l$ 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, $\mathrm{M}(n;R)$ denotes the ring of $n\times n$ matrices whose entries are in R and $\mathrm{GL}(n;R)$ denotes the group of invertible elements of $\mathrm{M}(n;R)$.

§2. The Ihara representation

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

§2.1. The outer Galois representation

Let $x_1,\dots,x_r$ be r letters ($r\geq 2$) and let F_r denote the free group of rank r on $x_1,\dots,x_r$. 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 $F_r=\langle x_1,\dots,x_r,x_{r+1}\mid x_1\cdots x_r x_{r+1}=1\rangle$. Let $\mathfrak{F}_r$ denote the pro-l completion of F_r. Let $\mathrm{Aut}(\mathfrak{F}_r)$ (resp. $\mathrm{Int}(\mathfrak{F}_r)$) 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, Cor. 1.22]) and that $\mathrm{Aut}(\mathfrak{F}_r)$ is virtually a pro-l group ([DDMS, Thm. 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 $X_1,\dots,X_r$ and we have $X_1+\cdots+X_r+X_{r+1}=0$. Each $\varphi\in\mathrm{Aut}(\mathfrak{F}_r)$ induces an automorphism of the $\mathbb{Z}_l$-module H, which is denoted by $[\varphi]\in\mathrm{GL}(H)$.

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 $P_1,\dots,P_{r+1}$ 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 $P_1,\dots,P_r$, so that all P_i's are k-rational points of $\mathbb{P}^1$. Let $\mathrm{Gal}_k:=\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ be the absolute Galois group of k equipped with the Krull topology. Note that Gal_k is the étale fundamental group $\pi_1^{\text{ét}}(\mathrm{Spec}\,k)$ with the base point $\mathrm{Spec}\,\overline{\mathbb{Q}}\to\mathrm{Spec}\,k$. 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 $\mathrm{Spec}\,\overline{\mathbb{Q}}\to\mathbb{P}^1_{\overline{\mathbb{Q}}}\setminus S$ which lifts $\mathrm{Spec}\,\overline{\mathbb{Q}}\to\mathrm{Spec}\,k$. By [G, XII, Cor. 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 with $\pi_1(\mathbb{P}^1(\mathbb{C})\setminus S)$ obtained by associating to each x_i the homotopy class of a small loop around P_i and hence an identification of $\pi_1^{\text{pro-}l}(\mathbb{P}^1_{\overline{\mathbb{Q}}}\setminus S)$ with $\mathfrak{F}_r$.

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

$$\Phi_S : \mathrm{Gal}_k \longrightarrow \mathrm{Out}(\mathfrak{F}_r) := \mathrm{Aut}(\mathfrak{F}_r)/\mathrm{Int}(\mathfrak{F}_r). \tag{2.1.1}$$

In terms of the field extensions, the representation Φ_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 $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ is the rational function field $\overline{\mathbb{Q}}(t)$. The k-rational points P_i are identified with places of $K/\overline{\mathbb{Q}}$. Let M be the maximal pro-l extension of K unramified outside P_i $(1 \le i \le r+1)$. We fix once and for all an identification of $\mathfrak{F}_r$ with $\mathrm{Gal}(M/K)$ 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 the P_i's are k-rational, $M/k(t)$ is a Galois extension and so we have the exact sequence

$$1 \to \mathfrak{F}_r = \mathrm{Gal}(M/K) \to \mathrm{Gal}(M/k(t)) \to \mathrm{Gal}(K/k(t)) = \mathrm{Gal}_k \to 1.$$

For $g \in \mathrm{Gal}_k$, choose $\tilde{g} \in \mathrm{Gal}(M/k(t))$, which lifts g. Consider the action of Gal_k on $\mathrm{Gal}(M/K)$ defined by $f \mapsto \tilde{g}f\tilde{g}^{-1}$ and regard it as an automorphism of $\mathfrak{F}_r$ via the isomorphism ι. The effect of changing a lift $\tilde{g}$ is given as an inner automorphism of $\mathfrak{F}_r$. Thus we obtain the representation Φ_S. Note further that $g \circ P_i^M \circ \tilde{g}^{-1}$ is a place of M that coincides with P_i^M on K $(1 \le i \le r+1)$. So we have $g \circ P_i^M \circ \tilde{g}^{-1} \circ h = P_i^M$ for some $h \in \mathrm{Gal}(M/K)$ so that $h^{-1}\tilde{g}x_i\tilde{g}^{-1}h$ is a topological generator of the inertia group 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 Gal_k on $\mathfrak{F}_r$ gives an element of the subgroup $\tilde{P}(\mathfrak{F}_r)$ of $\mathrm{Aut}(\mathfrak{F}_r)$ defined by

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

Here the exponent $N(\varphi)$, called the *norm* of φ, gives a homomorphism $N : \mathrm{Aut}(\mathfrak{F}_r) \to \mathbb{Z}_l^{\times}$. So each $\varphi \in \tilde{P}(\mathfrak{F}_r)$ acts on the abelianization H by the multiplication by $N(\varphi)$, $[\varphi](X_i) = N(\varphi)X_i$ for $1 \le i \le r$. It is easy to see $\mathrm{Int}(\mathfrak{F}_r) \subset \tilde{P}(\mathfrak{F}_r)$. Thus we have the outer Galois representation (2.1.1),

$$\Phi_S : \mathrm{Gal}_k \longrightarrow \tilde{P}(\mathfrak{F}_r)/\mathrm{Int}(\mathfrak{F}_r). \tag{2.1.2}$$

§2.2. The Ihara representation

We will lift Φ_S to a representation in $\mathrm{Aut}(\mathfrak{F}_r)$. For this, consider the subgroup $P(\mathfrak{F}_r)$ of $\tilde{P}(\mathfrak{F}_r)$ defined by

$$P(\mathfrak{F}_r) := \left\{ \varphi \in \mathrm{Aut}(\mathfrak{F}_r) \;\middle|\; \begin{array}{l} \varphi(x_i) \sim x_i^{N(\varphi)} \, (1 \le i \le r-1), \ \varphi(x_r) \approx x_r^{N(\varphi)}, \\ \varphi(x_{r+1}) = x_{r+1}^{N(\varphi)} \text{ for some } N(\varphi) \in \mathbb{Z}_l^{\times} \end{array} \right\}, \tag{2.2.1}$$

where $\approx$ denotes conjugacy by an element of the subgroup $\mathfrak{K}$ 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 $N|_{P(\mathfrak{F}_r)}$:

$$P^1(\mathfrak{F}_r) := \left\{ \varphi \in \mathrm{Aut}(\mathfrak{F}_r) \,\middle|\, \begin{array}{l} \varphi(x_i) \sim x_i \ (1 \le i \le r-1) \ \varphi(x_r) \approx x_r, \\ \varphi(x_{r+1}) = x_{r+1} \end{array} \right\}.$$

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

Proposition 2.2.2. *The natural homomorphism* $\mathrm{Aut}(\mathfrak{F}_r) \to \mathrm{Aut}(\mathfrak{F}_r)/\mathrm{Int}(\mathfrak{F}_r)$ *induces the isomorphism* $P(\mathfrak{F}_r) \simeq \tilde{P}(\mathfrak{F}_r)/\mathrm{Int}(\mathfrak{F}_r)$. *The representatives in* $P(\mathfrak{F}_r)$ *of* $\tilde{P}(\mathfrak{F}_r)/\mathrm{Int}(\mathfrak{F}_r)$ *are called* Belyĭ'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 $\langle x_i \rangle = x_i^{\mathbb{Z}_l}$ for $1 \le i \le r+1$.

Injectivity: Suppose $\varphi \in P(\mathfrak{F}_r)$ and $\varphi = \mathrm{Int}(f)$ with $f \in \mathfrak{F}_r$. Then $f x_{r+1} f^{-1} = x_{r+1}^{N(\varphi)}$. 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 $a \in \mathbb{Z}_l$. Since $\varphi \in P(\mathfrak{F}_r)$, $f x_r f^{-1} = \varphi(x_r) = g x_r g^{-1}$ for some $g \in \mathfrak{K}$ and hence $g^{-1} f = x_r^b$ for some $b \in \mathbb{Z}_l$. Passing to the abelianization H, we find $a = b = 0$. Hence $f = 1$ and $\varphi = 1$.

Surjectivity: Take $\varphi \in \tilde{P}(\mathfrak{F}_r)$. Multiplying φ by an element of $\mathrm{Int}(\mathfrak{F}_r)$, we may assume $\varphi(x_{r+1}) = x_{r+1}^{N(\psi)}$. Set $\varphi(x_r) = g x_r g^{-1}$ with $g \in \mathfrak{F}_r$. Write $[g] = c_1 X_1 + \cdots + c_r X_r$ in H ($c_i \in \mathbb{Z}_l$) and let $\varphi_1 := \mathrm{Int}(x_{r-1}^{-c_{r-1}} x_r^{-c_r}) \circ \varphi$. Then $\varphi_1(x_r) = g_1 x_r g_1^{-1}$ and $g_1 := x_{r-1}^{-c_{r-1}} x_r^{-c_r} g \in \mathfrak{K}$. Hence $\varphi_1 \in P(\mathfrak{F}_r)$ and $\varphi \equiv \varphi_1 \bmod \mathrm{Int}(\mathfrak{F}_r)$. □

By Proposition 2.2.2, we can lift Φ_S of (2.1.2) to the representation in $P(\mathfrak{F}_r)$, denoted by Ih_S:

$$\mathrm{Ih}_S : \mathrm{Gal}_k \longrightarrow P(\mathfrak{F}_r), \tag{2.2.3}$$

which we call the *Ihara representation* associated to S. Let Ω_S denote the subfield of $\overline{\mathbb{Q}}$ corresponding to the kernel of Ih_S so that Ih_S factors through the Galois group $\mathrm{Gal}(\Omega_S/k)$:

$$\mathrm{Ih}_S : \mathrm{Gal}(\Omega_S/k) \longrightarrow P(\mathfrak{F}_r). \tag{2.2.4}$$

We recall some arithmetic properties on the ramification in the Galois extension Ω_S/k. For this, let us prepare some notation. Let ζ_{l^n} be a primitive l^nth root of unity for a positive integer n such that $(\zeta_{l^{n+1}})^l = \zeta_{l^n}$ for $n \ge 1$. We set $k(\zeta_{l^\infty}) := \cup_{n \ge 1} k(\zeta_{l^n})$. The *l-cyclotomic character* $\chi_l : \mathrm{Gal}_k \to \mathbb{Z}_l^\times$ is defined by $g(\zeta_{l^n}) = \zeta_{l^n}^{\chi_l(g)}$ for $g \in \mathrm{Gal}_k$. 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 $1 \le i \le r$, and let $\mathcal{O}_S$ be the integral closure of $\mathbb{Z}[l^{-1}, (s_i - s_j)^{-1}(1 \le i \ne j \le r)]$ in k. We then define R_S by the maximal spectrum

$$R_S := \operatorname{Spm} \mathcal{O}_S. \tag{2.2.5}$$

Theorem 2.2.6. *With notation as above, the following assertions hold:*

(1) ([Ih1, Prop. 2, p. 53]). $N \circ \mathrm{Ih}_S : \mathrm{Gal}_k \to \mathbb{Z}_l^\times$ *coincides with* χ_l. *In particular, the restriction of* φ_S *to* $\mathrm{Gal}_{k(\zeta_{l^\infty})} := \mathrm{Gal}(\overline{\mathbb{Q}}/k(\zeta_{l^\infty}))$, *denoted by* Ih_S^1, *gives the representation*

$$\mathrm{Ih}_S^1 : \mathrm{Gal}_{k(\zeta_{l^\infty})} \longrightarrow P^1(\mathfrak{F}_r)$$

and we have $k(\zeta_{l^\infty}) \subset \Omega_S$.

(2) ([AI, Prop. 2.5.2, Thm. 3]). The Galois extension Ω_S/k *is unramified over* R_S *and* $\Omega_S/k(\zeta_l)$ *is a pro-*l *extension.*

Remark 2.2.7 (Cf. [Ih2]). By Artin's theorem ([Ar], [B, Thm. 1.9]), the Artin representation Ar_Q of the pure braid group P_r in Section 1 induces the isomorphism

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

So the representation $\mathrm{Ih}_S^1 : \mathrm{Gal}_{k(\zeta_{l^\infty})} \to P^1(\mathfrak{F}_r)$ (resp. $\mathrm{Ih}_S : \mathrm{Gal}_k \to P(\mathfrak{F}_r)$) may be seen as an (resp. extended) arithmetic analogue of the Artin representation Ar_Q.

§3. l-adic Milnor invariants and pro-l link groups

§3.1. Pro-l Magnus expansions

Let $\{\mathfrak{F}_r(n)\}_{n\ge1}$ be the lower central series of $\mathfrak{F}_r$ defined by

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

Note that each $\mathfrak{F}_r(n)$ is a closed normal subgroup of $\mathfrak{F}_r$ so that $\mathfrak{F}_r(n)/\mathfrak{F}_r(n+1)$ is central in $\mathfrak{F}_r/\mathfrak{F}_r(n+1)$, and that each $\mathfrak{F}_r(n)$ is a finitely generated pro-l group ([DDMS, 1.7, 1.14]). As in Section 2, let H denote the abelianization of $\mathfrak{F}_r$:

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

which is the free $\mathbb{Z}_l$-module with basis $X_1, \dots, X_r$, 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 $\bigoplus_{n\ge0} H^{\otimes n}$, 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 $n \ge 1$. It is nothing but the noncommutative polynomial algebra $\mathbb{Z}_l\langle X_1, \dots, X_r\rangle$ over $\mathbb{Z}_l$ with variables $X_1, \dots, X_r$:

$$T(H) = \bigoplus_{n\ge0} H^{\otimes n} = \mathbb{Z}_l\langle X_1, \dots, X_r\rangle.$$

Let $\widehat{T}(H)$ 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 noncommutative formal power series (called the *Magnus power series*) over $\mathbb{Z}_l$ with variables $X_1, \ldots, X_r$:

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

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

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

(3.1.1) $$\Theta : \mathbb{Z}_l[[\mathfrak{F}_r]] \xrightarrow{\sim} \widehat{T}(H),$$

which we call the *pro-l Magnus isomorphism.* Here $I^n_{\mathbb{Z}_l[[\mathfrak{F}_r]]}$ corresponds, under Θ, to $\widehat{T}(n)$ for $n \geq 0$. For $\alpha \in \mathbb{Z}_l[[\mathfrak{F}_r]]$, $\Theta(\alpha)$ is called the *pro-l Magnus expansion* of α. In the following, for a multiindex $I = (i_1 \cdots i_n)$, $1 \leq i_1, \ldots, i_n \leq r$, we set

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

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

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

Restricting Θ to $\mathfrak{F}_r$, we have an injective group homomorphism, denoted by the same Θ:

(3.1.3) $$\Theta : \mathfrak{F}_r \hookrightarrow 1 + \widehat{T}(1),$$

which we call the *pro-l Magnus embedding* of $\mathfrak{F}_r$ into $1 + \widehat{T}(1)$.

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

Property 3.1.4. For α, $\beta \in \mathbb{Z}_l[[\mathfrak{F}_r]]$ and a multiindex 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 multiindices such that $AB = I$, and we understand that $\mu(A;\alpha) = \epsilon_{\mathbb{Z}_l[[\mathfrak{F}_r]]}(\alpha)$ (resp. $\mu(B;\beta) = \epsilon_{\mathbb{Z}_l[[\mathfrak{F}_r]]}(\beta)$) if $|A| = 0$ (resp. $|B| = 0$).

Property 3.1.5 (Shuffle relation). For $f \in \mathfrak{F}_r$ and multiindices I, J with $|I|, |J| \geq 1$, we have

$$\mu(I; f)\mu(J; f) = \sum_{A \in \mathrm{Sh}(I,J)} \mu(A; f),$$

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

Property 3.1.6. For $f \in \mathfrak{F}_r$ and $d \geq 2$, we have

$$\begin{aligned} \mu(I; f) = 0 \text{ for } |I| < d, \text{ i.e., } \deg(\Theta(f-1)) \geq d &\Longleftrightarrow f \in \mathfrak{F}_r(d) \\ &\Longleftrightarrow f - 1 \in I^d_{\mathbb{Z}_l[[\mathfrak{F}_r]]}. \end{aligned}$$

An automorphism φ of the topological $\mathbb{Z}_l$-algebra $\mathbb{Z}_l[[\mathfrak{F}_r]]$ (resp. $\widehat{T}(H)$) 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. $\varphi(\widehat{T}(n)) = \widehat{T}(n)$) for all $n \geq 1$. Let $\mathrm{Aut}^{\mathrm{fil}}(\mathbb{Z}_l[[\mathfrak{F}_r]])$ (resp. $\mathrm{Aut}^{\mathrm{fil}}(\widehat{T}(H))$) be the group of filtration-preserving automorphisms of the topological $\mathbb{Z}_l$-algebras $\mathbb{Z}_l[[\mathfrak{F}_r]]$ (resp. $\widehat{T}(H)$). The pro-l Magnus isomorphism Θ in (3.1.1) induces the isomorphism

$$\text{(3.1.7)} \qquad \mathrm{Aut}^{\mathrm{fil}}(\mathbb{Z}_l[[\mathfrak{F}_r]]) \xrightarrow{\sim} \mathrm{Aut}^{\mathrm{fil}}(\widehat{T}(H)), \quad \varphi \mapsto \Theta \circ \varphi \circ \Theta^{-1}.$$

In the following we set

$$\text{(3.1.8)} \qquad \varphi^* := \Theta \circ \varphi \circ \Theta^{-1}.$$

We note by (3.1.6) that any automorphism φ 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 φ. It is easy to see by (3.1.8) that for $\varphi \in \mathrm{Aut}^{\mathrm{fil}}(\mathbb{Z}_l[[\mathfrak{F}_r]]), \alpha \in \mathbb{Z}_l[[\mathfrak{F}_r]]$, we have

$$\text{(3.1.9)} \qquad \Theta(\varphi(\alpha)) = \varphi^*(\Theta(\alpha)).$$

§3.2. l-adic Milnor invariants

Let $\mathrm{Ih}_S : \mathrm{Gal}_k \to P(\mathfrak{F}_r)$ be the Ihara representation associated to S in (2.2.3).

Lemma 3.2.1. *Let $g \in \mathrm{Gal}_k$. For each $1 \leq i \leq r$, there exists uniquely $y_i(g) \in \mathfrak{F}_r$ satisfying the following properties:*

(1) $\mathrm{Ih}_S(g)(x_i) = y_i(g) x_i^{\chi_l(g)} y_i(g)^{-1}$, where χ_l is the l-cyclotomic character.
(2) In the expression $[y_i(g)] = c_1^{(i)} X_1 + \cdots + c_r^{(i)} X_r$ $(c_j^{(i)} \in \mathbb{Z}_l)$, $c_i^{(i)} = 0$.

Proof. Although the proof is standard, we give it for the sake of readers because this lemma is basic in the theory of Milnor invariants.

Existence: By the definition (2.2.1) of $P(\mathfrak{F}_r)$ and Theorem 2.2.6(1), there is $z_i \in \mathfrak{F}_r$ such that $\mathrm{Ih}_S(g)(x_i) = z_i x_i^{\chi_l(g)} z_i^{-1}$ for each i. Let $[z_i] = a_1^{(i)} X_1 + \cdots + a_r^{(i)} X_r$, $(a_j^{(i)} \in \mathbb{Z}_l)$. We set $y_i := z_i x_i^{-a_i^{(i)}}$. Then conditions (1) and (2) are satisfied for y_i.

Uniqueness: Suppose that y_i and z_i in $\mathfrak{F}_r$ satisfy conditions (1) and (2). Since $z_i^{-1} y_i$ is in the centralizer of $x_i^{\chi_l(g)}$, $z_i^{-1} y_i = x_i^{b_i}$ for some $b_i \in \mathbb{Z}_l$. Comparing the coefficients of X_i in $[z_i^{-1} y_i]$ and $[x_i^{b_i}]$, we have $b_i = 0$ and hence $y_i = z_i$. □

We call $y_i(g) \in \mathfrak{F}_l$ in Lemma 3.2.1 the ith (*preferred*) *longitude* of $g \in \mathrm{Gal}_k$ for S. By Lemma 3.2.1, $\mathrm{Ih}_S(g)$ for $g \in \mathrm{Gal}_k$ is determined by the l-cyclotomic value $\chi_l(g)$ and the r-tuple $\mathbf{y}(g) := (y_1(g), \ldots, y_r(g))$ of longitudes of g for S. We note that $\mathrm{Ih}_S(g)$ acts on the abelianization H of $\mathfrak{F}_r$ by the multiplication by $\chi_l(g)$, $[\mathrm{Ih}_S(g)](X_i) = \chi_l(g) X_i$ for $1 \le i \le r$. We also note that $y_i : \mathrm{Gal}_k \to \mathfrak{F}_r$ is continuous, since Ih_S is continuous.

Following the case for pure braids ([Ko1], [Ko3, Chap. 1], [MK, Chaps. 6, 4]), we will define the l-adic Milnor numbers of $g \in \mathrm{Gal}_k$ by the l-adic Magnus coefficients of the ith longitude $y_i(g)$: Let $I = (i_1 \cdots i_n)$ be a multiindex, where $1 \le i_1, \ldots, i_n \le r$ and $|I| = n \ge 1$. The *l-adic Milnor number* of $g \in \mathrm{Gal}_k$ for I, denoted by $\mu(g; I) = \mu(g; i_1 \cdots i_n)$, is defined by the l-adic Magnus coefficient of $y_{i_n}(g)$ for $I' := (i_1 \cdots i_{n-1})$:

$$\mu(g; I) := \mu(I'; y_{i_n}(g)). \tag{3.2.2}$$

Here we set $\mu(g; I) := 0$ if $|I| = 1$. We note that the map $\mu(\ ; I) : \mathrm{Gal}_k \to \mathbb{Z}_l$ is continuous for each I, since $y_i : \mathrm{Gal}_k \to \mathfrak{F}_r$ is continuous. We define $\mathfrak{a}(g)$ to be the ideal of $\mathbb{Z}_l$ generated by $\chi_l(g) - 1$. Note that $\mathfrak{a}(g) = 0$ when $g \in \mathrm{Gal}_{k(\zeta_{l^\infty})}$. We then define the *indeterminacy* $\Delta(g; I)$ by

$$\Delta(g; I) := \left\{ \begin{array}{l} \text{the ideal of } \mathbb{Z}_l \text{ generated by } \mathfrak{a}(g) \text{ and } \mu(J; y_j(g)), \text{ where } J \\ \text{ranges over proper subsequence } I' \text{ and } j = i_n \text{ or } j \text{ is in } J \end{array} \right\} \tag{3.2.3}$$

We also write $\Delta(I'; y_{i_n}(g))$ for $\Delta(g; I)$ for later convenience. We then set

$$\overline{\mu}(g; I) := \mu(g; I) \bmod \Delta(g; I), \tag{3.2.4}$$

which we call the *l-adic Milnor invariant* of $g \in \mathrm{Gal}_k$ for I.

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

Lemma 3.2.5. *For $g, h \in \mathrm{Gal}_k$ and $1 \leq i \leq r$, we have*

(1) $y_i(h^{-1}) = \mathrm{Ih}_S(h^{-1})(y_i(h)^{-1})$*;*
(2) $y_i(hg) = \mathrm{Ih}_S(h)(y_i(g))y_i(h)$ *(cocycle property);*
(3) $y_i(hgh^{-1}) = \mathrm{Ih}_S(hg)(y_i(h^{-1}))\,\mathrm{Ih}_S(h)(y_i(g))y_i(h)$.

Proof. (1) By Lemma 3.2.1, we have

$$\begin{aligned} x_i &= \mathrm{Ih}_S(h^{-1})\,\mathrm{Ih}_S(h)(x_i) \\ &= \mathrm{Ih}_S(h^{-1})(y_i(h)x_i^{\chi_l(h)}y_i(h)^{-1}) \\ &= \mathrm{Ih}_S(h^{-1})(y_i(h))y_i(h^{-1})x_i y_i(h^{-1})^{-1}\,\mathrm{Ih}_S(h^{-1})(y_i(h)^{-1}), \end{aligned}$$

from which we find $\mathrm{Ih}_S(h^{-1})(y_i(h))y_i(h^{-1}) = x_i^{a_i}$ 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 3.2.1, we have

$$\mathrm{Ih}_S(hg)(x_i) = y_i(hg)x_i^{\chi_l(hg)}y_i(hg)^{-1}. \tag{3.2.5.1}$$

On the other hand, we have

$$\begin{aligned} \mathrm{Ih}_S(hg)(x_i) &= \mathrm{Ih}_S(h)\,\mathrm{Ih}_S(g)(x_i) \\ &= \mathrm{Ih}_S(h)(y_i(g)x_i^{\chi_l(g)}y_i(g)^{-1}) \\ &= \mathrm{Ih}_S(h)(y_i(g))\,\mathrm{Ih}_S(h)(x_i^{\chi_l(g)})\,\mathrm{Ih}_S(h)(y_i(g)^{-1}) \\ &= \mathrm{Ih}_S(h)(y_i(g))y_i(h)x_i^{\chi_l(hg)}y_i(h)^{-1}\,\mathrm{Ih}_S(h)(y_i(g)^{-1}). \end{aligned} \tag{3.2.5.2}$$

Comparing (3.2.5.1) and (3.2.5.2), we have $y_i(hg)^{-1}\,\mathrm{Ih}_S(h)(y_i(g))y_i(h) = x_i^{b_i}$ 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

$$y_i(hgh^{-1}) = \mathrm{Ih}_S(hg)(y_i(h^{-1}))y_i(hg) = \mathrm{Ih}_S(hg)(y_i(h^{-1}))\,\mathrm{Ih}_S(h)(y_i(g))y_i(h).$$

□

For $\rho \in \mathrm{Gal}_k$ and a multiindex J with $|J| \geq 1$, we define $\Theta_J(\rho)$ by

$$\Theta_J(\rho) := \mathrm{Ih}_S(\rho)^*(X_J) - \chi_l(\rho)^{|J|}X_J. \tag{3.2.6}$$

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

Lemma 3.2.7. *With notation 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:*

- *(i) If* $m_A(J;\rho)\neq 0$*, then* A *contains* J *as a proper subsequence. So we may* write $\Theta_J(\rho)=\sum_{J\subsetneq A} m_A(J;\rho)X_A$.
- *(ii) 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*

$$\begin{aligned}\Theta(\mathrm{Ih}_S(\rho)(y)) &= 1+\sum_{|J|\geq 1}\chi_l(\rho)^{|J|}\mu(J;y)X_J+\sum_{|J|\geq 1}\mu(J;y)\Theta_J(\rho)\\ &\equiv \Theta(y)+\sum_{|J|\geq 1}\mu(J;y)\Theta_J(\rho) \bmod \mathfrak{a}(\rho).\end{aligned}$$

Proof. (1) Let $1\leq j\leq r$ and write $\Theta(y_j(\rho))=1+Y_j(\rho)$. By (3.1.9) and Lemma 3.2.1, we have

$$\begin{aligned}\mathrm{Ih}_S(\rho)^*(X_j) &= \mathrm{Ih}_S(\rho)^*(\Theta(x_j-1))\\ &= \Theta(\mathrm{Ih}_S(\rho)(x_j-1))\\ &= \Theta(y_j(\rho)x_j^{\chi_l(\rho)}y_j(\rho)^{-1})-1\\ &= \Theta(y_j(\rho))\Theta(x_j)^{\chi_l(\rho)}\Theta(y_j(\rho)^{-1})-1\\ &= (1+Y_j(\rho))(1+X_j)^{\chi_l(\rho)}(1-Y_j(\rho)+Y_j(\rho)^2-\cdots)-1\\ &= \chi_l(\rho)X_j+\Theta_j(\rho),\end{aligned}\tag{3.2.7.1}$$

where $\Theta_j(\rho)$ is the sum of terms of the form $uY_j(\rho)^aX_j^bY_j(\rho)^c$ for some $a,c\geq 0$ with $a+c\geq 1$, $b\geq 1$ and $u\in\mathbb{Z}_l$. Write $\Theta_j(\rho)=\sum_{|A|\geq 2} m_A(j;\rho)X_A$. It is easy to see that if $m_A(j;\rho)\neq 0$, then A must contain j. Moreover, since $Y_j(\rho)=\sum_{|B|\geq 1}\mu(B;y_j(\rho))X_B$, then $m_A(j;\rho)$ is a multiple of $\mu(B;y_j(\rho))$ by an l-adic integer, where B is some proper subsequence of A. Let $J=(j_1\cdots j_n)$. By (3.2.7.1), we have

$$\begin{aligned}\sum_{|A|\geq|J|} m_A(J;\rho)X_A &:= \Theta_J(\rho)\\ &:= \mathrm{Ih}_S(\rho)^*(X_J)-\chi_l(\rho)^{|J|}X_J\\ &= \mathrm{Ih}_S(\rho)^*(X_{j_1})\cdots\mathrm{Ih}_S(\rho)^*(X_{j_n})-\chi_l(\rho)^{|J|}X_J\\ &= (\chi_l(\rho)X_{j_1}+\Theta_{j_1}(\rho))\cdots(\chi_l(\rho)X_{j_n}+\Theta_{j_n}(\rho))-\chi_l(\rho)^{|J|}X_J\\ &= \Phi_{j_1}(\rho)\cdots\Phi_{j_n}(\rho),\end{aligned}$$

where $\Phi_j(\rho)$ is $\chi_l(\rho)X_j$ 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 properties (i) and (ii).

(2) By (3.1.9) and (3.2.6), we have

$$\begin{aligned}
\Theta(\mathrm{Ih}_S(\rho)(y)) &= \mathrm{Ih}_S(\rho)^*(\Theta(y)) \\
&= \mathrm{Ih}_S(\rho)^*\left(1 + \sum_{|J|\geq 1} \mu(J;y)X_J\right) \\
&= 1 + \sum_{|J|\geq 1} \mu(J;y)\,\mathrm{Ih}_S(\rho)^*(X_J) \\
&= 1 + \sum_{|J|\geq 1} \mu(J;y)(\chi_l(\rho)^{|J|}X_J + \Theta_J(\rho)) \\
&= 1 + \sum_{|J|\geq 1} \chi_l(\rho)^{|J|}\mu(J;y)X_J + \sum_{|J|\geq 1} \mu(J;y)\Theta_J(\rho) \\
&\equiv \Theta(y) + \sum_{|J|\geq 1} \mu(J;y)\Theta_J(\rho) \bmod \mathfrak{a}(\rho).
\end{aligned}$$

□

We are ready to prove the following result.

Theorem 3.2.8. *For a multiindex I, the l-adic Milnor invariant $\overline{\mu}(g;I)$ for $g \in \mathrm{Gal}_k$ is unchanged when g is replaced with its conjugate by an element of $\mathrm{Gal}_{k(\zeta_{l^\infty})}$. To be precise, let I be a multiindex with $|I| \geq 1$. Let $g \in \mathrm{Gal}_k$ and $h \in \mathrm{Gal}_{k(\zeta_{l^\infty})}$. Then we have $\Delta(hgh^{-1};I) = \Delta(g;I)$ and*

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

Proof. Let I be a multiindex with $|I| \geq 1$ and $1 \leq i \leq r$. For $g \in \mathrm{Gal}_k$ and $h \in \mathrm{Gal}_{k(\zeta_{l^\infty})}$, we will show

$$\mu(I;y_i(hgh^{-1})) \equiv \mu(I;y_i(g)) \bmod \Delta(I;y_i(g)). \tag{3.2.8.1}$$

By Lemma 3.2.5(3), we have

$$\Theta(y_i(hgh^{-1})) = \Theta(\mathrm{Ih}_S(hg)(y_i(h^{-1})))\Theta(\mathrm{Ih}_S(h)(y_i(g)))\Theta(y_i(h)). \tag{3.2.8.2}$$

For simplicity, we set, for a multiindex J with $|J| \geq 1$,

$$a_J := \mu(J;\mathrm{Ih}_S(hg)(y_i(h^{-1}))), \quad b_J := \mu(J;\mathrm{Ih}_S(h)(y_i(g))), \quad c_J := \mu(J;y_i(h)).$$

Then, from (3.2.8.2) or (3.1.4), we have

(3.2.8.3)

$$\mu(I; y_i(hgh^{-1})) = a_I + b_I + c_I + \sum_{AB=I} a_A b_B + \sum_{BC=I} b_B c_C + \sum_{AC=I} a_A c_C + \sum_{ABC=I} a_A b_B c_C,$$

where A, B, C are multiindices with $|A|$, $|B|$, $|C| \geq 1$.

First, we look at b_B for a subsequence B of I. By Lemma 3.2.7(1), (2) and as $h \in \mathrm{Gal}_{k(\zeta_{l^\infty})}$, 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 (3.2.8.3) and the definition of $\Delta(I; y_i(g))$, we have

$$\mu(I; y_i(hgh^{-1})) - \mu(I; y_i(g)) \equiv a_I + c_I + \sum_{AC=I} a_A c_C \bmod \Delta(I; y_i(g)). \tag{3.2.8.4}$$

Here we note that the right-hand side of (3.2.8.4) is the coefficient of X_I of $\Theta(\mathrm{Ih}_S(hg)(y_i(h^{-1})))\Theta(y_i(h))$.

So, next we look at $\Theta(\mathrm{Ih}_S(hg)(y_i(h^{-1})))\Theta(y_i(h))$. By (3.1.9), Lemma 3.2.5(1) and Lemma 3.2.7(2), we have

$$\begin{aligned}\Theta(\mathrm{Ih}_S(hg)(y_i(h^{-1}))) &= \mathrm{Ih}_S(hg)^*(\Theta(y_i(h^{-1}))) \\ &= \mathrm{Ih}_S(h)^*\,\mathrm{Ih}_S(g)^*(\Theta(y_i(h^{-1}))) \\ &\equiv \mathrm{Ih}_S(h)^*(\Theta(y_i(h^{-1})) + \sum_{|J|\geq 1} \mu(J; y_i(h^{-1}))\Theta_J(g)) \pmod{\mathfrak{a}(g)} \\ &= \Theta(\mathrm{Ih}_S(h)(y_i(h^{-1}))) + \sum_{|J|\geq 1} \mu(J; y_i(h^{-1}))\,\mathrm{Ih}_S(h)^*(\Theta_J(g)) \\ &= \Theta(y_i(h)^{-1}) + \sum_{|J|\geq 1} \mu(J; y_i(h^{-1}))\,\mathrm{Ih}_S(h)^*(\Theta_J(g)).\end{aligned} \tag{3.2.8.5}$$

Here let us write $\Theta_J(g) = \sum_{J \subsetneq A} m_A(J; g) X_A$ as in Lemma 3.2.7(1). Then we have, as $h \in \mathrm{Gal}_{k(\zeta_{l^\infty})}$,

$$\begin{aligned}\mathrm{Ih}_S(h)^*(\Theta_J(g)) &= \sum_{J \subsetneq A} m_A(J; g)\,\mathrm{Ih}_S(h)^*(X_A) \\ &= \sum_{J \subsetneq A} m_A(J; g)(X_A + \Theta_A(h)) \\ &= \sum_{J \subsetneq A} m_A(J; g)(X_A + \sum_{A \subsetneq A'} m_{A'}(A; h) X_{A'}).\end{aligned} \tag{3.2.8.6}$$

By (3.2.8.5) and (3.2.8.6), we have

$$\begin{aligned}&\Theta(\mathrm{Ih}_S(hg)(y_i(h^{-1})))\\ &\quad\equiv \Theta(y_i(h)^{-1}) + \sum_{|J|\geq 1}\sum_{J\subsetneq A} \mu(J; y_i(h^{-1}))m_A(J;g)\\ &\quad\quad\times\left(X_A + \sum_{A\subsetneq A'} m_{A'}(A;h)X_{A'}\right) \pmod{\mathfrak{a}(g)}\end{aligned}$$

and hence

$$\begin{aligned}&\Theta(\mathrm{Ih}_S(hg)(y_i(h^{-1}))\Theta(y_i(h))\\ &\quad\equiv 1 + \sum_{|J|\geq 1}\sum_{J\subsetneq A} \mu(J; y_i(h^{-1}))m_A(J;g)\\ &\quad\quad\times\left(X_A + \sum_{A\subsetneq A'} m_{A'}(A;h)X_{A'}\right)\Theta(y_i(h)) \pmod{\mathfrak{a}(g)}.\end{aligned} \tag{3.2.8.7}$$

Here we note that by Lemma 3.2.7(2), $m_A(J;g)$ 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 (3.2.3) of $\Delta(I; y_i(g))$, the coefficient of X_I in the right-hand side of (3.2.8.7) must be congruent to $0 \bmod \Delta(I; y_i(g))$. By (3.2.8.4), we obtain (3.2.8.1).

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 $\mathfrak{a}(g) = \mathfrak{a}(hgh^{-1})$) 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 (3.2.8.1), we have, for all I with $|I| \leq n$ and $1 \leq i \leq r$,

$$\mu(I; y_i(hgh^{-1})) \equiv \mu(I; y_i(g)) \bmod \Delta(I; y_i(g)) \ (= \Delta(I; y_i(hgh^{-1})). \tag{3.2.8.8}$$

Using (3.2.8.8) and the definition (3.2.3) 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 $|I| = n + 1$. □

Remark 3.2.9. It is known that a braid β 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, Chap. 9]). In particular, they have the same Milnor invariants. So Theorem 3.2.8 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 3.2.10. *Let $g \in \mathrm{Gal}_k$. For multiindices I, J with $|I|, |J| \geq 1$ and $1 \leq i \leq r$, we have*

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

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

Proof. By (3.1.5), we have

$$\mu(g; Ii)\mu(g; Ji) = \sum_{A \in \mathrm{Sh}(I,J)} \mu(g; Ai).$$

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

Let R_S^∞ be the set of primes of $k(\zeta_{l^\infty})$ lying over R_S in (2.2.5). For $\mathfrak{p}_\infty \in R_S^\infty$, choose a prime $\mathfrak{P}$ of Ω_S lying over $\mathfrak{p}_\infty$. Since $\mathfrak{P}$ is unramified in the Galois extension Ω_S/k by Theorem 2.2.6(2), we have the Frobenius automorphism $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(\Omega_S/k)$ of $\mathfrak{P}$. By Theorem 3.2.8, $\overline{\mu}(\sigma_{\mathfrak{P}}; I)$ is independent of the choice of $\mathfrak{P}$ lying over $\mathfrak{p}_\infty$. So we define the *l-adic Milnor invariant* of $\mathfrak{p}_\infty$ for a multiindex I by

$$\overline{\mu}(\mathfrak{p}_\infty; I) := \overline{\mu}(\sigma_{\mathfrak{P}}; I). \tag{3.2.11}$$

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

$$R_S^1 := \{\mathfrak{p} \in R_S \mid \mathrm{N}\mathfrak{p} \equiv 1 \bmod l\}.$$

For $\mathfrak{p} \in R_S^1$, let $e(\mathfrak{p})$ denote the maximal integer such that

$$\mathrm{N}\mathfrak{p} \equiv 1 \bmod l^{e(\mathfrak{p})}.$$

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

Remark 3.2.12. In [Ms1] and [Ms2, Chap. 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, Chap. 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], [W2], [W3], [W4]) and multiple power residue symbols (in particular, Rédei symbols), which will be discussed in a forthcoming paper.

Finally, we introduce a filtration on Gal_k using l-adic Milnor numbers. We set $\mathrm{Gal}_k^{\mathrm{Mil}}[0] := \mathrm{Gal}_k$. For each integer $n \geq 1$, we define a subset $\mathrm{Gal}_k^{\mathrm{Mil}}[n]$ of Gal_k by

$$\begin{aligned} \mathrm{Gal}_k^{\mathrm{Mil}}[n] &:= \{g \in \mathrm{Gal}_{k(\zeta_{l^\infty})} \mid \mu(g; I) = 0 \text{ for } |I| \leq n\} \\ &= \{g \in \mathrm{Gal}_{k(\zeta_{l^\infty})} \mid \deg(\Theta(y_i(g)) - 1) \geq n \text{ for } 1 \leq i \leq r\}. \end{aligned} \tag{3.2.13}$$

We then have the descending series

$$\mathrm{Gal}_k = \mathrm{Gal}_k^{\mathrm{Mil}}[0] \supset \mathrm{Gal}_k^{\mathrm{Mil}}[1] \supset \cdots \supset \mathrm{Gal}_k^{\mathrm{Mil}}[n] \supset \cdots$$

and we call it the *Milnor filtration* of Gal_k.

Proposition 3.2.14. *For $n \geq 0$, $\mathrm{Gal}_k^{\mathrm{Mil}}[n]$ is a closed normal subgroup of 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 4.3.3. So we give herewith a direct and brief proof.

We may assume $n \geq 1$. Since $\mu(\ ; I) : \mathrm{Gal}_k \to \mathbb{Z}_l$ is continuous for each I and $\mathrm{Gal}_k^{\mathrm{Mil}}[n] = \bigcap_{|I| \leq n} \mu(\ ; I)^{-1}(0)$, then $\mathrm{Gal}_k^{\mathrm{Mil}}[n]$ is closed in Gal_k. Let $g, h \in \mathrm{Gal}_k^{\mathrm{Mil}}[n]$ and so $\deg(\Theta(y_i(\rho)) - 1) \geq n$ for $\rho = g, h$ and each $1 \leq i \leq r$. Then we can easily show $\deg(\Theta(y_i(g^{-1})) - 1) \geq n$, $\deg(\Theta(y_i(gh)) - 1) \geq n$ and $\deg(\Theta(y_i(hgh^{-1})) - 1) \geq n$ by using Lemma 3.2.5(1), (2) and (3), respectively. □

§3.3. Pro-l link groups and Massey products

Following the analogy with the link group of a pure braid link ([Ar],[B, Thm. 2.2]), we define the *pro-l link group* of each Galois element $g \in \mathrm{Gal}_k$ associated to Ih_S by

$$\begin{aligned} &\Pi_S(g) \\ &:= \left\langle x_1, \ldots, x_r \mid y_1(g) x_1^{\chi_l(g)} y_1(g)^{-1} = x_1, \ldots, y_r(g) x_r^{\chi_l(g)} y_r(g)^{-1} = x_r \right\rangle \\ &= \left\langle x_1, \ldots, x_r \mid x_1^{1-\chi_l(g)}[x_1^{-1}, y_1(g)^{-1}] = \cdots = x_r^{1-\chi_l(g)}[x_r^{-1}, y_r(g)^{-1}] = 1 \right\rangle \\ &:= \mathfrak{F}_r / \mathfrak{N}_S(g), \end{aligned} \tag{3.3.1}$$

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

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

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

such that

$$\begin{cases} [\omega_{i,i+1}] = c_i & (1 \leq i \leq n), \\ dw_{ij} = \displaystyle\sum_{a=i+1}^{j-1} w_{ia} \cup w_{aj} & (j \neq i+1). \end{cases}$$

Such an array W is called a *defining system* for $\langle c_1, \dots, c_n\rangle$. The value of $\langle c_1, \dots, c_n\rangle$ 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 $\langle c_1, \dots, c_n\rangle_W$. A Massey product $\langle c_1, \dots, c_n\rangle$ itself is taken to be the subset of $H^2(\Pi_S(g), \mathbb{Z}_l/\mathfrak{a})$ consisting of elements $\langle c_1, \dots, c_n\rangle_W$ for some defining system W. By convention, $\langle c\rangle = 0$. The following lemma is a basic fact ([Kr]).

Lemma 3.3.2. *We have $\langle c_1, c_2\rangle = c_1 \cup c_2$. For $n \geq 3$, $\langle c_1, \dots, c_n\rangle$ is defined and consists of a single element if $\langle c_{j_1}, \dots, c_{j_a}\rangle = 0$ for all proper subsets $\{j_1, \dots, j_a\}$ $(a \geq 2)$ of $\{1, \dots, n\}$.*

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 γ_i the image of x_i under ψ, $\gamma_i := x_i \bmod \mathfrak{N}_S(g)$, for $1 \leq i \leq r$. By the definition (3.3.1) of $\Pi_S(g)$ and our assumption, π induces the isomorphism $\mathfrak{F}_r/\mathfrak{F}_r^{l^a}\mathfrak{F}_r(2) \xrightarrow{\sim} \Pi_S(g)/\Pi_S(g)^{l^a}[\Pi_S(g), \Pi_S(g)] \simeq (\mathbb{Z}_l/\mathfrak{a})^{\oplus r}$ and so we have the isomorphism $H^1(\Pi_S(g),\mathbb{Z}_l/\mathfrak{a}) \simeq H^1(\mathfrak{F}_r,\mathbb{Z}_l/\mathfrak{a})$. Therefore the Hochschild–Serre spectral sequence yields the isomorphism

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

Here tg is the transgression defined as follows. For $a \in H^1(\mathfrak{N}_S(g),\mathbb{Z}_l/\mathfrak{a})^{\Pi_S(g)}$, choose a 1-cochain $b \in C^1(\mathfrak{F}_r,\mathbb{Z}_l/\mathfrak{a})$ 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-cocyle $c \in Z^2(\Pi_S(g),\mathbb{Z}_l/\mathfrak{a})$ such that $\psi^*(c) = db$. Then $\mathrm{tg}(a)$ is defined to be the class of c. The dual to tg is called the Hopf isomorphism:

$$\mathrm{tg}^\vee : H_2(\Pi_S(g),\mathbb{Z}_l/\mathfrak{a}) \xrightarrow{\sim} H_1(\mathfrak{N}_S(g),\mathbb{Z}_l/\mathfrak{a})_{\Pi_S(g)} = \mathfrak{N}_S(g)/\mathfrak{N}_S(g)^{l^a}[\mathfrak{N}_S(g),\mathfrak{F}_r].$$

Then we have the following proposition (cf. [St, Lem. 1.5], [Ms1, Thm. 2.2.2]).

Proposition 3.3.3. *With notation as above, let $c_1,\dots,c_n \in H^1(\Pi_S(g),\mathbb{Z}_l/\mathfrak{a})$ and $W=(w_{ij})$ be a defining system for the Massey product $\langle c_1,\dots,c_n\rangle$. Let $f \in \mathfrak{N}_S(g)$ and set $\mathfrak{r} := (\mathrm{tg}^\vee)^{-1}(f \bmod \mathfrak{N}_S(g)^{l^a}[\mathfrak{N}_S(g),\mathfrak{F}_r])$. Then we have*

$$\langle c_1,\dots,c_n\rangle_W(\mathfrak{r}) = \sum_{j=1}^{n}(-1)^{j+1}\sum_{e_1+\cdots+e_j=n}\ \sum_{I=(i_1\cdots i_j)} w_{1,1+e_1}(\gamma_{i_1})\cdots w_{n+1-e_j,n+1}(\gamma_{i_j})\mu(I;f)_{\mathfrak{a}},$$

where $e_1,\dots,e_j$ run over positive integers satisfying $e_1+\cdots+e_j=n$ and $\mu(I;f)_{\mathfrak{a}} := \mu(I;f) \bmod \mathfrak{a}$.

Now, let $\gamma_1^*,\dots,\gamma_r^* \in H^1(\Pi_S(g),\mathbb{Z}_l/\mathfrak{a})$ be the Kronecker dual to $\gamma_1,\dots,\gamma_r$, namely, $\gamma_i^*(\gamma_j)=\delta_{ij}$ for $1 \le i,j \le r$. Let $\mathfrak{r}_i := (\mathrm{tg}^\vee)^{-1}(x_i^{1-\chi_l(g)}[x_i^{-1},y_i(g)^{-1}] \bmod \mathfrak{N}_S(g)^{l^a}[\mathfrak{N}_S(g),\mathfrak{F}_r])$ for $1 \le i \le r$. Let $I=(i_1\cdots i_n)$ be a multiindex such that $|I| = n \ge 2$. Let $g \in \mathrm{Gal}_k$. We assume the following conditions:

$$(3.3.4)\qquad \begin{cases} (1) & \mu((j_1\cdots j_a);x_i^{1-\chi_l(g)}) \equiv 0 \bmod \mathfrak{a} \text{ for any subset} \\ & \{j_1,\dots,j_a\} \text{ of } \{i_1,\dots,i_n\} \text{ and } 1 \le i \le r, \\ (2) & i_1,\dots,i_n \text{ are distinct from each other, and} \\ & \mu(g;(j_1\cdots j_a)) \equiv 0 \bmod \mathfrak{a} \text{ for any proper subset} \\ & \{j_1,\dots,j_a\} \text{ of } \{i_1,\dots,i_n\}. \end{cases}$$

We note that condition (1) is unnecessary when $g \in \mathrm{Gal}_{k(\zeta_{l^\infty})}$. The following theorem gives a cohomological interpretation of $\mu(g;I)_{\mathfrak{a}} := \mu(g;I) \bmod \mathfrak{a}$ by the Massey product in the cohomology of $\Pi_S(g)$.

Theorem 3.3.5. *With notation and assumptions as above, the Massey product* $\langle \gamma_{i_1}^*, \ldots, \gamma_{i_n}^* \rangle$ *in* $H^2(\Pi_S(g), \mathbb{Z}_l/\mathfrak{a})$ *is uniquely defined and we have*

$$\mu(g; I)_{\mathfrak{a}} = (-1)^n \langle \gamma_{i_1}^*, \ldots, \gamma_{i_n}^* \rangle (\mathfrak{r}_{i_n}).$$

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

$$\begin{aligned}&\Theta(x_i^{1-\chi_l(g)}[x_i^{-1}, y_i(g)^{-1}]) \\ &\quad = \Theta(x_i^{1-\chi_l(g)})(1 + \Theta(x_i^{-1})\Theta(y_i(g)^{-1})(\Theta(x_i y_i(g)) - \Theta(y_i(g) x_i))).\end{aligned}$$

By our assumption (3.3.4)(1), we have

$$\begin{aligned}&\mu(J; x_i^{1-\chi_l(g)}[x_i^{-1}, y_i(g)^{-1}]) \\ &\quad \equiv \mu(J; x_i y_i(g)) - \mu(J; y_i(g) x_i) \\ &\qquad + \sum_A (\mu(A; x_i y_i(g)) - \mu(A; y_i(g) x_i)) \nu_A \bmod \mathfrak{a},\end{aligned} \tag{3.3.5.1}$$

where A runs over some proper subsequences of J and $\nu_A \in \mathbb{Z}_l$. By 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

$$\begin{aligned}&\mu(J; x_i y_i(g)) - \mu(J; y_i(g) x_i) \\ &\quad = \begin{cases} \mu(g; (j_2 \cdots j_a j_1)) - \delta_{j_1, j_a} \mu(g; J) & (i = j_1), \\ \mu(g; (j_2 \cdots j_a j_1)) \delta_{j_1, j_a} - \mu(g; J) & (i = j_a), \\ 0 & (\text{otherwise}). \end{cases}\end{aligned} \tag{3.3.5.2}$$

Now, let $n = 2$. Then we have $\langle \gamma_{i_1}^*, \gamma_{i_2}^* \rangle = \gamma_{i_1}^* \cup \gamma_{i_2}^*$. By Proposition 3.3.3, (3.3.4)(2), (3.3.5.1) and (3.3.5.2), we have

$$\langle \gamma_{i_1}^*, \gamma_{i_2}^* \rangle (\mathfrak{r}_{i_2}) = -\mu(I; [x_{i_2}, y_{i_2}(g)])_{\mathfrak{a}} = \mu(g; I)_{\mathfrak{a}}.$$

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 (3.3.4)(2), (3.3.5.1) and (3.3.5.2), we have

$$\mu(J; x_i^{1-\chi_l(g)}[x_i^{-1}, y_i(g)^{-1}]) \equiv 0 \bmod \mathfrak{a}$$

for $J = (j_1 \cdots j_a)$ and $1 \leq i \leq r$. So, by Proposition 3.3.3, we have

$$\langle \gamma_{j_1}^*, \ldots, \gamma_{j_a}^* \rangle(\mathfrak{r}_i) = 0$$

for $1 \leq i \leq r$. Since $H_2(\Pi(g), \mathbb{Z}_l/\mathfrak{a})$ is generated by $x_i^{1-\chi_l(g)}[x_i, y_i(g)]$ for $1 \leq i \leq r$, we have

$$\langle c_{j_1}, \ldots, c_{j_a} \rangle = 0.$$

Therefore, by Lemma 3.3.2, the Massey product $\langle c_{i_1}, \ldots, c_{i_n} \rangle$ is uniquely defined. By Proposition 3.3.3, (3.3.4)(2), (3.3.5.1) and (3.3.5.2) again, we have

$$\langle \gamma_{i_1}^*, \ldots, \gamma_{i_n}^* \rangle(\mathfrak{r}_{i_n}) = (-1)^{n+1}\mu(I; x_n^{1-\chi_l(g)}[x_{i_n}, y_{i_n}(g)])_{\mathfrak{a}} = (-1)^n \mu(g; I)_{\mathfrak{a}}.$$

□

§4. Pro-l Johnson homomorphisms

§4.1. Some algebras associated to lower central series

For each integer $n \geq 1$, we let

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

which is a free $\mathbb{Z}_l$-module whose rank $\ell_r(n)$ is given by the Witt formula ([MKS, 5.6, Thm. 5.11], [Se, Chap. 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

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

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

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

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

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

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

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

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

$$\Theta_n : \mathrm{gr}_n(\mathbb{Z}_l[[\mathfrak{F}_r]]) \simeq H^{\otimes n} \tag{4.1.2}$$

for each $n \geq 0$ and so $\mathrm{gr}(\mathbb{Z}_l[[\mathfrak{F}_r]])$ is identified with the tensor algebra $T(H)$:

$$\mathrm{gr}(\mathbb{Z}_l[[\mathfrak{F}_r]]) = T(H) = \mathbb{Z}_l\langle X_1, \dots, X_r\rangle.$$

The composition of the map of (4.1.1) with Θ_n in (4.1.2), denoted also by $\Theta_n : \mathrm{gr}_n(\mathfrak{F}_r) \hookrightarrow H^{\otimes n}$, is the degree-$n$ part of the pro-l Magnus embedding in (3.1.3):

$$\Theta_n = (\Theta - 1)|_{\mathfrak{F}_r(n)} \bmod \widehat{T}(n+1). \tag{4.1.3}$$

Here we may note that Θ is multiplicative, $\Theta(f_1 f_2) = \Theta(f_1)\Theta(f_2)$ for $f_1, f_2 \in \mathfrak{F}_r$, while Θ_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 $\bmod\, \mathfrak{F}_r(n+1)$.

Let $S(H)$ be the symmetric algebra of H over $\mathbb{Z}_l$ and let $q : T(H) \to S(H)$ be the natural map. We let $S^m(H) := q(H^{\otimes m})$ and $u_i := q(X_i)$ for $1 \leq i \leq r$ so that $S(H)$ is the graded algebra $\bigoplus_{m\geq 0} S^m(H)$ which is nothing but the commutative polynomial algebra over $\mathbb{Z}_l$ of variables $u_1, \dots, u_r$:

$$S(H) = \bigoplus_{m\geq 0} S^m(H) = \mathbb{Z}_l[u_1, \dots, u_r].$$

§4.2. 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 [Ka] in our pro-l setting.

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

Lemma 4.2.1. *A $\mathbb{Z}_l$-algebra endomorphism φ of $\widehat{T}(H)$ is a filtration-preserving automorphism of $\widehat{T}(H)$, $\varphi \in \mathrm{Aut}^{\mathrm{fil}}(\widehat{T}(H))$ if and only if the following conditions are satisfied:*

(1) $\varphi(\widehat{T}(n)) \subset \widehat{T}(n)$ for all $n \geq 0$.

(2) the induced $\mathbb{Z}_l$-endomorphism $[\varphi]$ on $\widehat{T}(1)/\widehat{T}(2) = H$ is an isomorphism.

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widehat{T}(2) & \longrightarrow & \widehat{T}(1) & \xrightarrow{\ p\ } & H & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi|_{\widehat{T}(2)}} & & \downarrow{\scriptstyle \varphi|_{\widehat{T}(1)}} & & \downarrow{\scriptstyle [\varphi]} & & \\ 0 & \longrightarrow & \widehat{T}(2) & \longrightarrow & \widehat{T}(1) & \longrightarrow & H & \longrightarrow & 0. \end{array}$$

Since $\varphi(\widehat{T}(n)) = \widehat{T}(n)$ for all $n \geq 0$, we have $\mathrm{Coker}(\varphi|_{\widehat{T}(i)}) = 0$ for $i = 1, 2$, in particular. Since φ is an automorphism, we have $\mathrm{Ker}(\varphi) = 0$, in particular, $\mathrm{Ker}(\varphi|_{\widehat{T}(i)}) = 0$ for $i = 1, 2$. By the snake lemma applied to the above diagram, we obtain $\mathrm{Ker}([\varphi]) = 0$ and $\mathrm{Coker}([\varphi]) = 0$, hence condition (2).

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

$$z = \varphi(y). \tag{4.2.1.1}$$

Note by conditions (1) and (2) that φ induces a $\mathbb{Z}_l$-linear automorphism of $\widehat{T}(m)/\widehat{T}(m+1) = H^{\otimes m}$, 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 $i < j$, equation (4.2.1.1) is equivalent to the following system of equations:

$$\begin{cases} z_0 = \varphi(y_0) = y_0, \\ z_1 = [\varphi](y_1), \\ z_2 = [\varphi]^{\otimes 2}(y_2) + \varphi(y_1)_2, \\ \cdots \\ z_m = [\varphi]^{\otimes m}(y_m) + \varphi(y_1)_m + \cdots + \varphi(y_{m-1})_m, \\ \cdots . \end{cases} \tag{4.2.1.2}$$

Since $[\varphi]^{\otimes m}$ is an automorphism, we can find the unique solution $y = (y_m)$ of (4.2.1.2) from the lower degree. Therefore φ 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 $\varphi^{-1}(\widehat{T}(n)) \subset \widehat{T}(n)$ and so φ is filtration preserving. □

By Lemma 4.2.1, each $\varphi \in \mathrm{Aut}^{\mathrm{fil}}(\widehat{T}(H))$ induces a $\mathbb{Z}_l$-linear automorphism $[\varphi]$ of $H = \widehat{T}(1)/\widehat{T}(2)$ and so we have a group homomorphism

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

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

$$\begin{aligned}\mathrm{IA}(\widehat{T}(H)) &:= \mathrm{Ker}([\ \ ]) \\ &= \{\varphi \in \mathrm{Aut}(\widehat{T}(H)) \mid \varphi(h) \equiv h \bmod \widehat{T}(2) \text{ for any } h \in H\}.\end{aligned}$$

We note that there is a natural splitting $s : \mathrm{GL}(H) \to \mathrm{Aut}^{\mathrm{fil}}(\widehat{T}(H))$ of $[\ \ ]$, which is defined by

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

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

Lemma 4.2.2. *We have a semidirect decomposition*

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

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

$$E : \mathrm{IA}(\widehat{T}(H)) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(H, \widehat{T}(2)); \quad \varphi \mapsto \varphi|_H - \mathrm{id}_H, \tag{4.2.3}$$

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

Proposition 4.2.4. *The map E is bijective.*

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

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

$$[\varphi](h \bmod \widehat{T}(2)) = \varphi(h) \bmod \widehat{T}(2) = h + \phi(h) \bmod \widehat{T}(2) = h \bmod \widehat{T}(2),$$

we have $[\varphi] = \mathrm{id}_H$. By Lemma 4.2.1, we have $\varphi \in \mathrm{IA}(\widehat{T}(H))$ and $E(\varphi) = \phi$. □

By Lemma 4.2.2 and Proposition 4.2.4, we have the following result.

Corollary 4.2.5. *We have a bijection*

$$\hat{E} : \mathrm{Aut}^{\mathrm{fil}}(\widehat{T}(H)) \simeq \mathrm{Hom}_{\mathbb{Z}_l}(H, \widehat{T}(2)) \times \mathrm{GL}(H)$$

defined by $\hat{E}(\varphi) = (E(\varphi \circ [\varphi]^{-1}), [\varphi])$.

Now, let $\mathrm{Ih}_S : \mathrm{Gal}_k \to P(\mathfrak{F}_r)$ be the Ihara representation associated to S in (2.2.3). We recall that the correspondence $\varphi \mapsto \varphi^* := \Theta \circ \varphi \circ \Theta^{-1}$ in (3.1.8) gives the injective homomorphism $\mathrm{Aut}(\mathfrak{F}_r) \to \mathrm{Aut}^{\mathrm{fil}}(\widehat{T}(H))$ and hence the inclusion $P(\mathfrak{F}_r) \hookrightarrow \mathrm{Aut}^{\mathrm{fil}}(\widehat{T}(H))$ which satisfies $[\varphi] = [\varphi^*]$ in $\mathrm{GL}(H)$. Composing Ih_S with this inclusion, we have the homomorphism $\hat{\eta}_S : \mathrm{Gal}_k \to \mathrm{Aut}^{\mathrm{fil}}(\widehat{T}(H))$ defined by

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

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

$$\begin{aligned} \eta_S(g) := \hat{\eta}_S(g) \circ [\mathrm{Ih}_S(g)]^{-1} &= \mathrm{Ih}_S(g)^* \circ [\mathrm{Ih}_S(g)]^{-1} \\ &= \Theta \circ \mathrm{Ih}_S(g) \circ \Theta^{-1} \circ [\mathrm{Ih}_S(g)]^{-1}. \end{aligned} \tag{4.2.6}$$

Thus, we have $\hat{\eta}_S(g) = (\eta_S(g), [\mathrm{Ih}_S(g)])$ for $g \in \mathrm{Gal}_k$ under the semidirect decomposition $\mathrm{Aut}^{\mathrm{fil}}(\widehat{T}(H)) = \mathrm{IA}(\widehat{T}(H)) \rtimes \mathrm{GL}(H)$ of Lemma 4.2.2.

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

$$\tau_S : \mathrm{Gal}_k \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(H, \widehat{T}(2))$$

by composing η_S with E in (4.2.3), and define the *extended pro-l Johnson map*

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

by composing $\hat{\eta}_S$ with $\hat{E}$ of Corollary 4.2.5. So we have, for $g \in \mathrm{Gal}_k$,

$$\begin{aligned} \tau_S(g) &:= E(\eta_S(g)) = \eta_S(g)|_H - \mathrm{id}_H \\ &= \mathrm{Ih}_S(g)^* \circ [\mathrm{Ih}_S(g)]^{-1}|_H - \mathrm{id}|_H \\ &= \Theta \circ \mathrm{Ih}_S(g) \circ \Theta^{-1} \circ [\mathrm{Ih}_S(g)]^{-1}|_H - \mathrm{id}|_H, \\ \hat{\tau}_S(g) &:= (\tau_S(g), [\mathrm{Ih}_S(g)]). \end{aligned} \tag{4.2.7}$$

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

$$\tau_S^{(m)} : \mathrm{Gal}_k \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)})$$

by the mth component of τ_S:

$$\tau_S(g) := \sum_{m \geq 1} \tau_S^{(m)}(g) \quad (g \in \mathrm{Gal}_k). \tag{4.2.8}$$

We note that the pro-l Johnson map τ_S is no longer a homomorphism. In fact, we have the following proposition.

Proposition 4.2.9. *For $g_1, g_2 \in \mathrm{Gal}_k$, we have*

$$\eta_S(g_1g_2) = \eta_S(g_1) \circ [\mathrm{Ih}_S(g_1)] \circ \eta_S(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1}.$$

Proof. By (4.2.6), we have

$$\begin{aligned}\eta_S(g_1g_2) &= \mathrm{Ih}_S(g_1g_2)^* \circ [\mathrm{Ih}_S(g_1g_2)]^{-1} \\ &= \Theta \circ \mathrm{Ih}_S(g_1g_2) \circ \Theta^{-1} \circ [\mathrm{Ih}_S(g_1g_2)]^{-1} \\ &= \Theta \circ \mathrm{Ih}_S(g_1) \circ \mathrm{Ih}_S(g_2) \circ \Theta^{-1} \circ [\mathrm{Ih}_S(g_2)]^{-1} \circ [\mathrm{Ih}_S(g_1)]^{-1} \\ &= \Theta \circ \mathrm{Ih}_S(g_1) \circ \Theta^{-1} \circ [\mathrm{Ih}_S(g_1)]^{-1} \circ [\mathrm{Ih}_S(g_1)] \circ \Theta \circ \mathrm{Ih}_S(g_2) \circ \Theta^{-1} \\ &\quad \circ [\mathrm{Ih}_S(g_2)]^{-1} \circ [\mathrm{Ih}_S(g_1)]^{-1} \\ &= \eta_S(g_1) \circ [\mathrm{Ih}_S(g_1)] \circ \eta_S(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1}.\end{aligned}$$

□

Proposition 4.2.9 yields coboundary relations among $\tau_S^{(m)}$. Here we give the formulas only for $\tau_S^{(1)}$ and $\tau_S^{(2)}$.

Proposition 4.2.10. *For $g_1, g_2 \in \mathrm{Gal}_k$, we have*

$$\begin{aligned}\tau_S^{(1)}(g_1g_2) &= \tau_S^{(1)}(g_1) + [\mathrm{Ih}_S(g_1)]^{\otimes 2} \circ \tau_S^{(1)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1}, \\ \tau_S^{(2)}(g_1g_2) &= \tau_S^{(2)}(g_1) + (\tau_S^{(1)}(g_1) \otimes \mathrm{id}_H + \mathrm{id}_H \otimes \tau_S^{(1)}(g_1)) \circ [\mathrm{Ih}_S(g_1)]^{\otimes 2} \\ &\qquad \circ \tau_S^{(1)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1} + [\mathrm{Ih}_S(g_1)]^{\otimes 3} \circ \tau_S^{(2)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1}.\end{aligned}$$

Proof. By definition (4.2.8), we have

$$\tau_S(g_1g_2) = \sum_{m\geq 1} \tau_S^{(m)}(g_1g_2). \tag{4.2.10.1}$$

On the other hand, by Proposition 4.2.9 and (4.2.7), we have, for $h \in H$,

$$\begin{aligned}\tau_S(g_1g_2)(h) &= -h + \eta_S(g_1g_2)(h) \\ &= -h + (\eta_S(g_1) \circ [\mathrm{Ih}_S(g_1)] \circ \eta_S(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h) \\ &= -h + (\eta_S(g_1) \circ [\mathrm{Ih}_S(g_1)] \circ (\mathrm{id}_H + \tau_S(g_2)))([\mathrm{Ih}_S(g_1)]^{-1}(h)) \\ &= -h + (\eta_S(g_1) \circ [\mathrm{Ih}_S(g_1)]) \\ &\quad \times \left([\mathrm{Ih}_S(g_1)]^{-1}(h) + \sum_{m\geq 1} (\tau_S^{(m)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h)\right) \\ &= -h + \eta_S(g_1)\left(h + \sum_{m\geq 1} ([\mathrm{Ih}_S(g_1)]^{\otimes m+1} \circ \tau_S^{(m)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h)\right)\end{aligned}$$

$$
\begin{aligned}
&= -h + \eta_S(g_1)(h) \\
&\quad + \eta_S(g_1)(([\mathrm{Ih}_S(g_1)]^{\otimes 2} \circ \tau_S^{(1)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h)) \\
&\quad + \eta_S(g_1)(([\mathrm{Ih}_S(g_1)]^{\otimes 3} \circ \tau_S^{(2)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h)) \bmod \widehat{T}(4).
\end{aligned}
$$

We note that

$$\eta_S(g)|_{H^{\otimes m}} = (\mathrm{id}_H + \tau_S(g))^{\otimes m} : H^{\otimes m} \longrightarrow H \times \widehat{T}(2m)$$

for any $g \in \mathrm{Gal}_k$ and so we have the following congruences $\bmod\, \widehat{T}(4)$:

$$\eta_S(g_1)(h) \equiv h + \tau_S^{(1)}(g_1)(h) + \tau_S^{(2)}(g_1)(h),$$

$$
\begin{aligned}
&\eta_S(g_1)(([\mathrm{Ih}_S(g_1)]^{\otimes 2} \circ \tau_S^{(1)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h)) \\
&\quad \equiv ([\mathrm{Ih}_S(g_1)]^{\otimes 2} \circ \tau_S^{(1)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h) \\
&\qquad + ((\tau_S^{(1)}(g_1) \otimes \mathrm{id}_H + \mathrm{id}_H \otimes \tau_S^{(1)}(g_1)) \circ [\mathrm{Ih}_S(g_1)]^{\otimes 2} \circ \tau_S^{(1)}(g_2) \\
&\qquad \circ [\mathrm{Ih}_S(g_1)]^{-1})(h),
\end{aligned}
$$

$$
\begin{aligned}
&\eta_S(g_1)(([\mathrm{Ih}_S(g_1)]^{\otimes 3} \circ \tau_S^{(1)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h)) \\
&\quad \equiv ([\mathrm{Ih}_S(g_1)]^{\otimes 3} \circ \tau_S^{(2)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h).
\end{aligned}
$$

Therefore we have

$$
\begin{aligned}
\tau_S(g_1 g_2)(h) &\equiv \tau_S^{(1)}(g_1)(h) + \tau_S^{(2)}(g_1)(h) \\
&\quad + ([\mathrm{Ih}_S(g_1)]^{\otimes 2} \circ \tau_S^{(1)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h) \\
&\quad + ((\tau_S^{(1)}(g_1) \otimes \mathrm{id}_H + \mathrm{id}_H \otimes \tau_S^{(1)}(g_1)) \circ [\mathrm{Ih}_S(g_1)]^{\otimes 2} \\
&\quad \circ \tau_S^{(1)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h) \\
&\quad + ([\mathrm{Ih}_S(g_1)]^{\otimes 3} \circ \tau_S^{(2)}(g_2) \circ [\mathrm{Ih}_S(g_1)]^{-1})(h) \bmod \widehat{T}(4).
\end{aligned}
\tag{4.2.10.2}
$$

Comparing (4.2.10.1) and (4.2.10.2), we obtain the assertions. □

§4.3. Pro-l Johnson homomorphisms

For $n \geq 0$, let $\pi_n : \mathfrak{F}_r \to \mathfrak{F}_r/\mathfrak{F}_r(n+1)$ be the natural homomorphism. Since each $\mathfrak{F}_r(n)$ is a characteristic subgroup of $\mathfrak{F}_r$, π_n induces the natural homomorphism $\pi_{n*} : P(\mathfrak{F}_r) \hookrightarrow \mathrm{Aut}(\mathfrak{F}_r) \to \mathrm{Aut}(\mathfrak{F}_r/\mathfrak{F}_r(n+1))$. Let $\mathrm{Ih}_S^{(n)}$ denote the composite of Ih_S with π_{n*}:

$$\mathrm{Ih}_S^{(n)} : \mathrm{Gal}_k \longrightarrow \mathrm{Aut}(\mathfrak{F}_r/\mathfrak{F}_r(n+1)).$$

In particular, $\mathrm{Ih}_S^{(1)}(g) = [\mathrm{Ih}_S(g)]$ for $g \in \mathrm{Gal}_k$. Let $\mathrm{Gal}_k^{\mathrm{Joh}}[n]$ denote the kernel of $\mathrm{Ih}_S^{(n)}$:

$$\begin{aligned}\mathrm{Gal}_k^{\mathrm{Joh}}[n] &:= \mathrm{Ker}(\mathrm{Ih}_S^{(n)}) \\ &= \{g \in \mathrm{Gal}_k \mid \mathrm{Ih}_S(g)(f)f^{-1} \in \mathfrak{F}_r(n+1) \text{ for all } f \in \mathfrak{F}_r\}.\end{aligned} \tag{4.3.1}$$

We then have a descending series of closed normal subgroups of Gal_k:

$$\mathrm{Gal}_k = \mathrm{Gal}_k^{\mathrm{Joh}}[0] \supset \mathrm{Gal}_k^{\mathrm{Joh}}[1] \supset \cdots \supset \mathrm{Gal}_k^{\mathrm{Joh}}[n] \supset \cdots$$

and we call it the *Johnson filtration* of Gal_k associated to the Ihara representation φ_S (cf. [Aa], [J1], [J2]). We note by Theorem 2.2.6(1),

$$\mathrm{Gal}_k^{\mathrm{Joh}}[1] = \mathrm{Ker}(\mathrm{Ih}_S^{(1)} : \mathrm{Gal}_k \to \mathrm{GL}(H)) = \mathrm{Gal}_{k(\zeta_{l^\infty})}. \tag{4.3.2}$$

The relation with the Milnor filtration defined in (3.2.13) is given as follows.

Proposition 4.3.3. *The Johnson filtration coincides with the Milnor filtration, namely, for each $n \geq 0$, we have*

$$\mathrm{Gal}_k^{\mathrm{Joh}}[n] = \mathrm{Gal}_k^{\mathrm{Mil}}[n].$$

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

$$\begin{aligned} g \in \mathrm{Gal}_k^{\mathrm{Joh}}[n] &\Leftrightarrow \mathrm{Ih}_S(g)(x_i)x_i^{-1} \in \mathfrak{F}_r(n+1) \text{ for all } 1 \leq i \leq r \\ &\Leftrightarrow y_i(g)x_iy_i(g)^{-1}x_i^{-1} \in \mathfrak{F}_r(n+1) \text{ for all } 1 \leq i \leq r \\ &\Leftrightarrow y_i(g) \in \mathfrak{F}_r(n) \text{ for all } 1 \leq i \leq r \\ &\Leftrightarrow \deg(\Theta(y_i(g)-1)) \geq n \text{ for all } 1 \leq i \leq r \\ &\Leftrightarrow g \in \mathrm{Gal}_k^{\mathrm{Mil}}[n]. \end{aligned}$$

□

Note that Proposition 4.3.3 yields Proposition 3.2.14. In the following, we simply write $\mathrm{Gal}_k[n]$ for the nth 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 $\mathrm{Gal}_k[n]$. By (4.3.2), we have $k[1] = k(\zeta_{l^\infty})$.

We give some basic properties of the Johnson filtration. The following Lemma 4.3.4, Proposition 4.3.5 and Theorem 4.3.6(2) were shown by Ihara for the case $r = 2$. See [Ih1, Prop. 7, p. 59] and also [O1]. We give, herewith, concise proofs for the sake of readers.

Lemma 4.3.4. *For $g \in \mathrm{Gal}_k[m]$ $(m \geq 0)$ and $f \in \mathfrak{F}_r(n)$ $(n \geq 1)$, we have*

$$\mathrm{Ih}_S(g)(f)f^{-1} \in \mathfrak{F}_r(m+n).$$

Proof. We fix $m \geq 0$ and $g \in \mathrm{Gal}_k[m]$. We prove the assertion by induction on n. For $n = 1$, the assertion $\mathrm{Ih}_S(g)(f)f^{-1} \in \mathfrak{F}_r(m+1)$ is true by the definition (4.3.1). Assume that

$$\mathrm{Ih}_S(g)(f)f^{-1} \in \mathfrak{F}_r(m+i) \quad \text{if } f \in \mathfrak{F}_r(i) \text{ and } 1 \leq i \leq n. \tag{4.3.4.1}$$

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

$$\mathrm{Ih}_S(g)(f)f^{-1} \in \mathfrak{F}_r(m+n+1) \quad \text{for } f \in [\mathfrak{F}_r(n),\ \mathfrak{F}_r]_{\mathrm{abst}}.$$

For this, we have only to show

$$\mathrm{Ih}_S(g)([b,c])[b,c]^{-1} \in \mathfrak{F}_r(m+n+1) \quad \text{if } b \in \mathfrak{F}_r(n),\ c \in \mathfrak{F}_r. \tag{4.3.4.2}$$

For simplicity, we shall use the notation $[\varphi, x] := \psi(x)x^{-1}$ and $[x, \varphi] := x\varphi(x)^{-1}$ for $x \in \mathfrak{F}_r$ and $\varphi \in \mathrm{Aut}(\mathfrak{F}_r)$. By the "three subgroup lemma" and the induction hypothesis (4.3.4.1), we have

$$\begin{aligned}
\mathrm{Ih}_S(g)([b,c])[b,c]^{-1} &= [\mathrm{Ih}_S(g), [b,c]] \\
&\in [\mathrm{Ih}_S(g), [\mathfrak{F}_r(n), \mathfrak{F}_r]] \\
&\subset [[\mathrm{Ih}_S(g), \mathfrak{F}_r(n)], \mathfrak{F}_r][[\mathfrak{F}_r, \mathrm{Ih}_S(g)], \mathfrak{F}_r(n)] \\
&\subset [\mathfrak{F}_r(m+n), \mathfrak{F}_r][\mathfrak{F}_r(m+1), \mathfrak{F}_r(n)] \\
&= \mathfrak{F}_r(m+n+1)
\end{aligned}$$

and our claim (4.3.4.2) follows. □

Lemma 4.3.4 yields the following proposition.

Proposition 4.3.5. *For $m, n \geq 0$, we have*

$$[\mathrm{Gal}_k[m], \mathrm{Gal}_k[n]] \subset \mathrm{Gal}_k[m+n] \quad \textit{for } m, n \geq 0.$$

In particular, the Johnson (or Milnor) filtration is a central series.

Proof. With the same notation as in the proof of (4.3.4.2) and Lemma 4.3.4, we have

$$\begin{aligned}
&[[\mathrm{Gal}_k[n], \mathfrak{F}_r], \mathrm{Gal}_k[m]] \subset [\mathfrak{F}_r[n+1], \mathrm{Gal}_k[m]] \subset \mathfrak{F}_r[m+n+1], \\
&[[\mathfrak{F}_r, \mathrm{Gal}_k[m]], \mathrm{Gal}_k[n]] \subset [\mathfrak{F}_r(m+1), \mathrm{Gal}_k[n]] \subset \mathfrak{F}_r(m+n+1).
\end{aligned}$$

By the three subgroup lemma, we have

$$\begin{aligned}
[[\mathrm{Gal}_k[m], \mathrm{Gal}_k[n]], \mathfrak{F}_r] &\subset [[\mathrm{Gal}_k[n], \mathfrak{F}_r], \mathrm{Gal}_k[m]][[\mathfrak{F}_r, \mathrm{Gal}_k[m]], \mathrm{Gal}_k[n]] \\
&\subset \mathfrak{F}_r(m+n+1),
\end{aligned}$$

which yields the assertion by the definition (4.3.1). □

For $n \geq 0$, let

$$\mathrm{gr}_n(\mathrm{Gal}_k) := \mathrm{Gal}_k[n]/\,\mathrm{Gal}_k[n+1],$$

which is a $\mathbb{Z}_l$-module. Then, by Proposition 4.3.5, the graded $\mathbb{Z}_l$-module

$$\mathrm{gr}(\mathrm{Gal}_k) := \bigoplus_{n \geq 0} \mathrm{gr}_n(\mathrm{Gal}_k)$$

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

$$[a, b] := [g, h] \bmod \mathrm{Gal}_k[m+n+1].$$

Now, for $m \geq 1$, we let $\tau_S^{[m]}$ denote the restriction of the mth l-adic Johnson map $\tau_S^{(m)}$ in (4.2.8) to $\mathrm{Gal}_k[m]$:

$$\tau_S^{[m]} := \tau_S^{(m)}|_{\mathrm{Gal}_k[m]} : \mathrm{Gal}_k[m] \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)}).$$

The following theorem asserts that $\tau_S^{[m]}$ describes the action of $\mathrm{Gal}_k[m]$ on $\mathfrak{F}_r/\mathfrak{F}_r(m+2)$.

Theorem 4.3.6. *With notation as above, the following assertions hold.*

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

$$\tau_S^{[m]}(g)([f]) = \Theta_{m+1}(\mathrm{Ih}_S(g)(f)f^{-1}),$$

where $\Theta_{m+1} : \mathrm{gr}_{m+1}(\mathfrak{F}_r) \hookrightarrow H^{\otimes(m+1)}$ is the degree-$(m+1)$ part of the Magnus embedding in (4.1.3).

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

$$\mathrm{gr}_m(\mathrm{Gal}_k) \simeq \mathbb{Z}_l^{\oplus r_m}$$

for some integer $r_m \geq 0$.

Proof. (1) We need to show that for $g \in \mathrm{Gal}_k[m]$,

$$\tau_S^{(m)}(g)(X_i) = \Theta_{m+1}(\mathrm{Ih}_S(g)(x_i)x_i^{-1}) \quad 1 \leq i \leq r. \tag{4.3.6.1}$$

By (4.2.7) and $[\mathrm{Ih}_S(g)] = \mathrm{id}_H$, we have

$$\begin{aligned}\tau_S(g)(X_i) &= (\Theta \circ \mathrm{Ih}_S(g) \circ \Theta^{-1})(\Theta(x_i) - 1) - (\Theta(x_i) - 1) \\ &= \Theta(\mathrm{Ih}_S(g)(x_i)) - \Theta(x_i).\end{aligned}$$

Therefore, by (4.2.8), we have

(4.3.6.2) $\tau_S^{(m)}(g)(X_i) =$ the component in $H^{\otimes(m+1)}$ of $\Theta(\mathrm{Ih}_S(g)(x_i)) - \Theta(x_i)$.

On the other hand, since $\mathrm{Ih}_S(g)(x_i)x_i^{-1} \in \mathfrak{F}_r(m+1)$, we have

$$\Theta(\mathrm{Ih}_S(g)(x_i)x_i^{-1}) \equiv 1 + \Theta_{m+1}(\mathrm{Ih}_S(g)(x_i)x_i^{-1}) \bmod \widehat{T}(m+2).$$

Multiplying the above equation by $\Theta(x_i)$ from the right, we have

(4.3.6.3) $$\Theta(\mathrm{Ih}_S(g)(x_i)) \equiv \Theta(x_i) + \Theta_{m+1}(\mathrm{Ih}_S(g)(x_i)x_i^{-1}) \bmod \widehat{T}(m+2).$$

By (4.3.6.2) and (4.3.6.3), we obtain (4.3.6.1).

(2) By (1), for $g, h \in \mathrm{Gal}_k[m]$ and $f \in \mathfrak{F}_r$, we have

$$\begin{aligned}\tau_S^{[m]}(gh)([f]) &= \Theta_{m+1}(\mathrm{Ih}_S(gh)(f)f^{-1})\\ &= \Theta_{m+1}(\mathrm{Ih}_S(g)(\mathrm{Ih}_S(h)(f))f^{-1})\\ &= \Theta_{m+1}(\mathrm{Ih}_S(g)(\mathrm{Ih}_S(h)(f)f^{-1})\,\mathrm{Ih}_S(g)(f)f^{-1}).\end{aligned}$$

Since $\mathrm{Ih}_S(h)(f)f^{-1} \in \mathfrak{F}_r(m+1)$, we have $\mathrm{Ih}_S(g)(\mathrm{Ih}_S(h)(f)f^{-1}) \equiv \mathrm{Ih}_S(h)(f)f^{-1} \bmod \mathfrak{F}_r(2m+1)$ $(\subset \mathfrak{F}_r(m+2))$ by Lemma 4.3.4, and hence

$$\begin{aligned}\tau_S^{[m]}(gh)([f]) &= \Theta_{m+1}(\mathrm{Ih}_S(g)(f)f^{-1}) + \Theta_{m+1}(\mathrm{Ih}_S(h)(f)f^{-1})\\ &= (\tau_S^{[m]}(g) + \tau_S^{[m]}(h))([f])\end{aligned}$$

for any $f \in \mathfrak{F}_r$. Since Ih_S is continuous, we see that $\tau_S^{[m]}$ is a $\mathbb{Z}_l$-homomorphism. By (1) and (4.3.1), $\mathrm{Ker}(\tau_S^{[m]}) = \mathrm{Gal}_k[m+1]$, and hence $\tau_S^{[m]}$ induces the injective $\mathbb{Z}_l$-homomorphism $\mathrm{gr}_m(\mathrm{Gal}_k) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)})$. Since $\mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)})$ is a free $\mathbb{Z}_l$-module of finite rank, the last assertion follows. □

By Theorem 4.3.6(1), $\tau_S^{[m]}$ factors through $\mathrm{Hom}_{\mathbb{Z}_l}(H, \mathrm{gr}_{m+1}(\mathfrak{F}_r))$,

$$\tau_S^{[m]} : \mathrm{Gal}_k[m] \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(H, \mathrm{gr}_{m+1}(\mathfrak{F}_r)); \quad g \mapsto ([f] \mapsto \mathrm{Ih}_S(g)(f)f^{-1})$$

followed by the map $\mathrm{Hom}_{\mathbb{Z}_l}(H, \mathrm{gr}_{m+1}(\mathfrak{F}_r)) \to \mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)})$ induced by Θ_{m+1}. We call $\tau_S^{[m]} : \mathrm{Gal}_k[m] \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)})$ $(m \geq 1)$ or the induced injective $\mathbb{Z}_l$-homomorphism $\mathrm{gr}_m(\mathrm{Gal}_k) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)})$, denoted by the same $\tau_S^{[m]}$, the *mth pro-l Johnson homomorphism*.

A relation between the mth pro-l Johnson homomorphisms and l-adic Milnor numbers in Section 3 is given as follows.

Theorem 4.3.7. *For $g \in \mathrm{Gal}_k[m]$ $(m \geq 1)$, we have*

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

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

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

Proof. By Theorem 4.3.6(1), we have

$$\begin{aligned} \tau_S^{[m]}(g)(X_i) = \Theta_{m+1}(\mathrm{Ih}_S(g)(x_i)x_i^{-1}) &= \Theta_{m+1}(y_i(g)x_i y_i(g)^{-1}x_i^{-1}) \\ &= -\Theta_{m+1}([x_i, y_i(g)]) \\ &= -\sum_{|J|=m+1} \mu(J; [x_i, y_i(g)]) X_J. \end{aligned} \tag{4.3.7.1}$$

By the computation in the proof of Proposition 3.3.3 we have, for $|J|{=}(j_1 \cdots j_{m+1})$,

$$\begin{aligned} \mu(J; [x_i, y_i(g)]) &= \mu(J; x_i y_i(g)) - \mu(J; y_i(g) x_i) \\ &= \begin{cases} \mu(g; j_2 \cdots j_{m+1} j_1) - \delta_{j_1, j_{m+1}} \mu(g; J) & (i = j_1), \\ \mu(g; j_2 \cdots j_{m+1} j_1) \delta_{j_1, j_{m+1}} - \mu(g; J) & (i = j_{m+1}), \\ 0 & (\text{otherwise}). \end{cases} \end{aligned} \tag{4.3.7.2}$$

By (4.3.7.1) and (4.3.7.2), the assertion follows. □

Remark 4.3.8. 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, Chap. 1] for pure braids.

We compute the pro-l Johnson homomorphisms on commutators.

Proposition 4.3.9. *For* $g \in \mathrm{Gal}_k[m], h \in \mathrm{Gal}_k[n]$ $(m, n \geq 0)$ *and* $f \in \mathfrak{F}_r$*, we have*

$$\begin{aligned} \tau_S^{[m+n]}([g,h])([f]) = \Theta_{m+n+1}(&\mathrm{Ih}_S(g)(\mathrm{Ih}_S(h)(f)f^{-1})(\mathrm{Ih}_S(h)(f)f^{-1})^{-1} \\ &- \mathrm{Ih}_S(h)(\mathrm{Ih}_S(g)(f)f^{-1})(\mathrm{Ih}_S(g)(f)f^{-1})^{-1}). \end{aligned}$$

Proof. For simplicity, we set $\psi := \mathrm{Ih}_S(g), \phi := \mathrm{Ih}_S(h)$. By a straightforward computation using $[g,h] \in \mathrm{Gal}_k[m+n]$ (Proposition 4.3.5) and $\psi(f)f^{-1} \in \mathfrak{F}_r(m+1)$ (Lemma 4.3.4), we obtain

$$\begin{aligned} &[\psi, \phi](f)f^{-1} \\ &\quad = [\psi, \phi]((\phi(f)f^{-1})^{-1}) \cdot (\psi\phi\psi^{-1})((\psi(f)f^{-1})^{-1}) \cdot \psi(\phi(f)f^{-1}) \cdot \psi(f)f^{-1} \\ &\quad \equiv (\phi(f)f^{-1})^{-1} \cdot \phi((\psi(f)(f^{-1}))^{-1}) \cdot \psi(\phi(f)f^{-1}) \\ &\qquad \cdot \psi(f)f^{-1} \bmod \mathfrak{F}_r(m+n+2). \end{aligned}$$

Since $\psi(f)f^{-1} \in \mathfrak{F}_r(m+1), \phi(f)f^{-1} \in \mathfrak{F}_r(n+1)$ and $[\mathfrak{F}_r(m+1), \mathfrak{F}_r(n+1)] \subset \mathfrak{F}(m+n+2)$, we have

$$\begin{aligned}[\psi,\phi](f)f^{-1} \equiv (\phi(f)f^{-1})^{-1} \cdot \psi(\phi(f)f^{-1}) \cdot \phi((\psi(f)f^{-1})^{-1}) \\ \cdot \psi(f)f^{-1} \bmod \mathfrak{F}_r(m+n+2).\end{aligned}$$

Since we easily see that

$$\begin{cases}(\phi(f)f^{-1})^{-1}\psi(\phi(f)f^{-1}) \equiv \psi(\phi(f)f^{-1})(\phi(f)f^{-1})^{-1} & \bmod \mathfrak{F}_r(m+n+2),\\ \phi((\psi(f)f^{-1})^{-1}) \cdot \psi(f)f^{-1} \equiv (\phi(\psi(f)f^{-1}) \cdot (\psi(f)f^{-1})^{-1})^{-1} & \bmod \mathfrak{F}_r(m+n+2),\end{cases}$$

we obtain the assertion. □

By Proposition 4.3.9, the direct sum of Johnson homomorphisms $\tau_S^{[m]}$ over all $m \geq 1$ defines a graded Lie algebra homomorphism from $\mathrm{gr}(\mathrm{Gal}_k)$ to the derivation algebra of $\mathrm{gr}(\mathfrak{F}_r)$ as follows. Recall that a $\mathbb{Z}_l$-linear endomorphism δ of $\mathrm{gr}(\mathfrak{F}_r)$ is called a *derivation* on $\mathrm{gr}(\mathfrak{F}_r)$ if it satisfies

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

Let $\mathrm{Der}(\mathrm{gr}(\mathfrak{F}_r))$ denote the associative $\mathbb{Z}_l$-algebra of all derivations on $\mathrm{gr}(\mathfrak{F}_r)$ 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 $\delta, \delta' \in \mathrm{Der}(\mathrm{gr}(\mathfrak{F}_r))$. For $m \geq 0$, we define the subspace $\mathrm{Der}_m(\mathrm{gr}(\mathfrak{F}_r))$ of $\mathrm{Der}(\mathrm{gr}(\mathfrak{F}_r))$, the degree-$m$ part, by

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

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

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

A derivation $\delta \in \mathrm{Der}_m(\mathrm{gr}(\mathfrak{F}_r))$ is called a *special derivation* if there are $Y_i \in \mathrm{gr}_m(\mathfrak{F}_r)$ 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* ([Ih4, §2]). It is easy to see that normalized special derivations form a graded Lie subalgebra

$$\mathrm{Der}^{\mathrm{n.s}}(\mathrm{gr}(\mathfrak{F}_r)) = \bigoplus_{m \geq 0} \mathrm{Der}^{\mathrm{n.s}}_m(\mathrm{gr}(\mathfrak{F}_r))$$

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

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

Hence we have the inclusions

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

where $\mathrm{Der}_+(\mathrm{gr}(\mathfrak{F}_r))$ (resp. $\mathrm{Der}_+^{\mathrm{n.s}}(\mathrm{gr}(\mathfrak{F}_r))$) is the Lie subalgebra of $\mathrm{Der}(\mathrm{gr}(\mathfrak{F}_r))$ (resp. $\mathrm{Der}^{\mathrm{n.s}}(\mathrm{gr}(\mathfrak{F}_r))$) 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 4.3.10. *The direct sum of $\tau_S^{[m]}$ over $m \geq 1$ defines the Lie algebra homomorphism*

$$\mathrm{gr}(\tau) := \bigoplus_{m\geq 1} \tau_S^{[m]} : \mathrm{gr}(\mathrm{Gal}_k) \longrightarrow \mathrm{Der}_+^{\mathrm{n.s}}(\mathrm{gr}(\mathfrak{F}_r)).$$

Proof (Cf. [Da, Prop. 3.18]). By Theorem 4.3.6(1), it suffices to show that for $g \in \mathrm{Gal}_k[m]$, the map $f \mapsto \mathrm{Ih}_S(g)(f)f^{-1}$ is indeed a special derivation on $\mathrm{gr}(\mathfrak{F}_r)$. This was shown in [Ih4, §2] for the case $r = 2$. We give, herewith, a proof for the sake of readers. Let $g \in \mathrm{Gal}_k[m]$ $(m \geq 1)$ and $s \in \mathfrak{F}_r(i), h \in \mathfrak{F}_r(j)$. By using the commutator formulas

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

we have

$$\begin{aligned}
&\mathrm{Ih}_S(g)([s,t])[s,t]^{-1}\\
&\quad = [\mathrm{Ih}_S(g)(s), \mathrm{Ih}_S(g)(t)][s,t]^{-1}\\
&\quad = [ss^{-1}\,\mathrm{Ih}_S(g)(s), \mathrm{Ih}_S(g)(t)t^{-1}t][s,t]^{-1}\\
&\quad = s[s^{-1}\,\mathrm{Ih}_S(g)(s), \mathrm{Ih}_S(g)(t)t^{-1}] \cdot (\mathrm{Ih}_S(g)(t)t^{-1})[s^{-1}\,\mathrm{Ih}_S(g)(s), t]\\
&\qquad \cdot (\mathrm{Ih}_S(g)(t)t^{-1})^{-1}s^{-1}[s, \mathrm{Ih}_S(g)(t)t^{-1}](\mathrm{Ih}_S(g)(t)t^{-1})[s,t]\\
&\qquad \cdot (\mathrm{Ih}_S(g)(t)t^{-1})^{-1}[s,t]^{-1}\\
&\quad = s[s^{-1}\,\mathrm{Ih}_S(g)(s), \mathrm{Ih}_S(g)(t)t^{-1}] \cdot (\mathrm{Ih}_S(g)(t)t^{-1})[s^{-1}\,\mathrm{Ih}_S(g)(s), t]\\
&\qquad \cdot (\mathrm{Ih}_S(g)(t)t^{-1})^{-1}s^{-1}[s, \mathrm{Ih}_S(g)(t)t^{-1}][\mathrm{Ih}_S(g)(t)t^{-1}, [s,t]].
\end{aligned}$$

Since $s^{-1}\,\mathrm{Ih}_S(g)(s) \in \mathfrak{F}_r(i+m), \mathrm{Ih}_S(g)(t)t^{-1} \in \mathfrak{F}_r(j+m)$ by Lemma 4.3.4, we have

$$\begin{aligned}
[s^{-1}\,\mathrm{Ih}_S(g)(s), \mathrm{Ih}_S(g)(t)t^{-1}] &\in \mathfrak{F}_r(i+j+2m),\\
[\mathrm{Ih}_S(g)(t)t^{-1}, [s,t]] &\in \mathfrak{F}_r(i+2j+m).
\end{aligned}$$

By these claims together, we obtain

$$\mathrm{Ih}_S(g)([s,t])[s,t]^{-1} \equiv s\,\mathrm{Ih}_S(g)(t)t^{-1}[s^{-1}\,\mathrm{Ih}_S(g)(s),t](s\,\mathrm{Ih}_S(g)(t)t^{-1})^{-1} \cdot [s,\mathrm{Ih}_S(g)(t)t^{-1}] \bmod \mathfrak{F}_r(i+j+m+1).$$

Noting that $x[s^{-1}\,\mathrm{Ih}_S(g)(s),t]x^{-1} \equiv [s^{-1}\,\mathrm{Ih}_S(g)(s),t] \bmod \mathfrak{F}_r(i+j+m+1)$ for $x \in \mathfrak{F}_r$, we proved that $f \mapsto \mathrm{Ih}_S(g)(f)f^{-1}$ is a derivation. That it is special and normalized follows from $\mathrm{Ih}_S(g)(x_i) = y_i(g)x_iy_i(g)^{-1}$ $(1 \le i \le r)$ and $\mathrm{Ih}_S(g)(x_1\cdots x_r) = x_1\cdots x_r$ for $g \in \mathrm{Gal}_k[m]$ $(m \ge 1)$. □

Finally we introduce an analogue of the Morita trace map ([Mt1, 6]). For each $m \ge 1$, we identify $\mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)})$ with $H^* \otimes_{\mathbb{Z}_l} H^{\otimes(m+1)}$, where $H^* := \mathrm{Hom}_{\mathbb{Z}_l}(H,\mathbb{Z}_l)$ is the dual $\mathbb{Z}_l$-module, and let

$$c_{m+1} : \mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)}) = H^* \otimes_{\mathbb{Z}_l} H^{\otimes(m+1)} \longrightarrow H^{\otimes m}$$

be the contraction at the $(m+1)$-component defined by

$$c_{m+1}(\phi \otimes h_1 \otimes \cdots \otimes h_{m+1}) := \phi(h_{m+1})h_1 \otimes \cdots \otimes h_m \tag{4.3.11}$$

for $\phi \in H^*, h_i \in H$. We then define the *mth pro-l Morita trace map*

$$\mathrm{Tr}^{[m]} : \mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)}) \longrightarrow S^m(H) \tag{4.3.12}$$

by the composite map $q \circ c_{m+1}$.

§5. Pro-l Magnus–Gassner cocycles

§5.1. Pro-l Fox free derivation

The *pro-l Fox free derivative* $\frac{\partial}{\partial x_j} : \mathbb{Z}_l[[\mathfrak{F}_r]] \to \mathbb{Z}_l[[\mathfrak{F}_r]]$ $(1 \le j \le r)$ is a continuous $\mathbb{Z}_l$-linear map satisfying the following property: For any $\alpha \in \mathbb{Z}_l[[\mathfrak{F}_r]]$,

$$\alpha = \epsilon_{\mathbb{Z}_l[[\mathfrak{F}_r]]}(\alpha) + \sum_{j=1}^{r} \frac{\partial \alpha}{\partial x_j}(x_j - 1). \tag{5.1.1}$$

We note by (5.1.1) that $\frac{\partial \alpha}{\partial x_j} \in I^{n-1}_{\mathbb{Z}_l[[\mathfrak{F}_r]]}$ if $\alpha - \epsilon_{\mathbb{Z}_l[[\mathfrak{F}_r]]}(\alpha) \in I^n_{\mathbb{Z}_l[[\mathfrak{F}_r]]}$ for $n \ge 1$.

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

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

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

(iii) $\dfrac{\partial f^{-1}}{\partial x_j} = -f^{-1}\dfrac{\partial f}{\partial x_j}$ $\quad(f \in \mathfrak{F}_r)$.

(iv) $\dfrac{\partial f^\alpha}{\partial x_j} = \beta \dfrac{\partial f}{\partial x_j}$ $(f \in \mathfrak{F}_r, \alpha \in \mathbb{Z}_l)$, where β is any element of $\mathbb{Z}_l[[\mathfrak{F}_r]]$ such that $\beta(f-1) = f^\alpha - 1$ exists.

(v) $\dfrac{\partial \varphi(\alpha)}{\partial \varphi(x_j)} = \varphi\Big(\dfrac{\partial \alpha}{\partial x_j}\Big)$ $(\varphi \in \mathrm{Aut}(\mathfrak{F}_r), \alpha \in \mathbb{Z}_l[[\mathfrak{F}_r]])$. (Note that $\varphi(x_1), \dots, \varphi(x_r)$ are free generators of $\mathfrak{F}_r$.)

(vi) If $\mathfrak{F}'$ is an open free subgroup of $\mathfrak{F}_r$ with free generators $y_1, \dots, y_s$, we have the chain rule: $\dfrac{\partial \alpha}{\partial x_j} = \sum_{i=1}^{s} \dfrac{\partial \alpha}{\partial y_i}\dfrac{\partial y_i}{\partial x_j}$ $(\alpha \in \mathbb{Z}_l[[\mathfrak{F}']])$.

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 (3.1.4) is written as

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

§5.2. Pro-l Magnus cocycles

Let $\mathrm{Ih}_S : \mathrm{Gal}_k \to P(\mathfrak{F}_r) \subset \mathrm{Aut}(\mathfrak{F}_r)$ be the Ihara representation associated to S in (2.2.3). Let $^{-} : \mathbb{Z}_l[[\mathfrak{F}_r]] \to \mathbb{Z}_l[[\mathfrak{F}_r]]$ 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* $\mathrm{M}_S : \mathrm{Gal}_k \to \mathrm{M}(r; \mathbb{Z}_l[[\mathfrak{F}_r]])$ associated to Ih_S by

(5.2.1) $$\mathrm{M}_S(g) := \left(\overline{\frac{\partial\, \mathrm{Ih}_S(g)(x_j)}{\partial x_i}}\right)$$

for $g \in \mathrm{Gal}_k$. In fact, we have the following lemma.

Lemma 5.2.2. *The map M_S is a 1-cocycle of Gal_k with coefficients in $\mathrm{GL}(r; \mathbb{Z}_l[[\mathfrak{F}_r]])$ with respect to the action Ih_S. To be precise, for $g, h \in \mathrm{Gal}_k$, we have*

$$\mathrm{M}_S(gh) = \mathrm{M}_S(g)\, \mathrm{Ih}_S(g)(\mathrm{M}_S(h)),$$

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

Proof. Let $y_j := \mathrm{Ih}_S(h)(x_j)$ for $1 \le j \le r$. Then we have

(5.2.2.1) $$\frac{\partial\, \mathrm{Ih}_S(gh)(x_j)}{\partial x_i} = \frac{\partial\, \mathrm{Ih}_S(g)(y_j)}{\partial x_i}.$$

Using the basic rules (v), (vi) of the pro-l Fox derivatives, we have

$$
\begin{aligned}
\frac{\partial\, \mathrm{Ih}_S(g)(y_j)}{\partial x_i} &= \sum_{a=1}^{r} \frac{\partial\, \mathrm{Ih}_S(g)(y_j)}{\partial\, \mathrm{Ih}_S(g)(x_a)} \frac{\partial\, \mathrm{Ih}_S(g)(x_a)}{\partial x_i} \\
&= \sum_{a=1}^{r} \mathrm{Ih}_S(g) \left(\frac{\partial y_j}{\partial x_a}\right) \frac{\partial\, \mathrm{Ih}_S(g)(x_a)}{\partial x_i}.
\end{aligned} \tag{5.2.2.2}
$$

By (5.2.2.1) and (5.2.2.2), we have

$$
\overline{\frac{\partial\, \mathrm{Ih}_S(gh)(x_j)}{\partial x_i}} = \sum_{a=1}^{r} \overline{\frac{\partial\, \mathrm{Ih}_S(g)(x_a)}{\partial x_i}} \cdot \overline{\mathrm{Ih}_S(g)\left(\frac{\partial y_j}{\partial x_a}\right)}.
$$

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

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

$$
\mathrm{M}_S^{[m]} : \mathrm{Gal}_k[m] \longrightarrow \mathrm{GL}(r; \mathbb{Z}_l[[\mathfrak{F}_r]]/I^{m+1}_{\mathbb{Z}_l[[\mathfrak{F}_r]]}).
$$

A relation between $\mathrm{M}_S^{[m]}$ and the mth pro-l Johnson homomorphism is given as follows. First, recall the identification $\Theta_n : \mathrm{gr}_n(\mathfrak{F}_r) \simeq H^{\otimes n}$ by the degree-n part of the Magnus isomorphism in (4.1.2). We then have a matrix representation of $\mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\oplus(m+1)})$ for $m \geq 1$,

$$
\|\ \ \| : \mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\oplus(m+1)}) \longrightarrow \mathrm{M}(r; \mathrm{gr}_m(\mathbb{Z}_l[[\mathfrak{F}_r]]))
$$

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

$$
\|\tau\| := \left(\frac{\partial(\Theta_{m+1}^{-1} \circ \tau)(X_j)}{\partial x_i}\right) \in \mathrm{M}(r; \mathrm{gr}_m(\mathbb{Z}_l[[\mathfrak{F}_r]])). \tag{5.2.3}
$$

Proposition 5.2.4. *For $g \in \mathrm{Gal}_k[m]$, we have*

$$
\mathrm{M}_S^{[m]}(g) = I + \overline{\|\tau_S^{[m]}(g)\|}.
$$

Proof. By Theorem 4.3.6, we have

$$
(\Theta_{m+1}^{-1} \circ \tau_S^{[m]}(g))(X_j) = \mathrm{Ih}_S(g)(x_j)x_j^{-1}
$$

and so

$$
\begin{aligned}
\frac{\partial(\Theta_{m+1}^{-1} \circ \tau_S^{[m]})(X_j)}{\partial x_i} &= \frac{\partial\, \mathrm{Ih}_S(g)(x_j)x_j^{-1}}{\partial x_i} \\
&= \frac{\partial\, \mathrm{Ih}_S(g)(x_j)}{\partial x_i} - \mathrm{Ih}_S(g)(x_j)x_j^{-1}\delta_{ij}.
\end{aligned}
$$

Since $\mathrm{Ih}_S(g)(x_j)x_j^{-1} \in \mathfrak{F}_r(m+1)$, we have $\mathrm{Ih}_S(g)(x_j)x_j^{-1}\delta_{ij} \equiv \delta_{ij} \bmod I^{m+1}_{\mathbb{Z}_l[[\mathfrak{F}_r]]}$ and hence the assertion is proved. □

In terms of $\|\cdot\|$, the mth pro-l Morita trace $\mathrm{Tr}^{[m]}(\tau)$ in (4.3.12) is, in fact, written as the trace of the matrix $\|\tau\|$.

Proposition 5.2.5. *For $m \geq 1$ and $\tau \in \mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)})$, we have*

$$\mathrm{Tr}^{[m]}(\tau) = q_m(\mathrm{tr}(\Theta_m(\|\tau\|))),$$

where $q_m : H^{\otimes m} \to S^m(H)$ is the natural map.

Proof. We identify $\mathrm{Hom}_{\mathbb{Z}_l}(H, H^{\otimes(m+1)})$ with $H^* \otimes H^{\otimes m}$. Let $\tau = \phi \otimes X_{i_1} \otimes \cdots \otimes X_{i_{m+1}}$ ($\phi \in H^*$). By (5.2.3), we have

$$\begin{aligned}\mathrm{tr}(\|\tau\|) &= \sum_{i=1}^{r} \frac{\partial(\Theta^{-1}_{m+1} \circ \tau)(X_i)}{\partial x_i} \\ &= \sum_{i=1}^{r} \phi(X_i) \frac{\partial \Theta^{-1}_{m+1}(X_{i_1} \otimes \cdots \otimes X_{i_{m+1}})}{\partial x_i}.\end{aligned} \tag{5.2.5.1}$$

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 (5.1.1),

$$\frac{\partial \Theta^{-1}_{m+1}(Y)}{\partial x_i} = \Theta^{-1}_m(Y_i).$$

Therefore we have

$$\frac{\partial \Theta^{-1}_{m+1}(X_{i_1} \otimes \cdots \otimes X_{i_{m+1}})}{\partial x_i} = \delta_{i,i_{m+1}} X_{i_1} \otimes \cdots \otimes X_{i_m}$$

and hence, by (5.2.5.1),

$$\mathrm{tr}(\Theta_m(\|\tau\|)) = \phi(X_{i_{m+1}}) X_{i_1} \otimes \cdots \otimes X_{i_m},$$

where the right-hand side is $c_{m+1}(\tau)$ by (4.3.11). By the definition (4.3.12), the assertion is proved. □

Now, for an 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 ψ 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 $\mathfrak{N} := \mathrm{Ker}(\psi)$ so that $\mathfrak{F}_r/\mathfrak{N} \simeq \mathfrak{G}$. We assume that $\mathfrak{N}$ is stable under the action of Gal_k through Ih_S, namely $\mathrm{Ih}_S(g)(\mathfrak{N}) \subset \mathfrak{N}$ for all $g \in \mathrm{Gal}_k$ (this is certainly satisfied if $\mathfrak{N}$ is a characteristic subgroup of $\mathfrak{F}_r$). Then we have a homomorphism $\mathrm{Ih}_{S,\psi} : \mathrm{Gal}_k \to \mathrm{Aut}(\mathbb{Z}_l[[\mathfrak{G}]])$ defined by

$$\mathrm{Ih}_{S,\psi}(g)(\psi(\alpha)) := \psi(\mathrm{Ih}_S(g)(\alpha)) \quad (\alpha \in \mathbb{Z}_l[[\mathfrak{F}_r]]). \tag{5.2.6}$$

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

$$\begin{aligned} \mathrm{Gal}_k[\psi] &:= \mathrm{Ker}(\mathrm{Ih}_{S,\psi}) \\ &= \{g \in \mathrm{Gal}_k \mid \psi \circ \mathrm{Ih}_S(g) = \psi\} \end{aligned} \tag{5.2.7}$$

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

$$\mathrm{M}_{S,\psi}(g) := \psi(\mathrm{M}_S(g)) \quad (g \in \mathrm{Gal}_k),$$

where the right-hand side is the matrix obtained by applying ψ to each entry of $\mathrm{M}_S(g)$. For $m \geq 1$, let $\mathrm{M}_{S,\psi}^{[m]}$ be the composite of $\mathrm{M}_S^{[m]}$ with the natural homomorphism $\mathrm{GL}(r; \mathbb{Z}_l[[\mathfrak{F}_r]]/I_{\mathbb{Z}_l[[\mathfrak{F}_r]]}^{m+1}) \to \mathrm{GL}(r; \mathbb{Z}_l[[\mathfrak{G}]]/I_{\mathbb{Z}_l[[\mathfrak{G}]]}^{m+1})$ induced by ψ. Lemma 5.2.2 and Proposition 5.2.4 are extended to the following proposition.

Proposition 5.2.8. *With notation as above, the following assertions hold:*

(1) For $g, h \in \mathrm{Gal}_k$, we have

$$\mathrm{M}_{S,\psi}(gh) = \mathrm{M}_{S,\psi}(g)\, \mathrm{Ih}_{S,\psi}(g)(\mathrm{M}_{S,\psi}(h)).$$

(2) For $g \in \mathrm{Gal}_k$, we have

$$\mathrm{M}_{S,\psi}^{[m]}(g) = I + \psi(\overline{\|\tau_S^{[m]}(g)\|}).$$

(3) The restriction of $\mathrm{M}_{S,\psi}$ to $\mathrm{Gal}_k[\psi]$, denoted by the same $\mathrm{M}_{S,\psi}$,

$$\mathrm{M}_{S,\psi} : \mathrm{Gal}_k[\psi] \longrightarrow \mathrm{GL}(r; \mathbb{Z}_l[[\mathfrak{G}]/I_{\mathbb{Z}_l[[\mathfrak{G}]]}^{m+1}),$$

is a homomorphism and factors through the Galois group $\mathrm{Gal}(\Omega_S/k[\psi])$, where Ω_S is the subfield of $\overline{\mathbb{Q}}$ corresponding to $\mathrm{Ker}(\mathrm{Ih}_S)$ as in (2.2.4). We call it the pro-l Magnus representation *of $\mathrm{Gal}_k[\psi]$ associated to Ih_S and ψ.*

Proof. (1) The formula is obtained by applying ψ to the both sides of the formula in Lemma 5.2.2.

(2) This is also obtained by applying ψ to the matrices of the both sides of the formula in Proposition 5.2.4.

(3) Suppose $g, h \in \mathrm{Gal}_{k,\psi}$. Since $\psi \circ \mathrm{Ih}_S(g) = \psi$, we have $\mathrm{Ih}_{S,\psi}(g)(\mathrm{M}_{S,\psi}(h)) = \mathrm{M}_{S,\psi}(h)$ and so $\mathrm{M}_{S,\psi}(gh) = \mathrm{M}_{S,\psi}(g)\mathrm{M}_{S,\psi}(h)$. Since $\mathrm{M}_{S,\psi}(g) = I$ for $g \in \mathrm{Ker}(\mathrm{Ih}_S)$, we have $\mathrm{Ker}(\mathrm{M}_{S,\psi}) \supset \mathrm{Ker}(\mathrm{Ih}_S)$ and hence $\mathrm{M}_{S,\psi}$ factors through $\mathrm{Gal}(\Omega_S/k[\psi])$. □

For $n \geq 0$, let $\pi_n : \mathfrak{F}_r \to \mathfrak{F}_r/\mathfrak{F}_r(n+1)$ be the natural homomorphism. We consider the case that $\psi = \pi_n$ and so $\mathrm{Ih}_{S,\psi} = \mathrm{Ih}_S^{(n)}$. By (4.3.1) and Proposition 4.3.3, we have

$$\begin{aligned}\mathrm{Gal}_k[\pi_n] &= \{g \in \mathrm{Gal}_k \mid \pi_n \circ \mathrm{Ih}_S(g) = \pi_n\} \\ &= \{g \in \mathrm{Gal}_k \mid \mathrm{Ih}_S(g)(f) \equiv f \bmod \mathfrak{F}_r(n+1) \text{ for all } f \in \mathfrak{F}_r\} \\ &= \mathrm{Gal}_k[n].\end{aligned}$$

Then we have a family of pro-l Magnus cocycles

$$\mathrm{M}_{S,\pi_n} : \mathrm{Gal}_k \longrightarrow \mathrm{GL}(r; \mathbb{Z}_l[[\mathfrak{F}_r/\mathfrak{F}_r(n+1)]]), \tag{5.2.9}$$

and the pro-l Magnus representation

$$\mathrm{M}_{S,\pi_n} : \mathrm{Gal}_k[n] \longrightarrow \mathrm{GL}(r; \mathbb{Z}_l[[\mathfrak{F}_r/\mathfrak{F}_r(n+1)]]) \tag{5.2.10}$$

associated to Ih_S and π_n for $n \geq 0$.

§5.3. 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,π_1} in (5.2.9). 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 $x_i \bmod \mathfrak{F}_r(2) \mapsto 1 + u_i$ $(1 \leq i \leq r)$ gives the abelianized pro-l Magnus isomorphism

$$\theta : \mathbb{Z}_l[[\mathfrak{F}_r/\mathfrak{F}_r(2)]] \xrightarrow{\sim} \Lambda_r.$$

We let $\pi := \pi_1$ and

$$\chi_{\Lambda_r} := \mathrm{Ih}_{S,\theta\circ\pi} : \mathrm{Gal}_k \to \mathrm{Aut}(\Lambda_r), \tag{5.3.1}$$

which is defined by (5.2.6) with $\psi = \theta \circ \pi$. In fact, by Lemma 3.2.1, χ_{Λ_r} is given by

$$\chi_{\Lambda_r}(g)(u_i) = (\theta \circ \pi)(\mathrm{Ih}_S(g)(x_i - 1)) = (1 + u_i)^{\chi_l(g)} - 1 \quad (1 \leq i \leq r). \tag{5.3.2}$$

Then the *pro-l Gassner cocycle* of Gal_k associated to Ih_S,

$$\mathrm{Gass}_S : \mathrm{Gal}_k \longrightarrow \mathrm{GL}(r; \Lambda_r),$$

is defined by

$$\mathrm{Gass}_S(g) := \left((\theta \circ \pi) \left(\frac{\partial\, \mathrm{Ih}_S(g)(x_j)}{\partial x_i} \right) \right) \quad (g \in \mathrm{Gal}_k), \tag{5.3.3}$$

where we note that we do not need to take the anti-automorphism $^-$ in (5.3.3) to obtain the 1-cocycle relation

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

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

Proposition 5.3.4. The (i, j)-entry of $\mathrm{Gass}_S(g)$ $(g \in \mathrm{Gal}_k)$ is expressed by

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

Proof. By Lemma 3.2.1 and a straightforward computation, we have

$$\begin{aligned} \frac{\partial\, \mathrm{Ih}_S(g)(x_j)}{\partial x_i} &= \frac{\partial y_j(g) x_j^{\chi_l(g)} y_j(g)^{-1}}{\partial x_i} \\ &= y_j(g) \frac{x_j^{\chi_l(g)} - 1}{x_j - 1} \delta_{ij} + \left(1 - y_j(g) x_j^{\chi_l(g)} y_j(g)^{-1} \right) \frac{\partial y_j(g)}{\partial x_i} \end{aligned}$$

and hence, by (5.3.2),

$$\begin{aligned} &(\theta \circ \pi) \left(\frac{\partial\, \mathrm{Ih}_S(g)(x_j)}{\partial x_i} \right) \\ &= (\theta \circ \pi)(y_j(g)) \frac{(1 + u_j)^{\chi_l(g)} - 1}{u_j} \delta_{ij} \\ &\quad + (1 - (1 + u_j)^{\chi_l(g)}) (\theta \circ \pi) \left(\frac{\partial y_j(g)}{\partial x_i} \right) \\ &= \frac{\chi_{\Lambda_r}(g)(u_j)}{u_j} (\theta \circ \pi)(y_j(g)) \delta_{ij} - \chi_{\Lambda_r}(g)(u_j) (\theta \circ \pi) \left(\frac{\partial y_j(g)}{\partial x_i} \right). \end{aligned} \tag{5.3.4.1}$$

Here we have

$$(5.3.4.2)\qquad (\theta\circ\pi)(y_j(g)) = 1 + \sum_{|I|\geq 1} \mu(g;Ij)u_I,$$

where we set $u_I := u_{i_1}\cdots u_{i_n}$ for $I=(i_1\cdots i_n)$, and (5.1.1) yields

$$(5.3.4.3)\qquad (\theta\circ\pi)\left(\frac{\partial y_j(g)}{\partial x_i}\right) = \sum_{|I|\geq 0} \mu(g;Iij)u_I.$$

By (5.3.3), (5.3.4.1), (5.3.4.2) and (5.3.4.3), we have

$$\begin{aligned}\mathrm{Gass}_S(g) &= (\theta\circ\pi)\left(\frac{\partial\,\mathrm{Ih}_S(g)(x_j)}{\partial x_i}\right)\\ &= \delta_{ij}\frac{\chi_{\Lambda_r}(g)(u_j)}{u_j}\left(1+\sum_{|I|\geq 1}\mu(g;Ij)u_I\right) - \chi_{\Lambda_r}(g)(u_j)\sum_{|I|\geq 0}\mu(g;Iij)u_I.\end{aligned}$$

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

By (5.2.10), when Gass_S is restricted to $\mathrm{Gal}_k[1]$, we have a representation

$$\mathrm{Gass}_S : \mathrm{Gal}_k[1] \longrightarrow \mathrm{GL}_r(\Lambda_r),$$

which we call the *pro-l Gassner representation* of $\mathrm{Gal}_k[1]$ associated to Ih_S. It factors through the Galois group $\mathrm{Gal}(\Omega_S/k[1])$ by Proposition 5.2.8(3).

In the following, for simplicity, we let

$$\mathfrak{F}'_r := \mathfrak{F}_r(2),\quad \mathfrak{F}''_r := [\mathfrak{F}'_r,\mathfrak{F}'_r],\quad \text{and}\quad \mathfrak{L}_r := \mathfrak{F}'_r/\mathfrak{F}''_r = H_1(\mathfrak{F}'_r,\mathbb{Z}_l).$$

We consider $\mathfrak{L}$ as a Λ_r-module by conjugation: For $f\in\mathfrak{F}_r$ and $f'\in\mathfrak{F}'_r$, we set

$$[f].(f' \bmod \mathfrak{F}''_r) := ff'f^{-1} \bmod \mathfrak{F}''_r$$

and extend it by the $\mathbb{Z}_l$-linearity and continuity. The structure of the Λ_r-module $\mathfrak{L}_r$ can be described by means of the pro-l Crowell exact sequence ([Ms2, Chap. 9]). Attached to the surjective homomorphism $\pi:\mathfrak{F}_r \longrightarrow \mathfrak{F}_r/\mathfrak{F}'_r$, the *pro-$l$ Crowell exact sequence* reads as the exact sequence of Λ_r-modules:

$$0\longrightarrow \mathfrak{L}_r \stackrel{\nu_1}{\longrightarrow} \Lambda_r^{\oplus r} \stackrel{\nu_2}{\longrightarrow} I_{\Lambda_r} \longrightarrow 0,$$

where I_{Λ_r} is the (augmentation) ideal of Λ_r generated by $u_1,\dots,u_r$, and ν_1, ν_2 are Λ_r-homomorphisms defined by

$$(5.3.5)\quad \nu_1(f' \bmod \mathfrak{F}''_r) := \left((\theta\circ\pi)\left(\frac{\partial f'}{\partial x_i}\right)\right)\quad (f'\in\mathfrak{F}'_r);\qquad \nu_2((\lambda_i)) := \sum_{i=1}^r \lambda_i u_i.$$

(*Convention*: An element (λ_i) of $\Lambda_r^{\oplus r}$ is understood as a column vector.) Hence we have the isomorphism of Λ_r-modules induced by ν_1, called the *Blanchfield–Lyndon isomorphism*:

$$\nu_1 : \mathfrak{L}_r \xrightarrow{\sim} \left\{(\lambda_i) \in \Lambda_r^{\oplus r} \mid \textstyle\sum_{i=1}^r \lambda_i u_i = 0\right\}. \tag{5.3.6}$$

We define the action Meta_S of Gal_k on $\mathfrak{L}_r$ through the Ihara representation Ih_S: For $g \in \mathrm{Gal}_k$ and $f' \in \mathfrak{F}'_r$,

$$\mathrm{Meta}_S(g)(f' \bmod \mathfrak{F}''_r) := \mathrm{Ih}_S(g)(f') \bmod \mathfrak{F}''_r.$$

It is easy to see that $\mathrm{Meta}_S(g)$ is a χ_{Λ_r}-linear automorphism of $\mathfrak{L}_r$, namely, a $\mathbb{Z}_l$-linear automorphism and satisfies

$$\mathrm{Meta}_S(g)(\lambda.(f' \bmod \mathfrak{F}''_r)) = \chi_{\Lambda_r}(g)(\lambda).(f' \bmod \mathfrak{F}''_r)$$

for $\lambda \in \Lambda_r$ and $f' \in \mathfrak{F}'_r$. When Meta_S is restricted to $\mathrm{Gal}_k[1]$, we have the representation, which we call the *pro-l meta-abelian representation* of $\mathrm{Gal}_k[1]$ associated to Ih_S,

$$\mathrm{Meta}_S : \mathrm{Gal}_k[1] \longrightarrow \mathrm{GL}_{\Lambda_r}(\mathfrak{L}_r),$$

where $\mathrm{GL}_{\Lambda_r}(\mathfrak{L}_r)$ is the group of Λ_r-module automorphisms of $\mathfrak{L}_r$. Regarding $\mathfrak{L}_r$ as a Λ_r-submodule of $\Lambda_r^{\oplus r}$ by the isomorphism (5.3.6), Meta_S and Gass_S has the following relation.

Proposition 5.3.7. *For $g \in \mathrm{Gal}_k$ and $f' \in \mathfrak{F}'_r$, we have*

$$(\nu_1 \circ \mathrm{Meta}_S(g))(f' \bmod \mathfrak{F}''_r) = \mathrm{Gass}_S(g)(\chi_{\Lambda_r}(g) \circ \nu_1)(f' \bmod \mathfrak{F}''_r).$$

When Meta_S and $\mathrm{Gass}_S|_{\mathfrak{L}_r}$ are restricted to $\mathrm{Gal}_k[1]$, they are equivalent representations over Λ_r.

Proof. The first assertion follows from direct computation: By (5.3.1), (5.3.3) and (5.3.5), we have, for any $g \in \mathrm{Gal}_k$ and $f' \in \mathfrak{F}'_r$,

$$\begin{aligned}
&(\nu_1 \circ \mathrm{Meta}_S(g))(f' \bmod \mathfrak{F}''_r)\\
&\quad = \nu_1(\mathrm{Ih}_S(g)(f') \bmod \mathfrak{F}''_r)\\
&\quad = \left((\theta \circ \pi)\left(\frac{\partial\, \mathrm{Ih}_S(g)(f')}{\partial x_i}\right)\right)\\
&\quad = \left((\theta \circ \pi)\left(\sum_{a=1}^r \frac{\partial\, \mathrm{Ih}_S(g)(f')}{\partial\, \mathrm{Ih}_S(g)(x_a)} \frac{\partial\, \mathrm{Ih}_S(g)(x_a)}{\partial x_i}\right)\right)\\
&\quad = \left(\sum_{a=1}^r (\theta \circ \pi)\left(\frac{\partial\, \mathrm{Ih}_S(g)(x_a)}{\partial x_i}\right)(\theta \circ \pi \circ \mathrm{Ih}_S(g))\left(\frac{\partial f'}{\partial x_a}\right)\right)\\
&\quad = \mathrm{Gass}_S(g)\chi_{\Lambda_r}(g)(\nu_1(f' \bmod \mathfrak{F}''_r)).
\end{aligned}$$

When Meta_S and Gass_S are restricted to $\mathrm{Gal}_k[1]$, by the first assertion, we have the commutative diagram of Λ_r-modules for any $g \in \mathrm{Gal}_k[1]$:

$$\begin{array}{ccc} \mathfrak{L}_r & \overset{\nu_1}{\hookrightarrow} & \Lambda_r^{\oplus r} \\ {\scriptstyle \mathrm{Meta}_S(g)} \downarrow & & \downarrow {\scriptstyle \mathrm{Gass}_S(g)} \\ \mathfrak{L}_r & \overset{\nu_1}{\hookrightarrow} & \Lambda_r^{\oplus r}, \end{array}$$

from which the latter assertion follows. □

Next, we introduce the pro-l reduced Gassner cocycle associated to the Ihara representation Ih_S. For this, we follow Oda's arguments ([O2]). We first define a certain Λ_r-submodule $\mathfrak{L}_r^{\mathrm{prim}}$ of $\mathfrak{L}_r$, which Oda calls the primitive part of $\mathfrak{L}$, as follows. For $1 \le i \le r$, let $\mathfrak{N}_i$ be the closed subgroup generated normally by x_i and let $\mathfrak{F}_r^{(i)} := \mathfrak{F}_r/\mathfrak{N}_i$. Let $\Lambda_r^{(i)} := \mathbb{Z}_l[[u_1, \ldots, \hat{u}_i, \ldots, u_r]] \simeq \mathbb{Z}_l[[\mathfrak{F}_r^{(i)}/(\mathfrak{F}_r^{(i)})']]$ ($\hat{u}_i$ 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 Λ_r-module via δ_i. Let $\mathfrak{L}_r^{(i)} := (\mathfrak{F}_r^{(i)})'/(\mathfrak{F}_r^{(i)})''$ and let $\xi_i : \mathfrak{L}_r \to \mathfrak{L}_r^{(i)}$ be the Λ_r-homomorphism induced by the natural homomorphism $\mathfrak{F}_r \to \mathfrak{F}_r^{(i)}$. Then the *primitive part* $\mathfrak{L}_r^{\mathrm{prim}}$ of $\mathfrak{L}_r$ is defined by

$$\mathfrak{L}_r^{\mathrm{prim}} := \bigcap_{i=1}^{r} \mathrm{Ker}(\xi_i). \tag{5.3.8}$$

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

Theorem 5.3.9 ([O2]). *With notation as above, the following assertions hold.*

(1) The Blanchfield–Lyndon isomorphism ν_1 in (5.3.6) restricted to $\mathfrak{L}_r^{\mathrm{prim}}$ induces the following isomorphism of Λ_r-modules

$$\mathfrak{L}_r^{\mathrm{prim}} \simeq \left\{ (\lambda_j \tfrac{w}{u_j}) \in \Lambda_r^{\oplus r} \mid \lambda_j \in \Lambda_r,\ \textstyle\sum_{j=1}^{r} \lambda_j = 0 \right\}.$$

In particular, $\mathfrak{L}_r^{\mathrm{prim}}$ is the free Λ_r-module of rank $r-1$ on the basis

$$\boldsymbol{v}_1 := {}^t\big(-\tfrac{w}{u_1}, \tfrac{w}{u_2}, 0, \ldots, 0\big), \ldots, \boldsymbol{v}_{r-1} := {}^t\big(0, \ldots, 0, -\tfrac{w}{u_{r-1}}, \tfrac{w}{u_r}\big).$$

(2) $\mathfrak{L}_r^{\mathrm{prim}}$ is stable under the action of Gal_k through Meta_S and defines the 1-cocycle

$$\mathrm{Gass}_S^{\mathrm{red}} : \mathrm{Gal}_k \longrightarrow \mathrm{GL}_{r-1}(\Lambda_r)$$

with respect to the basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{r-1}$ and the action χ_{Λ_r} in (5.3.1). We call $\mathrm{Gass}_S^{\mathrm{red}}$ the pro-l reduced Gassner cocycle *of Gal_k associated to Ih_S.*

Proof. (1) We define the Λ_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 $\xi_i = \tilde{\xi}_i|_{\mathfrak{L}_r}$ for $1 \le i \le r$ and the commutative diagram of Λ_r-modules:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{L}_r & \longrightarrow & \Lambda_r^{\oplus r} & \longrightarrow & I_{\Lambda_r} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \xi_i} & & \downarrow{\scriptstyle \tilde{\xi}_i} & & \downarrow{\scriptstyle \delta_i} & & \\
0 & \longrightarrow & \mathfrak{L}_r^{(i)} & \longrightarrow & (\Lambda_r^{(i)})^{\oplus(r-1)} & \longrightarrow & I_{\Lambda_r^{(i)}} & \longrightarrow & 0,
\end{array}$$

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

$$\mathrm{Ker}(\tilde{\xi}) = \{ {}^t(\lambda_1 u_i, \ldots, \lambda_{i-1} u_i, \lambda_i, \lambda_{i+1} u_i, \ldots, \lambda_r u_i) \mid \lambda_j \in \Lambda_r \ (1 \le j \le r)\}$$

and hence, by (5.3.6) and (5.3.8), we have

$$\mathfrak{L}_r^{\mathrm{prim}} = \left\{(\lambda_j) \in \Lambda_r^{\oplus r} \mid \textstyle\sum_{j=1}^r \lambda_j u_j = 0,\ \lambda_j \equiv 0 \mod u_i \text{ if } i \ne j\right\}.$$

Since Λ_r is a regular local ring, it is factorial. Therefore we have the first assertion,

$$\mathfrak{L}_r^{\mathrm{prim}} = \left\{(\lambda_j) \in \Lambda_r^{\oplus r} \mid \textstyle\sum_{j=1}^r \lambda_j u_j = 0,\ \lambda_j \equiv 0 \mod \frac{w}{u_j} \ (1 \le j \le r)\right\}.$$

The assertion for a basis of $\mathfrak{L}_r^{\mathrm{prim}}$ is clear.

(2) Since $\mathrm{Ih}_S(g)(x_i)$ is conjugate to $x_i^{\chi_l(g)}$ for $g \in \mathrm{Gal}_k$ and $1 \le i \le r$, definition (5.3.8) implies that $\mathfrak{L}_r^{\mathrm{prim}}$ is Gal_k-stable under the action Meta_S. So we may write, for $1 \le j \le r-1$,

(5.3.9.1)
$$\mathrm{Ih}_S(g)(\boldsymbol{v}_j) = \sum_{i=1}^{r-1} \mathrm{Gass}_S^{\mathrm{red}}(g)_{ij} \boldsymbol{v}_i,$$

where $\mathrm{Gass}_S^{\mathrm{red}}(g)_{ij} \in \Lambda_r$ is the (i,j)-entry of the representation matrix of $\mathrm{Ih}_S(g)$ with respect to $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{r-1}$. Then we have, for $g, h \in \mathrm{Gal}_k$,

$$\begin{aligned}
\mathrm{Ih}_S(gh)(\boldsymbol{v}_j) &= \mathrm{Ih}_S(g)(\mathrm{Ih}_S(h)(\boldsymbol{v}_j)) \\
&= \mathrm{Ih}_S(g)\left(\sum_{i=1}^{r-1} \mathrm{Gass}_S^{\mathrm{red}}(h)_{ij} \boldsymbol{v}_i\right) \\
&= \sum_{i=1}^{r-1} \chi_{\Lambda_r}(\mathrm{Gass}_S^{\mathrm{red}}(h)_{ij})\, \mathrm{Ih}_S(g)(\boldsymbol{v}_i) \quad \text{(by (5.3.1))} \\
&= \sum_{t=1}^{r-1} \left(\sum_{i=1}^{r-1} \mathrm{Gass}_S^{\mathrm{red}}(g)_{ti} \chi_{\Lambda_r}(g)(\mathrm{Gass}_S^{\mathrm{red}}(h)_{ij})\right) \boldsymbol{v}_t,
\end{aligned}$$

which means the cocycle relation

$$\mathrm{Gass}_S^{\mathrm{red}}(gh) = \mathrm{Gass}_S^{\mathrm{red}}(g)\chi_{\Lambda_r}(g)(\mathrm{Gass}_S^{\mathrm{red}}(h)).$$

Hence the assertion is proved. □

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

$$\mathrm{Gass}_S^{\mathrm{red}} : \mathrm{Gal}_k[1] \longrightarrow \mathrm{GL}(r-1; \Lambda_r),$$

which we call the *pro-l reduced Gassner representation* of Gal[1] associated to Ih_S.

Let Γ 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 $\mathfrak{z} : \mathfrak{F}_r \to \Gamma$ be the homomorphism defined by $\mathfrak{z}(x_i) := x$ for $1 \le i \le r$. Let χ_Λ be the action of Gal_k on Λ defined by $\chi_\Lambda(g)(u) := (1+u)^{\chi_l(g)} - 1$ for $g \in \mathrm{Gal}_k$ Then we have the pro-l Magnus cocycle associated to Ih_S and $\mathfrak{z}$,

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

which we call the *pro-l Burau cocycle* of Gal_k associated to Ih_S. It is the 1-cocycle of Gal_k with coefficients in $\mathrm{GL}(r;\Lambda)$ with respect to the action χ_Λ. By definition, we have

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

Similarly, we have the *pro-l reduced Burau cocycle* associated to Ih_S,

$$\mathrm{Bur}_S^{\mathrm{red}} : \mathrm{Gal}_k \longrightarrow \mathrm{GL}(r-1; \Lambda),$$

defined by

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

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

$$\mathfrak{z} \circ \mathrm{Ih}_S(g) = \mathfrak{z} \quad (g \in \mathrm{Gal}_k[1]).$$

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

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

which are called the *pro-l Burau representation* and the *pro-l reduced Burau representation* of $\mathrm{Gal}_k[1]$ associated to Ih_S, respectively.

§6. l-adic Alexander invariants

§6.1. Pro-l link modules

Let $g \in \mathrm{Gal}_k$. As in (3.3.1), let $\Pi_S(g)$ be the pro-l link group of g associated to the Ihara representation Ih_S:

$$\begin{aligned}\Pi_S(g) &= \langle x_1, \dots, x_r \mid y_1(g) x_1^{\chi_l(g)} y_1(g)^{-1} x_1^{-1} = \cdots = y_r(g) x_r^{\chi_l(g)} y_r(g)^{-1} x_r^{-1} = 1 \rangle \\ &= \mathfrak{F}_r / \mathfrak{N}_S(g),\end{aligned}$$

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

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

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

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

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

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

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

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

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

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, Chap. 9]).

Let $\varpi : \Pi_S(g) \to \Pi_S(g)/\Pi_S(g)'$ be the abelianization map. We define the *pro-l Alexander module* $\mathfrak{A}_S(g)$ of g associated to Ih_S by the *pro-l differential module* associated to ϖ, 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 $\gamma_1, \gamma_2 \in \Pi_S(g)$ ([Ms2, 9.3]):

$$\mathfrak{A}_S(g) := \bigoplus_{\gamma \in \Pi_S(g)} \Lambda_r(g) d\gamma / \langle d(\gamma_1\gamma_2) - d\gamma_1 - \varpi(\gamma_1) d\gamma_2 \ (\gamma_1, \gamma_2 \in \Pi_S(g)) \rangle_{\Lambda_r(g)}.$$

We define the *l-adic Alexander matrix* $Q_S(g)$ by the Jacobian matrix of the relators of $\Pi_S(g)$:

$$Q_S(g) := \left((\theta(g) \circ \varpi \circ \psi) \left(\frac{\partial \, y_j(g) x_j^{\chi_l(g)} y_j(g)^{-1} x_j^{-1}}{\partial x_i} \right) \right). \tag{6.1.1}$$

Proposition 6.1.2. *With notation as above, the following assertions hold.*

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

$$\mathfrak{A}_S(g) \xrightarrow{\sim} \mathrm{Coker}(Q_S(g) : \Lambda_r(g)^{\oplus r} \to \Lambda_r(g)^{\oplus r}),$$

where f *is any element of* $\mathfrak{F}_r$ *such that* $\gamma = \psi(f)$.

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

$$0 \longrightarrow \mathfrak{L}_S(g) \xrightarrow{\nu_1} \mathfrak{A}_S(g) \xrightarrow{\nu_2} I_{\Lambda_r(g)} \longrightarrow 0,$$

where ν_1, ν_2 *are given by*

$$\nu_1(\gamma' \bmod \Pi_S(g)'') := d\gamma \ (\gamma' \in \Pi_S(g)');$$
$$\nu_2(d\gamma) := (\theta(g)\circ\varpi)(\gamma) - 1 \ (\gamma \in \Pi_S(g)).$$

Proof. We refer to [Ms2, Thms. 9.3.6, 9.4.2]. □

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

Proposition 6.1.3. *We have*

$$Q_S(g) = \phi_g(\mathrm{Gass}_S(g) - I)$$

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

$$Q_S(g)_{ij} = \begin{cases} \phi_g\left(\sum_{n\geq 1} \sum_{\substack{1\leq i_1,\ldots,i_n\leq r \\ i_n\neq i}} \mu(g; i_1\cdots i_n i) u_{i_1}\cdots u_{i_n}\right) & (i=j), \\ \phi_g\left(-u_j\left(\mu(g;ij) + \sum_{n\geq 1}\sum_{1\leq i_1,\ldots,i_n\leq r} \mu(g; i_1\cdots i_n ii) u_{i_1}\cdots u_{i_n}\right)\right) & (i\neq j). \end{cases}$$

Proof. By definition (6.1.1), we have

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

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

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

By (5.3.3) and $\theta(g)\circ\varpi\circ\psi = \phi_g\circ\theta\circ\pi$, we have

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

and we also have

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

Therefore we have

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

The second assertion follows from Proposition 5.3.4 and

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

□

Corollary 6.1.4. *For $g, h \in \mathrm{Gal}_k[1]$, we have the following isomorphisms of Λ_r-modules:*

$$\mathfrak{A}_S(hgh^{-1}) \simeq \mathfrak{A}_S(g), \qquad \mathfrak{L}_S(hgh^{-1}) \simeq \mathfrak{L}_S(g).$$

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

$$Q_S(hgh^{-1}) = \phi_g(\mathrm{Gass}_S(hgh^{-1}) - I) = \phi_g(\mathrm{Gass}_S(h))Q_S(g)\phi_g(\mathrm{Gass}_S(h))^{-1}$$

by Proposition 6.1.3. Then the first assertion follows from Proposition 6.1.2(1). The second assertion follows from Proposition 6.1.2(2). □

§6.2. l-adic Alexander invariants

For $n \geq 0$, we define the *nth l-adic Alexander ideal* $\mathfrak{E}_S(g)^{(n)}$ of $g \in \mathrm{Gal}_k$ associated to Ih_S by the nth Fitting ideal of the pro-l Alexander module $\mathfrak{A}_S(g)$ over $\Lambda_r(g)$. The *nth l-adic Alexander invariant* $A_S(g)^{(n)}$ is then defined by a generator of the divisorial hull of $\mathfrak{E}_S(g)^{(n)}$. By Proposition 6.1.2(1), $\mathfrak{E}_S(g)^{(n)}$ is the ideal generated by all $(r-n)$-minors of $Q_S(g)$ if $r-n>0$ and $\mathfrak{E}_S(g)^{(n)} := \Lambda_r(g)$ if $r-n \leq 0$, and $A_S(g)^{(n)}$ is the greatest common divisor of all $(r-n)$-minors of $Q_S(g)$ if $r-n>0$ and $A_S(g)^{(n)} := 1$ if $r-n \leq 0$:

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

We note that $A_S(g)^{(n)}$ is defined up to multiplication of a unit of $\Lambda_r(g)$. We write $\mathfrak{E}_S(g)$ (resp. $A_S(g)$) for $\mathfrak{E}_S(g)^{(0)}$ (resp. $A_S(g)^{(0)}$) and call $\mathfrak{E}_S(g)$ (resp. $A_S(g)$) the l-adic Alexander ideal (resp. l-adic Alexander invariant) of g associated to Ih_S. From Proposition 6.1.3, the following proposition is immediate.

Proposition 6.2.1. *For $g \in \mathrm{Gal}_k$, we have*

$$A_S(g) = \phi_g(\det(\mathrm{Gass}_S(g) - I)).$$

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

Moreover, since the l-adic Alexander matrix $Q_S(g)$ is described by l-adic Milnor numbers as in Proposition 6.1.3, nth l-adic Alexander invariants are also described by l-adic Milnor numbers (cf. [Ms2, Chap. 10], [Mu]).

§7. 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 notation. The Ihara representation in this case is

$$\mathrm{Ih} : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow P(\mathfrak{F}_2),$$

which factors through the Galois group $\mathrm{Gal}(\Omega_l/\mathbb{Q})$ by Theorem 2.2.6(2), where Ω_l denotes the maximal pro-l extension of $\mathbb{Q}[1] = \mathbb{Q}(\zeta_{l^\infty})$ unramified outside l.

§7.1. The Ihara power series

The following lemma is a restatement of [Ih1, Thm. 2(i)]. See also [Ih2, §1(D) Example 2]. For the sake of readers, we give a proof using Theorem 5.3.9.

Lemma 7.1.1. *We have $\mathfrak{L}_2 = \mathfrak{L}_2^{\mathrm{prim}}$ with basis ${}^t(-u_2, u_1)$ over Λ_2, and ${}^t(-u_2, u_1) = \nu_1([x_1, x_2])$.*

Proof. By Theorem 5.3.9(1), $\mathfrak{L}_2^{\mathrm{prim}}$ is the free Λ_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 $\lambda_1 = -au_2$, $\lambda_2 = au_1$ for some $a \in \Lambda_2$, because Λ_2 is a unique factorization domain. Therefore $\mathfrak{L}_2$ is also the free Λ_2-module with basis ${}^t(-u_2, u_1)$ by (5.3.6). Hence $\mathfrak{L}_2 = \mathfrak{L}_2^{\mathrm{prim}}$. The second assertion follows from

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

□

Thanks to Lemma 7.1.1, Ihara introduced a power series $F_g(u_1, u_2) \in \Lambda_2$, called the *Ihara power series*, by the following equality in $\mathfrak{L}_2$:

$$\mathrm{Ih}_S(g)([x_1, x_2]) \equiv F_g(u_1, u_2)[x_1, x_2] \bmod \mathfrak{F}_2''. \tag{7.1.2}$$

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

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

We recall the pro-l Gassner and the pro-l reduced Gassner cocycles in (5.3.3) and (5.3.9.1):

$$\mathrm{Gass}: \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2;\Lambda_2); \qquad \mathrm{Gass}^{\mathrm{red}}: \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \Lambda_2^{\times}.$$

Theorem 7.1.3. *With notation as above, we have, for* $g \in \mathrm{Gal}_{\mathbb{Q}}$,

$$\begin{aligned} F_g(u_1,u_2) &= \mathrm{Gass}^{\mathrm{red}}(g) \\ &= \frac{\chi_{\Lambda_2}(g)(u_1u_2)}{u_1u_2}\left(1 + \sum_{n\geq 1} \sum_{\substack{1\leq i_1,\dots,i_n\leq 2 \\ i_n\neq i_{n+1}}} \mu(g;i_1\cdots i_n i_{n+1}) u_{i_1}\cdots u_{i_n}\right) \\ &= \frac{\chi_{\Lambda_2}(g)(u_1u_2)}{u_1u_2}\left(1 + \sum_{\substack{n_1,n_2\geq 0 \\ n_1+n_1\geq 1}} \mu(g;n_1,n_2)u_1^{n_1}u_2^{n_2}\right). \end{aligned}$$

Proof. Applying the Λ_2-homomorphism ν_1 to (7.1.2), we have, for $g \in \mathrm{Gal}_k$,

$$\nu_1(\mathrm{Ih}(g)([x_1,x_2])) = F_g(u_1,u_2)\nu_1([x_1,x_2]) = F_g(u_1,u_2)\begin{pmatrix} -u_2 \\ u_1 \end{pmatrix}.$$

On the other hand, by the definition of $\mathrm{Gass}_S^{\mathrm{red}}(g)$ (cf. (5.3.9.1)), we have

$$\nu_1(\mathrm{Ih}(g)([x_1,x_2])) = \mathrm{Gass}^{\mathrm{red}}(g)\begin{pmatrix} -u_2 \\ u_1 \end{pmatrix}.$$

Hence we have

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

By Proposition 5.3.7 and Lemma 7.1.1, we have

$$\begin{aligned} \nu_1(\mathrm{Ih}(g)([x_1,x_2])) &= \mathrm{Gass}(g)\chi_{\Lambda_2}(g)(\nu_1([x_1,x_2])) \\ &= \mathrm{Gass}(g)\begin{pmatrix} -\chi_{\Lambda_2}(g)(u_2) \\ \chi_{\Lambda_2}(g)(u_1) \end{pmatrix}. \end{aligned}$$

A straightforward calculation using Proposition 5.3.4 yields

$$\begin{aligned} &\mathrm{Gass}(g)\begin{pmatrix} -\chi_{\Lambda_2}(g)(u_2) \\ \chi_{\Lambda_2}(g)(u_1) \end{pmatrix} \\ &= \frac{\chi_{\Lambda_2}(g)(u_1u_2)}{u_1u_2}\left(1 + \sum_{n\geq 1} \sum_{\substack{1\leq i_1,\dots,i_n\leq 2 \\ i_n\neq i_{n+1}}} \mu(g;i_1\cdots i_n i_{n+1}) u_{i_1}\cdots u_{i_n}\right)\begin{pmatrix} -u_2 \\ u_1 \end{pmatrix} \\ &= \frac{\chi_{\Lambda_2}(g)(u_1u_2)}{u_1u_2}\left(1 + \sum_{\substack{n_1,n_2\geq 0 \\ n_1+n_1\geq 1}} \mu(g;n_1,n_2)u_1^{n_1}u_2^{n_2}\right)\begin{pmatrix} -u_2 \\ u_1 \end{pmatrix}. \end{aligned}$$

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 nonsingular, projective curve over $\mathbb{Q}$ defined by

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

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

$$\mathrm{T}(\mathrm{Jac}_n) := \mathrm{Hom}(\mathbb{Q}_l/\mathbb{Z}_l, \mathrm{Jac}_n(\overline{\mathbb{Q}})) \simeq H_1^{\mathrm{sing}}(C_n(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_l,$$

and let

$$\mathbb{T} := \varprojlim_n \mathrm{T}(\mathrm{Jac}_n),$$

where the inverse limit is taken with respect to the maps $\mathrm{T}(\mathrm{Jac}_{n+1}) \to \mathrm{T}(\mathrm{Jac}_n)$ 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 $\overline{C_n} := C_n \times_{\mathrm{Spec}\,\mathbb{Q}} \mathrm{Spec}\,\overline{\mathbb{Q}}$ over $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ defined by

$$g_{X,n} : (X, Y, Z) \mapsto (\zeta_{l^n} X, Y, Z), \qquad g_{Y,n} : (X, Y, Z) \mapsto (X, \zeta_{l^n} Y, Z)$$

and set $g_X := \lim_{\longleftarrow} g_{X,n}$, $g_Y := \lim_{\longleftarrow} g_{Y,n}$. Then $\mathrm{Gal}(\overline{C_n}/\mathbb{P}^1_{\overline{\mathbb{Q}}}) = (\mathbb{Z}/l^n\mathbb{Z}_l)g_{X,n} \oplus (\mathbb{Z}/l^n\mathbb{Z})g_{Y,n}$ and so $\lim_{\longleftarrow} \mathbb{Z}_l[\mathrm{Gal}(\overline{C_n}/\mathbb{P}^1_{\overline{\mathbb{Q}}})] \simeq \Lambda_2$ by the correspondence $g_X \mapsto 1 + u_1, g_Y \mapsto 1 + u_2$. Thus $\mathbb{T}$ is regarded as a Λ_2-module. Then we have the isomorphism of Λ_2-modules

$$\mathfrak{L}_2 \simeq \mathbb{T}.$$

For an explicit construction of the basis of $\mathbb{T}$ 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 lth-power roots of unity in terms of the Jacobi sums which arise from the Galois action on $\mathrm{T}(\mathrm{Jac}_n)$, 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 7.1.3, from the viewpoint of arithmetic topology.

§7.2. Values of the Ihara power series

Let p be a rational prime that is in R_S of (2.2.5) and let $\overline{p}$ be a prime of $\overline{\mathbb{Q}}$ lying over p. By Theorem 2.2.6(2), $\overline{p}$ is unramified in $\Omega_S/\mathbb{Q}$ and so we have the Frobenius automorphism $\sigma_{\overline{p}} \in \mathrm{Gal}(\Omega_S/\mathbb{Q})$. Let n be a fixed positive integer. Let $\mathfrak{p}_n$ be the prime of $\mathbb{Q}(\zeta_{l^n})$ lying below $\overline{p}$ and let $\left(\frac{x}{\mathfrak{p}_n}\right)_{l^n}$ denote the l^nth-power residue symbol at $\mathfrak{p}_n$ for $x \in (\mathbb{Z}[\zeta_{l^n}]/\mathfrak{p}_n)^\times$. For $a, b \in \mathbb{Z}/l^n\mathbb{Z} \setminus \{0\}$ with $(a, b, l) = 1$, we define the *Jacobi sum* by

$$J_{l^n}(\mathfrak{p}_n)^{(a,b)} = \sum_{\substack{x,y \in (\mathbb{Z}[\zeta_{l^n}]/\mathfrak{p}_n)^\times \\ x+y=-1}} \left(\frac{x}{\mathfrak{p}_n}\right)_{l^n}^a \left(\frac{y}{\mathfrak{p}_n}\right)_{l^n}^b.$$

For $l = 2$, $J_{l^n}(\mathfrak{p}_n)^{(a,b)}$ must be multiplied by $\left(\frac{-1}{\mathfrak{p}_n}\right)^a$. Let f be the order of p in $(\mathbb{Z}/l^n\mathbb{Z})^\times$. We note that $\sigma_{\overline{p}}^f \in \mathrm{Gal}(\Omega_S/\mathbb{Q}(\zeta_{l^n}))$. By using Weil's theorem, Ihara showed the following theorem.

Theorem 7.2.1 ([Ih1, Thm. 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*

$$F_{\sigma_{\overline{p}}^f}(\zeta_{l^n}^a - 1, \zeta_{l^n}^b - 1) = J_{l^n}(\mathfrak{p}_n)^{(a,b)}.$$

Combining Theorems 7.1.3 and 7.2.1, we obtain the following l-adic expansion of the Jacobi sum $J_{l^n}(\mathfrak{p}_n)^{(a,b)}$ with coefficients l-adic Milnor numbers.

Theorem 7.2.2. *With notation as above, we have*

$$J_{l^n}(\mathfrak{p}_n)^{(a,b)} = 1 + \sum_{\substack{n_1,n_2 \geq 0 \\ n_1+n_2 \geq 1}} \mu(\sigma_{\overline{p}}^f; n_1, n_2)(\zeta_{l^n}^a - 1)^{n_1}(\zeta_{l^n}^b - 1)^{n_2}.$$

Proof. Since we have $\zeta_{l^n}^{\chi_l(\sigma_{\overline{p}}^f)} = \zeta_{l^n}^{p^f} = \zeta_{l^n}$ by $p^f \equiv 1 \bmod l^n$, the formula follows from Theorems 7.1.3 and 7.2.1. □

§7.3. Coefficients of the Ihara power series

We will combine Theorem 7.1.3 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 Section 2.2, let ζ_{l^n} be a primitive l^nth 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 $a = \langle a \rangle_{l^n} \bmod l^n$. 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 *mth l-adic Soulé cocycle* $\chi^{(m)} : \mathrm{Gal}_\mathbb{Q} \to \mathbb{Z}_l$ by the Kummer cocycle attached to the system of cyclotomic l-units $\{\varepsilon_{l^n}^{(m)}\}_{n \geq 1}$,

$$\zeta_{l^n}^{\chi^{(m)}(g)} = \{(\varepsilon_{l^n}^{(m)})^{1/l^n}\}^{g-1} \quad (n \geq 1, g \in \mathrm{Gal}_\mathbb{Q}).$$

It is easy to see the cocycle relation

$$\chi^{(m)}(gh) = \chi^{(m)}(g) + \chi_l(g)\chi^{(m)}(h) \quad (g, h \in \mathrm{Gal}_{\mathbb{Q}})$$

and hence the restriction of $\chi^{(m)}|_{\mathrm{Gal}_{\mathbb{Q}[1]}}$ is a character. Let Ω_l^{ab} be the maximal abelian subextension of $\Omega_l/\mathbb{Q}[1]$. Since $\mathbb{Q}(\zeta_{l^n}, (\varepsilon_{l^n}^{(m)})^{1/l^n})$ is a cyclic extension of $\mathbb{Q}(\zeta_{l^n})$ unramified outside l, we have $(\varepsilon_{l^n}^{(m)})^{1/l^n} \in \Omega_l^{\mathrm{ab}}$ and so the Soulé character $\chi^{(m)}|_{\mathrm{Gal}_{\mathbb{Q}[1]}}$ factors through the Galois group $\mathrm{Gal}(\Omega_l^{\mathrm{ab}}/\mathbb{Q}[1])$. We note by Proposition 5.2.8(3) that the pro-l reduced Gassner representation $\mathrm{Gass}^{\mathrm{red}}$ also factors through $\mathrm{Gal}(\Omega_l^{\mathrm{ab}}/\mathbb{Q}[1])$.

We set

$$\kappa_m(g) := \frac{\chi^{(m)}(g)}{1 - l^{m-1}} \quad (g \in \mathrm{Gal}_{\mathbb{Q}}),$$

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

$$\mathcal{F}_g(U_1, U_2) := F_g(u_1, u_2)|_{u_i = \exp(U_i) - 1}.$$

Theorem 7.3.1 ([IKY, Thm. A$_2$]). *With notation as above, we have, for $g \in \mathrm{Gal}(\Omega_l^{\mathrm{ab}}/\mathbb{Q}[1])$,*

$$\mathcal{F}_g(U_1, U_2) = \exp\left\{ -\sum_{\substack{m \geq 3 \\ \mathrm{odd}}} \kappa_m(g) \left(\sum_{\substack{m_1, m_2 \geq 1 \\ m_1 + m_2 = m}} \frac{U_1^{m_1} U_2^{m_2}}{m_1!\, m_2!} \right) \right\}.$$

Combining Theorems 7.1.3 and 7.3.1, we can deduce relations between l-adic Milnor numbers and l-adic Soulé characters. For this, we prepare the following lemma.

Lemma 7.3.2. *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*

$$A(u_1, u_2) := 1 + \sum_{\substack{n_1, n_2 \geq 0 \\ n_1 + n_2 \geq 1}} a(n_1, n_2) u_1^{n_1} u_2^{n_2} \in \mathbb{Q}_l[[u_1, u_2]]$$

and set

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

Then we have

$$b(N_1, N_2) = \sum_{\substack{n_1+n_2\geq 1\\ 0\leq n_1\leq N_1, 0\leq n_2\leq N_2}} a(n_1, n_2)a_{n_1}(N_1)a_{n_2}(N_2),$$

where for $j = 1, 2$*,*

$$a_{n_j}(N_j) := \begin{cases} 1 & (n_j = 0), \\ \displaystyle\sum_{\substack{e_1,\dots,e_{n_j}\geq 1\\ e_1+\cdots+e_{n_j}=N_j}} \frac{1}{e_1!\cdots e_{n_j}!} & (n_j \geq 1). \end{cases}$$

Let

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

and set

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

Then we have

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

where the second sum ranges over integers $m_1^{(1)}, \dots, m_1^{(n)}, m_2^{(1)}, \dots, m_2^{(n)} \geq 0$ *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. Formulas for both $b(N_1, N_2)$ and $d(N_1, N_2)$ follow from straightforward computations. □

We apply Lemma 7.3.2 to the case that $A(u_1, u_2) = \mathrm{Gass}^{\mathrm{red}}(g)$, 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

$$c(m_1, m_2) = \begin{cases} -\dfrac{\kappa_{m_1+m_2}(g)}{m_1!\, m_2!} & (m_1 + m_2 \geq 3,\ \text{odd}), \\ 0 & \text{otherwise}. \end{cases}$$

Then, by comparing the coefficients of $U_1^{N_1}U_2^{N_2}$ in $\mathrm{Gass}^{\mathrm{red}}(g)|_{u_i=\exp(U_i)-1} = \mathcal{F}_g(U_1, U_2)$, we obtain the following theorem.

Theorem 7.3.3. *With notation as above, we have the following equality for* $g \in \mathrm{Gal}_{\mathbb{Q}}[1]$*:*

$$\sum_{\substack{n_1+n_2\geq 1\\ 0\leq n_1\leq N_1,\ 0\leq n_2\leq N_2}} \mu(g;n_1,n_2)a_{n_1}(N_1)a_{n_2}(N_2) = \sum_{1\leq n\leq N_1+N_2} \frac{(-1)^n}{n!} \sum \frac{\kappa_{m_1^{(1)}+m_2^{(1)}}(g)}{m_1^{(1)}!\,m_2^{(1)}!} \cdots \frac{\kappa_{m_1^{(n)}+m_2^{(n)}}(g)}{m_1^{(n)}!\,m_2^{(n)}!},$$

where the last sum ranges over integers $m_1^{(1)},\dots,m_1^{(n)},m_2^{(1)},\dots,m_2^{(n)} \geq 0$ 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

$$\mu(g;(12)) = \mu(g;(21)) = 0, \qquad \mu(g;(212)) + \mu(g;(121)) = 0,$$
$$\mu(g;(221)) + \mu(g;(2212)) + \mu(g;(1221)) + \mu(g;(2121)) = -\frac{\kappa_3(g)}{2},$$
$$\mu(g;(112)) + \mu(g;(1121)) + \mu(g;(2112)) + \mu(g;(1212)) = -\frac{\kappa_3(g)}{2}.$$

Acknowledgements

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. We would like to thank Hidekazu Furusho, Masanobu Kaneko, Nariya Kawazumi, Hiroaki Nakamura, Takayuki Oda, Kenji Sakugawa and Takao Satoh for communications. We also thank the referees for comments.

References

[Am] F. Amano, On a certain nilpotent extension over $\mathbb{Q}$ of degree 64 and the 4th multiple residue symbol, Tohoku Math. J. (2) **66** (2014), 501–522. Zbl 06431044 MR 3350281

[Ae] G. Anderson, The hyperadelic gamma function, Invent. Math. **95**, (1989), 63–131. Zbl 0682.14011 MR 0969414

[AI] G. Anderson and Y. Ihara, Pro-l branched coverings of $\mathbb{P}^1$ and higher circular l-units, Ann. of Math. (2) **128** (1988), 271–293. Zbl 0692.14018 MR 0960948

[Aa] S. Andreadakis, On the automorphisms of free groups and free nilpotent groups, Proc. London Math. Soc. **15** (1965), 239–268. Zbl 0135.04502 MR 0188307

[Ar] E. Artin, Theorie der Zöpfe, Abh. Math. Sem. Univ. Hamburg **4** (1925), 47–72. Zbl 51.0450.01 MR 3069440

[B] J. S. Birman, *Braids, links, and mapping class groups*, Annals of Mathematics Studies 82, Princeton University Press, Princeton, NJ; University of Tokyo Press, Tokyo, 1974. Zbl 0305.57013 MR 0375281

[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. Zbl 0142.22304 MR 0102539

[Da] M. Day, Nilpotence invariants of automorphism groups, Lecture notes (2010–2011).

[DDMS] J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups*, 2nd edition, Cambridge Studies in Advanced Mathematics 61, Cambridge University Press, Cambridge, 1999. Zbl 0934.20001 MR 1720368

[Dw] W. G. Dwyer, Homology, Massey products and maps between groups, J. Pure Appl. Algebra **6** (1975), 177–190. Zbl 0338.20057 MR 0385851

[F] R. H. Fox, Free differential calculus. I. Derivation in the free group ring, Ann. of Math. (2) **57** (1953), 547–560. Zbl 0050.25602 MR 0053938

[G] A. Grothendieck, *Revêtements étales et groupe fondamental*, Lecture Notes in Mathematics 224, Springer, 1971. Zbl 0234.14002 MR 0354651

[Ha] N. Habegger, Milnor, Johnson, and tree level perturbative invariants, Preprint (2000).

[HM] N. Habegger and G. Masbaum, The Kontsevich integral and Milnor's invariants, Topology **39** (2000), 1253–1289. Zbl 0964.57011 MR 1783857

[Hi] J. Hillman, *Algebraic invariants of links*, 2nd edition, Series on Knots and Everything 52, World Scientific, Hackensack, NJ, 2012. Zbl 1253.57001 MR 2931688

[Ih1] Y. Ihara, Profinite braid groups, Galois representations and complex multiplications, Ann. of Math. (2) **123** (1986), 43–106. Zbl 0595.12003 MR 0825839

[Ih2] Y. Ihara, On Galois representations arising from towers of coverings of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, Invent. Math. 86 (1986), 427–459. Zbl 0585.14020 MR 0860676

[Ih3] Y. Ihara, Arithmetic analogues of braid groups and Galois representations, in *Braids (Santa Cruz, CA, 1986)*, Contemporary Mathematics 78, Amer. Math. Soc., Providence, RI, 1988, 245–257. Zbl 0723.11063 MR 0975083

[Ih4] Y. Ihara, The Galois representation arising from $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and Tate twists of even degree, in *Galois groups over* $\mathbb{Q}$ *(Berkeley, CA, 1987)*, Math. Sci. Res. Inst. Publ. 16, Springer, New York, 1989, 299–313. Zbl 0706.14018 MR 1012169

[IKY] Y. Ihara, M. Kaneko and A. Yukinari, On some properties of the universal power series for Jacobi sums, in *Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986)*, Advanced Studies in Pure Mathematics 12, North-Holland, Amsterdam, 1987, 65–86. Zbl 0642.12012 MR 0948237

[J1] D. Johnson, An abelian quotient of the mapping class group $\mathcal{T}_g$, Math. Ann. **249** (1980), 225–242. Zbl 0409.57009 MR 0579103

[J2] D. Johnson, A survey of the Torelli group, in *Low-dimensional topology (San Francisco, Calif., 1981)*, Contemporary Mathematics 20, Amer. Math. Soc., Providence, RI, 1983, 165–179. Zbl 0553.57002 MR 0718141

[Ka] N. Kawazumi, Cohomological aspects of Magnus expansions, arXiv:math/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 Appl. **69** 1996, 165–172. Zbl 0852.55022 MR 1381688

[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, Doctoral Thesis, Kyushu University, 2017.

[Kr] D. Kraines, Massey higher products, Trans. Amer. Math. Soc. **124** (1966), 431–449. Zbl 0146.19201 MR 0202136

[MKS] W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory. Presentations of groups in terms of generators and relations*, Reprint of the 1976 2nd edition, Dover Publications, Mineola, NY, 2004. Zbl 1130.20307 MR 2109550

[Mi] J. Milnor, Isotopy of links, in *Algebraic geometry and topology, A symposium in honor of S. Lefschetz (eds. R. H. Fox, D. C. Spencer and A. W. Tucker)*, Princeton University Press, Princeton, NJ, 1957, 280–306. Zbl 0080.16901 MR 0092150

[Ms1] M. Morishita, Milnor invariants and Massey products for prime numbers, Compos. Math. **140** (2004), 69–83. Zbl 1066.11048 MR 2004124

[Ms2] M. Morishita, *Knots and primes – An introduction to arithmetic topology*, Universitext, Springer, 2011. Zbl 1267.57001 MR 2905431

[MT] M. Morishita and Y. Terashima, p-Johnson homomorphisms and pro-p groups, J. Algebra. **479** (2017), 102–136. Zbl 06766486 MR 3627278

[Mt1] S. Morita, Abelian quotients of subgroups of the mapping class group of surfaces, Duke Math. J. **70** (1993), 699–726. Zbl 0801.57011 MR 1224104

[Mt2] S. Morita, The extension of Johnson's homomorphism from the Torelli group to the mapping class group, Invent. Math. **111** (1993), 197–224. Zbl 0787.57008 MR 1193604

[Mu] K. Murasugi, On Milnor's invariant for links, Trans. Amer. Math. Soc. **124** (1966), 94–110. Zbl 0178.57602 MR 0198453

[MK] K. Murasugi and B. I. Kurpita, *A study of braids*, Mathematics and Its Applications 484, Kluwer Academic Publishers, Dordrecht, 1999. Zbl 0938.57001 MR 1731872

[N] H. Nakamura, Tangential base points and Eisenstein power series, in *Aspects of Galois theory (Gainesville, FL, 1996)*, London Math. Soc. Lecture Note Series 256, Cambridge University Press, Cambridge, 1999, 202–217. Zbl 0986.14013 MR 1708607

[NW] H. Nakamura and Z. Wojtkowiak, On explicit formulae for l-adic polylogarithms, in *Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999)*, Proc. Sympos. Pure Math. 70, Amer. Math. Soc., Providence, RI, 2002, 285–294. Zbl 1191.11022 MR 1935410

[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. Zbl 0021.00701 MR 1581597

[Sa] T. Satoh, A survey of the Johnson homomorphisms of the automorphism groups of free groups and related topics, in *Handbook of Teichmüller theory, volume V (ed. A. Papadopoulos)*, 2016, 167–209. Zbl 1344.30042 MR 3497296

[Se] J.-P. Serre, Lie algebras and Lie groups, Lecture Notes in Mathematics 1500, Springer, Berlin, 2006. Zbl 0742.17008 MR 2179691

[So] C. Soulé, On higher p-adic regulators, Lecture Notes in Mathematics 854, Springer, 1981, 372–401. Zbl 0488.12008 MR 0618313

[St] D. Stein, Massey products in the cohomology of groups with applications to link theory, Trans. Amer. Math. Soc. **318** (1990), 301–325. Zbl 0692.57002 MR 0958903

[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. Zbl 0354.55013 MR 0451251

[W1] Z. Wojtkowiak, On l-adic iterated integrals. I. Analog of Zagier conjecture, Nagoya Math. J. **176** (2004), 113–158. Zbl 1160.11333 MR 2108125

[W2] Z. Wojtkowiak, On l-adic iterated integrals. II. Functional equations and l-adic polylogarithms, Nagoya Math. J. **177** (2005), 117–153. Zbl 1161.11363 MR 2124549

[W3] Z. Wojtkowiak, On l-adic iterated integrals. III. Galois actions on fundamental groups, Nagoya Math. J. **178** (2005), 1–36. Zbl 1134.11331 MR 2145313

[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), 373–382. Zbl 1147.11034 MR 2376515