On Galois rigidity of fundamental groups of algebraic curves

Hiroaki Nakamura

This article has appeared in
Non-abelian Fundamental Groups and Iwasawa Theory,
(J.Coates, M.Kim, F.Pop, M.Saïdi, P.Schneider eds.)
London Mathematcial Society Lecture Note Series,
Vol. 393 (2012), pp. 56–71.
Published by Cambridge University Press.

On Galois rigidity of fundamental groups of algebraic curves

Hiroaki Nakamura
Okayama University

English translation of [31] (1989)

§1. Conjecture and result Let U be an (absolutely irreducible, nonsingular) algebraic curve defined over a number field k. It is well known that the etale fundamental group $\pi_1(U)$ is naturally regarded as a group extension of the absolute Galois group $G_k := \mathrm{Gal}(\bar{k}/k)$ by a finitely generated topological group. We shall consider a question of how much the equivalence class of this group extension depends on the isomorphism class of the issued curve.

First, let us recall that the etale fundamental group of the algebraic curve U/k is a profinite topological group defined as the projective limit of finite groups as follows:

Note 1

$$\pi_1(U) := \varprojlim_{Y} \mathrm{Aut}_U(Y),$$

where Y runs over the projective system of the connected finite etale Galois covers of U. If we restrict the projective system to a subsystem consisting of the covers of the form $\{Y = U \otimes K \mid K/k : \text{finite Galois extension}\}$ and note that $\mathrm{Aut}_U(U \otimes K) \cong \mathrm{Gal}(K/k)$, then we obtain a canonical surjective homomorphism

$$p_{U/k} : \pi_1(U) \longrightarrow G_k (:= \mathrm{Gal}(\bar{k}/k)).$$

We will treat $\pi_1(U)$ as an object associated with the "augmentation map" $p_{U/k}$ onto G_k. The kernel (= $\ker p_{U/k}$) is isomorphic to $\pi_1(U \otimes \bar{k})$, which in this article will often be denoted simply by π_1. In fact, we may present it by generators and relations as a topological group:

Non-abelian Fundamental Groups and Iwasawa Theory, eds. John Coates, Minhyong Kim, Florian Pop, Mohamed Saïdi and Peter Schneider. Published by Cambridge University Press.

$$(\Pi) \qquad \pi_1 = \pi_1(U \otimes \bar{k}) = \left\langle \begin{matrix} \alpha_1, \ldots, \alpha_g \\ \beta_1, \ldots, \beta_g \\ \gamma_1, \ldots, \gamma_n \end{matrix} \;\middle|\; \begin{matrix} \alpha_1\beta_1\alpha_1^{-1}\beta_1^{-1} \cdots \alpha_g\beta_g\alpha_g^{-1}\beta_g^{-1} \cdot \\ \cdot\gamma_1 \cdots \gamma_n = 1 \end{matrix} \right\rangle_{\text{top}}.$$

Here, α_i, β_i and γ_j $(1 \leq i \leq g,\ 1 \leq j \leq n)$ are taken as suitable loops at a base point on the associated complex curve $U_{\mathbb{C}}^{\text{an}}$ with U, which is assumed to be a Riemann surface of genus g with n punctures. The suffix *top* designates the profinite completion. Note here that in our issued group extension

$$1 \longrightarrow \pi_1 \longrightarrow \pi_1(U) \longrightarrow G_k \longrightarrow 1 \quad \text{(exact)},$$

the kernel part π_1 is a group whose isomorphism class is determined only by the topological type (g, n), hence may be written as $\pi_1 = \Pi_{g,n}$. In other words, whenever a topological space of type (g, n) gets a structure of an algebraic curve over k, it gives rise to a group extension of $\mathrm{Gal}(\bar{k}/k)$ by $\Pi_{g,n}$.

Conjecture (Part of Grothendieck's fundamental conjecture of "anabelian" algebraic geometry [2]) When $\Pi_{g,n}$ is non-abelian, namely, $(g, n) \neq (0, 0), (0, 1), (0, 2), (1, 0)$, the above correspondence Note 2

$$\text{algebraic curve } U/k \rightsquigarrow \text{group extension } \pi_1(U)/G_k$$

is faithful.

In this note, we would like to report the following result.

Theorem Conjecture is true for $(g, n) = (0, n)$ $(n \geq 3)$ and $(1, 1)$.

§2. Finiteness for π_1 modulo π_1'' As a non-abelian profinite group $\pi_1 = \Pi_{g,n}$ is so large, a basic approach to the above problem would be to look at suitable quotients of it. For any class of finite groups C, set

$$J_C := \bigcap_{G \in C} \bigcap_{f \in \mathrm{Hom}(\pi_1, G)} \ker(f).$$

Noting that J_C is a characteristic subgroup of π_1 determined by the class C, we obtain an exact sequence

$$(1) \qquad 1 \longrightarrow \pi_1/J_C \longrightarrow \pi_1(U)/J_C \longrightarrow G_k \longrightarrow 1.$$

(Here, π_1/J_C is so called the maximal pro-C quotient of the topological group π_1. In a particular case when $C = \{\text{all } l\text{-groups}\}$ for a fixed rational prime l, π_1/J_C (written $\pi_1^{\text{pro-}l}$) is called the pro-l fundamental group, and the Galois

representation $G_k \to \mathrm{Out}(\pi_1^{\text{pro-}l})$ associated with the above exact sequence have been studied in depth by Y. Ihara and other authors (cf. [3])).

For two algebraic curves U/k and U'/k, if there is a commutative diagram of profinite groups

$$\begin{array}{ccc} \pi_1(U)/J_C & \xrightarrow{\sim} & \pi_1(U')/J_C \\ & {\scriptstyle p_{U/k}}\searrow \quad \swarrow{\scriptstyle p_{U'/k}} & \\ & G_k & \end{array}$$

with the horizontal arrow being an isomorphism, then U and U' are called π_1-equivalent modulo J_C and written

$$\pi_1(U)/J_C \cong_{G_k} \pi_1(U')/J_C.$$

In the case C being the class of all finite groups, we find $J_C = \{1\}$. In this case, we just say that they are π_1-equivalent. It is obvious that

$$\pi_1(U) \cong_{G_k} \pi_1(U') \Rightarrow \pi_1(U)/J_C \cong_{G_k} \pi_1(U')/J_C. \tag{2}$$

Let us first consider the case $C = \{\text{abelian groups}\}$. In this case, $J_C = \overline{[\pi_1, \pi_1]} = \pi_1'$ is the (closure of the) commutator subgroup of π_1, and $\pi_1/\pi_1' = \pi_1^{\text{ab}}$ can be identified with the etale homology group $H_1(U \otimes \bar{k}, \hat{\mathbb{Z}})$. It then follows from (2) that

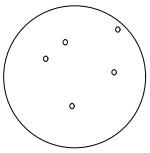
$$\pi_1(U) \cong_{G_k} \pi_1(U') \Longrightarrow H_1(U \otimes \bar{k}) \cong H_1(U' \otimes \bar{k}).$$
$$\langle \text{as } G_k\text{-modules} \rangle$$

Note 3 When U has genus ≥ 1, a rough application of the finiteness theorem of Shafarevich–Faltings implies finiteness of U'/k that are π_1-equivalent over k to a fixed U/k. However, when U has genus 0, it is impossible to deduce such finiteness only from H_1. In fact, suppose Λ is a finite subset of $\mathbf{P}^1(k)$ with cardinality $n(\geq 4)$ and let $U = \mathbf{P}^1_k - \Lambda$. Then, one should ask how the equivalence class of the group extension

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H_1 & & \longrightarrow \pi_1(U)/\pi_1' & \longrightarrow & G_k & \longrightarrow & 1 \\ & & \wr\| & & & & & & \\ & & \hat{\mathbb{Z}}^{\oplus n-1} & & & & & & \end{array} \tag{3}$$

varies according to the relative position of the point set Λ on $\mathbf{P}^1$. But one finds that (3) has no more information on the cardinality of Λ, immediately after observing that the above (3) splits and the associated Galois representation $G_k \to \mathrm{GL}_{n-1}(\hat{\mathbb{Z}})$ is a direct sum of the 1-dimensional scalar representation realized as multiplication by the cyclotomic character.

So, in the case of genus 0, let us take C to be the class of meta-abelian groups, i.e., finite solvable groups of derived length ≤ 2. Then, J_C becomes the double commutator subgroup $\pi_1'' = \overline{[\pi_1', \pi_1']}$.



distribution of points on $\mathbf{P}^1$

Notation For any finite subset $\Lambda = \{0, 1, \infty, \lambda_1, \ldots, \lambda_m\}$ ($\lambda_i \in k$), define the multiplicative subgroup $\Gamma(\Lambda)$ of $k^\times$ to be that generated by

$$\{-1, \lambda_i, 1 - \lambda_i, \lambda_i - \lambda_j \mid 1 \leq i \neq j \leq m\}.$$

Remark The group $\Gamma(\Lambda) \subset k^\times$ is independent of the choice of (the coordinate of $\mathbf{P}^1$ such that) $\{0, 1, \infty\} \subset \Lambda$.

Then we have the following theorem.

Theorem 1 ([6]) Let Λ, Λ' be finite subsets of $\mathbf{P}^1(k)$ containing $\{0, 1, \infty\}$, and set $U = \mathbf{P}^1_k - \Lambda$, $U' = \mathbf{P}^1_k - \Lambda'$. Then,

$$\pi_1(U)/\pi_1'' \cong_{G_k} \pi_1(U')/\pi_1'' \implies \Gamma(\Lambda) = \Gamma(\Lambda').$$
(not only $\cong$)

For a finitely generated multiplicative subgroup $\Gamma \subset k^\times$, it is known as Siegel's theorem (cf. [5]) that the set of solutions (x, y) to the equation $x + y = 1$ ($x, y \in \Gamma$) is (effectively) finite. From this follows that, for any fixed U, there are only a finite number of U' satisfying the assumption of Theorem 1. Note 4

§3. Rigidity of π_1 with no modding out When a nonsingular algebraic curve U/k is not complete, the fundamental group $\pi_1(U \otimes \bar{k})$ is a free profinite group of finite rank. The famous paper of Belyi [1] considers the group extension

$$1 \longrightarrow \pi_1 \longrightarrow \pi_1(U) \longrightarrow G_k \longrightarrow 1$$

without taking reduction of π_1 modulo any nontrivial subgroups. (It seems that there are not many other papers treating it in this way.)

In this note, we should like to report the following nature of $\pi_1(U)$. If the complex Riemann surface associated with U is of type (g, n), then one finds a subset $\mathcal{I}$ in $\pi_1 = \Pi_{g,n}$ which is the conjugacy union of the inertia subgroups corresponding to n punctures. It can be written in the presentation of §1 (Π) as

$$\mathcal{I} = \{x\gamma_i^a x^{-1} \mid x \in \Pi_{g,n},\ a \in \hat{\mathbb{Z}},\ i = 1, 2, \ldots, n\}.$$

Note that this is only a subset of π_1 (not closed under the group operation) of the form of a union of certain conjugacy classes. We shall call $\mathcal{I}$ the *inertia subset* of $\pi_1(U)$. Then we have the following result.

Key lemma ([7]) The inertia subset $\mathcal{I} \subset \pi_1$ can be characterized in terms of the Galois augmentation $\pi_1(U) \twoheadrightarrow G_k$ by a "non-abelian" weight filtration. Therefore, any Galois compatible isomorphism of topological groups $f : \pi_1(U) \xrightarrow[G_k]{\sim} \pi_1(U')$ should precisely keep their inertia subsets $\mathcal{I} \subset \pi_1(U)$ and $\mathcal{I}' \subset \pi_1(U')$, i.e., should induce $f(\mathcal{I}) = \mathcal{I}'$. Note 5

This lemma enables us to control *in a purely group-theoretical way*, say, open immersions of algebraic curves, or residue fields of cusps on finite etale covers of a curve. To prove this lemma, we need to use properly non-abelian phases such as: any open subgroup of a free profinite group is again profinite free; the ranks of those open subgroups increase in proportion to their indices (Schreier's formula). Therefore we could not prove similar characterization of inertia in the meta-abelian quotients of π_1. Still, we can show the similar lemma for the case of pro-l fundamental groups, where the proof turns out rather simpler than the profinite case as a consequence of a strong property of the pro-l free groups. However, for the pro-nilpotent π_1 (which is the direct product of $\pi_1^{\text{pro-}l}$ for all primes l), the corresponding lemma is not true. But if we take larger pro-solvable or profinite π_1, then, the lemma holds true again. By virtue of such characterization of inertia subsets in full profinite (or pro-solvable) π_1 beyond pro-nilpotent π_1, one could "interrelate" information of inertia subsets of $\pi_1^{\text{pro-}l}$ among different primes l. This was an important point to enable us to scoop up a powerful essence of profinite non-abelianity, that has led us to the following result.

Theorem 2 ([7]) Let U and U' be genus zero curves defined over a number field k with $\pi_1(U^{\text{an}}_{\mathbb{C}})$ non-abelian. Then,

$$\pi_1(U) \cong_{G_k} \pi_1(U') \Longrightarrow U \cong_k U'.$$

Note In the above statement, the converse implication $\Leftarrow$ trivially holds.

Note By rigidity we mean uniqueness rather than finiteness.

§4. Case of elliptic curves Let E be an elliptic curve with origin $O \in E(k)$. Then, $\pi_1(E)$ is an extension of the absolute Galois group G_k by $\pi_1(E \otimes \bar{k})$, where the kernel group can be identified with $H_1(E \otimes \bar{k}, \hat{\mathbb{Z}}) \cong \hat{\mathbb{Z}}^{\oplus 2}$:

$$1 \longrightarrow \begin{array}{c} \pi_1 \\ \wr \| \\ \hat{\mathbb{Z}}^{\oplus 2} \end{array} \longrightarrow \pi_1(E) \longrightarrow G_k \longrightarrow 1.$$

The existence of the rational point $O \in E(k)$ implies its splitness, so that considering the equivalence class of the above group extension is equivalent to

considering that of the associated Galois representation

$$G_k \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}}) = \prod_l \mathrm{GL}(T_l E_{\bar{k}}).$$

Then, when E has no complex multiplication, Faltings' theorem (Tate conjecture) implies that the group extension $\pi_1(E)/G_k$ determines the elliptic curve E/k. However, when E does have complex multiplication, it is not necessarily the case. For example, one can construct lots of pairs of elliptic curves (E, E') over a sufficiently large number field k with $E^{\mathrm{an}}_{\mathbb{C}} \ncong E'^{\mathrm{an}}_{\mathbb{C}}$ admitting k-isogeny maps $f\colon E \to E'$, $g\colon E' \to E$ with mutually prime degrees. For such a pair (E, E'), the Galois representations $G_k \to \mathrm{GL}(T_l E_{\bar{k}})$ and $G_k \to \mathrm{GL}(T_l E'_{\bar{k}})$ turn out to be equivalent for every l through f or g, although E and E' are not isomorphic over k.

Thus we are led to removing the origin O from E so as to consider $\pi_1(E-O)$ instead of $\pi_1(E)$. Note that $\pi_1(E-O)$ is a group extension of G_k by a free profinite group $\hat{F}_2$ of rank 2 (which is obviously non-abelian).

Theorem 3 Let (E, O), (E', O') be elliptic curves defined over k. Then,

$$\pi_1(E-O) \cong_{G_k} \pi_1(E'-O') \Longrightarrow E \cong_k E'.$$

Over the curve $E-O$ one has an etale cover $E - {}_4E$ (where ${}_4E$ is a divisor on the elliptic curve E consisting of 16 geometric points of order dividing 4) which can be regarded naturally as a Kummer cover of $\mathbf{P}^1 - \{0, 1, \infty, \lambda\}$. Using this trick, the proof of Theorem 3 may be reduced to the case of genus 0. Note 6

§5. On automorphisms According to theorems by Neukirch, Ikeda, Iwasawa, Uchida (cf. [8]), for algebraic number fields k, k', we know not only

$$\pi_1(\mathrm{Spec}\, k) \cong \pi_1(\mathrm{Spec}\, k') \Longleftrightarrow \mathrm{Spec}\, k \cong \mathrm{Spec}\, k'$$

$$(\text{i.e., } \mathrm{Gal}(\overline{\mathbb{Q}}/k) \cong \mathrm{Gal}(\overline{\mathbb{Q}}/k') \Longleftrightarrow k \text{ and } k' \text{ are } \mathbb{Q}\text{-isomorphic}),$$

but also

$$\mathrm{Out}(\pi_1(\mathrm{Spec}\, k)) \cong \mathrm{Aut}(k).$$

Regarding this as 0-dimensional case, we may expect the following for algebraic curves.

Problem X For U/k an algebraic curve with $\pi_1(U^{\mathrm{an}}_{\mathbb{C}})$ non-abelian, could Note 7

$$\frac{\mathrm{Aut}_{G_k}\pi_1(U)}{\mathrm{Inn}\,\pi_1} \cong \mathrm{Aut}_k(U)$$

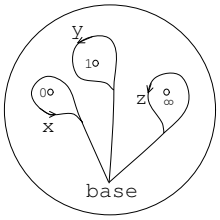
hold true? (In fact, Grothendieck conjectures such a phenomenon for a more general class of morphisms.)

Now, let us consider $U = \mathbf{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}$. The exact sequence

$$1 \longrightarrow \pi_1 \longrightarrow \pi_1(U) \longrightarrow G_{\mathbb{Q}} \longrightarrow 1$$

yields a big Galois representation

$$\varphi_{\mathbb{Q}} : G_{\mathbb{Q}} \longrightarrow \mathrm{Out}(\pi_1).$$



Presenting π_1 by use of the loops in the figure as

$$\pi_1 = \langle x, y, z \mid xyz = 1 \rangle_{\mathrm{top}},$$

one can lift the representation $\varphi_{\mathbb{Q}}$ to a unique representation $\tilde{\varphi}_{\mathbb{Q}} : G_{\mathbb{Q}} \to \mathrm{Aut}(\pi_1)$ whose Galois image lies in

$$\mathrm{Brd}(\pi_1) := \left\{ f \in \mathrm{Aut}(\pi_1) \;\middle|\; \begin{array}{c} \exists\, \alpha \in \hat{\mathbb{Z}}^{\times}, \exists\, s \in \pi_1, \exists\, t \in \pi_1' \text{ s.t.} \\ f(x) = s x^{\alpha} s^{-1}; \\ f(y) = t y^{\alpha} t^{-1}; \\ f(z) = z^{\alpha}. \end{array} \right\}$$

(Belyi [1]). Recalling that Belyi showed the injectivity of $\tilde{\varphi}_{\mathbb{Q}}$, one of our next interests is to ask "how much the representation image $\mathrm{Im}\,\tilde{\varphi}_{\mathbb{Q}}$ is smaller than $\mathrm{Brd}\,\pi_1$?" This last question is indeed related to the above mentioned Problem X as follows.

Proposition 4 To verify Problem X for $U = \mathbf{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}$ affirmatively, it is necessary and sufficient to show that the centralizer of $\mathrm{Im}\,\tilde{\varphi}_{\mathbb{Q}}$ in $\mathrm{Brd}(\pi_1)$ is $\{1\}$.

Here, the center of $\mathrm{Im}\,\tilde{\varphi}_{\mathbb{Q}} \approx G_{\mathbb{Q}}$ is known to be trivial. One can also show that the centralizer Z in the above proposition has trivial image in $\mathrm{Brd}(\pi_1^{(l)}/\pi_1^{(l)\prime\prime})$ ($\pi_1^{(l)} = \pi_1^{\text{pro-}l}$) for every prime l. Finally, we note that the problem of seeking the image of pro-l Galois representation $\varphi_{\mathbb{Q}}^{(l)} : G_{\mathbb{Q}} \to \mathrm{Brd}(\pi_1^{(l)})$ has been approached
Note 8 by several other authors by the use of lower central filtration (see e.g., [4]).

Complementary notes

The text above is one of the earliest publications of anabelian research, in the late 1980s in Japanese, which indicates some of the atmosphere of the dawn of investigations around Grothendieck's conjecture on fundamental groups of "anabelian" curves. As indicated in the introduction of [6], the research started under the strong influence of techniques from studies of Galois representations in $\pi_1(\mathbf{P}^1 - \{0, 1, \infty\})$ by Ihara [3] and Anderson–Ihara [9], of inverse Galois problems (especially Mike Fried's intensive use of the branch cycle argument

[17]) and analogous results in Hodge theory by Hain and Pulte [20]. In this complementary section, we shall add several notes to describe miscellaneous facts and later developments (with apologies for missing citations of many important works to be mentioned).

Throughout these notes, k denotes a number field (a finite extension of $\mathbb{Q}$).

Note 1

Here $\mathrm{Aut}_U(Y)$ should be understood to denote the opposite group of the covering transformation group of Y over U. As is well known, the theory of etale fundamental groups was established by A. Grothendieck and his collaborators in SGA1 [18]. Especially, the notion of *Galois category* in loc. cit. presents axioms unifying classical Galois theory of covers of a topological space and that of field extensions. This serves as a base for introducing our main mathematical object of study – an 'arithmetic' fundamental group equipped with a mixed structure as a group extension of the absolute Galois group of a number field by the profinite completion of a discrete fundamental group of the associated complex manifold.

Note 2

The fundamental conjecture of anabelian geometry was posed in Grothendieck's letter to Faltings [19] for hyperbolic curves (i.e., nonsingular algebraic curves of negative Euler characteristic). The references [19] and [2] had not been published for many years until the appearance of the proceedings volume [41] edited by L. Schneps and P. Lochak. As described in [19], Grothendieck proposed to study "extraordinary rigidity" of those arithmetic fundamental groups as the non-abelian analog of Faltings' theorem for abelian varieties [16]:

$$\mathrm{Hom}_k(A, A') \otimes \mathbb{Z}_l \xrightarrow{\sim} \mathrm{Hom}_{G_k}(T_l A, T_l A').$$

The fundamental conjecture (saying that the geometry of "anabelian varieties" should be reconstituted from their arithmetic fundamental groups) is only one aspect of his circle of ideas (anabelian philosophy) generalizing Belyi's theorem [1] to a vast theme extending from "Grothendieck dessin d'enfant" to "Galois–Teichmüller Lego". Grothendieck used the term "anabelian" to indicate "very far from abelian groups" ([2], p. 14). Typical candidates for anabelian varieties are hyperbolic curves, successive fiber spaces of them (Artin elementary neighborhoods), and moduli spaces of hyperbolic curves. At a very early stage, virtual center-triviality of geometric profinite fundamental groups was studied as a main feature of anabelianity (e.g., [32], [33], [24]). Belyi's injectivity result has been generalized to arbitrary hyperbolic curves by Mat-

sumoto [28] and Hoshi–Mochizuki [22]. The status of the fundamental conjecture has been pushed forward to ideal solutions by Tamagawa [45] and Mochizuki [30]. See Note 7. The Galois–Teichmüller Lego philosophy has been taken up by Drinfeld [14] and Ihara [23] in the genus zero case by introducing what is called the Grothendieck–Teichmüller group $\widehat{GT}$. For a survey including higher genus formulations of $\widehat{GT}$, see [27].

Note 3

If U/k is π_1-equivalent over k to U'/k, then $H_1(U \otimes \bar{k}) \cong H_1(U' \otimes \bar{k})$ as G_k-modules. Then, as their weight (-1) quotients (obtained by modding out the weight (-2) submodules after tensoring with $\mathbb{Z}_l$), the l-adic Tate modules of the Jacobian varieties of the smooth compactifications of U and of U' turn out to be equivalent G_k-modules. Faltings' theorem [16], together with the good reduction criterion of Neron–Ogg–Shafarevich, implies then finiteness of those complete curves which have G_k-equivalent l-adic Tate modules. When the genus ≥ 2, Faltings' theorem also guarantees finiteness of points of bounded degree (Mordell conjecture), and so finiteness of possible punctures giving the same arithmetic fundamental group. To see finiteness of such possible punctures on genus 1 curves, however, would involve the problem of bounding heights of punctured points from a given class in $\mathrm{Ext}_{G_k}(T_l E, \mathbb{Z}_l^r(1))$ (if we restrict ourselves to the use of only $H_1(U)$). This has apparently not been confirmed yet. We refer to a recent important paper of M. Kim [25] that, in turn, uses anabelian ideas to deduce finiteness of Diophantine problems.

Note 4

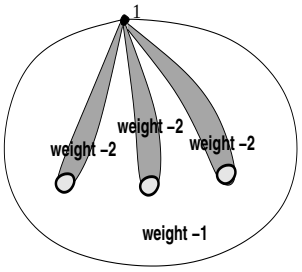
The clue to this modest result was to observe the Galois action on H_1 of the elementary abelian $(\mathbb{Z}/N\mathbb{Z})^{n-1}$-cover of $\mathbf{P}^1_{\bar{k}} - \{n \text{ points}\}$ so as to look at the kernel of its weight (-2) part, i.e., the kernel of the Galois permutation of cusps on the cover. A subtle point is that the Galois action depends on the choice of k-models of that cover, so that we need to extract a common invariant for all those possible k-models. At one other point, a technical lemma was employed "$k^\times \cap k(\mu_{l^r})^{\times l^r} = k^{\times l^r}$ for a number field $k \ni \sqrt{-1}$ and prime powers l^r" from Rubin's paper (*Invent. math.* 89 (1987), 511–526, lemma 5.7), accidentally found on the library bookshelves of the University of Tokyo. On a later day, I found the lemma traced back to Weil [47] chap. XIII, §8 lemma 9 (p. 273), while Rubin gave a much simpler proof by using Galois cohomology.

In the simplest case $\Lambda = \{0, 1, \infty, \lambda\}$, one has the multiplicative group $\Gamma(\Lambda) = \langle -1, \lambda, 1-\lambda \rangle \subset k^\times$. When $k = \mathbb{Q}$ or many quadratic fields, this can determine the isomorphism class of $\mathbf{P}^1 - \{0, 1, \infty, \lambda\}$. But already when $k = \mathbb{Q}(\sqrt{2})$, it fails: $\lambda = -1 + \sqrt{2}$, $\lambda' = (2 - \sqrt{2})/2$ giving the same $\Gamma(\Lambda)$ but non-isomorphic

$\mathbf{P}^1 - \Lambda$ ([6], example (4.6)). Efforts to improve the results of [6] required that we treat the Galois permutations of cusps directly, not only the kernel information about them. This motivated the group-theoretical characterization of the inertia subgroups in arithmetic fundamental groups described in §3, Key lemma. See also the next note.

Note 5

In the non-abelian free profinite group $\Pi_{g,n}$ ($n \geq 1$), the inertia subgroups over n punctures form a union $\mathcal{I}$ of conjugacy classes. Any individual inertia subgroup $I \subset \mathcal{I}$ is isomorphic to $\hat{\mathbb{Z}}$, which has a big normalizer in $\pi_1(U)$ of the form of an extension of the Galois group by $\hat{\mathbb{Z}}(1)$ (branch cycle argument). The Key lemma asserts the converse of this property, i.e., $\mathcal{I}$ can be characterized as the weight (-2) subset with weight (-1) complement in $\Pi_{g,n}$. This *anabelian weight filtration* was introduced in [7], [33] with certain techniques that pay careful attention to open neighborhoods.



It should be noted that this, in turn, can be used for a *purely group-theoretical characterization* of the set of sectional homomorphisms *at infinity*

$$\mathrm{Sect}_\infty := \left\{ s\colon G_k \to \pi_1(U) \;\middle|\; \begin{array}{c} s(G_k) \text{ lies in a decomposition} \\ \text{subgroup at a cusp} \end{array} \right\}$$

as the set of those sections $s\colon G_k \to \pi_1(U)$ each of which has a nontrivial pro-cyclic subgroup in $\Pi_{g,n}$ stabilized and acted on by $s(G_k)$ via multiplication by the cyclotomic character. This set includes sections arising from tangential base points formulated by Deligne [13] and Anderson–Ihara [9]. Recently, Esnault–Hai [15] shed new light on the set Sect_∞ and its cardinality. See also Koenigsmann [26] and Stix [43] for related discussions.

Note 6

The following argument was behind this passage. Let (E, O) be an elliptic curve over a number field k with lambda invariant $\lambda \in \bar{k}$. The 2-isogeny and the 4-isogeny induce etale covers $E - {}_2E$ and $E - {}_4E$ of the punctured curve $E - \{O\}$ respectively. Their function fields over $\bar{k}$ can be written as

$$\bar{k}(E - {}_2E) = \bar{k}(t, \sqrt{t(t-1)(t-\lambda)}),$$
$$\bar{k}(E - {}_4E) = \bar{k}(\sqrt{t}, \sqrt{t-1}, \sqrt{t-\lambda}).$$

Let $\Delta = (\mathbb{Z}/2\mathbb{Z})^2$ be the covering group between $E - {}_4E$ and $E - {}_2E$ over $\bar{k}$, and

regard the l-adic homology group $H_1(E - {}_4E, \mathbb{Z}_l)$ as a $(G_k \cdot \Delta)$-module. Then, (after taking a finite extension of k if necessary) the maximal Δ-coinvariant torsion-free quotient fits in the following exact sequence:

$$0 \longrightarrow \mathbb{Z}_l(1)^3 \longrightarrow H_1\left(E - {}_4E, \mathbb{Z}_l\right)_{\Delta}\Big/_{torsion} \longrightarrow H_1(E, \mathbb{Z}_l) \longrightarrow 0.$$

The group $H_1(E - {}_4E, \mathbb{Z}_l)$ has another interpretation as the Galois group of the maximal abelian pro-l extension of $\bar{k}(E - {}_4E)$ unramified outside the divisor ${}_4E$. It has a remarkable weight (-2) *quotient* corresponding to the Galois extension $\bar{k}(\sqrt[2l^\infty]{t}, \sqrt[2l^\infty]{t-1}, \sqrt[2l^\infty]{t-\lambda})$, which provides a canonical splitting of the above sequence. Once we know the sequence splits, we can recover the splitting uniquely by the weight argument, from which follows the group-theoretical characterization of the series of subgroups of $\pi_1(E - \{O\})$ corresponding to $\bar{k}(\sqrt[2l^n]{t}, \sqrt[2l^n]{t-1}, \sqrt[2l^n]{t-\lambda})$. Plugging this into the argument of looking at Galois permutations of cusps on abelian covers of $\mathbf{P}^1 - \{0, 1, \infty, \lambda\}$ discussed in §3, we conclude reconstitution of the cross ratio class of λ (hence $j(\lambda) \in k$) solely from information about $\pi_1(E - \{O\})$. This, together with k-isogeny $E \sim_k E'$ from Faltings' theorem, implies $E \cong_k E'$. One finds related extensions of this argument in Asada [10] §5.2 and Stix [43] §10.5.

The arithmetic fundamental group $\pi_1(E - \{O\})$ is a basic and fascinating object to study as well as $\pi_1(\mathbf{P}^1 - \{0, 1, \infty\})$. For instance, an elliptic analog of Ihara's theory [3] on Jacobi sum power series has been developed in [34], [36].

Note 7

Rigidity assertion discussed in §3:

$$(\text{Equiv})_U \qquad \pi_1(U) \cong_{G_k} \pi_1(U') \Longrightarrow U \cong_k U'$$

combined with the automorphism assertion of Problem X:

$$(\text{Aut})_U \qquad \frac{\text{Aut}_{G_k}\pi_1(U)}{\text{Inn}\,\pi_1} \cong \text{Aut}_k(U) : \textbf{a finite group!}$$

implies the isomorphism version of Grothendieck's conjecture:

$$\text{Isom}_k(U, U') \cong \text{Isom}_{G_k}(\pi_1(U), \pi_1(U'))/\text{Inn}(\pi_1(U' \otimes \bar{k})).$$

This has been settled by Tamagawa [45] and Mochizuki [29]. In both works, the assertions $(\text{Equiv})_V$ for finite etale covers V of U follow all together. Here remains a little open question. Does a collection of assertions $(\text{Equiv})_V$ for sufficiently many finite etale covers V of U imply $(\text{Aut})_U$ automatically?

Grothendieck suggested in [19](6) more generally to consider the mapping

$$(*) \qquad \text{Hom}_k(U, U') \longrightarrow \text{Hom}_{G_k}(\pi_1(U), \pi_1(U'))/\text{Inn}(\pi_1(U' \otimes \bar{k})).$$

The Hom-version of Grothendieck's conjecture asserts that the above mapping gives a bijection between the set of dominant k-morphisms $U \to U'$ and the set of classes of the G_k-compatible open homomorphisms $\pi_1(U) \to \pi_1(U')$. This has been settled by Mochizuki [30].

See also [38] for a review of works by Tamagawa and Mochizuki (and of the author) till 1997, where it was found important to investigate Grothendieck's conjecture after replacing the base number field k by other arithmetic fields (finite fields, sub-p-adic fields). Here, we do not enter into any more details. For further developments, see also the articles by Tamagawa, Saidi–Tamagawa, and Mochizuki contained in the book [42].

Grothendieck's section conjecture [19](7) comes from a special case of $(*)$ where $U = \mathrm{Spec}(k)$ and U' is a hyperbolic curve (written U instead of U'). Then, we obtain a mapping of the set of k-rational points $U(k)$ into $\mathrm{Sect}(\pi_1(U)/G_k)/\mathrm{conj}$, where Sect denotes the set of sectional homomorphisms and '/conj' means modulo conjugacy by elements of $\pi_1(U \otimes \bar{k})$. The section conjecture asserts the bijection of $U(k)$ onto those sections outside Sect_∞ of Note 5, namely,

$$U(k) \xrightarrow{\sim} \big(\mathrm{Sect}(\pi_1(U)/G_k) - \mathrm{Sect}_\infty\big)/\mathrm{conj}.$$

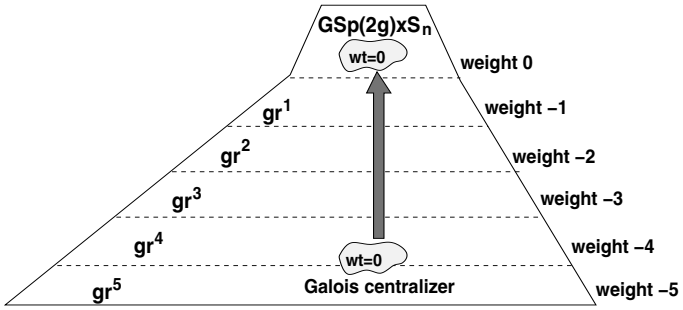
Injectivity for the section conjecture and its close relationship with injectivity for the general Hom-conjecture or with the above mentioned Equiv-conjecture under anticipated anabelian situations have been known at early stages of investigation (cf. [19], [32]). The section conjecture is still an open problem, but recently important evidence has appeared, such as Stix [44] and Harari–Szamuely [21].

Finally, one may consider cases where both U and U' are spectra of function fields of varieties in $(*)$. The 0-dimensional case is nothing but the Neukirch–Uchida theorem. For function field cases, there have been intensive studies and results initiated by Pop [40], Bogomolov [11] and their further developments (cf. the article by F. Pop in this volume).

Note 8

The left-hand side of Problem X turns out to be naturally isomorphic to the centralizer of the Galois image in $\mathrm{Out}(\Pi_{g,n})$ called the *Galois centralizer*. By virtue of the anabelian weight filtration, the Galois centralizer as well as the Galois image lies in $\mathrm{Out}^{\mathcal{I}}(\Pi_{g,n})$ defined as the group of outer automorphisms of $\Pi_{g,n}$ stabilizing the inertia subset $\mathcal{I}$. The pro-l version of Problem X mentioned here considers estimating the Galois centralizer in $\Gamma_{g,n}^{\text{pro-}l} := \mathrm{Out}^{\mathcal{I}}(\Pi_{g,n}^{\text{pro-}l})$, where we set up a certain natural filtration by normal subgroups having graded quotients $\mathrm{gr}^0 \cong \mathrm{GSp}(2g, \mathbb{Z}_l) \times S_n$ and gr^i $(i \geq 1)$ isomorphic to free $\mathbb{Z}_l$-modules

of finite ranks. By conjugation, each gr^i ($i \geq 1$) turns out to get a structure of "weight $(-i)$" GSp-module. Since the Galois centralizer is a priori of weight zero, it must inject into gr^0, i.e., into $\mathrm{Aut}(H_1(U \otimes \bar{k}))$ (cf. [37], [35]).



Indeed, more constraints to approximate the Galois centralizer to $\mathrm{Aut}_k(U)$ should be obtained from its commutativity with nontrivial Galois images distributed in $\Gamma_{g,n}^{\text{pro-}l}$. The Galois image in $\mathrm{gr}^0 = \mathrm{GSp}(2g) \times S_n$ is within standard knowledge from the theory of l-adic Galois representations on torsion points of Jacobians (e.g., Tate conjecture proved by Faltings), which also spreads weighted carpets on gr^i ($i \geq 1$) in the above sense according to Frobenius eigen-radii (Riemann–Weil hypothesis). On the other hand, to find Galois images submerging in negative weights (called *Torelli–Galois images*) requires new knowledge about Galois representations on fundamental groups. Deligne [12] and Oda [39] suggested that one could lift Ihara's theory on $\pi_1^{\text{pro-}l}(\mathbf{P}^1 - \{0, 1, \infty\})$ to any hyperbolic curve; namely, there should be a common factor for all Galois actions on pro-l fundamental groups (independent of the moduli) of hyperbolic curves. After the efforts of several authors, the last remaining case of this prediction – that of complete curves – has been settled (up to finite torsion) by Takao [46] (cf. [35], note (A4) added in English translation). Consequently, we have Torelli–Galois images in weights $-6, -10, -14, \ldots$ originated from Soule's cyclotomic characters, and find the pro-l Galois centralizer injected in $\mathrm{Sp}(2g) \times S_n$. In the original case $g = 0$, $n = 3$ considered here, it follows that the pro-l Galois centralizer for $\mathbf{P}^1 - \{0, 1, \infty\}$ coincides with S_3 as expected.

References

[Part 1] **References to [31] (1989)**

[1] G. V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk. SSSR **8** (1979), 267–276 (in Russian); *English transl. in* Math. USSR Izv. **14** (1980), 247–256.

[2] A. Grothendieck, *Esquisse d'un Programme*, mimeographed note 1984 (published later in [41]: Part 1, 5–48).

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

[4] Y. Ihara, *Some problems on three-point ramifications and associated large Galois representations*, in "Galois representations and arithmetic algebraic geometry", Adv. Stud. Pure Math., **12**, 173–188.

[5] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

[6] H. Nakamura, *Rigidity of the arithmetic fundamental group of* $\mathbf{P}^1 - \{0, 1, \infty, \lambda\}$, Preprint 1988 (UTYO-MATH 88-21); appeared under the title: *Rigidity of the arithmetic fundamental group of a punctured projective line*, J. Reine Angew. Math. 405 (1990), 117–130.

[7] H. Nakamura, *Galois rigidity of the etale fundamental groups of punctured projective lines*, Preprint 1989 (UTYO-MATH 89-2), appeared in final form from J. Reine Angew. Math. 411 (1990), 205–216.

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

[Part 2] **References added for Complementary notes**

[9] G. Anderson, Y. Ihara, *Pro-l branched coverings of* $\mathbf{P}^1$ *and higher circular l-units*, Part 1 : Ann. of Math. **128** (1988), 271–293; Part 2: Intern. J. Math. **1** (1990), 119–148.

[10] M. Asada, *The faithfulness of the monodromy representations associated with certain families of algebraic curves*, J. Pure and Applied Algebra, **159**, 123–147.

[11] F. A. Bogomolov, *On two conjectures in birational algebraic geometry*, in "Algebraic Geometry and Analytic Geometry" (A. Fujiki et al. eds.) (1991), 26–52, Springer Tokyo.

[12] P. Deligne, *letter to Y. Ihara*, December 11, 1984.

[13] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, in "Galois group over $\mathbb{Q}$" (Y. Ihara, K. Ribet, J.-P. Serre eds.), MSRI Publ. Vol. 16 (1989), 79–297.

[14] V. G. Drinfeld, *On quasitriangular quasi-Hopf algebras and a group closely connected with* $Gal(\bar{Q}/Q)$, Algebra i Analiz **2** (1990), 149–181 (in Russian); *English transl. in* Leningrad Math. J. **2(4)** (1991) 829–860.

[15] H. Esnault, P. H. Hai, *Packets in Grothendieck's section conjecture*, Adv. in Math., **218** (2008), 395–416.

[16] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[17] M. Fried, *Fields of definition of function fields and Hurwitz families — Groups as Galois groups*, Comm. in Algebra, **5** (1977), 17–82.

[18] A. Grothendieck, *Revêtement Etales et Groupe Fondamental* (SGA1), Lecture Note in Math. **224** Springer, Berlin Heidelberg New York, 1971.
[19] A. Grothendieck, *Letter to G. Faltings, June 1983*, in [41]: Part 1, 49–58.
[20] R. M. Hain, *The geometry of the mixed Hodge structures on the fundamental group*, Proc. Symp. Pure Math. **46** (1987), 247–282.
[21] D. Harari, T. Szamuely, *Galois sections for abelianized fundamental groups*, Math. Ann., **344** (2009), 779–800.
[22] Y. Hoshi, S. Mochizuki, *On the combinatorial anabelian geometry of nodally nondegenerate outer representations*, Preprint RIMS-1677, August 2009.
[23] Y. Ihara, *Braids, Galois groups and some arithmetic functions*, Proc. ICM, Kyoto, 99–120, 1990.
[24] Y. Ihara, H. Nakamura, *Some illustrative examples for anabelian geometry in high dimensions*, in [41]: Part 1, 127–138.
[25] M. Kim, *The motivic fundamental group of* $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ *and theorem of Siegel*, Invent. math. **161** (2005), 629–656.
[26] J. Koenigsmann, *On the 'Section Conjecture' in anabelian geometry*, J. reine angew. Math., **588** (2005), 221–235.
[27] P. Lochak, L. Schneps, *Open problems in Grothendieck-Teichmüller theory*, Proc. Symp. Pure Math. **74** (2006), 165–186.
[28] M. Matsumoto, *On Galois representations on profinite braid groups of curves*, J. reine angew. Math. **474** (1996), 169–219.
[29] S. Mochizuki, *The profinite Grothendieck conjecture for closed hyperbolic curves over number fields*, J. Math. Sci. Univ. Tokyo, **3** (1996), 571–627.
[30] S. Mochizuki, *The local pro-p anabelian geometry of curves*, Invent. Math. **138** (1999), 319–423.
[31] H. Nakamura, *On Galois rigidity of fundamental groups of algebraic curves* (in Japanese), Report Collection of the 35th Algebra Symposium held at Hokkaido University on July 19–August 1, pp. 186–199.
[32] —-, *Galois rigidity of algebraic mappings into some hyperbolic varieties*, Internat. J. Math. **4** (1993), 421–438.
[33] —-, *Galois rigidity of pure sphere braid groups and profinite calculus*, J. Math. Sci. Univ. Tokyo **1** (1994), 71–136.
[34] —-, *On exterior Galois representations associated with open elliptic curves*, J. Math. Sci., Univ. Tokyo **2** (1995), 197–231.
[35] —-. *Galois rigidity of profinite fundamental groups* (in Japanese), Sugaku **47** (1995), 1–17; *English transl. in* Sugaku Expositions (AMS) **10** (1997), 195-215.
[36] —-, *On arithmetic monodromy representations of Eisenstein type in fundamental groups of once punctured elliptic curves*, Preprint RIMS-1691, February 2010.
[37] H. Nakamura, H. Tsunogai, *Some finiteness theorems on Galois centralizers in pro-l mapping class groups*, J. Reine Angew. Math. 441 (1993), 115–144.
[38] H. Nakamura, A. Tamagawa, S. Mochizuki, *The Grothendieck conjecture on the fundamental groups of algebraic curves*, (in Japanese), Sugaku **50** (1998), 113–129; *English transl. in* Sugaku Expositions (AMS), **14** (2001), 31–53.
[39] T. Oda, *The universal monodromy representations on the pro-nilpotent fundamental groups of algebraic curves*, Mathematische Arbeitstagung (Neue Serie) 9-15 Juin 1993, Max-Planck-Institute preprint MPI/93-57 (1993).

[40] F. Pop, *On the Galois theory of function fields of one variable over number fields*, J. reine. angew. Math., **406** (1988), 200–218.

[41] L. Schneps, P. Lochak (eds.), *Geometric Galois Actions; 1.Around Grothendieck's Esquisse d'un Programme, 2.The Inverse Galois Problem, Moduli Spaces and Mapping Class Groups*, London Math. Soc. Lect. Note Ser. **242–243**, Cambridge University Press 1997.

[42] L. Schneps (ed.), *Galois groups and fundamental groups*, MSRI Publications, **41**, 2003.

[43] J. Stix, *On cuspidal sections of algebraic fundamental groups* Preprint 2008 (arXiv:0802.4125).

[44] J. Stix, *On the period-index problem in light of the section conjecture*, Amer. J. Math., **132** (2010), 157-180.

[45] A. Tamagawa *The Grothendieck conjecture for affine curves*, Compositio Math. **109** (1997), 135–194.

[46] N. Takao, *Braid monodormies on proper curves and pro-ℓ Galois representations*, Jour Inst. Math. Jussieu, (to appear).

[47] A. Weil, *Basic Number Theory*, Grundlehren der math. Wiss. in Einzeldarstellungen, Band 144, Springer 1974.