RIMS Kôkyûroku Bessatsu
B51 (2014), 55–70

Some remarks on field towers arising from pronilpotent universal monodromy representations

By

Naotake TAKAO*

Abstract

This article concerns Oda's problem on pronilpotent monodromy representations associated to universal families of curves (called pronilpotent universal monodromy representations for short). In the first half part, we review several known results and their recent applications, and in the second half part, we present some new results obtained by the author.

§ 1. Introduction

There are two purposes of this article. One is to introduce some problems on field towers (Ihara towers (Definition 1.7)) arising from pronilpotent universal monodromy representations and associated graded Lie algebras (Deligne-Ihara algebras (Definition 1.8)), especially Oda's problem (Problem 1.10). The other is to report some recent results on Oda's problem obtained by the author.

Let ℓ be a prime. The quotient of the image of the outer representation of the absolute Galois group of $\mathbb{Q}$ in the pro-ℓ geometric fundamental group of a hyperbolic algebraic curve by the subgroup which comes from the mapping class group is determined by the type of the curve (namely, the genus g and the number of cusps r), and does not depend on the moduli of the curve, from the connectedness of the moduli stack. This quotient has a natural central filtration induced by the weight filtration of the fundamental group of the curve. On each graded piece (which is a finitely generated $\mathbb{Z}_\ell$-module) of the graded $\mathbb{Z}_\ell$-Lie algebra associated to this filtration, $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q})$ acts by conjugation.

Hypothetically, this graded Lie algebra tensored with $\mathbb{Q}_\ell$ (with Galois action) might be related with the ℓ-adic étale realization of a mixed Tate motif over $\mathbb{Z}$. In conjunction

Received July 31, 2013. Revised September 6, 2013, September 11, 2013 and April 16, 2014.
2010 Mathematics Subject Classification(s): 14H30
*RIMS, Kyoto University, Kyoto 606-8502, Japan.
e-mail: takao@kurims.kyoto-u.ac.jp

with this hypothesis, Oda conjectured that the graded pieces in odd degrees (over $\mathbb{Z}_\ell$) should all vanish (cf. [O1] Conjecture A). Subsequently some related problems were submitted in the middle of the 90's.

1. (Nonfiltered Oda's problem) Is this quotient of the image of the outer representation independent of the type of the curve? This problem was solved affirmatively by Yasutaka Ihara, Makoto Matsumoto, Hiroaki Nakamura, Ryoichi Ueno and the author when the curve is affine (i.e. $r > 0$), and finally it was generally solved by the author. Another proof was given by Yuichiro Hoshi and Shinichi Mochizuki later.

2. (Filtered Oda's problem) Is the above graded $\mathbb{Z}_\ell$-Lie algebra tensored with $\mathbb{Q}_\ell$ independent of the type of the curve ? This problem was also solved affirmatively by Yasutaka Ihara, Makoto Matsumoto, Hiroaki Nakamura, Ryoichi Ueno and the author.

However, the conjecture by Oda mentioned above has not been solved yet. The author thinks that Ihara towers and Deligne-Ihara algebras might contain arithmetically interesting phenomenon (cf. Theorem 1.11). So the author studies a certain problem (Problem 1.10) posed in [NTU] that generalizes the conjecture and problems mentioned above. This generalized problem is called **(generalized) Oda's problem** in this article.

The organization of this article is as follows: In §1.1 the formulation of Oda's problem is introduced. In §1.2 known results on Oda's problem are stated. In §1.3 their applications are given. More concretely, in §1.3.1 an obstruction to the surjectivity of the Johnson homomorphism in low-dimensional topology is discussed. In §1.3.2 a certain result of Grothendieck conjecture type by Hoshi, which can be viewed as a genus zero analogue of Mochizuki's Tate conjecture type theorem for non-CM elliptic curves, is stated. In §1.3.3 a certain result related to anabelian property of the moduli space of curves by Iijima is given. In §2 some recent progress obtained by the author is reported. More specifically, we prove that the m-th graded piece of the Deligne-Ihara algebra vanishes if $m \leq 3$ or $g = 1$, $m = 5$ (Proposition 2.3), is independent of the type of the curve if $\ell \gg m$ (Corollary 2.6), and vanishes if $g = 1$, $m \equiv 1 \pmod 2$ and $\ell > 2$ (Proposition 2.4 (1)).

§ 1.1. Formulations

Let ℓ be a prime. We begin with the definition of pro-ℓ universal monodromy representations. Let g, $r \in \mathbb{Z}_{\geq 0}$ such that $2g - 2 + r > 0$. By $\mathcal{M}_{g,r}$, we denote the moduli stack over $\mathbb{Q}$ of (g,r)-curves, that is, proper smooth geometrically connected curves of genus g with ordered disjoint r sections. We sometimes refer to the pair (g,r) as the type of the curve. Then we have a short exact sequence ([O2])

$$1 \to \pi_1(\mathcal{M}_{g,r} \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}) \to \pi_1(\mathcal{M}_{g,r}) \overset{p_{g,r}}{\to} \mathrm{G}_{\mathbb{Q}} \to 1.$$

Here $\pi_1(S)$ stands for the étale fundamental group of a scheme/an algebraic stack S. And, for a field K, $\bar{K}$ is an algebraic closure of K and G_K is the absolute Galois group of K.

Let $x : \mathrm{Spec}(\kappa) \to \mathcal{M}_{g,r}$ be a point, where κ is a field of characteristic 0. Then we have a short exact sequence

$$1 \to \pi_1(\bar{X}) \to \pi_1(\mathcal{M}_{g,r+1}) \to \pi_1(\mathcal{M}_{g,r}) \to 1,$$

where $\kappa(x) := \kappa$, $X := \mathcal{M}_{g,r+1} \times_{\mathcal{M}_{g,r}} \mathrm{Spec}(\kappa(x))$ and $\bar{X} := X \times_{\mathrm{Spec}(\kappa(x))} \mathrm{Spec}(\overline{\kappa(x)})$.

This short exact sequence induces a continuous group homomorphism

$$\Phi_x^{(\ell)} : \pi_1(\mathcal{M}_{g,r}) \to \mathrm{Out}(\pi_1^{\ell}(\bar{X})),$$

as follows:

$$\begin{array}{ccccccccc}
1 \to & \pi_1(\bar{X}) & \to & \pi_1(\mathcal{M}_{g,r+1}) & \to & \pi_1(\mathcal{M}_{g,r}) & \to 1 \\
 & \downarrow & \circlearrowleft & \downarrow & \circlearrowleft & \downarrow & \\
1 \to & \mathrm{Inn}(\pi_1(\bar{X})) & \to & \mathrm{Aut}(\pi_1(\bar{X})) & \to & \mathrm{Out}(\pi_1(\bar{X})) & \to 1 \\
 & \downarrow & \circlearrowleft & \downarrow & \circlearrowleft & \downarrow & \\
1 \to & \mathrm{Inn}(\pi_1^{\ell}(\bar{X})) & \to & \mathrm{Aut}(\pi_1^{\ell}(\bar{X})) & \to & \mathrm{Out}(\pi_1^{\ell}(\bar{X})) & \to 1,
\end{array}$$

where all rows are exact. Here $\pi_1^{\ell}(S)$ denotes the maximal pro-ℓ quotient of $\pi_1(S)$ for a scheme/an algebraic stack S.

Definition 1.1 (Pro-ℓ universal monodromy representation). The continuous homomorphism $\Phi_x^{(\ell)}$, regarded as an outer representation of $\pi_1(\mathcal{M}_{g,r})$, is called the pro-ℓ universal monodromy representation associated to $x : \mathrm{Spec}(\kappa) \to \mathcal{M}_{g,r}$.

Remark 1.2 (The kernel and image of universal monodromy represetations). $\mathrm{Ker}(\Phi_x^{(\ell)}) \subset \pi_1(\mathcal{M}_{g,r})$, hence also $\mathrm{Im}(\Phi_x^{(\ell)}) \simeq \pi_1(\mathcal{M}_{g,r})/\mathrm{Ker}(\Phi_x^{(\ell)})$, are independent of the choice of x, and depend only on (g, r) and ℓ.

Remark 1.3 (Galois representations and universal monodromy represetations). For $x : \mathrm{Spec}(\kappa) \to \mathcal{M}_{g,r}$, the pro-$\ell$ outer Galois representation $\varphi_X^{(\ell)} = \varphi_x^{(\ell)} : G_{\kappa(x)} \to \mathrm{Out}(\pi_1^{\ell}(\bar{X}))$ factors through $\Phi_x^{(\ell)}$. Especially, $\varphi_x^{(\ell)} = \Phi_x^{(\ell)}$ when $(g, r) = (0, 3)$ and $\kappa(x) = \mathbb{Q}$.

Next we define truncated outer representations, Ihara towers of type (g,r), and Deligne-Ihara algebras of type (g,r). We denote $\pi_1^{\ell}(\bar{X})$ by $\Pi = \Pi_{g,r}$ when the type of X/κ is (g,r). (Note that $\pi_1^{\ell}(\bar{X})$ is determined up to isomorphism by the type of X/κ and ℓ.)

Definition 1.4 (Weight filtration). The weight filtration $\{\Pi(m)\}_{m\geq 1}$ of Π is defined as follows:

$$\begin{aligned} \Pi(1) &= \Pi, \\ \Pi(2) &= [\Pi, \Pi]\cdot\langle \text{all inertia subgroups}\rangle, \\ \Pi(m) &= \langle [\Pi(m'), \Pi(m'')] | m' + m'' = m\rangle \quad (m \geq 3). \end{aligned}$$

Remark 1.5. This filtration is central. When $r = 0, 1$, the weight filtration coincides with the lower central filtration. When $g = 0$, $\{\Pi(2m-1)\}_{m\geq 1} = \{\Pi(2m)\}_{m\geq 1}$ coincides with the lower central filtration.

Definition 1.6 (Truncated outer representaion).
For each $m \geq 1$, the continuous homomorphism

$$\Phi_x^{(\ell)}(m) : \pi_1(\mathcal{M}_{g,r}) \to \mathrm{Out}^c(\Pi)/\mathrm{Out}^c(\Pi)(m)$$

induced by $\Phi_x^{(\ell)}$ is called the m-th truncated representation, where

$$\begin{aligned} &\mathrm{Out}^c(\Pi) = \mathrm{Aut}^c(\Pi)/\mathrm{Inn}(\Pi), \\ &\mathrm{Aut}^c(\Pi) = \{f \in \mathrm{Aut}(\Pi) | f \text{ preserves the conjugacy class of each inertia subgroup}\}, \\ &\mathrm{Out}^c(\Pi)(m) = \mathrm{Aut}^c(\Pi)(m)\mathrm{Inn}(\Pi)/\mathrm{Inn}(\Pi), \\ &\mathrm{Aut}^c(\Pi)(m) = \left\{ f \in \mathrm{Aut}^c(\Pi) \,\middle|\, \begin{array}{ll} f(w) \equiv w & \pmod{\Pi(1+m)} \text{ for any } w \in \Pi, \\ f(v) \equiv v & \pmod{\Pi(2+m)} \text{ for any } v \in \Pi(2) \end{array} \right\}. \end{aligned}$$

The kernel and the image of $\Phi_x^{(\ell)}(m)$ are determined by (g, r), ℓ and m (and independent of the choice of x). We write $\Phi_x^{(\ell)}(\infty)$ for $\Phi_x^{(\ell)}$ and $\mathrm{G}_{g,r}(m) = \mathrm{G}_{g,r}^{(\ell)}(m)$ for $p_{g,r}(\mathrm{Ker}(\Phi_x^{(\ell)}(m)))$ $(1 \leq m \leq \infty)$. $\{\mathrm{G}_{g,r}(m)\}_{m\geq 1}$ is a central filtration of $\mathrm{G}_{g,r}(1)$ and $\bigcap_{m=1}^{\infty} \mathrm{G}_{g,r}(m) = \mathrm{G}_{g,r}(\infty)$.

Definition 1.7 (Ihara tower of type (g,r)). We set

$$\begin{aligned} \mathbb{Q}_{g,r}^{(\ell)} = \mathbb{Q}_{g,r}^{(\ell)}(\infty) &:= \bar{\mathbb{Q}}^{\mathrm{G}_{g,r}(\infty)}, \\ \mathbb{Q}_{g,r}^{(\ell)}(m) &:= \bar{\mathbb{Q}}^{\mathrm{G}_{g,r}(m)} \quad (m \geq 1). \end{aligned}$$

Thus we obtain a field tower $\mathbb{Q} \subset \mathbb{Q}_{g,r}^{(\ell)}(1) \subset \cdots \subset \mathbb{Q}_{g,r}^{(\ell)}(m) \subset \cdots \subset \mathbb{Q}_{g,r}^{(\ell)} \subset \bar{\mathbb{Q}}$, which is an infinite sequence of infinite extensions, called the **Ihara tower of type (g,r)** in this article.

Definition 1.8 (Deligne-Ihara algebra of type (g,r)). We set

$$\mathrm{gr}_{g,r}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} := \mathrm{Gal}(\mathbb{Q}_{g,r}^{(\ell)}(m+1)/\mathbb{Q}_{g,r}^{(\ell)}(m)),$$

which is a $\mathbb{Z}_\ell$-module on which $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q})$ acts by conjugation, and set

$$\mathrm{Gr}^{(\ell)}_{g,r}\mathrm{G}_\mathbb{Q} := \oplus_{m\geq 1}\mathrm{gr}^{(\ell)m}_{g,r}\mathrm{G}_\mathbb{Q},$$

which is a graded $\mathbb{Z}_\ell$-Lie algebra, called the **Deligne-Ihara algebra of type (g,r)** in this article.

We are interested in the following (a little vague)

Problem 1.9. *What structures/information do the Ihara tower and the Deligne-Ihara algebra have?*

Especially, we are interested in

Problem 1.10 ((generalized) Oda's problem)**.** ***Are the Ihara tower and the Deligne-Ihara algebra (over $\mathbb{Z}_\ell$) independent of the type (g,r)?***

§ 1.2. Known results

In this subsection known results on the problems mentioned above are collected.

Theorem 1.11 (Known results on Probem 1.9)**.**

(1) (e.g. [NTU]) $\mathbb{Q}^{(\ell)}_{g,r}(1) = \mathbb{Q}(\mu_{\ell^\infty})$.

(2) ([AI]) $\mathbb{Q}^{(\ell)}_{0,3} = \mathbb{Q}(\mathrm{E}^{(\ell)}(\{0,1,\infty\}))$. *Here* $\mathrm{E}^{(\ell)}(\{0,1,\infty\})$ *is the group of all higher circular ℓ-units.*

(3) (e.g. [I1]) $\mathbb{Q}^{(\ell)}_{0,3}$ *is a pro-ℓ extension of* $\mathbb{Q}(\mu_{\ell^\infty})$ *unramified outside ℓ.*

(4) ([S], [B]) *If ℓ is an odd regular prime, then* $\mathbb{Q}^{(\ell)}_{0,3}$ *is the maximal pro-ℓ extension of* $\mathbb{Q}(\mu_{\ell^\infty})$ *unramified outside ℓ.*

(5) (e.g. [NT], [I1], [N1]) $\mathrm{gr}^{(\ell)m}_{g,r}\mathrm{G}_\mathbb{Q}$ *is a finitely generated $\mathbb{Z}_\ell$-module. And* $\mathrm{gr}^{(\ell)0}_{g,r}\mathrm{G}_\mathbb{Q}(= \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}))$ *acts on* $\mathrm{gr}^{(\ell)2m}_{g,r}\mathrm{G}_\mathbb{Q}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$ *by conjugation via multiplication by χ^m, where* $\chi : \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) \to \mathbb{Z}_\ell^\times$ *is the ℓ-cyclotomic character.*

(6) (e.g. [I1]) $\mathrm{gr}^{(\ell)m}_{0,3}\mathrm{G}_\mathbb{Q} = \{0\}$ *when* $m \equiv 1 \pmod 2$ *or* $m \in \{2,4,8,12\}$, *and* $\mathrm{gr}^{(\ell)2m}_{0,3}\mathrm{G}_\mathbb{Q}$ *is a free $\mathbb{Z}_\ell$-module of finite rank, whose rank is denoted by r_m. (Thus,* $\mathrm{gr}^{(\ell)2m}_{0,3}\mathrm{G}_\mathbb{Q} \simeq \mathbb{Z}_\ell(m)^{\oplus r_m}$ *as* $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q})$*-modules.)*

(7) ([O1]) *For m odd,* $\mathrm{gr}^{(\ell)m}_{g,r}\mathrm{G}_\mathbb{Q}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell = \{0\}$. *If $\ell > 2$,* $\mathrm{gr}^{(\ell)1}_{g,r}\mathrm{G}_\mathbb{Q} = \mathrm{gr}^{(\ell)2}_{g,r}\mathrm{G}_\mathbb{Q} = \{0\}$. *If* $\ell \gg 0$, $\mathrm{gr}^{(\ell)3}_{g,r}\mathrm{G}_\mathbb{Q} = \{0\}$.

(8) ([HM], [B]) $\mathrm{Gr}^{(\ell)}_{0,3}\mathrm{G}_\mathbb{Q}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$ *is a free graded $\mathbb{Q}_\ell$-Lie algebra generated by a suitable set* $\{\sigma_m \in \mathrm{gr}^{(\ell)2m}_{0,3}\mathrm{G}_\mathbb{Q} | m \geq 3,\ \mathit{odd}\}$, *where σ_m is often called the m-th Soulé element.*

(9) ([HM], [B], [S]) *If ℓ is an odd regular prime, then* $\mathrm{Gr}_{0,3}^{(\ell)}\mathrm{G}_{\mathbb{Q}}$ *is generated by* $\{\sigma_m \in \mathrm{gr}_{0,3}^{(\ell)2m}\mathrm{G}_{\mathbb{Q}} | m \geq 3,\ odd\}$ *in (8).*

(10) ([HM], [B], [S]) *If ℓ is an irregular prime such that the generalized Greenberg conjecture for $\mathbb{Q}(\mu_\ell)$ holds, then* $\mathrm{Gr}_{0,3}^{(\ell)}\mathrm{G}_{\mathbb{Q}}$ *is not generated by* $\{\sigma_m \in \mathrm{gr}_{0,3}^{(\ell)2m}\mathrm{G}_{\mathbb{Q}} | m \geq 3,\ odd\}$ *in (8).*

Theorem 1.12 (Known results on Problem 1.10)**.**

(1) ([NTU],[N1],[M],[IN],[T],[HoMo]) $\mathbb{Q}_{g,r}^{(\ell)}$ *is independent of g and r.*

(2) ([NTU],[N1],[M],[IN],[T]) $\{\mathbb{Q}_{g,r}^{(\ell)}(m)\}_{m\geq 1}$ *is independent of r, and almost independent of g in the following sense :*

$$\mathbb{Q}_{1,1}^{(\ell)}(m) \supset \mathbb{Q}_{g,0}^{(\ell)}(m) \supset \mathbb{Q}_{0,3}^{(\ell)}(m)\ (g \geq 2),$$
$$[\mathbb{Q}_{1,1}^{(\ell)}(m) : \mathbb{Q}_{0,3}^{(\ell)}(m)] < \infty.$$

In particular, $\mathrm{Gr}_{g,r}^{(\ell)}\mathrm{G}_{\mathbb{Q}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \simeq \mathrm{Gr}_{0,3}^{(\ell)}\mathrm{G}_{\mathbb{Q}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

§ 1.3. Applications

In this subsection, we give some applications of Theorem 1.12.

1.3.1. The cokernel of Johnson homomorphism

At first, we introduce an application to low-dimensional topology. Denoting the mapping class group of a topological surface of type (g,r) by $\Gamma_{g,r}^{(top)}$ and the profinite completion of $\Gamma_{g,r}^{(top)}$ by $\widehat{\Gamma_{g,r}^{(top)}}$, the diagram

$$\begin{array}{ccccc}
 & & 1 & & \\
 & & \downarrow & & \\
\widehat{\Gamma_{g,r}^{(top)}} & \simeq & \pi_1(\mathcal{M}_{g,r} \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}) & & \\
 & & \downarrow & & \\
 & \Phi_x^{(\ell)} : & \pi_1(\mathcal{M}_{g,r}) & \to & \mathrm{Out}(\Pi) \\
 & & \downarrow & & \\
 & & \mathrm{G}_{\mathbb{Q}} & & \\
 & & \downarrow & & \\
 & & 1, & &
\end{array}$$

induces a $\mathbb{Q}_\ell$-linear map

$$\tau(g,r)_m : \mathrm{gr}^m\Gamma_{g,r}^{(top)} \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \to (\mathrm{Out}^c\mathrm{Gr}\Pi)_m \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

which is identified with the Johnson homomorphism tensored with $\mathbb{Q}_\ell$ ([J],[N1]). Here $\mathrm{Gr}\Pi$ is the graded $\mathbb{Z}_\ell$-Lie algebra associated to the weight filtration $\{\Pi(m)\}_{m\geq 1}$ (which is central), and $(\mathrm{Out}^c\mathrm{Gr}\Pi)_m$ is the m-th graded piece of the graded $\mathbb{Z}_\ell$-Lie algebra $\mathrm{Out}^c\mathrm{Gr}\Pi$ consisting of all derivations of $\mathrm{Gr}\Pi$ which preserve all inertia (Lie) ideals, divided by the inner derivation algebra $\mathrm{InnGr}\Pi$ of $\mathrm{Gr}\Pi$ (cf. more strict definition in the proof of Proposition 2.3). Theorem 1.12 implies

Corollary 1.13 ([N1] Theorem C, [T] Theorem 0.7). *If $2g-2+r>0$, then*

$$\mathrm{Coker}(\tau(g,r)_m) \hookleftarrow \mathrm{gr}^m_{0,3}\mathrm{G}_{\mathbb{Q}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

In particular,

$$\dim_{\mathbb{Q}_\ell} \mathrm{Coker}(\tau(g,r)_m) \geq \mathrm{rank}_{\mathbb{Z}_\ell}\mathrm{gr}^m_{0,3}\mathrm{G}_{\mathbb{Q}}.$$

Here, $r_m = \mathrm{rank}_{\mathbb{Z}_\ell}\mathrm{gr}^{2m}_{0,3}\mathrm{G}_{\mathbb{Q}}$ (cf. Theorem 1.11(6)) is given by

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

where α_i $(1 \leq i \leq 3)$ are the roots of $x^3 - x - 1$ (Theorem 1.11(8), [I2]).

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
r_m	0	0	1	0	1	0	1	1	1	1	2	2	3	3	4	5	7	8	11	13

$r_m = \mathrm{rank}_{\mathbb{Z}_\ell}\mathrm{gr}^{2m}_{0,3}\mathrm{G}_{\mathbb{Q}}$ $(1 \leq m \leq 20)$

We have $r_m > 0$ for $m \neq 1,2,4,6$ and $r_m \doteqdot 1.3^m$ when m is large enough. Thus, in particular, $\tau(g,r)_{2m}$ is not surjective for $m \neq 1,2,4,6$.

1.3.2. Galois-theoretic characterization of isomorphism classes of monodromically full hyperbolic curves of genus zero

Any one-pointed elliptic curve without complex multiplication over a number field can be restored group-theoretically from the kernels of all the associated Galois representations. More precisely,

Theorem 1.14 ([Mo] Theorem 1.1). *Let k be a number field, and E_i elliptic curves over k which admit no complex multiplication over $\bar{\mathbb{Q}}$ $(i=1,2)$. Then the following conditions are equivalent:*

(i) *E_1 is isomorphic to E_2 over k;*

(ii) *$k(E_1[N]) = k(E_2[N])$ for all natural numbers N.*

Here $k(E_i[N])$ is the minimal finite extension field of k over which all N-torsion points of E_i are defined ($i = 1, 2$).

In the proof of the following theorem, which can be viewed as a genus zero analogue of Theorem 1.14, Theorem 1.12 is used to recover the type of a given curve group-theoretically from the kernel of the associated pro-ℓ outer Galois representation.

Theorem 1.15 ([Ho] Theorem A). *Let ℓ be a prime number, k a field finitely generated over $\mathbb{Q}$, and X_i hyperbolic curves of type $(0, r_i)$ over k which are ℓ-monodromically full ($i = 1, 2$) and satisfy certain additional conditions. Then the following conditions are equivalent:*

(i) *X_1 is isomorphic to X_2 over k;*

(ii) $\mathrm{Ker}(\varphi^{(\ell)}_{X_1}) = \mathrm{Ker}(\varphi^{(\ell)}_{X_2})$.

1.3.3. The type (i.e. (g,r))-independency of the kernel of the Galois action on the relative pro-ℓ completion of a mapping class group

Theorem 1.12 brings us

Theorem 1.16 ([Ii] Theorem 3.4). *Let ℓ be a prime number and k a field of characteristic* 0. *Suppose that $3g - 3 + r > 0$ and either $(g, r) \neq (1, 1)$ or $\ell = 2$. Then*

$$\mathrm{Ker}(\mathrm{G}_k \to \mathrm{Out}(\Phi^{(\ell)}_x(\pi_1(\mathcal{M}_{g,r} \otimes_{\mathbb{Q}} \bar{\mathbb{Q}})))) = \mathrm{Ker}(\varphi^{(\ell)}_{\mathbb{P}^1_k \setminus \{0,1,\infty\}}),$$

for any point $x : \mathrm{Spec}(\kappa) \to \mathcal{M}_{g,r}$.

As a corollary, the title of this subsection is partially concluded:

Corollary 1.17 ([Ii] Corollary 3.8). *Under the same condition as in Theorem 1.16, we have*

$$\mathrm{Ker}(\mathrm{G}_k \to \mathrm{Out}(\Gamma^{rel-\ell}_{g,r})) \subset \mathrm{Ker}(\varphi^{(\ell)}_{\mathbb{P}^1_k \setminus \{0,1,\infty\}}),$$

where $\Gamma^{rel-\ell}_{g,r}$ is the relative pro-ℓ completion of $\Gamma^{(top)}_{g,r}$.

Remark 1.18. Very recently Iijima announced that he succeeded in dropping the assumption that either $(g, r) \neq (1, 1)$ or $\ell = 2$ in Theorem 1.16 and Corollary 1.17.

§ 2. Recent progress on Oda's problem

Based on the results of the foregoing section, we turn to the study of the Ihara tower and the Deligne-Ihara algebra (over $\mathbb{Z}_\ell$). Oda conjectured that $\mathrm{gr}^{(\ell)2m-1}_{g,r}\mathrm{G}_{\mathbb{Q}} =$

$\{0\}$ ([O1] Conjecture A). So one of our goal is to prove that $\mathrm{gr}_{g,r}^{(\ell)2m-1}\mathrm{G}_{\mathbb{Q}}$ is independent of the type (g,r) and to investigate the possible dependency on (g,r) of $\mathrm{gr}_{g,r}^{(\ell)2m}\mathrm{G}_{\mathbb{Q}}$.

Note that there exist maps $\mathrm{gr}_{1,1}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} \to \mathrm{gr}_{g,r}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} \to \mathrm{gr}_{0,3}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$ as $\mathbb{Z}_\ell$-modules and they are isomorphic after tensored with $\mathbb{Q}_\ell$ (Theorem 1.12 (2)).

Proposition 2.1. *Let ℓ be a prime. Let g and r be non-negative integers such that $2g-2+r>0$. For each $1 \le m_0 \le \infty$, consider the following conditions:*

(a) $\mathbb{Q}_{1,1}^{(\ell)}(m) = \mathbb{Q}_{g,r}^{(\ell)}(m) = \mathbb{Q}_{0,3}^{(\ell)}(m)$ $(1 \le m \le m_0+1)$,

(b) $\mathrm{gr}_{1,1}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} \xrightarrow{\sim} \mathrm{gr}_{g,r}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} \xrightarrow{\sim} \mathrm{gr}_{0,3}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$ $(1 \le m \le m_0)$,

(c) $\mathbb{Q}_{1,1}^{(\ell)}(m) = \mathbb{Q}_{0,3}^{(\ell)}(m)$ $(1 \le m \le m_0+1)$,

(d) $\mathrm{gr}_{1,1}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} \xrightarrow{\sim} \mathrm{gr}_{0,3}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$ $(1 \le m \le m_0)$,

(e) $\mathrm{gr}_{1,1}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} \hookrightarrow \mathrm{gr}_{0,3}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$ $(1 \le m \le m_0)$,

(f) $\mathrm{gr}_{1,1}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$ *is torsion-free* $(1 \le m \le m_0)$,

(g) $\mathrm{gr}_{1,1}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} \twoheadrightarrow \mathrm{gr}_{0,3}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$ $(1 \le m \le m_0+1)$.

Then we have (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c) $\Leftrightarrow$ (d) $\Leftrightarrow$ (e) $\Leftrightarrow$ (f) $\Rightarrow$ (g). *If, moreover, $m_0 = \infty$, then* (a)–(g) *are all equivalent.*

Proof. (a) $\Rightarrow$ (b) is trivial. (b) $\Rightarrow$ (a) follows (by induction on m) from the fact that $\mathbb{Q}_{1,1}^{(\ell)}(1) = \mathbb{Q}_{g,r}^{(\ell)}(1) = \mathbb{Q}_{0,3}^{(\ell)}(1)$ (cf. Theorem 1.11(1)). (c) $\Leftrightarrow$ (d) is proved similarly. (a) $\Leftrightarrow$ (c) follows from the fact that $\mathbb{Q}_{1,1}^{(\ell)}(m) \supset \mathbb{Q}_{g,r}^{(\ell)}(m) \supset \mathbb{Q}_{0,3}^{(\ell)}(m)$ (Theorem 1.12(2)). (d) $\Rightarrow$ (e) is trivial. (e) $\Rightarrow$ (f) follows from the fact that $\mathrm{gr}_{0.3}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$ is torsion-free (Theorem 1.11(6)). (f) $\Rightarrow$ (c) is proved by using that $\mathrm{Gr}_{g,r}^{(\ell)}\mathrm{G}_{\mathbb{Q}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \simeq \mathrm{Gr}_{0,3}^{(\ell)}\mathrm{G}_{\mathbb{Q}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ (Theorem 1.12 (2)), $\mathbb{Q}_{1,1}^{(\ell)}(1) = \mathbb{Q}_{0,3}^{(\ell)}(1)$ and the induction on m. More precisely, suppose that $\mathbb{Q}_{1,1}^{(\ell)}(m) = \mathbb{Q}_{0,3}^{(\ell)}(m)$. Then it is clear that $\mathrm{gr}_{1,1}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} \twoheadrightarrow \mathrm{gr}_{0,3}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$. Moreover the $\mathbb{Z}_\ell$-modules $\mathrm{gr}_{1,1}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$ and $\mathrm{gr}_{0,3}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$ have the same rank (Theorem 1.12 (2)) and are torsion-free from (f). Hence $\mathrm{gr}_{g,r}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} \simeq \mathrm{gr}_{0,3}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$. Hence $\mathbb{Q}_{1,1}^{(\ell)}(m+1) = \mathbb{Q}_{0,3}^{(\ell)}(m+1)$. This induction step, together with $\mathbb{Q}_{1,1}^{(\ell)}(1) = \mathbb{Q}_{0,3}^{(\ell)}(1)$ (Theorem 1.11(1)), leads us to (c). (c) $\Rightarrow$ (g) is trivial. Finally, we shall prove (g) $\Rightarrow$ (c) when $m_0 = \infty$. We first show the following

Claim 2.2. *For $i = 0, 1$, let H_i be a profinite group with a central filtration $H_i = H_i(0) \supset H_i(1) \supset \cdots \supset H_i(m) \supset \cdots$ such that* (1) *$H_1(m) \subset H_0(m)$ for any $0 \le m < \infty$,* (2) *$H_1(\infty) = H_0(\infty)$, where $H_i(\infty) = \cap_{m \ge 0} H_i(m)$ $(i = 0, 1)$, and* (3) *$\mathrm{gr}^m H_1 \twoheadrightarrow \mathrm{gr}^m H_0$ for any $0 \le m < \infty$. Then we have $H_1(m) = H_0(m)$ for any $0 \le m \le \infty$.*

Proof. The proof has three steps. First, for $0 \le m \le n < \infty$, we prove the assertion $P_m(n)$ that $H_1(m)/H_1(n) \twoheadrightarrow H_0(m)/H_0(n)$ by induction on n. More precisely $P_m(m)$ is trivial. Suppose we have $P_m(n)$. Then in the following commutative diagram

$$\begin{array}{ccccccccc} 0 \to & \mathrm{gr}^n H_1 & \to & H_1(m)/H_1(n+1) & \to & H_1(m)/H_1(n) & \to 1 & \text{(exact)} \\ & \downarrow & \circlearrowleft & \downarrow & \circlearrowleft & \downarrow & & \\ 0 \to & \mathrm{gr}^n H_0 & \to & H_0(m)/H_0(n+1) & \to & H_0(m)/H_0(n) & \to 1 & \text{(exact),} \end{array}$$

the left vertical arrow is surjective from assumption (3) and the right vertical arrow is also surjective from the induction hypothesis. Hence the central vertical arrow is also surjective, which means $P_m(n+1)$. Thus, for $m \le n$, $H_1(m)/H_1(n) \twoheadrightarrow H_0(m)/H_0(n)$. Second, we can see $H_1(m)/H_1(\infty) \twoheadrightarrow H_0(m)/H_0(\infty)$ by taking the inverse limit of $H_1(m)/H_1(n) \twoheadrightarrow H_0(m)/H_0(n)$ with respect to n. Third, in the following commutative diagram

$$\begin{array}{ccccccccc} 1 \to & H_1(\infty) & \to & H_1(m) & \to & H_1(m)/H_1(\infty) & \to 1 & \text{(exact)} \\ & \downarrow & \circlearrowleft & \downarrow & \circlearrowleft & \downarrow & & \\ 1 \to & H_0(\infty) & \to & H_0(m) & \to & H_0(m)/H_0(\infty) & \to 1 & \text{(exact),} \end{array}$$

the left vertical arrow is surjective from assumption (2) and the right vertical arrow is also surjective from the conclusion of the second step. Hence we have $H_1(m) \twoheadrightarrow H_0(m)$. In addition, we have $H_1(m) \subset H_0(m)$ (assumption (1)). Therefore we have $H_1(m) = H_0(m)$, which is the conclusion of the claim. □

Applying this claim to $H_1(m) = G_{1,1}(m)$ and $H_0(m) = G_{0,3}(m)$, we conclude (g) $\Rightarrow$ (c) when $m_0 = \infty$. More precisely, we have $G_{1,1}(m) \subset G_{0,3}(m)$ $(1 \le m < \infty)$ (Theorem 1.12 (2)), $G_{1,1}(\infty) = G_{0,3}(\infty)$ (Theorem 1.12 (1)) and $\mathrm{gr}_{1,1}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} \twoheadrightarrow \mathrm{gr}_{0,3}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$ $(1 \le m < \infty)$ (condition (g)). □

As $\mathrm{gr}_{0,3}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} = \{0\}$ when $m \equiv 1 \pmod 2$ or $m \in \{2,4,8,12\}$ (Theorem 1.11(6)), if Oda's problem (Problem 1.10) is solved affirmatively, then $\mathrm{gr}_{g,r}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} = \{0\}$ when $m \equiv 1$ (mod 2) or $m \in \{2, 4, 8.12\}$. In fact, Oda proved $\mathrm{gr}_{g,r}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \{0\}$ for $m \equiv 1$ (mod 2), $\mathrm{gr}_{g,r}^{(\ell)1}\mathrm{G}_{\mathbb{Q}} = \mathrm{gr}_{g,r}^{(\ell)2}\mathrm{G}_{\mathbb{Q}} = \{0\}$ when $\ell > 2$, and $\mathrm{gr}_{g,r}^{(\ell)3}\mathrm{G}_{\mathbb{Q}} = \{0\}$ when $\ell \gg 0$ (Theorem 1.11(7)).

Next propositions generalize Oda's result (Theorem 1.11(7)).

Proposition 2.3.

(1) *For* $1 \le m \le 3$ *or* $m = 5$, $\mathrm{gr}_{1,1}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} = \{0\}$.

(2) *For* $1 \le m \le 3$, $\mathrm{gr}_{g,r}^{(\ell)m}\mathrm{G}_{\mathbb{Q}} = \{0\}$.

Proof. (1) For $x : \mathrm{Spec}(\mathbb{Q}) \to \mathcal{M}_{1,1}$, we have $\mathrm{Ker}(\Phi_x^{(\ell)}(m))/\mathrm{Ker}(\Phi_x^{(\ell)}(m+1)) \twoheadrightarrow \mathrm{gr}_{1,1}^{(\ell)m}\mathrm{G}_{\mathbb{Q}}$ and $\mathrm{Ker}(\Phi_x^{(\ell)}(m))/\mathrm{Ker}(\Phi_x^{(\ell)}(m+1)) \hookrightarrow (\mathrm{Out}^c\mathrm{Gr}\Pi)_m$ from the definitions of the filtrations (Definitions 1.6-1.8,§1.3.1 and [NT] (5.6)). (Here $\Pi = \Pi_{1,1} = \pi_1(\bar{X}) = \langle \alpha, \beta, z | [\alpha, \beta]z = 1\rangle$ and $\bar{X} := \mathcal{M}_{1,2} \times_{\mathcal{M}_{1,1}} \mathrm{Spec}(\bar{\mathbb{Q}})$.) Moreover we have the following commutative diagram in which all rows and columns are exact and all homomorphisms are compatible with the actions of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ ([NT] (1.10.2), (1.13) and Theorem 1.14):

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \mathrm{gr}^m\Pi & \to & \mathrm{gr}^m\Pi & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & (\mathrm{Der}^c\mathrm{Gr}\Pi)_m & \overset{i_m}{\to} & \widetilde{C_m} & \overset{j_m}{\to} & \mathrm{gr}^{m+2}\Pi(-1) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & (\mathrm{Out}^c\mathrm{Gr}\Pi)_m & \to & C_m & \to & \mathrm{gr}^{m+2}\Pi(-1) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Here, (-1) denotes the twist by $\det^{-1}$, where $\det : \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathbb{Z}_\ell^\times$ is the determinant map. Writing A for $\alpha \mod \Pi(2)$ ($\in \mathrm{gr}^1\Pi$), B for $\beta \mod \Pi(2)$ ($\in \mathrm{gr}^1\Pi$), Z for $z \mod \Pi(3)$ ($\in \mathrm{gr}^2\Pi$),

$$\begin{aligned}
\mathrm{Der}^c\mathrm{Gr}\Pi &= \{D \in \mathrm{Der}(\mathrm{Gr}\Pi) | D \text{ induces an inner derivation on the inertia ideal } (Z)\}, \\
&= \{D \in \mathrm{Der}(\mathrm{Gr}\Pi) | D(Z) = [T, Z] \text{ for some } T \in \mathrm{Gr}\Pi\},
\end{aligned}$$

which is a $\mathbb{Z}_\ell$-graded Lie algebra, and $(\mathrm{Der}^c\mathrm{Gr}\Pi)_m$ is the m-th graded piece of $\mathrm{Der}^c\mathrm{Gr}\Pi$, namely

$$(\mathrm{Der}^c\mathrm{Gr}\Pi)_m = \{D \in \mathrm{Der}^c(\mathrm{Gr}\Pi) | D(\mathrm{gr}^d\Pi) \subset \mathrm{gr}^{d+m}\Pi \text{ for any } d \geq 1\}.$$

And

$$\begin{aligned}
&\mathrm{InnGr}\Pi = \{D \in \mathrm{Der}(\mathrm{Gr}\Pi) | \text{ there is some } T \in \mathrm{Gr}\Pi \text{ such that } D(W) = [T, W] \\
&\qquad\qquad \text{for any } W \in \mathrm{Gr}\Pi\}, \\
&\mathrm{Out}^c\mathrm{Gr}\Pi = \mathrm{Der}^c\mathrm{Gr}\Pi/\mathrm{InnGr}\Pi \text{ (cf.§1.3.1)}, \\
&(\mathrm{Out}^c\mathrm{Gr}\Pi)_m \text{ is the } m\text{-th graded piece of } \mathrm{Out}^c\mathrm{Gr}\Pi, \\
&\qquad\qquad \simeq (\mathrm{Der}^c\mathrm{Gr}\Pi)_m/\mathrm{Im}(\mathrm{gr}^m\Pi),
\end{aligned}$$

where

$$\begin{aligned}
&\mathrm{gr}^m\Pi \to (\mathrm{Der}^c\mathrm{Gr}\Pi)_m \text{ is defined by } W \mapsto \mathrm{ad}(W), \\
&\mathrm{ad}(W) \text{ is the inner derivation defined by } V \mapsto [W, V].
\end{aligned}$$

In addition,

$$\widetilde{C_m} = \begin{cases} \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathrm{gr}^1\Pi, \mathrm{gr}^{m+1}\Pi) \oplus \mathrm{gr}^m\Pi & (m \neq 2), \\ \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathrm{gr}^1\Pi, \mathrm{gr}^{m+1}\Pi) & (m = 2), \end{cases}$$

$$i_m : (\mathrm{Der}^c\mathrm{Gr}\Pi)_m \to \widetilde{C_m} \text{ is defined by } \begin{cases} D \mapsto (D|_{\mathrm{gr}^1\Pi}, T) & (m \neq 2), \\ D \mapsto D|_{\mathrm{gr}^1\Pi} & (m = 2), \end{cases}$$

$j_m : \widetilde{C_m} \to \mathrm{gr}^{m+2}\Pi(-1)$ is defined by

$$\begin{cases} (f, W) \mapsto [f(A), B] + [A, f(B)] + [W, Z] & (m \neq 2), \\ f \mapsto [f(A), B] + [A, f(B)] & (m = 2), \end{cases}$$

$\mathrm{gr}^m\Pi \to \widetilde{C_m}$ is defined by

$$\begin{cases} W \mapsto (\mathrm{ad}(W)|_{\mathrm{gr}^1\Pi}, W) & (m \neq 2), \\ W \mapsto \mathrm{ad}(W)|_{\mathrm{gr}^1\Pi} & (m = 2), \end{cases}$$

and

$$C_m = \widetilde{C_m}/\mathrm{gr}^m\Pi.$$

Moreover $(\mathrm{Out}^c\mathrm{Gr}\Pi)_m$ is a finitely generated free $\mathbb{Z}_\ell$-module ([NT] Corollary 1.16). Consequently, we have $(\mathrm{Out}^c\mathrm{Gr}\Pi)_m$ is a free $\mathbb{Z}_\ell$-module of rank

$$\begin{cases} 2r(m+1) - r(m+2) & (m \neq 2), \\ 2r(3) - r(2) - r(4) & (m = 2), \end{cases}$$

([NT] Corollary 1.16), where $r(m) = \mathrm{rank}_{\mathbb{Z}_\ell}\mathrm{gr}^m\Pi_{1,1}$. And we have $r(1) = 2$, $r(2) = 1$, $r(3) = 2$, $r(4) = 3$, $r(5) = 6$, $r(6) = 9$, $r(7) = 18$ ([K] Proposition 1 or [NT] (1.1.2)). Hence $(\mathrm{Out}^c\mathrm{Gr}\Pi)_m = \{0\}$ when $m = 1, 2, 3, 5$. Therefore $\mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_{\mathbb{Q}} = \{0\}$ when $m = 1, 2, 3, 5$.

(2) This follows from (1), together with Proposition 2.1 (b) $\Leftrightarrow$ (d) and the fact (Theorem 1.11(6)) that $\mathrm{gr}^{(\ell)m}_{0,3}\mathrm{G}_{\mathbb{Q}} = \{0\}$ $(1 \leq m \leq 3)$. □

Proposition 2.4.

(1) $\mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_{\mathbb{Q}} = \{0\}$ *if* $m \equiv 1 \pmod 2$ *and* $\ell > 2$.

(2) *(2) For each* $m \geq 1$, $\mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_{\mathbb{Q}} \simeq \mathrm{gr}^{(\ell)m}_{0,3}\mathrm{G}_{\mathbb{Q}}$ *for almost all* ℓ. *(More precisely,* $\mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_{\mathbb{Q}} \simeq \mathrm{gr}^{(\ell)m}_{0,3}\mathrm{G}_{\mathbb{Q}}$ *for* $\ell > m + 5$.*)*

Proof. $\mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_{\mathbb{Q}}$ may not be torsion-free, unlike $\mathrm{gr}^{(\ell)m}_{0,3}\mathrm{G}_{\mathbb{Q}}$. Thus, the usual weight argument does not work well. Instead, this proposition is proved by a certain "torsion weight argument". More precisely, this proposition is a direct consequence of Theorem 1.11 (7), Proposition 2.1 (d) $\Leftrightarrow$ (f) and the following

Claim 2.5.

(1) $\mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_{\mathbb{Q}}$ *is torsion-free if* $m \equiv 1 \pmod 2$ *and* $\ell > 2$.

(2) $\mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_{\mathbb{Q}}$ *is torsion-free if* $\ell > m+5$.

Proof. We may assume that $m \geq 4$ (Proposition 2.3). Let $p \neq \ell$ be a prime and denote by $\overline{Fr}_p$ the (p-th power) Frobenius element in $G_{\mathbb{F}_p}$. Let $\overline{E}$ be an elliptic curve over $\mathbb{F}_p$ for which the characteristic polynomial of $\overline{Fr}_p$ is X^2+p. (The existence of such an elliptic curve is shown, for example, by Honda-Tate theory. See [W], Theorem 4.1 (5).) Let E be any elliptic curve over $\mathbb{Q}$ which has good reduction at p and whose reduction at p is $\overline{E}$. We denote by Fr_p a lift in $\mathrm{G}_{\mathbb{Q}}$ of $\overline{Fr}_p$. Then Fr_p^2 acts on $\mathrm{gr}^1\Pi \simeq \mathrm{T}_\ell(E\otimes_{\mathbb{Q}}\bar{\mathbb{Q}})$ by $(-p)$-multiplication. Since $\mathrm{T}_\ell(E\otimes_{\mathbb{Q}}\bar{\mathbb{Q}})$ is self-dual, $C_m \simeq \mathrm{gr}^1\Pi(-1)\otimes\mathrm{gr}^{m+1}\Pi$. As $\mathrm{gr}^m\Pi$ is the m-th graded piece of the graded Lie algebra generated by $\mathrm{gr}^1\Pi$, we have $(\mathrm{gr}^1\Pi)^{\otimes m} \twoheadrightarrow \mathrm{gr}^m\Pi$. Hence $(\mathrm{gr}^1\Pi)^{\otimes(m+2)}(-1) \twoheadrightarrow \mathrm{gr}^1\Pi(-1)\otimes\mathrm{gr}^{m+1}\Pi$. Therefore Fr_p^2 acts on C_m by $(-p)^m$-multiplication. Consequently, Fr_p^2 acts on $\mathrm{gr}^m_{1,1}\mathrm{G}_{\mathbb{Q}}$ by $(-p)^m$-multiplication (the commutative diagram in the proof of Proposition 2.3).

Suppose that $(\mathrm{gr}^m_{1,1}\mathrm{G}_{\mathbb{Q}})_{tor} \neq \{0\}$. As the $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) (\simeq \mathbb{Z}_\ell^\times)$-module $(\mathrm{gr}^m_{1,1}\mathrm{G}_{\mathbb{Q}})_{tor}$ is of finite length, there exists a simple $\mathbb{Z}_\ell^\times$-module $M \subset (\mathrm{gr}^m_{1,1}\mathrm{G}_{\mathbb{Q}})_{tor}$. Because M is simple, $1+\ell\mathbb{Z}_\ell$ acts on M trivially. So, the action of $\mathbb{Z}_\ell^\times$ on M factors through $\mathbb{F}_\ell^\times$. Hence there exists an i with $1 \leq i \leq \ell-1$ such that $M \simeq \mathbb{F}_\ell(i)$ as a $\mathbb{Z}_\ell^\times$-module, namely $\gamma\cdot\sigma = \gamma^i\sigma$ for any $\gamma \in \mathbb{F}_\ell^\times$ and $\sigma \in M$. Thus, Fr_p^2 acts on M by p^{2i}-multiplication. On the contrary, Fr_p^2 acts on M by $(-p)^m$-multiplication since $M \subset \mathrm{gr}^m_{1,1}\mathrm{G}_{\mathbb{Q}}$. So $p^{2i} \equiv (-p)^m \pmod{\ell}$. For any $a \not\equiv 0 \pmod{\ell}$, there exists a prime p such that $a \equiv p \pmod{\ell}$ by Chebotarev's density theorem. Thus, we have $a^{2i} \equiv (-a)^m \pmod{\ell}$ for any $a \in \mathbb{F}_\ell^\times$.

Assume that m is odd. When $\ell \neq 2$, there exists $b \in \mathbb{F}_\ell^\times \setminus (\mathbb{F}_\ell^\times)^2$. For such a b, $(b^i)^2 \equiv (-b)^{2i} \equiv b^m \pmod{\ell}$ by the above discussion. On the contrary, $b^m \notin (\mathbb{F}_\ell^\times)^2$, because $b \notin (\mathbb{F}_\ell^\times)^2$ and m is odd. This is a contradiction. Thus, we get the first assertion (1).

Assume that m is even. Then we have $a^{2i} \equiv a^m \pmod{\ell}$ for any $a \in \mathbb{F}_\ell^\times$. Hence $m-2i \equiv 0 \pmod{\ell-1}$. Because $M \neq \{0\}$, there exists some $\tilde{\sigma} \in \mathrm{G}_{1,1}(m)\setminus\mathrm{G}_{1,1}(m+1)$ and $m' \geq m$ such that $\sigma := \tilde{\sigma} \bmod \mathrm{G}_{1,1}(m+1) \in M$ and $\tilde{\sigma} \in \mathrm{G}_{0,3}(m')\setminus\mathrm{G}_{0,3}(m'+1)$ (Theorem 1.12 (2)). We may suppose that m' is even (Theorem 1.11 (6) the first assertion). So $\mathbb{Z}_\ell^\times$ acts on $\tilde{\sigma} \bmod \mathrm{G}_{0,3}(m'+1)$ by Tate twist $\frac{m'}{2}$ (Theorem 1.11 (5)).

Since M is simple, $M \simeq \mathbb{F}_\ell(\frac{m'}{2})$. By this together with $M \simeq \mathbb{F}_\ell(i)$, we have $m' \equiv 2i \pmod{\ell - 1}$. Hence $m' - m \equiv 0 \pmod{\ell - 1}$. On the contrary, $0 \le m' - m \le m + 4$, because $m \le m' \le 2m + 4$ ([IN] the proof of Theorem 3C). Hence we have $m' = m$ since $m + 4 < \ell - 1$ from the assumption of (2). Therefore σ is a torsion-free element in $\mathrm{gr}^m_{1,1}\mathrm{G}_\mathbb{Q}$ (Theorem 1.12 (2) and Theorem 1.11 (6)). This is a contradiction. Thus, $(\mathrm{gr}^m_{1,1}\mathrm{G}_\mathbb{Q})_{tor} = \{0\}$ if m is even and $\ell > m + 5$. Combining this with (1), we get the second assertion (2).

Thus, we complete the proof of Claim 2.5. □

This completes the proof of Proposition 2.4. □

Corollary 2.6. *For each* $1 \le m_0 \le \infty$, $\mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_\mathbb{Q} \simeq \mathrm{gr}^{(\ell)m}_{g,r}\mathrm{G}_\mathbb{Q} \simeq \mathrm{gr}^{(\ell)m}_{0,3}\mathrm{G}_\mathbb{Q}$ $(1 \le m \le m_0)$ *for almost all* ℓ.

Proof. Immediate from Proposition 2.4 and Proposition 2.1 (b) ⇔ (d). □

By Proposition 2.1, the main difficulty to investigate the (g,r)-dependency of Ihara towers of type (g,r) is possible existence of nontrivial torsion. Thus, a good approach may be to choose a suitable single (1,1)-curve X corresponding to $x : \mathrm{Spec}(\kappa(x)) \to \mathcal{M}_{1,1}$ and to observe the natural map

$$\mathrm{gr}^{(\ell)m}_X\mathrm{G}_{\kappa(x)} \to \mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_\mathbb{Q}$$

because $\mathrm{gr}^{(\ell)m}_X\mathrm{G}_{\kappa(x)}$ is torsion-free. (We might even expect that this map is an isomorphism, which, in particular, implies that $\mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_\mathbb{Q}$ is torsion-free.) Here $\mathrm{gr}^{(\ell)m}_X\mathrm{G}_{\kappa(x)} = \mathrm{G}_X(m)/\mathrm{G}_X(m+1)$, $G_X(m) = \mathrm{Ker}(\varphi^{(\ell)}_X(m))$ and $\varphi^{(\ell)}_X(m)$ is the truncated Galois representation

$$\varphi^{(\ell)}_X(m) : G_{\kappa(x)} \to \mathrm{Out}^c(\pi^\ell_1(\bar{X}))/\mathrm{Out}^c(\pi^\ell_1(\bar{X}))(m)$$

(cf. Remark 1.3, Definition 1.4, Definition 1.6). However, another difficulty arises in this approach, as shown in the following

Remark 2.7. Let X be an elliptic curve over a number field $\kappa(x)$, which, together with the origin, is regarded as a (1,1)-curve over $\kappa(x)$. Then the natural $\mathbb{Q}_\ell$-linear map,

$$\rho_X(m) : \mathrm{gr}^{(\ell)m}_X\mathrm{G}_{\kappa(x)} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \to \mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_\mathbb{Q} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

is surjective ([N1] Lemma 4.5). But, as $\mathrm{G}_X(1) \neq \mathrm{G}_{1,1}(1)$, the induction to prove $\mathrm{gr}^{(\ell)m}_X\mathrm{G}_{\kappa(x)} \cong \mathrm{gr}^{(\ell)m}_{1,1}\mathrm{G}_\mathbb{Q}$ does not work well.

This remark implies that the above approach does not go well as far as we choose an elliptic curve X over a number field. A study from a different approach is in progress.

Acknowledgments

The author thanks the referee for careful reading his manuscript and for giving useful comments. The author thanks the organizers for having given him the opportunity of giving the lecture and having coped flexibly with a delay of his writing. The author would like to express his sincerest gratitude to Professor Akio Tamagawa for constant helpful suggestions and warm encouragements.

References

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

[B] F. Brown, *Mixed Tate motives over $\mathbb{Z}$, Annals of Math.* **175** (2012), 949–976.

[HM] 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), 119–167.

[HoMo] Y. Hoshi and S. Mochizuki *On the combinatorial anabelian geometry of nodally non-degenerate outer representations*, *Hiroshima Math. J.* **41** (2011), 275–342.

[Ho] Y. Hoshi *Galois-theoretic characterization of isomorphism classes of monodromically full hyperbolic curves of genus zero*, *Nagoya Math. J.* **203** (2011), pp.47–100.

[I1] Y. Ihara, *Some problems on three point ramifications and associated large Galois representations, Galois Representations and Arithmetic Algebraic Geometry, Adv. Stud. Pure Math.* **12** (1987), Y.Ihara (ed.), 247–273.

[I2] Y. Ihara, *Some arithmetic aspects on Galois actions on the pro-p fundamental group of* $\mathbf{P}^1 - \{0, 1, \infty\}$*, Arithmetic Fundamental Groups, Proc. Sympos. Pure Math.* **70** (2002), M.Fried and Y.Ihara (eds.), 247–273.

[IN] Y. Ihara and H. Nakamura, *On deformation of maximally degenerate stable marked curves and Oda's problem*, *J. reine angew. Math.* **487** (1997), 125–151.

[Ii] Y. Iijima, *Galois action on mapping class groups*, *RIMS preprint* **1761** (2012).

[J] D. Johnson, *An abelian quotient of the mapping class group* $\mathcal{I}_g$, *Math. Ann.* **249** (1980), 225–242.

[K] M. Kaneko, *Certain automorphism groups of pro-l fundamental groups of punctured Riemann surfaces*, *J. Fac. Sci. Univ. Tokyo* **36** (1989), 363–372.

[M] M. Matsumoto, *Galois representations on profinite braid groups on curves*, *J. reine angew. Math.* **474** (1996), 169–219.

[Mo] S. Mochizuki, *Topics surrounding the anabelian geometry of hyperbolic curves*, *Galois Groups and Fundamental Groups, Math. Sci. Res. Inst. Publ.* **41** (2003), L.Schneps (ed.), 119–165.

[N1] H. Nakamura, *Coupling of universal monodromy representations of Galois-Teichmüller modular groups*, *Math. Ann.* **304** (1996), 99–119.

[N2] H. Nakamura, *Limits of Galois representations in fundamental groups along maximal degeneration of marked curves I*, *Amer. J. Math.* **121** (1999), 315–358.

[NTU] H. Nakamura, N. Takao and R. Ueno, *Some stability properties of Teichmüller modular function fields with pro-l weight structures*, *Math. Ann.* **302** (1995), 197–213.

[NT] H. Nakamura and H. Tsunogai, *Some finiteness theorems on Galois centralizers in pro-l mapping class groups*, *J. reine angew Math.* **441** (1993), 115–144.

[O1] 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).

[O2] T. Oda, *Etale homotopy type of the moduli spaces of algebraic curves*, *Geometric Galois Actions 1*, *London Mathematical Society Lecture Note Series* **242** (1997), P.Lochak and L.Schneps (eds.), 85–95.

[S] R. Sharifi, *Relationships between conjectures on the structure of pro-p Galois groups unramified outside p, Arithmetic Fundamental Groups, Proc. Sympos. Pure Math.* **70** (2002), M.Fried and Y.Ihara (eds.), 275–284.

[T] N. Takao, *Braid monodromies on proper curves and pro-ℓ Galois representations*, *J. Inst. Math. Jussieu* **11** (2012), 161–188.

[W] W. C. Waterhouse, *Abelian varieties over finite fields*, *Ann. Sc. Ec. Norm. Sup.* **2** (1969), 521–560.