Arithmetic fundamental groups
and moduli of curves

Makoto Matsumoto*

Department of Mathematics, Kyushu University,
6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-8581 Japan

Lecture given at the
School on Algebraic Geometry
Trieste, 26 July – 13 August 1999

LNS001008

*matumoto@math.kyushu-u.ac.jp
Abstract

This is a short note on the algebraic (or sometimes called arithmetic) fundamental groups of an algebraic variety, which connects classical fundamental groups with Galois groups of fields. A large part of this note describes the algebraic fundamental groups in a concrete manner.

This note gives only a sketch of the fundamental groups of the algebraic stack of moduli of curves. Some application to a purely topological statement, i.e., an obstruction to the surjectivity of Johnson homomorphisms in the mapping class groups, which comes from Galois group of $\mathbb{Q}$, is explained.
1. Galois groups of field extension
2. A short way to arithmetic fundamental groups
   2.1. Profinite groups and algebraic fundamental groups
   2.2. Arithmetic fundamental groups
   2.3. Arithmetic monodromy
   2.4. The projective line minus two points
   2.5. The projective line minus three points
3. Arithmetic fundamental groups by etale topology
   3.1. Unramified coverings of a topological space and fiber functors
   3.2. Finite coverings
   3.3. Etale fundamental groups
4. Arithmetic mapping class groups
   4.1. The algebraic stack $M_{g,n}$ over $\text{Spec} \mathbb{Z}$
   4.2. The arithmetic fundamental group of the moduli stack
5. A conjecture of Takayuki Oda
   5.1. Weight filtration on the fundamental group
   5.2. Obstruction to the surjectivity of Johnson morphisms
   5.3. The projective line minus three points again
References
1. Galois groups of field extension

We recall some basic notions of classical Galois theory of fields. Let $K$ be a field, and fix its algebraic closure $\overline{K}$. Let $L$ be a finite extension of $K$. An extension $L/K$ is said to be separable if the cardinality of $\text{Hom}_K(L, \overline{K})$ is the same as the extension degree $[L : K]$. Let $\text{Aut}(L/K)$ be the group of automorphisms of $L$ as a field, fixing each element in $K$. Then, $\text{Aut}(L/K)$ acts on $\text{Hom}_K(L, \overline{K})$. If the action is transitive, then the extension $L/K$ is said to be a normal extension. A finite separable normal extension $L/K$ is called a finite Galois extension, and $\text{Aut}(L/K)$ is called the Galois group of $L/K$ and denoted by $G(L/K)$.

Suppose that $L/K$ is a finite Galois extension. Galois theory asserts that there exists a one-to-one correspondence between

$$\{M : \text{intermediate field between } L \text{ and } K\}$$

and

$$\{N : \text{subgroup of } G(L/K)\}$$

given by $M \mapsto G(L/M)$ and $N \mapsto L^N$, where $L^N$ denotes the subfield of elements fixed by the action of all elements of $N$. The correspondence reverses the inclusion relation, i.e., if $M \subset M'$ then $G(L/M) \supset G(L/M')$. If we use the terminology of categories, then the correspondence is a contravariant equivalence.

There is an infinite version. Let $L/K$ be an algebraic extension, which is allowed to be infinite. It is called an (infinite) Galois extension, if any finite extension of $K$ in $L$ is finite Galois. Then, $\text{Aut}(L/K)$ is called the Galois group of $L/K$, and denoted by $G(L/K)$ again.

This infinite Galois group is equipped with a natural topology, called profinite topology, as will be stated later. For $L \supset M \supset K$ with $M$ being Galois over $K$, we have a short exact sequence

$$1 \rightarrow G(L/M) \rightarrow G(L/K) \rightarrow G(M/K) \rightarrow 1. \quad (1.1)$$

**Exercise 1.1.** Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\xi_n)$, with $\xi_n = e^{2\pi \sqrt{-1}/n}$ being an $n$-th primitive root of unity. Show that $\chi : G(L/K) \cong (\mathbb{Z}/n)\times$, where $\sigma \in G(L/K)$ is mapped to the unique $\chi(\sigma) \in (\mathbb{Z}/n)\times$ such that $\sigma(\xi_n) = \xi_n^{\chi(\sigma)}$, by using the irreducibility of the minimal polynomial of $\xi_n$.

If we put $L' := \mathbb{Q}(\xi_n|n \in \mathbb{N})$, what is $G(L'/K)$?
2. A SHORT WAY TO ARITHMETIC FUNDAMENTAL GROUPS

Let $X$ be an arcwise connected topological space, and let $a$ be a point of $X$. The fundamental group of $X$ with base point $a$, denoted by $\pi_1(X,a)$, is defined to be the set of homotopy equivalence classes of closed paths from $a$ to itself. By the usual composition of paths, taking the homotopy classes, $\pi_1(X,a)$ becomes a group. For the composition rule, we denote by $\gamma' \circ \gamma$ the path first going along $\gamma$ and then along $\gamma'$.

For another choice of base point $b$, we have $\pi_1(X,a) \cong \pi_1(X,b)$, where the isomorphism is well-defined up to an inner automorphism.

More generally, let $\pi_1(X;a,b)$ denote the homotopy classes of paths from $a$ to $b$. Two paths $\gamma \in \pi_1(X;a,b)$ and $\gamma' \in \pi_1(X;b,c)$ can be composed to get an element $\gamma' \circ \gamma \in \pi_1(X;a,c)$, and the system $\{\pi_1(X;a,b) | (a,b \in X)\}$ constitutes a groupoid (i.e., a category where every homomorphism is invertible).

Assume that $X$ is a smooth complex algebraic variety. Let $a$ be a point of $X$.

**Definition 2.1.** Let $M_a$ be the field of the germs of meromorphic algebraic functions at $a$ on $X$, such that the germ has analytic continuation to a finitely multivalued meromorphic function along any path on $X$.

Algebraic means that every $h \in M_a$ is algebraic over the rational function field $\mathbb{C}(X)$ of algebraic variety $X$. Functions like $\exp(z)$ are not in $\mathbb{C}(\mathbb{A}^1)$.

Clearly $M_a$ is a field, which contains the rational function field $\mathbb{C}(X)$ as the single-valued meromorphic functions. By analytic continuation, we have an action

$$
\pi_1(X;a,b) \times M_a \rightarrow M_b,
$$

with $h \in M_a \mapsto \gamma h \in M_b$ being obtained by analytic continuation of the germ $h$ along the path $\gamma$. In particular, $\pi_1(X,a)$ acts on $M_a$ from the left, so we have a group homomorphism

$$
\pi_1(X,a) \rightarrow \text{Aut}(M_a/\mathbb{C}(X)),
$$

since $\mathbb{C}(X)$ is single-valued and is fixed elementwise by analytic continuation along a closed path. Because $h \in M_a$ is assumed to be finitely multivalued, the set of all the branches $S := \{\gamma h | \gamma \in \pi_1(X,a)\}$ is finite. Hence, the fundamental symmetric polynomials of $S := \{f_1, f_2, \ldots, f_n\}$ are single-valued, i.e. in $\mathbb{C}(X)$, since $\pi_1(X,a)$ acts on $S$ by permutations. Thus,
Let $F(T) := \prod_{i=1}^{n}(T-f_i) \in \mathbb{C}(X)[T]$, which is divisible by the minimal polynomial of $h$ over $\mathbb{C}(X)$. Thus, any algebraic conjugate of $h$ over $\mathbb{C}(X)$ is one of the $f_i$, and hence $M_a/\mathbb{C}(X)$ is a Galois extension.

Now we have a homomorphism
\[ \pi_1(X,a) \to G(M_a/\mathbb{C}(X)). \]

**Definition 2.2.** We define the algebraic fundamental group of a connected smooth algebraic variety $X$ over $\mathbb{C}$ by
\[ \pi_1^{\text{alg}}(X,a) := G(M_a/\mathbb{C}(X)). \]

We have a group homomorphism
\[ \pi_1(X,a) \to \pi_1^{\text{alg}}(X,a), \]
by analytic continuation.

It can be proved that this morphism is “completion,” i.e., the right-hand side is obtained by a purely group-theoretical operation called “profinite completion” of the left-hand side, and thus depends only on the homotopy type of $X$, as we shall see in the next section. The arithmetic part will come into sight when we consider $X$ over a non algebraically closed field $K$ in §2.2.

### 2.1. Profinite groups and algebraic fundamental groups

We want to describe the (possibly infinite) Galois group $G(L/K)$ for $L := M_a$, $K := \mathbb{C}(X)$. The answer is that it is the profinite completion of $\pi_1(X,a)$.

To see this, for a while, let $L/K$ be a general infinite Galois extension. We look at all finite Galois subextensions $M/K$ in $L$. The surjectivity of $G(L/K) \to G(M/K)$ in (1.1) says that $\sigma \in G(L/K)$ determines a family $\sigma_M \in G(M/K)$ for each finite Galois extension $M$, so that they are compatible in the sense that if $M \supset M'$, then $\sigma_M \to \sigma_{M'}$ via natural morphism $G(M/K) \to G(M'/K)$.

In general, let $\Lambda$ be a directed set (i.e. a partially ordered set such that for any $\lambda, \lambda' \in \Lambda$ there is a common upper element $\lambda'' \geq \lambda, \lambda'$ in $\Lambda$), and assume that we are given a family of finite groups $G_{\lambda}$ $(\lambda \in \Lambda)$ together with a group homomorphism $G_{\lambda} \to G_{\mu}$ for $\lambda \geq \mu$, with the following compatibility condition: the composition of $G_{\lambda} \to G_{\mu}$ with $G_{\mu} \to G_{\nu}$ coincides with $G_{\lambda} \to G_{\nu}$. We call this family a projective system of finite groups. (In the terminology of category theory, this is merely a functor from $\Lambda$ to the category of finite groups.) We define its *projective limit* $\varprojlim_{\lambda \in \Lambda} G_{\lambda}$ as follows. An element of $\varprojlim_{\lambda \in \Lambda} G_{\lambda}$ is a family $(\sigma_{\lambda})_{\lambda \in \Lambda}$, $\sigma_{\lambda} \in G_{\lambda}$, with the
property \( \sigma_\lambda \mapsto \sigma_\mu \) for \( \lambda \geq \mu \). This is a subset of the direct product:

\[
\operatorname{proj \lim}_{\lambda \in \Lambda} G_\lambda \subset \prod_{\lambda \in \Lambda} G_\lambda.
\]

We equip \( G_\lambda \) with the discrete (but compact, being finite) topology. Then, the product is compact by Tikhonov’s Theorem, and so is the projective limit, being a closed subgroup of the compact group.

If we apply this notion to the case: \( \Lambda \) is the set of finite Galois subextension \( M/K \) equipped with the inclusion ordering \( M \supseteq M' \iff M \supseteq M' \), we obtain a projective system of finite groups \( G(M/K) \). Our previous observation says that there is a morphism

\[
G(L/K) \to \operatorname{proj \lim}_{M} G(M/K),
\]

\( \sigma \in G(L/K) \mapsto (\sigma|_{M} \in G(M/K)) \). This is injective, since \( L \) being algebraic, \( L \) is the union of all finite Galois extensions \( M \). The above morphism is surjective, since if we have an element of \( (\sigma_M) \in \operatorname{proj \lim}_{M} G(M/K) \), then the compatibility assures that the action of \( \sigma_M \) restricts to that of \( \sigma_{M'} \) if \( M \supseteq M' \). Thus, the actions \( \sigma_M \) patch together to give an element of \( G(L/K) \). Thus we have

\[
G(L/K) = \operatorname{proj \lim}_{M} G(M/K).
\]

A topological group which can be written as the projective limit of finite groups is called a \textit{profinite group}. \( G(L/K) \) is an example. It is known that \( G \) is a profinite group if and only if it is a compact totally disconnected Hausdorff topological group.

Let \( G \) be an abstract group. The set of finite-index normal subgroups \( \Lambda := \{ N \triangleleft G \mid G/N : \text{finite group} \} \) is a directed set by \( N \geq N' \) if and only if \( N \subset N' \). Then, we have a projective system of finite groups \( G/N \), \( N \in \Lambda \).

**Definition 2.3.** For an abstract group \( G \), we define its profinite completion \( \hat{G} \) to be

\[
\hat{G} := \operatorname{proj \lim}_{N} (G/N),
\]

where \( N \) runs over the finite index normal subgroups of \( G \). We have a natural group homomorphism

\[
G \to \hat{G}
\]

by patching \( G \to G/N \) together, and its image is dense.
Fix a prime \( l \). Let \( N \) run over the finite index normal subgroups of \( G \) with the quotient \( G/N \) being an \( l \)-group, and take the similar projective limit. Then we obtain the pro-\( l \) completion of \( G \), denoted by \( G^l \).

**Theorem 2.1.** (SGA1[7, Corollary 5.2, p.337]) Let \( X \) be a connected algebraic variety over \( \mathbb{C} \). Then

\[
\pi_1(X,a) \to \pi_1^{alg}(X,a)
\]

gives an isomorphism of the profinite completion of the topological fundamental group and the algebraic fundamental group,

\[
\pi_1(X,a) \to \pi_1(\tilde{X},\tilde{a}) \cong \pi_1^{alg}(X,a).
\]

A rough sketch of the proof is as follows. It is enough to prove that there is a one-to-one correspondence between

\[
\{ N \triangleleft \pi_1^{alg}(X,a) \mid \pi_1^{alg}(X,a)/N : \text{finite group} \}
\]

and

\[
\{ M \subset M_a \mid M/K \text{ is finite Galois} \}
\]

so that

\[
\pi_1^{alg}(X,a)/N \cong G(M/K) \quad \tag{2.1}
\]

holds through

\[
\pi_1^{alg}(X,a) \to G(M_a/K) \to G(M/K),
\]

since then by taking the projective limit of (2.1) we have the desired isomorphism.

For \( N \), we construct a finite topological unramified covering \( p_N : Y_N \to X \) with \( a_N \in p_N^{-1}(a) \) fixed. This can be done as follows. Let \( \tilde{X} \) be the universal covering of \( X \), and \( \tilde{a} \in \tilde{X} \) be a point above \( a \). (These topological notions are recalled in §3.1 below.) It is well known that \( \pi_1(X,a) \) acts on the covering \( \tilde{X}/X \) from the right. Then, by taking the quotient of \( \tilde{X} \) by \( N \), we have a finite connected unramified covering \( p_N : Y_N \to X \), with a point \( a_N \in Y_N \) being fixed as the image of \( \tilde{a} \). A “Riemann existence theorem” in SGA1[7, Theorem 5.1, p.332] asserts that \( Y_N \) is actually an algebraic variety over \( \mathbb{C} \). We have a homomorphism \( \mathbb{C}(Y) \to M_a \) induced by \( a_N \), namely, a rational function \( h \in \mathbb{C}(Y) \) is a multivalued meromorphic function on \( X \), and it can be regarded as a germ at \( a \) by restricting \( h \) to a neighbourhood of \( a_N \in Y \). This gives a correspondence \( N \mapsto \mathbb{C}(Y) \subset M_a \), such that \( \pi_1(X,a)/N \cong G(\mathbb{C}(Y)/\mathbb{C}(X)) \), as desired. The converse correspondence is \( M/K \mapsto \text{Ker}(\pi_1(X,a) \to G(M/K)) \).

We shall again discuss this construction in a later section §3.
2.2. Arithmetic fundamental groups. So far, the algebraic fundamental group is obtained from the topological one by profinite completion, and it ignores the algebraic structure altogether. An interesting part comes from the absolute Galois groups of the field over which the algebraic variety is defined.

Let $K \subseteq \mathbb{C}$ be a subfield, $\overline{K}$ the algebraic closure of $K$ in $\mathbb{C}$. Assume that $X$ is a smooth algebraic variety over $\overline{K}$, which is geometrically connected. This can be paraphrased by saying that the defining polynomials of $X$ have coefficients in $K$, and $X(\mathbb{C})$ is connected as a complex variety.

If $X$ is defined over $K$, then $K(X)$ denotes the rational function field of $X$ over $K$. If $X$ is defined by polynomials, $K(X)$ is the set of the functions which can be described as rational expressions of the coordinate variables with coefficients in $K$.

Theorem 2.2. (c.f. SGA1[7, Chapter XIII p.393]) If $Y \rightarrow X$ is a finite unramified covering of a complex algebraic variety, and $X$ is defined over $\overline{K}$, then there is a model $Y_{\overline{K}} \rightarrow X_{\overline{K}}$ of varieties over $\overline{K}$, giving $Y \rightarrow X$ by base extension $\otimes_{\overline{K}} \mathbb{C}$. If $\mathbb{C}(Y)/\mathbb{C}(X)$ is Galois, then so is $\overline{K}(Y)/\overline{K}(X)$ and their Galois groups are isomorphic.

Corollary 2.1. Let $M_a^{\text{alg}}$ be the subfield of $M_a$ of the algebraic elements over $\overline{K}(X)$. Then

$$G(M_a^{\text{alg}}/\overline{K}(X)) = G(M_a/\mathbb{C}(X)).$$

One can show that if $X$ is defined over $\overline{K}$, then $M_a^{\text{alg}}/K(X)$ is a Galois extension.

Definition 2.4. If $X$ is a smooth algebraic variety over $K$, then we define its arithmetic fundamental group

$$\pi_1^{\text{alg}}(X, a) := G(M_a^{\text{alg}}/K(X)).$$

Corollary 2.2. We have a short exact sequence

$$1 \rightarrow \pi_1^{\text{alg}}(X \otimes_K \overline{K}, a) \rightarrow \pi_1^{\text{alg}}(X, a) \rightarrow G(\overline{K}/K) \rightarrow 1. \quad (2.2)$$

This is the exact sequence coming from Galois extensions $M_a^{\text{alg}} \supset \overline{K}(X) \supset K(X)$. Note that $G(\overline{K}(X)/K(X)) = G(\overline{K}/K)$ since $K(X) \otimes_K \overline{K} = \overline{K}(X)$, i.e., since $X$ is geometrically connected.

Now the left term of the short exact sequence (2.2) is the profinite completion of the topological fundamental group $\pi_1(X, a)$, which depends only on the homotopy type of $X$, while the right term $G(\overline{K}/K)$ is the absolute
Galois group of $K$, which controls the arithmetic of $K$ and depends only on the field $K$.

But the middle term, or the extension, highly depends on the structure of $X$ as an algebraic variety, for example if $K$ is a number field. Grothendieck conjectured [8] that $X$ is recoverable from the exact sequence of profinite group, if $X$ is “anabelian.” Recently much progress has been done in this direction, by H. Nakamura, F. Pop, A. Tamagawa, and S. Mochizuki, and others. For example, the conjecture is true for curves over $p$-adic fields with nonabelian fundamental groups. An exposition on these researches in Japanese is available, and its English translation is to appear [25].

2.3. **Arithmetic monodromy.** The exact sequence (2.2) can be considered to be an algebraic version of the “fiber exact sequence” for $X \to \text{Spec} K$.

Let us consider a topological fibration $F \to B$ which is locally trivial. Take a point $b \in B$, and let $F_b$ be the fiber at $b$. Fix $x \in F_b$. Assume $\pi_2(B) = \{1\}$. Then, we have the so-called homotopy exact sequence

$$1 \to \pi_1(F_b, x) \to \pi_1(F, x) \to \pi_1(B, b) \to 1.$$  

In the arithmetic case, $F \to B$ is $X \to \text{Spec} K$, $b$ is $a : \text{Spec} \bar{K} \to \text{Spec} K$, and $F_b$ is $X \times_K \bar{K}$, therefore (2.2) is an analogue of the above. Note that $\pi_1^{ab}(\text{Spec} K, a) = G(\bar{K}/K)$ holds, if we argue in the etale fundamental group, see §3 below.

In topology theory, it is often more convenient to consider the *monodromy* of the fibration $p : F \to B$, as follows. The rough idea is as follows: take a closed path $\gamma \in \pi_1(B, b)$. Then, because of the local triviality of the fibration, we can consider the family $F_c := p^{-1}(c)$ where $c$ moves along $\gamma$ as a deformation of $F_b$. Then, $\gamma$ induces a homeomorphism of $F_b$ to itself. Such a homeomorphism of $F_b$ is not unique, but its isotopy class is well defined. Thus, $\pi_1(B, b)$ acts on various homotopy invariants of $F_b$, like cohomologies and homotopy groups. Such a representation of $\pi_1(B, b)$ is called monodromy representation associated to $F \to B$. Let us concentrate on the monodromy on the fundamental group of $F_b$. In this case, we take $x \in F_b$, and take any lift $\gamma \in \pi_1(B, b)$ to $F$ with starting point $x$, and call it $\tilde{\gamma}$. Since $F_b$ is connected (i.e. $\pi_0(F_b) = \{1\}$), we may adjust $\tilde{\gamma}$ so that it lies in $\pi_1(F, x)$. The ambiguity of $\tilde{\gamma}$ is up to a composition with an element of $\pi_1(F_b, x)$. Take an element $\beta \in \pi_1(F_b, x)$. Then, its deformation along $\gamma$ can be considered to be $\tilde{\gamma}\beta\tilde{\gamma}^{-1}$. In this way $\pi_1(B, b)$ acts on $\pi_1(F_b, x)$, but the action is well defined up to the choice of $\tilde{\gamma}$, i.e., up to the inner automorphism of $\pi_1(F_b, x)$.
Then we have an outer monodromy representation associated to \( F \to B \),
\[
\rho : \pi_1(B, b) \to \text{Aut}(\pi_1(F_b, x))/\text{Inn}(\pi_1(F_b, x)) =: \text{Out}(\pi_1(F_b, x)).
\]
This is easier to treat than the exact sequence itself, since often the fundamental groups of a fiber and the base are well understood.

An analogue can be considered for the arithmetic version. Take \( \sigma \in G(\bar{K}/K) \), then take any lift \( \tilde{\sigma} \in \pi_1^{\text{alg}}(X, b) \), and let it act by conjugation \( \beta \mapsto \tilde{\sigma}(\beta)\tilde{\sigma}^{-1} \) on \( \beta \in \pi_1^{\text{alg}}(X \otimes K, b) \). This gives an arithmetic version of the monodromy representation
\[
\rho_X : G(\bar{K}/K) \to \text{Out}(\pi_1^{\text{alg}}(X \otimes \bar{K}, b)).
\]
(2.3)
The left-hand side depends only on \( K \), and the right-hand side depends only on the homotopy type of \( X \otimes \mathbb{C} \), and thus \( \rho_X \) connects arithmetic and topology. Sometimes \( \rho_X \) is called the outer Galois representation associated with \( X \).

2.4. The projective line minus two points. As a simplest example, we consider the case where \( X/\mathbb{Q} \) is an affine line minus one point \( \{0\} \), with coordinate function \( z \), and take \( a = 1 \) as the base point. The topological fundamental group of this space is \( \mathbb{Z} \). An element \( h \) of \( M_a^{\text{alg}} \) is finitely multivalued, say, \( N \)-valued. Then, \( h \) is a single-valued function of \( w \), if we take an \( N \)-th root \( w \) of \( z \). Since we assumed that \( h \) is algebraic over \( \mathbb{Q}(X) \), \( h \) is a rational function of \( w \) with coefficients in \( \overline{\mathbb{Q}} \). Thus, \( M_a^{\text{alg}} \) is generated by the functions \( z^{1/N} := \exp(\log z/N) \), with branch fixed so as to have positive real values around 1. Put \( \xi_N := \exp(2\pi\sqrt{-1}/N) \). The field extensions
\[
M_a^{\text{alg}} = \overline{\mathbb{Q}}(z^{1/N} | N \in \mathbb{N}) \supset \overline{\mathbb{Q}}(X) = \overline{\mathbb{Q}}(z) \supset \mathbb{Q}(X) = \mathbb{Q}(z)
\]
give
\[
\pi_1^{\text{alg}}(X \otimes \overline{\mathbb{Q}}, a) = \text{proj lim}_N G(\overline{\mathbb{Q}}(z^{1/N})/\overline{\mathbb{Q}}(z)) = \text{proj lim}_N(\mathbb{Z}/N) =: \hat{\mathbb{Z}}.
\]
Here, the identification \( G(\overline{\mathbb{Q}}(z^{1/N})/\overline{\mathbb{Q}}(z)) = \mathbb{Z}/N \) is given by \( \beta \in G(\overline{\mathbb{Q}}(z^{1/N})/\overline{\mathbb{Q}}(z)) \mapsto b \in \mathbb{Z}/N \), where \( b \) is the unique element such that \( \beta(z^{1/N}) \mapsto \xi_N^{b}z^{1/N} \). Then, the generator \( \gamma \) of \( \pi_1(X, a) \) which goes around 0 counterclockwise gives an element of the Galois group which maps
\[
\gamma : z^{1/N} \mapsto \exp(2\pi\sqrt{-1}/N)z^{1/N},
\]
so \( \gamma \) is, through \( G(\overline{\mathbb{Q}}(z^{1/N})/\overline{\mathbb{Q}}(z)) = \mathbb{Z}/N \), identified with \( 1 \in \hat{\mathbb{Z}} \). To compute
\[
\rho_X : G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Out}(\hat{\mathbb{Z}}) = \text{Aut}(\hat{\mathbb{Z}}),
\]
it suffices to see the action on $1 \in \hat{\mathbb{Z}}$, or equivalently on $\gamma \in G(\overline{\mathbb{Q}}(z^{1/N})/\mathbb{Q}(z))$, since it generates $\hat{\mathbb{Z}}$ topologically. We take a lift of $\sigma \in G(\overline{\mathbb{Q}}/\mathbb{Q}) = G(\overline{\mathbb{Q}}(z)/\mathbb{Q}(z))$ to $\tilde{\sigma} \in G(\overline{\mathbb{Q}}(z^{1/N})|N \in \mathbb{N})/\mathbb{Q}(z))$. For this, for example, we may take $\tilde{\sigma}$ acting trivially on $z^{1/N}$. Then, $\tilde{\sigma} \gamma \tilde{\sigma}^{-1}$ maps $z^{1/N} \mapsto z^{1/N} \mapsto \exp(2\pi \sqrt{-1}/N)z^{1/N} \mapsto \exp(2\pi \sqrt{-1}/N)\chi(\sigma)z^{1/N} = \gamma \chi(\sigma)(z^{1/N})$.

Here, 
\[
\chi(\sigma) = (\chi(\sigma_N)) \in \limproj_N(\mathbb{Z}/N)\hat{\times} = \hat{\mathbb{Z}}\hat{\times}
\]
is the cyclotomic character $G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \hat{\mathbb{Z}}\hat{\times}$, that is, $\chi(\sigma_N) \in \mathbb{Z}/N$ is uniquely determined by $\sigma : \xi_N \mapsto \xi_N^{\chi(\sigma)}$. This shows $\sigma(\gamma) = \gamma \chi(\sigma)$, so $\rho_X$ is nothing but the cyclotomic character
\[
\chi : G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \hat{\mathbb{Z}}\hat{\times} = \text{Aut}(\hat{\mathbb{Z}}).
\]

2.5. **The projective line minus three points.** A basic result by Belyi [3] says

**Theorem 2.3.** Let $X$ be the projective line minus three points $0, 1, \infty$ over $\mathbb{Q}$, and take an $a \in X$. Then,
\[
\rho_X : G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Out}(\pi_1(\widetilde{X}, a))
\]
is injective.

The right-hand side $\pi_1(\widetilde{X}, a)$ is the profinite completion of the free group $F_2$ with two generators, say, $x, y$. This implies that $G(\overline{\mathbb{Q}}/\mathbb{Q})$ is contained in a purely group-theoretic object. One can fix a lift
\[
\rho_X : G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}(\hat{F}_2)
\]
from $\text{Out}(\hat{F}_2)$, then two elements $\rho_X(\sigma)(x), \rho_X(\sigma)(y)$ in $\hat{F}_2$ characterise $\sigma$. It is convenient to fix the lift so that $\rho_X(\sigma) : x \mapsto x^{\chi(\sigma)}, y \mapsto f_\sigma(x, y)y^{\chi(\sigma)}f_\sigma(x, y)^{-1}$ with $f_\sigma(x, y) \in [\hat{F}_2, \hat{F}_2]$. This is possible in a unique way [3] [12].

There are roughly two directions of research:

(i) Characterize the image of $\rho_X$ in a group-theoretic way.

(ii) Use $\chi(\sigma), f_\sigma(x, y)$ to describe $\rho_Y(\sigma)$ for other varieties $Y$.

For (i), the Grothendieck-Teichmüller group was introduced by Drinfeld [6], and its profinite version $\widehat{\text{GT}}$ was given by Ihara [12] [13]. $\widehat{\text{GT}}$ is the subgroup of $\text{Aut}(\hat{F}_2)$ given by three conditions [12], with $G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{\text{GT}} \subset \text{Aut}(\hat{F}_2)$ being Belyi’s injection.

It is known that $\widehat{\text{GT}}$ acts on the profinite completion of the braid groups $\hat{B}_n$ ([6], for the profinite case, [15, Appendix]). $G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{\text{GT}} \to \text{Aut}(\hat{B}_n)$ is
known to come from the representation on the algebraic fundamental group of the configuration space of \( n \) points on the affine line [15].

Recently, Hatcher, Lochak, Nakamura, Schneps [10] [24] gave a subgroup \( \Gamma \) of \( \widehat{GT} \), \( G(\overline{\mathbb{Q}}/\mathbb{Q}) \subset \Gamma \subset \widehat{GT} \) (actually there are several variations of \( \Gamma \), but whether \( \Gamma = \widehat{GT} \) or not is still open), so that \( \Gamma \) acts on the profinite completion of mapping class groups of type \((g, n)\) systematically.

These researches are closely related to the program by Grothendieck [8], which tries to study \( G(\overline{\mathbb{Q}}/\mathbb{Q}) \) by towers of moduli spaces, but here we don’t pursue this direction.

These studies go with (ii): first the Galois action is described in terms of \( \chi(\sigma) \) and \( f_\sigma(x, y) \), then \( \widehat{GT} \)-action is described so that it generalizes the Galois action.

It is still open whether \( G(\overline{\mathbb{Q}}/\mathbb{Q}) = \widehat{GT} \) or not.

3. Arithmetic fundamental groups by etale topology

The definition of arithmetic fundamental groups in the previous section is concrete, but not intrinsic. For example, it cannot be applied for the positive characteristic case. A more sophisticated general definition uses the notion of Galois category [7, Chapter V].

3.1. Unramified coverings of a topological space and fiber functors.
In this section, we forget about algebraic varieties and consider only topological spaces. Though our aim is the theory of fundamental groups without paths, this section illustrates how the categorical machinery works.

Let \( X \) be an arcwise connected topological space. Let \( p : Y \to X \) be an unramified covering of \( X \). That is, \( p : Y \to X \) is a surjective continuous map such that for any \( x \in X \) there exists an open neighbourhood \( U \) of \( x \) with each connected component of \( p^{-1}(U) \) being homeomorphic to \( U \) via \( p \). It is a finite unramified covering if the number of the connected components is finite. The map \( p \) is called a covering map.

It is well known that the connected unramified coverings of \( X \) and the subgroups of \( \pi_1(X, a) \) are in one-to-one correspondence, but we shall start by recalling this fact.

Fix a point \( a \) on \( X \), and consider the category of connected unramified coverings with one point specified. Its objects are the pairs of an unramified connected covering \( p_Y : Y \to X \) and a point \( b \in p_Y^{-1}(a) \), and its morphisms are the continuous maps \( f : Y' \to Y \) compatible with the covering maps: \( p_Y \circ f = p_{Y'} \), and \( f(b') = b \). We denote this category by \( \text{Con}(X, a) \).
Assume that $X$ is arcwise connected, locally arcwise connected, and locally simply connected. Then there is a category equivalence between $\text{Con}(X, a)$ and \{ $N : \text{subgroup of } \pi_1(X, a)$ \}. The correspondence is: for $(Y, b) \in \text{Con}(X, a)$, we have $\pi_1(Y, b) \to \pi_1(X, a)$, which is injective, so $\pi_1(Y, b)$ considered as a subgroup corresponds to $(Y, b)$. For the converse, for $N \subset \pi_1(X, a)$, we consider the set of classes of paths

\[
Y_N := \{ \text{a path starting from } a \text{ with arbitrary end point in } X \} / \sim_N,
\]

where the equivalence is given by $\gamma \sim_N \gamma'$ if and only if they have the same end point and the closed path $\gamma^{-1} \circ \gamma'$ lies in the homotopy class in $N \subset \pi_1(X, a)$. $Y_N$ has a specified point $a_N$, which corresponds to the trivial path at $a$. Taking the end point of the path gives a map $p_N : Y_N \to X$, which is locally a homeomorphism by the assumption on locally arcwise simply connectedness. Thus, $(Y_N, a_N) \to (X, a)$ is an object of $\text{Con}(X, a)$.

If $N$ is a normal subgroup of $\pi_1(X, a)$, then $p_N : Y_N \to X$ is called a Galois covering. In this case, $\pi_1(X, a)$ acts on $Y_N/X$ from the right. Take $\alpha \in \pi_1(X, a)$, and let $\alpha$ act by $[\gamma] \in Y_N \mapsto [\gamma \circ \alpha] \in Y_N$. We need to check the well-definedness; if $\gamma \sim_N \gamma'$ then $\gamma \alpha \sim_N \gamma' \alpha$ should hold, which requires that, if $\gamma^{-1} \gamma' \in N$, then $\alpha^{-1} \gamma^{-1} \gamma' \alpha \in N$, that is, $N$ must be normal. In this case, we have

\[
\pi_1(X, a)/N \cong \text{Aut}(Y_N/X)^{\alpha},
\]

where $^{\alpha}$ denotes the opposite, i.e., the group obtained by reversing the order of multiplication.

If $N = \{1\}$, then $Y_{\{1\}}$ is called the universal covering of $X$, and denoted by $\hat{X}$. Then, we have

\[
\pi_1(X, a) \cong \text{Aut}(\hat{X}/X)^{\alpha}.
\]

Thus, if we can define a universal covering without using paths, then we can define the fundamental group. Essentially this is the case for schemes, a projective system (or a pro-object) plays the role of the universal covering. However, if we adopt $\text{Aut}(\hat{X}/X)$ as the definition of the fundamental group, it is not clear where the dependence on the choice of $a$ disappeared. The functoriality of $\pi_1$ is also not clear, and the definition of fundamental groupoid is difficult.

A smart idea is to use all (possibly non connected) coverings of $X$.

We consider the category $\mathcal{C}_X$ of unramified coverings of $X$, i.e., an object is a covering $f : Y \to X$, and a morphism is $Y' \to Y$ compatible with $f', f$. Thus, differently from $\text{Con}(X, a)$, a point is not specified, and the covering
may not be connected. Let \( a, b \in X \) be points. The discrete set \( f^{-1}(a) \subset Y \) is called the fiber of \( f \) at \( a \). Take an element \( a' \in f^{-1}(a) \). By lifting of the path \( \gamma \in \pi_1(X; a, b) \) to a path starting from \( a' \) in \( Y \) we have \( \tilde{\gamma} \in \pi_1(Y; a', b') \), and the end point \( b' \) of \( \tilde{\gamma} \) is uniquely determined. Thus, we obtain a bijection

\[
c_f(\gamma) : f^{-1}(a) \to f^{-1}(b), a' \mapsto b',
\]

in other words, an action of groupoid

\[
c_f : \pi_1(a, b) \times f^{-1}(a) \to f^{-1}(b)
\]

with \((\gamma, a') \mapsto c_f(\gamma)(a') = b'\). \( c_f(\gamma) \) is a bijection from \( f^{-1}(a) \) to \( f^{-1}(b) \), which is compatible with morphisms \( Y' \to Y \). The assignment \((f : Y \to X) \mapsto f^{-1}(a) \) gives a covariant functor

\[
\mathcal{C}_X \to \text{Sets}
\]

from the category of unramified coverings to the category of sets, which we denote by \( F_a \). Each element of \( \pi_1(X; a, b) \) gives a natural transformation \( F_a \mapsto F_b \), which is a natural equivalence.

On the other hand, a natural transformation \( F_a \mapsto F_b \) always comes from some element of \( \pi_1(X; a, b) \). To see this, note that \( \mathcal{C}_X \) has a special object, namely, the universal covering \( p : \tilde{X} \to X \). Actually, the object \( \tilde{X} \) represents the fiber functor \( F_a \), i.e., we have a natural isomorphism \( F_a(Y) \cong \text{Hom}_{\mathcal{C}_X}(\tilde{X}, Y) \). To fix the isomorphism, it is enough to fix a point \( \tilde{a} \in \tilde{X} \) above \( a \). Then, for every point \( b \in f^{-1}(a) \), there exists a unique homomorphism \( \tilde{X} \to Y \) with \( \tilde{a} \mapsto b \), by the property of the universal covering.

We shall see that a natural transformation \( F_a \to F_b \) comes from an element of \( \pi_1(X; a, b) \). A natural transformation \( \gamma : F_a \to F_b \) gives a map \( \gamma(\tilde{X}) : F_a(\tilde{X}) = p^{-1}(a) \to F_b(\tilde{X}) = p^{-1}(b) \). Then, once we choose a \( \tilde{a} \in p^{-1}(a) \), we have \( \gamma(\tilde{X})(\tilde{a}) \in p^{-1}(b) \), which we denote \( \tilde{b} \). Now, by the naturality of \( \gamma \), it commutes with any automorphism of \( \tilde{X}/X \). Since \( \tilde{X}/X \) is a Galois cover, for any \( \tilde{a}' \in p^{-1}(a) \), there is an automorphism \( \tau : \tilde{X} \to \tilde{X} \) such that \( \tau(\tilde{a}) = \tilde{a}' \). This shows that the image of \( \tilde{a}' \) by \( \gamma(\tilde{X}) \) must be \( \tau(\tilde{b}) \). Thus, \( \gamma(\tilde{X}) : p^{-1}(a) \to p^{-1}(b) \) is bijective, and it is uniquely determined, once \( \tilde{b} \) is chosen, by compatibility with \( \tau \). Let \( \tilde{\gamma} \) be a path from \( \tilde{a} \) to \( \tilde{b} \) in \( \tilde{X} \). \( \tau(\tilde{\gamma}) \) for \( \tau \in \text{Aut}(\tilde{X}/X) \) gives the bijection \( F_a(\tilde{X}) \to F_b(\tilde{X}) \).

Since connected components of other coverings are quotients of the universal covering, it is easy to see that any choice of \( \tilde{b} \) uniquely gives a natural transformation \( F_a \to F_b \), and it comes from the path from \( a \) to \( b \) which is the projection of \( \tilde{\gamma} \) to \( X \). Thus, we have \( \text{Hom}(F_a, F_b) \cong \pi_1(X; a, b) \) canonically.
This identifies the groupoid \( \{ \pi_1(X; a, b)|a, b \in X \} \) with the groupoid whose objects are \( F_a : C_X \to \text{Sets} \), and the morphisms are the natural transformations \( F_a \to F_b \), which are automatically invertible.

Since \( F_a \) is representable by \( X \), we can identify \( \pi_1(X, a) = \text{Aut}(F_a) \) with the opposite group of \( \text{Aut}(X/X) \), because of the Yoneda lemma

\[
\text{Aut}(F_a) \cong \text{Aut}(\text{Hom}_C(X, -)) = \text{Aut}(X)^\circ,
\]

where \( \cong \) is determined once \( \bar{a} \) is specified.

Now, \( F_a : C_X \to \text{Sets} \) induces a functor from \( C_X \) to the category \( \pi_1(X, a) \)-set, whose objects are the sets with an action of \( \pi_1(X, a) = \text{Aut}(F_a) \), and whose morphisms are the maps compatible with this action. This functor gives a categorical equivalence. To establish the equivalence, let \( S \) be a \( \pi_1(X, a) \)-set. We decompose \( S \) to orbits, and construct a covering corresponding to each orbit, then take the direct sum. For an orbit, take one point and let \( H \) be the stabilizer of the point. The covering corresponding to \( H \) gives the desired covering for that orbit.

**Proposition 3.1.** The category \( C_X \) of unramified coverings of an arcwise and locally arcwise simply connected topological space \( X \) is categorically equivalent to \( \pi_1(X, a) \)-set. The equivalence is given by the fiber functor

\[
F_a : (f : Y \to X) \mapsto f^{-1}(a).
\]

The \( \pi_1(X, a) \) action on \( f^{-1}(a) \) comes from \( \pi_1(X, a) = \text{Aut}(F_a) \).

### 3.2. Finite coverings

Roughly speaking, the etale fundamental groupoid of a connected scheme is defined by using the category of unramified covers in an algebraic sense. We don’t have an analogue of real-one dimensional “path”, say, in the positive characteristic world, but we have a good category and functors which allow us a categorical formulation of the algebraic (or etale) fundamental groupoid.

Before proceeding to etale fundamental groups, we note what will occur if we restrict \( C_X \) to the category \( C_{X, \text{fin}} \) of finite unramified coverings and the fiber functor

\[
F_a : C_{X, \text{fin}} \to \text{Finsets},
\]

where \( \text{Finsets} \) is the category of finite sets. This modification is essential when we work in the category of algebraic varieties.

A problem is that this functor \( F_a \) is not representable by an object in \( C_{X, \text{fin}} \). So, instead of the universal covering, we use a projective system, called a \textit{pro-object}, which represents the functor \( F_a \). Let \( (P_\lambda)_{\lambda \in \Lambda} \) be the system of all \textit{connected} finite Galois coverings of \( X \) with one point above \( a \).
specified. That is, an object of \( P_\lambda \) is a pair \((a_Y, Y)\) with a connected finite unramified covering \( p_Y : Y \to X \) and \( a_Y \mapsto a \), and a morphism is \( Y \mapsto Y' \) which maps \( a_Y \) to \( a_{Y'} \). We consider \( (P_\lambda) \) as a projective system in \( \mathcal{C}_{X, \text{fin}} \) (thus, \( a_Y \) for each \( Y \) gives no restriction on morphisms in \( \mathcal{C}_{X, \text{fin}} \)).

It can be shown that
\[
\mathrm{Hom}_{\text{pro-}\mathcal{C}_{X, \text{fin}}}((P_\lambda), Z) := \lim_{\to \lambda} \mathrm{Hom}_{\mathcal{C}_{X, \text{fin}}}(P_\lambda, Z) \cong p^{-1}_Z(a).
\]

Then, one can show
\[
\mathrm{Aut}(P_a)^{\text{opposite}} = \mathrm{Aut}((P_\lambda)) = \proj \lim_{\lambda} \mathrm{Aut}(P_\lambda)^{\text{opposite}} = \pi_1(\widehat{X}, a).
\]

The first identity comes from the Yoneda lemma, and the last equality is because \( \mathrm{Aut}(P_\lambda)^o \) is the finite quotient of \( \pi_1(X, a) \) corresponding to \( P_\lambda \). Both equalities are fixed because a system \( (a_\lambda) \) is fixed. In this case, the category \( \mathcal{C}_{X, \text{fin}} \) is equivalent to the category of finite sets with continuous action by \( \pi_1(\widehat{X}, a) \), which we call the category of finite \( \pi_1(\widehat{X}, a) \)-sets.

**Proposition 3.2.** \( \mathcal{C}_{X, \text{fin}} \) is categorically equivalent to the category of finite \( \pi_1(\widehat{X}, a) \)-sets. The equivalence is given by the fiber functor \( F_a \).

### 3.3. Etale fundamental groups

In the following, we work in the category of schemes. We shall only sketch the story of the etale fundamental groups here. For the precise notions, see SGA1 [7].

**Definition 3.1.** Let \( f : X \to Y \) be a morphism of finite type, \( x \in X \), \( y := f(x) \in Y \). We say \( f \) is unramified at \( x \), if \( \mathcal{O}_{X, x}/f(m_y)\mathcal{O}_{X, x} \) is a finite direct sum of finite separable field extensions of \( k(y) \). If moreover \( f \) is flat at \( x \), then \( f \) is said to be etale at \( x \). If \( f \) is etale at every point \( x \in X \), then \( f \) is called etale. If moreover \( f \) is finite and \( Y \) is connected, then \( f : X \to Y \) is called an etale covering.

If \( X \) and \( Y \) are algebraic varieties over an algebraically closed field \( K \subset \mathbb{C} \), and if \( x \) is a closed point, then it is known that \( f \) is etale at \( x \in X \) if and only if \( f \) is finite and unramified as an analytic morphism [7, Chapter XII]. Thus, the etale morphisms correctly generalize the notion of unramified coverings.

**Definition 3.2.** Let \( X \) be a locally noetherian connected scheme. Let \( C_X \) be the category of etale coverings of \( X \), i.e., objects are finite etale \( f : Y \to X \), and morphisms are \( Y' \to Y \) compatible with \( f', f \).

This category is an analogue of that of finite unramified coverings of a connected topological space \( X \).
There is a notion of Galois category. It consists of a category $C$ and a functor called the fiber functor, $F : C \rightarrow \text{Finsets}$, and satisfies six axioms stated in [7, Chapter V-64], which we shall omit here. Once we have a Galois category, we can define its fundamental group with base point $F$ as $\text{Aut}(F)$, i.e., the group of natural transformation from $F$ to itself. This becomes a profinite group. Two fiber functors $F, G : C \rightarrow \text{Finsets}$ are non-canonically isomorphic, and the set of natural transformations from $F$ to $G$ is a groupoid, with objects fiber functors and morphisms natural transformations.

Similarly to the topological case, one can show the category equivalence between $C_X$ and the category of the finite sets with $\text{Aut}(F)$-continuous action.

**Theorem 3.1.** [7, Chapter V] Let $X$ be a locally noetherian connected scheme. Take a geometric point $a : \text{Spec}\Omega \rightarrow X$, where $\Omega$ is an algebraically closed field. Then, the category $C_X$ of finite etale covers of $X$, with fiber functor $F_a : C_X \rightarrow \text{Finset}$, $(f : Y \rightarrow X) \mapsto f^{-1}(a) = Y \times_X \text{Spec}\Omega$, is a Galois category.

**Definition 3.3.**

$$\pi_1^{\text{alg}}(X, a) := \text{Aut}(F_a).$$

Thus, the category of finite etale covers of $X$ is equivalent to the category of finite sets with $\pi_1^{\text{alg}}(X, a)$-action. Similarly to the topological case, we may use $(P_\lambda)$, the projective system of connected finite Galois cover of $X$, with a geometric point $a_\lambda$ above $a$ compatibly specified. Then, by forgetting $a_\lambda$, we may regard $(P_\lambda)$ as a projective system in $C_X$, which pro-represents $F_a$. Then, we have

$$\pi_1^{\text{alg}}(X, a) := \text{Aut}(F_a) = \text{proj lim}_\lambda (P_\lambda).$$

In this setting, the functoriality of $\pi_1^{\text{alg}}$ is easy. For $f : X \rightarrow Y$, we have $\pi_1^{\text{alg}}(X, a) \rightarrow \pi_1^{\text{alg}}(Y, f(a))$, since $(\cdot) \times_Y X$ is a functor $f^* : C_Y \rightarrow C_X$, and $F_a \circ f^* = F_{f(a)} : C_Y \rightarrow \text{Finsets}$ holds, so an element of $\text{Aut}(F_a)$ gives an element of $\text{Aut}(F_{f(a)})$, inducing

$$\text{Aut}(F_a) = \pi_1^{\text{alg}}(X, a) \rightarrow \text{Aut}(F_{f(a)}) = \pi_1^{\text{alg}}(Y, f(a)).$$

Let $X$ be a geometrically connected scheme over a field $K$. Let $a : \text{Spec} \bar{K} \rightarrow X$ be a geometric point. The sequence

$$X \otimes \bar{K} \rightarrow X \rightarrow \text{Spec} K$$
gives a short exact sequence

\[ 1 \to \pi_1^{alg}(X \otimes_K \overline{K}, a) \to \pi_1^{alg}(X, a) \to \pi_1^{alg}(\text{Spec}K, \text{Spec}\overline{K}) \to 1, \]

which is nothing but (2.2) (for a proof, see [7, Chapter X, XIII]).

It is easy to show that an object of \( C_{\text{Spec} K} \) is a direct sum of a finite number of finite separable extensions of \( K \), and morphisms are usual homomorphisms of algebras over \( K \). A connected object is the spectrum of a field. Once we fix a geometric point \( a : \text{Spec}\Omega \to \text{Spec}K \), the pro-object which represents the fiber functor \( F_a \) is the system of finite Galois extensions of \( K \) inside \( \Omega \) (this inclusion into \( \Omega \) corresponds to choosing a point \( a_N \) in the fiber \( Y_N \to X \) above \( a \)). Thus, we have

\[ \pi_1^{alg}(\text{Spec}K, \text{Spec}\Omega) \overset{\text{contra}}{=} \text{proj lim}_{L} \text{Aut}(\text{Spec}L/\text{Spec}K) \overset{\text{contra}}{=} \text{proj lim}_{L} G(L/K), \]

where \( L \) runs through the finite Galois extensions of \( K \) in \( \Omega \), and it is nothing but \( G(K^{\text{sep}}/K) \) where \( K^{\text{sep}} \subset \Omega \) is the separable closure of \( K \) in \( \Omega \).

**Proposition 3.3.** Let \( \Omega \) be an algebraically closed field, and let \( K \subset \Omega \) be a subfield. Then

\[ \pi_1(\text{Spec}K, \text{Spec}\Omega) = G(K^{\text{sep}}/K) \]

holds, where \( K^{\text{sep}} \) is the separable closure of \( K \) in \( \Omega \).

The geometric part of the fundamental group can be obtained as follows. A theorem called “Riemann’s existence theorem” in SGA1[7, Theorem 5.1 P.332] assures that a finite unramified covering of an algebraic variety \( X \) over \( \mathbb{C} \) is algebraic and etale over \( X \), i.e., \( C_X \) and \( C_{X, \text{fin}} \) are categorically equivalent. An argument in SGA1[7, Chapter XIII] says that if \( X \) is an algebraic variety over an algebraically closed field \( \overline{K} \subset \mathbb{C} \), then the base change \((-) \otimes_K \overline{K} \mathbb{C} \) gives a category equivalence between \( C_{X \otimes \mathbb{C}} \) and \( C_X \). These category equivalences are compatible with fiber functors, so we have

\[ \pi_1^{\text{alg}}(X, a) = \pi_1^{\text{alg}}(X \otimes \mathbb{C}, a) = \text{Aut}_{C_{X, \text{fin}}}(F_a) = \pi_1(X, a). \]

**Exercise 3.1.** Show that the universal covering of the complex plane \( \mathbb{C} \) minus 0 is still an algebraic variety, but that of \( \mathbb{C} \) minus 0 and 1 is not. Even in the former case, the covering map is not algebraic.

**Exercise 3.2.** Describe the category \( C_X \) of finite etale coverings where \( X \) is the affine line minus one point 0 over \( \mathbb{Q} \).
4. Arithmetic mapping class groups

4.1. The algebraic stack $M_{g,n}$ over $\text{Spec}\mathbb{Z}$. I do not give the definition of an algebraic stack, the definition of the fundamental group of an algebraic stack, and so on, in this note, simply because of my lack of ability to state it concisely. I would just like to refer to [5] for the definition of an algebraic stack, the moduli stack of genus $g$ curves and the moduli stack of stable curves and to [19] for the case of $n$ pointed genus $g$ curves. For the arithmetic fundamental group of the moduli stack, see [26] (but this article requires prerequisites on etale homotopy [1]).

We just sketch the picture. Let $g, n$ be integers with $2g - 2 + n > 0$. We want to introduce the universal property of the moduli stack of $n$ pointed genus $g$ curves.

**Definition 4.1.** A family of $n$ pointed genus $g$ curves over a scheme $S$ (a family of $(g,n)$-curves in short), $C \to S$, is a proper smooth morphism $C^* \to S$, whose fibers are a proper smooth curves of genus $g$, with $n$ sections $s_1, s_2, \ldots, s_n : S \to C^*$ given, where the images of the $s_i$ do not intersect each other, and $C \to S$ is the complement of the image of these sections in $C^*$.

What we want is the universal family $\mathcal{C}_{g,n} \to \mathcal{M}_{g,n}$, which itself is a family of $(g,n)$-curves, with the universal property that for any family of $(g,n)$-curves $C \to S$, we have a unique morphism $S \to \mathcal{M}_{g,n}$ such that $C$ is isomorphic to the base change $\mathcal{C}_{g,n} \times_{\mathcal{M}_{g,n}} S$. Unfortunately, we don’t have such a universal family in the category of schemes. So, we need to enlarge the category to that of algebraic stacks.

I just describe some properties of algebraic stacks here. The category of algebraic stacks contains the category of schemes as a full subcategory, and algebraic stacks behave similarly to schemes. In the category of algebraic stacks, we have the correct universal family $\mathcal{C}_{g,n} \to \mathcal{M}_{g,n}$.

The notion of finite morphisms, etale morphisms, connectedness, etc. can be defined for algebraic stacks. In particular, for a connected algebraic stack, we have the category of its finite etale covers. It becomes a Galois category, and we have its etale fundamental group.

The algebraic stack $\mathcal{M}_{g,n}$ is defined over $\text{Spec}\mathbb{Z}$. But from now on, we consider $\mathcal{M}_{g,n}$ over $\text{Spec}\mathbb{Q}$.

4.2. The arithmetic fundamental group of the moduli stack. Takayuki Oda [26] showed that the etale homotopy type of the algebraic stack $\mathcal{M}_{g,n} \otimes \mathbb{Q}$
is the same as that of the analytic stack $\mathcal{M}^a_{g,n}$, and using Teichmüller space, showed that the latter object has the etale homotopy type $K(\Gamma_{g,n}, 1)$ in the sense of Artin-Mazur [1], where $\Gamma_{g,n}$ is the Teichmüller-modular group or the mapping class group of $n$-punctured genus $g$ Riemann surfaces.

This shows as a corollary

$$\pi_1^{alg}(\mathcal{M}_{g,n} \times \overline{\mathbb{Q}}, a) \cong \hat{\Gamma}_{g,n},$$

and gives a short exact sequence

$$1 \to \pi_1^{alg}(\mathcal{M}_{g,n} \times \overline{\mathbb{Q}}, a) \to \pi_1^{alg}(\mathcal{M}_{g,n}, a) \to G(\overline{\mathbb{Q}}/\mathbb{Q}) \to 1. \quad (4.1)$$

Also, the vanishing of $\pi_2$ of $\mathcal{M}_{g,n}$ gives a short exact sequence

$$1 \to \pi_1^{alg}(C_{g,n}, b) \to \pi_1^{alg}(C_{g,n}, b) \to \pi_1^{alg}(\mathcal{M}_{g,n}, a) \to 1, \quad (4.2)$$

where $a$ is a geometric point of $\mathcal{M}_{g,n}$, $C_{g,n}$ is the fiber on $a$, $b$ a geometric point of $C_{g,n}$. Hence, $C_{g,n}$ is a $(g, n)$-curve over an algebraically closed field, and $\pi_1^{alg}(C_{g,n}, b)$ is isomorphic to the profinite completion of the orientable surface of $(g, n)$-type, i.e., the profinite completion of

$$\Pi_{g,n} := \langle \alpha_1, \beta_1, \ldots, \alpha_g, \beta_g, \gamma_1, \gamma_2, \ldots, \gamma_n;$$

$$[\alpha_1, \beta_1][\alpha_2, \beta_2] \cdots [\alpha_g, \beta_g] \gamma_1 \cdots \gamma_n = 1 \rangle, \quad (4.3)$$

where $\gamma_i$ are paths around the punctures, $\alpha_i, \beta_i$ are usual generators of $\pi_1$ of an orientable surface.

Once we are given a short exact sequence (4.2), in the same way as §2.3, we have the monodromy representation

$$\rho_{g,n} : \pi_1^{alg}(\mathcal{M}_{g,n}, a) \to \text{Out}(\pi_1^{alg}(C_{g,n}, b)) \cong \text{Out}(\hat{\Pi}_{g,n}),$$

which is called arithmetic universal monodromy representation. This contains the usual representation of the mapping class group $\Gamma_{g,n}$ in the fundamental group of the orientable surface $\Pi_{g,n}$, since the restriction of $\rho_{g,n}$ to

$$\pi_1^{alg}(\mathcal{M}_{g,n} \otimes \overline{\mathbb{Q}}, b) \subset \pi_1^{alg}(\mathcal{M}_{g,n}, b)$$

coincides with

$$\hat{\Gamma}_{g,n} \to \text{Out}(\hat{\Pi}_{g,n}),$$

which comes from the natural homomorphism

$$\Gamma_{g,n} \to \text{Out}(\Pi_{g,n}).$$

This latter may be called the topological universal monodromy. What do we get if we consider the arithmetic universal monodromy instead of the
topological one? There is an interesting phenomenon: “arithmetic action gives an obstruction to topological action.”

5. A conjecture of Takayuki Oda

5.1. Weight filtration on the fundamental group. Let $C$ be a $(g,n)$-curve, and $\Pi_{g,n}$ be its (classical) fundamental group. We define its weight filtration as follows.

**Definition 5.1. (Weight filtration on $\Pi_{g,n}$.)**

We define a filtration on $\Pi_{g,n}$

$$\Pi_{g,n} = W_{-1}\Pi_{g,n} \supset W_{-2}\Pi_{g,n} \supset W_{-3}\Pi_{g,n} \supset \cdots$$

By $W_{-1} := \Pi_{g,n}$,

$$W_{-2} :=<[\Pi_{g,n},\Pi_{g,n}],\gamma_1,\gamma_2,\cdots,\gamma_n>_{\text{norm}},$$

where $<\cdot>_{\text{norm}}$ denotes the normal subgroup generated by elements inside $<$ and $[,]$ denotes the commutator product, $\gamma_i$ are elements in the presentation (4.3), and then

$$W_{-N} :=<[W_{-i},W_{-j}]|i+j = N>_{\text{norm}}$$

inductively for $N \geq 3$.

Fix a prime $l$. We define a similar filtration on the pro-$l$ completion of $\Pi_{g,n}^l$. There, $<\cdot>_{\text{norm}}$ and $[,]$ are the topological closure of the normal subgroup generated by the elements inside $<$, the commutators, respectively.

It is easy to check that $gr_j(\Pi_{g,n}) := W_{-j}/W_{-j-1}$ is abelian, and is central in $\Pi_{g,n}/W_{-j-1}$. In other words, $W_{-}$ is the fastest decreasing central filtration with $W_{-2}$ containing $\gamma_1,\ldots,\gamma_n$. It is known that each $gr_j$ is a free $\mathbb{Z}$-module (free $\mathbb{Z}_l$-module, respectively for pro-$l$ case) of finite rank $[2] [18]$.

This notion of weight filtration came from the study of the mixed Hodge structure on the fundamental groups, by Morgan and Hain [9], but for the particular case of $\mathbb{P}^1 - \{0, 1, \infty\}$, Ihara had worked on this [11] independently, from an arithmetic motivation.

For $x \in W_{-i}, y \in W_{-j}$, $[x,y] \in W_{-i-j}$ holds, and this defines a $\mathbb{Z}$-bilinear product $gr_{-i} \otimes gr_{-j} \to gr_{-i-j}$. We define

$$Gr_{\Pi_{g,n}} := \oplus_{i=1}^\infty gr_{-i}(\Pi_{g,n}).$$

With the product $[x,y]$, $Gr_{\Pi_{g,n}}$ becomes a Lie algebra over $\mathbb{Z}$. For $\Pi_{g,n}^l$, we have a Lie algebra over $\mathbb{Z}_l$. 

---

*Arithmetic fundamental groups* 377
Definition 5.2. (Induced filtration) We equip $\Gamma := \text{Aut}(\Pi_{g,n})$, with the following filtration $\Gamma = I_0 \supset I_1 \supset I_2 \supset \cdots$, called induced filtration:

$\gamma \in I_j \iff$ for any $k \in \mathbb{N}$ and $x \in W_{-k}(\Pi_{g,n})$, $\bar{\gamma}(x)x^{-1} \in W_{-k-j}(\Pi_{g,n})$ holds.

We pushout this filtration to $\text{Out}(\Pi_{g,n})$. For an outer representation $\rho : G \to \text{Out}(\Pi_{g,n})$ of any group $G$, we pullback the filtration to $G$, and call it induced filtration:

$$G = I_{-0}(G) \supset I_{-1}(G) \supset \cdots$$

The same kind of filtration is defined for $G \to \text{Out}(\Pi_{g,n})$.

In this case, we define

$$\text{Gr}(G) := \bigoplus_{i=1}^{\infty} \text{gr}_i(G) = \bigoplus_{i=1}^{\infty} I_{-i}(G)/I_{-i-1}(G)$$

(note that $i$ starts from 1, not 0), then $\text{Gr}(G)$ becomes a Lie algebra. By definition, if we induce filtrations by $G \to G' \to \text{Out}(\Pi_{g,n})$, then $\text{Gr}(G) \hookrightarrow \text{Gr}(G')$. By [18] [2], $\text{GrOut}(\Pi_{g,n})$ injects to $\text{GrOut}(\Pi_{g,n})$, and hence if

$$G \to \text{Out}(\Pi_{g,n}) \to \text{Out}(\Pi_{g,n})$$

factors through $G' \to \text{Out}(\Pi_{g,n})$, then $\text{Gr}G \hookrightarrow \text{Gr}G'$ holds.

The natural homomorphism

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

gives a natural filtration to $\Gamma_{g,n}$, which seems to go back to D. Johnson [17].

By composing with the natural morphism

$$\text{Out}(\widehat{\Pi_{g,n}}) \to \text{Out}(\Pi_{g,n}^l),$$

we have

$$\pi_{1}^{\text{alg}}(\mathcal{M}_{g,n},a) \to \text{Out}(\Pi_{g,n}^l),$$

hence $\pi_{1}^{\text{alg}}(\mathcal{M}_{g,n},a)$, $\pi_{1}^{\text{alg}}(\mathcal{M}_{g,n} \otimes \mathbb{Q},a)$, is equipped with an induced filtration, and we have a natural injection

$$\text{Gr}\pi_{1}^{\text{alg}}(\mathcal{M}_{g,n},a) \hookrightarrow \text{Gr}\pi_{1}^{\text{alg}}(\mathcal{M}_{g,n} \otimes \mathbb{Q},a),$$

and the image is a Lie algebra ideal.

Conjecture 5.1. (Conjectured by Takayuki Oda) The quotient of

$$\text{Gr}(\pi_{1}^{\text{alg}}(\mathcal{M}_{g,n},a))$$

by the ideal

$$\text{Gr}(\pi_{1}^{\text{alg}}(\mathcal{M}_{g,n} \otimes \mathbb{Q},a))$$

is independent of $g, n$ for $2g - 2 + n \geq 0$. 

This conjecture is almost proved by a collection of works by Nakamura, Ihara, Takaо, myself, et al. [21] [23] [16],

**Theorem 5.1.** The quotient of

\[ \text{Gr}(\pi_1^{\text{alg}}(\mathcal{M}_{g,n}, a)) \otimes \mathbb{Z}_l \mathbb{Q}_l \]

by

\[ \text{Gr}(\pi_1^{\text{alg}}(\mathcal{M}_{g,n} \otimes \overline{\mathbb{Q}}, a)) \otimes \mathbb{Z}_l \mathbb{Q}_l \]

is independent of \( g, n \) for \( 2g - 2 + n \geq 0 \).

The significance of this result is that for \( \mathcal{M}_{0,3} = \text{Spec} \mathbb{Q}_l \) the Lie algebra is understood to some extent by deep results such as Anderson-Coleman-Ihara’s power series and Soulé’s non-vanishing of Galois cohomology, and it implies a purely topological consequence: an obstruction to the surjectivity of the Johnson homomorphisms.

5.2. **Obstruction to the surjectivity of Johnson morphisms.** For simplicity, assume \( n = 0 \), and hence \( \Gamma_g \) denotes the mapping class group of genus \( g \) Riemann surfaces. Take \( \sigma \in \mathcal{M}_{g,n} \Gamma_g \), and take a suitable lift \( \tilde{\sigma} \in \mathcal{M}_{g,n} \text{Aut}(\Pi_g) \) as in Definition 5.2. Then, \( \tilde{\sigma}(\alpha)\alpha^{-1} \in \mathcal{W}_{m-1}\Pi_g \) for any \( \alpha \in \Pi_g \). The map

\[ \Pi_g \to \mathcal{W}_{m-1}\Pi_g; \quad \alpha \mapsto \tilde{\sigma}(\alpha)\alpha^{-1} \]

gives a linear map \( \Pi_g/\mathcal{W}_{-1}\Pi_g \to \mathcal{G}_{m-1}\Pi_g \). We denote \( H := \Pi_g/\mathcal{W}_{-1}\Pi_g \) for homology, then we have Poincaré duality \( H^* \cong H \), and define

\[ h_{g,*}(m) := \text{Ker}(\text{Hom}(H, \mathcal{G}_{m-1}\Pi_g) \to \mathcal{G}_{m-2}\Pi_g), \]

where

\[ \text{Hom}(H, \mathcal{G}_{m-1}\Pi_g) \to \mathcal{G}_{m-2}\Pi_g \]

comes from

\[ \text{Hom}(H, \mathcal{G}_{m-1}\Pi_g) \cong H \otimes \mathcal{G}_{m-1}\Pi_g \xrightarrow{[\mathbb{L}]} \mathcal{G}_{m-2}\Pi_g. \]

The lift \( \tilde{\sigma} \) in \( \text{Aut}(\Pi_g) \) is mapped into \( h_{g,*}(m) \). The ambiguity of taking the lift in \( \text{Aut} \) is absorbed by taking the quotient by the action of \( \mathcal{G}_{m}\Pi_g \) by \( \alpha \mapsto [\alpha, x] \) for \( x \in \mathcal{G}_{m}\Pi_g \), and we have an injective morphism

\[ \mathcal{G}_{m}(\Gamma_g) \hookrightarrow h_{g,*}/\mathcal{G}_{m}\Pi_g \quad (\subset \text{Hom}(H, \mathcal{G}_{m-1}\Pi_g)/\mathcal{G}_{m}\Pi_g). \]

This is called the Johnson homomorphism [17] (see Morita [22]).

D. Johnson proved that this is an isomorphism for \( m = 1 \), but for general \( m \) it is not necessarily surjective; actually S. Morita gave an obstruction called Morita-trace [22] for \( m \) odd, \( m \geq 3 \).
We can define the same filtration for 
\[ \pi_1^{alg}(\mathcal{M}_g) \to \text{Out}(\Pi^f_g), \]
and then we have an injection 
\[ gr_m(\pi_1^{alg}(\mathcal{M}_g)) \hookrightarrow (h_{g,n}/gr_m\Pi_g) \otimes \mathbb{Z}_l \subset \text{Hom}(H, gr_{m-1}\Pi^f_g)/gr_m\Pi^f_g. \]

Theorem 5.1 asserts that 
\[ gr_m(\pi_1^{alg}(\mathcal{M}_{g,n} \otimes \overline{Q})) \to gr_m(\pi_1^{alg}(\mathcal{M}_{g,n})) \]
is not surjective for some \( m \), it has cokernel of rank independent of \( g, n \). As I am going to explain in the next section, for \((g, n) = (3, 0)\), it is known that this cokernel is nontrivial at least for \( m = 4k + 2, k \geq 1 \) (and the rank has a lower bound which is a linear function of \( m \)). Thus, 
\[ gr_m(\pi_1^{alg}(\mathcal{M}_{g,n} \otimes \overline{Q})) \to h_{g,n}/gr_m\Pi_g \otimes \mathbb{Z}_l \]
has also cokernel of at least that rank. This homomorphism is given by \( \otimes \mathbb{Z}_l \)
from the Johnson homomorphism, hence this gives an obstruction to the surjectivity of Johnson homomorphisms, which is different from Morita’s trace. The existence of such an obstruction was conjectured by Takayuki Oda, and proved by myself [21] and H. Nakamura [23] independently.

5.3. The projective line minus three points again. Let \( \mathbb{P}^1_{01\infty} \) denote the projective line minus three points over \( \mathbb{Q} \). This curve does not deform over \( \overline{\mathbb{Q}} \), and hence the universal family is trivial, 
\[ c_{0,3} = \mathbb{P}^1_{01\infty} \text{ and } \mathcal{M}_{0,3} = \text{Spec} \mathbb{Q}. \]
Geometrically, thus, there is no monodromy, but arithmetically this has huge monodromy as proved by Belyi (see §2.3).

Fix a prime \( l \). We shall consider pro-\( l \) completion \( \hat{F}^l_2 \) of the free group \( F_2 \)
in two generators, so we have 
\[ \pi_1^{alg}(\mathbb{P}^1_{01\infty} \otimes \overline{\mathbb{Q}}, a) = \hat{F}^l_2 \to F^l_2. \]
Then, we have a group homomorphism 
\[ \rho^l_{\mathbb{P}^1_{01\infty}} : G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Out}(F^l_2). \]
The weight filtration for the \((g, n) = (0, 3)\) curve essentially coincides with the lower central series 
\[ F^l_2 = F^l_2(1) \supset F^l_2(2) \supset F^l_2(3) \supset \cdots \]
defined inductively by $F_2^I(1) = F_2^I$, $F_2^I(m) = [F_3^I(m-1), F_2^I]$ (here $[,]$ denotes the closure of the commutator); the correspondence is

$$W_{-2m+1}(F_2^I) = W_{-2m}(F_2^I) = F_2^I(m) \quad (m \geq 1).$$

Ihara [11] started to study the filtration of $G(\overline{\mathbb{Q}}/\mathbb{Q})$ induced by this filtration, independently of the notion of weight etc. Note that, the case of $(0, 3)$ in Theorem 5.1, the geometric part vanishes, so the quotient in the theorem is nothing but just $Gr G(\overline{\mathbb{Q}}/\mathbb{Q})$ in this case.

The following is a corollary of the theory of power-series by Anderson, Coleman, Ihara, together with Soulé’s nonvanishing of Galois cohomology (there is a list of references, see the references in [11]).

**Theorem 5.2.** In the Lie algebra $Gr(G(\overline{\mathbb{Q}}/\mathbb{Q}))$, each $gr_{-m}(G(\overline{\mathbb{Q}}/\mathbb{Q}))$ does not vanish for odd $m \geq 3$.

Roughly speaking, by using Anderson-Coleman-Ihara’s power-series, one can construct a homomorphism

$$gr_{-2m}(G(\overline{\mathbb{Q}}/\mathbb{Q})) \to \text{Hom}_{G(\overline{\mathbb{Q}}/\mathbb{Q})}(\pi_1(\text{Spec}\mathbb{Z}[1/l]), \mathbb{Z}_l(m)).$$

It can be described as a particular Kummer cocycle, and the morphism does not vanish for odd $m \geq 3$ by Soulé’s result. The right-hand side is rank 1 up to torsion. An element $\sigma_{2m} \in gr_{-2m}(G(\overline{\mathbb{Q}}/\mathbb{Q}))$ which does not vanish in the right-hand side is called a Soulé element.

The following conjecture is often contributed to Deligne [4].

**Conjecture 5.2.** (i) $Gr(G(\overline{\mathbb{Q}}/\mathbb{Q})) \otimes \mathbb{Q}_l$ is generated by $\sigma_{2m} \ (m \geq 3$, odd$)$.  
(ii) $Gr(G(\overline{\mathbb{Q}}/\mathbb{Q})) \otimes \mathbb{Q}_l$ is a free graded Lie algebra.

The rank of $Gr_m(G(\overline{\mathbb{Q}}/\mathbb{Q}))$ as $\mathbb{Z}_l$-module has a lower bound which is a linear function of $m$, and these conjectures are verified for $m \leq 11$ [20] [27], but both conjectures seem to be still open. Ihara [14] recently showed that (ii) implies (i).
References


