Iranian Journal of Mathematical Sciences and Informatics
Vol. 14, No. 2 (2019), pp 157-171
DOI: 10.7508/ijmsi.2019.02.014

Arithmetic Teichmuller Theory

Arash Rastegar

Department of Mathematics, Sharif University of Technology, Tehran, Iran.

E-mail: rastegar@sharif.edu, rastegar1352@gmail.com

This paper is dedicated to Maryam Mirzakhani's 40th birthdate and early elevation

Abstract. By Grothendieck's anabelian conjectures, Galois representations landing in outer automorphism group of the algebraic fundamental group which are associated to hyperbolic smooth curves defined over number-fields encode all the arithmetic information of these curves. The Goal of this paper is to develop an arithmetic Teichmuller theory, by which we mean, introducing arithmetic objects summarizing the arithmetic information coming from all curves of the same topological type defined over number-fields. We also introduce Hecke-Teichmuller Lie algebra which plays the role of Hecke algebra in the anabelian framework.

Keywords: Outer Galois representations, Arithmetic Teichmuller theory, Grothendieck's anabelian conjectures.
2000 Mathematics subject classification: 14G32(11F80).

1. Introduction

This paper is continuation of two papers on outer representations of Galois group [22, 23]. One canonically associates to a proper smooth curve X which is geometrically reduced and is defined over a number field K a continuous group homomorphism

$$\rho_X : Gal(\bar{K}/K) \longrightarrow Out(\pi_1^{alg}(X))$$

where $Out(\pi_1^{alg}(X))$ denotes the quotient of the aut. group $Aut(\pi_1^{alg}(X))$ by inner automorphisms of the algebraic fundamental group. By a conjecture of

Received 01 December 2016; Accepted 04 December 2017

Matsumoto [17] and Voevodski [29] the outer Galois representation is injective when topological fundamental group of X is nonabelian. Special cases of this conjecture are proved by Belyi for $\mathbb{P}^1 - \{0, 1, \infty\}$ [2], by Voevodski in cases of genus zero and one [29], and by Matsumoto for affine X using Galois action on profinite braid groups [17].

By Grothendieck's anabelian conjectures, in the case of hyperbolic curves, the Galois module structure of $Out(\pi_1(X))$ should inherit all the arithmetic information of the curve. In particular, it should produce all points defined over number-fields and should characterize the isomorphism class of X over K. The former is called Grothendieck's "section conjecture" and the latter is implied by Gorthendieck's "Hom conjecture" which is proved by Mochizuki [19]. Thus, given X and X' hyperbolic curves, the natural map

$$Isom_K(X, X') \longrightarrow Out_{Gal(\bar{K}/K)}(Out(\pi_1^{alg}(X)), Out(\pi_1^{alg}(X')))$$

is a one-to-one correspondence. Here $Out_{Gal(\bar{K}/K)}$ denotes the group of Galois equivariant isomorphisms between the two profinite groups.

In this paper, we introduce an arithmetic structure summarizing all such arithmetic information for hyperbolic smooth curves of given topological type defined over K. More precisely, we shall summarize all ρ_X in a single Galois representation. This would be the beginning of arithmetic Teichmuller theory.

From now on, we assume that $2g - 2 + n > 0$ to ensure hyperbolicity. The stack $M_{g,n}$ is defined as the moduli stack of n-pointed genus g curves. By a family of n-pointed genus g curves over a scheme S, we mean a proper smooth morphism $C \to S$ whose fibers are proper smooth curves of genus g, together with n sections $s_i : S \to C$ for $i = 1, ..., n$ whose images do not intersect.

The moduli stack $M_{g,n}$ is an algebraic stack over $Spec(\mathbb{Z})$. One can define the etale fundamental group of the stack $M_{g,n}$ in the same manner one defines etale fundamental group of schemes. Oda showed that the etale homotopy type of the algebraic stack $M_{g,n} \otimes \bar{\mathbb{Q}}$ is the same as the analytic stack $M_{g,n}^{an}$ and its algebraic fundamental group is isomorphic to the completion $\widehat{\Gamma_{g,n}}$ of the Teichmuller modular group, or the mapping class group of n-punctured genus g Riemann surfaces [16] :

$$\pi_1^{alg}(M_{g,n} \otimes \bar{\mathbb{Q}}) \cong \widehat{\Gamma_{g,n}}.$$

Triviality of π_2 implies exactness of the following short sequence for the universal family $C_{g,n} \longrightarrow M_{g,n}$ over the moduli stack

$$0 \longrightarrow \pi_1^{alg}(X, b) \longrightarrow \pi_1^{alg}(C_{g,n}, b) \longrightarrow \pi_1^{alg}(M_{g,n}, a) \longrightarrow 0$$

where X is the fiber on a and b is a point on $C_{g,n}$. Using this exact sequence, one defines the arithmetic universal monodromy representation

$$\rho_{g,n} : \pi_1^{alg}(M_{g,n}, a) \longrightarrow Out(\pi_1^{alg}(X))$$

In fact, after restriction to $\pi_1^{alg}(M_{g,n} \otimes \bar{\mathbb{Q}}, a)$, this is the completion of the natural map

$$\Gamma_{g,n} \longrightarrow Out(\Pi_{g,n})$$

where $\Pi_{g,n}$ denotes the topological fundamental group of the curve of genus g with n punctures.

On can think of the Galois module structure of $Out(\pi_1^{alg}(M_{g,n} \otimes \bar{\mathbb{Q}}))$ as a replacement for the Teichmuller space. This object has the information of all outer representations associated to smooth curves over $\mathbb{Q}$. Indeed, by fixing such a hyperbolic curve X of genus g with n punctures defined over $\mathbb{Q}$, we have introduced a rational point on the moduli stack $a \in M_{g,n}$ and thus a Galois representation

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \pi_1^{alg}(M_{g,n}, a)$$

which splits the following short exact sequence

$$0 \longrightarrow \pi_1^{alg}(M_{g,n} \otimes \bar{\mathbb{Q}}, a) \longrightarrow \pi_1^{alg}(M_{g,n}, a) \longrightarrow Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 0.$$

Composing with the arithmetic universal monodromy representation, we get

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Out(\pi_1^{alg}(X))$$

which recovers the canonical outer representation associated to X. Therefore, the following universal Galois representation

$$\rho_{univ} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Out(\pi_1^{alg}(M_{g,n} \otimes \bar{\mathbb{Q}})) = Out(\widehat{\Gamma_{g,n}})$$

is the arithmetic analogue of the Teichmuller space. Here, we have assumed that, one can treat $M_{g,n}$ as an anabelian space whose arithmetic is governed by Grothendieck's anabelian conjectures, as was expected by Grothendieck.

Having this picture in mind, we try to translate this arithmetic information to the language of Lie algebras in order to make it more accessible computationally.

2. Background Material

The study of outer representations of the Galois group has two origins. One root is the theme of anabelian geometry introduced by Grothendieck [7] which lead to results of Nakamura, Tamagawa and Mochizuki who solved the problem in dimension one [19]. The second theme which is originated by Deligne and Ihara independently deals with Lie-algebras associated to the pro-l outer representation [6, 10] . This lead to a partial proof of a conjecture by Deligne [8] . In the first part, we will review the weight filtration introduced by Oda (after Deligne and Ihara) and a circle of related results.

2.1. **Weight filtration on $\widetilde{Out}(\pi_1^l(X))$.** By a result of Grothendieck [7] the pro-l geometric fundamental group $\pi_1^l(X_{\bar{K}})$ of a smooth algebraic curve X over $\bar{K}$ is isomorphic to the pro-l completion of its topological fundamental group, after extending the base field to the field of complex numbers. The topological fundamental group of a Riemann surface of genus g with n punctured points has the following standard presentation:

$$\Pi_{g,n} \cong < a_1, ..., a_g, b_1, ..., b_g, c_1, ..., c_n | \prod_{i=1}^{g} [a_i, b_i] \prod_{j=1}^{n} c_j = 1 > .$$

Let $Aut(\pi_1^l(X))$ denote the group of continuous automorphisms of the pro-l fundamental group of X and $Out(\pi_1^l(X))$ denote its quotient by the subgroup of inner automorphisms. We will induce filtrations on particular subgroups of these two groups.

Let $\bar{X}$ denote the compactification of X obtained by adding finitely many points. $\bar{X}$ is still defined over K. Let $\lambda : Aut(\pi_1^l(\bar{X})) \to GL(2g, \mathbb{Z}_l)$ denote the map induced by abelianization. The natural actions of $Aut(\pi_1^l(\bar{X}))$ on cohomology groups $H^i(\pi_1^l(\bar{X}), \mathbb{Z}_l)$ are compatible with the non-degenerate alternating form defined by the cup product:

$$H^1(\pi_1^l(\bar{X}), \mathbb{Z}_l) \times H^1(\pi_1^l(\bar{X}), \mathbb{Z}_l) \to H^2(\pi_1^l(\bar{X}), \mathbb{Z}_l) \cong \mathbb{Z}_l.$$

This shows that the image of λ is contained in $GSp(2g, \mathbb{Z}_l)$. One can prove that λ is surjective and if $\tilde{\lambda}$ denotes the natural map

$$\tilde{\lambda} : Out(\pi_1^l(\bar{X})) \longrightarrow GSp(2g, \mathbb{Z}_l)$$

there are explicit examples showing that the Galois representation $\rho_X^l \circ \tilde{\lambda}$ does not fully determine the original anabelian Galois representation [1] .

Let $\widetilde{Aut}(\pi_1^l(X))$ denote the Braid subgroup of $Aut(\pi_1^l(X))$ which consists of those elements taking each c_i to a conjugate of a power c_i^{σ} for some σ in $\mathbb{Z}_l^*$. There is a natural surjective map

$$\pi_X : \widetilde{Aut}(\pi_1^l(X)) \longrightarrow Aut(\pi_1^l(\bar{X}))$$

Oda uses $\tilde{\lambda}$ to study natural filtrations on $\widetilde{Aut}(\pi_1^l(X))$ and $\widetilde{Out}(\pi_1^l(X))$. In the special case of $X = \mathbb{P}^1 - \{0, 1, \infty\}$ this is the same filtration as the filtration introduced by Deligne and Ihara. This filtration is also used by Nakamura in bounding Galois centralizers [20]. Consider the central series of the pro-l fundamental group

$$\pi_1^l(X) = I^1\pi_1^l(X) \supset I^2\pi_1^l(X) \supset ... \supset I^m\pi_1^l(X) \supset ...$$

and let $I^1Aut(\pi_1^l(X))$ denote the kernel of $\pi_X \circ \lambda$. The central series filtration is not the most appropriate for non-compact X. In general, we consider the weight filtration, namely the fastest decreasing central filtration such that

$$I^2\pi_1^l(X) = < [\pi_1^l(X), \pi_1^l(X)], c_1, ..., c_n >_{\text{norm}}$$

where $< \ . \ >_{\text{norm}}$ means the closed normal subgroup generated by these elements. For $m \geq 3$ we define

$$I^m \pi_1^l(X) =< [I^i \pi_1^l(X), I^j \pi_1^l(X)] | i + j = m >_{\text{norm}} .$$

The weight filtration induces a filtration on the automorphism group of braid type by normal subgroups

$$\widetilde{Aut}(\pi_1^l(X)) = I^0 \widetilde{Aut}(\pi_1^l(X)) \supset I^1 \widetilde{Aut}(\pi_1^l(X)) \supset ... \supset I^m \widetilde{Aut}(\pi_1^l(X)) \supset ...$$

$$I^m \widetilde{Aut}(\pi_1^l(X)) = \{\sigma \in \widetilde{Aut}(\pi_1^l(X)) | x^\sigma x^{-1} \in I^{m+1} \pi_1^l(X) \text{ for all } x \in \pi_1^l(X)\}$$

The following propositions are proved in [13] :

Proposition 2.1. *The weight filtration on $\widetilde{Aut}(\pi_1^l(X))$ satisfies*

$$[I^m \widetilde{Aut}(\pi_1^l(X)), I^n \widetilde{Aut}(\pi_1^l(X))] \subset I^{m+n} \widetilde{Aut}(\pi_1^l(X))$$

for all m and n, and induces a Lie-algebra structure on the associated graded object $Gr_I^\bullet \widetilde{Aut}(\pi_1^l(X)) = \bigoplus gr^m \widetilde{Aut}(\pi_1^l(X))$. The graded pieces

$$gr^m \widetilde{Aut}(\pi_1^l(X)) = I^m \widetilde{Aut}(\pi_1^l(X)) / I^{m+1} \widetilde{Aut}(\pi_1^l(X))$$

are free $\mathbb{Z}_l$-modules of finite rank for all positive m.

The weight filtration on the automorphism group of pro-l fundamental group induces a filtration on the outer automorphism group of braid type

$$\widetilde{Out}(\pi_1^l(X)) = I^0 \widetilde{Out}(\pi_1^l(X)) \supset I^1 \widetilde{Out}(\pi_1^l(X)) \supset ... \supset I^m \widetilde{Out}(\pi_1^l(X)) \supset ...$$

Proposition 2.2. *The induced filtration on $\widetilde{Out}(\pi_1^l(X))$ satisfies*

$$[I^m \widetilde{Out}(\pi_1^l(X)), I^n \widetilde{Out}(\pi_1^l(X))] \subset I^{m+n} \widetilde{Out}(\pi_1^l(X))$$

for all m and n, and induces a Lie-algebra structure on the associated graded object $Gr_I^\bullet \widetilde{Out}(\pi_1^l(X)) = \bigoplus gr^m \widetilde{Out}(\pi_1^l(X))$. The graded pieces

$$gr^m \widetilde{Out}(\pi_1^l(X)) = I^m \widetilde{Out}(\pi_1^l(X)) / I^{m+1} \widetilde{Out}(\pi_1^l(X))$$

are finitely generated $\mathbb{Z}_l$-module for all positive m.

These two propositions are proved in [13] . One can induce filtrations on $Aut(\pi_1^l(X))$ and $Out(\pi_1^l(X))$ using the natural surjection

$$Aut(\pi_1^l(X)) \longrightarrow GSp(2g, \mathbb{Z}_l)$$

which is induced by the action of $Aut(\pi_1^l(X))$ on $gr^1 \pi_1^l(X) \cong \mathbb{Z}_l^{2g}$.

2.2. **Graded pieces of $\widetilde{Out}(\pi_1^l(X))$.** The explicit presentation of the fundamental group of a Riemann surface given in the previous section implies that $\pi_1^l(X)$ is a one-relator pro-l group and therefore very close to a free pro-l group. The groups $Aut(\pi_1^l(X))$ and $Out(\pi_1^l(X))$ also look very similar to automorphism group and outer automorphism group of a free pro-l group [24] . This can be shown more precisely in the particular case of $\widetilde{Out}(\pi_1^l(X))$.

The graded pieces of $Gr_I^\bullet\widetilde{Out}(\pi_1^l(X))$ can be completely determined in terms of the graded pieces of $Gr_I^\bullet\pi_1^l(X)$ which are free $\mathbb{Z}_l$-modules. In fact, $Gr_I^\bullet\pi_1^l(X)$ is a free Lie-algebra over $\mathbb{Z}_l$ generated by images of a_i's and b_i's in $gr^2\pi_1^l(X)$ for $1 \leq i \leq g$ and c_j's in $gr^3\pi_1^l(X)$ for $1 \leq j \leq n$. We denote these generators by $\bar{a}_i$,$\bar{b}_i$ and $\bar{c}_j$ respectively.

Let g_m denote the following injective $\mathbb{Z}_l$-linear homomorphism

$$g_m : gr^m\pi_1^l(X) \longrightarrow (gr^{m+1}\pi_1^l(X))^{2g} \times (gr^m\pi_1^l(X))^n$$

$$g \mapsto ([g, \bar{a}_i])_{1\leq i\leq g} \times ([g, \bar{b}_i])_{1\leq i\leq g} \times (g)_{1\leq j\leq n}$$

and f_m denote the following surjective $\mathbb{Z}_l$-linear homomorphism

$$f_m : (gr^{m+1}\pi_1^l(X))^{2g} \times (gr^m\pi_1^l(X))^n \longrightarrow gr^{m+2}\pi_1^l(X)$$

$$(r_i)_{1\leq i\leq g} \times (s_i)_{1\leq i\leq g} \times (t_j)_{1\leq j\leq n} \mapsto \sum_{i=1}^{g}([\bar{a}_i, s_i] + [r_i, \bar{b}_i]) + \sum_{j=1}^{n}[t_j, \bar{c}_j].$$

Proposition 2.3. *The graded pieces of $Gr_I^\bullet\widetilde{Out}(\pi_1^l(X))$ fit into the following short exact sequence of $\mathbb{Z}_l$-modules*

$$gr^m\widetilde{Out}(\pi_1^l(X)) \hookrightarrow (gr^{m+1}\pi_1^l(X))^{2g} \times (gr^m\pi_1^l(X))^n / gr^m\pi_1^l(X) \twoheadrightarrow gr^{m+2}\pi_1^l(X)$$

where embedding of $gr^m\pi_1^l(X)$ inside $(gr^{m+1}\pi_1^l(X))^{2g} \times (gr^m\pi_1^l(X))^n$ is defined by g_m and the final surjection is induced by f_m.

This tool helps to work with the graded pieces of $Gr_I^\bullet\widetilde{Out}(\pi_1^l(X))$ as fluently as the graded pieces of $Gr_I^\bullet\pi_1^l(X)$. In particular, it enabled Koneko to prove the following profinite version of the Dehn-Nielson theorem [13] :

Theorem 2.4. *(Koneko) Let X be a smooth curve defined over a number-field K and let Y denote an embedded curve in X obtained by omitting finitely many K-rational points. Then the natural map*

$$\widetilde{Out}(\pi_1^l(Y)) \longrightarrow \widetilde{Out}(\pi_1^l(X))$$

is a surjection.

This can be easily proved by diagram chasing between the corresponding short exact sequences for Y and X. The above exact sequence first appeared in the work of Ihara [10] and then generalized by Asada and Koneko [1, **?**].

2.3. **Filtrations on the Galois group.** If all of the points in complement $\bar{X} - X$ are K-rational, then the pro-l outer representation of the Galois group lands in the braid type outer automorphism group

$$\tilde{\rho}_X^l : Gal(\bar{K}/K) \longrightarrow \widetilde{Out}(\pi_1^l(X))$$

and the weight filtration on the pro-l outer automorphism group induces a filtration on the absolute Galois group mapping to $\widetilde{Out}(\pi_1^l(X))$ and also an injection between associated Lie algebras over $\mathbb{Z}_l$ defined by each of these filtrations

$$Gr^\bullet_{X,l} Gal(\bar{K}/K) \hookrightarrow Gr^\bullet_I \widetilde{Out}(\pi_1^l(X)).$$

Proposition 2.5. *Let X and Y denote smooth curves over K and let $\phi : X \to Y$ denote a morphism also defined over K. Then ϕ induces a commutative diagram of Lie algebras*

$$\begin{array}{ccc} Gr^\bullet_{X,l} Gal(\bar{K}/K) & \hookrightarrow & Gr^\bullet_I \widetilde{Out}(\pi_1^l(X)) \\ \downarrow \phi_{**} & & \downarrow \phi_* \\ Gr^\bullet_{Y,l} Gal(\bar{K}/K) & \hookrightarrow & Gr^\bullet_I \widetilde{Out}(\pi_1^l(Y)) \end{array}$$

If ϕ induces a surjection on topological fundamental groups, then ϕ_* and ϕ_{**} will also be surjective.

Proof. The claim is true because ϕ_* is Galois equivariant and graded pieces of $Gr^\bullet_I \widetilde{Out}(\pi_1^l(X))$ can be represented in terms of exact sequences on graded pieces of $Gr^\bullet_I \pi_1^l(X)$ [**?**] . □

Proposition 2.6. *Let X be an affine smooth curve X over K whose complement has a K-rational point. Then there is a morphism*

$$Gr^\bullet_{X,l} Gal(\bar{K}/K) \to Gr^\bullet_{\mathbb{P}^1 - \{0,1,\infty\},l} Gal(\bar{K}/K).$$

Proof. This is a consequence of theorem 3.1 in [17] . □

Proposition 2.7. *There exists a finite set of primes S such that we have an isomorphism*

$$Gr^\bullet_{X,l} Gal(\bar{K}/K) \cong Gr^\bullet_{X,l} Gal(K_S^{un}/K)$$

where $Gal(K_S^{un}/K)$ denotes the Galois group of the maximal algebraic extension unramified outside S

Proof. Indeed, Grothendieck proved that the representation $\tilde{\rho}_X^l$ factors through $Gal(K_S^{un}/K)$ for a finite set of primes S. S can be taken to be primes of bad reduction of X and primes over l [Gro]. This is also proved independently by Ihara in the special case of $X = \mathbb{P}^1 - \{0, 1, \infty\}$ [Iha]. □

The importance of this result of Grothensieck is the fact that $Gal(K_S^{un}/K)$ is a finitely generated profinite group [21] and therefore, the moduli of its representations is a scheme of finite type.

For a Lie algebra L over $\mathbb{Z}_l$ let $Der(L)$ denote the set of derivations, which are defined to be $\mathbb{Z}_l$-linear homomorphisms $D : L \to L$ with

$$D([u,v]) = [D(u), v] + [u, D(v)]$$

for all u and v in L, and let $Inn(L)$ denote the set of inner derivations, which are defined to be derivations with $D(u) = [u, v]$ for some fixed $v \in L$. Then we have the following Lie algebra version of the outer representation of the Galois group

$$Gr^{\bullet}_{X,l}Gal(\bar{K}/K) \to Der(Gr^{\bullet}_{I}\pi_1^l(X))/Inn(Gr^{\bullet}_{I}\pi_1^l(X))$$

$$\sigma \in gr^m Gal(\bar{K}/K) \mapsto (u \mapsto \tilde{\sigma}(\tilde{u}).\tilde{u}^{-1}) \bmod I^{m+n+1}\pi_1^l(X)$$

where $u \in gr^n\pi_1^l(X)$ with $\tilde{u} \in I^n\pi_1^l(X)$ and $\tilde{\sigma} \in I^m Gal(\bar{K}/K)$ is a lift of σ. In fact, for a free graded algebra, one can naturally associate a grading on the the algebra of derivations. Let $L = \oplus_i L^i$ be a free graded Lie algebra and let D denote the derivation algebra of L. Then define

$$D^i = \{d \in D | d(L^j) \subset L^{i+j}\}.$$

Then every element $d \in D$ is uniquely represented in the form $d = \sum_i d^i$ with $d^i \in D^i$ such that for any $f \in L$ the component $d^i f$ vanishes for almost all i. One can prove that

$$[D^i, D^j] \subset D^{i+j} \text{ and } [D_1, D_2]^k = \sum_{i+j=k} [D_1^i, D_2^j].$$

One can mimic the same construction on the graded algebra associated to $\pi_1^l(X)$ to get a graded algebra of derivations [27] .

One shall notice that in case $X = \mathbb{P}^1 - \{0, 1, \infty\}$ the group $\pi_1^l(X)$ is the pro-l completion of a free group with two generators. Ihara proves that the associated Lie algebra $Gr^{\bullet}_{I}(\pi_1^l(X))$ is also free over two generators say x and y [10]. Now for f in the m-th piece of the grading of the Lie algebra, there is a unique derivation $D_f \in Der(Gr^{\bullet}_{I}(\pi_1^l(X)))$ which satisfies $D_f(x) = 0$ and $D_f(y) = [y, f]$. One can show that $D_f(y)$ is non-zero for non-zero m and that for any $\sigma \in Gr^{\bullet}_{I}(\pi_1^l(X))$ there exists a unique $f \in Gr^{\bullet}_{I}(\pi_1^l(X))$ with image of σ being equal to D_f [18] . Now it is enough to let $\sigma = \sigma_m$ the Soule elements, to get a non-zero image $D_{f_{\sigma_m}}$.

Conjecture 2.8. *(Deligne* [6] *) The graded Lie algebra*

$$(Gr^{\bullet}_{\mathbb{P}^1-\{0,1,\infty\},l}Gal(\bar{\mathbb{Q}}/\mathbb{Q})) \otimes \mathbb{Q}_l$$

is a free graded Lie algebra over $\mathbb{Q}_l$ which is generated by Soule elements and the Lie algebra structure is induced from a Lie algebra over $\mathbb{Z}$ independent of l.

Remark 2.9. It is reasonable to expect freeness to hold for

$$(Gr^{\bullet}_{X,l}Gal(\bar{\mathbb{Q}}/\mathbb{Q})) \otimes \mathbb{Q}_l.$$

This implies that the above graded Lie algebra representation is also injective. Ihara showed that Soule elements do generate $Gr^{\bullet}_{X,l}(Gal(\bar{\mathbb{Q}}/\mathbb{Q})) \otimes \mathbb{Q}_l$ if one assumes freeness of this Lie algebra [10] . Hain and Matsumoto proved the same result without assuming any part of Deligne's conjecture [8] .

3. The Completion of Mapping Class Group

The mapping class group $MC(X)$ of X is defined as the factor of the group of homeomorphisms of X as a Riemann surface by the subgroup of elements isotopic to identity. The mapping class group is isomorphic to the group of outer automorphisms of the topological fundamental group

$$MC(X) \cong Out(\pi_1^{top}(X)).$$

There has been many efforts to introduce a finite presentation for this group. The ones introduced by Birman [3] for the case of genus 2 look particularly simple. The generators $\sigma_1, ..., \sigma_5$ together with the following relations generate $MC(X_2)$.

$$\begin{array}{ll}
\sigma_i\sigma_j = \sigma_j\sigma_i, & \text{for } |i-j| \geq 2,\ 1 \leq i,j \leq 5 \\
\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, & 1 \leq i \leq 4 \\
(\sigma_1\sigma_2...\sigma_5)^6 = 1 & \\
(\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5^2\sigma_4\sigma_3\sigma_2\sigma_1)^2 = 1 & \\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5^2\sigma_4\sigma_3\sigma_2\sigma_1 \perp \sigma_i, & 1 \leq i \leq 5
\end{array}$$

where $x \perp y$ means that x and y commute. For $g \geq 3$ genus, Dehn 1938 [5] , Lickorish 1965 [15] , Hatcher and Thurston 1980 [9] , Wajnryb 1983 [30] , gave presentations of the mapping class group. In all these presentations, the number of generators increases with g. However, Suzuki in 1977 showed that one can manage with four generators [26]. We give automorphisms in $Aut(\pi_1^{top}(X))$ whose image in $MC(X) = Aut(\pi_1^{top}(X))/Inn(\pi_1^{top}(X))$ generate the mapping class group.

$$\alpha_0 : \left(\begin{array}{c} a_1 \to b_1^{-1}, a_j \to a_j, j \neq 1 \\ b_1 \to b_1^{-1}a_1b_1, b_j \to b_j, j \neq 1 \end{array} \right)$$

$$\alpha_1 : \left(\begin{array}{c} a_i \to a_{i+1}, 1 \leq i \leq g-1, a_g \to a_1 \\ b_i \to b_{i+1}, 1 \leq i \leq g-1, b_g \to b_1 \end{array} \right)$$

$$\alpha_2 : \left(\begin{array}{c} a_i \to a_i, 1 \leq i \leq g \\ b_1 \to b_1^{-1}, b_j \to b_j, 2 \leq j \leq g \end{array} \right)$$

$$\alpha_3 : \left(\begin{array}{c} a_2 \to b_2a_2(b_1^{-1}a_1b_1)(a_2^{-1}b_2^{-1}a_2) \\ a_j \to a_j, j \neq 2 \\ b_1 \to b_1(a_2^{-1}b_2^{-1}a_2) \\ b_j \to b_j, 2 \leq j \leq g \end{array} \right)$$

We define the groups $MC^-(X)$ and $MC^+(X)$ as the images of L^- and L^+ under the canonical homomorphism $Aut(\pi_1^{top}(X)) \longrightarrow MC(X)$. The generators for $MC^-(X)$ and $MC^+(X)$ are also introduced by Suzuki in 1977. The automorphisms α_1, α_2, and α_3 generate $MC^-(X)$. The generators of $MC^+(X)$ are the following. Here s_i denotes the word $b_i^{-1}a_i^{-1}b_ia_i$ for $1 \leq i \leq g$.

$$\alpha_4 : \begin{pmatrix} a_1 \to b_1^{-1}a_1^{-1}b_1, a_j \to a_j, 2 \leq j \leq g \\ b_1 \to b_1^{-1}s_1^{-1}, b_j \to b_j, 2 \leq j \leq g \end{pmatrix}$$

$$\alpha_5 : \begin{pmatrix} a_1 \to s_1^{-1}a_2s_1, a_2 \to a_1, a_j \to a_j, 3 \leq j \leq g \\ b_1 \to s_1^{-1}b_2s_1, b_2 \to b_1, b_j \to b_j, 3 \leq j \leq g \end{pmatrix}$$

$$\alpha_6 : \begin{pmatrix} a_i \to a_i, 1 \leq i \leq g \\ b_1 \to a_1b_1a_2^{-1}s_2(b_1^{-1}a_1^{-1}b_1) \\ b_2 \to b_2a_2(b_1^{-1}a_1^{-1}b_1)a_2^{-1} \\ b_j \to b_j, 3 \leq j \leq g \end{pmatrix}$$

By studying the mapping class group, we have considered generators of

$$Out(\pi_1^{top}(X)).$$

In order to understand the algebraic geometric analogue $Out(\pi_1^{alg}(X))$ we shall study $Aut(\pi_1^{alg}(X))$ in more detail.

It is well known that, for a profinite group G which admits a fundamental system of open neighborhoods of the identity consisting of characteristic subgroups, there exists a topological isomorphism,

$$Aut(G) \cong \varprojlim Aut(G/U)$$

where U runs over open characteristic subgroups of G. We have an injection $\pi_1^{top}(X) \longrightarrow \pi_1^{alg}(X))$. An element of $Aut(\pi_1^{top}(X))$ fixes every characteristic open subgroup U and induces a compatible system of elements in $Aut(A/U)$ for different U and therefore an element of $\lim Aut(G/U)$. We have constructed an injection

$$Aut(\pi_1^{top}(X)) \longrightarrow Aut(\pi_1^{alg}(X)).$$

Inner automorphisms of $\pi_1^{top}(X)$ induce inner automorphisms of the completion $\pi_1^{alg}(X)$. Thus we get a second injection,

$$Out(\pi_1^{top}(X)) \longrightarrow Out(\pi_1^{alg}(X)).$$

If we prove that $Aut(\pi_1^{alg}(X))$ is the profinite completion of $Aut(\pi_1^{top}(X))$, we have shown that $Out(\pi_1^{alg}(X))$ is the completion of $Out(\pi_1^{top}(X)) \cong MC(X)$ in the profinite topology . It is enough to show that $\pi_1^{alg}(X)$ has a fundamental system of open characteristic subgroups which are completions of open subgroups of $\pi_1^{top}(X)$ in the profinite topology. We know that every automorphism of $\pi_1^{top}(X)$ is induced by an automorphism of $F(a_1, ..., a_g, b_1, ..., b_g)$. So it is enough to show that every free group has a fundamental system of open

characteristic subgroups. But this is proved to be true for a finitely generated free group. Therefore we have a representation of Galois group landing on the profinite completion of $MC(X)$

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Out(\pi_1^{alg}(X)) \cong \widehat{MC(X)}.$$

Uchida in 1976 [28] and Ikeda in 1977 [12] proved that every automorphism of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is inner. Therefore the equivalence class of Galois representations

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Out(\pi_1^{alg}(X))$$

has only one element. This is unlike the case of p-adic Galois representations associated to elliptic curves.

Translating the Galois representation from the language of automorphisms to the language of mapping class group, gives us a opportunity to geometrically define invariants of the Galois representation. For example, one shall be able to give a purely geometric definition of the conductor of a Galois representation.

4. Arithmetic Teichmuller Theory

Here, we shall fulfill our promise of developing an arithmetic Teichmuller theory. The universal representation

$$\rho_{univ} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Out(\widehat{\Gamma_{g,n}})$$

as explained in the introduction summarizes the arithmetic information coming from all curves of the same topological type defined over number-fields. The aim is to translate this to the language of Lie algebras. Although we lose some information, Lie algebras are much more flexible for computations rather than Galois representations landing in outer automorphism groups.

In the first part, we introduce Hecke-Teichmuller Lie algebra which plays the role of Hecke algebra in the anabelian framework. Then, in the second section, we bring in the story of elliptic curves and modularity. Finally, Galois action on the Hecke-Teichmuller Lie algebra is related to elliptic curves.

4.1. **Hecke-Teichmuller graded Lie algebras.** There is no general analogue for Hecke operators in the context of Lie algebras constructed in this manner. What we need is an analogue of Hecke algebra which contains all the information of Galois outer representations associated to elliptic curves. In fact, we will provide an algebra containing such information for hyperbolic smooth curves of given topological type.

From now on, we assume that $2g - 2 + n > 0$. Note that elliptic curves punctured at the origin are included. By composition with the natural projection to outer automorphism group of the l-adic completion $\Pi_{g,n}^l$ we get a representation

$$\rho_{g,n} : \pi_1^{alg}(M_{g,n}, a) \longrightarrow Out(\pi_1^l(X))$$

for nice l. This map induces filtrations on $\pi_1^{alg}(M_{g,n})$ and its subgroup

$$\pi_1^{alg}(M_{g,n} \otimes \bar{\mathbb{Q}})$$

and an injection of $\mathbb{Z}_l$-Lie algebras

$$Gr^{\bullet}_{X,l}\pi_1^{alg}(M_{g,n} \otimes \bar{\mathbb{Q}}) \hookrightarrow Gr^{\bullet}_{X,l}\pi_1^{alg}(M_{g,n}).$$

It is conjectured by Oda and proved in a series of papers by Ihara, Matsumoto, Nakamura and Takao that the cokernel of the above map after tensoring with $\mathbb{Q}_l$ is independent of g and n [11, 18, 20] . Note that $M_{0,3} \cong Spec(\mathbb{Q})$.

Definition 4.1. We define the Hecke-Teichmuller Lie algebra to be the image of the following morphism of graded Lie algebras

$$Gr^{\bullet}_{X,l}\pi_1^{alg}(M_{g,n}) \longrightarrow Gr^{\bullet}_{I}\widetilde{Out}(\Pi^l_{g,n}).$$

Note that, the filtration induced on the Galois group by $Out(\Pi^l_{g,n})$ coincides with the filtration coming from $\pi_1^{alg}(M_{g,n}, a)$ by the Galois representation associated to the corresponding curve and we have morphisms

$$Gr^{\bullet}_{X,l}Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Gr^{\bullet}_{X,l}\pi_1^{alg}(M_{g,n}) \longrightarrow Gr^{\bullet}_{I}\widetilde{Out}(\Pi^l_{g,n}).$$

We expect Hecke-Teichmuller Lie algebra to serve the role of Hecke algebra in proving modularity results for elliptic curves or other motivic objects.

4.2. **Galois representations associated to elliptic curves.** The method of proving modularity results by finding isomorphisms between Hecke algebras and universal deformation rings as originated by Wiles [31] , can be reformulated in the language of Lie algebras. One can find a canonical graded representation of the Galois group to Hecke-Teichmuller Lie algebra which contains all the information of modular Galois representations.

Let us first reformulate the theory of Galois representations in the language of Lie algebras. We start with elliptic curves. To each elliptic curve E defined over $\mathbb{Q}$ which has a rational point, one associates a Galois outer representation

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Out(\pi_1^l(E - \{0\})).$$

By analogy to Shimura-Taniyama-Weil conjecture, we expect this representation to be encoded in the representations

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Out(\pi_1^l(Y_0(N)))$$

associated to modular curves $Y_0(N)$ which have a model over $\mathbb{Q}$. By $Y_0(N)$ we mean the non-compactified modular curve of level N which is given as the quotient of the upper half-plane by the congruence subgroup $\Gamma_0(N)$ of $SL_2(\mathbb{Z})$ consisting of matrices which are upper triangular modulo N.

For any smooth curve X defined over $\mathbb{Q}$ the outer automorphism group of braid type acts on $Gr_I^\bullet\widetilde{Out}(\pi_1^l(X))$ by conjugation and therefore for each m we get a Galois representation

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Aut(gr^m\widetilde{Out}(\pi_1^l(X))).$$

Knowing that Shimura-Tanyama-Weil conjecture proved by Wiles and his collaborators [31, 25, 4] we get the following Lie algebra version of Shimura-Taniyama-Weil conjecture:

Theorem 4.2. *Let E be an elliptic curve over $\mathbb{Q}$ together with a rational point $0 \in E$. Then, the Galois representation*

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Aut(Gr_I^\bullet\widetilde{Out}(\pi_1^l(E-\{0\})))$$

appears as the direct summand of the Galois representation

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Aut(Gr_I^\bullet\widetilde{Out}(\pi_1^l(Y_0(N))))$$

for some level N which can be chosen to be conductor of the elliptic curve.

Proof. In grade zero, we recover the usual abelian Galois representation and in higher grades one can canonically construct this representation by the grade-zero standard representation. Indeed, for each $m \geq 1$ the isomorphism in proposition 1.3 is $\widetilde{Out}(\pi_1^l(X))$-equivariant. From this we can determine the representation from the inner action of $\widetilde{Out}(\pi_1^l(X))$ on $Gr_I^\bullet\pi_1^l(X)$. This action is fully determined by the grade-zero action. Therefore, the Galois representations

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Aut(gr^m\widetilde{Out}(\pi_1^l(X)))$$

are all determined by the abelian Galois representation associated to X over $\mathbb{Q}$. □

4.3. **Galois actions on Hecke-Teichmuller algebra.** The arithmetic analogue of the Teichmuller space which is the universal Galois representation landing in outer automorphism group of the algebraic fundamental group of $M_{g,n} \otimes \bar{\mathbb{Q}}$

$$\rho_{univ} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Out(\pi_1^{alg}(M_{g,n} \otimes \bar{\mathbb{Q}})) = Out(\widehat{\Gamma_{g,n}})$$

induces a Galois action on the corresponding Lie algebra

$$Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Aut(Gr_{I,l}^\bullet Out(\pi_1^{alg}(M_{g,n} \otimes \bar{\mathbb{Q}})))$$

and thus a Galois action on the Hecke-Teichmuller Lie algebra. This is analogue of the Galois action on the abelian Hecke algebra, which is used to prove modularity of Galois representations in [31] . One can use the Hecke-Teichmuller Lie algebra to prove that certain Galois actions on Lie algebras do come from curves defined over number fields.

The general question would be recognition of Galois actions on Lie algebras or even, recognition of representations of Galois-Lie group as appropiriate

tools. In order to answer this general question, one shall find appropriate generalizations of arithmetic hyperbolicity and Grothendieck's conjectures or even a motivic formulation of hyperbolicity in higher dimensions.

Acknowledgements

I would like to thank M. Kontsevich, O. Gabber, N. Nikolov, V.B. Mehta, A.J. Parameswaran, D. Prasad, Y. Soibelman for enjoyable conversations which led to my interest in outer representations. I wish to thank Tata Institute of Fundamental Research and Institute des Hautes Ètudes Scientifiques for their warm hospitality during which these conversations took place. I would also like to thank Harish-Chandra research institute, particularly R. Kulkarni and R. Ramakrishnan for warm hospitality during the workshop on Teichmuller theory and moduli spaces, for which this note is prepared. This research is supported by an Oswald-Veblen grant from IAS. I would like to thanks many instructive comments by referee(s).

References

1. M. Asada, M. Koneko, *On the automorphism group of some pro-l fundamental groups*, Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986), 137159, Adv. Stud. Pure Math., 12, North-Holland, Amsterdam, 1987.
2. G.V. Bely, Translated by Neal Koblitz. Galois extensions of a maximal cyclotomic field. *Math. USSR Izv.*, **14**(2), 247256.
3. J. S. Birman, *Braids, links, and mapping class groups*, Annals of Mathematics Studies, No. 82. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1974.
4. C. Breuil, B. Conrad, F. Diamond, R. Taylor; On the modularity of elliptic curves over Q: wilde 3-adic excercises, *J. Amer. Math. Soc.*, **14**(4), (2001), 843939.
5. M. Dehn, Die Gruppen der Abbildungsklassen. (German) Das arithmetische Feld auf Flchen, *Acta Math.*, **69**(1), (1938), 135206.
6. P. Deligne, *Le groupe fundamental de la droite projective moins trois points,*(French) [The fundamental group of the projective line minus three points] Galois groups over Q. (Berkeley, CA, 1987), 79297, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.
7. A. Grothendieck, *Revetement Etale et Groupe Fondamental (SGA I).* (French) [tale coverings and fundamental group (SGA 1)] Sminaire de gomtrie algbrique du Bois Marie 196061. [Algebraic Geometry Seminar of Bois Marie 1960-61] Directed by A. Grothendieck. With two papers by M. Raynaud. Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651]. Documents Mathmatiques (Paris) [Mathematical Documents (Paris)], 3. Socit Mathmatique de France, Paris, 2003.
8. R. Hain, M. Matsumoto, Weighted completion of Galois groups and Galois actions on the fundamental group of P 10, 1,. *Compositio Mathematica*, **139**(2), (2003), 119-167.
9. A. Hatcher,W. Thurston, A presentation for the mapping class group of a closed orientable surface. *Topology*, **19**(3), (1980), 221237.
10. Y. Ihara, Profinite braid groups, Galois representations, and complex multiplications. *Ann. of Math. (2)*, **123**(1), (1986), 43106.

11. Y. Ihara, H. Nakamura; On deformation of mutually degenerate stable marked curves and Oda's problem, *J. Reine Angew. Math.*, **487**, (1997), 125151.
12. M. Ikeda, Completeness of the absolute Galois group of the rational number field, *J. Reine Angew. Math.*, **291**, (1977), 122.
13. M. koneko, Certain automorphism groups of pro-l fundamental groups of punctured Riemann surfaces. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, **36**(2), (1989), 363372.
14. J. Labute, On the descending central series of groups with single defining relation. *J. Algebra*, **14**, (1970), 1623.
15. W.B.R. Likorish, On the homeomorphisms of a non-orientable surface. *Proc. Cambridge Philos. Soc.*, **61**, (1965), 6164.
16. T. Oda, *Etale homotopy type of the moduli spaces of algebraic curves.* Geometric Galois actions, 1, 8595, London Math. Soc. Lecture Note Ser., 242, Cambridge Univ. Press, Cambridge, 1997.
17. M. Matsumoto, On the Galois image in the derivation algebra of π_1 of the projective line minus three points, *Contemp. Math.*, **186**, (1995), 201-201.
18. M. Matsumoto, Galois representations on profinite braid groups on curves, *J. Reine Angew. Math.*, **474**, (1996), 169219.
19. S. Mochizuki, The profinite Grothendieck conjecture for closed hyperbolic curves over number fields, *J. Math. Sci. Univ. Tokyo*, **3**(3), (1996), 571627.
20. H. Nakamura, Coupling of universal monodromy representations of Galois-Teichmller modular groups, *Math. Ann.*, **304**(1), (1996), 99119.
21. J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Second edition. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 323. Springer-Verlag, Berlin, 2008.
22. A. Rastegar, Deformation of outer representations of Galois group, *Iran. J. Math. Sci. Inform.*, **6**(1), (2011), 3352.
23. A. Rastegar, Deformation of outer representations of Galois group II., *Iran. J. Math. Sci. Inform.*, **6**(2), (2011), 3341.
24. L. Ribes, P. Zalesskii; *Profinite Groups.* Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 40. Springer-Verlag, Berlin, 2010.
25. R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.*, **141**(3), (1995), 553572.
26. S. Suzuki, On homeomorphisms of a 3-dimensional handle body, *Canad. J. Math.*, **29**(1), (1977), 111124.
27. H. Tsungai, On some derivations of Lie algebras related to Galois representations, *Publ. Res. Inst. Math. Sci.*, **31**(1), (1995), 113134.
28. K. Uchida, Isomorphisms of Galois groups, *J. Math. Soc. Japan*, **28**(4), (1976), 617620.
29. V.A. Voevodskii, Galois representations connected with hyperbolic curves., *Math. USSR-Izv.*, **39**(3), (1992), 12811291
30. B. Wajnryb, A simple presentation for the mapping class group of an orientable surface, *Israel J. Math.*, *45*(2-3), (1983), 157174.
31. A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.*, **141**(3), (1995), 443551.