J. Math. Sci. Univ. Tokyo
1 (1994), 71–136.

Galois rigidity of pure sphere braid groups and profinite calculus

By Hiroaki Nakamura

Abstract. Let $\mathfrak{C}$ be a class of finite groups closed under the formation of subgroups, quotients, and group extensions. For an algebraic variety X over a number field k, let $\pi_1^{\mathfrak{C}}(X)$ denote the ($\mathfrak{C}$-modified) profinite fundamental group of X having the absolute Galois group $Gal(\bar{k}/k)$ as a quotient with kernel $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ the maximal pro-$\mathfrak{C}$ quotient of the geometric fundamental group of X. The purpose of this paper is to show certain rigidity properties of $\pi_1^{\mathfrak{C}}(X)$ for X of hyperbolic type through the study of outer automorphism group $Out\pi_1^{\mathfrak{C}}(X)$ of $\pi_1^{\mathfrak{C}}(X)$. In particular, we show finiteness of $Out\pi_1^{\mathfrak{C}}(X)$ when X is a certain typical hyperbolic variety and $\mathfrak{C}$ is the class of finite l-groups (l: odd prime).

Indeed, we have a criterion of Gottlieb type for center-triviality of $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ under certain good hyperbolicity condition on X. Then our question on finiteness of $Out\pi_1^{\mathfrak{C}}(X)$ for such X is reduced to the study of the exterior Galois representation $\varphi_X^{\mathfrak{C}} : Gal(\bar{k}/k) \to Out\pi_1^{\mathfrak{C}}(X_{\bar{k}})$, especially to the estimation of the centralizer of the Galois image of $\varphi_X^{\mathfrak{C}}$ (§1.6). In §2, we study the case where X is an algebraic curve of hyperbolic type, and give fundamental tools and basic results. We devote §3, §4 and Appendix to detailed studies of the special case $X = M_{0,n}$, the moduli space of the n-point punctured projective lines ($n \geq 3$), which are closely related with topological work of N. V. Ivanov, arithmetic work of P. Delinge, Y. Ihara, and categorical work of V. G. Drinfeld. Section 4 deal with a Lie variant suggested by P. Deligne.

§0. Introduction

In this paper, we shall study some special algebraic varieties whose profi-

---

1991 *Mathematics Subject Classification.* Primary 14E20; Secondary 14F35, 20F34, 20F36.

nite fundamental groups possess certain "rigidity" properties under the Galois group operation.

Let X be an algebraic variety defined over a number field k, and $Aut_k X$ the group of all the k-automorphisms of X. Suppose that we have a good homotopy theory in which there is a canonical homomorphism

$$\Phi_X : Aut_k X \to E_k(X),$$

where $E_k(X)$ is the group of the classes of self-homotopy equivalences of X compatible with hypothetical Galois actions. Any "continuous" parameter in $Aut_k X$ should be mapped trivially into the target homotopy set $E_k(X)$ by Φ_X. Suppose that some suitable hyperbolicity condition is imposed on X, so that the finiteness of $Aut_k X$ eliminates such continuous parameters, and the map Φ_X approaches injectivity. Then at that stage, our basic question is to what extent one can expect $Aut_k X$ to be reflected faithfully or precisely in $E_k(X)$ via Φ_X. Especially, can one expect $E_k(X)$ to be finite?

The purpose of this paper is to provide some positively directed case studies around these questions, in the situation where X is $K(\pi, 1)$ and $E_k(X)$ is defined in the continuous outer automorphism group of the profinite fundamental group of $X_{\bar{k}} = X \otimes \bar{k}$.

To be more precise, let $\mathfrak{C}$ be a class of finite groups closed under the formation of subgroups, quotients and group extensions. We denote by $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ the maximal pro-$\mathfrak{C}$ quotient of the etale profinite fundamental group $\pi_1(X_{\bar{k}})$, and let $\pi_1^{\mathfrak{C}}(X)$ be the quotient of $\pi_1(X)$ divided by the kernel of $\pi_1(X_{\bar{k}}) \to \pi_1^{\mathfrak{C}}(X_{\bar{k}})$. If G_k denotes the absolute Galois group of k, then there is an exact sequence

$$1 \longrightarrow \pi_1^{\mathfrak{C}}(X_{\bar{k}}) \longrightarrow \pi_1^{\mathfrak{C}}(X) \xrightarrow{p^{\mathfrak{C}}_{X/k}} G_k \longrightarrow 1,$$

together with a canonical exterior Galois representation

$$\varphi_X^{\mathfrak{C}} : G_k \to Out\pi_1^{\mathfrak{C}}(X_{\bar{k}}).$$

We shall say that a continuous group automorphism f of $\pi_1^{\mathfrak{C}}(X)$ is G_k-compatible, if it satisfies the condition $p^{\mathfrak{C}}_{X/k} \circ f = p^{\mathfrak{C}}_{X/k}$, and denote the group of all the G_k-compatible automorphisms of $\pi_1^{\mathfrak{C}}(X)$ by $Aut_{G_k}\pi_1^{\mathfrak{C}}(X)$. Moreover, we put

$$E_k^{\mathfrak{C}}(X) = Aut_{G_k}\pi_1^{\mathfrak{C}}(X)/Inn\pi_1^{\mathfrak{C}}(X_{\bar{k}}),$$

where $Inn\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ is the subgroup formed by the inner automorphisms of $\pi_1^{\mathfrak{C}}(X)$ induced by the elements of $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$. It follows from the functoriality of etale fundamental groups ([13]) that there is a canonical homomorphism

$$\Phi_X^{\mathfrak{C}} : Aut_k X \to E_k^{\mathfrak{C}}(X),$$

whose image is not necessarily a normal subgroup of $E_k^{\mathfrak{C}}(X)$. This paper will provide several examples of $(X, \mathfrak{C})$ with $E_k^{\mathfrak{C}}(X)$ finite or $\Phi_X^{\mathfrak{C}}$ bijective, in the case where

$$\mathfrak{C} = \mathfrak{C}_l = \{\text{all finite } l\text{-groups}\} \quad (l : \text{a prime}).$$

In this pro-l case, we shall also write as

$$E_k^{\mathfrak{C}}(X) = E_k^{(l)}(X), \quad \Phi_X^{\mathfrak{C}} = \Phi_X^{(l)}, \quad \pi_1^{\mathfrak{C}}(X) = \pi_1^{(l)}(X).$$

Let us here introduce our central basic object: the moduli space of ordered n-pointed projective lines $M_{0,n}$ defined by

$$M_{0,n} = (\mathbf{P}^1)^n - \{\text{week diagonals}\}/PGL_2 \quad (n \geq 3).$$

For example, $M_{0,3}$ is a point, $M_{0,4}$ is $\mathbf{P}^1 - \{0, 1, \infty\}$, and $M_{0,5}$ is $\mathbf{P}^2$ minus 6 lines (complete quadrangle). The topological fundamental group $\pi_1(M_{0,n}(\mathbb{C}))$ is isomorphic to the Teichmüller modular group of type $(0, n)$, denoted by Γ_0^n. Fixing a number field k of finite degree over $\mathbb{Q}$, we consider $M_{0,n}$ to be defined over k.

Theorem A. *Let l be an odd prime. Then $Out\pi_1^{(l)}(M_{0,n})$ is finite, and the homomorphism*

$$\Phi_{M_{0,n}}^{(l)} : Aut_k M_{0,n} \to E_k^{(l)}(M_{0,n})$$

gives a bijection ($n \geq 4$)*. Moreover, if* $\mathit{\Gamma}_0^{n,pro-l}$ *denotes the pro-l completion of* $\mathit{\Gamma}_0^n$*, then the canonical exterior representation*

$$\varphi_{0,n}^{(l)} : G_k \to Out\mathit{\Gamma}_0^{n,pro-l}$$

induced from the variety $M_{0,n}$ *over* k *has image whose centralizer is isomorphic to* S_3 *when* $n = 4$*, and to* S_n *when* $n \geq 5$*.*

It is known that the automorphism group of $M_{0,n}$ is just the symmetric group S_n when $n \geq 5$, while the action of S_4 on $M_{0,4}$ factors through S_3 ([45], [29]; see also [34] §5). Actually, for more general $\mathfrak{C}$ satisfying certain admissibility condition for $\mathit{\Gamma}_0^n$ (1.2.2), we show that $\Phi_{M_{0,n}}^{\mathfrak{C}}$ has an inverse $\Psi_n^{\mathfrak{C}} : E_k^{\mathfrak{C}}(M_{0,n}) \to Aut_k M_{0,n}$ with $\Psi_n^{\mathfrak{C}} \circ \Phi_{M_{0,n}}^{\mathfrak{C}} = 1$ (Theorem (3.1.13)). Moreover, if $U_k^{\mathfrak{C}}(M_{0,n})$ denotes the kernel of $\Psi_n^{\mathfrak{C}}$, then we can construct an embedding $U_k^{\mathfrak{C}}(M_{0,n}) \hookrightarrow U_k^{\mathfrak{C}}(M_{0,n-1}) \times U_k^{\mathfrak{C}}(M_{0,n-1})$ ($n \geq 5$) (Corollary (3.2.3)). Therefore for proving the bijectivity of $\Phi_{M_{0,n}}^{\mathfrak{C}}$ ($n \geq 5$), we are reduced to the case of $M_{0,4} = \mathbf{P}^1 - \{0, 1, \infty\}$ ("le premier étage"). In particular, Theorem A follows from [31]. We remark that rough description of the proof of Theorem A was announced in [32].

There is a Lie variant of Theorem A suggested by P.Deligne. It is formulated in terms of l-adic realizations of the motivic fundamental groups of $M_{0,n}$ ($n \geq 5$) in the sense of [8].

THEOREM B. *Assume that* l *is an odd prime. Let* $\mathcal{L}_l(\mathit{\Gamma}_0^n)$ *be the projective limit of the Lie algebras of* l*-adic analytic groups associated with nilpotent quotients of* $\mathit{\Gamma}_0^n$ *(see 4.2.2 for the precise definition), and let*

$$\varphi_n^{Lie} : G_k \to Out\mathcal{L}_l(\mathit{\Gamma}_0^n).$$

be the canonical Galois representation. Then the centralizer of the Galois image $\varphi_n^{Lie}(G_k)$ *in* $Out\mathcal{L}_l(\mathit{\Gamma}_0^n)$ *is isomorphic to the symmetric group* S_n *when* $n \geq 5$*.*

Theorems A and B may be considered as profinite analogues of a topological theorem by N.V.Ivanov which asserts that the outer automorphism group of the discrete group $\mathit{\Gamma}_0^n$ ($n \geq 5$) is a finite group, an extension of S_n by $\mathbb{Z}/2\mathbb{Z}$ ([21], see also [26]). It seems remarkable that Theorem A is valid even in the 1-dimensional case of $n = 4$, while in this case the Lie variant has not yet been assured. As $M_{0,4} = \mathbf{P}^1 - \{0, 1, \infty\}$ is a typical algebraic curve of hyperbolic type, we will be led to the following conjecture.

CONJECTURE C. *Let C be a smooth hyperbolic curve over a number field k, and let l be a prime number. Then $Out\pi_1^{(l)}(C)$ would be finite.*

In this paper, Conjecture C will be verified for hyperbolic lines together with hyperbolic curves with special stable reductions and Jacobians (Theorems (2.2.5), (2.3.1)). Further examples supporting the Conjecture C will be obtained in a joint work with H.Tsunogai ([35]).

In §1, we prepare relatively general statements about pro-$\mathfrak{C}$ groups, and establish basic relations among three objects: $E_k^{\mathfrak{C}}(X)$, $Out\pi_1^{\mathfrak{C}}(X)$, and the centralizers of the Galois image of $\varphi_X^{\mathfrak{C}}$. As a result, we realize that the center-triviality of $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ makes the situation quite clear. In §2, we study the case where X is a smooth hyperbolic curve. Weight characterization of inertia subgroups in 2.1 will give a technical key point in later parts of the present paper. In 2.2, 2.3, some examples supporting Conjecture C will be given. In §3, we study the case where $X = M_{0,n}$. Subsection 3.1 is devoted to showing that certain special inertia subgroups are invariant under the Galois-compatible automorphisms of $\pi_1^{\mathfrak{C}}(M_{0,n})$. In 3.2, Theorem A is proved by inductive reduction to the case of $n = 4$ [31]. In §4, Lie variants are discussed. In 4.1, we compute the automorphism group of the graded Lie algebras associated with the lower central series of Γ_0^n (4.1.2). By applying it, we prove Theorem B in 4.2. The line of the proof of Theorem B is due to P.Deligne. In Appendix, we give another proof of Drinfeld's pentagon formula [9] (which is reformulated by Y.Ihara [20] in the presented cyclic form) concerning the Galois image in the automorphism group of the fundamental group of $\mathbf{P}^1 - \{0, 1, \infty\}$. Our proof is purely group-theoretical, and is closely related with the technique developed in §3. A sketch of a more geometric proof of it can be found in Ihara's article [20].

As explained in Drinfeld's paper [9], consideration of the varieties $M_{0,n}$ as primitive examples of so-called "anabelian" varieties is recommended in Grothendieck's mysterious note [14]. The present study of this paper also started from a desire to understand [14] more mathematically through concrete materials.

The author would like to express his sincere gratitude to Professors P.Deligne, Y.Ihara and Takayuki Oda. Professor Oda kindly inspired in the author various fundamental material including [12], [45], etc., and gave warm encouragement and suggestions. Pioneer work and attitudes of Professor Ihara often indicated leading principle in the course of this study. Professor Deligne, after reading the original version of this paper, gave several comments on it, and especially suggested the possibility of the Lie variant of Theorem A through kind letters. Finally, the author also thanks Professors M.Asada and H.Konno for valuable discussion and communication.

Contents

§1. Preliminaries

1.1. $\mathfrak{C}$-good groups

A class $\mathfrak{C}$ of finite groups is said to be *almost full*, if it is closed under the formation of subgroups, quotients, and finite products. If it is further closed under the formation of group extensions, it is called a *full* class of finite groups. When $\mathfrak{C}$ is almost full, a pro-$\mathfrak{C}$ group is, by definition, a profinite group obtained as the limit of a projective system in $\mathfrak{C}$.

Given a discrete group Γ and an almost full class $\mathfrak{C}$ of finite groups, the set $\mathcal{N} = \mathcal{N}(\Gamma, \mathfrak{C})$ of all the normal subgroups of Γ with quotients in $\mathfrak{C}$ forms a family such that
(1.1.1) $N \in \mathcal{N}, N \subset N' \lhd \Gamma \Rightarrow N' \in \mathcal{N}$;
(1.1.2) $N, N' \in \mathcal{N} \Rightarrow N \cap N' \in \mathcal{N}$.
From this, we see that $\{\Gamma/N | N \in \mathcal{N}\}$ forms naturally a projective system in $\mathfrak{C}$, and we define the pro-$\mathfrak{C}$ completion $\hat{\Gamma} = \hat{\Gamma}(\mathfrak{C})$ of Γ to be the projective limit $\varprojlim_{N \in \mathcal{N}} \Gamma/N$. The canonical map $i : \Gamma \to \hat{\Gamma}$ has a dense image and satisfies the universal property: every homomorphism of Γ into a pro-$\mathfrak{C}$ group always factors through i.

The pro-$\mathfrak{C}$ completion of $\mathbb{Z}$ is denoted by $\mathbb{Z}_{\mathfrak{C}}$. If $\mathfrak{C}$ is a full class, then $\mathbb{Z}_{\mathfrak{C}} = \prod_{p \in |\mathfrak{C}|} \mathbb{Z}_p$. Here we define $|\mathfrak{C}|$ to be the set of all primes p such that $\mathbb{Z}/p\mathbb{Z} \in \mathfrak{C}$.

Let $\mathcal{S} = \mathcal{S}(\Gamma, \mathfrak{C})$ be the family of subgroups of Γ containing some elements in $\mathcal{N}(\Gamma, \mathfrak{C})$, and for each $\Pi \in \mathcal{S}$, denote by $\bar{\Pi}$ the closure of the image of Π by $i : \Gamma \to \hat{\Gamma}$. The map $\Pi \to \bar{\Pi}$ gives a bijection of $\mathcal{S}(\Gamma, \mathfrak{C})$ into the set of open subgroups of $\hat{\Gamma}$ such that $(\Gamma : \Pi) = (\hat{\Gamma} : \bar{\Pi})$ ([10]15.14). Moreover, if $\mathfrak{C}$ is a full class, it is easy to see $\mathcal{S}(\Pi, \mathfrak{C}) \subset \mathcal{S}(\Gamma, \mathfrak{C})$ for every $\Pi \in \mathcal{S}(\Gamma, \mathfrak{C})$. From this we see, in this case, that $\bar{\Pi}$ is isomorphic to the pro-$\mathfrak{C}$ completion of Π itself ([25]).

In what follows, $\mathfrak{C}$ is assumed to be a full class of finite groups. Let Γ be a discrete group, G the pro-$\mathfrak{C}$ completion of Γ, and $\mathfrak{C}(G)$ the abelian category of (finite) continuous G-modules in $\mathfrak{C}$. Each object M of $\mathfrak{C}(G)$ can be considered as a Γ-module via $i : \Gamma \to \hat{\Gamma} = G$, and a finite Γ-module $M \in \mathfrak{C}$ comes from $\mathfrak{C}(G)$ if and only if the image of $\Gamma \to Aut(M)$ belongs to $\mathfrak{C}$. Trivial G (or equivalently Γ)-modules are called constant. The restriction of the standard cochains induces a canonical homomorphism of the profinite group cohomology $H^q(G, M)$ into the discrete group cohomology $H^q(\Gamma, M)$ for every $M \in \mathfrak{C}(G)$ and $q \geq 0$.

Definition (1.1.3) (Serre [41] I-36/Artin-Mazur [2] §6). Notations being as above, the discrete group Γ is called $\mathfrak{C}$-*good*, if the canonical homomorphism $H^q(G, M) \to H^q(\Gamma, M)$ gives an isomorphism for every $q \geq 1$ and $M \in \mathfrak{C}(G)$.

Definition (1.1.4) (Serre [42]). A discrete group Γ is said to be *of* *type FP*, if the trivial $\mathbb{Z}[\Gamma]$-module $\mathbb{Z}$ has a finite projective resolution:

$$0 \to P_n \to \cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0,$$

where P_i $(0 \le i \le n)$ are finitely generated projective $\mathbb{Z}[\Gamma]$-modules. If we can take finitely generated free $\mathbb{Z}[\Gamma]$-modules for P_i $(0 \le i \le n)$ above, then we say Γ is *of type FL*.

If Π varies in $\mathcal{S}(\Gamma, \mathfrak{C})$, the cohomology groups $H^q(\Pi, M)$ form an inductive system with respect to the restriction maps, and the homology groups $H_q(\Pi, M)$ form a projective system with respect to the corestriction maps.

PROPOSITION (1.1.5). *Let Γ be a discrete group, $\mathfrak{C}$ a full class of finite groups, and G the pro-$\mathfrak{C}$ completion of Γ. Then the following conditions (1) and (2) are equivalent:*
(1) Γ is $\mathfrak{C}$-good;
(2) $\varinjlim_{\Pi \in \mathcal{S}(\Gamma, \mathfrak{C})} H^q(\Pi, M) = 0$ for every (constant) $M \in \mathfrak{C}(G)$ and $q \ge 1$.
If furthermore Γ is of type FP, then the above conditions are also equivalent to
(3) $\varprojlim_{\Pi \in \mathcal{S}(\Gamma, \mathfrak{C})} H_q(\Pi, M) = 0$ for every (constant) $M \in \mathfrak{C}(G)$ and $q \ge 1$.

PROOF. Observe first that, in (2) and (3), the limitation of $M \in \mathfrak{C}(G)$ running only over constant coefficients does not alter the conditions, because every $M \in \mathfrak{C}(G)$ becomes constant for sufficiently small $\Pi \in \mathcal{S}(\Gamma, \mathfrak{C})$.

The equivalence (1)⇔(2) is derived from [39] I-15/16. (2)⇒(1): We shall prove $i_q : H^q(G, M) \xrightarrow{\sim} H^q(\Gamma, M)$ $(M \in \mathfrak{C}(G))$ by induction on $q \ge 1$. If $q = 1$, we are reduced to the case of M being constant, by the Hochschild-Serre spectral sequence (5-exact sequence). Then the desired isomorphism is just $Hom(G, M) \cong Hom(\Gamma, M)$. So let $q \ge 2$. For each $\Pi \in \mathcal{N}(\Gamma, \mathfrak{C})$, the Γ-module M' coinduced from the Π-module M belongs also to $\mathfrak{C}(G)$, as $\mathfrak{C}$ is a full class. The canonical embedding $M \hookrightarrow M'$ yields the commutative diagram of two long exact sequences

$$\begin{array}{ccccccc}
H^{q-1}(G, M') & \xrightarrow{\hat{f}_\Pi} & H^{q-1}(G, M'/M) & \longrightarrow & H^q(G, M) & \xrightarrow{res} & H^q(\hat{\Pi}', M) \\
\downarrow \wr & & \downarrow \wr & & \downarrow i_q & & \downarrow \\
H^{q-1}(\Gamma, M') & \xrightarrow{f_\Pi} & H^{q-1}(\Gamma, M'/M) & \longrightarrow & H^q(\Gamma, M) & \xrightarrow{res} & H^q(\Pi', M)
\end{array}$$

in which by induction hypothesis the left two vertical arrows are isomorphisms. When Π varies in $\mathcal{N}(\Gamma, \mathfrak{C})$, the cokernels of $\hat{f}_\Pi$ cover the whole

$H^q(G, M)$ so that the injectivity of i_q follows. The assumption (2) implies that the cokernels of f_Π ($\Pi \in \mathcal{N}(\Gamma, \mathfrak{C})$) cover $H^q(\Gamma, M)$, from which we conclude the surjectivity of i_q. (1)$\Rightarrow$(2): Suppose Γ is $\mathfrak{C}$-good. Then by Shapiro's lemma, every $\Pi \in \mathcal{S}(\Gamma, \mathfrak{C})$ is also $\mathfrak{C}$-good. To prove (2), it suffices to show that for any $\Pi \in \mathcal{S}(\Gamma, \mathfrak{C})$ and $x \in H^q(\Pi, M)$ ($q \geq 1, M \in \mathfrak{C}(G)$), there exists $\Pi' \in \mathcal{S}(\Gamma, \mathfrak{C})$ such that the image of x by the restriction map $res^{\Pi}_{\Pi'} : H^q(\Pi, M) \to H^q(\Pi', M)$ is 0. By assumption, x is represented by a continuous (i.e. locally constant) q-cochain $\xi : \hat{\Pi}^q \to M$. So we find an open subgroup U of $\hat{\Pi}(\mathfrak{C})$ with $\xi|U^q = 0$. If we take $\Pi' \in \mathcal{S}(\Pi, \mathfrak{C})$ with $\hat{\Pi}' = U$, then we have a commutative diagram

$$\begin{array}{ccc} H^q(\hat{\Pi}, M) & \longrightarrow & H^q(\Pi, M) \\ {\scriptstyle res}\downarrow & & \downarrow{\scriptstyle res} \\ H^q(\hat{\Pi}', M) & \longrightarrow & H^q(\Pi', M), \end{array}$$

which shows $res^{\Pi}_{\Pi'}(x) = 0$. We next prove (2) $\Leftrightarrow$ (3) under the assumption that Γ is of type FP with M being constant in $\mathfrak{C}(G)$. Since a finite index subgroup of a FP group is also of type FP, $H_q(\Pi, M)$ is finite for every $q \geq 0$ and $\Pi \in \mathcal{S}(\Gamma, \mathfrak{C})$. Therefore the condition (2) (resp. (3)) is equivalent to the assertion that for each $\Pi \in \mathcal{S}$ there exists $\Pi' \in \mathcal{S}$ such that the restriction map $res^{\Pi}_{\Pi'} : H^q(\Pi, M) \to H^q(\Pi', M)$ (resp. the corestriction map $cor^{\Pi'}_{\Pi} : H_q(\Pi', M) \to H_q(\Pi, M)$) is 0-mapping. By the universal coefficient theorem, we have two exact sequences

(1) $0 \to Ext^1_{\mathbb{Z}}(H_{q-1}(\Pi, \mathbb{Z}), M) \to H^q(\Pi, M) \to Hom(H_q(\Pi, \mathbb{Z}), M) \to 0,$

(2) $0 \to H_q(\Pi, \mathbb{Z}) \otimes M \to H_q(\Pi, M) \to Tor^{\mathbb{Z}}_1(H_{q-1}(\Pi, \mathbb{Z}), M) \to 0,$

together with two isomorphisms

(3) $Hom(H_q(\Pi, \mathbb{Z}), M^*) \cong H_q(\Pi, \mathbb{Z}) \otimes M^*$ ([7] Chap.II, §5)),

(4) $Tor^{\mathbb{Z}}_1(M^*, H_{q-1}(\Pi, \mathbb{Z})) \cong Ext^1_{\mathbb{Z}}(H_{q-1}(\Pi, \mathbb{Z}), M)^*$ ([7] Chap.VI, §5),

where X^* denotes $Hom(X, \mathbb{Q}/\mathbb{Z})$ for any module X. (We use finite generation of $H_{q-1}(\Pi, \mathbb{Z})$ to get (4).) As (1)-(4) are functorial in Π, and as $M^* \cong M$ for finite M, we see that $res^{\Pi}_{\Pi'} = 0$ if and only if $cor^{\Pi'}_{\Pi} = 0$ for any pair (Π, Π') of $\mathcal{S}(\Gamma, \mathfrak{C})$ with $\Pi \supset \Pi'$. This completes the proof. □

1.2. Extension properties

Let $\mathfrak{C}$ be a full class of finite groups. In this subsection, we review some standard facts about extension properties of the pro-$\mathfrak{C}$ completion functor $^\wedge(\mathfrak{C})$ known by Serre [41], Friedlander [11] and Anderson [1].

Let $(\Gamma) : 1 \to \Pi \to \Gamma \to \Sigma \to 1$ be an exact sequence of discrete groups. In general, it is easy to see that the functor $^\wedge(\mathfrak{C})$ is right exact so that $\hat{\Pi}(\mathfrak{C}) \to \hat{\Gamma}(\mathfrak{C}) \to \hat{\Sigma}(\mathfrak{C}) \to 1$ is exact. For the injectivity of $\hat{\Pi}(\mathfrak{C}) \to \hat{\Gamma}(\mathfrak{C})$, it is necessary and sufficient that for each $N \in \mathcal{N}(\Pi, \mathfrak{C})$ there exists $\Gamma' \in \mathcal{N}(\Gamma, \mathfrak{C})$ such that $\Gamma' \cap \Pi \subset N$. If this is the case, the following weaker condition holds:

(1.2.1) For each $N \in \mathcal{N}(\Pi, \mathfrak{C})$ with $N \lhd \Gamma$, the canonical map by conjugation

$$\Gamma \to Aut(\Pi/N)$$

has image belonging to $\mathfrak{C}$.

Definition (1.2.2). We say a group extension (Γ) is $\mathfrak{C}$-*admissible* if it satisfies the condition (1.2.1).

(1.2.3) If $\mathfrak{C} = \mathfrak{C}_{fin}$, i.e., $\mathfrak{C}$ is the class of all finite groups, then the condition (1.2.1) is obviously empty. In the case $\mathfrak{C} = \mathfrak{C}_l := \{\text{all finite } l \text{ groups}\}$ for a prime l, we have a simple criterion to satisfy (1.2.1) as follows. By a well known theorem of P.Hall, the group of automorphisms of a finite l-group G which act trivially on the quotient $G/[G,G]G^l$ form a l-group. So if Σ acts on $\Pi/[\Pi,\Pi]\Pi^l$ trivially by conjugation, then (1.2.1) holds for $\mathfrak{C} = \mathfrak{C}_l$. Convenient criteria for other classes $\mathfrak{C}$ do not seem to be known.

Proposition (1.2.4). *Let* $(\Gamma) : 1 \to \Pi \to \Gamma \to \Sigma \to 1$ *be a group extension with* Π *finitely generated, and suppose that* Σ *is* $\mathfrak{C}$*-good. Then the canonical map* $\hat{\Pi}(\mathfrak{C}) \to \hat{\Gamma}(\mathfrak{C})$ *is injective if and only if* (Γ) *is* $\mathfrak{C}$*-admissible.*

Proof. The 'only if ' part is already mentioned. We shall prove the 'if' part. For an arbitrary $N \in \mathcal{N}(\Pi, \mathfrak{C})$, it suffices to find $\Gamma' \in \mathcal{S}(\Gamma, \mathfrak{C})$ with $\Pi \cap \Gamma' \subset N$. As Π is finitely generated, $X = Hom(\Pi, \Pi/N)$ is a finite set. Replacing N by $\bigcap_{x \in X} ker(x)$, we may assume that N is normal in Γ. Let I be the kernel of the map $\Gamma \to Aut(\Pi/N)$ induced by conjugation. Then the $\mathfrak{C}$-admissibility insures $I \subset \mathcal{N}(\Gamma, \mathfrak{C})$. Moreover, if we put $M = (I \cap \Pi)/N$, $\Delta = I/I \cap \Pi$, then we see that $M \in \mathfrak{C}(\hat{\Delta}(\mathfrak{C}))$ by the conjugate action of

Δ on M. Since Σ is $\mathfrak{C}$-good, by the natural inclusion $\Delta \hookrightarrow \Sigma$, Δ is also $\mathfrak{C}$-good. Then by Proposition (1.1.5), $\varinjlim_{\Delta' \in \mathcal{N}(\Delta,\mathfrak{C})} H^2(\Delta', M) = 0$. As the extension class of

$$1 \longrightarrow M \longrightarrow I/N \xrightarrow{\ p\ } \Delta \longrightarrow 1$$

vanishes in $H^2(\Delta', M)$ for some $\Delta' \in \mathcal{N}(\Delta, \mathfrak{C})$, we obtain a complement $\Gamma'_0 \subset I/N$ with $p(\Gamma'_0) = \Delta'$. Take for Γ' the inverse image of Γ'_0 via the canonical projection $\Gamma \to \Gamma/N$. Then $\Gamma' \in \mathcal{N}(I, \mathfrak{C}) \subset \mathcal{S}(\Gamma, \mathfrak{C})$. Moreover, $\Gamma'_0 \cap M = 0$ leads to $\Gamma' \cap \Pi = N$ as desired. $\square$

(1.2.5) Let $1 \to \Pi \to \Gamma \to \Sigma \to 1$ be an extension of discrete groups, and suppose that the pro-$\mathfrak{C}$ completion functor $^\wedge$ yields an exact sequence

$$1 \to \hat{\Pi} \to \hat{\Gamma} \to \hat{\Sigma} \to 1,$$

and that Π, Σ are $\mathfrak{C}$-good with Π being of type FP. Then Γ is also $\mathfrak{C}$-good.

Proof. Let $M \in \mathfrak{C}(\hat{\Gamma})$. The FP-ness of Π insures the finiteness of $H^q(\Pi, M)$. Then, from the standard cochains description, we see $H^q(\Pi, M) \in \mathfrak{C}$. Therefore, the $\mathfrak{C}$-goodness of Π and Σ implies that there are natural isomorphisms between E_2-terms of the Hochschild-Serre spectral sequences

$$H^p(\hat{\Sigma}, H^q(\hat{\Pi}, M)) \cong H^p(\Sigma, H^q(\Pi, M)).$$

From this we obtain $H^{p+q}(\hat{\Gamma}, M) \cong H^{p+q}(\Gamma, M)$ at E_∞. $\square$

1.3. Center-triviality of pro-$\mathfrak{C}$ groups

Let k be a commutative ring with unit, G a group, and kG the group algebra of G over k. The (discrete) Hattori-Stallings space (cf.[43]) is by definition the quotient module of kG by the k-submodule generated by $x-y$ (x, y: conjugate in G). Let $T : kG \to T(kG)$ denote the canonical projection. Each element of $T(kG)$ can be identified with a k-valued function r on the set of conjugacy classes of G, ${}^cG$, which we write as $\sum_{\tau \in {}^cG} r(\tau)\tau$. We have

$$T(\sum_g a_g \cdot g) = \sum_{\tau \in {}^cG} (\sum_{g \in \tau} a_g)\tau.$$

It is easy to see that for $\alpha_1, \alpha_2 \in kG$, $T(\alpha_1 + \alpha_2) = T(\alpha_1) + T(\alpha_2)$ and $T(\alpha_1\alpha_2) = T(\alpha_2\alpha_1)$.

Given a pair of $(f, \bar{f})$ of a group homomorphism $f : G \to G'$ and a ring homomorphism $\bar{f} : k \to k'$, we have a commutative diagram:

$$\begin{array}{ccc} kG & \xrightarrow{\varphi} & k'G' \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle T} \\ T(kG) & \xrightarrow[T\varphi]{} & T(k'G') \end{array}$$

where φ and $T\varphi$ are defined by

$$\varphi(\sum_{g\in G} a_g g) = \sum_{g\in G} \bar{f}(a_g)f(g),$$
$$T\varphi(\sum_{\tau\in^c G} r(\tau)\tau) = \sum_{\tau'\in^c G'} (\sum_{\substack{\tau\in^c G \\ f(\tau)\subset\tau'}} \bar{f}(r(\tau)))\tau'.$$

Let G be a profinite group, and p a rational prime number. Recall that the completed group algebra $\mathbb{Z}_p[[G]]$ is defined to be the limit of the projective system $\{A_{n,N} := (\mathbb{Z}/p^n\mathbb{Z})[G/N]\}$ indexed by the pairs (n, N) of positive integers n and open normal subgroups N of G, with morphisms $\varphi^{(n,N)}_{(m,M)} : A_{n,N} \to A_{m,M}$ for $n \geq m$, $N \subset M$ induced from the canonical projections $f : G/N \to G/M$ and $\bar{f} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ as in the previous paragraph. For each level $A_{n,N}$ of this projective system, we can associate a canonical surjection to its Hattori-Stallings space: $T_{n,N} : A_{n,N} \to T(A_{n,N})$ to get the commutative diagram

$$\begin{array}{ccc} A_{n,N} & \xrightarrow{\varphi} & A_{m,M} \\ {\scriptstyle T_{n,N}}\downarrow & & \downarrow{\scriptstyle T_{m,M}} \\ T(A_{n,N}) & \xrightarrow{T\varphi} & T(A_{m,M}) \end{array}$$

whenever $n \geq m$, $N \subset M$. Thus we define the profinite Hattori-Stallings space of G with respect to p by

$$T(\mathbb{Z}_p[[G]]) := \varprojlim_{n,N} T(A_{n,N}),$$

together with a canonical projection $T : \mathbb{Z}_p[[G]] \to T(\mathbb{Z}_p[[G]])$ in the obvious manner. The properties $T(\lambda + \mu) = T(\lambda) + T(\mu)$, $T(\lambda\mu) = T(\mu\lambda)$ for $\lambda, \mu \in \mathbb{Z}_p[[G]]$ are obviously inherited from those of the discrete level.

The set ${}^cG$ of the conjugacy classes of G has canonically a structure of a profinite space, as ${}^cG = \varprojlim_N {}^c(G/N)$, where N runs over the open normal subgroups of G.

In general, a $\mathbb{Z}_p$-valued measure on a profinite set X is by definition a rule λ which associates with each compact open subset U of X a p-adic integer $\lambda(U)$ such that $\lambda(U \cup U') = \lambda(U) + \lambda(U')$ whenever $U \cap U' = \emptyset$. Each element $x \in X$ defines a Dirac measure δ_x on X which takes 1 for open compact $U \ni x$ of X, and 0 otherwise.

Since each element of $A_{n,N}$ (resp. $T(A_{n,N})$) is considered to be a $(\mathbb{Z}/p^n\mathbb{Z})$-valued function on G/N (resp.${}^c(G/N)$), the elements of $\mathbb{Z}_p[[G]]$ (resp. $T(\mathbb{Z}_p[[G]])$) are interpreted as the $\mathbb{Z}_p$-valued measures on G (resp. ${}^cG$). (See e.g. [28].) The projection $T : \mathbb{Z}_p[[G]] \to T(\mathbb{Z}_p[[G]])$ then in the usual sense sends a $\mathbb{Z}_p$-valued measure on G to a $\mathbb{Z}_p$-valued measure on ${}^cG$ with respect to the canonical map $G \to {}^cG$ of profinite sets.

Definition (1.3.1). Let F be a finitely generated free $\mathbb{Z}_p[[G]]$-module with basis $x_1, \ldots, x_r$ and let $f : M \to M$ be a $\mathbb{Z}_p[[G]]$-linear endomorphism. We define the Hattori-Stallings trace $tr(f) \in T(\mathbb{Z}_p[[G]])$ of f to be the sum $\sum_{i=1}^r T(a_{ii})$, where $a_{ij} \in \mathbb{Z}_p[[G]]$ $(1 \le i, j \le r)$ are defined by $f(x_i) = \sum_{i=1}^r a_{ij}x_j$.

In the definition, it is easy to see that $tr(f)$ does not depend on the choice of the basis $x_1, \ldots, x_r$ of F, and that for two $\mathbb{Z}_p[[G]]$-endomorphisms f, g, we have $tr(f + g) = tr(f) + tr(g)$, $tr(fg) = tr(gf)$.

Theorem (1.3.2). *Let G be a profinite group, and p be a prime number. Suppose that the trivial $\mathbb{Z}_p[[G]]$-module $\mathbb{Z}_p$ has a finite free resolution*

$$(F): \quad 0 \to F_n \to \cdots \to F_1 \to F_0 \to \mathbb{Z}_p \to 0,$$

where F_i $(1 \le i \le n)$ are finitely generated free $\mathbb{Z}_p[[G]]$-modules, with Euler characteristic $\chi := \sum(-1)^i rank(F_i) \ne 0$. Then G has trivial center.

Proof. We follow the argument of Stallings [43] in our profinite context. Suppose that we have a nontrivial central element γ in G, and consider two $\mathbb{Z}_p[[G]]$-endomorphisms $(f_i), (g_i)$ of the complex (F) such that

f_i =identity and g_i = multiplication by γ on F_i for every $0 \leq i \leq n$. By standard argument in homology theory, we can construct a chain homotopy $d_i : F_i \to F_{i+1}$ with $f_i - g_i = \partial_{i+1} d_i + d_{i-1}\partial_i$ $(0 \leq i \leq n)$. Here $\partial_i : F_i \to F_{i-1}$ $(i \geq 1)$ denotes the boundary map of (F), and ∂_0 and d_{-1} are understood to be 0. Then

$$\begin{aligned}\sum(-1)^i tr(f_i) - \sum(-1)^i tr(g_i) &= \sum(-1)^i\{tr(\partial_{i+1}d_i) + tr(d_{i-1}\partial_i)\}\\ &= \sum(-1)^i\{tr(\partial_{i+1}d_i) - tr(d_i\partial_{i+1})\}\\ &= 0.\end{aligned}$$

On the other hand, by the definition of trace, we have

$$tr(f_i) = rank(F_i)\delta_1, \quad tr(g_i) = rank(F_i)\delta_\gamma,$$

where δ_1 (resp. δ_γ) is the Dirac measure supported at the conjugacy class $\{1\}$ (resp. $\{\gamma\}$). Thus

$$\chi(\delta_1 - \delta_\gamma) = 0$$

in $T(\mathbb{Z}_p[[G]])$. But since $\delta_1 \neq \delta_\gamma$, for ${}^cG$ is a Hausdorff space, we get $\chi = 0$. This contradicts our assumption. □

In the remainder of this subsection, $\mathfrak{C}$ denotes a full class of finite groups.

COROLLARY (1.3.3) (The profinite Gottlieb theorem). *If Γ is a $\mathfrak{C}$-good group of type FL with Euler characteristic $\neq 0$, then the pro-$\mathfrak{C}$ completion $\hat{\Gamma}$ has trivial center.*

PROOF. By assumption, there is a finite free resolution

$$(F.): \quad 0 \to F_n \to \cdots \to F_1 \to F_0 \to 0, \quad H_0(F.) \cong \mathbb{Z},$$

such that $F_i \cong \mathbb{Z}[\Gamma]^{\oplus r_i}$ with $\sum_i(-1)^i r_i \neq 0$. Fix a prime $p \in |\mathfrak{C}|$, and define for each pair of $m \geq 1$ and $\Pi \in \mathcal{N}(\Gamma, \mathfrak{C})$,

$$\begin{aligned}F_i(m,\Pi) :&= (\mathbb{Z}/p^m\mathbb{Z})[\Gamma/\Pi] \otimes_{\mathbb{Z}[\Gamma]} F_i \quad (1 \leq i \leq n)\\ &(= (\mathbb{Z}/p^m\mathbb{Z}) \otimes_{\mathbb{Z}[\Pi]} F_i)\end{aligned}$$

Then $\hat{F}_i := \varprojlim_{(m,\Pi)} F_i(m,\Pi) \cong \mathbb{Z}_p[[\hat{\Gamma}]]^{\oplus r_i}$. Since, for each i, the projective system $\{H_i(F.(m,\Pi))\}_{(m,\Pi)}$ satisfies the Mittag-Leffler condition,

$$H_i(\varprojlim F.(m,\Pi)) = \varprojlim H_i(F.(m,\Pi)) = \varprojlim H_i(\Pi, \mathbb{Z}/p^m\mathbb{Z}).$$

The $\mathfrak{C}$-goodness of Γ assures that $H_i(\varprojlim F.(m,\Pi)) = 0$ for $i \geq 1$. For $i = 0$, we have $H_0(F.(m,\Pi)) = H_0(\Pi, \mathbb{Z}/p^m\mathbb{Z}) = \mathbb{Z}/p^m\mathbb{Z}$. Hence $H_0(\varprojlim F.(m,\Pi))$ $= \mathbb{Z}_p$. Thus we obtain the exact sequence

$$0 \to \hat{F}_n \to \cdots \to \hat{F}_1 \to \hat{F}_0 \to \mathbb{Z}_p \to 0$$

with $rank(\hat{F}_i) = rank(F_i)$ $(1 \leq i \leq n)$. We may apply Theorem (1.3.2) to get the conclusion. □

It is easy to see that a free group of finite rank r, F_r, is a $\mathfrak{C}$-good group of type FL. If Π_g denotes the surface group (i.e. the fundamental group of a compact Riemann surface) of genus g, then Π_g is also $\mathfrak{C}$-good of type FL. In fact, the FL-ness follows from the fact that $K(\Pi_g, 1)$ has a homotopy type of a finite simplicial complex. Since each $\Pi \in \mathcal{N}(\Pi_g, \mathfrak{C})$ is also a surface group, $H_2(\Pi, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$. If we take a normal subgroup Π' of Π such that $[\Pi : \Pi'] = n$, then the corestriction map $cor_{\Pi}^{\Pi'}$ is multiplication by n. This leads us to $\varprojlim_{\Pi} H_2(\Pi, \mathbb{Z}/n\mathbb{Z}) = 0$ for $\mathbb{Z}/n\mathbb{Z} \in \mathfrak{C}$. By (1.1.5), we conclude the $\mathfrak{C}$-goodness of Π_g.

Considering the Euler characteristics of F_r and Π_g, we obtain

Corollary (1.3.4) ([1], [25]). *The pro-$\mathfrak{C}$ completion of F_r $(r \geq 2)$ and Π_g $(g \geq 2)$ have trivial center.*

Note We can also apply Theorem (1.3.2) to get "the pro-p Gottlieb theorem" which implies the centerfreeness of pro-p groups with nonzero Euler characteristics. The key point of the application lies in the fact that $\mathbb{Z}_p[[G]]$ is a pseudocompact local ring for any pro-p group G in the sense of A.Brumer. We discuss this topic in a separate paper [33]. For a number theoretic application for pro-p Galois groups, see Yamagishi [48].

1.4. Two remarks on profinite groups

The following proposition is useful and can be found in [23] (with small typographical errors).

Proposition (1.4.1). *Let G be a profinite group, K a closed subgroup of G.*
(i) For any open subgroup M of K, there exists an open subgroup L of G such that $L \cap K = M$.
(ii) If K is normal in G, then for any open normal subgroup M of K, there exists an open normal subgroup L of G such that $L \cap K \subset M$.

Proof. (i): Let $\{N_\alpha\}_{\alpha \in A}$ be the system of open normal subgroups of G, and put $M_\alpha = MN_\alpha$. Then, as G is a Hausdorff topological space, it is easy to see that $M = \bigcap_{\alpha \in A} M_\alpha$. In particular, $M = \bigcap_{\alpha \in A}(M_\alpha \cap K)$. By assumption, $K \setminus M$ is compact. So we find a finite subset A_0 of A such that $M = \bigcap_{\alpha \in A_0}(M_\alpha \cap K) = \bigcap_{\alpha \in A_0} M_\alpha \cap K$. We may take $\bigcap_{\alpha \in A_0} M_\alpha$ for L.
(ii): By (i), we have an open subgroup L of G with $L \cap K = M$. Replace L by $\bigcap_{g \in G} gLg^{-1}$, we get the desired one. □

(1.4.2) *Notations* : For a profinite group G, $[G, G]$ (or G') denotes the closure of the commutator subgroup of G, and $G^{ab} = G/[G, G]$. If p is a prime number, Syl_pG means a p-Sylow subgroup of G. For a subset $\mathfrak{S}$ of G, we denote by $\langle \mathfrak{S} \rangle$ the smallest closed subgroup containing $\mathfrak{S}$. Moreover, $N_G(\mathfrak{S})$ (resp. $C_G(\mathfrak{S})$) denotes the normalizer of $\langle \mathfrak{S} \rangle$ (resp. centralizer of $\mathfrak{S}$) in G.

Remark. In the above notations, it is easy to see that $C_G(\mathfrak{S}) = C_G(\langle \mathfrak{S} \rangle)$. Moreover we can show that $C_G(\mathfrak{S})$ and $N_G(\mathfrak{S})$ are closed subgroups of G. (Use the compactness of $\langle \mathfrak{S} \rangle$ for the latter.)

Proposition (1.4.3). *Let $\mathfrak{C}$ be a full class of finite groups, and let $G = \hat{F}_r$ be the pro-$\mathfrak{C}$ completion of a free group of rank $r \geq 1$. Let $z \in G$ be an element such that there exist only finitely many primes p with $Syl_p\langle z \rangle \neq 1$. Then $[N_G(z) : C_G(z)] < \infty$.*

Proof. We may assume $z \neq 1$. Let P be the set of primes p with $Syl_p\langle z \rangle \neq 1$. As P is finite, we can take an open normal subgroup N of G, such that the image of $\langle z \rangle$ in G/N has a nontrivial p-Sylow subgroup for each $p \in P$. Let $U = N \cdot \langle z \rangle$. Then U is a free pro-$\mathfrak{C}$ group ([25](1.4)) and $\langle z \rangle$ is injectively mapped into U^{ab}. Any element $x \in U$ normalizing $\langle z \rangle$ centralizes $\langle z \rangle$. In fact, if we put $xzx^{-1} = z^a$ ($a \in \prod_{p \in P} \mathbb{Z}_p$), going to the abelianization of U, we get $a = 1$. Therefore the conjugate action of $N_G(z)$

on $\langle z \rangle$ factors through $N_G(z)/N_G(z) \cap U$ which is a finite group. $\square$

REMARK. In the case $\mathfrak{C} = \mathfrak{C}_l$ (l an odd prime), the group $N_G(z)/N_G(z) \cap U$ in the above proof is a finite l-group, therefore must be trivially mapped into $Aut\langle z \rangle \cong \mathbb{Z}_l^\times$. Thus, in this case, we have $N_G(z) = C_G(z)$.

1.5. Automorphisms of group extensions

(1.5.1) For a profinite group G, let $AutG$ denote the group of all the continuous group automorphisms of G. (We recall that a continuous bijection of a compact space onto a Hausdorff space is automatically bicontinuous.) If N is an open normal subgroup of G, then

$$A_N = \{f \in AutG \mid f(x)x^{-1} \in N \ (x \in G)\}$$

forms a subgroup of $AutG$. We can introduce a topology in $AutG$ by letting the family $\{A_N \mid N \lhd G \text{ open}\}$ be a fundamental system of neighborhoods of the identity. It is easy to see that $AutG$ is a totally disconnected Hausdorff topological group which is in general not compact.

We consider $AutG$ to be acting on G on the left. So, an inner automorphism by an element $g \in G$ is written as

$$inn(g) : x \to gxg^{-1} \qquad (x \in G).$$

The (normal closed) subgroup of inner automorphisms of G is denoted by $InnG$ which has a topology as a subgroup of $AutG$. If Z_G is the center of G, the canonical homomorphism $G/Z_G \to InnG$ gives a continuous bijection. By the above remark, this map is also bicontinuous. The outer automorphism group $OutG$ of G is defined as the quotient group of $AutG$ by $InnG$. For each $f \in AutG$, we denote by $\bar{f}$ the image of f in $OutG$.

(1.5.2) Let π be a profinite group, π_1 a closed normal subgroup of π, and $p : \pi \to G = \pi/\pi_1$ the projection. By the cross section theorem of profinite groups ([41] I, Prop.1), there is a continuous map $s : G \to \pi$ with $p \circ s = id$. (Here s is not necessarily a homomorphism.) If μ denotes a continuous map $G \times G \to \pi_1$ defined by

$$s(\sigma)s(\tau) = \mu(\sigma,\tau)s(\sigma\tau) \quad (\sigma,\tau \in G), \tag{1.5.2.1}$$

then it satisfies the property

$$\mu(\sigma,\tau)\mu(\sigma\tau,\rho)=s(\sigma)\mu(\tau,\rho)s(\sigma)^{-1}\mu(\sigma,\tau\rho)\quad(\sigma,\tau,\rho\in G). \tag{1.5.2.2}$$

Recall that we can recover the group π, if we are given π_1 and G together with the data s, μ.

(1.5.3) We have two basic representations of G which actually do not depend on the choice of s. The first one is in the center Z of π_1. The action of G on Z is given by

$$\sigma\cdot m=s(\sigma)ms(\sigma)^{-1}\qquad(\sigma\in G, m\in Z).$$

By this action, Z is a topological G-module, and the continuous cochain cohomology groups $H^*_{cont}(G,Z)$ are defined (Tate [44]).

The second one is an associated exterior representation

$$\varphi: G\to Out\pi_1,$$

where for each $\sigma\in G$, $\varphi(\sigma)$ is the class of the restriction of the inner automorphism by $s(\sigma)$ to π_1.

(1.5.4) Our first task in this subsection is to study the group $Aut(\pi,\pi_1)$ of all the continuous group automorphisms f of π with $f(\pi_1)=\pi_1$. Following Wells [47], we shall say a pair $(f_0,f_1)\in AutG\times Aut\pi_1$ is *compatible* if the following two conditions hold:
1) $f_0(ker(\varphi))=ker(\varphi)$;
2) $\bar{f}_1\varphi(\sigma)\bar{f}_1^{-1}=\varphi(f_0(\sigma))$ in $Out\pi_1$ $(\sigma\in G)$.
The compatible pairs naturally form a subgroup of $AutG\times Aut\pi_1$ which we denote by C.

A profinite version of Wells' exact sequence [47] is described as follows:

Lemma (1.5.5). *There is a canonical exact sequence*

$$0\to Z^1_{cont}(G,Z)\to Aut(\pi,\pi_1)\to C\to H^2_{cont}(G,Z).$$

The middle two maps are group homomorphisms, but the last map is in general not.

In the above lemma, $Z^1_{cont}(G,Z)$ is the group of the continuous 1-cochains $\gamma : G \to Z$ such that

$$(1.5.5.1) \qquad \gamma(\sigma\tau) = \gamma(\sigma)s(\sigma)\gamma(\tau)s(\sigma)^{-1} \quad (\sigma,\tau \in G).$$

The second cohomology group $H^2_{cont}(G,Z)$ is by definition the quotient group $Z^2_{cont}(G,Z)/B^2_{cont}(G,Z)$, where $Z^2_{cont}(G,Z)$ is a collection of the continuous 2-cochains $h : G \times G \to Z$ such that

$$(1.5.5.2) \qquad h(\sigma,\tau)h(\sigma\tau,\rho) = s(\sigma)h(\tau,\rho)s(\sigma)^{-1}h(\sigma,\tau\rho) \quad (\sigma,\tau,\rho \in G),$$

and $B^2_{cont}(G,Z)$ is a subgroup of $Z^2_{cont}(G,Z)$ consisting of the 2-cochains of the form

$$(1.5.5.3) \qquad h(\sigma,\tau) = s(\sigma)v(\tau)s(\sigma)^{-1}v(\sigma\tau)^{-1}v(\sigma) \quad (\sigma,\tau \in G).$$

for some continuous maps $v : G \to Z$.

The second map in (1.5.5) sends $\gamma \in Z^1_{cont}(G,Z)$ to an automorphism $f \in Aut(\pi,\pi_1)$ such that

$$(1.5.5.4) \qquad f(xs(\sigma)) = x\gamma(\sigma)s(\sigma) \quad (x \in \pi_1, \sigma \in G).$$

The exactness at $Z^1_{cont}(G,Z)$ is straightfoward from the definition.

The third map in (1.5.5) associates with $f \in Aut(\pi,\pi_1)$ a compatible pair (f_0,f_1) in $AutG \times Aut\pi_1$ in an obvious way. For any element $f \in Aut(\pi,\pi_1)$ with associated pair (f_0,f_1), define $\beta : G \to \pi_1$ by

$$(1.5.5.5) \qquad f(s(\sigma)) = \beta(\sigma)s(f_0(\sigma)).$$

Then we can deduce the following two formulae in which we understand $\sigma,\tau \in G, x \in \pi_1$:

(1.5.5.6)

$$\beta(\sigma\tau) = f_1(\mu(\sigma,\tau))^{-1}\beta(\sigma)s(f_0(\sigma))\beta(\tau)s(f_0(\sigma))^{-1}\mu(f_0(\sigma),f_0(\tau));$$

$$(1.5.5.7) \quad f_1(s(\sigma)xs(\sigma)^{-1}) = \beta(\sigma)s(f_0(\sigma))f_1(x)s(f_0(\sigma))^{-1}\beta(\sigma)^{-1}.$$

Conversely, if a pair $(f_0,f_1) \in AutG \times Aut\pi_1$ admits a map $\beta : G \to \pi_1$ with (1.5.5.6), (1.5.5.7), then (1.5.5.5) defines an automorphism $f \in Aut(\pi,\pi_1)$

corresponding to the pair. The exactness at $Aut(\pi, \pi_1)$ follows from this observation: if f_0 and f_1 are trivial, then $\gamma = \beta$ gives a desired 1-cocycle.

To define the fourth map, we need some argument. Let $(f_0, f_1) \in C$. The compatibility condition assures the existence of a unique continuous map $\delta : G \to Inn\pi_1$ for which the formula

$$f_1 \circ inn(s(\sigma)) = \delta(\sigma) \circ inn(s(f_0(\sigma))) \circ f_1$$

holds in $Aut\pi_1$ for every $\sigma \in G$. Lifting back δ by the cross section theorem, we obtain a continuous map $\gamma : G \to \pi_1$ satisfying (1.5.5.7) (with $\beta = \gamma$). Define at first a function $k : G \times G \to \pi_1$ by

(1.5.5.8)
$$\begin{aligned} k(\sigma, \tau) = \mu(f_0(\sigma), f_0(\tau))^{-1} s(f_0(\sigma)) \gamma(\tau)^{-1} \\ \cdot s(f_0(\sigma))^{-1} \gamma(\sigma)^{-1} f_1(\mu(\sigma, \tau)) \gamma(\sigma\tau) \end{aligned}$$

for $\sigma, \tau \in G$. Eliminating x from (1.5.5.7) by $y = s(f_0(\sigma)) f_1(x) s(f_0(\sigma))^{-1}$, and then replacing σ by $\sigma\tau$ there, we see that $k(\sigma, \tau)$ commutes with every $y \in \pi_1$, i.e., $k(\sigma, \tau) \in Z$ $(\sigma, \tau \in G)$. Moreover if we apply (1.5.2.2), (1.5.5.7), (1.5.5.8)×2, and (1.5.2.1) to the middle portion of $k(\sigma\tau, \rho) k(\sigma, \tau\rho)^{-1}$ in this order, and independently apply (1.5.2.2) to the last two factors of it, we obtain

$$k(\sigma\tau, \rho) k(\sigma, \tau\rho)^{-1} = k(\sigma, \tau)^{-1} s(f_0(\sigma)) k(\tau, \rho) s(f_0(\sigma))^{-1} \quad (\sigma, \tau, \rho \in G).$$

(We also use iteratedly the fact that $k(*, *)$ lies in the center of π_1.) From this together with (1.5.5.7), we see that $h : G \times G \to Z$ defined by

$$h(\sigma, \tau) = f_1^{-1}(k(\sigma, \tau)) \qquad (\sigma, \tau \in G)$$

satisfies the 2-cocycle condition (1.5.5.2). If we change the lift γ of δ into another one γ', then we obtain another 2-cocycle h' in the same way. The difference of these two 2-cocycles comes from a 2-coboundary as follows:

$$h(\sigma, \tau)^{-1} h'(\sigma, \tau) = s(\sigma) v(\tau) s(\sigma)^{-1} v(\sigma\tau)^{-1} v(\sigma) \quad (\sigma, \tau \in G),$$

where $v(\sigma) = f_1^{-1}(\gamma(\sigma)\gamma'(\sigma)^{-1})$ which lies in Z $(\sigma \in G)$. Therefore we can define the fourth map by letting the image of $(f_0, f_1) \in C$ be the class of h.

Finally, if $(f_0, f_1) \in C$ is mapped to a 2-coboundary (1.5.5.3), then the map $\beta : G \to \pi_1$ defined by

$$\beta(\sigma) = \gamma(\sigma) f_1(v(\sigma)) \quad (\sigma \in G)$$

satisfies (1.5.5.6). This produces an automorphism $f \in Aut(\pi, \pi_1)$ mapped to the (f_0, f_1). Thus the exactness at C follows and the proof of Lemma (1.5.5) is completed. □

(1.5.6) We proceed with the situation in (1.5.2)-(1.5.3). An automorphism $f \in Aut(\pi, \pi_1)$ is said to be G-compatible if the induced automorphism on G by f is identity. We denote the group of all the G-compatible automorphisms by $Aut_G \pi$. The inner automorphisms of π by the elements of π_1 form a subgroup of $Aut_G \pi$ (denoted also $Inn \pi_1$). We put

$$E_G(\pi) = Aut_G \pi / Inn \pi_1.$$

Let $Out_G(\pi_1)$ denote the centralizer of $\varphi(G)$ in $Out \pi_1$. Then it is easy to see that the restriction map $Aut_G \pi \to Aut \pi_1$ gives a canonical homomorphism

$$\mathcal{R} : E_G(\pi) \to Out_G(\pi_1).$$

As an application of Lemma (1.5.5), we obtain

Corollary (1.5.7). *Suppose that the center of π_1 is trivial. Then the above homomorphism $\mathcal{R} : E_G(\pi) \to Out_G(\pi_1)$ gives a group isomorphism.* □

1.6. Galois centralizers and outer automorphisms of π_1

(1.6.1) Let X be an absolutely irreducible algebraic variety defined over a number field k, and $\mathfrak{C}$ an almost full class of finite groups. As usual, we denote by $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ the maximal pro-$\mathfrak{C}$ quotient of the geometric fundamental group of X, and by $\pi_1^{\mathfrak{C}}(X)$ the unique quotient of $\pi_1(X)$ naturally fitting into the exact sequence

$$1 \to \pi_1^{\mathfrak{C}}(X_{\bar{k}}) \to \pi_1^{\mathfrak{C}}(X) \to G_k \to 1.$$

In this setting, we shall write $E_k^{\mathfrak{C}}(X)$ for $E_{G_k}(\pi_1^{\mathfrak{C}}(X))$ (1.5.6).

LEMMA (1.6.2). *The notations being as above, $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ is a characteristic subgroup of $\pi_1^{\mathfrak{C}}(X)$. If $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ has trivial center, then there is a canonical exact sequence of groups*

$$1 \to E_k^{\mathfrak{C}}(X) \to Out\pi_1^{\mathfrak{C}}(X) \to Out(G_k).$$

Moreover if X has a descent model X_0 over a subfield k_0 of k, then the image of the third map above contains a subgroup isomorphic to $Aut(k/k_0)$.

PROOF. It is known by [39] that $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ is always finitely generated. On the other hand, since k is hilbertian, every nontrivial normal closed subgroup of G_k is not finitely generated ([10] Theorem 15.10; [46]). Thus $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ is maximum among the finitely generated closed normal subgroups of $\pi_1^{\mathfrak{C}}(X)$; hence it is characteristic in $\pi_1^{\mathfrak{C}}(X)$.

Let $\pi = \pi_1^{\mathfrak{C}}(X)$, $\pi_1 = \pi_1^{\mathfrak{C}}(X_{\bar{k}})$ and $G = G_k$. By the above, $Aut(\pi) = Aut(\pi, \pi_1)$. Since G_k has trivial center, $Aut_G\pi \cap Inn\pi = Inn\pi_1$. Hence, we have a canonical embedding

$$E_G(\pi) = Aut_G\pi/Inn\pi_1 \hookrightarrow Aut\pi/Inn\pi (= Out\pi).$$

The cokernel of this embedding is isomorphic to

$$D := Aut\pi/Aut_G\pi \cdot Inn\pi.$$

Let us identify $Aut(\pi, \pi_1)$ with the group of compatible pairs in $AutG \times Aut\pi_1$ by Lemma (1.5.5), and consider the first projection p_G. Then $ker(p_G) = Aut_G\pi$, and $p_G(Inn\pi) = InnG$. Therefore D is embedded into $AutG/InnG = OutG$.

If X has a descent model X_0/k_0, then $\pi_1^{\mathfrak{C}}(X)$ is an open subgroup of $\pi_1^{\mathfrak{C}}(X_0)$. The inner automorphisms by elements of G_{k_0} is lifted to those by elements of $\pi_1^{\mathfrak{C}}(X_0)$. From this the last assertion follows. $\square$

By the Neukirch-Ikeda-Iwasawa-Uchida theorem [36], we know $OutG_k \cong Aut(k/\mathbb{Q})$ which is obviously a finite group. Therefore,

COROLLARY (1.6.3). *Under the assumption that $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ is centerfree, finiteness of $Out\pi_1^{\mathfrak{C}}(X)$ is equivalent with finiteness of $E_k^{\mathfrak{C}}(X)$.*

§2. Fundamental groups of algebraic curves

2.1. Weight characterization of inertia subgroups

Naively speaking, weight filtration in an l-adic cohomology group $H^*(X \otimes \bar{k}, \mathbb{Q}_l)$ gives a family of (linear) subspaces which are characterized by conditions on Frobenius eigenvalues. As introduced by Deligne [8], Oda-Kaneko [22] and other authors in Hodge theory, such weight filtration can also exist in the (Lie algebras of the) pronilpotent fundamental groups of algebraic varieties, in which filtered components form a system of subgroups (or Lie subalgebras).

In this subsection, we shall present an attempt to formulate another weight filtration in pro-$\mathfrak{C}$ fundamental groups of punctured smooth curves. This weight filtration characterizes the conjugacy union of the inertia subgroups in $\pi_1^{\mathfrak{C}}(X \otimes \bar{k})$ which is therefore not closed under the group operation of the ambient space. For this reason, we want to say our weight filtration is 'of nonlinear type', or if it deserves, 'of anabelian type'.

This type of weight filtration was firstly considered in the previous paper [30], and applied to show that the exterior Galois representations in the full profinite fundamental groups of punctured projective lines over fields finitely generated over the rationals determine the isomorphism classes of the lines themselves. We shall present the following exposition by adding some technical improvements to [30].

Let $\mathfrak{C}$ be a full class of finite groups, X a smooth noncomplete (absolutely irreducible) curve defined over a number field k, $X_{\bar{k}} = X \otimes \bar{k}$, and $\pi_1^{\mathfrak{C}}(X)$ the quotient of the etale fundamental group of X divided by the kernel of $\pi_1(X_{\bar{k}})$ into the maximal pro-$\mathfrak{C}$ quotient $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$. Then we have an exact sequence of profinite groups

$$1 \longrightarrow \pi_1^{\mathfrak{C}}(X_{\bar{k}}) \longrightarrow \pi_1^{\mathfrak{C}}(X) \xrightarrow{p_{X/k}} G_k \longrightarrow 1.$$

By the Grothendieck comparison theorem, $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ is isomorphic to the pro-$\mathfrak{C}$ completion of the discrete group

$$\Pi_{g,n} = \langle x_1, \ldots, x_{2g}, z_1, \ldots, z_n | [x_1, x_2] \cdots [x_{2g-1}, x_{2g}] z_1 \cdots z_n = 1 \rangle$$

where $[x, y] = xyx^{-1}y^{-1}$, g is the genus of the smooth compactification X^c of X with geometric complement $\{p_1, \ldots, p_n\}$ and each z_i generates an inertia subgroup over p_i $(1 \leq i \leq n)$. We shall assume $n \geq 1$, $2-2g-n<0$ so that $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ is a free pro-$\mathfrak{C}$ group of rank $2g+n-1$.

DEFINITION. Let z be a nontrivial element of $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$. A closed subgroup N of $\pi_1^{\mathfrak{C}}(X)$ is said to be a *cyclotomic normalizer* of z, if and only if the following conditions 1)-3) hold.
1) N normalizes $\langle z \rangle$.
2) $p_{X/k}(N)$ is open in G_k.
3) The conjugate action of N on $\langle z \rangle$ factors through $N/N \cap \pi_1^{\mathfrak{C}}(X_{\bar{k}})$ and the induced homomorphism

$$N/N \cap \pi_1^{\mathfrak{C}}(X_{\bar{k}})(\subset G_k) \to Aut\langle z \rangle$$

gives the cyclotomic character.

THEOREM (2.1.1) ('Nonlinear' weight filtration). *Let $\mathfrak{C}$ be a full class of finite groups. Then a nontrivial element z in $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ is contained in an inertia group if and only if z has a cyclotomic normalizer in $\pi_1^{\mathfrak{C}}(X)$.*

The 'only if' part of the above theorem follows from the classical branch cycle argument: We may assume that $\mathfrak{C} = \mathfrak{C}_{fin}$ and that each $p_i \in X^c \setminus X$ is a k-rational point $(1 \leq i \leq n)$. After replacing z by its conjugate if necessary, we may furthermore assume that $z \in \langle z_i \rangle$ for some $1 \leq i \leq n$. Let R be the completion of the local ring $\mathcal{O}_{X^c,p_i}$ with field of fractions F. The canonical morphism $Spec\, R \to X^c$ induces $Spec\, F \to X$ together with $\rho_i : G_F = \pi_1(F) \to \pi_1(X)$. By [40] II, Th.2, F is isomorphic to $k((T))$ with a uniformizing parameter T, and the embedding $k \hookrightarrow k((T))$ gives the exact sequence

$$1 \to I \to G_F \to G_k \to 1,$$

where I is the absolute Galois group of $K = \bar{k}((T))$. Since the algebraic closure of K is the union of the Kummer extensions $K_n = \bar{k}((T^{1/n}))$ of K ([40] IV Prop.8, Puiseax's theorem), the Kummer character

$$Gal(K_n/K) \ni \sigma \to \sigma(T^{1/n})/T^{1/n} \in \mu_n(\bar{k})$$

yields a canonical isomorphism $I \cong \varprojlim_n \mu_n(\bar{k})$. (Here μ_n denotes the group of n-th roots of unity.) From this, we can see that the conjugate action of

G_k on I is given by the cyclotomic character. As $\langle z_i \rangle$ is (conjugate to) the image of I by ρ_i, it suffices to take (a conjugate of) $\rho_i(G_F)$ for N.

Before going to the proof of the 'if' part, we shall prepare some lemmas, in which $\mathfrak{C}$ is assumed to be a full class of finite groups (1.1).

LEMMA (2.1.2). *Let $\hat{F}_n$ be a free pro-$\mathfrak{C}$ group with free generators $x_1, \dots, x_n$, and z an arbitrary element of $\langle x_1 \rangle \setminus \{1\}$. Then the centralizer of z is just $\langle x_1 \rangle$.*

This lemma follows as a special case of [16] Theorem B′, in the proof of which the Kurosh subgroup theorem in free pro-$\mathfrak{C}$ products by Binz-Neukirch-Wenzel was used as a main tool. Here, we shall give a different and direct proof due to Akio Tamagawa. The author would like to thank him for communicating this elegant proof and permitting us to share it here.

PROOF. Let y be in the centralizer of $\langle z \rangle$ in $\hat{F}_n$, and N an open normal subgroup of $\hat{F}_n$ with projection $\pi : \hat{F}_n \to G = \hat{F}_n/N$. It suffices to show that $\pi(y) \in \langle \pi(x_1) \rangle$ in G. Let us write z as x_1^{α} ($\alpha \in \mathbb{Z}_{\mathfrak{C}} = \prod_{p \in |\mathfrak{C}|} \mathbb{Z}_p$), and choose a prime p such that the p-component α_p of α is nontrivial. Then, we fix an embedding $G \hookrightarrow GL_r(\mathbb{Z}_p)$ for a sufficiently large $r \geq 1$ and consider the pro-$\mathfrak{C}$ group

$$G' = \{X = \begin{pmatrix} A & B \\ O & C \end{pmatrix} \in GL_{2r}(\mathbb{Z}_p) | A \in G, C \in \langle \pi(x_1) \rangle\}$$

together with the surjection $\lambda : G' \ni X \to A \in G$. Since $\hat{F}_n$ is free, it is possible to define a continuous homomorphism $\psi : \hat{F}_n \to G'$ by putting

$$\psi(x_1) = \begin{pmatrix} \pi(x_1) & \pi(x_1) \\ O & \pi(x_1) \end{pmatrix}, \quad \psi(x_i) = \begin{pmatrix} \pi(x_i) & O \\ O & 1_r \end{pmatrix} \quad (i \geq 2)$$

so that the lifting condition $\pi = \lambda \circ \psi$ holds. Then, letting g denote the cardinality of G, we have

$$\psi(z^g) = \psi(x_1^{g\alpha}) = \begin{pmatrix} 1_r & g\alpha_p 1_r \\ O & 1_r \end{pmatrix}.$$

If we put $\psi(y) = \begin{pmatrix} \pi(y) & B \\ O & C \end{pmatrix} \in G'$, then the commutativity of y and z^g gives $g\alpha_p C = g\alpha_p \pi(y)$. Therefore $\pi(y) = C \in \langle \pi(x_1) \rangle$ as desired. □

Corollary (2.1.3). *Notations being as in Lemma (2.1.2), there exist no abelian subgroups* $A \subset \hat{F}_n$ *such that* $A \cap \langle x_i \rangle \neq 1$, $A \cap \langle x_j \rangle \neq 1$ *for* $1 \leq i < j \leq n$. □

Lemma (2.1.4). *Let* G *be the pro-*$\mathfrak{C}$ *completion of the surface group*

$$\Pi_{g,n} = \langle x_1, \dots, x_{2g}, z_1, \dots, z_n | [x_1, x_2] \cdots [x_{2g-1}, x_{2g}] z_1 \cdots z_n = 1 \rangle$$

with $n \geq 1$, $2 - 2g - n < 0$, *and define closed subsets* $\mathfrak{Z}$, $\mathfrak{Z}_i$ $(1 \leq i \leq n)$ *by*

$$\mathfrak{Z} = \bigcup_{i=1}^{n} \mathfrak{Z}_i \quad \mathfrak{Z}_i = \{ g z_i^a g^{-1} | g \in G,\, a \in \mathbb{Z}_{\mathfrak{C}} \}.$$

Then the following two conditions on $z \in G$ *are equivalent.*
(1) $z \in \mathfrak{Z}$.
(2) For every prime l *in* $|\mathfrak{C}|$ *and for every open subgroup* H *containing* z,

$$z \in [H, H] H^l \langle \mathfrak{Z} \cap H \rangle.$$

Proof. It suffices to show that (2) implies (1). Let us first assume $n \geq 2$. Then $z_1, \dots, z_n$ can be members of a free generator system of the free pro-$\mathfrak{C}$ group G. Suppose $z \notin \mathfrak{Z}$. Then by Lemma (2.1.2), we see $\langle z \rangle \cap \mathfrak{Z} = \{1\}$. Let l be a prime with $\langle z \rangle \neq \langle z^l \rangle$ and B an open subgroup of G with $B \cap \langle z \rangle = \langle z^l \rangle$ (1.4.1). Since $\mathfrak{Z} \setminus B$ and $\langle z \rangle \setminus B$ are disjoint compact subsets in the Hausdorff space G, we can find an open normal subgroup $M (\subset B)$ of G such that $\mathfrak{Z} \setminus B$ and $\langle z \rangle \setminus B$ are disjoint still in the quotient G/M. This means in turn that $\mathfrak{Z} \cap M\langle z \rangle$ is contained in B. If H denotes $M\langle z \rangle$, then $H/M\langle z^l \rangle \cong \mathbb{Z}/l\mathbb{Z}$; hence $[H,H]H^l \subset M\langle z^l \rangle \subset B$. Thus we conclude $[H,H]H^l \langle \mathfrak{Z} \cap H \rangle \subset B \not\ni z$.

Next we consider the case $n = 1$. Let l be a prime in $|\mathfrak{C}|$. Then the open normal subgroup $N = [G,G]G^l \langle \mathfrak{Z} \rangle$ corresponds to the fundamental group of a certain unramified covering of degree l^{2g} over the Riemann surface with fundamental group $\Pi_{g,1}$. Therefore we may do the same argument as above after replacing G by N. □

Now we are in a position to give the proof of the 'if' part of Theorem (2.1.1). Let z be in $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$ with a cyclotomic normalizer N in $\pi_1^{\mathfrak{C}}(X)$, and let $\mathfrak{Z}$ be the total subset of the inertia subgroups in $\pi_1^{\mathfrak{C}}(X_{\bar{k}})$. If z is not contained in $\mathfrak{Z}$, then by Lemma (2.1.4), we have an open subgroup $H(\ni z)$ and a prime l in $|\mathfrak{C}|$ such that

$$(*) \qquad z \notin [H,H]H^l\langle \mathfrak{Z} \cap H \rangle.$$

Choose an open subgroup $H' \subset \pi_1^{\mathfrak{C}}(X)$ with $H' \cap \pi_1^{\mathfrak{C}}(X_{\bar{k}}) = H$, and let Y be the finite etale cover of X with $\pi_1^{\mathfrak{C}}(Y) \cong H'$. Since $p_{X/k}(H' \cap N)$ is open in G_k, there exists a finite extension K of k in $\bar{k}$ such that Y is defined over K with $p_{Y/K} : \pi_1^{\mathfrak{C}}(Y) \to G_K$ sending $N \cap \pi_1^{\mathfrak{C}}(Y)$ onto G_K. It is known that the target of the pro-l abelianization map

$$\pi^{ab} : \pi_1^{\mathfrak{C}}(Y_{\bar{k}})(= H) \to H_1^{et}(Y_{\bar{k}}, \mathbb{Z}_l)$$

has a G_K-module structure by conjugation with torsion free weight filtration in the ordinary sense:

$$\begin{aligned} W_{-1} &= H_1^{et}(Y_{\bar{K}}, \mathbb{Z}_l), \\ W_{-2} &= \pi^{ab}(\langle \mathfrak{Z} \cap H \rangle), \\ W_{-3} &= 0. \end{aligned}$$

Since the image of $\langle z \rangle$ in $H_1^{et}(Y_{\bar{K}}, \mathbb{Z}_l)$ is acted on by G_K via the cyclotomic character, z must lie in (W_{-2})-part. (By the Riemann-Weil hypothesis, the complex absolute value of a Frobenius image in W_{-1}/W_{-2} of an unramified prime $\mathfrak{p}$ of K must be the half square of the absolute norm of $\mathfrak{p}$.) This contradicts the condition (*).

2.2. Probraid calculus: genus 0 case

In this subsection, generalizing [31], we shall discuss the finiteness of $E_k^{(l)}(X)$ for hyperbolic lines X over number fields k. The main statement is Theorem(2.2.5).

(2.2.1) Let l be a prime, and $\hat{\Pi}_{0,n}$ the free pro-l group with free generators $x_1, \ldots, x_{n-1}$ ($n \geq 3$). Put $x_n = (x_1 \cdots x_{n-1})^{-1}$. The abelianization Λ of $\hat{\Pi}_{0,n}$ is a free $\mathbb{Z}_l$-module of rank $n-1$ generated by the images of x_i (denoted X_i) ($1 \leq i \leq n-1$). We define Λ_i ($1 \leq i \leq n-1$) to be the

$\mathbb{Z}_l$-submodule of Λ generated by $X_1, \ldots, \check{X}_i, \ldots, X_{n-1}$ (X_i: omitted), and $\Lambda^*_{n-1} \subset \Lambda_{n-1}$ by

$$\Lambda^*_{n-1} = \begin{cases} \langle X_1, \ldots, X_{n-3} \rangle, & \text{if } n \geq 4, \\ 0, & \text{if } n = 3. \end{cases}$$

(2.2.2) A continuous group automorphism f of $\hat{\Pi}_{0,n}$ is called *braid-like*, if there exist $a \in \mathbb{Z}_l^\times$ and $t_i \in \hat{\Pi}_{0,n}$ $(1 \leq i \leq n)$ such that $f(x_i) = t_i x_i^a t_i^{-1}$ $(1 \leq i \leq n)$. The constant $a \in \mathbb{Z}_l^\times$ is determined uniquely by f, hence is denoted by a_f. If we impose on t_i the condition $t_i \pmod{\hat{\Pi}'_{0,n}} \in \Lambda_i$ $(1 \leq i \leq n-1)$, then we see that t_i is also determined uniquely by f. (Use e.g. (2.1.2).) We will write such t_i as $t_i(f)$ for each $i \in \{1, \ldots, n-1\}$. The group of all the braid-like automorphisms is denoted by $Aut^\flat(\hat{\Pi}_{0,n})$. Further we put $Out^\flat(\hat{\Pi}_{0,n}) = Aut^\flat(\hat{\Pi}_{0,n})/Inn(\hat{\Pi}_{0,n})$. It is easy to see that for $f, g \in Aut^\flat(\hat{\Pi}_{0,n})$,

$$a_{fg} = a_f a_g, \tag{2.2.2.1}$$

$$t_i(fg) = f(t_i(g)) t_i(f) \quad (1 \leq i \leq n-1). \tag{2.2.2.2}$$

If a braid-like automorphism $f \in \hat{\Pi}_{0,n}$ satisfies further the condition $t_n(f) = 1$, $t_{n-1}(f) \pmod{\hat{\Pi}'_{0,n}} \in \Lambda^*_{n-1}$, then f is called a *normalized probraid*. The normalized probraids form a subgroup of $Aut^\flat(\hat{\Pi}_{0,n})$, which is denoted by $Brd(\hat{\Pi}_{0,n})$. The following proposition is easy to see.

PROPOSITION (2.2.3). *The group $Aut^\flat(\hat{\Pi}_{0,n})$ is a semidirect product of $Inn\hat{\Pi}_{0,n}$ with $Brd(\hat{\Pi}_{0,n})$. In particular, $Out^\flat(\hat{\Pi}_{0,n}) \cong Brd(\hat{\Pi}_{0,n})$.* □

Now we shall generalize Lemma 2 of [31]. Let $\hat{\Pi}_{0,n} = \Pi(1) \supset \Pi(2) \supset \cdots$ be the lower central series of $\hat{\Pi}_{0,n}$, and set

$$A[m] = \{f \in Aut^\flat(\hat{\Pi}_{0,n}) \mid a_f = 1,\, t_i(f) \in \Pi(m),\ 1 \leq i \leq n-1\}.$$

for each $m \geq 1$. The mapping $f \mapsto a_f$ gives a homomorphism $a : Aut^\flat(\hat{\Pi}_{0,n}) \to \mathbb{Z}_l^\times$ with kernel $A[1]$.

LEMMA (2.2.4). *Let G be a subgroup of $Aut^\flat(\hat{\Pi}_{0,n})$ and assume that there exist an integer $m (\geq 1)$ and elements $g, h \in G$ such that*

1) $a_g \in \mathbb{Z}_l^\times$ is nontorsion;
2) $h \in A[m] \setminus A[m+1]$.
Then the centralizer of G in $Aut^\flat(\hat{\Pi}_{0,n})$ is injectively mapped into the torsion subgroup of $\mathbb{Z}_l^\times$ via a.

Proof. Let f be an element of $Aut^\flat(\hat{\Pi}_{0,n})$ centralizing G. By using (2.2.2.2), we compute

$$t_i(fhf^{-1}) = fhf^{-1}(t_i(f)^{-1}) \cdot f(t_i(h)) \cdot t_i(f) \quad (1 \leq i \leq n-1).$$

Since the image of $t_i(h)$ in $\hat{\Pi}_{0,n}/\Pi(m+1)$ is central, and since h therefore acts trivially on $\hat{\Pi}_{0,n}/\Pi(m+1)$, we obtain

$$t_i(fhf^{-1}) \equiv f(t_i(h)) \bmod \Pi(m+1) \quad (1 \leq i \leq n-1).$$

Moreover, since f acts on $\Pi(m)/\Pi(m+1)$ by multiplication by a_f^m, it follows that

$$t_i(fhf^{-1}) \equiv a_f^m t_i(h) \bmod \Pi(m+1).$$

By assumption, there exists at least one $i \in \{1, \dots n-1\}$ such that $t_i(h) \notin \Pi(m+1)$. Therefore we get $a_f^m = 1$. It remains to show that $f = 1$ under the assumption $f \in A[1]$. Suppose that there exists $N \geq 1$ with $f \in A[N] \setminus A[N+1]$. Then by the similar argument as above, we see

$$t_i(gfg^{-1}) \equiv a_g^N t_i(f) \bmod \Pi(N+1) \quad (1 \leq i \leq n-1).$$

Since f commutes with g, and since there exists $1 \leq i \leq n-1$ with $t_i(f) \notin \Pi(N+1)$ by assumption, we get $a_g^N = 1$; contradiction. Thus $f \in \bigcap_{N \geq 1} A[N] = \{1\}$. This completes the proof of Lemma (2.2.4). $\square$

Theorem (2.2.5). *Let $n \geq 3$, X an n-point punctured projective line defined over a number field k, and l an odd prime. If $\pi_1(X_{\bar{k}})^{pro-l}$ denotes the maximal pro-l quotient of $\pi_1(X_{\bar{k}})$, then the centralizer of the image of the canonical Galois representation*

$$\varphi_X : G_k \to Out\pi_1(X_{\bar{k}})^{pro-l},$$

or equivalently $E_k^{(l)}(X)$ by (1.5.7), is a finite group isomorphic to a subgroup of S_n. In particular, $Out\pi_1^{(l)}(X)$ is finite.

Proof. Let us identify $\pi_1(X_{\bar{k}})^{pro-l}$ with $\hat{\Pi}_{0,n}$ so that x_i generates an inertia subgroup of the former group ($1 \leq i \leq n$). By Corollary (1.5.7), $Out_{G_k}\hat{\Pi}_{0,n}$ is isormophic to $E_k^{(l)}(X)$. Then, it follows from the nonlinear weight filtraition (2.1.1), that each G_k-compatible automorphism of $\pi_1^{(l)}(X)$ permutes the conjugacy unions of the inertia subgroups over the deleted points on $\mathbf{P}^1$. Thus we have a canonical map $E_k^{(l)}(X) \to S_n$. The kernel E_1 of this map is contained in $Out^\flat(\hat{\Pi}_{0,n}) \cong Brd(\hat{\Pi}_{0,n})$ (2.2.3). It remains to show that $E_1 = \{1\}$. Let $\phi_n : G_k \to Brd(\hat{\Pi}_{0,n})$ be the unique lift of φ_X, and consider the canonical map $p : Brd(\hat{\Pi}_{0,n}) \to Brd(\hat{\Pi}_{0,3})$ obtained by setting $x_1 = \cdots = x_{n-3} = 1$. Let f be an arbitrary element of $E_1 \subset Brd(\hat{\Pi}_{0,n})$. Then, since $p(f)$ commutes with $\phi_3(G_k)$, we obtain $1 = a_{p(f)} = a_f$ from [31]. In particular, we see $f \in A[1]$. On the other hand, since there is a nontrivial Galois image σ lying in $\phi_3(G_k)$ with $a_\sigma = 1$ ([31] §4), there exists also an element $h \in \phi_n(G_k)$ which satisfies the condition 2) of (2.2.4) for some $m \geq 1$. Thus we can apply Lemma (2.2.4) for $G = \phi_n(G_k)$ to conclude $f = 1$. The last statement follows from (1.6.3) and the proof of Theorem (2.2.5) is completed. □

2.3. Curves with special stable reductions and Jacobians

Let k be a number field with absolute Galois group G_k, C a complete nonsingular (absolutely irreducible) curve of genus $g \geq 2$ defined over k. For a prime l, we denote the maximal pro-l quotient of the geometric fundamental group of C simply by π_1. Let $\varphi : G_k \to Out\pi_1$ be the canonical exterior representation.

In this subsection, we shall show the following theorem (2.3.1) which suggests that $E_k^{(l)}(C)$ should be finite for a wide class of hyperbolic curves C over number fields. In a crucial step of the proof, we make use of a recent result of Takayuki Oda [37].

Theorem (2.3.1). *Let J be the Jacobian variety of C, and suppose that*
(1) $End_k(J) \cong \mathbb{Z}$;
(2) there exists a prime $p(\nmid l)$ of k such that J has good reduction at p but

C has stable bad reduction at p.
Then the centralizer of the Galois image $\varphi(G_k)$ in $Out\pi_1$, or equivalently $E_k^{(l)}(C)$ by (1.5.7), is a finite group of order at most 2. In particular, $Out\pi_1^{(l)}(C)$ is finite (1.6.3).

Before going to the proof, we shall briefly review some results of Asada-Kaneko [4]. Let $\Gamma' = Aut\pi_1$, $\Gamma = Out\pi_1$, and let $\pi_1 = \pi_1(1) \supset \pi_1(2) \supset \dots$ denote the lower central series of π_1. We choose a standard generator system $x_1, ..., x_{2g}$ of π_1 with the defining relation $[x_1, x_2] \cdots [x_{2g-1}, x_{2g}] = 1$. For each i $(1 \leq i \leq 2g)$ and $f \in \Gamma'$, let $s_i(f) = f(x_i)x_i^{-1}$, and define the filtration of Γ' (resp. Γ) by

$$\Gamma'[m] = \{f \in \Gamma' \mid s_i(f) \in \pi_1(m+1);\ 1 \leq i \leq 2g\}$$
$$(\text{ resp. } \quad \Gamma[m] = \Gamma'[m] \cdot Inn\pi_1 / Inn\pi_1)$$

for $m \geq 1$. It is shown that $\Gamma[m] = \Gamma'[m]/Inn\pi_1(m)$. So the homomorphism

$$(2.3.2) \quad i'_m : \Gamma'[m] \to (gr_{m+1}\pi_1)^{\oplus 2g}, \quad f \mapsto (s_i(f) \bmod \pi_1(m+2))_{1 \leq i \leq 2g}$$

induces a canonical injection

$$(2.3.3.) \qquad i_m : gr_m\Gamma \to (gr_{m+1}\pi_1)^{\oplus 2g}/H_m$$

for $m \geq 1$, where H_m is the image of $Inn\pi_1(m)$ by i'_m. As the target space of i_m is shown to have no torsion, $gr_m\Gamma$ turns out to be a torsion free $\mathbb{Z}_l$-module [3]. Every element of Γ' acts canonically on $\pi_1/\pi_1(2)$ so that we have a surjective homomorphism $\lambda : \Gamma \to GSp(2g, \mathbb{Z}_l)$. Letting X_i denote the image of x_i in $\pi_1/\pi_1(2)$, we define the matrix $(\lambda_{ij}(f))_{1 \leq i,j \leq 2g}$ for $f \in \Gamma$ by $\lambda(f)(X_j) = \sum_i \lambda_{ij}(f)X_i$. We have a $GSp(2g, \mathbb{Z}_l)$-bimodule structure on $(gr_{m+1}\pi_1)^{\oplus 2g}$ as follows. The left action of $\lambda \in GSp(2g)$ is the diagonal one: λ acts componentwise on $gr_{m+1}\pi_1$ in a canonical way. The right action of $\lambda = (\lambda_{ij}) \in GSp(2g)$ on $(s_i) \in (gr_{m+1}\pi_1)^{\oplus 2g}$ is defined by

$$(2.3.4) \qquad (s_1, ..., s_{2g}) \cdot \lambda = (\sum_{u=1}^{2g} \lambda_{ui}s_u)_{1 \leq i \leq 2g}.$$

The action of the inner automorphism by $f \in \Gamma'$ on $gr_m\Gamma'$ is calculated in the module $(gr_{m+1}\pi_1)^{\oplus 2g}$ by the following fundamental formula of [4]:

$$(2.3.5)\quad (s_i(fhf^{-1}))_{1\le i\le 2g} = \lambda(f)\cdot(s_1(h),\dots,s_{2g}(h))\cdot\lambda(f^{-1}),\quad h\in\Gamma[m].$$

(Here we write the formula via left action of $Aut\pi_1$ on π_1. This formula was described in [4] in a slightly different style via right action of $Aut\pi_1$ on π_1.)

Proof of the Theorem. Let f be an arbitrary element of $\Gamma = Out\pi_1$ centralizing $\varphi(G_k)$. By the Tate conjecture proved by Faltings, we have

$$End_{G_k}T_l(J(\bar{k})) \cong End_k(J)\otimes\mathbb{Z}_l \cong \mathbb{Z}_l.$$

As the Tate module $T_l(J(\bar{k}))$ is canonically isomorphic to $\pi_1/\pi_1(2)$, we may assume that f acts on $\pi_1/\pi_1(2)$ via a_f-multiplication for some $a_f\in\mathbb{Z}_l^\times$.

Step 1. We first prove that $a_f = \pm 1$. Let $I_p\subset G_k$ be an inertia subgroup over p, and consider the restrction φ_p of $\varphi: G_k\to\Gamma$ to I_p. Then, by using the nonabelian Picard-Lefschetz formula, Takayuki Oda [37] proved under the condition (2) that φ_p has a nontrivial image δ in $\Gamma[2]\setminus\Gamma[3]$. Let $[\delta']\in(gr_3\pi_1)^{\oplus 2g}$ be the image of a lift δ' of δ in $\Gamma'[2]$ via (2.3.2), and apply the formula (2.3.5) to $h=\delta'$. Then, since δ commutes with f in Γ, we obtain $[\delta']\equiv a_f^3[\delta']a_f^{-1}$ mod H_m. As the map (2.3.3) is injective, we obtain $a_f^2=1$, i.e., $a_f=\pm 1$.

Step 2. Assume $a_f = 1$. We may prove $f=1$. If $f\neq 1$, there exists $m\ge 1$ such that $f\in\Gamma[m]\backslash\Gamma[m+1]$. Let $\sigma_p\in G_k$ represent a Frobenius class modulo I_p, and put $\phi_p=\varphi(\sigma_p)$. Then by the Riemann-Weil hypothesis, $\lambda(\phi_p)\in GSp(2g)$ has algebraic eigenvalues with complex absolute values $Np^{1/2}$ (Np is the absolute norm of p). From this and the formula (2.3.5), it follows that the inner automorphism by ϕ_p acts on $\Gamma[m]/\Gamma[m+1]\otimes\mathbb{Q}_l$ via the algebraic eigenvalues with complex absolute values $Np^{m/2}$. In particular, since $gr_m\Gamma$ is torsion free, no nontrivial elements of $gr_m\Gamma$ are fixed by the conjugate action of ϕ_p. This contradicts the commutativity of f and ϕ_p. □

Remarks. 1) The author does not assure yet how to construct algebraic curves satisfying (1),(2) of the above theorem explicitly. We just notice here that (1) is generic condition for algebraic curves over $\mathbb{C}$, and expect that (2) happens frequently around certain boundaries of the moduli space of curves.

2) Generalization of the theorem to the case of punctured curves will be studied in a joint work with H.Tsunogai. (See [35].)

§3. Galois-braid groups

3.1. Combinatorics in Galois-braid groups

(3.1.1) Let us begin our study of the case of the moduli variety $M_{0,n}$ introduced in §0 ($n \geq 3$). We assume that it is defined over a fixed number field k. Each point of $M_{0,n}$ ($n \geq 3$) corresponds to an isomorphism class of n-pointed projective lines $(\mathbf{P}^1; a_1, \ldots, a_n)$ where the a_i ($1 \leq i \leq n$) are distinct points on $\mathbf{P}^1$. As in [12], adding the points of isomorphism classes of "stable n-pointed P^1-trees", we obtain a smooth compactification B_n of $M_{0,n}$. The complement $B_n - M_{0,n}$ consists of several irreducible divisors, each of which reflects a type of stable n-pointed P^1-tree of two projective lines. The *special irreducible divisor* D_{ij} ($1 \leq i < j \leq n$) is one of them such that each point of a dense open subset of D_{ij} represents an isomorphism class of $(C; a_1, \ldots, a_n)$ in which:
1) C is the union of two projective lines normally crossing at one point a;
2) a_i and a_j are distinct points on one component of $C - \{a\}$;
3) all other a_r ($r \neq i, j$) are on another component of $C - \{a\}$ and distinct from each other.

We denote by Γ_0^n the (discrete) fundamental group of the analytic manifold $M_{0,n}(\mathbb{C})$. Fix a full class of finite groups $\mathfrak{C}$. The pro-$\mathfrak{C}$ completion $\hat{\Gamma}_0^n(\mathfrak{C})$ of Γ_0^n is isomorphic to the maximal pro-$\mathfrak{C}$ quotient of the geometric fundamental group $\pi_1(M_{0,n} \otimes \bar{k})$. If $\pi_1^{\mathfrak{C}}(M_{0,n})$ denotes the quotient of the profinite fundamental group $\pi_1(M_{0,n})$ divided by the kernel of $\pi_1(M_{0,n} \otimes \bar{k}) \to \hat{\Gamma}_0^n(\mathfrak{C})$, then the following exact sequence holds:

$$1 \to \hat{\Gamma}_0^n(\mathfrak{C}) \to \pi_1^{\mathfrak{C}}(M_{0,n}) \to G_k \to 1.$$

Each irreducible divisor D_{ij} gives in $\hat{\Gamma}_0^n(\mathfrak{C})$ a conjugacy union $\mathfrak{X}_{ij}$ of the inertia groups of valuations lying over D_{ij}. We put conventionally $\mathfrak{X}_{ij} = \mathfrak{X}_{ji}$ and $\mathfrak{X}_{ii} = \{1\}$.

(3.1.2) Let $n \geq m \geq 3$ and S a subset of $\{1, \ldots, n\}$ with cardinality $n - m$. There is a canonical morphism $f_S : M_{0,n} \to M_{0,m}$ obtained by forgetting the points a_i ($i \in S$) on $\mathbf{P}^1$ and renumbering the suffixes of the other a_k ($k \notin S$) without change of order in a unique way. The homomorphism

$\pi_1^{\mathfrak{C}}(M_{0,n}) \to \pi_1^{\mathfrak{C}}(M_{0,m})$ (resp. $\mathit{\Gamma}_0^n \to \mathit{\Gamma}_0^m$) induced from f_S is denoted by p_S (resp. p_S^{cl}), and when $S = \{\nu\}$ $(1 \le \nu \le n)$ simply by p_ν (resp. p_ν^{cl}). We call p_S or p_S^{cl} the *forgetful homomorphism* associated to $S \subset \{1, \ldots, n\}$.

Let (Γ_0^n) denote the exact sequence of discrete groups:

$$1 \to ker(p_\nu^{cl}) \to \mathit{\Gamma}_0^n \to \mathit{\Gamma}_0^{n-1} \to 1$$

for some $\nu \in \{1, \ldots, n\}$ $(n \ge 5)$. We notice that, by symmetry, the group extension is independent of the choice of ν and that $ker(p_\nu^{cl})$ is isomorphic to the fundamental group of an $(n-1)$-point punctured sphere denoted by $\Pi_{0,n-1}$. Let us now assume that (Γ_0^n) is $\mathfrak{C}$-admissible (see (1.2.2)). Then, for any $m \le n$ $(m \ge 5)$, (Γ_0^m) is also $\mathfrak{C}$-admissible, because the following commutative diagram of group extensions holds:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \Pi_{0,n-1} & \longrightarrow & \mathit{\Gamma}_0^n & \xrightarrow{p_0^{cl}} & \mathit{\Gamma}_0^{n-1} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle surj.} & & \downarrow{\scriptstyle p_n^{cl}} & & \downarrow{\scriptstyle p_{n-1}^{cl}} & & \\
1 & \longrightarrow & \Pi_{0,n-2} & \longrightarrow & \mathit{\Gamma}_0^{n-1} & \xrightarrow{p_0^{cl}} & \mathit{\Gamma}_0^{n-2} & \longrightarrow & 1.
\end{array}$$

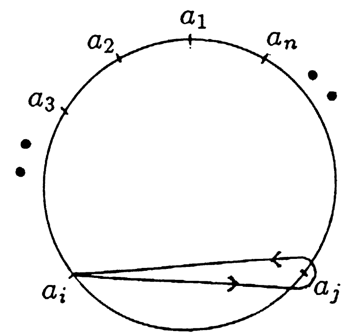
By using Propositions (1.2.4), (1.2.5) iteratedly, we see that $\mathit{\Gamma}_0^n$ is a $\mathfrak{C}$-good group (of type FL). Moreover, $ker(p_\nu)$ is isomorphic to the pro-$\mathfrak{C}$ completion of $ker(p_\nu^{cl}) \cong \Pi_{0,n-1}$. Thus $\hat{\mathit{\Gamma}}_0^n(\mathfrak{C})$ is a successive extension of free pro-$\mathfrak{C}$ groups, hence has trivial center. (This last assertion also follows from Proposition (1.3.3).)

(3.1.3) Let D^1 be the unit disk on $\mathbf{P}^1(\mathbb{C})$ with boundary S^1 and choose n points $a_1, \ldots, a_n$ on S^1 in the anticlockwise order around D^1. Let $a \in M_{0,n}(\mathbb{C})$ be the points corresponding to $(\mathbf{P}^1; a_1, \ldots, a_n)$. Then, for each i, j $(1 \le i < j \le n)$, we define $A_{ij} \in \pi_1(M_{0,n}(\mathbb{C}), a)$ to be the homotopy class of the loop represented by the diagram in Fig.1, and put $A_{ij} = A_{ji}, A_{ii} = 1$ for all $1 \le i, j \le n$.

It is known that $\pi_1(M_{0,n}(\mathbb{C}), a)$ is generated by the A_{ij} $(1 \le i, j \le n)$ and that the defining relations are given by the following (3.1.3.1) $\sim$ (3.1.3.7) (c.f. [27] §3.7, [5] §4.2), in which we shall say a sequence of natural numbers $(i_1, \ldots, i_m)$ is *in fair order* if $a_{i_1}, \ldots, a_{i_m}$ are distinct from each other and lie on S^1 in the anticlockwise order around D^1.

(3.1.3.1) $A_{ij} = A_{ji},\ A_{ii} = 1 \quad (1 \le i, j \le n)$.

Fig. 1



(3.1.3.2) $A_{rs}A_{ij}A_{rs}^{-1} = A_{ij}$, if (i,j,r,s) is in fair order.
(3.1.3.3) $A_{js}A_{ij}A_{js}^{-1} = A_{is}^{-1}A_{ij}A_{is}$, if (i,j,s) is in fair order.
(3.1.3.4) $A_{rj}A_{ij}A_{rj}^{-1} = A_{ij}^{-1}A_{ir}^{-1}A_{ij}A_{ir}A_{ij}$, if (i,r,j) is in fair order.
(3.1.3.5) $A_{rs}A_{ij}A_{rs}^{-1} = A_{is}^{-1}A_{ir}^{-1}A_{is}A_{ir}A_{ij}A_{ir}^{-1}A_{is}^{-1}A_{ir}A_{is}$, if (i,r,j,s) is in fair order.
(3.1.3.6) $A_{1i}\cdots A_{ni} = 1$ for each $1 \le i \le n$.
(3.1.3.7) $(A_{12})(A_{13}A_{23})\cdots(A_{1n}A_{2n}\cdots A_{n-1,n}) = 1$.

Remark. Let $\mathcal{B}_n$ be the Artin braid group with n strings, presented by the usual generators $\sigma_1,\dots,\sigma_{n-1}$ and by relations

$$\begin{cases} \sigma_i\sigma_j = \sigma_j\sigma_i \quad (|i-j| \ge 2), \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \quad (1 \le i \le n-2) \end{cases}$$

Then the pure braid group $\mathcal{P}_n$ is generated by the $\mathcal{A}_{ij} = \sigma_i^{-1}\cdots\sigma_{j-2}^{-1}\sigma_{j-1}^2\sigma_{j-2}\cdots\sigma_i$ $(1 \le i < j \le n)$. If $y_i = \sigma_{i-1}\cdots\sigma_2\sigma_1^2\sigma_2\cdots\sigma_{i-1}$ $(2 \le i \le n)$ and $z_n = y_2y_3\cdots y_n$, then the center of $\mathcal{B}_n$ (and of $\mathcal{P}_n$) is known to be an infinite cyclic group generated by the z_n. Moreover we know the canonical isomorphisms

$$\mathit{\Gamma}_0^n \cong \mathcal{P}_{n-1}/\langle z_{n-1}\rangle \cong \mathcal{P}_n/\langle z_n,\, \mathcal{B}_n\text{-conjugates of } y_n\rangle.$$

(3.1.4) In the following of this section, we fix the situation as follows. We let $n \ge 5$, and assume that the group extension (Γ_0^n) is $\mathfrak{C}$-admissible for a full class of finite groups $\mathfrak{C}$. (We see that (Γ_0^n) is $\mathfrak{C}$-admissible not only for $\mathfrak{C}_{fin}$

but also for $\mathfrak{C}_l$ (l: any prime) by observing the relations (3.1.3.2)$\sim$(3.1.3.5). See (1.2.3).) We fix a k-rational point $a = (\mathbf{P}^1; a_1, \dots, a_n) \in M_{0,n}$ and a geometric point $\bar{a}$ lying over it, together with an embedding of $\bar{k}$ into $\mathbb{C}$, so that the pro-$\mathfrak{C}$ completion $\hat{\Gamma}_0^n$ of $\Gamma_0^n = \pi_1(M_{0,n}(\mathbb{C}), a)$ is canonically identified with the maximal pro-$\mathfrak{C}$ quotient of $\pi_1(M_{0,n} \otimes \bar{k}, \bar{a})$. Let x_{ij} denote the image of A_{ij} ($1 \leq i, j \leq m$) in $\pi_1^{\mathfrak{C}}(M_{0,m})$ under this identification. Then, we have

$$\mathfrak{X}_{ij} = \{ g x_{ij}^c g^{-1} \mid c \in \mathbb{Z}_{\mathfrak{C}}, g \in \hat{\Gamma}_0^n \}.$$

Given a forgetful homomorphism $p_S : \pi_1^{\mathfrak{C}}(M_{0,n}, \bar{a}) \to \pi_1^{\mathfrak{C}}(M_{0,m}, f_S(\bar{a}))$ associated to $S \subset \{1, \dots, n\}$, we identify the geometric part of the target group with the pro-$\mathfrak{C}$ completion of $\pi_1(M_{0,m}(\mathbb{C}), f_S(a))$. In the latter group, we introduce a generator system as in (3.1.3) by using the configuration obtained from Fig.1 by deleting the a_i ($i \in S$) from $S^1 \subset \mathbf{P}^1(\mathbb{C})$, and by renumbering the suffices of the remaining a_j ($j \notin S$) without change of order in a unique way. We denote the image of A_{ij} ($1 \leq i, j \leq m$) in $\pi_1^{\mathfrak{C}}(M_{0,m})$ under the above identification by x_{ij} again. Then, if i or j ($1 \leq i < j \leq n$) belongs to S, then $p_S(x_{ij}) = 1$. Otherwise, $p_S(x_{ij})$ coincides with x_{rs} for some suitable $1 \leq r < s \leq m$. We remark that for $m < n$, the element $x_{ij} \in \pi_1^{\mathfrak{C}}(M_{0,m})$ is determined only up to conjugacy in $\hat{\Gamma}_0^m$, because it depends on the choice of S for which $M_{0,m}$ is regarded as the target space of f_S.

(3.1.5) Now, let us take an arbitrary G_k-compatible automorphism

$$f \in Aut_{G_k} \pi_1^{\mathfrak{C}}(M_{0,n}).$$

The remainder of this subsection is devoted to considering how $\mathfrak{X}_{\lambda\mu}$ ($1 \leq \lambda, \mu \leq n, \lambda \neq \mu$) are mapped by f. In Theorem (3.1.13), we will obtain a conclusion that f permutes these $\mathfrak{X}_{\lambda\mu}$ among them in such a way that the action is induced from a permutation of the set of indices $\{1, \dots, n\}$. Letting $m \geq 4$ and $\nu \in \{1, \dots m\}$, suppose that for a forgetful homomorphism $p_S : \pi_1^{\mathfrak{C}}(M_{0,n}) \to \pi_1^{\mathfrak{C}}(M_{0,m})$ associated to $S \subset \{1, \dots, n\}$, the following two conditions hold:

(3.1.5.1) $p_S \circ f(\mathfrak{X}_{\lambda\mu}) \neq 1$;

(3.1.5.2) $p_\nu \circ p_S \circ f(\mathfrak{X}_{\lambda\mu}) = 1$.

Proposition (3.1.6). *Let* $z = p_S \circ f(x_{\lambda\mu})$ *and assume* $\bigcup_{1 \leq i \leq n} f(\mathfrak{X}_{\lambda i}) \subset ker(p_\nu \circ p_S)$. *Then for each* $g \in \hat{\Gamma}_0^m$ *there exists* $g_0 \in ker(p_\nu)$ *such that* $gzg^{-1} = g_0 z g_0^{-1}$.

PROOF. Since $\hat{\Gamma}_0^n$ is generated by the centralizer of $x_{\lambda\mu}$ and the $x_{\lambda i}(1 \leq i \leq n)$, this is obvious from the assumption. (cf. [19] Proposition 2.3.1) □

Let us choose a group section $s_\infty : G_k \to \pi_1^{\mathfrak{C}}(M_{0,n})$ of $p_{0,n}$ (whose image is) normalizing the inertia subgroup $\langle x_{\lambda\mu}\rangle$ (and acting on it by conjugation) via the cyclotomic character. Such a section can be constructed, for example, as follows. Consider the forgetful homomorphism $p_\lambda : \pi_1^{\mathfrak{C}}(M_{0,n}) \to \pi_1^{\mathfrak{C}}(M_{0,n-1})$ so that $x_{\lambda\mu} \in ker(p_\lambda)$. The rational point $\alpha = f_\lambda(a)$ gives a morphism $Spec\, k \to M_{0,n-1}$, and induces a group section $s_\alpha : G_k \to \pi_1^{\mathfrak{C}}(M_{0,n-1})$ of $p_{0,n-1}$. If C_α is the $(n-1)$-point punctured projective line represented by $\alpha \in M_{0,n-1}(k)$, then $p_\lambda^{-1}(s_\alpha(G_k))$ is canonically identified with $\pi_1^{\mathfrak{C}}(C_\alpha)$ as G_k-augmented profinite groups. Then, by Belyi's well-known method, we can construct a complement of $\pi_1^{\mathfrak{C}}(C_\alpha \otimes \bar{k})$ in $\pi_1^{\mathfrak{C}}(C_\alpha)$ normalizing $\langle x_{\lambda\mu}\rangle$ via the cyclotomic character. [For example, define such a complement by

$$\left\{ w \in \pi_1^{\mathfrak{C}}(C_\alpha) \mid \begin{array}{c} w x_{\lambda\mu} w^{-1} = x_{\lambda\mu}^a, \quad w x_{\lambda\rho} w^{-1} = t x_{\lambda\rho}^a t^{-1}, \\ \exists\, a \in \mathbb{Z}_{\mathfrak{C}}^\times \quad \exists\, t \in (ker(p_\lambda))' \langle x_{\lambda i} \mid i \neq \lambda, \mu, \rho, \rho' \rangle \end{array} \right\}.$$

for some $\rho, \rho' \in \{1, \ldots, n\} \setminus \{\lambda, \mu\}$, $\rho \neq \rho'$.] This gives desired s_∞. The Galois compatibility of f assures that $p_S \circ f \circ s_\infty$ gives also a section $G_k \to \pi_1^{\mathfrak{C}}(M_{0,m})$ of $p_{0,m}$ normalizing $\langle p_S \circ f(x_{\lambda\mu})\rangle$ via the cyclotomic character. Let $\chi : \pi_1^{\mathfrak{C}}(M_{0,m}) \to \mathbb{Z}_{\mathfrak{C}}^\times$ denote the homomorphism obtained by composing $p_{0,m} : \pi_1^{\mathfrak{C}}(M_{0,m}) \to G_k$ with the cyclotomic character of G_k. Then since $\pi_1^{\mathfrak{C}}(M_{0,m})$ is a semidirect product of $\hat{\Gamma}_0^m$ with $p_S \circ f \circ s_\infty(G_k)$, we can generalize (3.1.6) to the following

PROPOSITION (3.1.7). *Let $z = p_S \circ f(x_{\lambda\mu})$ and assume $\bigcup_{1\leq i\leq n} f(\mathfrak{X}_{\lambda i}) \subset ker(p_\nu \circ p_S)$. Then for each $g \in \pi_1^{\mathfrak{C}}(M_{0,m})$, there exists $g_0 \in ker(p_\nu)$ such that $gzg^{-1} = g_0 z^{\chi(g)} g_0^{-1}$.* □

We proceed under the assumption of Proposition (3.1.7). Let x denote the rational point $f_\nu \circ f_S(a) \in M_{0,m-1}(k)$, and C_x the $(m-1)$-point punctured projective line over k represented by $x \in M_{0,m-1}(k)$. Then, we see that $\Pi = p_\nu^{-1}(s_x(G_k))$ is isomorphic to $\pi_1^{\mathfrak{C}}(C_x)$ with geometric part

$\pi = ker(p_\nu)$, and obtain the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi & \longrightarrow & \Pi & \longrightarrow & s_x(G_k) & \longrightarrow & 1 \quad \text{(exact)} \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & ker(p_\nu) & \longrightarrow & \pi_1^{\mathfrak{C}}(M_{0,m}) & \underset{p_\nu}{\longrightarrow} & \pi_1^{\mathfrak{C}}(M_{0,m-1}) & \longrightarrow & 1 \quad \text{(exact).} \end{array}$$

Let l be a prime such that $Syl_l\langle z\rangle \neq 1$, and z_l the l-component of z. We notice that the same statement as Proposition (3.1.7) holds even if z is replaced by z_l there. From this, it follows that $N_\Pi(z_l)$ is surjectively mapped onto $s_x(G_k)$ by p_ν. Since $[N_\pi(z_l) : C_\pi(z_l)] < \infty$ by (1.4.3), Proposition (1.4.1) yields an open subgroup M of $N_\Pi(z_l)$ such that $M \cap \pi = C_\pi(z_l)$. Let K be a finite extension of k in $\bar{k}$ with $p_\nu(M) = s_x(G_K)$. Then the conjugate action of M on $\langle z_l\rangle$ gives a Galois character

$$\psi : G_K \to Aut\langle z_l\rangle = \mathbb{Z}_l^\times.$$

On the other hand, we have another Galois character χ induced from the conjugate action of $p_S \circ f \circ s_\infty(G_k)$ on $\langle z_l\rangle$:

$$\chi : G_K \to Aut\langle z_l\rangle = \mathbb{Z}_l^\times$$

which apriori coincides with the cyclotomic character. To compare ψ and χ, let $\mathfrak{N}$ be the normalizer of z_l in $\pi_1^{\mathfrak{C}}(M_{0,m})$. Then, by the construction, we see that for each $\sigma \in G_K$ there exists $g(\sigma) \in \mathfrak{N} \cap \hat{\Gamma}_0^m$ such that

$$z_l^{\chi(\sigma)\psi(\sigma)^{-1}} = g(\sigma) z_l g(\sigma)^{-1}.$$

Proposition (3.1.7) (on z_l) assures that these $g(\sigma)$ may be taken from $\pi = ker(p_\nu)$. But since $[N_\pi(z_l) : C_\pi(z_l)] < \infty$, the image of the Galois character $\chi\psi^{-1}$ is contained in the torsion of $\mathbb{Z}_l^\times$. From this, we get a finite extension L of K in $\bar{k}$ such that, on G_L, $\psi \equiv \chi$ (i.e. the cyclotomic character). This means that $N := M \cap p_\nu^{-1}(s_x(G_L))$ gives a 'cyclotmic normalizer' of z_l in $\Pi \cong \pi_1^{\mathfrak{C}}(C_x)$ (see 2.1). It follows from the "nonlinear weight filtration" (2.1.1) that z_l is contained in an inertia group of $\pi = \pi_1^{\mathfrak{C}}(C_x \otimes \bar{k})$. Moreover, by Lemma (2.1.2), the same statement holds for z itself. Since the union of inertia groups in $\pi = ker(p_\nu)$ is $\bigcup_{1\leq j\leq m} \mathfrak{X}_{\nu j}$, we obtain

Lemma (3.1.8). *Besides the hypothesis of (3.1.5), assume that* $\bigcup_{1\le i\le n} f(\mathfrak{X}_{\lambda i}) \subset ker(p_\nu \circ p_S)$. *Then* $p_S \circ f(\mathfrak{X}_{\lambda\mu})$ *is contained in one of the* $\mathfrak{X}_{\nu j}$ $(1 \le j \le m, j \ne \nu)$. □

(3.1.9) Two special irreducible divisors D_{ij} and D_{rs} in B_n normally cross each other if and only if $\{i,j\} \cap \{r,s\} = \emptyset$. [In fact, this latter condition is necessary and sufficient for $D_{ij} \cap D_{rs} \ne \emptyset$ ([12] p.153). Assume $s > i, j$ without loss of generality. The canonical morphism $f_{\{s\}} : M_{0,n} \to M_{0,n-1}$ is extended naturally to a flat morphism $\bar{f}_{\{s\}} : B_n \to B_{n-1}$ giving the universal family of stable $(n-1)$-pointed P^1-trees over B_{n-1} together with an isomorphism $D_{rs} \tilde{\to} B_{n-1}$ ([12]). Since D_{rs} has a neighborhood where $\bar{f}_{\{s\}}$ is smooth, and since $D_{ij} \subset B_n$ is a unique irreducible component of $\bar{f}_{\{s\}}^{-1}(D_{ij})$ intersecting D_{rs}, they normally cross each other.] In this case, the local monodromy in $M_{0,n}$ near a general point of $D_{ij} \cap D_{rs}$ gives a homomorphism $\rho : \mathbb{Z}_{\mathfrak{C}}^2 \to \hat{\Gamma}_0^n$. The image $A = Im(\rho)$ is an abelian subgroup such that
(*) $\mathfrak{X}_{ij} \cap A \ne \{1\}$, $\mathfrak{X}_{rs} \cap A \ne \{1\}$.
This can also be seen directly from the presentation described in (3.1.3), if we put $A = \langle x_{ij}, x_{rs}\rangle$ when (i,j,r,s) is in fair order, and $A = \langle x_{ij}, x_{ir}^{-1} x_{rs} x_{ir}\rangle$ when (i,r,j,s) is in fair order. (For the latter case, use (3.1.3.3) for (i,r,s) together with (3.1.3.5).)

Definition. A closed abelian subgroup A of $\hat{\Gamma}_0^n$ satisfying the condition (*) is called a *connecting abelian subgroup* between $\mathfrak{X}_{ij}$ and $\mathfrak{X}_{rs}$.

Roughly speaking, we see in $\hat{\Gamma}_0^n$ a regular graph system of the special weight (-2) subsets $\mathfrak{X}_{ij}$ $(1 \le i, j \le n)$ connected by "edges" of abelian subgroups. An arbitrary Galois compatible automorphism $f \in Aut_{G_k} \pi_1^{\mathfrak{C}}(M_{0,n})$ preserves this graph structure, but we do not apriori know that the images $f(\mathfrak{X}_{ij})$ actually coincide with the original $\mathfrak{X}_{ij}$ as subsets of $\hat{\Gamma}_0^n$. To verify this last assertion later in Theorem (3.1.13), we need two more lemmas. In the remainder of this section, we sometimes omit the symbol "$\circ$" making composition of homomorphisms.

Remark. In connection with Hyperbolicity Conjecture on sufficiently open varieties, F.A.Bogomolov suggested a somewhat related idea of rank-2 abelian subgroups. See [6] §3.

Lemma (3.1.10). *Under the hypothesis of (3.1.5), either* $\bigcup_{1\le i\le n}\cdot$

$f(\mathfrak{X}_{\lambda i})$ or $\bigcup_{1\le i\le n} f(\mathfrak{X}_{\mu i})$ is contained in $ker(p_\nu \circ p_S)$.

PROOF. Since the statement is obvious when $m=4$, we may assume $m\ge 5$. Define three sets $\mathfrak{T}, \mathfrak{T}_1, \mathfrak{T}_2$ by

$$\mathfrak{T} = \{T \subset \{1,\dots,m-1\} \mid 0 \le |T| \le m-5\},$$

$$\mathfrak{T}_1 = \left\{ T \in \mathfrak{T} \;\middle|\; \begin{array}{c} \bigcup_{1\le i\le n} f(\mathfrak{X}_{\lambda i}) \not\subset ker(p_T p_\nu p_S), \\ \bigcup_{1\le i\le n} f(\mathfrak{X}_{\mu i}) \not\subset ker(p_T p_\nu p_S) \end{array} \right\},$$

$$\mathfrak{T}_2 = \left\{ (\tau, T) \;\middle|\; \begin{array}{c} T \in \mathfrak{T}_1,\ \tau \in \{1,\dots,m-1-|T|\}, \\ \bigcup_{1\le i\le n} f(\mathfrak{X}_{\lambda i}) \text{ or } \bigcup_{1\le i\le n} f(\mathfrak{X}_{\mu i}) \subset ker(p_\tau p_T p_\nu p_S) \end{array} \right\}.$$

Let us deny the conclusion of the lemma. Then $\emptyset \in \mathfrak{T}_1$. Observe that if $T \in \mathfrak{T}_1$, then there exists $(\tau, T') \in \mathfrak{T}_2$ such that $T \subset T'$.

We first claim that $\mathfrak{T}_1$ has an element with cardinality $m-5$. If $m=5$, there is nothing to prove. So let $m\ge 6$ and suppose that we have $(\tau, T) \in \mathfrak{T}_2$ with $|T| < m-5$. To prove the claim, it suffices to show that there exists $T' \in \mathfrak{T}_1$ with $|T'| = |T|+1$. By symmetry, without loss of generality we may assume $\bigcup_{1\le i\le n} f(\mathfrak{X}_{\lambda i}) \subset ker(p_\tau p_T p_\nu p_S)$. As $T \in \mathfrak{T}_1$, we can choose i_0 such that $f(\mathfrak{X}_{\lambda i_0}) \not\subset ker(p_T p_\nu p_S)$. Then by Lemma (3.1.8), $p_T p_\nu p_S f(\mathfrak{X}_{\lambda i_0}) \subset \mathfrak{X}_{\tau j_0}$ for some $1 \le j_0 \le m-1-|T|$. Let ε be such that $1 \le \varepsilon \le m-1-|T|$, $\varepsilon \notin \{\tau, j_0\}$, and define $T'' \subset \{1,\dots,m-1\}$ by $p_\varepsilon p_T = p_{T''}$. Then $f(\mathfrak{X}_{\lambda i_0}) \not\subset ker(p_{T''} p_\nu p_S)$. If $\bigcup_{1\le i\le n} f(\mathfrak{X}_{\mu i}) \not\subset ker(p_{T''} p_\nu p_S)$, then we may take T'' as T'. So let $\bigcup_{1\le i\le n} f(\mathfrak{X}_{\mu i}) \subset ker(p_\varepsilon p_T p_\nu p_S)$ and choose r such that $f(\mathfrak{X}_{\mu r}) \not\subset ker(p_T p_\nu p_S)$. Then by Lemma (3.1.8) again, there exists $1 \le s \le m-1-|T|$ such that $p_T p_\nu p_S(\mathfrak{X}_{\mu r}) \subset \mathfrak{X}_{\varepsilon s}$. Since $m-1-|T| \ge 5$, we can choose $1 \le \delta \le m-1-|T|$ with $\delta \notin \{\tau, j_0, \varepsilon, s\}$. Then we may define our desired T' by $p_\delta \circ p_T = p_{T'}$. Thus our claim follows.

By the claim, we obtain $T \in \mathfrak{T}_1$ with $|T| = m-5$. To deduce contradiction, consider the projection $p = p_T p_\nu p_S : \pi_1^{\mathfrak{C}}(M_{0,n}) \to \pi_1^{\mathfrak{C}}(M_{0,4})$. Then neither $\bigcup_{1\le i\le n} f(\mathfrak{X}_{\lambda i})$ nor $\bigcup_{1\le i\le n} f(\mathfrak{X}_{\mu i})$ is contained in $ker(p)$. As $f(\mathfrak{X}_{\lambda\mu}) \subset ker(p)$ by (3.1.5.2) and $x_{\lambda 1}\cdots x_{\lambda n} = 1$ (resp. $x_{\mu 1}\cdots x_{\mu n} = 1$), there exist at least two i's outside $\{\lambda, \mu\}$ such that $f(\mathfrak{X}_{\lambda i}) \not\subset ker(p)$ (resp. $f(\mathfrak{X}_{\mu i}) \not\subset ker(p)$). Therefore we may assume $f(\mathfrak{X}_{\lambda\gamma}), f(\mathfrak{X}_{\mu\alpha}) \not\subset ker(p)$ for some α, γ with $\{\alpha, \gamma\} \cap \{\lambda, \mu\} = \emptyset$, $\alpha \neq \gamma$. Let p_{ab} denote the composite of the restriction of p to $\hat{\Gamma}_0^n$ with the abelianization map $(\ )^{ab}$ of $\hat{\Gamma}_0^4$. Then, since there exists a connecting abelian subgroup between $\mathfrak{X}_{\lambda\gamma}$ and $\mathfrak{X}_{\mu\alpha}$, and since $\hat{\Gamma}_0^4$ admits no connecting abelian subgroups between any two of $\mathfrak{X}_{14}$, $\mathfrak{X}_{24}$, $\mathfrak{X}_{34}$ (see Corollary (2.1.3)), we get $p_{ab}f(\mathfrak{X}_{\lambda\gamma})$ and $p_{ab}f(\mathfrak{X}_{\mu\alpha})$ are contained in the same line Z of either $\mathfrak{X}_{14}^{ab}$, $\mathfrak{X}_{24}^{ab}$ or $\mathfrak{X}_{34}^{ab}$. For similar reason, all $p_{ab}f(\mathfrak{X}_{ij})$ with $\{i,j\} \neq \{\lambda,\mu\}, \{\lambda,\alpha\}, \{\mu,\gamma\}, \{\alpha,\gamma\}$ lie in the same image Z. But since $x_{\lambda 1} \cdots x_{\lambda n} = 1$, $x_{\mu 1} \cdots x_{\mu n} = 1$ and $f(\mathfrak{X}_{\lambda\mu}) \subset ker(p)$ as above, we see that $p_{ab}f(\mathfrak{X}_{\lambda\alpha})$ and $p_{ab}f(\mathfrak{X}_{\mu\gamma})$ are also contained in Z. Finally follows that $p_{ab}f(\mathfrak{X}_{\alpha\gamma}) \subset Z$ from $x_{\alpha 1} \cdots x_{\alpha n} = 1$, and thus we conclude that all $f(\mathfrak{X}_{ij})\,(1 \leq i,j \leq n)$ are sent into Z by p_{ab}. As $\hat{\Gamma}_0^n$ is generated by these $\mathfrak{X}_{ij}\,(1 \leq i,j \leq n)$, this contradicts the surjectivity of p_{ab}. The proof of Lemma (3.1.10) is completed. □

As a special case of Lemma (3.1.10) where $m = n$ and $S = \emptyset$, we obtain the following

Corollary (3.1.11). *Let $f \in Aut_{G_k}\pi_1^{\mathfrak{C}}(M_{0,n})$, and $\lambda, \mu, \nu \in \{1, \ldots, n\}$ with $\lambda \neq \mu$. Assume $f(\mathfrak{X}_{\lambda\mu}) \subset ker(p_\nu)$. Then either $\bigcup_{1 \leq i \leq n} f(\mathfrak{X}_{\lambda i})$ or $\bigcup_{1 \leq i \leq n} f(\mathfrak{X}_{\mu i})$ is contained in $ker(p_\nu)$.* □

Lemma (3.1.12). *Let $f \in Aut_{G_k}\pi_1^{\mathfrak{C}}(M_{0,n})$ and $\nu \in \{1, \ldots, n\}$. Then there exists at least one $\mathfrak{X}_{ij}$ $(1 \leq i < j \leq n)$ such that $f(\mathfrak{X}_{ij})$ is contained in $ker(p_\nu)$.*

Proof. The statement is nontrivial when $n \geq 5$. Assume $f(\mathfrak{X}_{ij}) \not\subset ker(p_\nu)$ for all $1 \leq i < j \leq n$. Then there exist $S \subset \{1, \ldots, n-1\}$, $\varepsilon \in \{1, \ldots, n-1-|S|\}$ and $\mathfrak{X}_{\lambda\mu}$ with $1 \leq \lambda < \mu \leq n$ such that

(3.1.12.1) $$f(\mathfrak{X}_{ij}) \not\subset ker(p_S p_\nu) \quad (1 \leq i < j \leq n),$$

(3.1.12.2) $$f(\mathfrak{X}_{\lambda\mu}) \subset ker(p_\varepsilon p_S p_\nu).$$

Put $m = n - 1 - |S|$. Then $m \geq 4$ by (3.1.12.1).

By (3.1.8) and (3.1.10), we may assume that each $p_S p_\nu f(\mathfrak{X}_{\lambda i})\,(1 \leq i \leq n, i \neq \lambda)$ is contained in some $\mathfrak{X}_{\varepsilon\alpha(i)}\,(1 \leq \alpha(i) \leq m, \alpha(i) \neq \varepsilon)$. If all $\alpha(i)$ are the same α, then since $\hat{\Gamma}_0^n$ is generated by the $x_{\lambda i}\,(1 \leq i \leq n)$ and their centralizers, $\hat{\Gamma}_0^m$ must be generated by conjugates of the centralizers of $x_{\varepsilon\alpha}$.

This is absurd as $m \geq 4$. So we obtain $r(\neq \mu)$ such that

$$p_S p_\nu f(\mathfrak{X}_{\lambda r}) \subset \mathfrak{X}_{\varepsilon\alpha(r)} \neq \mathfrak{X}_{\varepsilon\alpha(\mu)} \supset p_S p_\nu f(\mathfrak{X}_{\lambda\mu}).$$

Let $\delta = \alpha(\mu)$. Then $f(\mathfrak{X}_{\lambda\mu}) \subset ker(p_\delta p_S p_\nu)$, $f(\mathfrak{X}_{\lambda r}) \not\subset ker(p_\delta p_S p_\nu)$. Therefore by (3.1.8) and (3.1.10), each $p_S p_\nu f(\mathfrak{X}_{\mu j})\,(1 \leq j \leq n, j \neq \mu)$ must be contained in some $\mathfrak{X}_{\delta\beta(j)}\,(1 \leq \beta(j) \leq m, \delta \neq \beta(j))$.

Thus we get to a situation where (3.1.12.1) holds and there are two maps

$$\begin{aligned}\alpha &: \{1,\dots,n\} \setminus \{\lambda\} \to \{1,\dots,m\} \setminus \{\varepsilon\},\\ \beta &: \{1,\dots,n\} \setminus \{\mu\} \to \{1,\dots,m\} \setminus \{\delta\},\end{aligned}$$

with $\alpha(\mu) = \delta,\ \beta(\lambda) = \varepsilon$ such that

$$\text{(3.1.12.3)} \qquad \begin{cases} p_S p_\nu f(\mathfrak{X}_{\lambda i}) \subset \mathfrak{X}_{\varepsilon\alpha(i)} & (1 \leq i \leq n, i \neq \lambda), \\ p_S p_\nu f(\mathfrak{X}_{\mu j}) \subset \mathfrak{X}_{\delta\beta(j)} & (1 \leq j \leq n, j \neq \mu). \end{cases}$$

(3.1.12.4) CLAIM. The above map α (resp. β) satisfies either of the following:
(i) α (resp. β) is surjective and at least one fibre has cardinality ≥ 2;
(ii) the image of α (resp. β) has cardinality ≥ 2, and each nonempty fibre has cardinality ≥ 2.

It suffices to prove the Claim in the case of α, because the argument can also be applied to the case of β in a parallel way by the symmetry of α and β. (Notice that (3.1.12.2) results from (3.1.12.3).) Let X_{ij} denote the image of $x_{ij}\,(1 \leq i, j \leq m)$ in the abelianization of $\hat{\Gamma}_0^m$. Then applying $p_S p_\nu f$ to $x_{\lambda 1} \cdots x_{\lambda n} = 1$, we obtain

$$\sum_{\substack{i \neq \lambda \\ 1 \leq i \leq n}} c_i X_{\varepsilon\alpha(i)} = 0 \quad (\exists\, c_i \in \mathbb{Z}_{\mathfrak{C}} \setminus \{0\})$$

Rewrite this as

$$\sum_{\substack{j \neq \varepsilon \\ 1 \leq j \leq m}} d_j X_{\varepsilon j} = 0 \quad (d_j = \sum_{\alpha(i)=j} c_i),$$

and compare it with the basic equation from (3.1.3.6): $\sum_{1\leq j\leq m} X_{\varepsilon j} = 0$. Then either of the following holds.
Case (i): $0 \neq \exists\, d = d_j\,(1 \leq j \leq m, j \neq \varepsilon)$. In this case, the map α must be surjective. Since $n > m$, this case yields (i) of the Claim.
Case (ii): $\forall\, d_j = 0\,(1 \leq j \leq m, j \neq \varepsilon)$. In this case, for each j, $\sum_{\alpha(i)=j} c_i = 0$. Since $c_i \neq 0$, we have at least two i's with $\alpha(i) = j$ if $\alpha^{-1}(j) \neq \emptyset$. As we already know $\alpha(r) \neq \alpha(\mu)$, this case yields (ii) of the Claim.
Thus the Claim (3.1.12.4) follows.

Let us deduce contradiction by using this Claim. Assume first that $|\beta^{-1}(\varepsilon)| \geq 2$, i.e., there exists $v \neq \lambda$ such that $\beta(v) = \beta(\lambda) = \varepsilon$. If $v \neq r$, then a connecting abelian subgroup between $\mathfrak{X}_{v\mu}$ and $\mathfrak{X}_{\lambda r}$ exists. But $p_S p_\nu f(\mathfrak{X}_{v\mu}) \subset \mathfrak{X}_{\varepsilon\delta}$ and $p_S p_\nu f(\mathfrak{X}_{\lambda r}) \subset \mathfrak{X}_{\varepsilon\alpha(r)}$ are both contained non-trivially in $ker(p_\varepsilon)$ which is free of rank $m-2$. This forces $\delta = \alpha(r)$, hence contradiction. Therefore we may assume $v = r$. We apply (3.1.8) and (3.1.10) to

$$\begin{cases} p_S p_\nu f(\mathfrak{X}_{\lambda r}) \subset \mathfrak{X}_{\varepsilon\alpha(r)} \subset ker(p_{\alpha(r)}), \\ p_S p_\nu f(\mathfrak{X}_{\lambda\mu}) \subset \mathfrak{X}_{\varepsilon\delta} \not\subset ker(p_{\alpha(r)}). \end{cases}$$

Then there exists q $(1 \leq q \leq m, q \neq \alpha(r))$ such that

$$p_S p_\nu f(\mathfrak{X}_{\mu r}) \subset \mathfrak{X}_{q\alpha(r)}.$$

But since $p_S p_\nu f(\mathfrak{X}_{\mu r}) \subset \mathfrak{X}_{\delta\beta(r)}$ and $\delta \neq \alpha(r)$, we obtain $q = \delta$. On the other hand, when $r = v$, we have

$$p_S p_\nu f(\mathfrak{X}_{\mu r}) = p_S p_\nu f(\mathfrak{X}_{\mu v}) \subset \mathfrak{X}_{\delta\beta(v)} = \mathfrak{X}_{\delta\varepsilon}.$$

Therefore we must conclude $\alpha(r) = \varepsilon$. This is a contradiction.

By (3.1.12.4) and the symmetry of α and β, it remains to consider the case where $|\beta^{-1}(\varepsilon)| = 1$ and α is surjective. But then, we can take $\tau \notin \{\varepsilon, \delta\}$ such that $|\beta^{-1}(\tau)| \geq 2$, and further $u \in \alpha^{-1}(\tau)$ and $v \in \beta^{-1}(\tau)$ such that $u \neq v$. Then $p_S p_\nu f(\mathfrak{X}_{\lambda u}) \subset \mathfrak{X}_{\varepsilon\tau}$ and $p_S p_\nu f(\mathfrak{X}_{\mu v}) \subset \mathfrak{X}_{\delta\tau}$ are both contained in $ker(p_\tau)$ which is free of rank $m-2$. This contradicts the existence of a connecting abelian subgroup between $\mathfrak{X}_{\lambda u}$ and $\mathfrak{X}_{\mu v}$. Thus the proof of Lemma (3.1.12) is completed. $\square$

Now we are in a position to prove the following

THEOREM (3.1.13). *Let f be a G_k-compatible automorphism of $\pi_1^{\mathfrak{C}}(M_{0,n})$ $(n \geq 4)$. Then, there exists a G_k-compatible automorphism h of it coming from $Aut_k(M_{0,n})$ such that $f \circ h$ maps each $\mathfrak{X}_{ij}$ onto itself $(1 \leq i < j \leq n)$.*

PROOF. The case of $n = 4$ follows from the weight filtration of non-linear type (Theorem (2.1.1)). We assume $n \geq 5$. Let f be an arbitrary element of $Aut_{G_k}\pi_1^{\mathfrak{C}}(M_{0,n})$, and $p_n : \pi_1^{\mathfrak{C}}(M_{0,n}) \to \pi_1^{\mathfrak{C}}(M_{0,n-1})$ the forgetful homomorphism defined in (3.1.2). By Lemma (3.1.12) there exists $\mathfrak{X}_{\lambda\mu}$ such that $f(\mathfrak{X}_{\lambda\mu}) \subset ker(p_n)$. Applying Corollary (3.1.11) we may assume without loss of generality that

$$\bigcup_{1 \leq i \leq n} f(\mathfrak{X}_{\lambda i}) \subset ker(p_n). \tag{3.1.13.1}$$

Then by Lemma (3.1.8), each of the $f(\mathfrak{X}_{\lambda i})$ $(1 \leq i \leq n, i \neq \lambda)$ coincides with one of the $\mathfrak{X}_{nj}$ $(1 \leq j \leq n-1)$ respectively. Therefore we can take an element h of $Aut_{G_k}\pi_1^{\mathfrak{C}}(M_{0,n})$ coming from $S_n (\cong Aut_k(M_{0,n}))$ such that

$$f \circ h(\mathfrak{X}_{ni}) = \mathfrak{X}_{ni} \quad (1 \leq i \leq n-1). \tag{3.1.13.2}$$

Next, let us consider the other forgetful homomorphisms $p_\nu : \pi_1^{\mathfrak{C}}(M_{0,n}) \to \pi_1^{\mathfrak{C}}(M_{0,n-1})$ $(1 \leq \nu \leq n-1)$. Since we already know $f \circ h(\mathfrak{X}_{n\nu}) \subset ker(p_\nu)$ by (3.1.13.2), by applying (3.1.8), (3.1.11) and (3.1.13.2) again, we see that $f \circ h$ must induce a permutation of the set

$$\mathfrak{X}^{(\nu)} = \{\mathfrak{X}_{j\nu} \mid 1 \leq j \leq n-1,\, j \neq \nu\}$$

for each ν. (Notice that $\mathfrak{X}_{n\nu}$ is preserved by $f \circ h$.) Then observing $\{\mathfrak{X}_{ij}\} = \mathfrak{X}^{(i)} \cap \mathfrak{X}^{(j)}$, we conclude $f \circ h(\mathfrak{X}_{ij}) = \mathfrak{X}_{ij}$ $(1 \leq i, j \leq n-1)$. This completes the proof of Theorem (3.1.13). □

3.2. Reduction to $\mathbf{P}^1 - \{0, 1, \infty\}$, Proof of Theorem A

Let $\mathfrak{C}$ be a full class of finite groups, and $\hat{\Gamma}_0^n$ denote the pro-$\mathfrak{C}$ completion of Γ_0^n $(n \geq 4)$.

DEFINITION (3.2.1). A continuous automorphism f of $\hat{\Gamma}_0^n$ is said to be *quasi-special* if it satisfies

$$f(\mathfrak{X}_{ij}) = \mathfrak{X}_{ij}$$

for all $1 \leq i < j \leq n$. (See (3.1.1) or (3.1.4) for the definition of $\mathfrak{X}_{ij}$.) We denote by $Aut^\flat(\hat{\Gamma}_0^n)$ the group of all the quasi-special automorphisms of $\hat{\Gamma}_0^n$. Moreover we put $Out^\flat(\hat{\Gamma}_0^n) = Aut^\flat(\hat{\Gamma}_0^n)/Inn\hat{\Gamma}_0^n$. It is easy to see that each $f \in Aut^\flat(\hat{\Gamma}_0^n)$ acts on $\hat{\Gamma}_0^n/[\hat{\Gamma}_0^n, \hat{\Gamma}_0^n]$ by multiplication by a constant $a_f \in \mathbb{Z}_{\mathfrak{C}}^\times$. When $a_f = 1$, we say that f is a *special* automorphism of $\hat{\Gamma}_0^n$ (cf. [19]).

Let $n \geq 5$, and $p_\nu : \hat{\Gamma}_0^n \to \hat{\Gamma}_0^{n-1}$ the forgetful homomorphism associated to $\nu \in \{1, \ldots, n\}$. Since $ker(p_\nu)$ is generated by the $\mathfrak{X}_{i\nu}$ $(1 \leq i \leq n)$, there are canonical homomorphisms

$$q_\nu : Aut^\flat(\hat{\Gamma}_0^n) \to Aut^\flat(\hat{\Gamma}_0^{n-1}),$$
$$\bar{q}_\nu : Out^\flat(\hat{\Gamma}_0^n) \to Out^\flat(\hat{\Gamma}_0^{n-1})$$

induced by p_ν $(1 \leq \nu \leq n)$.

LEMMA (3.2.2). *Let $n \geq 5$ and assume that the group extension (Γ_0^n) is $\mathfrak{C}$-admissible (3.1.2). Then for each pair of $\lambda, \mu \in \{1, \ldots, n\}$ with $\lambda \neq \mu$, the homomorphism*

$$(\bar{q}_\lambda, \bar{q}_\mu) : Out^\flat(\hat{\Gamma}_0^n) \to Out^\flat(\hat{\Gamma}_0^{n-1}) \times Out^\flat(\hat{\Gamma}_0^{n-1}), \quad h \mapsto (\bar{q}_\lambda(h), \bar{q}_\mu(h))$$

is injective.

PROOF. By symmetry, we may assume $\lambda = 1, \mu = n$. Let us introduce the generator system $\{x_{ij} \mid 1 \leq i < j \leq n\}$ of $\hat{\Gamma}_0^n$ as in (3.1.3). Suppose we are given an automorphism $f \in Aut^\flat(\hat{\Gamma}_0^n)$ such that $q_1(f)$ and $q_n(f)$ are inner automorphisms. Then $a_f = 1$. Since the centralizer of $x_{n-1,n}$ in $\hat{\Gamma}_0^n$ is mapped surjectively onto $\hat{\Gamma}_0^{n-1}$ via p_n, replacing f by a composition with an inner automorphism of $\hat{\Gamma}_0^n$, we may normalize f to satisfy
(3.2.2.1) $f(x_{n-1,n}) = x_{n-1,n}$;
(3.2.2.2) $f(x_{n-2,n}) = tx_{n-2,n}t^{-1}$, $\exists\, t \in (ker(p_n))'\langle x_{1n}, \ldots, x_{n-4,n}\rangle$;
(3.2.2.3) $q_n(f) =$identity.
If $\mathfrak{B}$ is a subgroup of $\hat{\Gamma}_0^n$ defined by

$$\mathfrak{B} = \left\{ g \in \hat{\Gamma}_0^n \mid \begin{array}{c} gx_{n-1,n}g^{-1} = x_{n-1,n}, \quad gx_{n-2,n}g^{-1} = tx_{n-2,n}t^{-1}, \\ \exists\, t \in (ker(p_n))'\langle x_{1n}, \ldots, x_{n-4,n}\rangle \end{array} \right\}.$$

then (3.2.2.1)-(3.2.2.2) assures $f(\mathfrak{B}) = \mathfrak{B}$. Moreover, by (3.2.2.3), $\mathfrak{B}$ is pointwise fixed by f, for the restriction of p_n to $\mathfrak{B}$ gives an isomorphism of $\mathfrak{B}$ onto $\hat{\Gamma}_0^{n-1}$. We next define subgroups $\mathfrak{B}' \subset \hat{\Gamma}_0^n$, $\mathfrak{B}'_0 \subset \hat{\Gamma}_0^{n-1}$ by

$$\mathfrak{B}' = \left\{ g \in \hat{\Gamma}_0^n \mid \begin{array}{c} gx_{12}g^{-1} = x_{12}, \quad gx_{13}g^{-1} = tx_{13}t^{-1}, \\ \exists\, t \in (ker(p_1))'\langle x_{15}, \ldots, x_{1n} \rangle \end{array} \right\},$$

$$\mathfrak{B}'_0 = \left\{ g \in \hat{\Gamma}_0^{n-1} \mid \begin{array}{c} gx_{12}g^{-1} = x_{12}, \quad gx_{13}g^{-1} = tx_{13}t^{-1}, \\ \exists\, t \in (ker(p_1))'\langle x_{15}, \ldots, x_{1,n-1} \rangle \end{array} \right\}.$$

As $x_{12}, x_{13} \in \mathfrak{B}$, we have $f(x_{12}) = x_{12}, f(x_{13}) = x_{13}$, from which we see $f(\mathfrak{B}') = \mathfrak{B}'$. Since p_1 gives an isomorphism $\mathfrak{B}' \cong \hat{\Gamma}_0^{n-1}$, f acts on $\mathfrak{B}'$ as an inner automorphism by an element γ of $\mathfrak{B}'$. Now there is a commutative diagram

$$\begin{array}{ccc} \hat{\Gamma}_0^n \supset \mathfrak{B}' & \xrightarrow[p_1]{\sim} & \hat{\Gamma}_0^{n-1} \\ {\scriptstyle p_n}\downarrow & & \downarrow{\scriptstyle p_{n-1}} \\ \hat{\Gamma}_0^{n-1} \supset \mathfrak{B}'_0 & \xrightarrow[p_1]{\sim} & \hat{\Gamma}_0^{n-2} \end{array}$$

and by the definition of $\mathfrak{B}'_0$, the restriction of p_n maps $\mathfrak{B}'$ into (hence onto) $\mathfrak{B}'_0$. From this and (3.2.2.3) together with the center-triviality of $\mathfrak{B}'$, it follows that $\gamma \in ker(p_n) \cap \mathfrak{B}'$. Moreover, noticing that $x_{n-1,n}, x_{n-2,n} \in \mathfrak{B}'$, by (3.2.2.1)-(3.2.2.2), we conclude that $\gamma = 1$. Thus f acts trivially on $\mathfrak{B}'$, and hence $q_1(f)$ =identity. In particular, since $x_{in} \in \mathfrak{B}'$ $(3 \le i \le n-1)$,

(3.2.2.4) $$f(x_{in}) = x_{in} \quad (3 \le i \le n-1).$$

Next we consider

$$\mathfrak{B}'' = \left\{ g \in \hat{\Gamma}_0^n \mid \begin{array}{c} gx_{13}g^{-1} = x_{13}, \quad gx_{12}g^{-1} = tx_{12}t^{-1}, \\ \exists\, t \in (ker(p_1))'\langle x_{15}, \ldots, x_{1n} \rangle \end{array} \right\}.$$

Then, for the similar reason as for $\mathfrak{B}'$, f preserves setwise $\mathfrak{B}''$. But since $q_1(f)$ is trivial, the action of f on it must be trivial. By (3.1.3), we compute

$$x_{2n}x_{13}x_{2n}^{-1} = (x_{1n}^{-1}x_{12}^{-1}x_{1n}x_{12})x_{13}(x_{12}^{-1}x_{1n}^{-1}x_{12}x_{1n});$$
$$x_{2n}x_{12}x_{2n}^{-1} = x_{1n}^{-1}x_{12}x_{1n}.$$

From this together with (3.1.3.4), we see that

$$x_{1n}x_{2n}x_{1n}^{-1} = (x_{1n}^{-1}x_{12}^{-1}x_{1n}x_{12})^{-1}x_{2n} \in \mathfrak{B}'' \text{ is fixed by } f. \tag{3.2.2.5}$$

On the other hand, it follows from (3.2.2.4) and (3.1.3.6) that

$$x_{1n}x_{2n} = (x_{3n}\dots x_{n-1,n})^{-1} \text{ is also fixed by } f. \tag{3.2.2.6}$$

Thus, by (3.2.2.4)-(3.2.2.6), we conclude that f acts trivially on $ker(p_n)$. Since $\hat{\Gamma}_0^n = ker(p_n) \rtimes \mathfrak{B}$, this completes the proof of Lemma (3.2.2). □

Remark. When $\mathfrak{C} = \mathfrak{C}_l$ (l: a prime), Ihara [19] proved a stronger result that

$$\bar{q}_\nu : Out^\flat\Gamma_0^n \to Out^\flat\Gamma_0^{n-1}$$

is already injective ($1 \le \nu \le n$).

We shall apply Lemma (3.2.2) to Galois compatible automorphisms of $\pi_1^{\mathfrak{C}}(M_{0,n})$. Let

$$\Phi_n = \Phi_{M_{0,n}}^{\mathfrak{C}} : Aut_k(M_{0,n}) \to E_k^{\mathfrak{C}}(M_{0,n})$$

be the canonical homomorphism introduced in §0. By Theorem (3.1.13), we have a homomorphism

$$\Psi_n : E_k^{\mathfrak{C}}(M_{0,n}) \to Aut_k(M_{0,n})$$

such that the restriction of any element of $ker(\Psi_n)$ to $\hat{\Gamma}_0^n$ belongs to $Out^\flat(\hat{\Gamma}_0^n)$. Let $U_k^{\mathfrak{C}}(M_{0,n})$ denote the kernel of Ψ_n. Then since $E_k^{\mathfrak{C}}(M_{0,n})$ is identified with $Out_{G_k}\hat{\Gamma}_0^n$ by (1.5.7), $U_k^{\mathfrak{C}}(M_{0,n})$ is isomorphic to the centralizer of the Galois image in $Out^\flat(\hat{\Gamma}_0^n)$. On the other hand, the exterior Galois representation $\varphi_{0,n} : G_k \to Out\hat{\Gamma}_0^n$ also has its image in $Out^\flat(\hat{\Gamma}_0^n)$, and satisfies the compatibility condition $\varphi_{0,n-1} = q_\nu \circ \varphi_{0,n}$ for every $1 \le \nu \le n$. Therefore Lemma (3.2.2) implies the following

Corollary (3.2.3). *Under the same assumption of Lemma (3.2.2), we have an injective homomorphism* $U_k^{\mathfrak{C}}(M_{0,n}) \to U_k^{\mathfrak{C}}(M_{0,n-1}) \times U_k^{\mathfrak{C}}(M_{0,n-1})$.

Remark. In the above discussion, the fact that $Aut_k(M_{0,n}) \cong S_n$ for $n \geq 5$ ([45],[29]) is not used yet. Using this fact, we can conclude at once that Ψ_n gives an inverse of Φ_n with $\Psi_n \circ \Phi_n = 1$ and that $Aut_k(M_{0,n})$ is embedded into $E_k^{\mathfrak{C}}(M_{0,n})$. In the proof of the following theorem, we will admit this fact as in §0, but actually we do not need it for the result that $E_k^{(l)}(M_{0,n}) \cong S_n$ for $n \geq 5$. In fact, from this latter result we can compute $Aut_k(M_{0,n})$ conversely as in [34] §5.

Now we are in a position to prove Theorem A.

Theorem A. *If l is an odd prime, then $Out\pi_1^{(l)}(M_{0,n})$ is finite, and the homomorphism*

$$\Phi^{(l)}_{M_{0,n}} : Aut_k M_{0,n} \to E_k^{(l)}(M_{0,n})$$

gives a bijection ($n \geq 4$). Moreover, If $\mathit{\Gamma}_0^{n,pro-l}$ denotes the pro-l completion of $\mathit{\Gamma}_0^n$, then the canonical exterior representation

$$\varphi^{(l)}_{0,n} : G_k \to Out\mathit{\Gamma}_0^{n,pro-l}$$

induced from the variety $M_{0,n}$ over k has image whose centralizer is isomorphic to S_3 when $n = 4$, and to S_n when $n \geq 5$.

Proof. By (1.5.7), (1.6.3), we have only to show the bijectivity of $\Phi^{(l)}_{M_{0,n}}$ for $n \geq 4$ (l: an odd prime). For this it suffices to show that $U_k^{\mathfrak{C}}(M_{0,n}) = \{1\}$ for $\mathfrak{C} = \mathfrak{C}_l$. But by Corollary (3.2.3), we are reduced to the case of $M_{0,4} = \mathbf{P}^1 - \{0, 1, \infty\}$ which was dealt in [31]. (See also 2.2) □

§4. Lie variants

4.1. Graded automorphisms

We denote the lower central series of a group $\mathit{\Gamma}$ by $\mathit{\Gamma} = \mathit{\Gamma}(1) \supset \mathit{\Gamma}(2) \supset \dots$, and the associated graded Lie algebra by

$$gr\mathit{\Gamma} = \bigoplus_{i=1}^{\infty} gr_i \mathit{\Gamma}.$$

Each graded piece $gr_i\Gamma$ is the quotient abelian group $\Gamma(i)/\Gamma(i+1)$, and the Lie bracket $[X,Y] \in gr_{i+j}\Gamma$ of $X \in gr_i\Gamma$ and $Y \in gr_j\Gamma$ is defined by

$$[X,Y] = xyx^{-1}y^{-1} \quad mod\, \Gamma(i+j+1)$$

where $x \in \Gamma(i), y \in \Gamma(j)$ are representatives of X, Y respectively.

The notations being as in (3.1.1)∼(3.1.3), we consider the discrete group $\Gamma_0^n = \pi_1(M_{0,n}(\mathbb{C}), a)$ for $n \geq 3$, and let X_{ij} denote the image of $A_{ij} \in \Gamma_0^n$ in $gr_1\Gamma_0^n$.

PROPOSITION (4.1.1) (Kohno/Hain; in this form, see Ihara[19] 3.1). *The Lie algebra $gr\Gamma_0^n$ has the following presentation:*

$$\textit{generators:} \qquad X_{ij} \quad (1 \leq i,j \leq n),$$

$$\textit{relations:} \begin{cases} X_{ii} = 0 & (1 \leq i \leq n), \\ X_{ij} = X_{ji} & (1 \leq i,j \leq n), \\ \sum_{j=1}^{n} X_{ij} = 0 & (1 \leq i \leq n), \\ [X_{ij}, X_{rs}] = 0, & \textit{if } \{i,j\} \cap \{r,s\} = \emptyset. \end{cases}$$

We shall denote by $p_S : \Gamma_0^n \to \Gamma_0^m$ the canonical homomorphism induced from the morphism $f_S : M_{0,n}(\mathbb{C}) \to M_{0,m}(\mathbb{C})$ (3.1.2), and call it the forgetful homomorphism associated to $S \subset \{1,\ldots,n\}$. Each p_S induces a graded Lie algebra homomorphism

$$grp_S \otimes K : gr\Gamma_0^n \otimes K \to gr\Gamma_0^m \otimes K$$

for any commutative ring K. It follows from Lemma 3.1.1 of [19] and the presentation in (3.1.3) that $ker(grp_S \otimes K) \cong gr(kerp_S) \otimes K$. In particular when $S = \{\nu\}$, $ker(grp_\nu \otimes K)$ is isomorphic to the free Lie algebra generated by $gr_1(kerp_\nu) \otimes K$.

Observe that the product group $S_n \times K^\times$ acts on $gr_1\Gamma_0^n \otimes K$ by

$$(\sigma,\lambda)(X_{ij}) = \lambda \cdot X_{\sigma(i)\sigma(j)} \quad (\sigma \in S_n,\, \lambda \in K^\times),$$

and that these operations extend naturally to graded automorphisms of the Lie algebra $gr\mathit{\Gamma}_0^n\otimes K$. The purpose of this subsection is to verify the following lemma expected by P.Deligne.

Lemma (4.1.2). *Let K be a field. Then the group of the graded automorphisms of the graded Lie algebra $gr\mathit{\Gamma}_0^n\otimes K$ is isomorphic to $S_n\times K^\times$ when $n\geq 5$.*

We can prove this lemma by modifying combinatorial arguments developed in §3 in a suitable way in the context. But in the present fully linearized situation, there is a more natural "characterization of infinity" due to P.Deligne which makes the proof of the lemma very simple. So, in the following, we shall take the latter line for the proof of Lemma (4.1.2).

Lemma (4.1.3) (P.Deligne). *Let X be an element of $gr_1\mathit{\Gamma}_0^n\otimes K$ ($n\geq 5$), $C(X)$ the centralizer of X in $gr\mathit{\Gamma}_0^n\otimes K$, $C_1(X)=C(X)\cap gr_1\mathit{\Gamma}_0^n\otimes K$. Then the following two conditions on X are equivalent:*
(a) $dim\, C_1(X)\geq\frac{(n-1)(n-4)}{2}+1$;
(b) X is a scalar multiple of one of the X_{ij} ($1\leq i<j\leq n$).

Proof. We first notice that $dim\, gr_1\mathit{\Gamma}_0^n\otimes K=n(n-3)/2$. As was proved by Ihara [19] Proposition 3.3.1(ii), (b) implies the equality in (a). So we let X satisfy (a), and argue by induction on $n\geq 5$. Let us denote $grp_\nu\otimes K: gr\mathit{\Gamma}_0^n\otimes K\to gr\mathit{\Gamma}_0^{n-1}\otimes K$ simply by p_ν. For $X\neq 0$, we can always find ν ($1\leq\nu\leq n$) such that $p_\nu(X)\neq 0$. Therefore, by symmetry, we may assume $p_n(X)\neq 0$.

Step 1: $n=5$. By assumption, we have $dim\, C_1(X)\geq 3$ with $p_5(X)\neq 0$. Since $gr\mathit{\Gamma}_0^4$ is a free Lie algebra of rank 2, there are no rank 2 commutative subspaces in $gr_1\mathit{\Gamma}_0^4\otimes K$. Therefore $dim\, C_1(X)\cap kerp_5=2$. This means that the linear homomorphism $ad(X): gr_1(kerp_5)\to gr_2(kerp_5)$ has exactly 2-dimensional kernel. Let

$$\mathfrak{B}=\{Y\in gr_1\mathit{\Gamma}_0^5\otimes K|\,[Y,X_{45}]=0,[Y,X_{35}]=[T,X_{35}]\ \exists\, T\in KX_{25}\}.$$

It is easy to see that $\mathfrak{B}\cap kerp_5=0$, and that p_5 gives an isomorphism $\mathfrak{B}\cong gr_1\mathit{\Gamma}_0^4\otimes K$. We choose free generators (X_1,X_2,X_3) of $kerp_5$ and basis (Y_1,Y_2) of $\mathfrak{B}$ as follows: $X_1=X_{25},X_2=X_{35},X_3=X_{45},Y_1=X_{23},Y_2=$

$X_{12}+X_{23}$. Then we have

$$[Y_1,X_1]=[X_1,X_2],\ [Y_1,X_2]=-[X_1,X_2],\ [Y_1,X_3]=0,$$
$$[Y_2,X_1]=[X_3,X_1],\ [Y_2,X_2]=-[X_1,X_2],\ [Y_2,X_3]=0.$$

Put $X=aY_1+bY_2+cX_1+dX_2+eX_3$ $(a,b,c,d,e\in K)$. Then the linear homomorphism $ad(X): gr_1(kerp_5)\to gr_2(kerp_5)$ is expressed as follows:

$$ad(X)(X_1,X_2,X_3)$$
$$=([X_1,X_2],[X_2,X_3],[X_3,X_1])\begin{pmatrix} a-d & -a-b+c & 0\\ 0 & -e & d\\ b+e & 0 & -c\end{pmatrix}.$$

When $a\neq 0$, we may assume $a=1$. Then the above condition on the degeneration of $ad(X)$ gives four solutions:

$$(a,b,c,d,e)=(1,0,0,0,0),(1,-1,0,0,0),(1,0,1,1,0),(1,-1,0,1,1),$$

which correspond to $X=X_{23},-X_{12},X_{14},-X_{34}$ respectively. (In the computation, we use equations like $X_{12}+X_{23}+X_{13}=X_{45}$ which are derived easily from (3.1.3.6) and (3.1.3.7).) When $a=0$, we may assume $b=1$ as $p_5(X)\neq 0$. In this case we obtain two solutions:

$$(a,b,c,d,e)=(0,1,1,0,0),(0,1,0,0,-1),$$

which give $X=-X_{24},-X_{13}$ respectively.

Step 2: $n\geq 6$. We consider the exact sequence

$$0\to C_1(X)\cap kerp_n\to C_1(X)\to C_1(p_n(X)).$$

Case 1: $dim\, C_1(p_n(X))\leq (n-2)(n-5)/2$.
In this case, $dim(C_1(X)\cap kerp_n)\geq n-2=dim(kerp_n)$. Therefore $C_1(X)\supset kerp_n$. This is impossible: we may express X as $\sum_{1\leqslant i<j<n}a_{ij}X_{ij}$ $(a_{ij}\in K)$. Then $[X_{in},\sum_{j\neq i,n}a_{ij}X_{jn}]=0$. (Use $[X_{in},X_{ij}]=[X_{jn},X_{in}]$.) As $gr(kerp_n)$ is free of rank $n-2$, we get all $a_{ij}=0$, i.e., contradiction.

Case 2: $dim\, C_1(p_n(X))>(n-2)(n-5)/2$.
In this case, we may apply the induction hypothesis to $p_n(X)(\neq 0)$, and may

assume $p_n(X) = X_{rs}$ for some $1 \le r < s \le n-1$. Then $dim\, p_n(C_1(X)) \le dim\, C_1(p_n(X)) = 1 + (n-2)(n-5)/2$. From this we get (*): $dim(C_1(X) \cap ker p_n) \ge n-3$. Let us put $X = X_{rs} + \sum_{k=1}^{n-1} a_k X_{kn}$ ($a_k \in K$), and choose three indices l_i ($i = 1, 2, 3$) from $\{1, ..., n-1\} \setminus \{r, s\}$. By (*), there is a linear combination Y_{ij} of $X_{l_i n}$ and $X_{l_j n}$ contained in $C_1(X) \setminus \{0\}$ for every $(i, j) = (1, 2), (2, 3), (3, 1)$. Then $[X, Y_{ij}] = [\sum_{k=1}^{n-1} a_k X_{kn}, Y_{ij}] = 0$, from which it follows that $\sum_{k=1}^{n-1} a_k X_{kn}$ is a scalar multiple of Y_{ij}. Since $KY_{12} \cap KY_{23} \cap KY_{31} = 0$, we conclude $X = X_{rs}$. □

We are now in a position to prove Lemma (4.1.2).

Proof of Lemma (4.1.2). Let f be an arbitrary graded Lie algebra automorphism of $gr\Gamma_0^n \otimes K$ ($n \ge 5$). By Lemma (4.1.3), f permutes the lines generated by X_{ij} ($1 \le i < j \le n$). Considering the commutation relations: $[X_{ij}, X_{rs}] = 0(\{i, j\} \cap \{r, s\} = \emptyset)$, we find that there exists a permutation $\sigma \in S_n$ such that $f(X_{ij}) = \lambda_{ij} X_{\sigma(i)\sigma(j)}$ for some $\lambda_{ij} \ne 0$ ($1 \le i < j \le n$). But since f preserves the relations $\sum_{1 \le j \le n} X_{ij} = 0$ ($1 \le i \le n$), all λ_{ij} must coincide with a constant $\lambda \in K^\times$. This completes our proof of the lemma. □

4.2. Pure sphere braid Lie algebras

In this subsection, we show that the pure sphere braid Lie algebras with n strings ($n \ge 5$) have also Galois rigidity properties, along the lines suggested by P.Deligne. The synthetic reference for the formulation of this section is [8]. In the following, we fix a prime l, and denote by Γ^{pro-l} the pro-l completion of a discrete group Γ.

(4.2.1) Let us begin by considering the quotient nilpotent group $\Gamma_0^n/\Gamma_0^n(N)$ for $N \ge 1$. This is obviously finitely generated, and has no torsion for $gr\Gamma_0^n$ is torsion-free. Therefore $\Gamma_0^n/\Gamma_0^n(N)$ is residually finite-l ([15] Theorem 2.1). It follows that the pro-l completion of $\Gamma_0^n/\Gamma_0^n(N)$ is isomorphic to $\Gamma_0^{n,pro-l}/\Gamma_0^{n,pro-l}(N)$, where $\{\Gamma_0^{n,pro-l}(N)\}_{N=1}^{\infty}$ denotes the lower central series of the pro-l group $\Gamma_0^{n,pro-l}$. Since $\Gamma_0^{n,pro-l}(N)$ is a characteristic subgroup of $\Gamma_0^{n,pro-l}$, we have a canonical representation

$$\varphi_{n,N}^{(l)} : G_k \to Out(\Gamma_0^{n,pro-l}/\Gamma_0^{n,pro-l}(N)).$$

As is well known, $(\Gamma_0^n/\Gamma_0^n(N))^{pro-l}$ is an l-adic analytic group (e.g. [24] Proposition 2.6), the Lie algebra of which we denote by $\mathcal{L}_l^{[N]}$ (or $\mathcal{L}_l^{[N]}(\Gamma_0^n)$).

Then $\mathcal{L}_l^{[N]}$ is a nilpotent Lie algebra over $\mathbb{Q}_l$ on which the exterior Galois action $\varphi_{n,N}^{(l)}$ defines a weight filtration $\{W.\}$ via the Frobenius eigenvalues.

(4.2.2) On the other hand, we have a rational mixed Hodge structure $\{W., F^\cdot\}$ on the Malcev Lie algebra $L_{\mathbb{Q}}^{[N]}$ of $\Gamma_0^n/\Gamma_0^n(N)$ and have a canonical isomorphism $\mathcal{L}_l^{[N]} \cong L_{\mathbb{Q}}^{[N]} \otimes \mathbb{Q}_l$ which preserves the weight filtration [8]. From this together with a result of D.Quillen ([38] Appendix A), we obtain

$$gr^W \mathcal{L}_l^{[N]} \cong gr^W L_{\mathbb{Q}}^{[N]} \otimes \mathbb{Q}_l \cong \bigoplus_{i=1}^{N} gr_i \Gamma_0^n \otimes \mathbb{Q}_l.$$

It follows from the Campbell-Baker-Hausdorff formula that the set

$$Int\mathcal{L}_l^{[N]} := \{\exp ad(X) \mid X \in \mathcal{L}_l^{[N]}\}$$

forms a group of automorphisms of $\mathcal{L}_l^{[N]}$. Moreover we see that $\{\mathcal{L}_l^{[N]}\}_{N=1}^{\infty}$ (resp. $\{Int\mathcal{L}_l^{[N]}\}_{N=1}^{\infty}$) gives a surjective projective system of Lie algebras (resp. of unipotent algebraic groups). Let $\mathcal{L}_l (= \mathcal{L}_l(\Gamma_0^n)) := \varprojlim_N \mathcal{L}_l^{[N]}$ and $Int\mathcal{L}_l := \varprojlim_N Int\mathcal{L}_l^{[N]}$. Then $Int\mathcal{L}_l$ forms a normal subgroup of $Aut\mathcal{L}_l$. If we denote the quotient group by $Out\mathcal{L}_l(\Gamma_0^n)$, we obtain a new Galois representation

$$\varphi_n^{Lie} : G_k \to Out\mathcal{L}_l(\Gamma_0^n).$$

induced from the family of $\varphi_{n,N}^{(l)}$ $(1 \le N < \infty)$.

The Lie version of our Galois rigidity can be stated as follows:

THEOREM B. *Assume that l is an odd prime. Then the centralizer of the Galois image $\varphi_n^{Lie}(G_k)$ in $Out\mathcal{L}_l(\Gamma_0^n)$ is isomorphic to the symmetric group S_n when $n \ge 5$.*

PROOF. We first take a system of Galois representations

$$\phi^n : G_k \to Aut\Gamma_0^{n,pro-l} \quad (n \ge 4)$$

such that
1) each ϕ^n is a lift of $\varphi_n^{(l)} : G_k \to Out\Gamma_0^{n,pro-l}$ $(n \ge 4)$ unramified outside l;
2) ϕ^n and ϕ^{n-1} are compatible with $p_n : \Gamma_0^{n,pro-l} \to \Gamma_0^{n-1,pro-l}$ $(n \ge 5)$,

i.e., $\phi^{n-1}(\sigma)\circ p_n = p_n \circ \phi^n(\sigma)$ $(\sigma \in G_k)$;
3) the image of ϕ^4 is contained in

$$\left\{ g \in Aut\Gamma_0^{4,pro-l} \mid \begin{array}{c} \exists\, s \in \Gamma_0^{4,pro-l},\ \exists\, t \in \Gamma_0^{4,pro-l}(2),\ \exists\, c \in \mathbb{Z}_l^\times\ s.t. \\ g(x_{14}) = s x_{14}^c s^{-1},\ g(x_{24}) = t x_{24}^c t^{-1},\ g(x_{34}) = x_{34}^c \end{array} \right\}.$$

The existence of such a system is easy to see, for example by Belyi's group theoretical method, or more directly by Deligne's tangential base points. The Galois representation $G_k \to Aut\mathcal{L}_l(\Gamma_0^n)$ induced from ϕ^n is also denoted by the same symbol.

Fix a prime $p \nmid l$ of k with absolute norm $\mathfrak{N}p$, and choose $\sigma_p \in G_k$ with $\phi^n(\sigma_p)$ a Frobenius image over p. Let us denote $\phi^n(\sigma_p)$ simply by ϕ_p (for all $n \geq 4$). Then ϕ_p respects the weight filtration in $\mathcal{L}_l$ $(= \mathcal{L}_l(\Gamma_0^n))$, and acts on graded pieces via multiplication by distinct positive powers of $\mathfrak{N}p$. Therefore the action of ϕ_p on $\mathcal{L}_l$ is semisimple, and gives "the weight *graduation* by ϕ_p" , i.e., if $\mathcal{L}_{l,N}(= \mathcal{L}_{l,N}(\Gamma_0^n)) = \{Z \in \mathcal{L}_l \mid \phi_p(Z) = (\mathfrak{N}p)^N Z\}$, then $\mathcal{L}_l = \prod_{N=1}^\infty \mathcal{L}_{l,N}$ with $\bigoplus_{n=1}^\infty \mathcal{L}_{l,N}$ a dense Lie subalgebra of $\mathcal{L}_l$ isomorphic to $gr\Gamma_0^n \otimes \mathbb{Q}_l$.

We recall here a standard fact about linear unipotent algebraic groups.

LEMMA (4.2.3) (A.Borel). *Let U be a connected unipotent subgroup of a linear algebraic group G, s a semisimple element of G normalizing U with trivial centralizer in U. Then for each $u' \in U$, there exists a unique $u \in U$ such that $su' = usu^{-1}$.*

PROOF. See [17] Theorem 18.3(b). □

We continue the proof of Theorem B. Let us take an arbitrary automorphism f of $\mathcal{L}_l(\Gamma_0^n)$ $(n \geq 5)$ whose image in $Out\mathcal{L}_l$ centralizes $\varphi_n^{Lie}(G_k)$. Then there exists $u' \in Int\mathcal{L}_l$ such that $\phi_p f = f\phi_p u'$. If $\phi_{p,N}$ and u'_N denote the operators on $\mathcal{L}_l^{[N]}$ induced from ϕ_p and u' respectively, then, applying the above fact to the unipotent subgroup $Int\mathcal{L}_l^{[N]}$, we obtain a unique $u_N \in Int\mathcal{L}_l^{[N]}$ such that $\phi_{p,N}u'_N = u_N\phi_{p,N}u_N^{-1}$. The uniqueness assertion insures the compatibility of the sequence $(u_N)_{N=1}^\infty$; hence yields an element $u \in Int\mathcal{L}_l$ with $\phi_p u' = u\phi_p u^{-1}$. From this we obtain $fu\phi_p = \phi_p fu$. Thus fu induces a graded automorphism of the graded Lie algebra $\bigoplus_{N=1}^\infty \mathcal{L}_{l,N}$. Let $(\tau, a_f) \in S_n \times \mathbb{Q}_l^\times$ be the corresponding pair by Lemma (4.1.2) to fu. Then, it remains only to show that $a_f = 1$. Let $h_\tau \in Aut\mathcal{L}_l$ be a representative of an element of $Out\mathcal{L}_l(\Gamma_0^n)$ coming from a k-automorphism of $M_{0,n}$ corresponding to the permutation $\tau \in S_n$. Since apriori h_τ centralizes $\varphi_n^{Lie}(G_k)$ in $Out\mathcal{L}_l(\Gamma_0^n)$, we may apply the same argument above to h_τ (instead of f), and may assume after suitable replacement that h_τ commutes with ϕ_p in $Aut\mathcal{L}_l(\Gamma_0^n)$. Put $f' = fuh_\tau^{-1}$. Then f' acts on each $\mathcal{L}_{l,N} \subset \mathcal{L}_l(\Gamma_0^n)$ by multiplication by a_f^N, and therefore preserves every graded ideal of $\bigoplus_N \mathcal{L}_{l,N}$. As the Galois equivariant homomorphism $\mathcal{L}_l(\Gamma_0^n) \to \mathcal{L}_l(\Gamma_0^4)$ respects the weight graduation by ϕ_p, f' induces a graded scalar automorphism f'_4 of $\mathcal{L}_l(\Gamma_0^4)$ by powers of a_f, with image in $Out\mathcal{L}_l(\Gamma_0^4)$ lying in the centralizer of the Galois image $\varphi_4^{Lie}(G_k)$.

On the other hand, we know that there exist many nontrivial unipotent elements u_4 in the Galois image $\phi^4(G_k) \subset Aut\mathcal{L}_l(\Gamma_0^4)$ coming from cyclotomic elements in K-theory. For any of such u_4, we have $f'_4 u_4 = u_4 f'_4 u'$ for some $u' \in Int\mathcal{L}_l(\Gamma_0^4)$. If $a_f \in \mathbb{Q}_l^\times$ is nontorsion, then the above Borel's fact yields $u \in Int\mathcal{L}_l(\Gamma_0^4)$ with $f'_4(u_4 u) = (u_4 u) f'_4$. But since $Int\mathcal{L}_l(\Gamma_0^4) \cap \phi^4(G_k) = \{1\}$ (c.f. [De] 16.29), $u_4 u$ has to be a nontrivial unipotent element. From this, we see a_f is torsion, and get a contradiction.

To eliminate the possibility of a_f being nontrivial torsion, we need more refined argument. In the following, we denote $\mathcal{L}_l = \mathcal{L}_l(\Gamma_0^4)$, and let $\phi_\sigma = \phi^4(\sigma)$ for $\sigma \in G_k$. Choose an odd integer $m \geq 3$ prime to $l-1$, and let $\sigma \in G_k$ be such that $\phi_\sigma - 1$ conveys $\mathcal{L}_l (= W_{-2}\mathcal{L}_l)$ into $W_{-2m-2}\mathcal{L}_l$ but not into $W_{-2m-4}\mathcal{L}_l$. (The existence of such σ follows from the nonvanishing of the cyclotomic element in $H^1(\mathbb{Z}[1/l], \mathbb{Z}_l(m))$ due to Soule, Schneider. See e.g. [20],[8]) Then we have $U \in \mathcal{L}_l$ such that

$$\phi_\sigma f'_4 = f'_4 \phi_\sigma \exp(ad\, U).$$

If we consider this equation modulo $W_{-2m-2}\mathcal{L}_l$, we see $U \in W_{-2m}\mathcal{L}_l$. Next we consider it modulo $\mathcal{M} = W_{-2m-4}\mathcal{L}_l$, and apply it to any element Y of $\mathcal{L}_{l,1}(\Gamma_0^4)$. Then, noticing that the action of f'_4 on $\mathcal{L}_{l,N}$ is via a_f^N-multiplication, and observing that $\phi_\sigma - 1 \equiv \mathrm{Log}\phi_\sigma$ on $\mathcal{L}_l/\mathcal{M}$, we obtain

$$(a_f - a_f^{m+1})\mathrm{Log}\phi_\sigma(Y) \equiv a_f^{m+1}(ad\, U)(Y) \mod \mathcal{M}.$$

Since $\mathcal{L}_l^{[m+2]} = \mathcal{L}_l/\mathcal{M}$ is generated by the image of $\mathcal{L}_{l,1}$ in $\mathcal{L}_l^{[m+2]}$, we conclude $(a_f - a_f^{m+1})\mathrm{Log}\phi_\sigma$ and $a_f^{m+1}(ad\, U)$ induce the same derivation on $\mathcal{L}_l^{[m+2]}$.

We recall here that $\mathcal{L}_l^{[m+2]}$ is the Malcev Lie algebra of $\varGamma_0^4/\varGamma_0^4(m+2)$ tensored by $\mathbb{Q}_l$, and has special generators $X_{34}=\log x_{34}$, $X_{24}=\log x_{24}$ such that

$$(1)\,\mathrm{Log}\phi_\sigma(X_{34})=0;\quad (2)\,\mathrm{Log}\phi_\sigma(X_{24})\not\equiv 0\mod \mathcal{M}.$$

Since the centralizer of X_{34} in $\mathcal{L}_l^{[m+2]}$ is easily seen to be $\mathbb{Q}_l X_{34}\oplus W_{-2m-2}$, we obtain $ad(U)=0$ on $\mathcal{L}_l^{[m+2]}$ by (1). Therefore $(a_f-a_f^{m+1})\mathrm{Log}\phi_\sigma$ is also zero derivation of $\mathcal{L}_l/\mathcal{M}$. This together with (2) implies $a_f=1$, as m is chosen to be prime to $l-1$. The proof of Theorem B is thus completed. □

(4.2.4) Let $\mathcal{G}_l^{[N]}(\varGamma_0^n)$ be the group of the group-like elements in the Hopf algebra associated with $\mathcal{L}_l^{[N]}(\varGamma_0^n)$ $(N\ge 1)$, and let $\mathcal{G}_l(\varGamma_0^n)=\varprojlim_N \mathcal{G}_l^{[N]}(\varGamma_0^n)$ (See [36] Appendix A). Then, since $\mathcal{G}_l^{[N]}(\varGamma_0^n)$ is isomorphic to the $\mathbb{Q}_l$-valued points of the unipotent algebraic envelope of $\varGamma_0^n/\varGamma_0^n(N)$ ([8] 9.5), $\varGamma_0^{n,pro-l}$ is identified with a subgroup of $\mathcal{G}_l(\varGamma_0^n)$. In particular, there is a canonical embedding

$$Aut\varGamma_0^{n,pro-l}\hookrightarrow Aut\mathcal{G}_l(\varGamma_0^n)(=Aut\mathcal{L}_l(\varGamma_0^n)).$$

One can expect that if $Inn\varGamma_0^{n,pro-l}$ is not so different from $Int\mathcal{L}_l(\varGamma_0^n)\cap Aut\varGamma_0^{n,pro-l}$, then Theorem A will follow from Theorem B when $n\ge 5$. We do not here try to estimate this possible gap directly. Instead, we shall sketch a method of deducing Theorem A for $n\ge 5$ from Theorem B *with the help of Theorem (3.1.13).* Let $\gamma\in\mathcal{G}_l(\varGamma_0^n)$ be such that $inn(\gamma)$ preserves $\varGamma_0^{n,pro-l}\subset\mathcal{G}_l(\varGamma_0^n)$, and assume that the image of $inn(\gamma)$ in $Out\varGamma_0^{n,pro-l}$ commutes with the image of G_k $(n\ge 5)$. By Theorem C, it suffices to show that γ lies actually in $\varGamma_0^{n,pro-l}$. Since the group extension (Γ_0^n):

$$1\to\Pi_{0,n-1}\to\varGamma_0^n\to\varGamma_0^{n-1}\to 1$$

has a splitting homomorphism $\varGamma_0^{n-1}\to\varGamma_0^n$, and since the action of $\varGamma_0^{n-1}$ on $\Pi_{0,n-1}/[\Pi_{0,n-1},\Pi_{0,n-1}]$ is trivial, we have an exact sequence

$$1\to\Pi_{0,n-1}/\Pi_{0,n-1}(N)\to\varGamma_0^n/\varGamma_0^n(N)\to\varGamma_0^{n-1}/\varGamma_0^{n-1}(N)\to 1$$

for each $N\ge 1$ (cf. [19] Proposition 3.1.1). Then, by the exactness of the Malcev completion functor, we obtain from the above a surjective projective system of exact sequences of Malcev Lie algebras over $\mathbb{Q}$. Tensoring them with $\mathbb{Q}_l$, and taking $\varprojlim_N$, we get the following two exact sequences

$$0 \to \mathcal{L}_l(\Pi_{0,n-1}) \to \mathcal{L}_l(\Gamma_0^n) \to \mathcal{L}_l(\Gamma_0^{n-1}) \to 1,$$
$$0 \to \mathcal{G}_l(\Pi_{0,n-1}) \to \mathcal{G}_l(\Gamma_0^n) \to \mathcal{G}_l(\Gamma_0^{n-1}) \to 1,$$

where $\mathcal{L}_l(\Pi_{0,n-1})$ is the projective limit of the Lie algebras $\mathcal{L}_l^{[N]}(\Pi_{0,n-1})$ associated with the l-adic analytic groups $\Pi_{0,n-1}^{pro-l}/\Pi_{0,n-1}^{pro-l}(N)$ $(N \geq 1)$, and $\mathcal{G}_l(\Pi_{0,n-1})$ is the group of the group-like elements in the complete Hopf algebra associated with $\mathcal{L}_l(\Pi_{0,n-1})$. By Theorem (3.1.13), $inn(\gamma)$ preserves $\mathfrak{X}_{ij}$ for each $1 \leq i < j \leq n$. Therefore, (through some inductive arguments) we are reduced to the following simple

PROPOSITION (4.2.5). *Let $\Pi_{0,n}$ be the free group with free generators $x_1, \ldots, x_{n-1}$ $(n \geq 3)$, and let $\gamma \in \mathcal{G}_l(\Pi_{0,n})$ satisfy the following two conditions:*
(1) $inn(\gamma)$ preserves $\Pi_{0,n}^{pro-l} \subset \mathcal{G}_l(\Pi_{0,n})$;
(2) $inn(\gamma)(x_1) = \gamma x_1 \gamma^{-1}$ is conjugate to x_1 in $\Pi_{0,n}^{pro-l}$.
Then $\gamma \in \Pi_{0,n}^{pro-l}$.

PROOF. Let $inn(\gamma)(x_1) = t x_1 t^{-1}$ $(t \in \Pi_{0,n}^{pro-l})$. Replacing γ by $t^{-1}\gamma$, we may assume that γ commutes with x_1. Since the centralizer of $\log x_1$ in $\mathcal{L}_l(\Pi_{0,n})$ is $\mathbb{Q}_l \log x_1$, we get $\log \gamma = a \log x_1$ for some $a \in \mathbb{Q}_l$. Then, from the Campbell-Baker-Hausdorff formula, it follows that

$$inn(\gamma)(x_2)x_2^{-1} = [\gamma, x_2] = a \cdot [x_1, x_2]$$

in $gr_2\mathcal{G}_l(\Pi_{0,n})$. But since $[x_1, x_2]$ is a member of a $\mathbb{Z}_l$-basis of $gr_2\Pi_{0,n}^{pro-l}$, we get $a \in \mathbb{Z}_l$. Therefore $\gamma = x_1^a \in \Pi_{0,n}^{pro-l}$. □

Appendix. Generalization of the Belyi lifting to $M_{0,5}$

In this note, we shall follow the notations introduced in §3 with fixing a full class of finite groups $\mathfrak{C}$.

We first recall the case of $M_{0,4}$. Let $X = M_{0,4} = \mathbf{P}^1 - \{0, 1, \infty\}$ be defined over a number field k, and let $p_{0,4} : \pi_1^{\mathfrak{C}}(X) \to G_k$ be the canonical surjection. For convinience, we put $x = x_{14}, y = x_{24}, z = x_{34}$ to present $\hat{\Gamma}_0^4 = \langle x, y, z | xyz = 1 \rangle$. The Belyi lifting for $M_{0,4}$ is defined to be a homomorphism $\beta : G_k \to \pi_1^{\mathfrak{C}}(X)$ with $p_{0,4} \circ \beta = id$ characterized by the following properties of the images $\beta_\sigma = \beta(\sigma)$ for $\sigma \in G_k$:

$$\text{(A1)} \qquad \beta_\sigma z \beta_\sigma^{-1} = z^{a_\sigma} \qquad \exists a_\sigma \in \mathbb{Z}_{\mathfrak{C}}^\times;$$

$$\text{(A2)} \qquad \beta_\sigma y \beta_\sigma^{-1} = t_\sigma y^{a_\sigma} t_\sigma^{-1} \quad \exists t_\sigma \in [\hat{\Gamma}_0^4, \hat{\Gamma}_0^4];$$

$$\text{(A3)} \qquad \beta_\sigma x \beta_\sigma^{-1} = s_\sigma x^{a_\sigma} s_\sigma^{-1} \quad \exists s_\sigma \in \hat{\Gamma}_0^4.$$

It is easy to see that a_σ and $t_\sigma \in [\hat{\Gamma}_0^4, \hat{\Gamma}_0^4]$ are uniquely determined for $\sigma \in G_k$ by the above conditions (A1), (A2), and that if we impose the conditon $s_\sigma \equiv y^{\frac{a_\sigma - 1}{2}} \bmod [\hat{\Gamma}_0^4, \hat{\Gamma}_0^4]$, then s_σ is also determined uniquely for $\sigma \in G_k$ by (A3) ([18] Proposition 4). In addition, we know a_σ is the cyclotomic character of $\sigma \in G_k$. As $\hat{\Gamma}_0^4$ is a free pro-$\mathfrak{C}$ group with free generators y and z, t_σ and s_σ are considered to be "pro-words" in noncommutative indeterminates y and z, and written as $t_\sigma = t_\sigma(y, z), s_\sigma = s_\sigma(y, z)$.

Let

$$\Phi_X^{\mathfrak{C}} : Aut_k X \to \frac{Aut_{G_k} \pi_1^{\mathfrak{C}}(X)}{Inn \hat{\Gamma}_0^4}$$

be the canonical map introduced in §0. After suitably lifting the image of an involution (resp. a 3-cyclic) of $Aut_k X \cong S_3$, we obtain Galois compatible automorphisms $f, g \in Aut_{G_k} \pi_1^{\mathfrak{C}}(X)$ such that

$$\text{(A4)} \qquad f(x) = z^{-1} y z, \quad f(y) = x, \quad f(z) = z;$$

$$\text{(A5)} \qquad g(x) = y, \quad g(y) = z, \quad g(z) = x.$$

Applying f to (A1)-(A3), and making suitable transposition, we obtain

$$\text{(A6)} \qquad z^{\frac{1-a_\sigma}{2}} f(\beta_\sigma) z f(\beta_\sigma)^{-1} z^{\frac{a_\sigma - 1}{2}} = z^{a_\sigma},$$

$$\text{(A7)} \quad z^{\frac{1-a_\sigma}{2}} f(\beta_\sigma) y f(\beta_\sigma)^{-1} z^{\frac{a_\sigma - 1}{2}}$$
$$= (z^{\frac{1+a_\sigma}{2}} s_\sigma(x, z) z^{-1} y^{\frac{a_\sigma - 1}{2}}) y^{a_\sigma} (z^{\frac{1+a_\sigma}{2}} s_\sigma(x, z) z^{-1} y^{\frac{a_\sigma - 1}{2}})^{-1},$$

(A8) $$z^{\frac{1-a_\sigma}{2}} f(\beta_\sigma) x f(\beta_\sigma)^{-1} z^{\frac{a_\sigma-1}{2}} = (z^{\frac{1-a_\sigma}{2}} t_\sigma(x,z) x^{\frac{1-a_\sigma}{2}}) x^{a_\sigma} (z^{\frac{1-a_\sigma}{2}} t_\sigma(x,z) x^{\frac{1-a_\sigma}{2}})^{-1}.$$

Comparing these with (A1)-(A3), we get the following formulae:

(A9) $$t_\sigma(y,z) = z^{\frac{a_\sigma+1}{2}} s_\sigma(x,z) z^{-1} y^{\frac{a_\sigma-1}{2}},$$

(A10) $$s_\sigma(y,z) = z^{\frac{1-a_\sigma}{2}} t_\sigma(x,z) x^{\frac{1-a_\sigma}{2}}$$

(A11) $$\beta_\sigma = z^{\frac{1-a_\sigma}{2}} f(\beta_\sigma)$$

Similarly, if we apply g to (A1)-(A3), we get

(A12) $$z^{\frac{1-a_\sigma}{2}} t_\sigma(z,x)^{-1} g(\beta_\sigma) z g(\beta_\sigma)^{-1} t_\sigma(z,x) z^{\frac{a_\sigma-1}{2}} = z^{a_\sigma},$$

(A13) $$z^{\frac{1-a_\sigma}{2}} t_\sigma(z,x)^{-1} g(\beta_\sigma) y g(\beta_\sigma)^{-1} t_\sigma(z,x) z^{\frac{a_\sigma-1}{2}} = [z^{\frac{1-a_\sigma}{2}} t_\sigma(z,x)^{-1} s_\sigma(z,x)] y^{a_\sigma} [z^{\frac{1-a_\sigma}{2}} t_\sigma(z,x)^{-1} s_\sigma(z,x)]^{-1}$$

(A14) $$z^{\frac{1-a_\sigma}{2}} t_\sigma(z,x)^{-1} g(\beta_\sigma) x g(\beta_\sigma)^{-1} t_\sigma(z,x) z^{\frac{a_\sigma-1}{2}} = [z^{\frac{1-a_\sigma}{2}} t_\sigma(z,x)^{-1} x^{\frac{1-a_\sigma}{2}}] x^{a_\sigma} [z^{\frac{1-a_\sigma}{2}} t_\sigma(z,x)^{-1} x^{\frac{1-a_\sigma}{2}}]^{-1},$$

and obtain

(A15) $$t_\sigma(y,z) = z^{\frac{1-a_\sigma}{2}} t_\sigma(z,x)^{-1} s_\sigma(z,x),$$

(A16) $$s_\sigma(y,z) = z^{\frac{1-a_\sigma}{2}} t_\sigma(z,x)^{-1} x^{\frac{1-a_\sigma}{2}},$$

(A17) $$\beta_\sigma = z^{\frac{1-a_\sigma}{2}} t_\sigma(z,x)^{-1} g(\beta_\sigma).$$

From (A10) and (A16), we see that $t = t_\sigma$ $(\sigma \in G_k)$ satisfies

(A18) $$t(y,z) = t(z,y)^{-1}.$$

If g^{-1} is applied to (A15), then $t_\sigma(x,y) = y^{(1-a_\sigma)/2} t_\sigma(y,z)^{-1} s_\sigma(y,z)$. Eliminating $s_\sigma(y,z)$ from this and (A10), we obtain the following hexagon relation for $a = a_\sigma$ and $t = t_\sigma$ $(\sigma \in G_k)$:

(A19) $$t(z,x) z^{\frac{a-1}{2}} t(y,z) y^{\frac{a-1}{2}} t(x,y) x^{\frac{a-1}{2}} = 1.$$

The purpose of this note is to show the following

THEOREM (A20). *Let $p_{0,5} : \pi_1^{\mathfrak{C}}(M_{0,5}) \to G_k$ be the canonical surjective homomorphism, and suppose that the group extension (Γ_0^5) is $\mathfrak{C}$-admissible (3.1.2). Then there exists a unique group section $\beta : G_k \to \pi_1^{\mathfrak{C}}(M_{0,5})$ of $p_{0,5}$ such that the images $\beta_\sigma = \beta(\sigma)$ for $\sigma \in G_k$ satisfy the following four conditions (A21)-(A24).*

$$\beta_\sigma x_{12} \beta_\sigma^{-1} = x_{12}^{a_\sigma}, \tag{A21}$$

$$\beta_\sigma x_{23} \beta_\sigma^{-1} = t_\sigma(x_{23}, x_{12}) x_{23}^{a_\sigma} t_\sigma(x_{23}, x_{12})^{-1}, \tag{A22}$$

$$\beta_\sigma x_{34} \beta_\sigma^{-1} = t_\sigma(x_{34}, x_{45}) x_{34}^{a_\sigma} t_\sigma(x_{34}, x_{45})^{-1}, \tag{A23}$$

$$\beta_\sigma x_{45} \beta_\sigma^{-1} = x_{45}^{a_\sigma}. \tag{A24}$$

Moreover, these β_σ satisfy also the following formula (A25):

$$\beta_\sigma x_{51} \beta_\sigma^{-1} = t_\sigma(x_{23}, x_{12}) t_\sigma(x_{51}, x_{45}) x_{51}^{a_\sigma} t_\sigma(x_{51}, x_{45})^{-1} t_\sigma(x_{23}, x_{12})^{-1}. \tag{A25}$$

It is known that the universal covering space $T_{0,5}$ of $M_{0,5}$ over $\mathbb{C}$ is the same as the Teichmüller space of type (0,5), and that $Aut T_{0,5} \cong \mathit{\Gamma}_0^{[5]}$ (the full Teichmüller modular group). (See e.g. [29].) Here we have an exact sequence

$$1 \to \mathit{\Gamma}_0^5 \to \mathit{\Gamma}_0^{[5]} \to S_5 \to 1,$$

and $\mathit{\Gamma}_0^{[5]}$ is the quotient of the Artin braid group B_5 by the normal closure generated by y_5 and z_5. (See Remark after (3.1.3).) From this it follows that the images of

$$\Phi_{M_{0,5}}^{\mathfrak{C}} : Aut_k M_{0,5} \cong S_5 \to \frac{Aut_{G_k} \pi_1^{\mathfrak{C}}(M_{0,5})}{Inn \hat{\mathit{\Gamma}}_0^5}$$

can be in principle calculated by seeing conjugacy actions of the standard generators σ_i $(1 \leq i \leq 4)$ on $\mathit{\Gamma}_0^5$.

Recall we have forgetful homomorphisms $p_\nu : \pi_1^{\mathfrak{C}}(M_{0,5}) \to \pi_1^{\mathfrak{C}}(M_{0,4})$ for $\nu \in \{1, \ldots, 5\}$.

Proof of Theorem (A20). We begin by considering the following conditions on $\beta \in \pi_1^{\mathfrak{C}}(M_{0,5})$. (For a profinite group G, G' or $[G,G]$ denotes the closure of the commutator subgroup of G.)

$$\beta x_{12}\beta^{-1} = x_{12}^a \quad \exists a \in \mathbb{Z}_{\mathfrak{C}}^\times, \tag{A26}$$

$$\beta x_{23}\beta^{-1} = t x_{23}^a t^{-1} \quad \exists a \in \mathbb{Z}_{\mathfrak{C}}^\times,\ \exists t \in (kerp_2)'\langle x_{24}\rangle, \tag{A27}$$

$$\beta x_{45}\beta^{-1} = x_{45}^a \quad \exists a \in \mathbb{Z}_{\mathfrak{C}}^\times, \tag{A28}$$

$$\beta x_{34}\beta^{-1} = s x_{34}^a s^{-1} \quad \exists a \in \mathbb{Z}_{\mathfrak{C}}^\times,\ \exists s \in \langle x_{34}, x_{45}\rangle', \tag{A29}$$

$$\beta x_{34}\beta^{-1} = s x_{34}^a s^{-1} \quad \exists a \in \mathbb{Z}_{\mathfrak{C}}^\times,\ \exists s \in (kerp_4)'\langle x_{24}\rangle, \tag{A30}$$

$$\beta x_{23}\beta^{-1} = t x_{23}^a t^{-1} \quad \exists a \in \mathbb{Z}_{\mathfrak{C}}^\times,\ \exists t \in \langle x_{12}, x_{23}\rangle', \tag{A31}$$

If we let $\mathfrak{L} = \{\beta | (A26), (A27)\}$, then $\mathfrak{L}$ is a subgroup of $\pi_1^{\mathfrak{C}}(M_{0,5})$ isomorphic to $\pi_1^{\mathfrak{C}}(M_{0,4})$ via p_2. Therefore we may apply the Belyi lifting for $M_{0,4}$ in the exact sequence

$$1 \to \langle x_{34}, x_{45}\rangle \to \mathfrak{L} \to G_k \to 1,$$

and get

$$\mathfrak{B} := \{\beta | (A26), (A27), (A28), (A29)\} \cong G_k.$$

If we denote by β_σ the unique element of $\mathfrak{B}$ lying over $\sigma \in G_k$, then we have $\beta_\sigma x_{34}\beta_\sigma^{-1} = t_\sigma(x_{34}, x_{45}) x_{34} t_\sigma(x_{34}, x_{45})^{-1}$ by the definition of the pro-word t_σ. Moreover, since $\langle x_{34}, x_{45}\rangle' = \langle x_{34}, x_{45}\rangle \cap (kerp_4)'\langle x_{24}\rangle$,

$$\begin{aligned}\mathfrak{B} &= \{\beta | (A26), (A27), (A28), (A29)\}\\ &= \{\beta | (A26), (A27), (A28), (A30)\}\\ &= \{\beta | (A26), (A28), (A30), (A31)\} \text{ (by symmetry)}\\ &= \{\beta | (A26), (A28), (A29), (A31)\} \text{ (by existence and uniqueness).}\end{aligned}$$

As $\mathfrak{L}' = \{\beta \mid (A28), (A30)\}$ is an extension of G_k by $\langle x_{12}, x_{23}\rangle$ and is isomorphic to $\pi_1^{\mathfrak{C}}(M_{0,4})$ via p_4, it follows that $\beta_\sigma \in \mathfrak{B}$ also satisfies (A23). Thus, we conclude that $\beta_\sigma \in \mathfrak{B}$ is characterized as a unique element in $p_{0,5}^{-1}(\sigma)$ satisfying the properties (A21)-(A24).

Let g be a Galois compatible automorphism of $\pi_1^{\mathfrak{C}}(M_{0,5})$ induced from the conjugation by $(\sigma_1\sigma_2\sigma_3\sigma_4)^3$ (g sends x_{ij} to $x_{\tau(i)\tau(j)}$ where τ denotes the cyclic permutation (14253)), and define

$$\mathfrak{B}' = \{t_\sigma(x_{23}, x_{12}) g(\beta_\sigma) | \sigma \in G_k\}.$$

Then it follows that $\beta'_\sigma = t_\sigma(x_{23}, x_{12})g(\beta_\sigma)$ is characterized as a unique element of $p_{0,5}^{-1}(\sigma)$ such that

$$\text{(A32)} \qquad \beta'_\sigma x_{45} {\beta'}_\sigma^{-1} = x_{45}^{a_\sigma};$$

$$\text{(A33)} \qquad \beta'_\sigma x_{51} {\beta'}_\sigma^{-1} = t_\sigma(x_{23}, x_{12}) t_\sigma(x_{51}, x_{45}) x_{51}^{a_\sigma} t_\sigma(x_{51}, x_{45})^{-1} t_\sigma(x_{23}, x_{12})^{-1};$$

$$\text{(A34)} \qquad \beta'_\sigma x_{12} {\beta'}_\sigma^{-1} = x_{12}^{a_\sigma};$$

$$\text{(A35)} \qquad \beta'_\sigma x_{23} {\beta'}_\sigma^{-1} = t_\sigma(x_{23}, x_{12}) x_{23}^{a_\sigma} t_\sigma(x_{23}, x_{12})^{-1}.$$

From this we also see that $\mathfrak{B}'$ forms a subgroup of $\pi_1^{\mathfrak{C}}(M_{0,5})$ and that β' gives a section of $p_{0,5}$.

For the proof of Theorem (A20) it suffices to show $\mathfrak{B} = \mathfrak{B}'$. As $\langle x_{12}, x_{45} \rangle$ is selfnormalizing in Γ_0^5, after observing the conditions (A21), (A24), (A32), (A34) together with (A22) and (A35), we may put $\beta'_\sigma = x_{45}^{\lambda_\sigma} \beta_\sigma$ for some $\lambda_\sigma \in \mathbb{Z}_{\mathfrak{C}}$. Then, by (A35), we have

$$\text{(A36)} \qquad \beta_\sigma x_{51} \beta_\sigma^{-1} = x_{45}^{-\lambda_\sigma} t_\sigma(x_{23}, x_{12}) t_\sigma(x_{51}, x_{45}) x_{51}^{a_\sigma} t_\sigma(x_{51}, x_{45})^{-1} t_\sigma(x_{23}, x_{12})^{-1} x_{45}^{\lambda_\sigma}.$$

Let f be a Galois compatible automorphism of $\pi_1^{\mathfrak{C}}(M_{0,5})$ induced from the conjugation by $\sigma_4 \sigma_1^{-1} \sigma_2 \sigma_1$. Then

$$\begin{aligned} f(x_{12}) &= x_{12}^{-1} x_{23} x_{12}; \quad & f(x_{23}) &= x_{12}; \\ f(x_{34}) &= x_{13} x_{51} x_{13}^{-1}; \quad & f(x_{45}) &= x_{45}; \\ f(x_{51}) &= x_{45} x_{34} x_{45}^{-1}. \end{aligned}$$

If we put $\beta''_\sigma = t_\sigma(x_{23}, x_{12}) x_{45}^{\frac{a_\sigma - 1}{2}} x_{12} f(\beta'_\sigma) x_{12}^{-1}$ for $\sigma \in G_k$, then after some computations we see that β''_σ satisfies the same conditions as (A21)-(A24) for β_σ together with

$$\text{(A37)} \qquad \beta''_\sigma x_{51} {\beta''}_\sigma^{-1} = x_{45}^{\lambda_\sigma} t_\sigma(x_{23}, x_{12}) t_\sigma(x_{51}, x_{45}) x_{51}^{a_\sigma} t_\sigma(x_{51}, x_{45})^{-1} t_\sigma(x_{23}, x_{12})^{-1} x_{45}^{-\lambda_\sigma}.$$

The coincidence of the first four conditions assures that $\beta_\sigma = \beta''_\sigma$. We conclude then by comparing (A37) with (A36) that $\lambda_\sigma = 0$. This completes the proof of Theorem (A20). □

COROLLARY (Drinfeld [9]; in this form, see Ihara [20]). *The pro-word $t = t_\sigma$ ($\sigma \in G_k$) satisfies the following pentagon relation in $\hat{\Gamma}_0^5$:*

$$\text{(A38)} \qquad t(x_{12}, x_{23})t(x_{34}, x_{45})t(x_{51}, x_{12})t(x_{23}, x_{34})t(x_{45}, x_{51}) = 1.$$

PROOF. Let β_σ be as in the theorem, and put $\beta'_\sigma = t_\sigma(x_{12}, x_{23})\beta_\sigma$, and $\beta''_\sigma = (\sigma_1\sigma_2\sigma_3\sigma_4)^3\beta_\sigma(\sigma_1\sigma_2\sigma_3\sigma_4)^{-3}$. By observing the resulting first four conditions for β'_σ and β''_σ, we see $\beta'_\sigma = \beta''_\sigma$. Repeating this 5 times, we get the assertion. □

Lines of a more geometric proof of (A38) is illustrated in Ihara's article [20]. In [9], Drinfeld considered the Grothendieck-Teichmüller group GT

$$GT = \{(a,t) \in \mathbb{Z}_{\mathfrak{C}}^\times \times \langle y, z\rangle | (A18), (A19), (A38)\}^\times$$

with group operation $(a,t)(a',t') = (aa', t(t'(y,z)y^{a'}t'(y,z)^{-1}, z^{a'}))$, and asserted that GT operates on profinite Artin braid groups $\hat{\mathcal{B}}_n$ in a uniform way for $n \geq 4$. (Prof. Ihara showed a method to verify this assertion.) If we compose this operation with the map $G_k \ni \sigma \to (a_\sigma, t_\sigma) \in GT$, we obtain Galois representations in $Aut\hat{\Gamma}_0^n$ after suitable reduction $\hat{\mathcal{B}}_n \supset \hat{\mathcal{P}}_n \twoheadrightarrow \hat{\Gamma}_0^n$ ($n \geq 4$). It would be very plausible that this representation gives a lifting of the Galois representations $\varphi_{0,n}^{\mathfrak{C}} : G_k \to Out\hat{\Gamma}_0^n$ coming from the geometric object $M_{0,n}$. But the rigorous proof of this for $n \geq 6$ seems not to have appeared yet.

References

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

[2] Artin, M. and B. Mazur, Etale Homotopy, Lecture Note in Math. **100** (1969), Springer, Berlin Heidelberg New York.

[3] Asada, M., Two properties of the filtration of the outer automorphism groups of certain groups, Math. Z. (to appear).

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

[5] Birman, J. S., Braids, links, and mapping class groups, Ann. of Math. Studies 82, Princeton University Press, 1974.

[6] Bogomolov, F. A., Brauer groups of fields of invariants of algebraic groups, Math. USSR Sb. **66-1** (1990), 285–299.

[7] Cartan, H. and S. Eilenberg, Homological Algebra, Princeton Univ. Press, 1956.

[8] Deligne, P., Le groupe fondamental de la droite projective moins troi points, The Galois Group over Q, ed. by Y.Ihara, K.Ribet, J.-P.Serre, Springer, 1989 pp. 79–297.

[9] Drinfeld, V. G., On quasitriangular quasi-Hopf algebras and a group closely connected with $Gal(\bar{Q}/Q)$, Leningrad Math. J. **2(4)** (1991), 829–860.

[10] Fried, M. and M. Jarden, Field Arithmetic, Springer-Verlag, Berlin Heidelberg, 1980.

[11] Friedlander, E. M., $K(\Pi, 1)$ in characteristic $p > 0$, Topology **12** (1973), 9–18.

[12] Gerritzen, L., Herrlich, F. and M. Put, Stable n-pointed trees of projective lines, Indag. Math. **91** (1988), 131–163.

[13] Grothendieck, A., Revêtement Etales et Groupe Fondamental (SGA1), Lecture Note in Math. **288** (1971), Springer.

[14] Grothendieck, A., Esquisse d'un programme, preprint (1984).

[15] Gruenberg, K. W., Residual properties of infinite soluble groups, Proc. London Math. Soc. (3) **7**, 29–62.

[16] Herfort, W. and L. Ribes, Torsion elements and centralizers in free products of profinite groups, J. reine angew. Math. **358** (1985), 155–161.

[17] Humphreys, J. E., Linear algebraic groups, Graduate Texts in Math. 21, Springer, 1975.

[18] Ihara, Y., Profinite braid groups, Galois representations, and complex multiplications, Ann. of Math. **123** (1986), 43–106.

[19] Ihara, Y., Automorphisms of pure sphere braid groups and Galois representations, The Grothendieck Festschrift, Volume II, Birkhäuser, pp. 353–373.

[20] Ihara, Y., Braids, Galois groups and some arithmetic functions, Proc. ICM, Kyoto (1990), 99–120.

[21] Ivanov, N. V., Algebraic properties of mapping class groups of surfaces, Geometric and Algebraic Geometry., Banach Center Publ., 1986, pp. 15–35.

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

[23] Lubotzky, A., Combinatorial group theory for pro-p groups, J. Pure and Appl. Alg. **25** (1982), 311–325.

[24] Lubotzky, A., Group presentation, p-adic analytic groups and lattices in $SL_2(\mathbb{C})$, Ann. of Math. **118** (1983), 115–130.

[25] Lubotzky, A. and L. Van Den Dries, Subgroups of free profinite groups and large subfields of $\bar{Q}$, Israel J. Math. **39(1-2)** (1981), 25–45.

[26] McCarthy, J. D., Automorphisms of surface mapping class groups. A recent theorem of N. Ivanov, Invent. math. **84** (1986), 49–71.

[27] Magnus, W., Karrass, A. and D. Solitar, Combinatorial group theory, Interscience, 1966.

[28] Mazur, B. and P. Swinnerton-Dyer, Arithmetic of Weil curves, Invent. math. **25** (1974), 1–61.

[29] Nag, S., The complex analytic theory of Teichmüller spaces, A Wiley Interscience Publication, 1988.

[30] Nakamura, H., Galois rigidity of the etale fundamental groups of punctured projective lines, J. reine angew. Math. **411** (1990), 205–216.

[31] Nakamura, H., On galois automorphisms of the fundamental group of the projective line minus three points, Math. Z. **206** (1991), 617–622.

[32] Nakamura, H., Centralizers of Galois representations in pro-l pure sphere braid groups, Proc. Japan Acad. **67(A)** (1991), 208–210.

[33] Nakamura, H., On the pro-p Gottlieb theorem, Proc. Japan Acad. **68(A)** (1992), 279–282.

[34] Nakamura, H., Galois rigidity of algebraic mappings into some hyperbolic varieties, Intern. J. Math. **4** (1993), 421–438.

[35] Nakamura, H. and H. Tsunogai, Some finiteness theorems on Galois centralizers in pro-l mapping class groups, J. reine angew. Math. **441** (1993), 115–143.

[36] Neukirch, J., Über die absoluten Galoisgruppen algebraischer Zahlkölper, Astérisque **41/42** (1977), 67–79.

[37] Oda, T., A note on ramification of the Galois representation on the fundamental group of an algebraic curve II, J. Number Theory (to appear).

[38] Quillen, D., Rational homotopy theory, Ann. of Math. **90** (1969), 205–295.

[39] Raynaud, M., Propriétés de finitude du groupe fondamental (SGA7,Exposé II) (1972), Springer, Berlin-Heidelberg-New York.

[40] Serre, J. P., Corps Locaux, Hermann, Paris, 1962.

[41] Serre, J. P., Cohomologie Galoisienne, Lecture Note in Math. **5** (1973), Springer, Berlin Heidelberg New York.

[42] Serre, J. P., Cohomologie des groupes discrets, Ann. of Math. Studies **70** (1971), Princeton Univ. Press, 77–169.

[43] Stallings, J., Centerless groups – An algebraic formulation of Gottlieb's theorem, Topology **4** (1965), 129–134.

[44] Tate, J., Relations between K_2 and Galois Cohomology, Invent. math. **36** (1976), 257–274.

[45] Terada, T., Quelques Propriétés Géométriques du Domaine de F_1 et le Groupe de Tresses Colorées, Publ. RIMS, Kyoto Univ. **17** (1981), 95–111.

[46] Weissauer, R., Der Hilbertsche Irreduzibilitätssatz, J. reine angew. Math. **334** (1982), 203–220.

[47] Wells, C., Automorphisms of group extensions, Trans. Amer. Math. Soc. **155** (1971), 189–194.

[48] Yamagishi, M., On the center of Galois groups of maximal pro-p extensions of algebraic number fields with restricted ramification, J. reine angew. Math. **436** (1993), 197–208.

Notes added in proof. The main part §3 of this paper was written before [33,34,35] in 1991, so it would be appropriate here to explain some history of the present paper. After receiving comments from Prof. Deligne on the original version, the author wrote §4, and in the process of enlarging §3 to the pro-$\mathfrak{C}$ context, began to equip the paper with some technical tools §1–2 which were expected to suggest lines for future developments of the 'anabelian' world. This latter effort seemed more or less successful, as it clarified the importance of "universal center-triviality" of fundamental groups, and lead to the work [34]. The use of weights as in 2.3 occurred to the author when he examined lines of Deligne's letter suggesting Lie variant §4. Combining the linear weights in 2.3 with non-linear weights in 2.1, we were lead to the construction of weight coordinate formalism in a joint work with H.Tsunogai [35]. The body of the present paper was thus established in 1992. Since then the problem of estimating the centralizers of Galois images in $Out\pi_1^{pro-l}$ has been developed, and our understanding of the problem has been gradually deepened. In particular, the author has realized that Theorem A can be deduced from Theorem B without help of (3.13.3), contrary to the discussion in (4.2.4). It comes from the observation that the Galois centralizer can act faithfully on the abelianization of π_1^{pro-l} by a suitable weight argument. This point of view was pursued further in a recent collaboration with N.Takao on the pro-l fundamental groups of braid configuration spaces of higher genus curves.

(Received March 10, 1992)

Department of Mathematical Sciences
University of Tokyo
7-3-1 Hongo
Bunkyoku, Tokyo
113 Japan