PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 139, Number 4, April 2011, Pages 1215–1220
S 0002-9939(2010)10846-8
Article electronically published on December 1, 2010

DIFFERENCE BETWEEN GALOIS REPRESENTATIONS IN AUTOMORPHISM AND OUTER-AUTOMORPHISM GROUPS OF A FUNDAMENTAL GROUP

MAKOTO MATSUMOTO

(Communicated by Ted Chinburg)

Dedicated to Professor Takayuki Oda on his 60th birthday

Abstract. Let C be a proper smooth geometrically connected curve over a number field of K of genus $g \geq 3$. For a fixed ℓ, let Π^ℓ denote the pro-ℓ completion of the geometric fundamental group of C. For an L-rational point x of C, we have $\rho_{A,x} : G_L \to \operatorname{Aut} \Pi^\ell$ associated to the base point x, and its quotient by the inner automorphism group $\rho_O : G_L \to \operatorname{Out} \pi^\ell := \operatorname{Aut} / \operatorname{Inn}$, which is independent of the choice of x. We consider whether the equality $\operatorname{Ker} \rho_{A,x} = \operatorname{Ker} \rho_{O,x}$ holds or not. Deligne and Ihara showed the equality when the curve is the projective line minus three points with a choice of tangential basepoint. The result here is: Fix an ℓ dividing $2g-2$. Then there are infinitely many curves of genus g such that for any L-rational point x with $[L : K]$ finite and coprime to ℓ, the index $[\operatorname{Ker} \rho_{O,x} : \operatorname{Ker} \rho_{A,x}]$ is infinite.

1. Introduction

Let $\Pi_{g,n}$ denote the fundamental group of a Riemann surface of genus $g \geq 3$ with n points punctured, and let $\Pi'_{g,n}$ denote its commutator subgroup. The quotient by this commutator, namely the abelianization of $\Pi_{g,n}$, is denoted by H, since it is isomorphic to the first homology group. Let $\Gamma_{g,n}$ denote the mapping class group of an n-pointed genus g surface. In this manuscript, when $n = 0$, we omit the subscript n and write $\Pi_g := \Pi_{g,0}$ and $\Gamma_g := \Gamma_{g,0}$. Based on Morita's result [9, (5.4)], Hain and Reed [4, Prop. 23] proved that the class $e \in H^2(\Gamma_g, H)$ corresponding to the extension

$$1 \to H \to \Gamma_{g,1}/\Pi'_g \to \Gamma_g \to 1 \tag{1}$$

has order $2g - 2$. In particular, this sequence does not split. Based on this topological theorem, we prove a theorem on Galois representations.

Received by the editors September 2, 2009 and, in revised form, April 19, 2010.
2010 *Mathematics Subject Classification.* Primary 11R32; Secondary 14H30, 14H10, 20J05.
The author was supported in part by the Scientific Grants-in-Aid 16204002 and 19204002 and by the Core-to-Core grant 18005 from the Japan Society for the Promotion of Science. Part of this study was done while the author visited the Newton Institute in August 2009.

Let $K \subset \mathbb{C}$ be a number field, and C a smooth geometrically connected curve over K. We call C a (g,n)-curve if it is a proper smooth genus g curve with n K-rational points being removed.

Suppose that $x \in C(K)$ is a K-rational point, and let $\bar{x}$ be a geometric point $\mathrm{Spec}(\overline{K})$ over x taken in $\mathbb{C}$. Let $\overline{C} := C \otimes_K \overline{K}$ be the geometric fiber. For a (g,n) curve C, by SGA1 [3], we have a short exact sequence

$$1 \to \pi_1^{\mathrm{alg}}(\overline{C}, \bar{x}) \to \pi_1^{\mathrm{alg}}(C, \bar{x}) \to G_K \to 1,$$

where π_1^{alg} denotes the algebraic fundamental groups and $G_K := \mathrm{Gal}(\overline{K}/K)$ is the absolute Galois group of K.

Let $\Pi_{g,n}$ denote the topological fundamental group $\pi_1(C(\mathbb{C}), \bar{x})$, as above. By the comparison theorem, $\pi_1^{\mathrm{alg}}(\overline{C}, \bar{x})$ is canonically isomorphic to the profinite completion of $\Pi_{g,n}$ denoted by $\Pi_{g,n}^{\wedge}$. Let $\Pi_{g,n}^{(\ell)}$ denote its maximal pro-ℓ quotient, for a fixed prime ℓ.

In the above short exact sequence, the middle group acts on the left group by conjugation. Since $\Pi_{g,n}^{(\ell)}$ is a characteristic quotient of the left group, the middle group also acts on it. This gives the following diagram:

$$\begin{array}{ccccccccc}
 & & & & G_K & & & & \\
 & & & & \downarrow x_* & & & & \\
1 & \to & \pi_1^{\mathrm{alg}}(\overline{C}, \bar{x}) & \to & \pi_1^{\mathrm{alg}}(C, \bar{x}) & \to & G_K & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \mathrm{Inn}\,\Pi_{g,n}^{(\ell)} & \to & \mathrm{Aut}\,\Pi_{g,n}^{(\ell)} & \to & \mathrm{Out}\,\Pi_{g,n}^{(\ell)} & \to & 1,
\end{array}$$

where Aut (respectively Inn) denotes the continuous automorphism group (the inner automorphism group) of $\Pi_{g,n}^{(\ell)}$, and Out is the quotient, so that the horizontal rows are both exact. The middle vertical map from G_K is induced by $x \to C$, and its composition with the lower-middle vertical map gives the automorphism representation

$$\rho_{A,C,x} : G_K \to \mathrm{Aut}\,\Pi_{g,n}^{(\ell)}.$$

The right vertical map gives the outer Galois representation

$$\rho_{O,C} : G_K \to \mathrm{Out}\,\Pi_{g,n}^{(\ell)}.$$

The absence of x in the subscript reflects the fact that $\rho_{O,C}$ does not depend on the choice of x. Actually, it can be defined using any geometric base point $\bar{x}$; two different choices of base point give an identification on $\pi_1^{\mathrm{alg}}(\overline{C}, \bar{x})$ with ambiguity by inner isomorphisms, which are trivialized in Out.

The commutativity of the above diagram implies that

$$\mathrm{Ker}(\rho_{A,C,x}) \subset \mathrm{Ker}(\rho_{O,C}). \tag{2}$$

Our question is whether equality holds. Consider the statement:

$$E(C,x,\ell): \quad \mathrm{Ker}(\rho_{A,C,x}) = \mathrm{Ker}(\rho_{O,C}).$$

It is equivalent to the statement $\mathrm{Im}(\rho_{A,C,x}) \cap \mathrm{Inn}\,\Pi_{g,n}^{(\ell)} = \{1\}$. Our main result is that there are many examples such that $E(C,x,\ell)$ does not hold.

2. Projective line minus three points

Deligne and Ihara proved $E(\mathbb{P}^1-\{0,1,\infty\},\vec{01},\ell)$ for all ℓ, where $\vec{01}$ is a $\mathbb{Q}$-rational tangential base point.

We start with a general remark. Suppose that $n \geq 1$ and that C is a curve of type (g,n). Fix a K-rational puncture u and a nonzero tangent vector $\vec{v}$ in the compactification at u. One can construct

$$\rho_{A,C,\vec{v}} : G_K \to \pi_1^{\mathrm{alg}}(C,\vec{v})^{(\ell)},$$

as in [2], [6]. If ξ is a small loop at the base point $\vec{v}$ that encircles the puncture u, then one can show that for all $\sigma \in G_K$,

$$\rho_{A,C,\vec{v}}(\sigma) : \xi \mapsto \xi^{\chi(\sigma)},$$

where χ is the ℓ-adic cyclotomic character $\chi : G_K \to \mathbb{Z}_\ell^\times$. Let $\langle\xi\rangle$ denote the subgroup topologically generated by ξ. If $2g-2+n>0$ and $n \geq 1$, then the normalizer of $\langle\xi\rangle \subset \Pi_{g,n}^{(\ell)}$ is $\langle\xi\rangle$ itself ([1]). Therefore, if $\rho_{A,C,\vec{v}}(\sigma)$ is an inner automorphism, since it normalizes $\langle\xi\rangle$, it is an inner automorphism by a power of ξ, which is a very restrictive condition.

In the case of $\mathbb{P}^1-\{0,1,\infty\}$ with base point $\vec{01}$, Ihara [5, p. 55] showed that $E(\mathbb{P}^1-\{0,1,\infty\},\vec{01},\ell)$ is true.

Historically, by a group-theoretic method, Belyi constructed a lift of the outer Galois representation to an automorphism representation that contains no inner automorphisms. Then, Deligne gave its geometric realization using a tangential base point: see [5, p. 47].

3. Main result

Let C/K be a $(g,0)$ curve with $2g-2>0$. Let x be a closed point of C and let $L := k(x)$ be the residue field at x (hence L/K is a finite extension and $x \in C(L)$). In the same way as in §1, we have $\rho_{A,C,x} : G_L \to \operatorname{Aut}\Pi_{g,n}^{(\ell)}$. We consider whether the following equality holds:

$$\operatorname{Inn}\Pi_g^{(\ell)} \cap \rho_{A,C,x}(G_L) = \{1\}, \tag{3}$$

which we designate by $E'(C,x,\ell)$. It is equivalent to the statement $E(C\times_K L,x,\ell)$ in the previous notation.

The following is the main theorem of this article.

Theorem 1. *Suppose that $g \geq 3$ and a prime ℓ divides $2g-2$. Let ℓ^ν be the highest power of ℓ that divides $2g-2$. Then, there are infinitely many C/K, where K moves over number fields, and C moves over a proper smooth geometrically connected curve over K of genus g, with the following property. For any closed point x of C with residue field $L := k(x)$ such that ℓ^ν does not divide $[L:K]$, the intersection*

$$\rho_{A,C,x}(G_L) \cap \operatorname{Inn}\Pi_g^{(\ell)}$$

is an infinite group (hence not trivial). Consequently, $E'(C,x,\ell)$ is false for any such x.

4. Proof

4.1. **Universal monodromy.** Again fix a number field K. Let $\mathcal{M}_{g,n}$ be the moduli stack of (g,n)-curves, with base field extended to K. (Again, if $n=0$, then it is omitted in the subscript.) Then, $\mathcal{M}_{g,n+1} \to \mathcal{M}_{g,n}$ is the universal family of (g,n)-curves. Thus, for a (g,n)-curve C/K, there is a classifying map $[C/K] : \operatorname{Spec} K \to \mathcal{M}_{g,n}$ such that C/K is isomorphic to the pullback of the universal curve. This induces the following diagram consisting of exact rows:

$$\begin{array}{ccccccccc}
 & & & & G_L & & & & \\
 & & & & \downarrow x_* & & & & \\
1 & \to & \pi_1^{\mathrm{alg}}(\overline{C},\bar{x}) & \to & \pi_1^{\mathrm{alg}}(C,\bar{x}) & \to & G_K & \to & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \to & \pi_1^{\mathrm{alg}}(\overline{C},\bar{x}) & \to & \pi_1^{\mathrm{alg}}(\mathcal{M}_{g,n+1},\bar{x}) & \to & \pi_1^{\mathrm{alg}}(\mathcal{M}_{g,n},\bar{x}) & \to & 1 \\
 & & \downarrow & & \downarrow \rho_{A,univ,x} & & \downarrow \rho_{O,univ} & & \\
1 & \to & \operatorname{Inn}\Pi_{g,n}^{(\ell)} & \to & \operatorname{Aut}\Pi_{g,n}^{(\ell)} & \to & \operatorname{Out}\Pi_{g,n}^{(\ell)} & \to & 1.
\end{array}$$

The definition and the exactness of the middle row is due to Takayuki Oda [10]: note that the left injectivity of this row follows from the center-freeness of the $\pi_1^{\mathrm{alg}}(\overline{C})$ under the condition $2g-2+n>0$, which injects through $\pi_1^{\mathrm{alg}}(\mathcal{M}_{g,n+1}) \to \operatorname{Aut}\Pi_{g,n}^{\wedge}$. The commutativity of the diagram implies that $\rho_{A,C,x}$ is the composition of the three middle vertical arrows, and $\rho_{O,C}$ is the composition of the two right vertical arrows.

The Main Theorem 1 is now a consequence of the following two theorems.

Theorem 2 (Theorem 1.2 in [8])**.** *There exist infinitely many (g,n)-curves over number fields such that* $\operatorname{Im}\rho_{O,C} = \operatorname{Im}\rho_{O,univ}$.

Remark 4.1. In the above, the existence is proved by choosing a dominating quasifinite map from the moduli stack $\mathcal{M}_{g,n}/\mathbb{Q}$ to the projective space $f : \mathcal{M}_{g,n}/\mathbb{Q} \to \mathbb{P}^{3g-3+n}/\mathbb{Q}$. For any such f, one can conclude that the set of the closed points in $\mathcal{M}_{g,n}$ corresponding to curves with the above property is not thin in $\mathbb{P}^{3g-3+n}(\mathbb{Q})$ in the sense of Hilbert's irreducibility theorem. In particular, if the moduli stack is rational, then we have infinitely many such curves for any one fixed number field K.

One can also assume that C has at least one K-rational point. Then one can show that there exist infinitely many $x \in C$ with $[k(x):K]$ being coprime to ℓ.

An essential ingredient of the proof of Theorem 2 is Hilbert's irreducibility theorem, and the first half of Remark 4.1 follows the proof there. We may assume that moreover C has at least one K-rational point, by applying the theorem to $(g,n+1)$-curves. Once C has a K-rational point, then, by Riemann-Roch, there are functions to $\mathbb{P}^1/K$ with a pole at the rational point with order d if d is sufficiently large. In particular, we may assume that d is prime to ℓ. Hilbert's irreducibility shows that there are infinitely many closed points on C with residue extension degree being d. This proves the last part of Remark 4.1.

Consider the exact sequence

$$1 \to \operatorname{Inn}\Pi_g^{(\ell)} \to \operatorname{Im}\rho_{A,univ,x} \to \operatorname{Im}\rho_{O,univ} \to 1. \tag{4}$$

For a finite index subgroup $S < \operatorname{Im}\rho_{O,univ}$, a group homomorphism $S \to \operatorname{Im}\rho_{A,univ,x}$ is called a section on S to the above exact sequence if its composite with the projection is an identity on S.

Theorem 3. *Suppose that ℓ divides $2g-2$. Let ν be the multiplicity of ℓ in $2g-2$. Suppose $n=0$, so we treat $\mathcal{M}_{g,1} \to \mathcal{M}_g$. If the index $[\operatorname{Im}\rho_{O,univ} : S]$ is not a multiple of ℓ^ν, then there is no section on S. Moreover, under the same condition, if $S' < \operatorname{Im}\rho_{A,univ,x}$ is a subgroup that surjects to S, then $S' \cap \operatorname{Inn}\Pi_g^{(\ell)}$ is an infinite group.*

More strongly, the image of $S' \cap \operatorname{Inn}\Pi_g^{(\ell)}$ in the pro-ℓ abelianization of $\operatorname{Inn}\Pi_g^{(\ell)}$ is infinite.

A proof is given in the next section. Now we prove Theorem 1. Take a (g,n)-curve C/K satisfying the condition in Theorem 2. For $x \in C(L)$, let S' be $\rho_{A,C,x}(G_L)$ and let S be its image in $\operatorname{Im}\rho_{O,univ}$. Then $S = \rho_{O,C}(G_L)$, which has a finite index in $\rho_{O,C}(G_K)$ that divides $[L:K]$, hence is not divisible by ℓ^ν by the assumption on $[L:K]$. Then, Theorem 2 assures that $\rho_{O,C}(G_K) = \operatorname{Im}\rho_{O,univ}$, and hence S' and S satisfy the condition in Theorem 3, which implies that $S' \cap \operatorname{Inn}\Pi_g^{(\ell)}$ is infinite and has an infinite image in the abelianization of $\operatorname{Inn}\Pi_g^{(\ell)}$, as desired.

4.2. **Proof of Theorem 3.** Since $\Pi_g^{(\ell)}$ is center free [1], the natural map $\Pi_g^{(\ell)} \to \operatorname{Inn}\Pi_g^{(\ell)}$ is an isomorphism of topological groups, and these groups are identified. Let $\Pi^{(\ell)\prime}$ denote the topological (i.e. the closure of the) commutator subgroup of $\Pi_g^{(\ell)}$. Let $H^{(\ell)}$ be the abelianization $\Pi_g^{(\ell)}/\Pi^{(\ell)\prime}$. By taking the quotient of the exact sequence in the statement of Theorem 3 by $\Pi^{(\ell)\prime}$, we have the following diagram:

$$\begin{array}{ccccccccc}
1 & \to & H^{(\ell)} & \to & \operatorname{Im}\rho_{A,univ,x}/\Pi^{(\ell)\prime} & \to & \operatorname{Im}\rho_{O,univ} & \to & 1 \\
 & & || & & \uparrow & & \uparrow & & \\
1 & \to & H^{(\ell)} & \to & \widetilde{\Gamma_g} & \to & \Gamma_g & \to & 1 \\
 & & \uparrow & & \uparrow & & || & & \\
1 & \to & H & \to & \Gamma_{g,1}/\Pi' & \to & \Gamma_g & \to & 1.
\end{array}$$

Here, the top row is the exact sequence obtained by dividing by $\Pi^{(\ell)\prime}$ at the left and middle groups of the exact sequence (4).

The group $\Gamma_{g,n}$ is the topological fundamental group of the analytic stack $\mathcal{M}_{g,n}(\mathbb{C})$ in the orbifold sense with the base point $\bar{x}$. Accordingly, there is a natural morphism $\Gamma_g \to \pi_1^{\mathrm{alg}}(\mathcal{M}_g, \bar{x}) \to \operatorname{Im}\rho_{O,univ}$. Oda proved that $\Gamma_{g,n}$ is isomorphic to the mapping class groups of (g,n) curves [10]. The middle row is the pullback of the first row along this homomorphism, in the category of discrete groups (i.e., the topology is forgotten). That is, $\widetilde{\Gamma_g}$ is the fiber product of the upper-middle group and the right-middle group over the right-upper group. It is a group-theoretic conclusion that the kernel of $\widetilde{\Gamma_g} \to \Gamma_g$ is $H^{(\ell)}$.

The bottom row is obtained from the fiber homotopy sequence in the (usual discrete) fundamental groups

$$1 \to \Pi_g \to \Gamma_{g,1} \to \Gamma_g \to 1$$

by dividing by the commutator subgroup Π' of Π_g in a way similar to the above. The abelianization of Π_g is canonically isomorphic to the first homology H of the curve $C(\mathbb{C})$ with $\mathbb{Z}$-coefficient. By the comparison theorem of GAGA type shown in [10], the bottom short exact sequence has a morphism to the top exact sequence, and it factors through the middle because the middle exact sequence is defined by pullback.

By Schreier Theory, these three extensions give extension classes in the second cohomologies: e_{univ}, e_ℓ, and e, in the following three cohomologies:

$$H^2(\operatorname{Im}\rho_{O,univ}, H^{(\ell)}) \to H^2(\Gamma_g, H^{(\ell)}) \leftarrow H^2(\Gamma_g, H).$$

Here, every cohomology is the cohomology of discrete groups. Because the middle row is the pullback, e_{univ} is mapped to e_ℓ. On the other hand, it is clear that e is mapped to e_ℓ. Hain and Reed [4, Prop. 23] show that the degree of e is exactly $2g-2$ for $g \geq 3$, as mentioned in the introduction.

Since $H^{(\ell)} \cong H \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ (see [7]), the flatness of $\mathbb{Z}_\ell$ over $\mathbb{Z}$ implies that the order of e_ℓ is ℓ^ν, that is, the highest power dividing $2g-2$. Consequently, the order of e_{univ} is either infinite or a multiple of ℓ^ν. In Theorem 3, $\nu \geq 1$ is assumed. If a subgroup $S < \operatorname{Im}\rho_{O,univ}$ has index d, then it is well known that the composition of the corestriction and the restriction is multiplication by d. Thus, if d does not divide ℓ^ν, then the restriction of e_{univ} to $H^2(S, H^\ell)$ is nonzero; hence there is no section on S. This implies that any subgroup $\widetilde{S} \subset \rho_{A,univ,x}/\Pi_g^{(\ell)\prime}$ that surjects to S has a nontrivial kernel; namely, $\widetilde{S} \cap H^{(\ell)}$ is nonempty. Since $H^{(\ell)} \cong \mathbb{Z}_l^{2g}$ is torsion-free, this intersection is infinite.

Returning to (4), let $S' < \operatorname{Im}\rho_{A,univ,x}$ be a subgroup that surjects to S and let N be the kernel of $S' \to S$. Consider the image $\overline{N}$ of N by the abelianization $N < \Pi_g^{(\ell)} \to H^{(\ell)}$. If $\overline{N}$ is trivial, then $S' \to \widetilde{S}$ factors through $S \cong S'/N$. This and the surjectivity of $\widetilde{S} \to S$ imply the existence of a section on S to the top exact sequence in the diagram, thus contradicting the nonvanishing of $e_{univ}|_S \in H^2(S, H^\ell)$. This implies the latter statements in Theorem 3.

References

[1] M. Anderson: *Exactness properties of profinite completion functors*, Topology 13 (1974), 229–239. MR0354882 (50:7359)

[2] P. Deligne: *Le groupe fondamental de la droite projective moins trois points*, in Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), 79–297, Math. Sci. Res. Inst. Publ., 16, Springer, New York-Berlin, 1989. MR1012168 (90m:14016)

[3] A. Grothendieck: *Revêtement Étales et Groupe Fondamental (SGA 1)*, Lecture Notes in Math., 224, Springer-Verlag, 1971. MR0354651 (50:7129)

[4] R. Hain and D. Reed: *Geometric proofs of some results of Morita*, J. Algebraic Geom. 10 (2001), 199–217. MR1811554 (2001m:14041)

[5] Y. Ihara: *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) 123 (1986), 43–106. MR825839 (87c:11055)

[6] Y. Ihara: *Braids, Galois groups and some arithmetic functions*, Proc. Int. Congress of Math., Kyoto, 1990, Springer-Verlag, Tokyo (1991) vol. 1, 99-120. MR1159208 (95c:11073)

[7] J. Labute: *On the descending central series of groups with a single defining relation*, J. Algebra 14 (1970), 16–23. MR0251111 (40:4342)

[8] M. Matsumoto and A. Tamagawa: *Mapping-class-group action versus Galois action on profinite fundamental groups*, American Journal of Mathematics 122 (2000), 1017–1026. MR1781929 (2002a:14022)

[9] S. Morita: *Families of Jacobian manifolds and characteristic classes of surface bundles, I*, Ann. Inst. Fourier, Grenoble 39 (1989), 777–810. MR1030850 (91d:32028)

[10] T. Oda, *Etale homotopy type of the moduli spaces of algebraic curves*, Geometric Galois actions, 1, 85–95, London Math. Soc. Lecture Note Ser., 242, Cambridge Univ. Press, Cambridge, 1997. MR1483111 (2000a:14030)

Graduate School of Mathematical Sciences, University of Tokyo, Tokyo, 153-8914 Japan

E-mail address: matumoto@ms.u-tokyo.ac.jp