Galois representations in fundamental groups and their Lie algebras

Makoto Matsumoto[*]

March 9, 2005

Contents

[*]Dept. Math. Hiroshima Univ. m-mat@math.sci.hiroshima-u.ac.jp

Abstract

Let X be a geometrically connected scheme over a field K. Then, the absolute Galois group G_K of K acts on the algebraic fundamental group $\pi_1^{\mathrm{alg}}(X \otimes \overline{K}, \overline{x})$.

This lecture explains the following:

1. This action is an analogy of "geometric monodromy of deformation family" in the topology.
2. Lie algebraization of the fundamental group is effective to extract some information from this action.

1 Algebraic fundamental group

1.1 The classic-topological fundamental group

Let $\mathcal{X}$ be an arcwise connected topological space, and x be a point on $\mathcal{X}$. Then, the (classical) fundamental group of $\mathcal{X}$ with base point x is defined by

$$\pi_1(\mathcal{X}, x) := \{\text{paths from } x \text{ to } x\}/\text{homotopy with } x \text{ fixed.}$$

For the ordering in composing two paths, we define $\gamma \circ \gamma'$ to be the path first going along γ' and then γ. (Some papers adopt the converse ordering.)

It is well-known that the fundamental group of a (real two-dimensional) sphere or a sphere minus one point is trivial, and that of the sphere minus two points is isomorphic to the additive group $\mathbb{Z}$. The fundamental group of a sphere minus three points is a free group of two generators, and this is a main subject of this lecture.

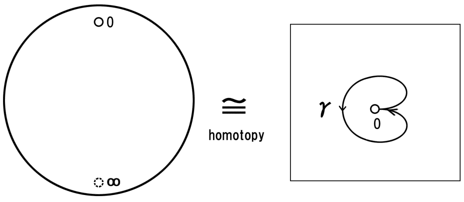
1.2 Unramified covering

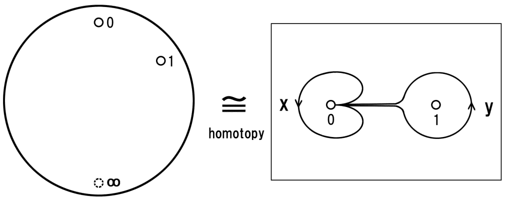
The fundamental group is an important (homotopy) invariant of a topological space. The importance may be justified by the following theorem.

Theorem 1.1. Let $\mathcal{X}$ be an arcwise connected and locally simply connected topological scheme, and x be a point on it. Then, there is an equivalence of categories

$$F_x : \{\text{unramified coverings of } \mathcal{X}\} \to \{\pi_1(\mathcal{X}, x)\text{-sets}\},$$

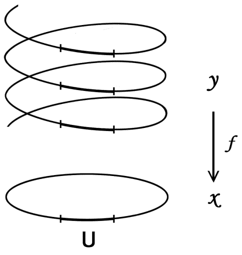
given by taking the inverse image of x.





We shall give precise definitions of the above two categories.

Definition 1.2. A continuous map $f : \mathcal{Y} \to \mathcal{X}$ is an *unramified covering*, if for every $x \in \mathcal{X}$ there is an open neighborhood $U \subset \mathcal{X}$ of x such that every connected component of $f^{-1}(U)$ is isomorphic to U through f.



Morphisms between $f : \mathcal{Y} \to \mathcal{X}, f' : \mathcal{Y}' \to \mathcal{X}$ are defined to be the continuous maps from $h : \mathcal{Y} \to \mathcal{Y}'$ satisfying $f = f' \circ h$. (By abuse of language, we simply say that h is compatible with f.)

An important example of unramified covering of $\mathcal{X}$ is its universal covering $\widetilde{\mathcal{X}}$. This is constructed as follows: take a point $x \in \mathcal{X}$. Then consider the set

$$\widetilde{\mathcal{X}} := \{\gamma : \text{path on } \mathcal{X} \text{ starting from } x\}/\text{homotopy}$$

where the homotopy is considered with the both ends of the path fixed.

Consider the morphism

$$p : \widetilde{\mathcal{X}} \to \mathcal{X}, \quad [\gamma] \mapsto \text{the end point of } \gamma.$$

Then, $\widetilde{\mathcal{X}}$ is equipped with a topology as follows. Take $[\gamma] \in \widetilde{\mathcal{X}}$, and set $z := p([\gamma])$ to be the end point of γ. Take a simply connected open neighborhood U of z. For each point u of U, there is a unique path (zu) (modulo homotopy) connecting z to u in U. By mapping $u \mapsto [(zu) \circ \gamma]$, we have a mapping $U \to \mathcal{X}$. Let $\tilde{U}$ denote its image. We can check that by taking $\tilde{U}$ as an open neighborhood of $[\gamma]$, $\widetilde{\mathcal{X}}$ is equipped with a topology such that p is an unramified covering. The fundamental group $\pi_1(\mathcal{X}, x)$ acts on $\widetilde{\mathcal{X}}$ (over $\mathcal{X}$) from right, by

$$\widetilde{\mathcal{X}} \times \pi_1(\mathcal{X}, x) \to \widetilde{\mathcal{X}}, \quad ([\gamma], [\beta]) \mapsto [\gamma \circ \beta].$$

We define the right hand side of Theorem 1.1.

Definition 1.3. For a group G, a G-set means a set S with a left action of G is specified, i.e.,

$$\rho : G \to \mathrm{Aut}(S)$$

is given. A morphism between two G-sets $S_1 \to S_2$ is a mapping compatible with G-actions. (I.e. $\rho_1(g)(h(s)) = h(\rho_2(g)(s))$ holds.)

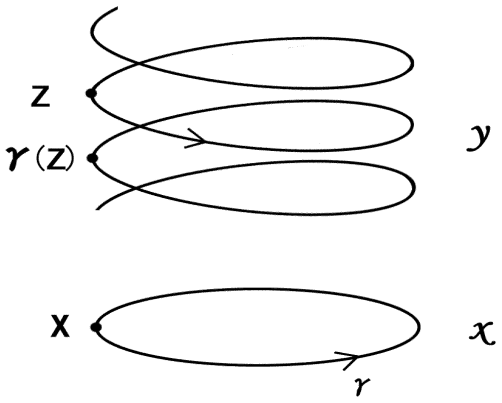
There is an obvious functor from the left category to the right one in Theorem 1.1:

$$F_x : (f : \mathcal{Y} \to \mathcal{X}) \mapsto f^{-1}(x).$$

The action of $\pi_1(\mathcal{X}, x)$ on $f^{-1}(x)$ is given by the *monodromy*: for $\gamma \in \pi_1(\mathcal{X}, x)$ and $z \in f^{-1}(x)$, there is a unique lift γ' in $\mathcal{Y}$ of γ starting from z. Then $\gamma(z)$ is defined as the endpoint of γ'. [1] Clearly this gives a left action of $\pi_1(\mathcal{X}, x)$ on $f^{-1}(x)$. Thus, we defined

$$F_x : \{\text{unramified coverings of } \mathcal{X}\} \to \{\pi_1(\mathcal{X}, x)\text{-sets}\}, \ (f : \mathcal{Y} \to \mathcal{X}) \mapsto f^{-1}(x).$$

[1] To be precise, we take open sets U_λ ($\lambda \in \Lambda$) of $\mathcal{X}$ whose union contains γ (here a path and its homotopy class are both denoted as γ), and each U_λ satisfies the property in Definition 1.2. By compactness, we may assume that $U_1, U_2, \ldots, U_n$ cover γ and $U_1 \cap \gamma$, $U_2 \cap \gamma$, $\ldots$, $U_n \cap \gamma$ are paths composable in this order. Then, there is a unique lift of $U_1 \cap \gamma$ in $\mathcal{Y}$ starting from $z \in f^{-1}(x) \subset \mathcal{Y}$. Then, there is a unique lift of $U_2 \cap \gamma$ starting from the end point of the previous lift. Thus, there is a unique lift γ' of γ in $\mathcal{Y}$ starting from z.



In the converse direction, we can construct an unramified covering of $\mathcal{X}$ from a $\pi_1(\mathcal{X}, x)$-set S as follows. For each orbit $O \subset S$ of the action of $\pi_1(\mathcal{X}, x)$, we take a point $o \in O$ and consider $\mathcal{Y}_O := \widetilde{\mathcal{X}}/G_o$ where G_o is the stabilizer of o in $\pi_1(\mathcal{X}, x)$. It follows from the construction that $\mathcal{Y}_O \to \mathcal{X}$ corresponds to the transitive $\pi_1(\mathcal{X}, x)$-set O. By taking direct sum over all orbits O, we have the desired covereing of $\mathcal{X}$. From the above, it is seen that the subcategory of the connected covering corresponds to the subcategory of the transitive $\pi_1(\mathcal{X}, x)$-sets.

We may define the fundamental group without using paths, in the following manner. Consider the functor

$$F_x : \{\text{unramified coverings of } \mathcal{X}\} \to \{\text{sets}\}, \quad (\pi_{\mathcal{Y}} : \mathcal{Y} \to \mathcal{X}) \mapsto \pi_{\mathcal{Y}}^{-1}(x).$$

This is called a fiber functor. Any path $\gamma \in \pi_1(X, x)$ acts on $F_x(\mathcal{Y}) = \pi_{\mathcal{Y}}^{-1}(x)$ by the monodromy. This action is compatible with any unramified maps $\mathcal{Y} \to \mathcal{Y}'$, i.e.,

$$\begin{tikzcd}
F_x(\mathcal{Y}) \arrow[r, "\gamma"] \arrow[d] & F_x(\mathcal{Y}) \arrow[d] \\
F_x(\mathcal{X}) \arrow[r, "\gamma"] & F_x(\mathcal{X})
\end{tikzcd}$$

commutes. This means that the action of γ is a natural (invertible) transformation from the functor F_x to itself.

This amounts to saying that we have a group homomorphism

$$\pi_1(X, x) \to \mathrm{Aut}(F_x).$$

This is proved to be an isomorphism. It is injective since $F_x(\widetilde{\mathcal{X}})$ is one to one with $\pi_1(X, x)$. It is surjective since any element σ of $\mathrm{Aut}(F_x)$ is the image of the path $\in \pi_1(X, x)$ that lifts to a path $\tilde{x} \to \sigma(\tilde{x})$ in $\widetilde{\mathcal{X}}$.

This is the way to define the algebraic fundamental group in SGA1[3]: we consider a suitable analogue to the unramified coverings and fiber functors. Then, the algebraic fundamental group is defined as the automorphism group of a fiber functor.

The suitable analogue to the unramified coverings in the algebraic situation is *étale*.

1.3 Galois groups

Before stating the definition of étale morphisms, we treat another concrete example: the absolute Galois groups. Here, we assume the reader to have the basic knowledge on (finite) Galois theory of field extension.

Let K be a field. A good analogy of a finite connected unramified covering is a finite field extension L of K. To be precise, we consider the following category $(\mathrm{Spec}K)_{et}$: its object is a ring R with injective homomorphism $K \to R$, where R is a finite direct product of finite separable extension field of K:

$$K \to R = \prod_i L_i,$$

and morphisms are those ring homomorphisms $R \to R'$ compatible with $K \to R$.

To compare with the unramified coverings, it is better to reverse the direction of the morphism. So, to each ring (commutative with unit) R, we associate an object $\mathrm{Spec}R$ (the spectrum of R) and to each ring homomorphism $R \to R'$ we associate a morphism $\mathrm{Spec}R' \to \mathrm{Spec}R$. Now,

$$\mathrm{Spec}R = \mathrm{Spec}(\prod_i L_i) \to \mathrm{Spec}K$$

is the analogue of a finite unramifed covering. We denote by

$$(\mathrm{Spec}K)_{et} := \text{category of } \mathrm{Spec}R \text{ as above},$$

where the morphisms are just ring homomorphisms $R \to R'$ compatible with $K \to R$, $K \to R'$. Why one can say that this is a good analogue? Because the following category equivalence holds:

$$\mathrm{Spec}K_{et} \cong \{G_K = \pi_1(\mathrm{Spec}K, x)\text{-finite sets}\}, \tag{1}$$

which we shall explain soon below (but $\pi_1(\mathrm{Spec}K, x)$ in the next section, in Example 1.5).

Take an algebraically closed field Ω with injective homomorphism

$$K \to \Omega, \text{ in other words, } x : \mathrm{Spec}\Omega \to \mathrm{Spec}K.$$

This is called a geometric point of $\mathrm{Spec}K$. Let $K^{\mathrm{sep}} \subset \Omega$ be the separable closure of K in Ω. Then, $\mathrm{Spec}K^{\mathrm{sep}} \to \mathrm{Spec}K$ surves as the universal covering of $\mathrm{Spec}K$, with a fiber $\tilde{x} : \mathrm{Spec}\Omega \to \mathrm{Spec}K^{\mathrm{sep}}$ above x is specified.

The above G_K is the absolute Galois group of K, i.e., it is the group of automorphisms of the field K^{sep} with trivial actions on K:

$$G_K := \mathrm{Aut}(K^{\mathrm{sep}}/K).$$

For any Galois extension $L \subset K^{\mathrm{sep}}$ of K, we have the restriction morphism

$$G_K := \mathrm{Aut}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(L/K) = G(L/K),$$

which can be proved to be surjective. An element $\sigma \in G_K$ gives a system of elements

$$\sigma|_L \in G(L/K) \text{ for all sub Galois extension } L,$$

and conversely, by giving such a system of elements compatible with restrictions $G(L'/K) \to G(L/K)$, we have an element of G_K. Using the terminology of projective limits, we have

$$G_K = \lim_{\leftarrow} G(L/K),$$

where L runs through all the finite sub Galois extension of K inside K^{sep}. The symbol $\lim_{\leftarrow}$ means the set of all the systems, i.e., choosing $\sigma_L \in G(L/K)$ for every L so that they are compatible with respect to $G(L'/K) \to G(L/K)$. Such set of the systems is called the projective limit of $G(L/K)$'s. [2]

A group which is a projective limit of finite groups is called a profinite group. It is naturally a topological group, by equipping the weakest topology such that every $G_K \to G(L/K)$ becomes continuous.

A G_K-finite set S is a (discrete) finite set with continuous G_K-action. This means that $G_K \to \mathrm{Aut}S$ factors through $G_K \to G(L/K) \to \mathrm{Aut}S$ with some finite Galois subextension L.

The functor from the left to the right in (1) is

$$\mathrm{Spec}R \mapsto \mathrm{Hom}_K(\mathrm{Spec}K^{\mathrm{sep}}, \mathrm{Spec}R) = \mathrm{Hom}_K(\mathrm{Spec}\Omega, \mathrm{Spec}R).$$

[2] See PP.116-121 of [2] for projective limits and profinite groups.

The right hand side is the set of fibers of Spec$R$ above the geometric point $x : \mathrm{Spec}\Omega \to \mathrm{Spec}K$. The group G_K naturally acts on this finite set from the left, by letting it act on K^{sep} from the left.

To construct the inverse, we start from a finite set S on which G_K acts continuously and transitively. Take an element $s \in S$, then we have $S \cong G_K/G_s$ as G_K-finite set, where G_s is the stabilizer of s. Now we consider the invariant subfield

$$L := (K^{\mathrm{sep}})^{G_s}.$$

Then Spec$L$ is the corresponding object in the left hand side. For non-transitive cases, we construct orbit-wise, as in the topological case.

All the basic properties of the Galois theory are included in the category equivalence (1). For example, let L/K be a finite Galois extension. Then, through (1) K corresponds to a one point set $\{*\}$ with trivial G_K action, and L corresponds to the transitive G_K-set $S_L := \mathrm{Hom}_K(L, K^{\mathrm{sep}})$, where the action factors through $G(L/K)$. The category equivalence amounts to saying that an intermediate field M is one to one with a $G(L/K)$-set Q which is a quotient of S_L. A qutotients Q of S_L is one to one with a subgroup of $G(L/K)$.

It is not hard to check that the correspondence is

$$M \to G(L/M),$$

which is one to one from the intermidiate fields to the subgroups of $G(L/K)$.

1.4 Galois category

There is a notion of Galois category [3, V, 4]. It is a category C with terminal objects, fiber products, initial objects, direct sums, and quotient by finite group actions, with a functor

$$F : C \to \{\text{finite sets}\}$$

satisfying suitable conditions (see [3, p.118, G1-G6]). We saw two examples: one is the category SpecK_{et} with a fiber functor $\mathrm{Spec}R \to \mathrm{Hom}_K(\mathrm{Spec}\Omega, \mathrm{Spec}R)$, and the other is the category of (not necessary connected) finite unramified coverings of $\mathcal{X}$ in Theorem1.1, with a fiber functor F_x.

Then, Theorem 4.1 in [3] states the following.

Theorem 1.4. Let C be a Galois category and F be a fiber functor. Define the fundamental group of C with base point F by

$$\pi_1(C, F) := \mathrm{Aut}F.$$

Then, this is a profinite group, and there is a category equivalence

$$C \to \{\pi_1(C,F)\text{-finite sets}\}$$

given by $C \mapsto F(C)$.

Example 1.5. Suppose that $C := (\mathrm{Spec}K)_{et}$ and $x : \mathrm{Spec}\Omega \to \mathrm{Spec}K$. Let us define

$$F_x : C \to \{\text{finite sets}\}$$

by

$$\mathrm{Spec}R \mapsto \mathrm{Hom}_K(\mathrm{Spec}\Omega, \mathrm{Spec}R) = \mathrm{Hom}_K(\mathrm{Spec}K^{\mathrm{sep}}, \mathrm{Spec}R).$$

Then, one can show that [3]

$$\pi_1((\mathrm{Spec}K)_{et}, F_x) := \mathrm{Aut}(F_x) \cong G(K^{\mathrm{sep}}/K) = G_K.$$

Example 1.6. Let C' be the category of unramified coverings of $\mathcal{X}$, and C be its full subcategory consisting of finite coverings. Then, C' is not a Galois category but C is. For $x \in \mathcal{X}$, the functor F'_x taking the fiber over x

$$F'_x : C' \to \{\text{sets}\}$$

restricts to

$$F_x : C \to \{\text{finite sets}\},$$

and this satisfies the axiom of the fiber functors. By restriction, we have

$$\pi_1(\mathcal{X}, x) \cong \mathrm{Aut}F'_x \to \mathrm{Aut}F_x.$$

We do not prove, but it follows (from the axioms of Galois categories) that in computing $\mathrm{Aut}F_x$, it suffices to consider $F_x(\mathcal{Y})$ where $\mathcal{Y} \to \mathcal{X}$ is a (finite) normal covering, i.e. $\mathcal{Y} \cong \tilde{\mathcal{X}}/N$ where N is a normal subgroup of $\pi_1(\mathcal{X}, x)$ of finite index. Thus, we have

$$\pi_1(C, F_x) := \mathrm{Aut}F_x \cong \varprojlim \pi_1(\mathcal{X}, x)/N,$$

where N runs over all the finite index normal subgroups.

For a (discrete) group G, its profinite completion $G^{\frown}$ is the profinite group defined by

$$G^{\frown} := \varprojlim G/N,$$

where N runs over all the finite index normal subgroups.

In sum, we have

$$\pi_1(C, F_x) \cong \pi_1(\mathcal{X}, x)^{\frown}.$$

[3] This is almost an immediate consequence of Yoneda Lemma:

$$\mathrm{Aut}(\mathrm{Hom}(X, -)) \cong (\mathrm{Aut}X)^{opposite}.$$

1.5 Finite etale coverings

A good generalization of both topological unramified *finite* coverings (§1.2) and finite separable extension of field (§1.3) is the notion of finite etale coverings[3, I].

First we state the definition in the language of schemes.

Definition 1.7. Let $f : Y \to X$ be a morphism of finite type between locally noetherian schemes. Let $y \in Y$. We say that f is etale at y if the induced morphism of local rings $f^* : \mathcal{O}_{f(y)} \to \mathcal{O}_y$ is flat, and

$$\mathcal{O}_{f(y)}/m_{f(y)} \to \mathcal{O}_y/(f^*(m_{f(y)})\mathcal{O}_y)$$

is a finite separable extension.

We say f is etale if it is etale at every point on Y. If f is finite and etale and X is connected, then $f : Y \to X$ is said to be a finite etale covering.

Suppose that X is connected. Let us define X_{et} to be the category of the finite etale coverings of X.

Definition 1.8. (Algebraic fundamental group, See SGA1[3, V].)

Let X be a connected locally noetherian scheme, and X_{et} be the category of finite etale coverings of X. Then, X_{et} is a Galois category. Let Ω be an algebraic closed field, and $x : \mathrm{Spec}\Omega \to X$ is a geometric point. Then, $F_x : Y \mapsto \pi_Y^{-1}(x)$ is a fiber functor. We define the algebraic fundamental group by

$$\pi_1(X, x) := \pi_1(X_{et}, F_x) = \mathrm{Aut}F_x.$$

To explain the language of schemes is beyond the scope of this lecture. However, the following results will almost suffice for this lecture.

Example 1.9. Let K be a field. The finite etale coverings $\mathrm{Spec}R \to \mathrm{Spec}K$ are the same with those defind in §1.3, i.e., the direct product of finite separable extensions. Thus $(\mathrm{Spec}K)_{et}$ in the sense of this section coincides with that in Example 1.5.

A geometric point $x : \mathrm{Spec}\Omega \to \mathrm{Spec}K$ gives a fiber functor F_x as in the same example, so we have

$$\pi_1(\mathrm{Spec}K, x) = \pi_1((\mathrm{Spec}K)_{et}, F_x) = \mathrm{Aut}(F_x) \cong G_K.$$

Example 1.10. Let $K \subset \mathbb{C}$ be an algebraically closed field. Let X be a scheme of finite type over K. Let X^{an} be the corresponding complex analytic set. Then, a morphism $f : Y \to X$ is finite etale if and only if its analytification $f^{\mathrm{an}} : Y^{\mathrm{an}} \to X^{\mathrm{an}}$ is finite and unramified. For detail, see [3, XII].

Without using terminology of schemes

You don't need to be bothered with "schemes." The scheme we are going to deal with is only the projective line minus three points, defined over $\mathbb{Q}$, denoted by $\mathbb{P}^1_{0,1,\infty_{\mathbb{Q}}}$.

Its definition is

$$\mathbb{P}^1_{0,1,\infty_{\mathbb{Q}}} := \mathrm{Spec}\mathbb{Q}[t, 1/t, 1/(1-t)].$$

Its set of complex points is

$$\begin{aligned}\mathbb{P}^1_{0,1,\infty_{\mathbb{Q}}}(\mathbb{C}) &:= \mathrm{Hom}_{\mathbb{Q}}(\mathrm{Spec}\mathbb{C}, \mathrm{Spec}\mathbb{Q}[t, 1/t, 1/(1-t)]) \\ &= \mathrm{Hom}(\mathbb{Q}[t, 1/t, 1/(1-t)], \mathbb{C}).\end{aligned}$$

By looking at the image of t, the latter set is one to one with

$$\mathbb{C} - \{0, 1\}.$$

This has a natural structure as a complex manifold, which is denoted by ${\mathbb{P}^1_{0,1,\infty}}^{\mathrm{an}}$. What Example 1.10 asserts is that $Y \to \mathbb{P}^1_{0,1,\infty}$ is finite and étale if and only if the corresponding map

$$Y^{\mathrm{an}} \to {\mathbb{P}^1_{0,1,\infty}}^{\mathrm{an}}$$

is finite and unramified, in the classical sense.

1.6 Comparison theorem

Theorem 1.11. Let $K \subset \mathbb{C}$ be an algebraically closed field, and let X be a connected scheme locally of finite type over K. Let x be a $\mathbb{C}$-rational point of X. Then, there is a (canonical) isomorphism

$$\pi_1^{\mathrm{alg}}(X, x) \cong \pi_1(X^{\mathrm{an}}, x)\hat{}.$$

Here, the left hand side is the algebraic fundamental group of X defined in Definition 1.8. (The $^{\mathrm{alg}}$ is to stress that it is algebraic fundamental group; it may be omitted.) The right hand side is the profinite completion of the classical topological fundamental group, see Example 1.6. The above theorem is an immediate consequence of this example and the following

Theorem 1.12. Let $K \subset \mathbb{C}$ be an algebraically closed field, and let X be a connected scheme locally of finite type over K. Then, the analytification functor

$$X_{et} \to \{\text{finite unramified topological coverings of } X^{\mathrm{an}}\}$$

is a category equivalence.

This theorem ([3, XII, Th.5.1]) is called Grothendieck's Riemann Existence Theorem, since it asserts that any finite unramified topological covering of X^{an} is the analytification of an *algebraic* covering of X.

Both categories are Galois categories, and by choosing a fiber functor F_x, the category equivalence implies Theorem 1.11.

2 Algebraic fundamental group as Galois groups

2.1 Rephrase by Galois theory

We may state these definitions in terms of Galois groups. Let X be a geometrically connected *normal* scheme of finite type over $K \subset \mathbb{C}$. It suffices to imagine X to be $\mathbb{P}^1_{0,1,\infty_{\mathbb{Q}}}$ with $K = \mathbb{Q}$. Let $K(X)$ be the function field of X (cf. $K(\mathbb{P}^1_{0,1,\infty_{\mathbb{Q}}}) = \mathbb{Q}(t)$). Let $\overline{X} := X \times \overline{K}$ (cf. $K(\overline{\mathbb{P}^1_{0,1,\infty_{\mathbb{Q}}}}) = \overline{\mathbb{Q}}(t)$). Let M be the maximal algebraic extension of $K(X)$ which is unramified (in the algebraic sense) at every point on X. Then, we have a Galois extension

$$K(X) \subset K(\overline{X}) \subset M$$

and a short exact sequence

$$1 \to G(M/K(\overline{X})) \to G(M/K(X)) \to G(K(\overline{X})/K(X)) \to 1.$$

Let x be a geometric point of X. Now, it is known that there are the following isomorphisms:

$$G(M/K(\overline{X})) \overset{\text{non canon.}}{\cong} \pi_1^{\mathrm{alg}}(\overline{X}, x) = \pi_1(X^{\mathrm{an}}, x)\hat{},$$

$$G(M/K(X)) \overset{\text{non canon.}}{\cong} \pi_1(X, x),$$

$$G(K(\overline{X})/K(X)) \overset{\text{canon.}}{\cong} G(\overline{K}/K) \overset{\text{non canon.}}{\cong} \pi_1^{\mathrm{alg}}(\mathrm{Spec}K, x).$$

Thus, we have a short exact sequence

$$1 \to \pi_1^{\mathrm{alg}}(\overline{X}, x) \to \pi_1^{\mathrm{alg}}(X, x) \to \pi_1^{\mathrm{alg}}(\mathrm{Spec}K, x) \to 1. \tag{2}$$

A proof can be found in Proposition 8.2 in SGA1[3, V, P.143], but see the following remark.

Remark 2.1. In the above, let us consider the functor

$$F_M : X_{et} \to \{\text{finite sets}\}, Y \mapsto \mathrm{Hom}_{K(X)}(K(Y), M).$$

Then this can be proved to be a fiber functor (using that X is normal), and it holds that

$$\mathrm{Aut}F_M = G(M/K(X)),$$

and hence non-canonically

$$\pi_1^{\mathrm{alg}}(X,x) \cong \pi_1(X_{et}, F_M) = G(M/K(X)).$$

Remark 2.2. It is easy to see that π_1^{alg} is a functor

$$\{(X,x) : \text{scheme with one geometric point}\} \to \{\text{profinite groups}\}.$$

If there is a morphism $f : (X,x) \to (Y,y)$, then the pull-back functor

$$f^* : Y_{et} \to X_{et}$$

satisfies $F_y = F_x \circ f^*$, and hence

$$f_* : \pi_1^{\mathrm{alg}}(X,x) := \mathrm{Aut}(F_x) \to \mathrm{Aut}(F_y) =: \pi_1^{\mathrm{alg}}(Y,y).$$

2.2 Analytic continuation

We shall proceed in a different, a more concrete manner (but a little artificial, and restrictions to $\mathbb{C}$). Let K, X be as in the previous section. Let $x \in X$ be a $\mathbb{C}$-rational point of X. Let $\mathcal{M}_x$ be the field of germs of meromorphic functions around x on X^{an}. If $Y \to X$ is a finite etale covering, then $Y^{\mathrm{an}} \to X^{\mathrm{an}}$ is a finite unramified covering. A meromorphic function f_Y on Y^{an} may be regarded as a (finitely) multivalued function on X^{an}. If we fix $y \in Y^{\mathrm{an}}$ in the fiber above $x \in X$, then $f_Y|_y$ gives a germ of meromorphic function around x, which can be analytically continuated to whole X but as a multivalued meromorphic function.

We construct the maximal unramified extension M_x of $K(X)$ in $\mathcal{M}_x$ as follows. Let $\pi_Y : Y \to X$ be a finite etale covering. Then, an element h of $K(Y)$ can be regarded as a meromorphic function on Y^{an}, and by choosing one $y \in \pi_Y^{-1}(x)$, we can regard $h|_y \in \mathcal{M}_x$. Thus, by choosing y, we have an embedding

$$K(Y) \to \mathcal{M}_x.$$

Let M_x be the union of the image of these embeddings, with (Y,y) varying. Then, M_x is a maximal unramified extension of $K(X)$. The analytic continuation of $h|_y$ along $\gamma \in \pi_1(X^{\mathrm{an}}, x)$ gives another function $\gamma(h|_y) \in M_x$, which gives

$$\pi_1(X^{\mathrm{an}}, x) \to G(M_x/K(\overline{X})). \tag{3}$$

This is (in general) not an isomorphism, but Theorem 1.12 says that for any finite index normal subgroup N of the left hand side there is a corresponding finite etale cover $Y \to \overline{X}$ such that

$$\pi_1(X^{\mathrm{an}}, x)/N \cong G(K(Y)/K(\overline{X})).$$

By passing to the projective limit we have

$$\pi_1(X^{\mathrm{an}}, x)\widehat{\ } \cong G(M_x/K(\overline{X})) = \pi_1^{\mathrm{alg}}(\overline{X}, x).$$

To justify the canonical isomorphism

$$\pi_1^{\mathrm{alg}}(X, x) \cong G(M_x/K(X)) \tag{4}$$

we need to show that

1. The functor
$$F'_x : Y \mapsto \mathrm{Hom}_{K(X)}(K(Y), M_x)$$
is a fiber functor canonically isomorphic to F_x, with the correspondence
$$y \in F_x(Y) \mapsto (h \mapsto h|_y). \tag{5}$$

2. $\mathrm{Aut}F'_x = G(M_x/K(X))$.

It is immediate that

$$\pi_1(X^{\mathrm{an}}, x) \to \pi_1(\overline{X}, x) = \mathrm{Aut}F_x \cong \mathrm{Aut}F'_x = G(M/K(X))$$

is given by the analytic continuation.

We leave it to the readers to show $G(K(\overline{X})/K(X)) = G(\overline{K}/K)$.

3 Galois representation on fundamental groups, as monodromy

The short exact sequence (2) is considered to be an analogue to the fiber-exact sequence of homotopy groups. That is, $X \to \mathrm{Spec}K$ is a family, and $\overline{X}$ is a fiber above $\mathrm{Spec}\overline{K} \to \mathrm{Spec}K$.

In topology, there is a notion of geometric monodromy on the fundamental group. Let $F \to B$ be a locally trivial fibration, $b \in B$ be a point, and $x \in F$ a point over b. Then, there is an exact sequence

$$\pi_1(F_b, x) \to \pi_1(F, x) \to \pi_1(B, b) \to 1. \tag{6}$$

Suppose that the left most morphism is injective, so that this is a short exact sequence by supplying $1 \to$ at the left hand side. (This occurs if $\pi_2(B) = 1$ or $\pi_1(F_b, x)$ is center free.)

For an element $\gamma \in \pi_1(B, b)$, we can consider the deformation of the fiber F_b along γ. Then, it induces an automorphism of F_b, hence of $\pi_1(F_b, x)$, but the base point $x \in F_b$ may move along the deformation. This action is well-defined upto the move of the base point, giving the *outer monodromy representation on π_1 of the fiber*:

$$\rho : \pi_1(B, b) \to \mathrm{Aut}(\pi_1(F_b, x))/\mathrm{Inn}(\pi_1(F_b, x)) =: \mathrm{Out}(\pi_1(F_b, x)). \tag{7}$$

This can be stated purely group theoretically: take $\gamma \in \pi_1(B, b)$. Let it act on $\alpha \in \pi_1(F_b, x)$ as follows:

$$\rho(\gamma)(\alpha) := \tilde{\gamma} \circ \alpha \circ \tilde{\gamma}^{-1},$$

where $\tilde{\gamma}$ is a lift of γ in $\pi_1(F, x)$, and α is considered to be an element of $\pi_1(F, x)$ by inclusion. The right hand side depends on the lift $\tilde{\gamma}$, but any other lift is of the form of $\beta\tilde{\gamma}$ for some $\beta \in \pi_1(F_b, x)$. Thus, $\rho(\gamma)$ is well-defined after taking modulo the inner automorphism of $\pi_1(F_b, x)$. This gives the outer monodromy (7).

If we have a section $s : B \to F$ to $F \to B$, then we have a canonical choice of $x := s(b)$ and $\tilde{\gamma} :=$ the image in $\pi_1(B, b) \to \pi_1(F, x)$. Thus we have a section to the short exact sequence (6), and hence (non-outer) monodromy representation

$$\rho : \pi_1(B, b) \to \mathrm{Aut}(\pi_1(F_b, x)).$$

Because of the existence of the algebraic analogue (2) of the short exact sequence (6), we have *the outer Galois representation* on π_1^{alg}:

$$\rho_X : G_K = \pi_1^{\mathrm{alg}}(\mathrm{Spec} K) \to \mathrm{Out}(\pi_1^{\mathrm{alg}}(\overline{X}, x)) \tag{8}$$

and if x is over a K-rational point $x : \mathrm{Spec}\mathbb{C} \to \mathrm{Spec} K \to X$, then we have a section to (2) and have the *Galois representation on* π_1^{alg}:

$$\rho_{X,x} : G_K \to \mathrm{Aut}(\pi_1^{\mathrm{alg}}(\overline{X}, x)). \tag{9}$$

An interesting observation is that G_K is a mysterious group arizing from the number theory: it is even difficult to describe any element except for the complex conjugation, while $\mathrm{Aut}(\pi_1^{\mathrm{alg}}(\overline{X}, x))$ is rather a combinatorial group: in the case of $\mathbb{P}^1_{0,1,\infty}$, it is $\mathrm{Aut}(\widehat{F_2})$ where F_2 denotes the free group with two generators.

Such two different groups are closely intertwinned: Belyi [1] proved that $\rho_{\mathbb{P}^1_{0,1,\infty}}$ is *injective* for $K = \mathbb{Q}$. This implies the possibility that use of combinatorial group theory on $\widehat{F_2}$ may yield some interesting structure on $G_{\mathbb{Q}}$. We shall treat such examples in the following sections.

4 Computation of Galois actions

4.1 Taking a section

As explained in §2, we have a short exact sequence (2)

$$1 \to \pi_1^{\mathrm{alg}}(\overline{X}, x) \to \pi_1^{\mathrm{alg}}(X, x) \to \pi_1^{\mathrm{alg}}(\mathrm{Spec}K, x) \to 1,$$

which is canonically isomorphic to

$$1 \to G(M_x/\overline{K}(X)) \to G(M_x/K(X)) \to G(\overline{K}(X)/K(X)) \to 1. \tag{10}$$

If x is on a K-rational point, we have a section

$$s_{x*} : G_K = \pi_1^{\mathrm{alg}}(\mathrm{Spec}K, x) \to \pi_1^{\mathrm{alg}}(X, x),$$

and the monodromy representation

$$\rho_{X,x} : G_K \to \mathrm{Aut}(\pi_1^{\mathrm{alg}}(\overline{X}, x)),$$

where

$$\rho_{X,x}(\sigma)(\gamma) = s_{x*}(\sigma)\gamma s_{x*}(\sigma)^{-1}$$

for $\sigma \in G_K$ and $\gamma \in \pi_1^{\mathrm{alg}}(\overline{X}, x)$. So we need to know what is $s_{x*}(\sigma) \in G(M_x/K(X))$. For this, we need to return to the definition of the algebraic fundamental group by fiber functors. For the K rational point $x' : \mathrm{Spec}K \to X$, we have functors

$$G : X_{et} \to (\mathrm{Spec}K)_{et}, \quad Y \mapsto Y \times_X x',$$

and

$$H : (\mathrm{Spec}K)_{et} \to \{\text{finite sets}\}, \quad \mathrm{Spec}R \mapsto \mathrm{Hom}_K(\mathrm{Spec}\overline{K}, \mathrm{Spec}R),$$

satisfying

$$F_x = H \circ G.$$

The section s_{x*} is by definition

$$G_K \cong \mathrm{Aut}H \to \mathrm{Aut}(H \circ G) = \mathrm{Aut}F_x.$$

The identification given in (4)

$$\pi_1(X,x) = \mathrm{Aut}F_x \cong \mathrm{Aut}F'_x = G(M_x/K(X))$$

is through (5), which we need to make precise. Let $\mathcal{O}_{X,x} \subset K(X)$ be the meromorphic functions on X with no pole at x, and let M_x^{fin} be the integral closure of $\mathcal{O}_{X,x}$ in M_x. If $g \in K(Y)$ is embedded in M_x^{fin} by $g \mapsto g|_y$, then g_y has no pole at x, and $g_y(x) \in \overline{K}$.

The identification of two fiber functors is given through

$$\begin{array}{rcl} \mathrm{Hom}_{K(X)}(K(Y), M_x) & \cong & \mathrm{Hom}_{\mathcal{O}_{X,x}}(\mathcal{O}_{Y,x}, M_x^{fin}) \\ & \cong & \mathrm{Hom}_{\mathcal{O}_{X,x}}(\mathcal{O}_{Y,x}, \overline{K}) \cong \mathrm{Hom}_x(\mathrm{Spec}\overline{K}, Y), \end{array}$$

where $\mathcal{O}_{Y,x}$ is the integral closure of $\mathcal{O}_{X,x}$ in $K(Y)$. Take an element $\alpha : K(Y) \to M_x$. The corresponding point of Y is given by

$$\mathcal{O}_{Y,x} \to \overline{K}, h \mapsto \alpha(h)(x) \in \overline{K}.$$

An element $\sigma \in G_K$ acts on this point by

$$\sigma(\alpha) : h \mapsto \sigma(\alpha(h)(x)).$$

The corresponding element in $\mathrm{Hom}_{K(X)}(K(Y), M_x)$, which should be denoted $\sigma(\alpha)$, is $h \mapsto h'$ where h' is a unique conjugate of h with $\alpha(h')(x) = \sigma(\alpha(h)(x))$.

Thus, for $g \in M_x^{fin}$, $\sigma(g)$ is defined as the unique conjugate g' of g over $K(X)$ with $g'(x) = \sigma(g(x))$. This gives

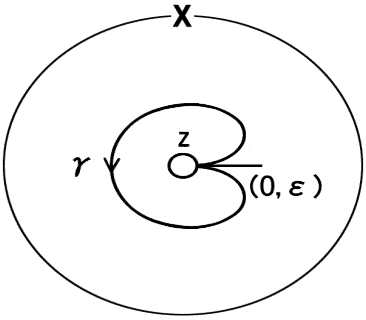
$$s_{x*} : G_K \to G(M_x/K(X)).$$

One way to compute s_{x*} is by Taylor expansion. For this, choose a set of local coordinate $t_1, \ldots, t_n \in m_{X,x}$. Then, any $g \in M_x^{fin}$ can be expanded as a convergent power series with coefficients in $\overline{K}$. Let σ acts on the coefficents of g, then we get a conjugate $\sigma(g)$ of g over $K(X)$. Because g is a meromorphic function on Y, $\sigma(g)$ is a meromorphic function on Y^σ, and since $\sigma(x) = x$ we have $\sigma(g) \in M_x$. This gives the G_K action on M_x, and hence the section s_{x*}.

Tangential base point and Puiseux series

There is a notion of tangential base point. For simplicity, assume that X is a curve, and $X := X' - \{z\}$ where z is a K-rational point of X'. Choose a local coordinate function $t \in K(X)$, i.e., z is the zero of t with multplicity one.

Choosing t is regarded as choosing a tangent vector at z. Consider t as a meromorphic function on $X^{\rm an}$. Then, the tangent vector is the one given by an infinitesimal move of t from zero to positive real number ϵ. We denote by $(0,\epsilon)$ the open line segment on X starting from $t=0$ and ending at $t=\epsilon$. This inifinitesimally small line is called a tangential base point, which we donote by $\vec{t}$.



We define $\mathcal{M}_{\vec{t}}$ as the germ of meromorphic functions around this infinitesimally small vector, i.e., meromorphic functions defined at an open neibourhood of some $(0,\epsilon)$. Let $M_{\vec{t}}$ be the maximal unramified extension of $K(X)$ in $\mathcal{M}_{\vec{t}}$. (It coincides with those finitely multivalued meromorphic functions on whole X, algebraic over $K(X)$.)

Similarly to the previous case, we have by analytic continuation

$$\pi_1(X^{\rm an}, (0,\epsilon)) \to G(M_{\vec{t}}/\overline{K}(X))$$

and thus we define

$$\pi_1(\overline{X}, \vec{t}) := G(M_{\vec{t}}/\overline{K}(X)) \cong \pi_1(X^{\rm an}, (0,\epsilon))\widehat{\ },$$

and

$$\pi_1(X, \vec{t}) := G(M_{\vec{t}}/K(X)).$$

Then, we define the section

$$s_{\vec{t}*} : G(\overline{K}/K) \to \pi_1(X, \vec{t}) := G(M_{\vec{t}}/K(X))$$

as follows. Take an $f \in M_{\vec{t}}$. Since f is finitely multivalued, for some $N \in \mathbb{N}$ $\gamma^N(f) = f$ holds for the path γ circling z counter clockwise. Let $t^{1/N}$ denotes the function in $\mathcal{M}_{\vec{t}}$, whose N-th power is t and takes positive real values on $(0, \epsilon)$. Then, $f((t^{1/N})^N)$ is a monovalued function with variable $t^{1/N}$, around z. This implies that there is a unique expansion

$$f((t^{1/N})^N) = \sum_{i=-m}^{\infty} a_i(t^{i/N}).$$

Let $G(\overline{K}/K)$ act on the coefficients a_i:

$$s_{\vec{t}}(\sigma)(f) = \sum_{i=-m}^{\infty} \sigma(a_i)(t^{i/N}).$$

This gives

$$s_{\vec{t}*} : G(\overline{K}/K) \to \pi_1(X, \vec{t}).$$

Note that this section depends on the choice of t: for example, $\vec{t}$ and $\vec{2t}$ are different.

To justify this computation, we need to define a functor

$$\vec{t} : X_{et} \to (\mathrm{Spec} K)_{et}.$$

I don't know a good reference for this. A concrete description is given in [5].

Cyclotomic character

Here we explain one of the merits of tangential base points. Let $\gamma \in \pi_1(X, \vec{t})$ as above. We shall compute explicitly the Galois action

$$\rho_{X,\vec{t}}(\sigma)(\gamma)$$

for $\sigma \in G(\overline{K}/K)$, in the sense of (9). Since

$$\rho_{X,\vec{t}}(\sigma)(\gamma) = s_{\vec{t}}(\sigma)(\gamma)s_{\vec{t}}(\sigma)^{-1},$$

it suffices to let it act on $f \in M_{\vec{t}}$. We see that

$$f = \sum a_i t^{i/N} \overset{\gamma}{\mapsto} \gamma(f) = \sum a_i \zeta_N^i t^{i/N},$$

where $\zeta_N = \exp(1\pi i/N)$ is one of the roots of unity. Now $\rho_{X,\vec{t}}(\sigma)(\gamma)$ maps

$$f = \sum a_i t^{i/N} \overset{\sigma^{-1}}{\mapsto} \sum \sigma^{-1}(a_i) t^{i/N} \overset{\gamma}{\mapsto} \sum \sigma^{-1}(a_i)\zeta_N^i t^{i/N} \overset{\sigma}{\mapsto} \sum (a_i)\sigma(\zeta_N^i) t^{i/N}.$$

Thus, the action of σ on γ is determined by the action on ζ_N.

Since the conjugates of ζ_N over K are (some of) $\zeta_N^{m_N}$, $m_N \in (\mathbb{Z}/N)^\times$, we have

$$\sigma(\zeta_N) = \zeta_N^{\chi_N(\sigma)}$$

for some $\chi_N(\sigma) \in (\mathbb{Z}/N)^\times$. Thus, we have

$$\chi : G(\overline{K}/K) \mapsto \hat{\mathbb{Z}}^\times = \lim_{\leftarrow}(\mathbb{Z}/N)^\times, \quad \sigma \mapsto (\chi_N(\sigma))(N \in \mathbb{N}).$$

The χ is called the cyclotomic character. It is a surjection if $K = \mathbb{Q}$, which is equivalent to the irreducibility of cyclotomic polynomials.

Now we can write

$$\rho_{X,\vec{t}}(\sigma)(\gamma) = \gamma^{\chi(\sigma)} \tag{11}$$

The meaning of the right hand side is as follows. Let $G = \lim_{\leftarrow} G_\lambda$ be a profinite group. Then, for any $\gamma = (\gamma_\lambda) \in G$ and $\hat{n} \in \hat{\mathbb{Z}}$, we can define $\gamma^{\hat{n}}$ as a system of $(\gamma_\lambda^{n_\lambda})$, where n_λ is the image of $\hat{n}$ in $\mathbb{Z}/N_\lambda$ with N_λ being the order of γ_λ.

It is left to the readers to verify the equality (11). It suffices to let the both sides act on various f.

4.2 Case of $\mathbb{P}^1_{0,1,\infty}$

We consider the case where $X = \mathbb{P}^1_{0,1,\infty}$, and t is the standard coordinate of $\mathbb{P}^1_{0,1,\infty}$. We denote

$$\vec{01} := \vec{t}.$$

So far we have used the letter x for the base point, but from now on we use x, y, z to denote the elements in $\pi_1({\mathbb{P}^1_{0,1,\infty}}^{\mathrm{an}}, \vec{01})$ with x being a path circling 0 counter-clockwise, y being a path going from $\vec{01}$ to 1, circling 1 counter-clockwise, then return to $\vec{01}$. We put $z = (yx)^{-1}$, so that $zyx = 1$ holds.

We have

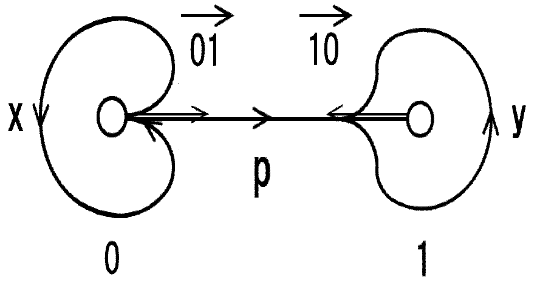
$$\rho_{\vec{01}} : G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\pi_1(\overline{\mathbb{P}^1_{0,1,\infty}}, \vec{01})) = \mathrm{Aut}(\widehat{F_2}),$$

and as seen in the previous section we have

$$\rho_{\vec{01}}(\sigma)(x) = x^{\chi(\sigma)}.$$

Since $\widehat{F_2}$ is generated by x, y, it suffices to compute

$$\rho_{\vec{01}}(\sigma)(y),$$



but this is very difficult. One can show that

$$\rho_{\vec{01}}(\sigma)(y) = f_\sigma(x,y)^{-1} y^{\chi}(\sigma) f_\sigma(x,y)$$

for a (unique) element in the commutator subgroup of $\widehat{F_2}$, $f_\sigma(x,y) \in [\widehat{F_2}, \widehat{F_2}]$.

This can be proved rather group theoretically, but in a more intrinsic way in terms of groupoids.

Let X^{an} be a connected topological space, and let x, x' be two points. Then we define

$$\pi_1(X^{\mathrm{an}}; x, x') := \{\text{paths from } x \text{ to } x'\}/\text{homotopy}.$$

Such system is called a groupoid: a groupoid is a category, where every objects are isomorphic and every arrows are invertible.

In the Galois category C, for two fiber functors $F_x, F_{x'}$, we define

$$\pi_1(X; F_x, F'_x) := \mathrm{Isom}(F_x, F'_x).$$

In the example of $\mathbb{P}^1_{0,1,\infty}$, let $\vec{10}$ be another tangential basepoint specified by $1 - t$.

Then, the corresponding fiber functor $F_{\vec{10}}$ is

$$Y \mapsto \mathrm{Hom}_{K(X)}(K(Y), M_{\vec{10}}),$$

where $M_{\vec{10}}$ is the germ of meromorphic functions around $(1-\epsilon, 1)$ similarly to $\vec{01}$. Then we have

$$\pi_1(X; \vec{01}, \vec{10}) := \mathrm{Isom}_X(F_{\vec{01}}, F_{\vec{10}}) \cong \mathrm{Isom}_{K(X)}(M_{\vec{01}}, M_{\vec{10}}).$$

By analytic continuation, we have

$$\pi_1(X^{\mathrm{an}}; \vec{01}, \vec{10}) \to \mathrm{Isom}_{K(\overline{X})}(M_{\vec{01}}, M_{\vec{10}}),$$

which becomes an isomorphism after taking the profinite completion of the left hand side. The right hand side is denoted by $\pi_1(X; \vec{01}, \vec{10})$.

Now, there is a unique path p from $\vec{01}$ to $\vec{10}$ on the real $(0,1)$ interval. We identify it with the mapping

$$p \in \mathrm{Isom}_{K(\overline{X})}(M_{\vec{01}}, M_{\vec{10}}) = \pi_1(X; \vec{01}, \vec{10}).$$

Now, there are two sections

$$s_{\vec{01}} : G(\overline{K}/K) \to \mathrm{Aut}(M_{\vec{10}}), \quad s_{\vec{10}} : G(\overline{K}/K) \to \mathrm{Aut}(M_{\vec{01}}).$$

We define the action of $\sigma \in G(\overline{K}/K)$ on p by

$$\sigma(p) = s_{\vec{10}}(\sigma) \circ p \circ s_{\vec{01}}(\sigma)^{-1} \in \pi_1(X; \vec{01}, \vec{10}).$$

Now, we put

$$f_\sigma(x, y) := p^{-1} \circ \sigma(p) \in \pi_1(\overline{X}, \vec{01}).$$

Let γ_{10} be the path circling 1, starting from and ending at $(1, 1-\epsilon)$. Then since $y = p^{-1} \circ \gamma_{10} \circ p$, we have

$$\rho_{\vec{01}}(\sigma)(y) = (s_{\vec{01}}(\sigma) p^{-1} s_{\vec{10}}(\sigma)^{-1})(s_{\vec{10}}(\sigma)\gamma_{10} s_{\vec{10}}(\sigma)^{-1})(s_{\vec{10}}(\sigma) p s_{\vec{01}}(\sigma)^{-1}).$$

By

$$s_{\vec{10}}(\sigma) p s_{\vec{01}}(\sigma)^{-1} = p f_\sigma(x, y)$$

and the symmetry

$$s_{\vec{10}}(\sigma)\gamma_{10} s_{\vec{10}}(\sigma)^{-1} = \gamma_{10}^{\chi}(\sigma),$$

we obtain

$$\rho_{\vec{01}}(\sigma)(y) = f_\sigma(x, y)^{-1} y^{\chi(\sigma)} f_\sigma(x, y).$$

To show $f_\sigma(x, y) \in [\widehat{F_2}, \widehat{F_2}]$, it is enough to show that $f_\sigma(x, y)$ trivially acts on $t^{1/N}$ and $(1-t)^{1/N}$, since

$$\widehat{F_2}/[\widehat{F_2}, \widehat{F_2}] \cong G(M_{\vec{01}}/K(\overline{X}))^{ab} = G(\overline{\mathbb{Q}}(t^{1/N}, (1-t)^{1/N} | N \in \mathbb{N})/\overline{\mathbb{Q}}(t)).$$

This is easy:

$$p : t^{1/N} \in M_{\vec{01}} \mapsto (1 - (1-t))^{1/N} \in M_{\vec{10}},$$

where the right hand side is expanded with respect to $(1-t)$. The key is that the coefficients in the expansion are all in $\mathbb{Q}$, and hence $G_{\mathbb{Q}}$ acts trivially. Thus, $s_{\vec{10}}(\sigma) p s_{\vec{01}}(\sigma)^{-1}$ acts in the same way with p on $t^{1/N}$. Similar conclusion can be deduced for $(1-t)^{1/N}$, so $f_\sigma(x, y) = p^{-1}\sigma p \sigma^{-1}$ trivially acts on $t^{1/N}, (1-t)^{1/N}$.

5 Lie algebraization

Nonabelian groups such as the free profinite groups $\widehat{F_2}$ are hard to deal with. So, we try to approximate such groups by "linear algebra." For a Lie group, its linearization is its Lie algebra. There is a similar notion for arbitrary groups, which is called Malcev completion. Roughly saying, we embed a group G in a suitably completed ring $K[G]\hat{}$, and then take $\log(g)$ for $g \in G$ to obtain a Lie algebra.

5.1 Group rings (discrete case)

Let K be a field of characteristic zero (mostly $K = \mathbb{Q}$ or $\mathbb{Q}_\ell$, where l is a fixed prime). We consider the group ring $K[G]$, namely, the set of (finite) linear combination of elements of G over K. There is an augumentation map

$$\epsilon : K[G] \to K$$

obtained by summing the coefficients. Its kernel is called the augumentation ideal

$$I := \mathrm{Ker}(\epsilon) = \text{the ideal generated by } g-1,\ g \in G.$$

We consider

$$K[G]\hat{} := \lim_{\leftarrow, n} K[G]/I^n.$$

The closure of the image of I in $K[G]\hat{}$ is denoted by $I\hat{}$. By taking $I\hat{}^n$ as a neighborhood of 0, $K[G]\hat{}$ is a topological ring.

Let us define the so-called coproduct

$$\Delta : K[G] \to K[G] \otimes_K K[G], \quad g \mapsto g \otimes g$$

by the linear extension, and then extend it continuously to

$$\Delta : K[G]\hat{} \to K[G]\hat{}\hat{\otimes}_K K[G]\hat{}.$$

We define the set of group-like elements

$$\mathcal{G} := \{x \in K[G]\hat{} | \Delta(x) = x \otimes x, x \equiv 1 \bmod I\hat{}\}.$$

It cotains the image of G in $K[G]\hat{}$, and is called the Malcev completion of G over K.

There is the logarithm map

$$\log : (1+I) \to I, \quad 1+u \mapsto \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} u^n$$

and the exponential map

$$\exp : I \to (1+I), \quad u \mapsto \sum_{n=0}^{\infty} \frac{1}{n!} u^n,$$

which are mutually inverse. Then, the image of the group-like elements by the logaritmic map satisfies

$$\mathcal{L} := \log(\mathcal{G}) = \{x \in I | \Delta(x) = 1 \otimes x + x \otimes 1, \}$$

which are called the Lie-like elements. (These follow from the theory of Hopf algebras.)

It is not difficult to show that $\mathcal{G}$ is a group (by the product of the group algebra) and $\mathcal{L}$ is a Lie algebra (by the commutator product $[X, Y] := XY - YX$). They have natural filterations

$$I^n(\mathcal{G}) = \mathcal{G} \cap (1 + I^n), \quad I^n(\mathcal{L}) = \mathcal{L} \cap I^n$$

preserved by $\log, \exp$.

This construction is functorial. In particular, an automorphism of G induces an automorphism of $\mathcal{G}$ as group and an automorphism of $\mathcal{L}$ as a Lie algebra.

The functor $G \mapsto \mathcal{G}$ may lose a lot of information, depending on G. However, if G is a free group F_n with generators $x_1, \dots, x_n$, then

$$K[F_n]\hat{} \cong K << u_1, u_2, \dots, u_n >>$$

(non-commutative associative formal power series ring, where $u_i = \log(x_i)$) and

$$\mathcal{L} \cong \text{completed free Lie algebra with generators } u_i.$$

5.2 Group rings (pro-ℓ case)

Let ℓ be a fixed prime number. A finite group is an ℓ group if its order is a power of ℓ, and a pro-ℓ group is a profinite group that is a projective limit of ℓ-groups. Pro-ℓ completion of a discrete group G is defined by

$$G^{(\ell)} := \lim_{\leftarrow} G/N,$$

where N runs over normal subgroups with finite index of an ℓ-power. There is a surjective homomorphism

$$G\hat{} \to G^{(\ell)},$$

which is functorial. Hence, we have a pro-ℓ version of (9):

$$\rho^{(\ell)}_{X,x} : G_K \to \mathrm{Aut}(\pi_1^{(\ell)}(\overline{X}, x)).$$

Let G be a pro-ℓ group. A good pro-ℓ analogue of $K[G]\hat{}$ in the previous section is the completed group algebra

$$\mathbb{Z}_\ell[[G]] := \lim_{\leftarrow} \mathbb{Z}_\ell[G/N],$$

where N runs over open normal (hence index being ℓ power) subgroups.

We have the augumentation

$$\epsilon : \mathbb{Z}_\ell[[G]] \to \mathbb{Z}_\ell,$$

and if $G = F_n^{(\ell)}$ then

$$\mathbb{Z}_\ell << \xi_1, \dots, \xi_n >> \cong \mathbb{Z}_\ell[[G]]$$

where $\xi_i \mapsto x_i - 1$.

We can define $\mathbb{Q}_\ell[[G]]$ and Δ in the same way, and we have continuous Malcev completion of G and its Lie algebra

$$G \to \mathcal{G} \subset \mathbb{Q}_\ell[[G]]^\times, \quad \mathcal{L} \subset \mathbb{Q}_\ell[[G]].$$

If G is free pro-ℓ group of rank n, then $\mathcal{L}$ is a completed free Lie algebra with n generators.

5.3 Lie Algebraization of Galois representation

Apply the above to the pro-ℓ completion $F_2^{(\ell)}$ of $\hat{F_2} = \pi_1(\overline{\mathbb{P}^1_{0,1,\infty}}, \vec{01})$. Then we have

$$\rho : G_\mathbb{Q} \to \mathrm{Aut}\mathbb{Q}_\ell << \xi, \eta >> \to \mathrm{Aut}\mathcal{L}$$

where $x, y \in \widehat{F_2}$ are mapped to $\exp(\xi)$, $\exp(\eta)$ in $\mathbb{Q}_\ell << \xi, \eta >>$, and $\mathcal{L}$ is the free Lie algebra of two generators ξ, η.

6 Soulé's cocycle

Let G be a group, K a field, and

$$0 \to A \to E \to K \to 0$$

be a short exact sequence of K-vector spaces with G-actions (the right K has trivial G-action). To this short exact sequence, we have a corresponding cohomology class

$$[E] \in H^1(G, A),$$

as follows. Let take an arbitrary section as K-vector space, i.e., an element $e \in E$ which is mapped to $1 \in K$, then define the function

$$f : G \to A, \quad \sigma \mapsto f(\sigma) = \sigma(e) - e.$$

This satisfies the cocycle condition

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau),$$

and hence defines a class $[E]$ in $H^1(G, A)$. The ambiguity of the choice of e is absorbed in coboundary.

There is a topological version of this: if G is a topological group, K a topological field and G-actions are continuous, then we consider the continuous cocycles to define $H^1(G, A)$.

Let $G_\ell := G(\mathbb{Q}^{ur,\ell}/\mathbb{Q})$ be the Galois group of the maximal extension $\mathbb{Q}^{ur,\ell}$ of $\mathbb{Q}$ unramified outside the prime ℓ. It is proved by Ihara [4] (but it also follows from the smooth and proper base change theorem in [3]) that the pro-ℓ representation obtained from $\mathbb{P}^1_{0,1,\infty}$

$$\rho^{(\ell)} : G_\mathbb{Q} \to \mathrm{Aut} F_2^{(\ell)}$$

is unramified outside ℓ, so $F_2^{(\ell)}$ is a G_ℓ-module. The ℓ-part of the cyclotomic character χ:

$$\chi_\ell : G_\mathbb{Q} \to \hat{\mathbb{Z}}^\times \to {\mathbb{Z}_\ell}^\times$$

factors through G_ℓ. This is called the ℓ-adic cyclotomic character $\chi_\ell : G_\ell \to {\mathbb{Z}_\ell}^\times$.

Soulé [7] proved that

$$H^1(G_\ell, \mathbb{Z}_\ell(m)) \cong \mathbb{Z}_\ell(\text{ if } m > 0 \text{ is odd}), \cong 0(\text{ if } m > 0 \text{ is even}).$$

Here, $\mathbb{Z}_\ell(m)$ is so-called Tate twist: it is isomorphic to $\mathbb{Z}_\ell$ as an abelian group, but $\sigma \in G_\ell$ acts by multiplication by the m-th power of ℓ-adic cyclotomic character, $\chi_\ell(\sigma)^m$.

Soulé gave a concrete construction of a cocycle

$$\chi_m : G_\mathbb{Q} \to \mathbb{Z}_\ell(m)$$

for every odd m, which we omit here. Anyway, this implies that there exists a nontrivial extension

$$0 \to \mathbb{Z}_\ell(m) \to E_m \to \mathbb{Z}_\ell \to 0,$$

and any other such extension is obtained by multiplying an elment of $\mathbb{Z}_\ell$.

Returning to the Galois representation, we have an extension of G_ℓ-modules

$$0 \to \mathcal{L}'/[\mathcal{L}', \mathcal{L}'] \to \mathcal{L}/[\mathcal{L}', \mathcal{L}'] \to \mathcal{L}/[\mathcal{L}, \mathcal{L}] \to 0, \tag{12}$$

where $\mathcal{L}$ is completed free Lie algebra with two generators ξ, η and $\mathcal{L}'$ is its commutator. By a direct computation, we have

$$\mathcal{L}/[\mathcal{L}, \mathcal{L}] = \mathbb{Q}_\ell\bar{\xi} \oplus \mathbb{Q}_\ell\bar{\eta} \cong \mathbb{Q}_\ell(1) \oplus \mathbb{Q}_\ell(1),$$

and

$$\mathcal{L}'/[\mathcal{L}', \mathcal{L}'] = \mathbb{Q}_\ell[\xi, \eta] \oplus \mathbb{Q}_\ell[\xi, [\xi, \eta]] \oplus \mathbb{Q}_\ell[\eta, [\xi, \eta]] \oplus \cdots, \cong \mathbb{Q}_\ell[[\xi, \eta]] \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell(2),$$

where $\mathbb{Q}_\ell(2)$ is the module generated by $[\xi, \eta]$ and $\mathbb{Q}_\ell[[\xi, \eta]] \cong \bigoplus_n \mathbb{Q}_\ell(n)^{n+1}$. Now (12) is an extension of the form

$$0 \to (\bigoplus_n \mathbb{Q}_\ell(n)^{n+1}) \otimes \mathbb{Q}_\ell(2) \to E \to \mathbb{Q}_\ell(1) \oplus \mathbb{Q}_\ell(1) \to 0,$$

but we have a sub G_ℓ-module $\mathbb{Q}_\ell\xi \in E$ which we can be divided out. Then we have

$$0 \to (\bigoplus_n \mathbb{Q}_\ell(n)^{n+1}) \otimes \mathbb{Q}_\ell(2) \to E/(\mathbb{Q}_\ell\xi) \to \mathbb{Q}_\ell(1) \to 0$$

where the right $\mathbb{Q}_\ell(1)$ is spanned by $\bar{\eta}$. By tensoring $\mathbb{Q}_\ell(-1)$, we have an extension

$$0 \to (\bigoplus_n \mathbb{Q}_\ell(n)^{n+1}) \otimes \mathbb{Q}_\ell(1) \to E/(\mathbb{Q}_\ell\xi)(-1) \to \mathbb{Q}_\ell(0) \to 0, \tag{13}$$

hence a cohomology class

$$\Pi \in H^1(G_\ell, \bigoplus_n \mathbb{Q}_\ell(n+1)^{n+1}) \cong \bigoplus_n H^1(G_\ell, \mathbb{Q}_\ell(n+1))^{n+1}.$$

Here, the right $\mathbb{Q}_\ell(0)$ in (13) is spanned by

$$\bar{\eta} \otimes 1_{(-1)} \in \mathcal{L}/\mathcal{L}' \otimes \mathbb{Q}_\ell(-1),$$

where $1_{(-1)}$ denotes the 1 in $\mathbb{Q}_\ell(-1)$.

Anderson, Coleman, and Ihara proved that this cohomology class is a nonzero constant multiple of Soulé's cocycle χ_{n+1} for $n \geq 2$ is even, which means that the pro-ℓ fundamental group $F_2^{(\ell)}$ has a rich structure as a G_ℓ-module.

More precise statement is as follows. For $\sigma \in G_{\mathbb{Q}}$, the Galois action on $F_2^{(\ell)}$ is given by

$$x \mapsto x^{\chi_\ell(\sigma)}, \quad y \mapsto f_\sigma^{-1} y^{\chi_\ell(\sigma)} f_\sigma,$$

as in the previous sections (here f_σ denotes its image in $F_2^{(\ell)}$, by abuse of the notation: it should have been written as $f_\sigma^{(\ell)}$). By taking log, the action of σ on the Lie algebra $\mathcal{L}$ is given by

$$\xi = \log x \mapsto \chi_\ell(\sigma)\xi, \quad \eta \mapsto \chi_\ell(\sigma) f_\sigma^{-1} \eta f_\sigma.$$

If we denote

$$F_\sigma := -\log(f_\sigma),$$

then by Baker-Campel-Hausdorff formula we have

$$\begin{aligned} f_\sigma^{-1}\eta f_\sigma &= \eta + [F_\sigma, \eta] + 1/2[F_\sigma, [F_\sigma, \eta]] + \cdots \\ &= \exp(ad(F_\sigma))(\eta). \end{aligned}$$

Now, the cocycle corresponding to the section $\bar{\eta} \otimes 1_{(-1)} \mapsto \eta \otimes 1_{(-1)}$ in (13) is $\sigma(\eta \otimes 1_{(-1)}) - \eta \otimes 1_{(-1)}$. In this extension, we took modulo $[\mathcal{L}', \mathcal{L}']$, so $[F_\sigma, [F_\sigma, \eta]]$ etc. is neglected.

Thus, the corresponding cocycle Π to (13) is given by

$$\sigma \mapsto [F_\sigma, \eta] \otimes 1_{(-1)} \equiv \sum_n \sum_{i+j=n+1} c_{i,j}(\sigma) ad(\xi)^i ad(\eta)^j [\xi, \eta] \otimes 1_{(-1)} \bmod [\mathcal{L}', \mathcal{L}'] \otimes 1_{(-1)},$$

where $c_{i,j}$ is a cocycle whose class consequently lies in

$$[c_{i,j}(\sigma)] \in H^1(G_\ell, \mathbb{Q}_\ell(i+j)).$$

Anderson, Coleman and Ihara proved that

$$c_{i,j}(\sigma) = \frac{1}{(i!j!)(\ell^{i+j-1} - 1)} \chi_{i+j}(\sigma),$$

where χ_{i+j} is Soulé's cocycle.

The original proofs by Anderson, Coleman, or Ihara are not so straight forward. However, at least for $c_{i,0}(\sigma)$, Nakamura and Wojtkowiak [6] gave a direct computational proof of the above formula.

Open questions

A moderate open question: is it possible to obtain $c_{i,j}(\sigma)$ for $j \neq 0$, in terms of a direct computation?

A little more ambitious: is it possible to obtain some formulae for other coefficients of F_σ not taking modulo $[\mathcal{L}', \mathcal{L}']$?

References

[1] G.V. Belyĭ, *On Galois extensions of a maximal cyclotomic field*, Math. USSR Izv. **14** (1980), 247–256.

[2] "Algebraic Number Theory," J.W.S. Cassels and A. Frohlich Ed., Academic Press 1967

[3] A. Grothendieck and Mme M. Raynaud, "Revêtement Etales et Groupe Fondamental (SGA 1)", Lecture Notes in Math. **224**, Springer-Verlag, 1971.

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

[5] M. Matsumoto, *Galois group G_Q, singularity E_7, and moduli $\mathcal{M}_3$*. Geometric Galois actions, 2, 179–218, London Math. Soc. Lecture Note Ser., 243, Cambridge Univ. Press, Cambridge, 1997.

[6] H. Nakamura and Z. Wojtkowiak, *On explicit formulae for l-adic polylogarithms.* Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), 285–294, Proc. Sympos. Pure Math., 70, Amer. Math. Soc., Providence, RI, 2002.

[7] C. Soulé, *On higher p-adic regulators*, Lecture Notes in Math. 854 (1981), 372–401.