RIMS-1709

BRAID MONODROMIES ON PROPER CURVES AND PRO-ℓ GALOIS REPRESENTATIONS

By

Naotake TAKAO

November 2010

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

BRAID MONODROMIES ON PROPER CURVES AND PRO-ℓ GALOIS REPRESENTATIONS

NAOTAKE TAKAO

Abstract. Let C be a proper smooth geometrically connected hyperbolic curve over a field of characteristic 0 and ℓ a prime number. We prove the injectivity of the homomorphism from the pro-ℓ mapping class group attached to the two dimensional configuration space of C to the one attached to C, induced by the natural projection. We also prove a certain graded Lie algebra version of this injectivity. Consequently we show that the kernel of the outer Galois representation on the pro-ℓ pure braid group on C with n strings does not depend on n, even if $n = 1$. This extends a previous result by Ihara-Kaneko. By applying these results to the universal family over the moduli space of curves, we solve completely Oda's problem on the independency of certain towers of (infinite) algebraic number fields, which has been studied by Ihara, Matsumoto, Nakamura, Ueno and the author. Sequentially we obtain certain information of the image of this Galois representation and get obstructions to the surjectivity of the Johnson-Morita homomorphism at each sufficiently large even degree (as Oda predicts), for the first time for a proper curve.

0. Introduction and motivation

Many predecessors have been studying the Galois action on the étale fundamental group of an algebraic variety over an 'arithmetic' field. From this point of view, it is known that actual higher dimensional configuration spaces of an affine hyperbolic curve do not contain more information on the Galois group than the one dimensional configuration space, namely, the original curve in the pro-ℓ situation ([11], [15], [25]). The main purpose of this paper is to show that this also holds true for a proper (hyperbolic) curve.

This new result seems even more highly non-trivial and more mysterious, at least to the author, than the known results in the affine case.

Let k be a field, Y a connected scheme of finite type over Spec$k$, and $\bar{y}$ a geometric point on Y. Then we have a profinite group $\pi_1(Y, \bar{y})$ called the étale fundamental group ([8]). This topological group classifies finite étale coverings of Y: roughly speaking, there exists a one-to-one correspondence between the connected finite étale coverings of Y and the open subgroups of $\pi_1(Y, \bar{y})$. The isomorphism class of $\pi_1(Y, \bar{y})$ does not depend on the choice of the base point $\bar{y}$, and usually we do not specify $\bar{y}$ in the rest of this paper. Fix a separable closure $\bar{k}$ of k and assume that

2000 *Mathematics Subject Classification.* 14H30.

Key words and phrases. proper hyperbolic curve, braid group, mapping class group, Lie algebra, pro-ℓ Galois representation, universal monodromy representation.

The author dedicates this work to the memory of his mother, Yayoi, and grandmother, Maki Kawahara.

$\bar{Y} := Y \otimes_k \bar{k}$ is connected. Then the following exact sequence of profinite groups exists

$$1 \to \pi_1(\bar{Y}) \to \pi_1(Y) \overset{p_{Y/k}}{\to} G_k \to 1,$$

where G_k stands for the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$ of k.

This exact sequence gives rise to the following continuous homomorphism:

$$\begin{aligned} \rho_{Y/k} : G_k &\to \mathrm{Out}(\pi_1(\bar{Y})), \\ \sigma &\mapsto (\gamma \mapsto \tilde{\sigma}\gamma\tilde{\sigma}^{-1}) \bmod \mathrm{Inn}(\pi_1(\bar{Y})), \end{aligned} \tag{1}$$

where $\sigma \in G_k$, $\tilde{\sigma} \in p_{Y/k}^{-1}(\sigma)$ (an arbitrary lift of σ), $\gamma \in \pi_1(\bar{Y})$ and, for a topological group G, $\mathrm{Out}(G)$ denotes the group $\mathrm{Aut}(G)$ of all automorphisms of G divided by the group $\mathrm{Inn}(G)$ of all inner automorphisms of G. This homomorphism, which is often called outer Galois representation, carries the information of fields of definition of each covering of Y.

Suppose that k is of characteristic 0 and is embedded into $\mathbb{C}$. Then we have a comparison isomorphism

$$\pi_1(\bar{Y}) \cong \widehat{\pi_1^{top}(Y(\mathbb{C}))}.$$

Here $Y(\mathbb{C})$ means the complex analytic space associated to Y. $\pi_1^{top}(A)$ stands for the topological fundamental group of a complex analytic space A and $\widehat{G}$ stands for the profinite completion of a discrete group G.

So the isomorphism class of the geometric fundamental group $\pi_1(\bar{Y})$ is determined only by the homotopy type of $Y(\mathbb{C})$.

Moreover suppose that Y is separated smooth over $\mathrm{Spec}k$ and of dimension 1. Let g and r denote the geometric genus of the smooth compactification Y^* of Y and the number of $\bar{k}$-rational points on $Y^* \setminus Y$ respectively. We refer to such Y as a (g,r)-curve over k throughout this paper. The representation (1) in the case that Y is hyperbolic (*i.e.* $2-2g-r<0$) has been studied by many predecessors for this quarter of a century.

For each $n = 1, 2, \cdots$, the configuration space of distinct ordered n points on Y is defined as follows:

$$\begin{aligned} F_n(Y) &= Y^n \setminus \cup_{1 \le i < j \le n} \Delta_Y(i,j), \\ \Delta_Y(i,j) &= \{(y_1, \ldots, y_n) \in Y^n \mid y_i = y_j\}. \end{aligned}$$

Note that $F_1(Y) = Y$. We denote by $\Pi_{g,r}^{(n)top}$ the fundamental group of the configuration space of distinct ordered n points on a fixed r-punctured Riemann surface of genus g. Then there is an isomorphism

$$\pi_1^{top}(F_n(Y)(\mathbb{C})) \cong \Pi_{g,r}^{(n)top}.$$

Let ℓ be a prime number. Let $\Pi_{g,r}^{(n)}$ be the pro-ℓ completion of the discrete group $\Pi_{g,r}^{(n)top}$, that is to say, the maximal pro-ℓ quotient of $\widehat{\Pi_{g,r}^{(n)top}}$. Let $\widetilde{\Gamma}_{g,r}^{(n)(\text{pro-}\ell)}$ be the subgroup of $\mathrm{Aut}(\Pi_{g,r}^{(n)})$ which consists of all the elements preserving each 'fiber subgroup' and the conjugacy class of each inertia subgroup. Let $\Gamma_{g,r}^{(n)(\text{pro-}\ell)}$ be the subgroup $\widetilde{\Gamma}_{g,r}^{(n)(\text{pro-}\ell)}/\mathrm{Inn}(\Pi_{g,r}^{(n)})$ of $\mathrm{Out}(\Pi_{g,r}^{(n)})$, which is often called the 'n-dimensional' pro-ℓ mapping class group (cf. [26] §1, [25] §1 and §2, *etc.*).

There is a natural central filtration $\{\Pi_{g,r}^{(n)}(m)\}_{m\geq 1}$ of $\Pi_{g,r}^{(n)}$, called the weight filtration ([25] (2.3), [18] §1, *etc.*), which is preserved by the elements of $\widetilde{\Gamma}_{g,r}^{(n)(\text{pro-}\ell)}$. Sequentially this filtration induces a natural filtration $\{\Gamma_{g,r}^{(n)(\text{pro-}\ell)}(m)\}_{m\geq 1}$ of $\Gamma_{g,r}^{(n)(\text{pro-}\ell)}$. More precisely, $\Gamma_{g,r}^{(n)(\text{pro-}\ell)}(m)$ is defined to be the image of

$$\mathrm{Ker}(\tilde{\Gamma}_{g,r}^{(n)(\text{pro-}\ell)} \to \prod_{d\geq 1} \mathrm{Aut}(\Pi_{g,r}^{(n)}(d)/\Pi_{g,r}^{(n)}(d+m)))$$

in $\Gamma_{g,r}^{(n)(\text{pro-}\ell)}$. In what follows, for simplicity, we sometimes denote $\Pi_{g,r}^{(n)}$ by P_n and $\Gamma_{g,r}^{(n)(\text{pro-}\ell)}$ by Γ_n. Depending on the context, we use both notations.

For each $n \geq 1$, there is a natural projection $P_{n+1} \longrightarrow P_n$, obtained by forgetting a strand and it induces continuous group homomorphisms

$$\Gamma_{n+1}/\Gamma_{n+1}(m) \longrightarrow \Gamma_n/\Gamma_n(m) \quad (m \geq 1), \tag{2}$$

and

$$\Gamma_{n+1} \longrightarrow \Gamma_n. \tag{3}$$

Theorem 0.1. *(cf. Corollary 2.8, Corollary 2.11)*
If $2-2g-r<0$, the homomorphisms (2) and (3) are injective.

Remark 0.2. *The injectivity of (2) is an expansion of* [25] *which treats the case $r+n \geq 2$ (i.e. Y is affine or the dimension ≥ 2). The injectivity of (3) is a consequence of the first one combined with*

$$\bigcap_{m\geq 0} \Gamma_n(m) = \{1\} \quad (\textit{Lemma 2.10}),$$

which is a higher dimensional version of [2] *Theorem 2.*

Y.Ihara and M.Kaneko have already proved the injectivity of (3) when $3-2g-r-n<0$ and $r+n\geq 2$ ([15] *Theorem 1).*

This theorem is a rather immediate consequence of a certain Lie algebra version (Theorem 2.5) of it. Therefore Theorem 2.5 is the main technical result of this paper. However we would like to state an exact formulation of Theorem 2.5 in §2, since we need a lengthy preparation for it.

When $r+n \geq 2$, we profile derivations with some conditions to prove the assertion of Theorem 2.5 (*i.e.* [25] Theorem 4.3). However, in the case $r+n=1$, the Lie algebra does not have enough relations to profile derivations in the same way as in [25]. Thus, we prove it after going through various complicated calculations of Lie algebras in §1 and in §2.

Theorem 0.1 brings us the following many important arithmetical consequences. We begin with considering two kinds of pro-ℓ monodromy representations.

The first one is associated with a single curve. Let k be a field of characteristic 0 and embedded into $\mathbb{C}$. Let C be a (g,r)-curve over k. For each $n \geq 1$, we can consider the quotient representation of $\rho_{F_n(C)/k}$:

$$\rho_{F_n(C)/k}^{(\text{pro-}\ell)} : G_k \to \mathrm{Out}(\Pi_{g,r}^{(n)}). \tag{4}$$

The second one is associated with the universal family of curves. Let $\mathcal{M}_{g,r}$ be the moduli stack over $\mathbb{Q}$ of proper smooth geometrically connected curves of genus

g with disjoint ordered r sections. In [29], Takayuki Oda developed a theory of fundamental groups of algebraic stacks, from which, as in the case of a single curve, we obtain a monodromy representation

$$\Phi_{g,r}^{(n)(\text{pro-}\ell)} : \pi_1(\mathcal{M}_{g,r}) \to \text{Out}(\Pi_{g,r}^{(n)}), \tag{5}$$

called the pro-ℓ universal monodromy representation. It is known that the images of both $\rho_{F_n(C)/k}^{(\text{pro-}\ell)}$ and $\Phi_{g,r}^{(n)(\text{pro-}\ell)}$ are contained in the 'n-dimensional' pro-ℓ mapping class group $\Gamma_{g,r}^{(n)(\text{pro-}\ell)}$ when all points of $C^* \setminus C$ are k-rational. See the second paragraph in §3 for more detail.

With each of these two kinds of representations, a field tower is associated. More precisely it is defined as follows:
The field tower $\{k_C^{(n)(\text{pro-}\ell)}(m)\}_{m\geq 1}$ for $\rho_{F_n(C)/k}^{(\text{pro-}\ell)}$ is defined by

$$k_C^{(n)(\text{pro-}\ell)}(m) := \bar{k}^{(\rho_{F_n(C)/k}^{(\text{pro-}\ell)})^{-1}(\Gamma_{g,r}^{(n)(\text{pro-}\ell)}(m))}.$$

The field tower $\{\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)}(m)\}_{m\geq 1}$ for $\Phi_{g,r}^{(n)(\text{pro-}\ell)}$ is defined by

$$\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)}(m) := \bar{\mathbb{Q}}^{p_{g,r}((\Phi_{g,r}^{(n)(\text{pro-}\ell)})^{-1}(\Gamma_{g,r}^{(n)(\text{pro-}\ell)}(m)))}.$$

where $p_{g,r}$ is the projection $\pi_1(\mathcal{M}_{g,r}) \to G_{\mathbb{Q}}$. The field tower $\{\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)}(m)\}_{m\geq 1}$ is defined by Y.Ihara ($g = 0$, $r = 3$ and $n = 1$ in [10]), T.Oda ($g \geq 2$, $r = 0$ and $n = 1$ in [28]) and H.Nakamura (g, r and n general in [25]).
Moreover the fields $k_C^{(n)(\text{pro-}\ell)}$ and $\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)}$ are defined as follows:

$$k_C^{(n)(\text{pro-}\ell)} := \bar{k}^{\text{Ker}\rho_{F_n(C)/k}^{(\text{pro-}\ell)}},$$
$$\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)} := \bar{\mathbb{Q}}^{p_{g,r}(\text{Ker}\Phi_{g,r}^{(n)(\text{pro-}\ell)})}.$$

In what follows we shall often omit the superscript (1) that expresses one dimension. For example we write $\Pi_{g,r} = \Pi_{g,r}^{(1)}$, $\Gamma_{g,r}^{(\text{pro-}\ell)} = \Gamma_{g,r}^{(1)(\text{pro-}\ell)}$, $k_C^{(\text{pro-}\ell)} = k_C^{(1)(\text{pro-}\ell)}$, $\mathbb{Q}_{g,r}^{(\text{pro-}\ell)} = \mathbb{Q}_{g,r}^{(1)(\text{pro-}\ell)}$, and $\mathbb{Q}_{g,r}^{(\text{pro-}\ell)}(m) = \mathbb{Q}_{g,r}^{(1)(\text{pro-}\ell)}(m) \quad (m \geq 1)$.

Roughly speaking, $\mathbb{Q}_{g,r}^{(\text{pro-}\ell)}$ is the maximal subfield of $k_C^{(\text{pro-}\ell)}$ which does not depend on the moduli of the (g,r)-curve C. We note that $\mathbb{Q}_{g,r}^{(\text{pro-}\ell)}(1) = \mathbb{Q}(\mu_{\ell^\infty})$. It is known that $[\mathbb{Q}_{g,r}^{(\text{pro-}\ell)}(2m) : \mathbb{Q}_{g,r}^{(\text{pro-}\ell)}(2m-1)] < \infty$ (cf. [25] (6.2)) and the tower $\{\mathbb{Q}_{0,3}^{(\text{pro-}\ell)}(2m)\}_{m\geq 1}$ coincides with Ihara's tower $\{\mathbb{Q}(m)\}_{m\geq 1}$ ([10], [12]). Note that the union $\cup_{m\geq 1}\mathbb{Q}(m)$ is described explicitly in terms of higher circular ℓ-units in [1].

Remark 0.3. *(cf. Remark 3.1) (1)We have*

$$k_C^{(n)(pro\text{-}\ell)} = \bigcup_{m\geq 1} k_C^{(n)(pro\text{-}\ell)}(m),$$

and

$$\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)} = \bigcup_{m\geq 1} \mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}(m).$$

(2)We have

$$\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}(m) \subset k_C^{(n)(pro\text{-}\ell)}(m) \qquad (m \geq 1).$$

(3) We have

$$\mathbb{Q}^{(n)(pro\text{-}\ell)}_{\mathbb{P}^1\setminus\{0,1,\infty\}}(m) = \mathbb{Q}^{(n)(pro\text{-}\ell)}_{0,3}(m) \qquad (m \geq 1).$$

We proceed in studying various independency of the above two kinds of field towers.

At first it is known that the field tower $\{k_C^{(n)(\text{pro-}\ell)}(m)\}_{m\geq 1}$ is independent of n if $r+n \geq 2$ by Ihara and Kaneko ([11], [15]). In this paper we remove the assumption $r+n \geq 2$.

Theorem 0.4. *(cf. Theorem 3.2) Suppose that C is hyperbolic. For $n \geq 1$,*

$$k_C^{(n)(pro\text{-}\ell)}(m) = k_C^{(pro\text{-}\ell)}(m) \qquad (m \geq 1).$$

In particular,

$$k_C^{(n)(pro\text{-}\ell)} = k_C^{(pro\text{-}\ell)}.$$

Theorem 0.4 gives a non-trivial example in which the kernel of the Galois action on the pro-ℓ fundamental group of a proper variety is the same as that of the variety minus a divisor. It implies that the smallest common field of definition of finite étale Galois coverings of $F_n(C)$ $(n \geq 2)$ of degree ℓ-th power is not larger than that of C even in the case where C is proper. This conclusion looks highly non-trivial and mysterious at least to the author.

Next in the situation of the universal family of curves, Oda predicts that this tower is independent of (g, r) ([28]). It has been already established that the tower $\{\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)}(m)\}_{m\geq 1}$ is almost independent of g, r and n under the assumption $r+n \geq 2$ ([20], [25], [22], [16]) We extend these results by removing the assumption $r+n \geq 2$.

Theorem 0.5. *(cf. Theorem 3.6) If $2-2g-r < 0$, $n \geq 1$, then*

(1) $\{\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}(m)\}_{m\geq 1}$ is independent of r and n and almost independent of g, r and n in the following sense :

$$\mathbb{Q}^{(pro\text{-}\ell)}_{1,1}(m) \supset \mathbb{Q}^{(n)(pro\text{-}\ell)}_{g,r}(m) \supset \mathbb{Q}^{(pro\text{-}\ell)}_{0,3}(m),$$
$$[\mathbb{Q}^{(pro\text{-}\ell)}_{1,1}(m) : \mathbb{Q}^{(n)(pro\text{-}\ell)}_{g,r}(m)], [\mathbb{Q}^{(n)(pro\text{-}\ell)}_{g,r}(m) : \mathbb{Q}^{(pro\text{-}\ell)}_{0,3}(m)] < \infty.$$

(2) $\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}$ is independent of g, r and n.

We have two applications of Theorem 0.5. The first one is on the image of the Galois representation $\rho_{C/k}^{(\text{pro-}\ell)}$. For each $m \geq 1$, set

$$\text{gr}_C^{[\ell]^m} G_k := \text{Gal}(k_C^{(\text{pro-}\ell)}(m+1)/k_C^{(\text{pro-}\ell)}(m)),$$
$$\text{gr}_{g,r}^{[\ell]^m} G_{\mathbb{Q}} := \text{Gal}(\mathbb{Q}_{g,r}^{(\text{pro-}\ell)}(m+1)/\mathbb{Q}_{g,r}^{(\text{pro-}\ell)}(m)).$$

Theorem 0.6. *(cf. Corollary 4.1) Suppose that C is hyperbolic. Then we have*

$$dim_{\mathbb{Q}_\ell}(\text{gr}_C^{[\ell]^m} G_k \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) \geq r_m,$$

where $r_m = dim_{\mathbb{Q}_\ell}(\text{gr}_{0,3}^{[\ell]^m} G_{\mathbb{Q}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$.

For the value of r_m, see Remark 4.4. In the affine case, Theorem 0.6 is proved ([22] §4).

The second application is one on the so-called Johnson-Morita homomorphism τ_m in low-dimensional topology ([17], [21]). (See §4 for a definition of τ_m).

Theorem 0.7. *(cf. Corollary 4.5) If $2-2g-r<0$, then*

$$dim_{\mathbb{Q}_\ell}\mathrm{Coker}(\tau_m \otimes_{\mathbb{Z}} \mathbb{Q}_\ell) \geq r_m \qquad (m \geq 1).$$

In particular, if $m \neq 2, 4, 8, 12$ and m is even, then $\tau_m \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ is not surjective.

For the dimension of the cokernel of the Johnson-Morita homomorphism τ_m, several kinds of bounds have been obtained so far by S.Morita ([21]), T.Oda ([27]) and H.Nakamura ([22]). However, we remark that any single obstruction to the surjectivity of τ_m has not been known in the proper case $r=0$.

The contents of this paper are as follows. In Section 1, we show some lemmas on free Lie algebras, among which Proposition 1.3 is the main result. In Section 2, we show some properties of the graded Lie algebra associated to $\Pi_{g,r}^{(n)}$. Especially in the case $(r,n)=(0,2)$, we study this Lie algebra in detail by using its presentation, together with the results of Section 1, and get Lemma 2.2, which is the main tool to prove the main technical result Theorem 2.5 of this paper. After establishing Theorem 2.5, we deduce the main injectivity results (Corollary 2.8 and Corollary 2.11). In Section 3, we accomplish the main independency theorems (Theorem 3.2 and Theorem 3.4) and give a solution to Oda's problem (Theorem 3.6). In Section 4, we present the above-mentioned two applications (Corollary 4.1 and Corollary 4.5).

1. Some lemmas on free Lie algebras

The purpose of this section is to show Proposition 1.3, which is at the core to verify Lemma 2.2 in §2. Since the proof of Proposition 1.3 is elementary but needs lengthy and complicated calculation, the reader may skip through this section to the next section at the first reading.

Notations. Throughout this section, we fix an integral domain K with fraction field of characteristic 0 and a set S. We denote by $L\langle S\rangle$ the free Lie algebra over K with free generating set S. For $s \in S$ and $w \in L\langle S\rangle$, we denote by $deg_s(w)$ the degree of s in w. For a Lie algebra L over K and a subset T of L, we denote the centralizer of T in L by $C_L(T)$, the center $C_L(L)$ by $Z(L)$, and the Lie subalgebra (resp. the submodule) generated by T over K by $\langle T\rangle_{Lie}$ (resp. $\langle T\rangle_{vec}$). For $w, w', \cdots \in L$, $C_L(w, w', \cdots)$ means $C_L(\{w, w', \cdots\})$ and $\langle w, w', \cdots\rangle_{Lie}(resp.\langle w, w', \cdots\rangle_{vec})$ means $\langle\{w, w', \cdots\}\rangle_{Lie}(resp.\langle\{w, w', \cdots\}\rangle_{vec})$. For a Lie algebra L over K, a derivation on L means a K-linear endomorphism D on L such that $D[A,B]=[D(A),B]+[A,D(B)]$ for any A, $B \in L$. We denote by $\mathrm{Der}(L)$ the set of all derivations on L, which is equipped with the structure of K-Lie algebra by operation $[D,D']=DD'-D'D$. For $A, B \in L$, we denote $ad(A)^n(B)=\underbrace{[A,[A,...,[A}_{n},B]]...]$ by A^nB and write $AB=A^1B$.

Lemma 1.1. *We have*

$$C_{L\langle S\rangle}(\{s\}) = \langle s\rangle_{vec}$$

for any $s \in S$.

Proof. See, e.g., [7] Lemma 2.2. □

Lemma 1.2. *(cf.* [31]*) Set* $L = L\langle S\rangle$. *Let* $T \subset L$ *and* $w \in L$. *If there exist* $S' \subset L$, $\lambda \in K^\times$, $s'_0 \in S'$, $w' \in \langle S' \setminus \{s'_0\}\rangle_{Lie}$, *such that* $T \subset S' \setminus \{s'_0\}$, *that* $\langle S'\rangle_{Lie}$ *is free with free generating set* S' *(namely,* $\langle S'\rangle_{Lie} \overset{\sim}{\leftarrow} L\langle S'\rangle$*), and that*

$$w = \lambda s'_0 + w',$$

then $\langle T, w\rangle_{Lie}$ *is free with free generating set* $T \amalg \{w\}$ *(namely,* $\langle T, w\rangle_{Lie} \overset{\sim}{\leftarrow} L\langle T \amalg \{w\}\rangle$*).*

Proof. $\langle S'\rangle_{Lie} \cong L\langle S'\rangle$ admits a Lie algebra automorphism θ defined by $\theta(s'_0) = \lambda^{-1}(s'_0 - w')$ and $\theta(s') = s'$ for $s' \in S' \setminus \{s'_0\}$. (The inverse map θ^{-1} is given by $\theta^{-1}(s'_0) = w$ and $\theta^{-1}(s') = s'$ for $s' \in S' \setminus \{s'_0\}$.) We see that $\theta|_T = id_T$ and $\theta(w) = s'_0$. As $T \cup \{s'_0\}$ is a free generating set, so is $T \cup \{w\}$ □

Proposition 1.3. *Assume that* S *is a finite set* $\{A_1, ..., A_h\}$ *of cardinality* $h \geq 4$ *and set* $L_A = L\langle S\rangle$. *Let* $\mathcal{D}$ *be a derivation on* L_A *such that* $\mathcal{D}(A_2) + A_3A_4 \in \langle\{A_\alpha; 4 \leq \alpha \leq h\}\rangle_{Lie}$ *and that* $\mathcal{D}(A_\alpha) = A_1A_\alpha$ *for all* $\alpha \neq 2$. *Then* $\mathrm{Ker}\mathcal{D} = \langle A_1, E_\mathcal{D}\rangle_{Lie}$, *where* $E_\mathcal{D} := \mathcal{D}(A_2) - A_1A_2$.

Proof. By the assumption on $\mathcal{D}$, $\mathrm{Ker}\mathcal{D} \supset \langle A_1, E_\mathcal{D}\rangle_{Lie}$. We shall prove the other inclusion.

First of all we shall eliminate A_1 to compute $\mathrm{Ker}\mathcal{D}$. The elimination theorem ([6] Ch.2 §2 Proposition 10) ensures that a K-linear isomorphism

$$L_A \simeq \langle A_1\rangle_{Lie} \oplus L'_A,$$

where

$$L'_A := \langle A_1^m A_\alpha; m \geq 0, \alpha \geq 2\rangle_{Lie}.$$

Applying Lemma 1.2 to $L = L_A$, $T = \{A_1\}$, $w = E_\mathcal{D}$, $S' = \{A_2^m A_\alpha; m \geq 0, \alpha \neq 2\}$, $\lambda = 1$ and $s'_0 = A_2A_1$, we have $\langle A_1, E_\mathcal{D}\rangle_{Lie} = L\langle A_1, E_\mathcal{D}\rangle$. Hence

$$\langle A_1, E_\mathcal{D}\rangle_{Lie} \simeq \langle A_1\rangle_{Lie} \oplus \langle A_1^{m-1}E_\mathcal{D}; m \geq 1\rangle_{Lie},$$

by the elimination theorem. Observing that $\{A_1^{m-1}E_\mathcal{D}; m \geq 1\} \subset L'_A$ and the above isomorphism ($L_A \simeq \langle A_1\rangle_{Lie} \oplus L'_A$), we have

$$\langle A_1, E_\mathcal{D}\rangle_{Lie} \cap L'_A = \langle A_1^{m-1}E_\mathcal{D}; m \geq 1\rangle_{Lie}.$$

Taking $\mathrm{Ker}\mathcal{D} \supset \langle A_1\rangle_{Lie}$ into account, $\mathrm{Ker}\mathcal{D} \subset \langle A_1, E_\mathcal{D}\rangle_{Lie}$ if and only if $\mathrm{Ker}(\mathcal{D}|_{L'_A}) \subset \langle A_1^{m-1}E_\mathcal{D}; m \geq 1\rangle_{Lie}$.

Next we shall take another free generating set of the free K-Lie algebra L'_A, extending $\{A_1^{m-1}E_\mathcal{D}; m \geq 1\}$.

Let $B_{n,\beta}$ ($n \geq 0$ and $h \geq \beta \geq 2$) be mutually distinct indeterminates and $L_B := L\langle\{B_{n,\beta}; n \geq 0, \beta \geq 2\}\rangle$. By the assumption of $\mathcal{D}$, $A_1^{m-1}\mathcal{D}(A_2) \in \langle A_1^m A_\alpha; m \geq 0, \alpha \geq 3\rangle_{Lie}$. Thus we have the following Lie algebra homomorphism

$$\begin{aligned}
&\theta : L'_A \longrightarrow L_B,\\
&A_1^m A_\alpha \longmapsto B_{m,\alpha} \qquad (\alpha \neq 2 \quad or \quad m = 0),\\
&A_1^m A_2 \longmapsto -B_{m,2} + \theta(A_1^{m-1}\mathcal{D}(A_2)) \qquad (m \geq 1),
\end{aligned}$$

which is bijective, with the inverse map being given by

$$\begin{aligned} B_{n,2} &\longmapsto A_1^{n-1}E_{\mathcal{D}} \qquad (n \geq 1), \\ B_{n,\beta} &\longmapsto A_1^n A_\beta \qquad (\beta \neq 2 \quad or \quad n = 0), \end{aligned}$$

because of the assumption on $\mathcal{D}(A_2)$. We denote $L\langle B_{n,\beta}; n \geq 0, \beta \geq 2\rangle$ by L_B. From the assumption of $\mathcal{D}$, $\mathcal{D}$ induces on L_B the following derivation $\mathcal{D}_B$:

$$\begin{aligned} \mathcal{D}_B : L_B &\longrightarrow L_B, \\ B_{n,\beta} &\longmapsto B_{n+1,\beta} \qquad (\beta \geq 3), \\ B_{0,2} &\longmapsto \theta(\mathcal{D}(A_2)), \\ B_{n,2} &\longmapsto 0 \qquad (n \geq 1). \end{aligned}$$

It is easy to see $\mathrm{Ker}(\mathcal{D}|_{L'_A}) \subset \langle A_1^{m-1}E_{\mathcal{D}}; m \geq 1\rangle_{Lie}$ if and only if $\mathrm{Ker}\mathcal{D}_B \subset \langle B_{n,2}; n \geq 1\rangle_{Lie}$.

To prove the latter inclusion, we shall first prove $\mathrm{Ker}\mathcal{D}_B \subset \langle B_{n,2}; n \geq 0\rangle_{Lie}$. For each $n \geq 0$, $n' \geq 0$, $h \geq \beta \geq 2$, $h \geq \beta' \geq 2$, $s \geq 0$, $t \geq 0$, let $L_B(B_{n,\beta}, B_{n',\beta'}; s, t)$ be $\langle$ all monomials with the degree of $B_{n,\beta}$ being s and the degree of $B_{n',\beta'}$ t $\rangle_{vec}$, $p(B_{n,\beta}, B_{n',\beta'}; s, t)$: $L_B \to L_B(B_{n,\beta}, B_{n',\beta'}; s, t)$ the canonical projection. For $n \geq 0$ and $h \geq \beta \geq 2$, let $u(n, \beta)$:$L_B \to L_B$ be the K-Lie algebra endomorphism of L_B given by

$$\begin{aligned} B_{n+1,\beta} &\mapsto B_{n,\beta}, \\ B_{n',\beta'} &\mapsto B_{n',\beta'} \quad ((n', \beta') \neq (n+1, \beta)). \end{aligned}$$

If $b \in L_B \setminus \langle B_{n,2}; n \geq 0\rangle_{Lie}$, then there exists $n_0 \geq 0$, $\beta_0 \geq 3$, $d_0 \geq 1$ such that

$$\begin{aligned} deg_{B_{n,\beta}}(b) &= 0 \qquad (n \geq 0 \quad and \quad \beta > \beta_0), \\ deg_{B_{n,\beta_0}}(b) &= 0 \qquad (n > n_0), \\ deg_{B_{n_0,\beta_0}}(b) &= d_0. \end{aligned}$$

Then we have

$$\begin{aligned} u(n_0, \beta_0) \circ p(B_{n_0,\beta_0}, B_{n_0+1,\beta_0}; d_0 - 1, 1) \circ \mathcal{D}_B(b) \\ &= d_0 p(B_{n_0,\beta_0}, B_{n_0+1,\beta_0}; d_0, 0)(b) \\ &\neq 0. \end{aligned}$$

Hence $\mathcal{D}_B(b) \neq 0$. Therefore $\mathrm{Ker}\mathcal{D}_B \subset \langle B_{n,2}; n \geq 0\rangle_{Lie}$.

Next we shall proceed to show that $\mathrm{Ker}\mathcal{D}_B \subset \langle B_{n,2}; n \geq 1\rangle_{Lie}$. Applying Lemma 1.2 to $S = \{B_{n,\beta}; n \geq 0, 2 \leq \beta \leq h\}$, $w = \mathcal{D}_B(B_{0,2})$, $T = \{B_{n,2}; n \geq 0\}$, $S' = \{B_{0,3}^\nu B_{n,\beta}; 2 \leq \beta \leq h, n \geq 0, \nu \geq 0, (n, \beta) \neq (0, 3)\}$, $\lambda = -1$, $s'_0 = B_{0,3}B_{0,4}$, and $w' = \mathcal{D}_B(B_{0,2}) + B_{0,3}B_{0,4}$, we can see that $\langle B_{n,2}, \mathcal{D}_B(B_{0,2}); n \geq 0\rangle_{Lie} \simeq L\langle B_{n,2}, \mathcal{D}_B(B_{0,2}); n \geq 0\rangle$, denoted by $L_{\mathcal{D}_B}$. Hence we can define $u_2 : L_{\mathcal{D}_B} \to L_B$, a K-Lie algebra homomorphism, given by

$$\begin{aligned} \mathcal{D}_B(B_{0,2}) &\mapsto B_{0,2}, \\ B_{n,2} &\mapsto B_{n,2} \quad (n \geq 0). \end{aligned}$$

If $b \in \langle B_{n,2}; n \geq 0\rangle_{Lie} \setminus \langle B_{n,2}; n \geq 1\rangle_{Lie}$, then there exists $d_0 \geq 1$ such that $deg_{B_{0,2}}(b) = d_0$. Then we have

$$u_2 \circ p(B_{0,2}, \mathcal{D}_B(B_{0,2}); d_0 - 1, 1) \circ \mathcal{D}_B(b) = d_0 p(B_{0,2}, \mathcal{D}_B(B_{0,2}); d_0, 0)(b) \neq 0.$$

Here $p(B_{0,2}, \mathcal{D}_B(B_{0,2}); s, t)$ is the canonical projection, which is defined in a similar way as the above-mentioned $p(B_{n,\beta}, B_{n',\beta'}; s, t)$. Hence $\mathcal{D}_B(b) \neq 0$. Therefore $\mathrm{Ker}\mathcal{D}_B \subset \langle B_{n,2}; n \geq 1\rangle_{Lie}$, which completes the proof. □

2. Braid groups on compact Riemann surfaces and injectivity results for their outer automorphism groups

The main purpose of this section is as follows. First, we show Lemma 2.2 by using Proposition 1.3. Second, we obtain Theorem 2.5 by using Lemma 2.2. Third, we establish the main injectivity results (Corollary 2.8 and Corollary 2.11), as corollaries of Theorem 2.5. These corollaries are key ingredients of the proof of the main results Theorem 3.2 and Theorem 3.6 of this paper.

2.1. **Some basic facts about surface groups and braid groups.** We shall begin by recalling some facts about surface groups and braid groups ([15], [24], [25],etc). Let $g \geq 0$ and $r \geq 0$. Let $R_{g,r}$ be an r-punctured Riemann surface of genus g, and for each $n = 1, 2, \ldots$ set

$$F_n(R_{g,r}) := R^n_{g,r} \setminus \bigcup_{1 \leq i < j \leq n} \Delta_{i,j},$$

where $\Delta_{i,j} := \{(x_1, \ldots, x_n) \in R^n_{g,r} | x_i = x_j\}$. We denote by $\Pi^{(n)top}_{g,r}$ the topological fundamental group $\pi^{top}_1(F_n(R_{g,r}), b)$ of $F_n(R_{g,r})$ with the base point $b = (b_1, \ldots, b_n) \in F_n(R_{g,r})$ and write $\Pi^{top}_{g,r}$ for $\Pi^{(1)top}_{g,r}$.

We fix $g \geq 0, r \geq 0, n \geq 1$. For each $j = 1, \ldots, n+1$, the canonical projection $R^{(n+1)}_{g,r} \stackrel{f_j}{\to} R^{(n)}_{g,r}$ defined by $f_j(p_1, \cdots, p_{n+1}) = (p_1, \stackrel{j}{\cdots}, p_{n+1})$ gives a locally trivial topological fibration. By means of topological homotopy theory, we see that f_j induces a short homotopy exact sequence

$$(6) \quad 1 \to \pi^{top}_1(R_{g,r} \setminus \{b_1, \stackrel{j}{\cdots}, b_{n+1}\}, b_j) \to \pi^{top}_1(F_{n+1}(R_{g,r}), (b_1, \cdots, b_{n+1})) \stackrel{\pi^{top}_1(f_j)}{\to} \pi^{top}_1(F_n(R_{g,r}), (b_1, \stackrel{j}{\cdots}, b_{n+1})) \to 1.$$

We shall denote the leftmost group $\pi^{top}_1(R_{g,r} \setminus \{b_1, \stackrel{j}{\cdots}, b_{n+1}\}, b_j)$ of the above exact sequence (6) by $N^{(j)top}_{n+1} (\simeq \Pi^{top}_{g,r+n})$.

Let $x^{(j)}_i, z^{(j)}_k$ $(1 \leq i \leq 2g, 1 \leq j \leq n+1, 1 \leq k \leq r+n+1, k \neq r+j)$ be the canonical generators of $N^{(j)\,top}_{n+1}$ (cf. Fig.1);

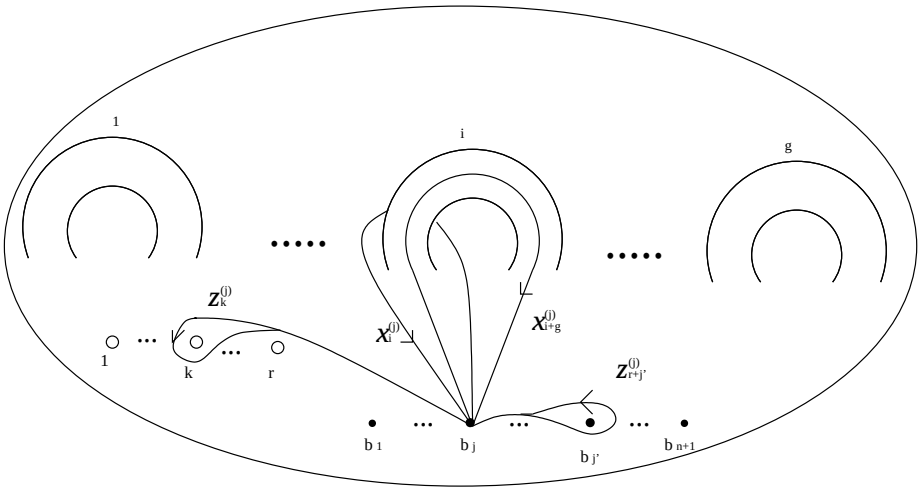

Fig.1.Generators of $N_{n+1}^{(j)top}(\simeq \Pi_{g,r+n}^{top}) \subset \pi_1^{top}(F_{n+1}(R_{g,r}),(b_1,\ldots,b_{n+1}))(\simeq \Pi_{g,r}^{(n+1)top})$

Let ℓ be a prime number. We denote the pro-ℓ completion of $\Pi_{g,r}^{(n)top}$ by $\Pi_{g,r}^{(n)}$ or P_n and write $\Pi_{g,r}$ for $\Pi_{g,r}^{(1)}$. The exact sequence (6) of (discrete) groups induces one of pro-ℓ groups

$$1 \to N_{n+1}^{(j)} \to P_{n+1} \overset{\pi_1(f_j)}{\to} P_n \to 1, \tag{7}$$

(cf.[15] (1.2.2)), where $N_{n+1}^{(j)}$ means the pro-ℓ completion of $N_{n+1}^{(j)top}$.

For $1 \le i \le 2g, 1 \le j \le n+1, 1 \le k \le r+n+1$ and $k \ne r+j$, we identify $x_i^{(j)}, z_k^{(j)}$ with their images in $N_{n+1}^{(j)}$ and moreover with those in P_{n+1}. They make up a generating set of P_{n+1}. We remark that a presentation of P_n is well-known for $n = 1, 2, \cdots$([30]). We have a natural central filtration $\{P_n(m)\}_{m=1}^{\infty}$ of P_n, called the weight filtration ([18] §1, [25] (2.3)). We note that this filtration coincides with the lower central filtration in the case $r \le 1$ and $n = 1$. For $m \ge 1$, let $\mathrm{gr}^m P_n$ denote the m-th graded piece $P_n(m)/P_n(m+1)$ of P_n with respect to the weight filtration. The direct sum

$$\mathrm{Gr}\Pi_{g,r}^{(n)} = \mathrm{Gr}P_n := \bigoplus_{m \ge 1} \mathrm{gr}^m P_n$$

becomes a graded $\mathbb{Z}_\ell$-Lie algebra naturally.

The exact sequence (7) of pro-ℓ groups induces one of graded $\mathbb{Z}_\ell$-Lie algebras

$$0 \to \mathrm{Gr}N_{n+1}^{(j)} \to \mathrm{Gr}P_{n+1} \overset{\mathrm{Gr}\pi_1(f_j)}{\to} \mathrm{Gr}P_n \to 0 \tag{8}$$

for $j = 1, \cdots, n+1$ (cf. [25] (2.8.1)). We note that $\mathrm{gr}^m P_{n+1}$ is generated by $\bigcup_{1 \le j \le n+1} \mathrm{gr}^m N_{n+1}^{(j)}$ as $\mathbb{Z}_\ell$-module for each $m \ge 1$([25] (2.7)), and that $\mathrm{Gr}P_{n+1}$ is center-trivial when $2-2g-r < 0$ (cf. [25] (2.8)).

2.2. **Some properties of** $\mathrm{Gr}\Pi_{g,0}^{(2)}$**.** Throughout this subsection, we consider $\mathrm{Gr}P_2$ for $g \ge 2$ and $r = 0$ (namely, $\mathrm{Gr}P_2 = \mathrm{Gr}\Pi_{g,0}^{(2)}$) in detail. At first we recall a presentation of $\mathrm{Gr}P_2$ ([25] (2.8.2)).

We denote $x_i^{(j)} \bmod \Pi_{g,0}^{(2)}(2)$ by $X_i^{(j)}$ and $z_{j'}^{(j)} \bmod \Pi_{g,0}^{(2)}(3)$ by $Z^{(j)}$, where $\{j, j'\} = \{1, 2\}$. We remark that $\mathrm{Gr}N_2^{(j)} = L\langle\{X_i^{(j)}; 1 \le i \le 2g\}\rangle$. We also note that

$Z^{(1)} = Z^{(2)}$ and denote this element by Z. Now, we have the following presentation of $\mathrm{Gr}P_2$:

$$\text{(9)} \qquad \text{generators} \qquad X_i^{(j)}, Z \qquad (1 \le i \le 2g, 1 \le j \le 2),$$

$$\text{(10)} \qquad \text{relations} \qquad \sum_{i=1}^{g} [X_i^{(j)}, X_{i+g}^{(j)}] + Z = 0 \qquad (1 \le j \le 2),$$

$$\text{(11)} \qquad [X_i^{(j)}, X_{i'}^{(j')}] = \begin{cases} 0 & (j \ne j',\ i \le i' \text{ and } i' \ne i+g), \\ Z & (j \ne j',\ i \le i' \text{ and } i' = i+g). \end{cases}$$

Observe that (10) and (11) imply

$$\text{(12)} \qquad [X_i^{(1)} + X_i^{(2)}, Z] = 0 \qquad (1 \le i \le 2g).$$

For simplicity we shall denote $C_{\mathrm{Gr}P_2}(w)$ by $C(w)$ for $w \in \mathrm{Gr}P_2$. We shall also abbreviate suffix signifying the second strand (e.g. $N_2^{(2)} = N_2$, $X_i^{(2)} = X_i$, *etc.*) and write just N for N_2.

Lemma 2.1. *(1)* $\mathrm{Gr}P_2 = \mathrm{Gr}N + C(Z)$.
(2) $\mathrm{Gr}N \cap C(Z) = \langle Z \rangle_{vec}$.

Proof. (1) Thanks to (12), it is easy to see that $X_i^{(1)} \in \mathrm{Gr}N + C(Z)$. Since $\mathrm{Gr}N$ is a Lie ideal and $C(Z)$ is a Lie subalgebra, the conclusion follows immediately.

(2) Let $T = \{X_1^n X_i\,;\, n \ge 0,\, 2g \ge i \ge 2\}$. As $\mathrm{Gr}N = L\langle\{X_i; 1 \le i \le 2g\}\rangle$, by the elimination theorem ([6] Ch.2 §2 Proposition 10), we have an isomorphism as $\mathbb{Z}_\ell$-modules

$$\mathrm{Gr}N \simeq \langle X_1 \rangle_{Lie} \oplus \langle T \rangle_{Lie},$$

and

$$\langle T \rangle_{Lie} \simeq L\langle T \rangle.$$

Let $V_{n,i}$ $(n \ge 0,\, 2g \ge i \ge 2)$ be mutually distinct variables and $L_V := L\langle V_{n,i}; 2 \le i \le 2g, n \ge 0\rangle$. Then we have an isomorphism as $\mathbb{Z}_\ell$-Lie algebras

$$\theta : L\langle T \rangle \to L_V,$$

$$X_1^n X_{1+g} \mapsto -V_{n,1+g} - \sum_{i=2}^{g} \sum_{\nu=0}^{n-1} \binom{n-1}{\nu} [V_{\nu,i}, V_{n-1-\nu,i+g}] \qquad (n \ge 1),$$

$$X_1^n X_i \mapsto V_{n,i} \qquad (otherwise),$$

whose inverse homomorphism is given in the following:

$$V_{n,1+g} \mapsto -X_1^n X_{1+g} - \sum_{i=2}^{g} \sum_{\nu=0}^{n-1} \binom{n-1}{\nu} [X_1^\nu X_i, X_1^{n-1-\nu} X_{i+g}] \qquad (n \ge 1),$$

$$V_{n,i} \mapsto X_1^n X_i \qquad (otherwise).$$

Observed that $\theta(Z) = V_{1,1+g}$ and $\theta([X_1, Z]) = V_{2,1+g}$. Hence $[X_1, Z]$ is transformed to an element of degree 1 in L_V and $[W, Z]$ to one of degree ≥ 2 in L_V for

any $W \in L\langle T\rangle$. Thus

$$\mathrm{Gr}N \cap C(Z) \subset L\langle T\rangle$$

or, equivalently,

$$\mathrm{Gr}N \cap C(Z) = C_{L\langle T\rangle}(Z).$$

Now, we have

$$\begin{aligned}\theta(\mathrm{Gr}N \cap C(Z)) &= \theta(C_{L\langle T\rangle}(Z)) \\ &= C_{L_V}(V_{1,1+g}) \\ &= \langle V_{1,1+g}\rangle_{vec} \quad \text{(Lemma 1.1)},\end{aligned}$$

whence

$$\mathrm{Gr}N \cap C(Z) = \langle Z\rangle_{vec},$$

which is the desired conclusion. □

Lemma 2.2.

$$C(X_i^{(1)} + X_i) \cap \mathrm{Gr}N = \langle X_i, Z\rangle_{Lie} \qquad for \quad 1 \le i \le 2g \tag{13}$$

Proof. We prove this in a similar way to Lemma 2.1 (2), but here we have the extra difficulty that $X_i + X_i^{(1)} \notin \mathrm{Gr}N$. Note that for each $1 \le i \le 2g$,

$$\begin{aligned} ad(X_i^{(1)} + X_i) : \mathrm{Gr}N &\longrightarrow \mathrm{Gr}N, \\ X_j &\longmapsto [X_i, X_j] && (j \ne i \pm g), \\ X_{i+g} &\longmapsto \sum_{\iota=1,\iota\ne i}^{g} [X_{\iota+g}, X_\iota] && (i \le g), \\ X_{i-g} &\longmapsto \sum_{\iota=1,\iota\ne i-g}^{g} [X_\iota, X_{\iota+g}] && (i > g). \end{aligned}$$

We may suppose that $i = 1$ without loss of generality. Since $g \ge 2$, we can apply Proposition 1.3 to $h = 2g$, $A_{2\iota-1} = X_\iota$, $A_{2\iota} = X_{\iota+g}$ $(1 \le \iota \le g)$ and $\mathcal{D} = ad(X_1 + X_1^{(1)})$. Consequentially we can prove this lemma. □

We denote the set $\{X_i, X_{i'}, Z\}$ by $S_{i,i',Z}$.

Lemma 2.3. $\langle S_{i,i',Z}\rangle_{Lie} = L\langle S_{i,i',Z}\rangle \quad (1 \le i \ne i' \le 2g)$.

Proof. As $g \ge 2$, we may assume $i, i' \ne 1$ without loss of generality. Eliminating X_1 as in the proof of Lemma 2.1, it suffices to apply Lemma 1.2 to $S = \{X_1, \dots, X_{2g}\}$, $w = Z$, $T = \{X_i, X_{i'}\}$, $S' = \{X_1^n X_\iota; \iota = 2, \dots, 2g,\ n \ge 0\}$, $\lambda = -1$, $s_0' = X_1 X_{1+g}$, $w' = -\sum_{\iota=2}^{g} X_\iota X_{\iota+g}$. □

Lemma 2.4. *Let i and i' be integers with $1 \le i \le 2g$ and $1 \le i' \le 2g$ such that $i \not\equiv i' \pmod g$. Let m be an integer ≥ 1. Let $W_i \in \langle X_i, Z\rangle_{Lie} \cap \mathrm{gr}^{m+1}N, W_{i'} \in \langle X_{i'}, Z\rangle_{Lie} \cap \mathrm{gr}^{m+1}N$ such that*

$$[W_i, X_{i'}] + [X_i^{(1)}, W_{i'}] = 0. \tag{14}$$

If $m \ne 2$, then $W_i = W_{i'} = 0$. If $m = 2$, then $W_i + W_{i'} \in \langle [Z, X_i - X_{i'}]\rangle_{vec}$.

Proof. At first, we note

$$[W_i, X_{i'}],\ [X_i^{(1)}, W_{i'}] \in \langle S_{i,i',Z}\rangle_{Lie}$$

from (11) and (12). We denote $\{X_i^n X_{i'}, X_i^n Z; n \geq 0\}$ by $S_{X_{i'},Z}$. By Lemma 2.3 and the elimination theorem ([6]), we have

$$\langle S_{i,i',Z}\rangle_{Lie} \simeq \langle X_i\rangle_{Lie} \oplus \langle S_{X_{i'},Z}\rangle_{Lie}$$

and

$$\langle S_{X_{i'},Z}\rangle_{Lie} \simeq L\langle S_{X_{i'},Z}\rangle. \tag{15}$$

As $m \geq 1$, we notice

$$[W_i, X_{i'}],\ [X_i^{(1)}, W_{i'}] \in L\langle S_{X_{i'},Z}\rangle.$$

The case $m = 1$: It is clear that $\langle X_i, Z\rangle_{Lie} \cap \mathrm{gr}^2 N = \langle X_{i'}, Z\rangle_{Lie} \cap \mathrm{gr}^2 N = \langle Z\rangle_{vec}$. Hence there are $\lambda, \mu \in \mathbb{Z}_\ell$ such that $W_i = \lambda Z$ and $W_{i'} = \mu Z$. From (12) and (14), we have

$$[Z, \lambda X_{i'} + \mu X_i] = 0.$$

By lemma 2.1(2), we have

$$\lambda X_{i'} + \mu X_i \in \langle Z\rangle_{vec}.$$

Observing the difference of degrees in $\mathrm{Gr}P_2$, we have $\lambda = \mu = 0$. Thereby we conclude that $W_i = W_{i'} = 0$.

The case $m = 2$: Note that $\langle X_i, Z\rangle_{Lie} \cap \mathrm{gr}^3 N = \langle [Z, X_i]\rangle_{vec}$ and $\langle X_{i'}, Z\rangle_{Lie} \cap \mathrm{gr}^3 N = \langle [Z, X_{i'}]\rangle_{vec}$. Hence there are $\lambda, \mu \in \mathbb{Z}_\ell$ such that $W_i = \lambda[Z, X_i]$ and $W_{i'} = \mu[Z, X_{i'}]$. From (12) and (14), we have

$$(\lambda + \mu)[[Z, X_i], X_{i'}] = 0.$$

From Lemma 2.3, we have $\lambda + \mu = 0$. Hence we have

$$W_i + W_{i'} = \lambda[Z, X_i - X_{i'}],$$

as desired.

The case $m \geq 3$: From (15), we can define a Lie algebra homomorphism u as follows:

$$\begin{aligned} u : \langle S_{X_{i'},Z}\rangle_{Lie} &\longrightarrow \langle S_{i,i',Z}\rangle_{Lie}, \\ X_i^n X_{i'} &\longmapsto X_i^n X_{i'}, \\ X_i^n Z &\longmapsto Z. \end{aligned}$$

By Lemma 2.3, we can define the canonical projection p_d from $\langle S_{i,i',Z}\rangle_{Lie}$ to $\langle$ all monomials of degree d with respect to Z in $L\langle S_{i,i',Z}\rangle\rangle_{vec}$.

Then we can see

$$\begin{aligned} 0 &= p_d \circ u([W_i, X_{i'}] + [X_i^{(1)}, W_{i'}]) \\ &= \begin{cases} \lambda[Z, X_{i'}] - p_1(W_{i'}) & \text{for some } \lambda \in \mathbb{Z}_\ell \text{ if } d{=}1 \\ -dp_d(W_{i'}) & \text{otherwise.} \end{cases} \end{aligned}$$

Moreover as $m \geq 3$, the total degree of $p_1(W_{i'})$ in $\mathrm{Gr}N$ is greater than 4, unless $p_1(W_{i'}) = 0$. Consequently $p_d(W_{i'}) = 0$ for $d \geq 1$, which means $W_{i'} = 0$. Hence $[W_i, X_{i'}] = 0$ by (14). Applying Lemma 1.1 to $L = \mathrm{Gr}N \simeq L\langle X_1, \cdots, X_{2g}\rangle$ and $s = X_{i'}$, we have $W_i \in \langle X_{i'}\rangle_{vec} \cap \mathrm{gr}^{m+1} N = \{0\}$, which completes the proof. $\square$

2.3. **Filtered injectivity.** The purpose of this subsection is to show Theorem 2.5 by using results of §2.2 and to prove Corollary 2.8 and Corollary 2.11, which lead us to the main results Theorem 3.2, Theorem 3.6 of this paper.

Notations. We define some $\mathbb{Z}_\ell$-modules as follows: For $m \geq 1$, set

$$\mathrm{Der}^\flat(\mathrm{Gr}P_n)(m) := \left\{ D \in \mathrm{Der}(\mathrm{Gr}P_n) \;\middle|\; \begin{array}{c} D(\mathrm{gr}^d \mathrm{Gr}P_n) \subset \mathrm{gr}^{d+m}\mathrm{Gr}P_n \ (d \geq 1), \\ D(\mathrm{Gr}N_n^{(j)}) \subset \mathrm{Gr}N_n^{(j)} \ (1 \leq j \leq n), \\ D(Z_k^{(j)}) = [T_k^{(j)}, Z_k^{(j)}] \ for\ some\ T_k^{(j)} \in \mathrm{gr}^m P_n \\ (1 \leq j \leq n, \quad 1 \leq k \leq r+n) \end{array} \right\}.$$

Here $Z_k^{(j)} := z_k^{(j)} \bmod \Pi_{g,r}^{(n)}(3)$ $(1 \leq j \leq n,\ 1 \leq k \leq r+n)$. For $n \geq 1$, set

$$\begin{aligned} &\mathrm{Der}^\flat(\mathrm{Gr}P_n) := \langle \bigcup_{m \geq 1} \mathrm{Der}^\flat(\mathrm{Gr}P_n)(m) \rangle_{vec} \simeq \oplus_{m \geq 1} \mathrm{Der}^\flat(\mathrm{Gr}P_n)(m), \\ &\mathrm{Inn}(\mathrm{Gr}P_n) := \{ adT : \mathrm{Gr}P_n \to \mathrm{Gr}P_n \,|\, T \in \mathrm{Gr}P_n \}, \\ &\mathrm{Out}^\flat(\mathrm{Gr}P_n) := \mathrm{Der}^\flat(\mathrm{Gr}P_n)/\mathrm{Inn}(\mathrm{Gr}P_n). \end{aligned}$$

Note that each of the last three $\mathbb{Z}_\ell$-modules is naturally endowed with structure of graded $\mathbb{Z}_\ell$-Lie algebra. The projection $\mathrm{Gr}\pi_1(f) : \mathrm{Gr}P_{n+1} \to \mathrm{Gr}P_n$, obtained by forgetting the $(n+1)$-th strand, induces a graded $\mathbb{Z}_\ell$-Lie algebra homomorphism

$$\mathrm{Out}^\flat \mathrm{Gr}\pi_1(f) : \mathrm{Out}^\flat(\mathrm{Gr}P_{n+1}) \longrightarrow \mathrm{Out}^\flat(\mathrm{Gr}P_n).$$

Theorem 2.5. *If $2-2g-r<0$, $n \geq 1$, then $\mathrm{Out}^\flat \mathrm{Gr}\pi_1(f)$ is injective.*

Remark 2.6. *This map has already been studied by many predecessors. Y.Ihara proved the injectivity when $g=r=0$ and $n \geq 4$(*[11]*) and surjectivity (S_n-fixed parts) when $g=r=0$ and $n \geq 5$(*[13]*). H.Nakamura, R.Ueno and the author proved the injectivity in the case $2-2g-r<0$ and $r+n \geq 2$ (*[25] *Theorem 4.3). H.Tsunogai proved the surjectivity when $g \geq 1, r=1$ and $n \geq 3$(*[32]*).*

Proof of Theorem 2.5. Before we begin the proof, we would like to explain the main difference between the proof for $r+n \geq 2$ in [25] Theorem 4.3 and the proof for $r+n=1$ given below. To prove the theorem, we need to profile $\mathcal{D} \in \mathrm{Der}^\flat(\mathrm{Gr}P_{n+1})$ which maps to an inner derivation on $\mathrm{Gr}P_n$ by the projection $\mathrm{Gr}\pi_1(f)$. To do this, we may put the extra condition that $\mathcal{D}$ is homogeneous, $\mathcal{D}(\mathrm{Gr}P_{n+1}) \subset \mathrm{Gr}N_{n+1}^{(n+1)}$ and $\mathcal{D}(Z)=0$, where $Z := Z_1^{(n+1)}$. When $r+n \geq 2$, we do so by using $[Z,V]=0$ for any $V \in \{X_1^{(n)}, \cdots, X_{2g}^{(n)}, Z_2^{(n)}, \cdots, Z_{r+n-1}^{(n)}\}$. However, when $r+n=1$ (*i.e.* $r=0$ and $n=1$), we have $[Z,V] \neq 0$ for any $V \in \{X_1^{(1)}, \cdots, X_{2g}^{(1)}\}$. Thus, we resort to the relation $[X_i^{(1)}+X_i^{(2)}, Z]=0$ $(1 \leq i \leq 2g)$ (12) instead. As $X_i^{(1)}+X_i^{(2)}$ does not belong to any 'fiber subalgebra', calculations are difficult. We overcome this difficultly by the elimination theorem on free Lie algebras. (See Subsection 2.2.)

Now we enter into details about the proof in the case $r+n=1$ (*i.e.* $(r,n)=(0,1)$ and therefore $g\geq 2$). We follow the notations of Subsection 2.2. Let $\mathcal{D}\in \mathrm{Der}^\flat(\mathrm{Gr}P_2)$ and assume that $\mathcal{D}$ induces an inner derivation on $\mathrm{Gr}P_1$ by $\mathrm{Gr}\pi_1(f)$. We shall prove that $\mathcal{D}$ is inner. We may assume that $\mathcal{D}\in \mathrm{Der}^\flat(\mathrm{Gr}P_1)(m)$ for some $m\geq 1$. As the map $\mathrm{Inn}(\mathrm{Gr}P_2)\to \mathrm{Inn}(\mathrm{Gr}P_1)$ is surjective, we may assume $\mathcal{D}(\mathrm{Gr}P_2)\subset \mathrm{Gr}N$. Moreover we may assume $\mathcal{D}(Z)=0$ by means of lemma 2.1(1). We denote $\mathcal{D}(X_i^{(j)})$ by $D_{i,j}$ in this proof.

From (11),

$$[D_{i,1},X_{i'}]+[X_i^{(1)},D_{i',2}]=0, \tag{16}$$

for any i,i'. By combining (12) with lemma 2.1(2),

$$D_{i,1}+D_{i,2}\in\langle Z\rangle_{vec}\qquad (1\leq i\leq 2g). \tag{17}$$

The case $m=1$: Observing that the relations (10) and (11) of $\mathrm{Gr}P_2$, we have

$$\begin{aligned}\mathrm{Gr}N^{(1)}\cap \mathrm{Gr}N =&\mathrm{Ker}(\mathrm{Gr}\pi_1(f)|_{\mathrm{Gr}N^{(1)}})\\ =&(Z),\end{aligned}$$

where (Z) is the ideal generated by Z in $\mathrm{Gr}N^{(1)}$, whence

$$\mathrm{gr}^2N^{(1)}\cap \mathrm{gr}^2N=\langle Z\rangle_{vec}.$$

Hence $D_{i,1}\in\langle Z\rangle_{vec}$ $(1\leq i\leq 2g)$ by the assumption on $\mathcal{D}$. From this and (17), $D_{i,2}\in\langle Z\rangle_{vec}$ $(1\leq i\leq 2g)$. Combining these with (12), equation (16) can be regarded as one in $\langle S_{i,i',Z}\rangle_{Lie}$. Since $g\geq 2$, $\langle S_{i,i',Z}\rangle_{Lie}=L\langle S_{i,i',Z}\rangle$ if $i\neq i'$, by Lemma 2.3. Hence $C_{\langle S_{i,i',Z}\rangle_{Lie}}(Z)$ is $\langle Z\rangle_{vec}$ by Lemma 1.1. Considering the difference between the degree of Z and those of X_i and $X_{i'}$ in $\mathrm{Gr}P_2$, we get $D_{i,1}=D_{i',2}=0$ $(1\leq i\neq i'\leq 2g)$, because X_i and $X_{i'}$ are linearly independent. Thereby,

$$D_{i,1}=D_{i,2}=0\quad (1\leq i\leq 2g).$$

Since $\mathrm{Gr}P_2$ is generated by $\{X_i^{(1)},X_i;1\leq i\leq 2g\}$, $\mathcal{D}=0\in\mathrm{Inn}(\mathrm{Gr}P_2)$.

The case $m\geq 2$: Using (17) and observing the degrees, $D_{i,1}+D_{i,2}=0$ for $1\leq i\leq 2g$. Since $[X_i^{(j)},X_i^{(1)}+X_i]=0$ $(1\leq j\leq 2,\ 1\leq i\leq 2g)$ by (11),

$$D_{i,j}\in C(X_i^{(1)}+X_i)\cap \mathrm{Gr}N\qquad (1\leq j\leq 2, 1\leq i\leq 2g).$$

By virtue of Lemma 2.2,

$$D_{i,j}\in\langle X_i,Z\rangle_{Lie}\qquad (1\leq j\leq 2, 1\leq i\leq 2g). \tag{18}$$

By (16) and (18), we may apply Lemma 2.4 to $W_i=D_{i,1}$, $W_{i'}=D_{i',2}$ and conclude that for each i,i' such that $i\not\equiv i'\pmod g$,

$$D_{i,1}+D_{i',2}\in\langle[X_{i'}-X_i,Z]\rangle_{vec}\quad \text{when } m=2, \tag{19}$$

$$D_{i,1}=D_{i',2}=0\quad \text{when } m\geq 3. \tag{20}$$

When $m=2$, by (18) and (12), it can be checked that

$$D_{i,j}\in\langle[X_i^{(j)},Z]\rangle_{vec}, \tag{21}$$

for $j=1,2$. Hence there exists $\lambda_{i,j}\in\mathbb{Z}_\ell$ such that $D_{i,j}=\lambda_{i,j}[X_i^{(j)},Z]$. From (19), (12) and Lemma 2.1(2), we have

$$\lambda_{i',2}X_{i'}-\lambda_{i,1}X_i-\mu(X_{i'}-X_i)\in\langle Z\rangle_{vec},$$

for some $\mu \in \mathbb{Z}_\ell$. By the difference between the degree of X_i and that of Z, we get

$$\lambda_{i',2} = \lambda_{i,1} (= \mu),$$

if $i \not\equiv i' \pmod{g}$.

Now, when $g \geq 3$, we conclude that $\lambda_{i,j} = \lambda_{1,1}$ $(1 \leq i \leq 2g,\, 1 \leq j \leq 2)$ and

$$\mathcal{D} = ad(\lambda_{1,1} Z)$$

directly. When $g = 2$, we have

$$\lambda_{1,1} = \lambda_{2,2} = \lambda_{3,1} = \lambda_{4,2},$$
$$\lambda_{1,2} = \lambda_{2,1} = \lambda_{3,2} = \lambda_{4,1}.$$

Since $\mathcal{D}(Z) = 0$, we have

$$\begin{aligned} 0 &= \mathcal{D}([X_1, X_3] + [X_2, X_4]) \\ &= [\lambda_{1,2}[X_1, X_3] + \lambda_{2,2}[X_2, X_4], Z]. \end{aligned}$$

By Lemma 2.1(2), we have

$$(\lambda_{1,2} - \mu')[X_1, X_3] + (\lambda_{2,2} - \mu')[X_2, X_4] = 0,$$

for some $\mu' \in \mathbb{Z}_\ell$. As $\mathrm{Gr}N \simeq L\langle X_1, X_2, X_3, X_4 \rangle$, we obtain

$$\lambda_{1,2} = \lambda_{2,2} (= \mu'),$$

which completes the proof of the case $m = 2$.

When $m \geq 3$,

$$D_{i,1} = D_{i,2} = 0 \quad (1 \leq i \leq 2g)$$

from (20) together with $g \geq 2$, which means $D = 0$.

Thus, we have completed the proof. □

Now we apply the above filtered injectivity for Lie algebras to show that for pro-ℓ groups.

Notations. For $n \geq 1$,

$$\widetilde{\Gamma}_n := \left\{ f \in \mathrm{Aut}P_n \;\middle|\; \begin{array}{c} f(N_n^{(j)}) \subset N_n^{(j)}\, (1 \leq j \leq n), \\ f(z_k^{(j)}) \overset{conj.}{\sim} z_k^{(j)\alpha} \text{ for some } \alpha \in \mathbb{Z}_\ell^\times \\ (1 \leq j \leq n, \quad 1 \leq k \leq r+n) \end{array} \right\},$$

$$\Gamma_n := \tilde{\Gamma}_n / \mathrm{Inn}P_n.$$

For $n \geq 1$ and $m \geq 1$,

$$\tilde{\Gamma}_n(m) := \left\{ \sigma \in \tilde{\Gamma}_n \;\middle|\; \begin{array}{c} \sigma(x)x^{-1} \in P_n(1+m)\, (x \in P_n), \\ \sigma(x')x'^{-1} \in P_n(2+m)\, (x' \in P_n(2)) \end{array} \right\},$$

$$\Gamma_n(m) := (\tilde{\Gamma}_n(m)\mathrm{Inn}P_n)/\mathrm{Inn}P_n,$$

$$\mathrm{gr}^m\tilde{\Gamma}_n := \tilde{\Gamma}_n(m)/\tilde{\Gamma}_n(m+1),$$

$$\mathrm{gr}^m\Gamma_n := \Gamma_n(m)/\Gamma_n(m+1).$$

Moreover

$$\mathrm{Gr}\Gamma_n := \oplus_{m \geq 1} \mathrm{gr}^m \Gamma_n$$

has a natural graded $\mathbb{Z}_\ell$-Lie algebra structure, for $\{\Gamma_n(m)\}_{m \geq 1}$ is central in $\Gamma_n(1)$ ([25], cf. also [4] Theorem 2, [18] Proposition 6(1)). Note that Γ_n is denoted by $\Gamma_{g,r}^{(n)}$ in [25].

Corollary 2.7. *For $n \geq 1$, the $\mathbb{Z}_\ell$-Lie algebra homomorphism*

$$\mathrm{Gr}\Gamma_{n+1} \longrightarrow \mathrm{Gr}\Gamma_n, \tag{22}$$

induced by the projection $P_{n+1} \to P_n$ is injective.

Proof. (cf. [25] (2.13); also [18] Lemma 5) We have injective $\mathbb{Z}_\ell$-Lie algebra homomorphisms

$$\bar{\delta} : \mathrm{Gr}\Gamma_n \hookrightarrow \mathrm{Out}^\flat(\mathrm{Gr}P_n), \tag{23}$$

for $n \geq 1$ (cf. [25] (2.13.2)), compatible with the projection. Thus the assertion follows from Theorem 2.5. □

Corollary 2.8. *The continuous group homomorphism*

$$\Gamma_{n+1}/\Gamma_{n+1}(m) \longrightarrow \Gamma_n/\Gamma_n(m) \tag{24}$$

induced by the projection $P_{n+1} \to P_n$ is injective for each $m \geq 1$.

Proof. (cf. [25] (2.9) $\sim$ (2.11)) By using the relations of $\mathrm{Gr}P_{n+1}$ ([25] (2.8.2)), we see that Γ_{n+1} acts diagonally on

$$\mathrm{gr}^1 P_{n+1} \simeq (\mathrm{gr}^1 P_1)^{\oplus(n+1)}.$$

Thus we have

$$\Gamma_{n+1}/\Gamma_{n+1}(1) \hookrightarrow \Gamma_n/\Gamma_n(1). \tag{25}$$

Now we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \to & \mathrm{gr}^m\Gamma_{n+1} & \to & \Gamma_{n+1}/\Gamma_{n+1}(m+1) & \to & \Gamma_{n+1}/\Gamma_{n+1}(m) & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \mathrm{gr}^m\Gamma_n & \to & \Gamma_n/\Gamma_n(m+1) & \to & \Gamma_n/\Gamma_n(m) & \to & 1 \end{array}$$

for each $m \geq 1$, in which both rows are exact. Now, considering (22) and (25), we get the conclusion by induction on m. □

We also have the injectivity result (Corollary 2.11) for the whole pro-ℓ mapping class groups. We shall begin with:

Lemma 2.9. *Let G be finitely generated pro-ℓ group and $\{G(m)\}_{m\geq 1}$ a central filtration such that $\cap_{m\geq 1} G(m) = \{1\}$. Let $\tilde{\Gamma}$ be a subgroup of $\mathrm{Aut}G$ such that $\tilde{\Gamma}G(m) \subset G(m)$ and $\tilde{\Gamma} \supset \mathrm{Inn}G$. Denote $\tilde{\Gamma}/\mathrm{Inn}G$ ($\subset \mathrm{Out}G$) by Γ. Denote $\mathrm{Ker}(\tilde{\Gamma} \to \mathrm{Aut}G/G(m+1))$ by $\tilde{\Gamma}[m]$ and $\tilde{\Gamma}[m]/(\mathrm{Inn}G \cap \tilde{\Gamma}[m])$ by $\Gamma[m]$ for $m = 1, 2, \cdots$. If $Z(\mathrm{Gr}G) = \{0\}$, then we have*

$$\bigcap_{m\geq 1} \Gamma[m] = \{1\}.$$

Here $\mathrm{Gr}G$ is the graded $\mathbb{Z}_\ell$-Lie algebra induced by the central filtration $\{G(m)\}_{m\geq 1}$.

Proof. This lemma is a generalization of [2] Theorem 2, which treats the case where $\{G(m)\}_{m\geq 1}$ is the lower central filtration. The proof of the lemma is done in the same way as that of [2] Theorem 2 except for obvious modifications. □

Lemma 2.10.

$$\bigcap_{m\geq 1} \Gamma_n(m) = \{1\},$$

for $n \geq 1$.

Proof. As mentioned after (8), $Z(\mathrm{Gr}P_n) = \{0\}$. Hence applying the above lemma 2.9 to $G = P_n$, $G(m) = P_n(m)$ and $\tilde{\Gamma} = \tilde{\Gamma}_n$ for $m = 1, 2, \cdots$, we have $\cap_{m\geq 1}\Gamma_n[m] = \{1\}$. As $\Gamma_n(m) \subset \Gamma_n[m]$, the lemma follows. □

Corollary 2.11. *The continuous group homomorphism*

$$\Gamma_{n+1} \longrightarrow \Gamma_n$$

induced by the projection $P_{n+1} \to P_n$ is injective.

Proof. Combining Corollary 2.8 and Lemma 2.10 (for $n+1$), we complete the proof. □

Remark 2.12. *We can consider a discrete situation by substituting the topological mapping class group Γ_n^{top} for the pro-ℓ mapping class group Γ_n. In exactly the same way as the pro-ℓ situation, $\Pi_{g,r}^{(n)top}$ has a central filtration called the weight filtration and it induces a filtration $\{\Gamma_n^{top}(m)\}_{m\geq 1}$ on Γ_n^{top}(cf. [5] (2.1.1) and (2.1.6)). The results of this section also hold in the discrete case except possibly for Corollary 2.11. For the present, the validity of the analogue of Corollary 2.11 in the discrete case is unclear, since we do not know whether*

$$\cap_{m\geq 1}\Gamma_n^{top}(m) = \{1\}$$

or not in general. (It is known that it is true when $n = 1$ and $(g, r) \neq (2, 0)$ cf. [3] Proposition 2).

3. Galois representations and universal monodromy representations

The purpose of this section is to show the main independency theorems of this paper. The one (Theorem 3.2) extends and completes previous results by Y.Ihara and M.Kaneko ([11] The Galois Kernel Theorem, [15] Theorem 2) and the other (Theorem 3.6) almost verifies Oda's prediction on pro-ℓ universal monodromy representations ([28]).

In this section we continue to employ the notation in the previous section.

Let k be a subfield of $\mathbb{C}$ and C a (g, r)-curve over k (*i.e.* smooth separated geometrically irreducible curve over k such that its smooth compactification C^* has geometric genus g and the number of $\bar{k}$-rational points on $C^* \setminus C$ is r). As we have seen in (4), to each $n \geq 1$, we can attach the following continuous group homomorphism

$$\rho_{F_n(C)/k}^{(\text{pro-}\ell)} : G_k \to \mathrm{Out}P_n.$$

For simplicity we denote $\rho_{F_n(C)/k}^{(\text{pro-}\ell)}$ by φ_n in the rest of this paper. We denote by $k_C^{(n)(\text{pro-}\ell)}$ the fixed subfield of $\bar{k}$ by $\mathrm{Ker}\varphi_n$. Let k' be the compositum of the residue fields of the points of $C^* \setminus C$, which is a finite Galois extension of k. Then we can see that the image of $G_{k'}$ under φ_n is contained in the pro-ℓ mapping class group Γ_n as follows: for $\sigma \in G_{k'}$ and $1 \leq j \leq n$, $\varphi_n(\sigma)$ preserves $N_n^{(j)}$ by the functoriality of π_1 and the definition of φ_n. By means of the branch cycle argument, $\varphi_n(\sigma)$ maps the inertia generator $z_{j'}^{(j)}$ to a conjugate of $z_{j'}^{(j)\chi_\ell(\sigma)}$ $(1 \leq j' \leq r+n)$ where $\chi_\ell : G_{k'} \to \mathbb{Z}_\ell^\times$ is the ℓ-adic cyclotomic character. Hence $\varphi_n(G_{k'}) \subset \Gamma_n$.

Then we obtain the following field tower $\{k_C^{(n)(\text{pro-}\ell)}(m)\}_{m\geq 1}$:

$$k_C^{(n)(\text{pro-}\ell)}(m) := \bar{k}^{\varphi_n^{-1}(\Gamma_n(m))}.$$

Another kind of field tower $\{\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)}(m)\}_{m\geq 1}$ (defined by Ihara, Oda, Nakamura, cf. §0) is obtained by considering the universal family of curves instead of a single curve. Let $2-2g-r<0$ and $\mathcal{M}_{g,r}$ be the moduli stack over $\mathbb{Q}$ of smooth geometrically connected curves of genus g with disjoint ordered r sections. In [29], Takayuki Oda developed a theory of fundamental groups of algebraic stacks and showed that there are two exact sequences

$$1\to\pi_1(\mathcal{M}_{g,r}\otimes_{\mathbb{Q}}\overline{\mathbb{Q}})\to\pi_1(\mathcal{M}_{g,r})\overset{p_{g,r}}{\to}G_{\mathbb{Q}}\to 1, \tag{26}$$

and for each $n\geq 1$,

$$1\to\pi_1(F_n(\mathcal{C}_{\overline{y}}))\to\pi_1(\mathcal{M}_{g,r+n})\to\pi_1(\mathcal{M}_{g,r})\to 1. \tag{27}$$

Here $(\mathcal{C}^*\to\mathcal{M}_{g,r},s_1,\cdots,s_r)$ is the universal family of proper smooth geometrically connected curves of genus g with r disjoint sections $\{s_1,\cdots,s_r:\mathcal{M}_{g,r}\to\mathcal{C}^*\},\mathcal{C}=\mathcal{C}^*\setminus\amalg_{1\leq k\leq r}s_k(\mathcal{M}_{g,r}),\overline{y}\to\mathcal{M}_{g,r}$ is a geometric point and $\mathcal{C}_{\overline{y}}$ is the geometric fiber at $\overline{y}$.
As in the case of a single curve, (27) induces a continuous homomorphism

$$\Phi_{g,r}^{(n)(\text{pro-}\ell)}:\pi_1(\mathcal{M}_{g,r})\to\text{Out}P_n,$$

called the pro-ℓ universal monodromy representation, and $\text{Im}\Phi_{g,r}^{(n)(\text{pro-}\ell)}$ is also contained in the pro-ℓ mapping class group Γ_n. Then the filtration $\{\Gamma_n(m)\}_{m\geq 1}$ induces the following tower of fields:

$$\mathbb{Q}\subset\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)}(1)\subset\cdots\subset\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)}(m)\subset\cdots\subset\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)}\subset\bar{\mathbb{Q}},$$

where

$$\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)}(m):=\bar{\mathbb{Q}}^{p_{g,r}((\Phi_{g,r}^{(n)(\text{pro-}\ell)})^{-1}(\Gamma_n(m)))}\quad(m\geq 1),$$

and

$$\mathbb{Q}_{g,r}^{(n)(\text{pro-}\ell)}:=\bar{\mathbb{Q}}^{p_{g,r}(\text{Ker}\Phi_{g,r}^{(n)(\text{pro-}\ell)})}.$$

Just as in §0, in what follows we shall often omit the superscript (1) expressing one dimension.

Roughly speaking, $\mathbb{Q}_{g,r}^{(\text{pro-}\ell)}$ is the maximal subfield of $k_C^{(\text{pro-}\ell)}$ which does not depend on the moduli of the (g,r)-curve C.

Remark 3.1. *(1)By Lemma 2.10 and the higher dimensional version of* [25] *(6.6), we can prove*

$$k_C^{(n)(pro\text{-}\ell)}=\bigcup_{m\geq 1}k_C^{(n)(pro\text{-}\ell)}(m),$$

and

$$\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}=\bigcup_{m\geq 1}\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}(m).$$

(2)By extending [25] *(6.4) to higher dimensional cases, we can prove*

$$\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}(m)\subset k_C^{(n)(pro\text{-}\ell)}(m)\qquad(m\geq 1).$$

(3)By definition, we have

$$\mathbb{Q}^{(n)(pro\text{-}\ell)}_{\mathbb{P}^1\setminus\{0,1,\infty\}}(m) = \mathbb{Q}^{(n)(pro\text{-}\ell)}_{0,3}(m) \qquad (m \geq 1).$$

(4)(cf. [25] *(6.4)) We have*

$$\mathbb{Q}^{(pro\text{-}\ell)}_{g,r}(m) \subset \bigcap_{\substack{C/k:\ (g,r)\text{-}curve,\\ [k:\mathbb{Q}]<\infty}} k_C^{(pro\text{-}\ell)}(m) \quad (m \geq 1), \tag{28}$$

and

$$\mathbb{Q}^{(pro\text{-}\ell)}_{g,r} \subset \bigcap_{\substack{C/k:\ (g,r)\text{-}curve,\\ [k:\mathbb{Q}]<\infty}} k_C^{(pro\text{-}\ell)}. \tag{29}$$

The author does not know whether the equality holds in (28), (29) or not.

Theorem 3.2. *Suppose that C is hyperbolic. Then, for $n = 1, 2, \cdots$, we have*

(1) $k_C^{(n)(pro\text{-}\ell)}(m) = k_C^{(n+1)(pro\text{-}\ell)}(m) \quad (m \geq 1).$

In particular,

(2) $k_C^{(n)(pro\text{-}\ell)} = k_C^{(n+1)(pro\text{-}\ell)}.$

When $r + n \geq 2$, (2) has been proved in [15] Theorem 2 (under the assumption $3 - 2g - r - n < 0$, weaker than the hyperbolicity assumption $2 - 2g - r < 0$).

Proof. The following commutative diagram exists

$$\begin{array}{ccccc} & & \Gamma_{n+1} & \to & \Gamma_{n+1}/\Gamma_{n+1}(m) \\ & \nearrow & & & \\ G_{k'} & & \downarrow & & \downarrow \qquad\qquad (m \geq 1) \\ & \searrow & & & \\ & & \Gamma_n & \to & \Gamma_n/\Gamma_n(m), \end{array}$$

where vertical maps are induced by the projection $P_{n+1} \to P_n$. The commutativity of the diagram is due to the functoriality of π_1 and the definitions of pro-ℓ mapping class groups and their weight filtrations. By virtue of Corollary 2.8 and Corollary 2.11, vertical maps are both injective. The conclusion follows from this and $\varphi_n^{-1}(\Gamma_n) = G_{k'}$. □

Remark 3.3. *According to* [15]*, we have assumed that k is a subfield of $\mathbb{C}$. However the same statement is still true when k is any field of characteristic 0. Indeed, choosing a suitable model and using various standard arguments, we reduce the proof for the general case to the case where k is a subfield of $\mathbb{C}$.*

Theorem 3.4. *Suppose that $2 - 2g - r < 0$. Then, for $n = 1, 2, \cdots$, we have*

(1) $\mathbb{Q}^{(n)(pro\text{-}\ell)}_{g,r}(m) = \mathbb{Q}^{(n+1)(pro\text{-}\ell)}_{g,r}(m) \quad (m \geq 1).$

In particular,

(2) $\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)} = \mathbb{Q}_{g,r}^{(n+1)(pro\text{-}\ell)}$.

When $r + n \geq 2$, the theorem has been proved in [25] Corollary (4.4).

Proof. Similarly as in the proof of Theorem 3.2, the following commutative diagram exists:

$$\begin{array}{ccccc} & & \Gamma_{n+1} & \to & \Gamma_{n+1}/\Gamma_{n+1}(m) \\ & \nearrow & & & \\ \pi_1(\mathcal{M}_{g,r}) & & \downarrow & & \downarrow \qquad\qquad (m \geq 1) \\ & \searrow & & & \\ & & \Gamma_n & \to & \Gamma_n/\Gamma_n(m). \end{array}$$

Now Corollary 2.8 and Corollary 2.11 complete the proof. □

Theorem 3.5. *Suppose that $g \geq 2$ and $n \geq 1$. Then, for $r \geq 0$, we have*

(1) $\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}(m) = \mathbb{Q}_{g,r+1}^{(n)(pro\text{-}\ell)}(m) \quad (m \geq 1)$.

In particular,

(2) $\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)} = \mathbb{Q}_{g,r+1}^{(n)(pro\text{-}\ell)}$.

When $r + n \geq 2$, the theorem has been proved in [25] Theorem B(1).

Proof. This is a direct consequence of Theorem 3.4 and [25] Theorems B(1). □

Theorem 3.6 (Oda Prediction)**.** *If $2 - 2g - r < 0$ and $n \geq 1$, then*

(1) $\{\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}(m)\}_{m\geq 1}$ *is independent of (r, n) and almost independent of (g, r, n) in the following sense:*

$$\mathbb{Q}_{1,1}^{(pro\text{-}\ell)}(m) \supset \mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}(m) \supset \mathbb{Q}_{0,3}^{(pro\text{-}\ell)}(m),$$
$$[\mathbb{Q}_{1,1}^{(pro\text{-}\ell)}(m) : \mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}(m)],\ [\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}(m) : \mathbb{Q}_{0,3}^{(pro\text{-}\ell)}(m)] < \infty.$$

(2) $\mathbb{Q}_{g,r}^{(n)(pro\text{-}\ell)}$ *is independent of (g, r, n).*

Proof. The conclusion follows immediately from Theorem 3.4 and Theorem 3.5 together with known results ([25] Theorem B, [22] Theorem A and [16] Theorem 3B). □

4. Images of Galois groups and mapping class groups

In this section we present applications of Theorem 3.6, which generalize [22] Section 4 to the case of proper curves. Let ℓ be a prime number and C a hyperbolic (g, r)-curve over a number field k. For a $\mathbb{Z}_\ell$-module M, we denote $M \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ by $M_{\mathbb{Q}_\ell}$.

Notations. For each $m \geq 1$, set

$$\mathrm{gr}_{g,r}^{[\ell]\,m} G_{\mathbb{Q}} := \mathrm{Gal}(\mathbb{Q}_{g,r}^{(\mathrm{pro}\text{-}\ell)}(m+1)/\mathbb{Q}_{g,r}^{(\mathrm{pro}\text{-}\ell)}(m)),$$
$$\mathrm{gr}_{C}^{[\ell]\,m} G_{k} := \mathrm{Gal}(k_{C}^{(\mathrm{pro}\text{-}\ell)}(m+1)/k_{C}^{(\mathrm{pro}\text{-}\ell)}(m)).$$

Corollary 4.1. $dim_{\mathbb{Q}_\ell}(\mathrm{gr}_C^{[\ell]\,m}G_k)_{\mathbb{Q}_\ell} \geq dim_{\mathbb{Q}_\ell}(\mathrm{gr}_{0,3}^{[\ell]\,m}G_{\mathbb{Q}})_{\mathbb{Q}_\ell} \quad (m \geq 1)$.

Proof.

Lemma 4.2.

$$(\mathrm{gr}_{g,r}^{[\ell]\,m}G_{\mathbb{Q}})_{\mathbb{Q}_\ell} \cong (\mathrm{gr}_{0,3}^{[\ell]\,m}G_{\mathbb{Q}})_{\mathbb{Q}_\ell} \quad (m \geq 1).$$

Proof. Immediate from Theorem 3.6. □

As $\mathbb{Q}_{g,r}^{(\text{pro-}\ell)}(m) \subset k_C^{(\text{pro-}\ell)}(m)$ (Remark 3.1(2)), there exists a natural $\mathbb{Q}_\ell$-linear map

$$\phi_C^{[\ell]\,(m)} : (\mathrm{gr}_C^{[\ell]\,m}G_k)_{\mathbb{Q}_\ell} \to (\mathrm{gr}_{g,r}^{[\ell]\,m}G_{\mathbb{Q}})_{\mathbb{Q}_\ell} \quad (m \geq 1).$$

Lemma 4.3. *The map $\phi_C^{[\ell]\,(m)}$ is surjective for each $m \geq 1$.*

Proof. The proof of this lemma for hyperbolic (g,r)-curves with $r > 0$ is in [22] (4.5). It works just as it is for $r = 0$. □

Corollary 4.1 is a direct consequence of the above two lemmas. □

Remark 4.4. *For the value of $r_m = dim_{\mathbb{Q}_\ell}(\mathrm{gr}_{0,3}^{[\ell]\,m}G_{\mathbb{Q}})_{\mathbb{Q}_\ell}$ the following are known:*

$$r_m \begin{cases} \geq 1 & \text{if } m \text{ is even and } m \neq 2,4,8,12, \text{ ([10], [12], [19], [9])} \\ = 0 & \text{otherwise,} \end{cases}$$

$$r_{2m} \to \infty \quad as \quad m \to \infty \text{ ([19])}.$$

Moreover it is conjectured by P. Deligne and Y. Ihara (resp. proved by R. Hain and M. Matsumoto [9]*) that the graded $\mathbb{Q}_\ell$-Lie algebra $\oplus_{m\geq 1}(\mathrm{gr}_{0,3}^{[\ell]\,m}G_{\mathbb{Q}})_{\mathbb{Q}_\ell}$ is generated freely (resp. generated) by certain elements $\sigma_{4m+2} \in (\mathrm{gr}_{0,3}^{[\ell]\,4m+2}G_{\mathbb{Q}})_{\mathbb{Q}_\ell}\,(m \geq 1)$, called 'Soulé elements'. This conjecture gives a (conjectural) formula for the exact value of r_m ([14] (4.2)):*

$$r_m = \frac{1}{m}\sum_{d|m}\mu\left(\frac{m}{d}\right)\left(\sum_{i=1}^{3}(\alpha_i^d - 1 - (-1)^d)\right),$$

where α_i $(1 \leq i \leq 3)$ are the roots of $x^3 - x - 1$. For the value of r_m for $m \leq 20$, see [22] *(4.3).*

Finally we shall give an application of Lemma 4.2 to pure topology. Here we follow the notation of Remark 2.12. We have a natural homomorphism

$$\tau_m \otimes_{\mathbb{Z}} \mathbb{Q}_\ell : (\mathrm{gr}^m\Gamma_1^{top}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \to (\mathrm{gr}^m\Gamma_1)_{\mathbb{Q}_\ell},$$

where

$$\mathrm{gr}^m\Gamma_1^{top} := \Gamma_1^{top}(m)/\Gamma_1^{top}(m+1).$$

This homomorphism essentially coincides with the Johnson-Morita homomorphism τ_m tensored with $\mathbb{Q}_\ell$ (cf. [5], [22]). By [3] Theorem B, we know that $\mathrm{Ker}(\tau_m \otimes_{\mathbb{Z}} \mathbb{Q}_\ell)$ is trivial.

Corollary 4.5. *For $m \geq 1$,*

$$dim_{\mathbb{Q}_\ell}\mathrm{Coker}(\tau_m \otimes_{\mathbb{Z}} \mathbb{Q}_\ell) \geq r_m,$$

where $r_m = dim_{\mathbb{Q}_\ell}(\mathrm{gr}_{0,3}^{[\ell]\,m}G_{\mathbb{Q}})_{\mathbb{Q}_\ell}$. In particular, if $m \neq 2,4,8,12$ and m is even, then $\tau_m \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ is not surjective.

Proof. The affine case has been proved in [22] (4.8). The proper case can be proved in the same way by using Lemma 4.2 and Remark 4.4. □

Acknowledgments

The author proved the main results of this paper at the beginning of 1995 (see [23] (A4), [16] the comment after Corollary 4.2.2). After that he had been out of health for many years, which is the reason for the big delay of the completion of this paper.

He is very grateful to Professor Yasutaka Ihara for having introduced some suitable problems around the Galois representations on fundamental groups of curves and for warm encouragements during the period of his long struggle against disease. The author would like to express his sincere gratitude to Professor Akio Tamagawa for helpful communications, warm encouragements, useful comments, constructive suggestions and valuable advices over public and private matters. He is deeply indebted to Professor Makoto Matsumoto for the idea of the proof of Lemma 2.2 and for considerate and instructive guidances. To Professor Hiroaki Nakamura he heavily owes his understanding/knowledge of profinite groups (especially including Asada's work [2]) and of Grothendieck's anabelian philosophy. He thanks Professor Mamoru Asada for sending a copy of [2] used in the final step to Corollary 2.11, for informing him of [3] which tells him some results on the filtrations of discrete and pro-ℓ mapping class groups and for sympathy toward him. He thanks Professor Makoto Nagata for friendship with him. Certainly without any of them this paper would not have existed.

He would like to express his sincerest gratitude to all of them and last but not least to the referee for her/his various useful suggestions.

References

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

[2] M.Asada, *Two properties of the filtration of the outer automorphism groups of certain groups, Math.Z.* **218** (1995), pp.122–133.

[3] M.Asada, *On the filtration of topological and pro-l mapping class groups of punctured Riemann surfaces, J. Math. Soc. Japan* **48** (1996), no.1, pp.13–36.

[4] M.Asada and M.Kaneko, *On the automorphism groups of some pro-ℓ fundamental groups, Advanced Studies in Pure Math.* **12** (1987), pp.137–159.

[5] M.Asada and H.Nakamura, *On graded quotient modules of mapping class groups of surfaces, Israel J. Math.* **90** (1995), pp.93–113.

[6] N.Bourbaki, *Lie groups and Lie algebras*, Chapter 2, (English translation) Hermann, Paris (1976).

[7] F.R.Cohen and S.Prassidis, *On injective homomorphisms for pure braid groups and associated Lie algebras*, *J. Algebra* **298** (2006), pp.363–370.

[8] A.Grothendieck and M.Raynaud, *Revêtement Étale et Groupe Fondamental (SGA1)*, *Lecture Notes in Math.* **224**, Springer (1971).

[9] R.Hain and M.Matsumoto, *Weighted completion of Galois groups and Galois actions on the fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$*, *Compositio Math.* **139** (2003), pp.119–167.

[10] Y.Ihara, *The Galois representation arising from $\mathbf{P}^1 - \{0, 1, \infty\}$ and Tate twists of even degree, Galois Groups over $\mathbb{Q}$, Math. Sci. Res. Inst. Pub.* **16**, *Y.Ihara, K.Ribet, J.-P.Serre (eds.)*, Springer (1989), pp.299–313.

[11] Y.Ihara, *Automorphisms of pure sphere braid groups and Galois representations*, *The Grothendieck Festschrift, Volume II*, *Progress in Mathematics* **87**, Birkhäuser (1991), pp.353–373.

[12] Y.Ihara, *Braids,Galois groups, and some arithmetic functions*, *Proceedings of the ICM90(I)*, Math. Soc. Japan, Tokyo (1991), pp.99–120.
[13] Y.Ihara, *On the stable derivation algebra associated to some braid groups*, *Isral J. of Math.* **80**, (1992), pp.135–153.
[14] Y.Ihara, *Some arithmetic aspects on Galois actions on the pro-p fundamental group of* $\mathbf{P}^1 - \{0, 1, \infty\}$*, Arithmetic Fundamental Groups, PSPUM* **70**, M.Fried and Y.Ihara (eds.), AMS (2002), pp.247–273.
[15] Y.Ihara and M.Kaneko, *Pro-ℓ pure braid groups of Riemann surfaces and Galois representations*, *Osaka J. Math.* **29** (1992), pp.1–19.
[16] Y.Ihara and H.Nakamura, *On deformation of maximally degenerate stable marked curves and Oda's problem*, *J. reine angew Math.* **487** (1997), pp.125–151.
[17] D.Johnson, *An abelian quotient of the mapping class group* $\mathcal{I}_g$, *Math. Ann.* **249** (1980), pp.225–242.
[18] M.Kaneko, *Certain automorphism groups of pro-l fundamental groups of punctured Riemann surfaces*, *J. Fac. Sci. Univ. Tokyo* **36** (1989), pp.363–372.
[19] M.Matsumoto, *On the galois image in the derivation algebra of* π_1 *of the projective line minus three points*, *Recent Developments in Inverse Galois Problem*, *Contemp. Math.* **186** (1996), pp.201–213.
[20] M.Matsumoto, *Galois representations on profinite braid groups on curves*, *J. reine angew Math.* **474** (1996), pp.169–219.
[21] S.Morita, *Abelian quotients of subgroups of the mapping class group of surfaces*, *Duke. Math. J.* **70** (1993), pp.699–726.
[22] H.Nakamura, *Coupling of universal monodromy representations of Galois-Teichmüller modular groups*, *Math. Ann.* **304** (1996), pp. 99–119.
[23] H.Nakamura, *Galois rigidity of profinite fundamental groups*, *Sugaku Expositions* **10(2)** (1997), pp. 195–215.
[24] H.Nakamura and N.Takao, *Galois rigidity of pro-ℓ pure braid groups of algebraic curves*, *Trans. Amer. Math. Soc.* **350** (1998), pp.1079–1102.
[25] H.Nakamura, N.Takao and R.Ueno, *Some stability properties of Teichmüller modular function fields with pro-l weight structures*, *Math. Ann.* **302** (1995), pp.197–213.
[26] H.Nakamura and H.Tsunogai, *Some finiteness theorems on Galois centralizers in pro-l mapping class groups*, *J. reine angew Math.* **441** (1993), pp.115–144.
[27] T.Oda, *A lower bound for the graded modules associated with the relative weight filtration on Teichmüller group*, *preprint*, (1992).
[28] T.Oda, *The universal monodromy representations on the pro-nilpotent fundamental groups of algebraic curves*, *Mathematische Arbeitstagung (Neue Serie)* **9-15 Juin 1993**, Max-Planck-Institute preprint MPI/93-57 (1993).
[29] T.Oda, *Etale homotopy type of the moduli spaces of algebraic curves*, *Geometric Galois Actions 1*, London Mathematical Society Lecture Note Series **242**, Cambridge Univ. Press (1997), pp.85–95.
[30] G.P.Scott, *Braid groups and the group of homeomorphisms of a surface*, *Proc. Camb. Phil. Soc.* **68** (1970), pp. 605–617.
[31] A.I.Shirshov, *Subalgebras of free Lie algebras(Russian)*, *Mat. Sbornik N. S.* **33** (1953), pp. 441–452.
[32] H.Tsunogai, *The stable derivation algebras for higher genera*, *Israel J. Math.* **136** (2003), pp.221–250.

Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan

E-mail address: takao@kurims.kyoto-u.ac.jp