Basepoint Dependence of the Unipotent Fundamental Group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$

Navin Dasigi

A dissertation submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

of

University College London.

Department of Mathematics

University College London

February 2011

I, Navin Dasigi, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Abstract

Let $\bar{X}$ be the scheme $\mathbb{P}^1_{\bar{\mathbb{Q}}_p} \setminus \{0, 1, \infty\}$. We can assign a fundamental group to each rational basepoint on this scheme. These groups are non-canonically isomorphic, so they need not have isomorphic Galois actions. We study a description of this map from points to groups with Galois action, in terms of non-abelian cohomology. Using this description, we see that the fundamental groups associated to different basepoints are not isomorphic.

Acknowledgements

I thank my advisor, Professor Minhyong Kim, for teaching me a little of the mathematics that he knows, and the majority of the mathematics that I know, for making this work possible, for his patience; and also for many hours of stimulating conversation, mathematical and non-mathematical.

I thank many other teachers who made mathematics interesting and beautiful; especially Donu Arapura, Kevin Buzzard, and Edray Goins. I also thank my fellow students, especially Christine Berkesch, Minette D'Lima, and Phil Hackney, with whom learning maths was so enjoyable.

For their support and constant encouragement, I thank my family. And most of all, and for too many things to mention here, I thank my darling wife, Minette D'Lima.

Contents

Chapter 1

Introduction

1.1 Overview

This work concerns the etale fundamental groups on the thrice punctured projective line over $\bar{\mathbb{Q}}_p$.

The usual, topological fundamental group of a space is a well-understood functorial invariant capturing certain topological data. From one point of view, the etale fundamental group may be viewed as a generalisation of this functor to the category of schemes.

For another point of view, we quote the words of Nakamura, Tamagawa, and Mochizuki in [17]

> *"This notion of 'etale fundamental group' was introduced into algebraic geometry in the 1960's to keep track of the 'Galois theory of schemes'."*

For a third viewpoint, which may be seen as a synthesis of the previous two, we recall that the etale fundamental group of a scheme may be expressed as an extension of a Galois group by (the profinite completion of) a topological fundamental group. Indeed, let k be a field of characteristic 0, $\bar{k}$ its closure, and G the group $\mathrm{Gal}(\bar{k}/k)$. Then, for a scheme X defined over k, and with a rational basepoint x, the following sequence is exact.

$$\begin{tikzcd} 1 \arrow[r] & \pi_1(\bar{X},\bar{x}) \arrow[r] & \pi_1(X,x) \arrow[r] & G \arrow[r] \arrow[l, bend right, "s_x"'] & 1 \end{tikzcd}$$

The basepoint x gives a map from $\operatorname{Spec} k$ to X, and by functoriality this yields a splitting of the left-hand map. Then the problem of understanding the structure of $\pi_1(X, x)$ is equivalent to understanding the extension, or, equivalently, to understanding the action of G on $\pi_1(\bar{X}, \bar{x})$.

It is an interesting problem to understand the extent to which one can recover X or x from $\pi_1(X, x)$ or this extension data.

1.2 Formulation of Motivating Question

1.2.1 The Anabelian Conjectures of Grothendieck

This section follows the clear and illuminating exposition in [17]. We ignore basepoints for the moment. This is equivalent to considering only the intrinsic group structure of $\pi_1(X, x)$ without the splitting s_x above.

Grothendieck made a series of conjectures on the data that can be recovered from the fundamental groups of schemes. In particular, he conjectured that it is possible to recover an "anabelian" scheme X from the fundamental group $\pi_1(X)$. The term "anabelian" here was imprecisely defined in general, but was intended to suggest being 'beyond' or 'far from' abelian. For curves, it can be more precisely defined as follows:

A curve X is said to be anabelian if $\pi_1(\bar{X})$ is not abelian.

With this definition, Grothendieck's conjecture was proved, in various cases, and over various fields, by Nakamura, Tamagawa, and Mochizuki, as is outlined in their summary paper, [17]. Thus it is possible, from only the group structure on $\pi_1(X, x)$, to recover X. However, this approach deliberately ignored the basepoint of the fundamental group, from which it might be possible to recover more data.

1.2.2 Concerning Basepoints

One could ask whether it is possible to recover the pointed scheme (X, x) from the group $\pi_1(X, x)$ with certain extra structures.

As mere groups, and with no additional structure, it is well known that the various fundamental groups on a curve are isomorphic. However, additional structures on X will yield additional structures on $\pi_1(X)$. Considered as groups with these additional structures, it is no longer necessarily true that the various fundamental groups on X should agree.

In particular, if X is defined over k and if $x \in X(k)$ is a rational basepoint, we note that G acts on the pointed scheme (X, x). As discussed before, we may construct the group $\pi_1(X, x)$ as an extension of G by $\pi_1(\bar{X}, \bar{x})$. The intrinsic group structure of the latter does not depend on x, so that understanding the G-structure of $\pi_1(X)$ for a particular x is the same as understanding the G-structure on $\pi_1(\bar{X})$ for that x.

This action may also be understood as the conjugation action resulting from the splitting s_x above.

We can now formulate the motivating question of this work thus:

Motivating Question:*To what extent does the Galois structure on $\pi_1(\bar{X}, \bar{x})$ vary with x?*

1.2.3 Anabelian Revisited

We observe the following simple relation between the property of being anabelian and basepoint-dependent variation in the G-structure of $\pi_1(\bar{X})$.

Let X be a curve. If $\pi_1(\bar{X}, \bar{x})$ is abelian, then, for any x, we can make the identification

$$\pi_1(\bar{X}, \bar{x}) \cong \pi_1(\bar{X}, \bar{x})^{ab} \cong H_1^{et}(\bar{X}, \hat{\mathbb{Z}})$$

which holds even when we consider the various G-actions on these objects. Since H_1^{et} has a natural basepoint-free definition, we conclude that the G-structure on $\pi_1(\bar{X})$ is independent of the basepoint. Since the anabelian property for a curve is equivalent to possessing a non-abelian geometric fundamental group, we easily conclude the following inverse statement

If X is **not** Anabelian, then the G-structure on $\pi_1(\bar{X})$ does **not** vary with the basepoint.

Over an algebraically closed field of characteristic zero, the question of which curves have non-abelian geometric fundamental groups is equivalent to the question of which algebraic, complex 1-manifolds have non-abelian fundamental groups.

It is well known that a r-times punctured $\mathbb{C}$-manifold of genus g has the fundamental group

$$\Pi_{g,r} := \left\langle a_1, b_1, ..., a_g, b_g, c_1, ..., c_r | \prod_i [a_i, b_i] \prod_j c_j = 1 \right\rangle$$

This is non-abelian for $g = 0$ and $r \geq 3$, for $g = 1$ and $r \geq 1$, and for $g \geq 2$.

We can therefore conclude that, in some sense, the simplest anabelian curves occur when (g, r) is $(0, 3)$, $(1, 1)$, or $(2, 0)$.

These cases correspond to a proper curve of genus 2, a punctured elliptic curve (since we assume the existence of a k-rational basepoint), and the thrice-punctured projective line.

We will study our questions in the particular case of the last example, which we can, without loss of generality, describe concretely as $\mathbb{P}^1 \setminus \{0, 1, \infty\}$.

1.2.4 Approach

Our basic approach will be as follows. We fix a rational baspeoint $\bar{b} \in \bar{X}$. To any other rational basepoint, $\bar{x} \in \bar{X}$, we can associate a paths torsor $\pi_1(\bar{X}, \bar{x}, \bar{b})$, and also the fundamental group $\pi_1(\bar{X}, \bar{x})$ at $\bar{x}$.

We can therefore view the association of points to fundamental groups as a composition

$$\{\text{Points}\} \to \{\text{Paths Torsors}\} \to \{\text{Fundamental Groups}\}$$

We formulate algebraic descriptions of these two component maps and study them. In the particular case of the punctured projective line, the first map may be understood easily in terms of Kummer theory. The second map is thus the main focus of our attention.

1.3 Outline of Thesis

In chapter two we review some properties, and a slightly non-standard definition, of the fundamental group of a topological space.

We use this exposition to introduce the parallel theory of etale fundamental groups, taking particular note of the analogous theories of universal covering spaces.

In chapter three we introduce the parallel theories of paths torsors in topology and in arithmetic. We discuss an algebraic classification, in terms of Galois cohomology, for the set of arithmetic paths torsors on a scheme.

Building on the treatment of torsors, we discuss the rational universal covering space, and treat two examples. In doing so, we develop some technical tools for later use.

In chapter four we introduce the notion of twists of groups, and recall some classifying results for twists. This yields an algebraic description of the twists of a fundamental group on $\bar{X}$ which inculdes, in particular, all other fundamental groups on $\bar{X}$.

Fix a particular basepoint $\bar{b}$ on $\bar{X}$. We now have algebraic descriptions of the torsors of $\pi_1(\bar{X}, \bar{b})$ and of the twists of $\pi_1(\bar{X}, \bar{b})$. The former include path torsors such as $\pi_1(\bar{X}, \bar{x}, \bar{b})$, while the latter includes other fundamental groups such as $\pi_1(\bar{X}, \bar{x})$.

We end chapter four by recalling a result relating the algebraic description of $\pi_1(\bar{X}, \bar{x}, \bar{b})$ to the algebraic description of $\pi_1(\bar{X}, \bar{x})$. This will be seen to be closely related to the non-commutativity of $\pi_1(\bar{X}, \bar{b})$.

Chapter five concerns an earlier result of Hain that bears upon this work. Working in the analytic category, Hain showed that the Hodge structure on the derived groups of $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus \{0, 1, \infty\})$ varies faithfully with the basepoint. That is, it is possible to recover the basepoint x from the second derived group of $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus \{0, 1, \infty\}, x)$ with its Hodge structure.

This issue is closely related to our motivating question, so we review the main features of Hain's proof. We then ask why a naive translation of that proof to the arithmetic case category fails.

In chapter six we recall some constructions and basic properties of the unipotent completion of the fundamental group on X, as well as some known results concerning its structure. We observe that this may be viewed as a 'linearisation' of the full profinite group and that it naturally comes equipped with an associated Lie algebra.

In chapter seven we begin by formulating our question with greater rigour and understand how the question arises naturally. In particular, we concentrate on the derived groups of the unipotent completion of the fundamental groups.

We combine the tools and lemmata developed over the previous chapters to understand how the Galois structure of the second derived group of the fundamental group varies with the basepoint. It turns out that the Galois structure of the second derived group is identical for any rational basepoint.

In chapter eight we refine the structure used for the main result of chapter seven in an attempt to extend our understanding. We study the variations of the Galois structure with the basepoint on higher derived groups.

Chapter 2

Background - Definitions and Universal Covers

2.1 The Topological Fundamental Group

We aim in this chapter to develop a theory of etale fundamental groups as an analogy and an extension of the theory of topological fundamental groups.

Before doing so, we will review some aspects of the theory of topological fundamental groups that will be of interest to us, and we will use these to develop a formulation of the topological case that will be of use in the algebraic case.

2.1.1 Preliminaries in Topology

Let X be a path-connected, locally simply connected topological space. We recall that there exists a space $\tilde{X}$ and a map $u : \tilde{X} \to X$ such that

- u is a local homeomorphism
- $\tilde{X}$ is simply connected

Furthermore, this pair $(\tilde{X}, u)$ is unique up to isomorphism. We also recall two universal properties of $\tilde{X}$. Firstly, that it is a covering space of any space which is a covering space of X. Secondly, that given a choice of basepoint $b \in X$, and a choice of a preimage $\tilde{b} \in \tilde{X}_b = u^{-1}(b)$, the pointed space $(\tilde{X}, \tilde{b})$ is initial in the category of pointed covers of (X, b).

2.1.2 Some Fundamental Isomorphisms - Topological Case

We present four descriptions of the fundamental group of a topological space and discuss their relationships.

Fix a path connected, semi-locally simply connected topological space X, and a basepoint $b \in X$. Denote the category of covering spaces of X by $Cov(X)$.

We will begin by defining a fibre functor e_b from $Cov(X)$ to the category of sets as follows. For a cover $\phi : Y \to X$,

$$e_b(Y) := Y_b = \phi^{-1}(b)$$

Now let $[\gamma] \in \pi_1(X, b)$ be the homotopy class of some loop γ in X based at b. For any cover $\phi : Y \to X$ we can define an action of γ on the set $e_b(Y)$ in the following way.

2.1.2.1 Automorphisms of a Fibre Functor

For each $y \in e_b(Y)$, define $\gamma(y)$ to be the endpoint of the unique lift $\gamma_{Y,y}$ of γ that starts at y. Since γ itself has an inverse, it is clear that this map on $e_b(Y)$ is a set automorphism. In fact, we can say that

Lemma 2.1. *The association above gives a canonical isomorphism*

$$\pi_1(X, b) \to \mathrm{Aut}(e_b)$$

Proof. This is [20], theorem 2.3.7. □

2.1.2.2 Fibres in the Universal Cover

We also will make use of a map between $\pi_1(X, b)$ and $\tilde{X}_b$ defined as follows.

Fix a point $\tilde{b} \in \tilde{X}_b$. Define a map

$$T_{\tilde{b}} : \pi_1(X, b) \longrightarrow \tilde{X}_b$$

by $T_{\tilde{b}}(\gamma) =$ (endpoint of $\gamma_{\tilde{X},\tilde{b}}$), where, as before, the latter means the (unique) lift of γ to $\tilde{X}$ that starts at $\tilde{b}$.

Lemma 2.2. *The map $T_{\tilde{b}}$ is injective.*

Proof. Indeed, we have already shown that, for any $\tilde{\tilde{b}} \in \tilde{X}_b$, there is at most one automorphism θ of e_b with $\theta(\tilde{b}) = \tilde{\tilde{b}}$. Since every homotopy class of loops gives an automorphism of e_b, the result follows. □

Lemma 2.3. *The map $T_{\tilde{b}}$ is surjective.*

Proof. Let $\tilde{\tilde{b}} \in \tilde{X}_b$. Choose a path from $\tilde{b}$ to $\tilde{\tilde{b}}$. Then the class γ of the associated loop in X satisfies $T_{\tilde{b}}(\gamma) = \tilde{\tilde{b}}$. □

2.1.2.3 Automorphisms of the Universal Cover

Finally, we define a map

$$\Omega : \mathrm{Aut}_X(\tilde{X}) \longrightarrow \tilde{X}_b$$

by $\phi \to \phi(\tilde{b})$ for $\phi \in \mathrm{Aut}_X(\tilde{X})$.

The assertion that this map is bijective is simply a reformulation of the statement that $(\tilde{X}, \tilde{b})$ is initial in the category of pointed covers of (X, b).

2.1.3 The Limits of this Analogy

We have defined three set isomorphisms:

$$\begin{aligned} \pi_1(X,b) &\cong \mathrm{Aut}(e_b) \\ \pi_1(X,b) &\cong \tilde{X}_b \\ \pi_1(X,b) &\cong \mathrm{Aut}_X(\tilde{X}) \end{aligned}$$

The first of these is canonical, the second and third are not. To this list we may add a fourth isomorphism; for any $x \in X$, choose a homotopy class of paths p from b to x and define a map

$$\pi_1(X,b) \longrightarrow \pi_1(X,x) \tag{2.1}$$

by $\gamma \to p\gamma p^{-1}$.

In this section, we have recalled some properties of the topological fundamental group. It associates a group functorially to a pointed space. All groups associated to the various points on a space are isomorphic via the isomorphism 2.1. Since this depends on a choice of path, it is non-canonical.

In the next sections, we shall recall the analogous theory of etale fundamental groups for schemes. These will have extra structure that may be of interest, such as Galois actions, and, if the association of a π_1 group is to be functorial, so should the fundamental groups of these schemes have extra structure.

For an appropriate notion of path, the isomorphism 2.1 will still hold. However, we stress the fact that these non-canonical maps may alter the additional, more delicate structures on the fundamental groups of schemes. In particular, we shall make use of the fact that, for two points x and b on a scheme, it may be true that $\pi_1(X, b) \cong \pi_1(X, x)$ in the category of groups but that it is not true in the category of groups with an action by a certain Galois group.

2.2 The Etale Fundamental Group

2.2.1 Finite Etale Covers

We wish to develop a theory of the etale fundamental group in a manner analogous to the theory of the topological fundamental group developed in section 1. For the rest of this work, all the schemes we consider shall be **Noetherian, geometrically connected, and of finite type**.

First we describe a replacement for the category $Cov(T)$ of covering spaces of a topological space T. A topological covering space is, locally, a topological isomorphism. We cannot replace these by maps of schemes which are locally algebraic isomorphisms, as the Zariski topology is far too coarse and would therefore yield a very poor theory.

Instead we will replace the category of covering spaces with the category of etale maps, which we will define in stages below, first for local rings, then for arbitrary rings, and finally for schemes:

Definition 1. Let $(A, \mathcal{M})$ and $(B, \mathcal{N})$ be local rings. Then a homomorphism

$$\phi : (A, \mathcal{M}) \longrightarrow (B, \mathcal{N})$$

is called local etale if

- B is flat over A.
- $\phi(\mathcal{M}) = \mathcal{N}$
- $\frac{B}{\mathcal{N}}$ is a finite separable extension of $\frac{A}{\mathcal{M}}$

Definition 2. Let A and B be rings. Then a homomorphism

$$\phi : A \longrightarrow B$$

is called etale if, for all primes $\mathcal{N} \in \operatorname{Spec} B$, the local map $\phi_{\mathcal{N}} : A_{\phi^{-1}(\mathcal{N})} \to B_{\mathcal{N}}$ is local etale.

Definition 3. Let X and Y be schemes. A morphism

$$\phi : X \longrightarrow Y$$

is called etale if, for some affine cover $Y = \cup_i U_i$ and $U_i = \operatorname{Spec} A_i$ and some affine subcovers $\phi^{-1}(U_i) = \cup_j V_{i,j}$ and $V_{i,j} = \operatorname{Spec} B_{i,j}$, the induced ring maps $A_i \to B_{i,j}$ are etale for all i and j.

Finally, we will have frequent cause to refer to the notion of a finite etale cover. ([20], 5.2.1)

Definition 4. Recall that a finite morphism of schemes $\phi : X \to Y$ is said to be locally free if the direct image sheaf $\phi_* O_X$ is a locally free O_Y-sheaf of finite rank. If, in addition, each fibre scheme X_p is Spec of an etale $k(p)$-algebra, then we say that the morphism ϕ is *finite etale*.

Definition 5. An finite etale morphism of schemes that is surjective on points is called an *etale cover*.

We can obtain the following structure theorem for etale maps of varieties over algebraically closed fields:

Lemma 2.4. *Let k be an algebraically closed field, and let X and Y be separated integral schemes over k. Then, for a morphism $\phi : X \to Y$, we have*

$$(\phi \textit{ is etale}) \Leftrightarrow (\phi \textit{ is a tangent cone isomorphism})$$

See [13], chapter I, for the proof.

Tangent spaces are only useful when dealing with varieties over algebraically closed fields, so the hypothesis of this result is, in some sense, necessary.

This lemma tells us that an etale morphism takes smooth points to smooth points, and singularities to singularities of the same type. In fact, this continues to be true over base schemes which are not algebraically closed fields. See [13] chapter I for details.

We will now review some basic properties of etale and finite etale maps. Though this will be a very incomplete account of the subject, it will hopefully remind the reader of analogous theories noted in the topological case, and further underline this analogy.

Lemma 2.5. *Let X be a smooth variety of finite type over $\mathbb{C}$. Let X^{an} denote its analytification. Then the category of etale covers of X and the category of finite covering maps of X^{an} are equivalent.*

For the proof, which involves the local isomorphism theorem, the structure theorem above, GAGA applied to sheaves of etale algebras, and a hard result of Grauert and Remmert, see [6], XII.

In the topological category, we are often interested in the morphisms in $Cov(X)$ (deck transformations). Recall the following well-known result.

Lemma 2.6. *Let (S, θ) and (T, ϕ) be two connected covering spaces of a connected, Hausdorff space X. Let ω be the one point space, and $s : \omega \to S$ a map to S. Let ψ_1 and ψ_2 be two maps such that*

$$\begin{tikzcd} S \arrow[rr, "\psi_1", "\psi_2"'] \arrow[dr, "\theta"'] & & T \arrow[dl, "\phi"] \\ & X & \end{tikzcd}$$

commutes. If $\psi_1 s = \psi_2 s$, then $\psi_1 = \psi_2$.

Proof. See [20], Proposition 2.2.2. □

We aim to make a similar statement in the algebraic case.

We begin by listing some basic properties of compositions of etale maps and covers, which are analogous to well-known properties of topological covering maps.

Lemma 2.7. *Let*

$$Z \xrightarrow{\psi} Y \xrightarrow{\phi} X$$

be morphisms between schemes X, Y, and Z.

- *If $\phi\psi$ and ϕ are finite etale and if ψ is separated, then ψ is finite etale.*
- *If ϕ and ψ are finite etale, then so is $\phi\psi$. If ϕ and ψ are etale covers, then $\phi\psi$ is an etale cover.*
- *If $\phi\psi$ and ψ are etale, ϕ need not be etale.*

Proof. Omitted. See [20], chapter 5, or [13] for details. □

A map $\bar{s}$ from the spectrum of an algebraically closed field $\bar{k}$ to a scheme defined over k is called a **geometric point**. It is equivalent to a choice of a closed point s on the scheme and an embedding $k(s) \hookrightarrow \bar{k}$.

We shall see in the next section that these geometric points play the same role in the theory of etale fundamental groups that ordinary points play in the theory of topological fundamental groups.

With this terminology, we can formulate an analogy of Lemma 2.6 above.

Lemma 2.8. *Let S, T, and X be schemes over a field k. Let (S, θ) and (T, ϕ) be two connected etale covers of a connected scheme X. Let $\bar{s}$ be a geometric point of S. Let ψ_1 and ψ_2 be two deck transformations such that*

$$\begin{tikzcd} S \arrow[rr, "\psi_1", "\psi_2"'] \arrow[dr, "\theta"'] & & T \arrow[dl, "\phi"] \\ & X & \end{tikzcd}$$

commutes. If $\psi_1\bar{s} = \psi_2\bar{s}$, then $\psi_1 = \psi_2$.

Proof. This is a particular case of [20], Corollary 5.3.3. □

We stress that this lemma would clearly fail if we replaced ‘geometric point’ with ‘point’. This coincides with the general principle that the role of the point in the topological category is taken by $\operatorname{Spec} \bar{k}$ in the category of $\operatorname{Spec} k$ schemes.

2.2.2 Definition of the Etale Fundamental Group

We wish to define a concept for the category of schemes analogous to the fundamental group of topology. As mentioned in the previous section, in the topological case, we have a **canonical** isomorphism

$$\pi_1(X, b) \cong \operatorname{Aut}(e_b)$$

Considered from another point of view, we could define the fundamental group of a topological space in as the automorphism group of a fibre functor, and thus avoid any use of path- or loop-spaces. Since this is a canonical isomorphism, such a definition will preserve any higher structures on the fundamental group.

This will therefore motivate our definition of the fundamental group of a scheme. Before following this recipe, we will need to review some of the essential ingredients.

Definition 6. Let X be a scheme defined over a field k. Let Ω be the separable closure of X over k. Then a *geometric point* of X is a map $\operatorname{Spec} \Omega \to X$.

That is, a geometric point is a topological point x on X and a choice of embedding $k(x) \to \Omega$. Since we are working in the category of k-schemes, if x is a k-rational point, there is only one choice of embedding.

We also have the following generalisation, from [5].

Definition 7. Let X, k, and Ω be as above. Then a *tangential basepoint* is a map $\operatorname{Spec} \Omega((t)) \to X$.

We will replace the topological fibre functor of section 1 with

Definition 8. Let X be a scheme defined over a field k. Fix a geometric point b in X. We construct a functor

$$e_b : Et(X) \longrightarrow \text{Sets}$$

by $e_b(\phi : Y \to X) := Y \times_X b$. The fibre product here means the product of Y and Ω, where Ω maps to X by the geometric point b.

We can equivalently consider $e_b(Y)$ to be the set of lifts of the map b along the etale cover ϕ.

We are now in a position to define the etale fundamental group.

Definition 9. We define the etale fundamental group of a scheme X/k with basepoint b to be

$$\pi_1(X, b) := \text{Aut}(e_b)$$

2.2.3 A Digression on Geometric Points

It is not unreasonable at this point to ask why we ought to use geometric points rather than points in the usual sense.

We return to the earlier view that the etale fundamental group is 'an accouting device to keep track of the Galois theory of schemes'.

From this point of view, we consider that we are interested also in the Galois theory of the residue field of the point (in the usual sense) that we choose as our basepoint for π_1. We must therefore distinguish between different geometric points.

2.3 Universal Covers

In the study of the topological fundamental group it was very convenient to make use of the 'universal' cover of the space under consideration.

This was shown to be a covering map of the base space which is also a covering map of any other cover of the base space.

Fix a scheme X defined over a field k. To use the idea of universal covers, we want to build an etale cover $\tilde{\tilde{X}}$ such that, for any other etale cover Y of X, $\tilde{\tilde{X}}$ is also an etale cover of Y. More precisely, we would like to construct a scheme $\tilde{\tilde{X}}$ and an etale cover $\theta : \tilde{\tilde{X}}$ such that, for any etale cover $\phi : Y \to X$, there exists an etale map ψ such that the triangle below commutes.

$$\begin{tikzcd} \tilde{\tilde{X}} \arrow[rr, "\exists\psi"] \arrow[dr, "\theta"'] & & Y \arrow[dl, "\phi"] \\ & X & \end{tikzcd}$$

The reason for the notation $\tilde{\tilde{X}}$ rather than $\tilde{X}$ will be explained in section 3.3.

It will also be shown that this universal cover $\tilde{\tilde{X}}$ has the (appropriately modified) universal property that we should expect it to have: that, given a choice of a geometric point $\tilde{b}$ in the fibre over some geometric basepoint b of X, $(\tilde{\tilde{X}}, \tilde{b})$ is initial among pointed covers of (X, b).

2.3.1 The Universal Cover Cannot be a Scheme

We begin by considering a motivating example.

Fix a natural number n. Let $X := \mathbb{A}^1_{\bar{\mathbb{Q}}} \setminus \{0\}$ be the punctured affine line over $\bar{\mathbb{Q}}$. We observe that the map $X \to X$ defined on rings by sending x to x^n is everywhere etale, and is of degree n.

If a scheme acting as the universal cover were to exist, it must would have degree at least n, in order to cover this cover. Hence, a universal cover could not have finite degree over X.

On the other hand, an etale cover is finite by definition 5 and hence quasi-finite, so that we are naturally driven to consider a definition of the universal cover as something other than a scheme.

If we allow this possibility, the first required property of $\tilde{\tilde{X}}$, that it be initial among pointed cover of X, naturally suggests the following definition.

Definition 10. Let X be a scheme, and b a geometric point. We define the *pointed universal etale cover* of (X, x) to be

$$(\tilde{\tilde{X}}, \tilde{x}, \theta) := \varprojlim (Y, y, \phi)$$

where the limit is taken over all connected pointed etale covers $\phi : (Y, y) \to (X, x)$ of X by schemes Y. We also write $\tilde{\tilde{X}}$ to mean the same pro-object, ignoring the basepoint.

We write $\varprojlim$ here to mean the pro-object which corresponds to the entire inverse system of pointed finite etale covers.

Note that all triangles in the system thus described must commute, by lemma 2.8.

Recall the following standard definition of a morphism of pro-objects. Given two pro-objects corresponding to systems $\{A_\alpha\}$ and $\{B_\beta\}$, we have $\mathrm{Hom}(\{A_\alpha\}, \{B_\beta\}) := \varprojlim_\beta \varinjlim_\alpha \mathrm{Hom}(A_\alpha, B_\beta)$. We will often specify maps to pro-objects by specifying only maps to cofinal subsystems.

To be explicit, a morphism from the universal cover to a pointed finite cover (Y, y) may be defined by a map from any pointed cover in the system defining $\tilde{\tilde{X}}$ to (Y, y). In particular, we can use the cover (Y, y) itself.

It is then simple to check that the first required property of the universal cover is satisfied.

Lemma 2.9. *Let $\phi : Y \to X$ be any finite etale cover of Y. Then there is a map $\psi : \tilde{\tilde{X}} \to Y$ that commutatively completes the following triangle.*

$$\begin{tikzcd} \tilde{\tilde{X}} \arrow[rr, "\exists\phi"] \arrow[dr, "\theta"'] & & Y \arrow[dl, "\phi"] \\ & X & \end{tikzcd}$$

The map ψ is simply projection onto the factor corresponding to Y, as described above.

2.3.2 Interlude on Galois Covers

Before we can consider the second of the properties which we require from our universal cover, we need to make a brief digression to study Galois covers.

Definition 11. Let G be a finite group. An etale cover Y of the scheme X is said to be Galois with Galois group G if there is a scheme-theoretic isomorphism:

$$Y \times_X Y \longrightarrow \coprod_{g \in G} Y_g$$

Here the right hand side simply means finitely many disjoint copies of Y, indexed by the elements of G.

More explicitly, we can say:

Definition 12. Let $\phi : Y \to X$ be an etale cover and let G be a finite group acting on Y over X. We define two maps from $\coprod_G Y_g$ to Y. The first sends each component $Y_g \cong Y$ to Y by the identity, and the second map sends each Y_g to Y by g. These two maps are clearly compatible over X, so that they define a morphism

$$\coprod_G Y_g \longrightarrow Y \times_X Y$$

If this morphism is an isomorphism, we say that the cover is Galois with Galois group G.

These particular covers are of great importance for the following reason.

Lemma 2.10. *Let $\phi : Y \to X$ be a connected Galois cover of schemes. Pick a geometric basepoint b for X, and some geometric point y in $e_b(Y)$. Then the map*

$$Aut_X(Y) \longrightarrow e_b(Y)$$

given by $\theta \to \theta(y)$ is a bijection.

Proof. Injectivity follows from Lemma 2.8. Indeed, an automorphism $\theta \in \mathrm{Aut}_X(Y)$ is exactly a commutative triangle

$$\begin{tikzcd} Y \arrow[rr, "\theta"] \arrow[dr, "\phi"'] & & Y \arrow[dl, "\phi"] \\ & X & \end{tikzcd}$$

and hence θ is etale. By lemma 2.8, if two such θ agree on y, they agree on Y. Hence the map is injective.

The map

$$Y \times_X Y \cong \coprod_G Y \to Y$$

clearly has degree equal to the order of G; and it is a flat base change of the map $Y \xrightarrow{\phi} X$. Hence the map ϕ also has degree equal to the order of G. Thus it will suffice to show that the order of the group $\mathrm{Aut}_X(Y)$ is the order of the group G.

Elements of G correspond to morphisms $\alpha : Y \to \coprod_G Y$ such that the composition of α with the natural projection $\coprod_G Y \to Y$ is the identity on Y. Under the isomorphism given in the definition above, such morphisms correspond in turn to morphisms $\beta : Y \to Y \times Y$ such that the first projection map is the identity.

These morphisms in their turn correspond to pairs of maps $(id : Y \to Y)$ and $(\theta : Y \to Y)$ that are compatible with the map ϕ to X. But the group of such maps is exactly what we mean by $\mathrm{Aut}_X(Y)$. □

Having defined the notion of Galois covers, we next turn our attention to their usefulness, as highlighted by:

Lemma 2.11. *Let $\phi : Y \to X$ be an etale cover. Then there exists a Galois cover $\theta : Z \to X$ and a map $\psi : Z \to Y$ (necessarily etale) such that the triangle*

$$\begin{tikzcd} Z \arrow[rr, "\psi"] \arrow[dr, "\theta"'] & & Y \arrow[dl, "\phi"] \\ & X & \end{tikzcd}$$

commutes.

Proof. See Serre's proof in [20], Proposition 5.3.9. □

The usefulness Galois covers is more evident when we reformulate the last result as:

Lemma 2.12. *Let X be a scheme. The subcategory of finite Galois covers of X is cofinal in the category of finite etale covers of X.*

By lemma 2.12, we could replace the limit in definition 10 with the limit taken over all pointed finite Galois covers.

2.3.3 The Second Universal Property of the Universal Cover

We now verify the second universal property of $\tilde{\tilde{X}}$. To do this, we must better understand what a basepoint in the universal cover is. We will continue to assume that X is geometrically connected and separated.

By the definition following definition 10, a map to an inverse limit of schemes must be a compatible collection of maps to each of the schemes in the inverse system. Explicitly, in our case:

Definition 13. A geometric (respectively tangential) basepoint $\tilde{b} \in \tilde{\tilde{X}}_b$ is a compatible collection of geometric (respectively tangential) basepoints $y \in Y_b$ for each etale cover Y of X.

By lemma 2.12, we could replace the phrase 'every etale cover' in this definition with 'every Galois cover'.

With this definition in hand, the property of being initial among pointed covers may be precisely formulated as

Lemma 2.13. *Let $\tilde{b} \in \tilde{\tilde{X}}_b$ be a compatible collection of basepoints as described above. Let $\phi : (Y, y) \to (X, b)$ be any finite etale cover.*

Then there exists a unique map $\psi : \tilde{\tilde{X}} \to Y$ such that the following triangle commutes.

$$\begin{tikzcd}
(\tilde{\tilde{X}}, \tilde{b}) \arrow[rr, "\psi"] \arrow[dr, "\theta"'] & & (Y, y) \arrow[dl, "\phi"] \\
& (X, b) &
\end{tikzcd}$$

Proof. By lemma 2.12, we can take the limit of 10 over the system of pointed Galois covers. By the same lemma, for any cover Y, we can find some Galois cover $\beta : Z \to X$ that covers Y, so that the following triangle commutes.

$$\begin{tikzcd}
(Z, z) \arrow[rr, "\alpha"] \arrow[dr, "\beta"'] & & (Y, y) \arrow[dl, "\phi"] \\
& (X, b) &
\end{tikzcd}$$

The cover Z appears in the inverse system defining $\tilde{\tilde{X}}$, and we denote by z' the image of $\tilde{b}$ in Z. By the Galois property of Z, there is a unique X-automorphism of Z carrying z' to z. Call this σ.

It is sufficient to provide a map $\psi_Z : (\tilde{\tilde{X}}, \tilde{b}) \to (Z, z)$; when composed with α, this will yield ψ. Recall that a morphism from $\tilde{\tilde{X}}$ to Z is specified by a map from any member of the system defining $\tilde{\tilde{X}}$ to Z. We observe that σ defines such a map, and carries $\tilde{b}$ to z.

Thus the map induced by σ, composed with α, yields the required map ψ of pointed spaces.

□

Our final observation in this subsection will be

Lemma 2.14. *Let X be a scheme, and $\phi : Y \to X$ an etale cover. Then the universal cover $\tilde{\bar{X}}$ of X is also the universal cover of Y.*

Proof. Fix a choice $y \in Y_b$. We will define mutually inverse maps between $\tilde{\bar{X}}$ and $\tilde{\bar{Y}}$. Indeed, let (Z, z) be a cover of (Y, y). Then by composition (lemma 2.7), (Z, z) is also a cover of (X, b), and so it appears in the system defining $\tilde{\bar{X}}$. We map (Z, z) appearing in $\tilde{\bar{X}}$ to (Z, z) appearing in $\tilde{\bar{Y}}$, by the identity. Since Z was arbitrary, this defines a map from $\tilde{\bar{Y}}$ to $\tilde{\bar{X}}$.

Conversely, let (W, w) appear in the system defining $\tilde{\bar{X}}$. By base-change ([20], remark 5.2.3) and composition, $(W, w) \times_{(X,x)} (Y, y)$ is an etale cover of (Y, y), and hence (by composition) also of (X, x). We map the copy appearing in $\tilde{\bar{Y}}$ to the copy appearing in $\tilde{\bar{X}}$ by the identity. By composition, this gives a map from a member of the system defining $\tilde{\bar{Y}}$ to W. Since (W, w) was arbitrary, and since the maps we have defined are compatible (by lemma 2.8), this defines a map from $\tilde{\bar{Y}}$ to $\tilde{\bar{X}}$.

The compositions of these two maps yield automorphisms of $\tilde{\bar{X}}$, respectively $\tilde{\bar{Y}}$, which is the identity map on a cofinal susbsystem. The two maps are thus inverse.

□

In particular, we find that

Corollary. *Let X/k. Let $\bar{X}$ denote $X \times_k \bar{k}$, the base change of X to a separable closure of k. Then the universal etale cover of $\bar{X}$ is $\tilde{\bar{X}}$.*

We will develop this idea further in the next chapter.

2.3.4 Some Fundamental Isomorphisms - Algebraic Case

Having established a useful definition of the universal cover $\tilde{\bar{X}}$ of X, and having shown it to have two universal mapping properties similar to those of a topological universal cover, our next aim is to establish results analogous to the fundamental isomorphisms that hold in the topological case.

For this section, X will be a scheme, $\tilde{\tilde{X}}$ its universal cover as described above, b a chosen geometric basepoint of X, and $\tilde{b}$ a chosen geometric basepoint lying over this in $\tilde{\tilde{X}}$. We begin with a reformulation of lemma 2.13.

Lemma 2.15. *For any cover $\phi : Y \to X$, define a map*

$$Hom_X(\tilde{\tilde{X}}, Y) \longrightarrow Y_b$$

by $\psi \to \psi(\tilde{b})$. This map is a bijection.

This formulation leads, by general nonsense, to the

Corollary. *Fix a geometric basepoint $\tilde{b} \in \tilde{\tilde{X}}_b$. Then there is a bijective map*

$$Aut_X(\tilde{\tilde{X}}) \longrightarrow \tilde{\tilde{X}}_b$$

Proof. For any finite etale cover Y, we have $\mathrm{Hom}_X(\tilde{\tilde{X}}, Y) = Y_b$. By the definition of a morphism of pro-objects, we have $\mathrm{Hom}_X(\tilde{\tilde{X}}, \tilde{\tilde{X}}) := \varprojlim_V \varinjlim_W \mathrm{Hom}_X(W, V)$ where V and W range over all finite pointed covers, as in definition 10.

We make the identifications $\varinjlim_W \mathrm{Aut}_X(W, V) \cong V_b$ and $\varprojlim_V V_b \cong \tilde{\tilde{X}}_b$, to complete the proof. ∎

The relationship between $\pi_1(X, b) := \mathrm{Aut}(e_b)$ and the two objects linked above is expressed by

Lemma 2.16. *Fix $\tilde{b} \in \tilde{\tilde{X}}_b$. Then the map*

$$\pi_1(X, x) \to \tilde{\tilde{X}}_b$$

given by $\gamma \to \gamma(\tilde{b})$ is a bijection.

Proof. Represent $\tilde{\tilde{X}}$ by a limit over Galois covers. Fix $\tilde{b} \in \tilde{\tilde{X}}_b$. Let $\tilde{\tilde{b}} \in \tilde{\tilde{X}}_b$. Define $\gamma \in \pi_1(X, b)$ by defining $\gamma|_{\tilde{\tilde{X}}} \in \mathrm{Aut}(e_b(\tilde{\tilde{X}}))$ via $\gamma(\tilde{b}) = \tilde{\tilde{b}}$. This totally defines γ. Indeed, if $\bar{b} \in \tilde{\tilde{X}}_b$, then by the second universal property there is some $\phi \in \operatorname{Aut} \tilde{\tilde{X}}$ such that $\phi(\tilde{b}) = \bar{b}$. Then for γ to be in $\operatorname{Aut}(e_b)$, we require that $\gamma(\bar{b}) = \phi(\tilde{\tilde{b}})$, so that specifying $\gamma(\tilde{b})$ specifies $\gamma(\bar{b})$ for any $\bar{b}$. Hence the map is surjective.

On the other hand, suppose that $\gamma(\tilde{b})$ and $\gamma'(\tilde{b})$ agree for some other loop γ'. By the same argument, $\gamma(\tilde{b})$ specifies γ and $\gamma'(\tilde{b})$ specifies γ', so that $\gamma = \gamma'$. Hence the map must be injective. $\square$

We take this opportunity to stress again that these isomorphisms are non-canonical. Thus there is no reason why they should preserve any higher structures that π_1, as a functor, may inherit from the class of schemes to which we apply it.

Chapter 3

On Certain Properties of Torsors

On Torsors

The main reference for the results summarised in this chapter and the next is [19]

A torsor may be thought of as a group that has forgotten who its identity element is; just as an affine space may be thought of as a vector space that has forgotten who its origin is.

Definition 14. Let G be a group. A left G-set T is called a torsor for G if, for all $t \in T$, the map

$$G \longrightarrow T$$

given by $g \to gt$ is an isomorphism.

This explains the informal definition given above: for any $t \in T$, we can give T a group structure such that t is the identity.

Indeed, for any $t_1, t_2 \in T$, we find the unique $g_1, g_2 \in G$ such that $g_i t = t_i$, and then we define $t_1 t_2 := g_1 g_2 t$. The choices of g_1, g_2 are unique by the torsor axiom.

3.1 Paths Torsors

3.1.1 In topology

Let X be a topological space as in the previous chapter, and let b, x be two points on X. Then the set of (homotopy classes of) paths from b to x is naturally a left torsor for the fundamental group $\pi_1(X, b)$ based at b.

Indeed, fix $p \in \pi_1(X, b, x)$. The for any $p_1 \in \pi_1(X, b, x)$, the composition $p_1 p^{-1}$ is an element of $\pi_1(X, b)$, and $(p_1 p^{-1})p = p$ in $\pi_1(X, b, x)$, so that the map

$$\pi_1(X, b) \longrightarrow \pi_1(X, b, x)$$

given by $\gamma \to \gamma p$ is surjective. This map is injective because, if $\gamma_1 p$ and $\gamma_2 p$ are homotopic paths, the composition $(\gamma_1 p)(\gamma_2 p)^{-1}$ is a null homotopic loop. But $(\gamma_1 p)(\gamma_2 p)^{-1} = \gamma_1 p p^{-1} \gamma_2^{-1} = \gamma_1 \gamma_2^{-1}$, whence $\gamma_1 = \gamma_2$.

Taking a cue from our earlier canonical identification

$$\pi_1(X, b) \cong \mathrm{Aut}(e_b)$$

we wish to consider the relationship between $\pi_1(X, b, x)$ and $\mathrm{Isom}(e_b, e_x)$. This is expressed in

Lemma 3.1. *There is a canonical set isomorphism*

$$\pi_1(X, b, x) \longrightarrow \mathrm{Isom}(e_b, e_x)$$

Sketch of Proof. Let p be a (homotopy class of) path(s) in X from b to x. Define $f_p \in \mathrm{Isom}(e_b, e_x)$ as follows. Let $\phi : Y \to X$ be any cover. For any $y \in Y_b$, lift p to a path in Y beginning at y, and define $f_p(y)$ to be the endpoint of this lift. As in Chapter 1, we can check that any deck transformation moves this lift, so that this f_p commutes with the action of any deck transformation. That is, $f_p \in \mathrm{Isom}(e_b, e_x)$.

To check that this association yields an isomorphism is very similar to the checks necessary in the group case considered in chapter 2. □

The fact that this map is canonical suggests that the torsor structure ought to be preserved, if we can formulate this correctly:

Lemma 3.2. *Identifying $\pi_1(X, b)$ and* $\mathrm{Aut}(e_b)$ *via the canonical isomorphism given in chapter 2, the map above defined by $p \to f_p$ produces a torsor isomorphism.*

Proof. We need only check that the actions of $\pi_1(X, b)$ on p and on f_p are the same. Let $\gamma \in \pi_1(X, b)$, and let Y be a cover of X, and let $y \in Y_b$.

Then $(\gamma p)(y)$, by the uniqueness of path-lifting, is the endpoint of the lift of p that starts at $\gamma(y)$. On the other hand, $(\gamma f_p)(y)$ is the image of y under the composition of γ and f_p, which is $f_p(\gamma(y))$, defined to be the endpoint of $\gamma(y)$. □

3.1.2 In Arithmetic

In the algebraic case, the lemmata above motivate the following definition:

Definition 15. Let X be a separated scheme defined over a field k. Let b and x be two geometric points on the scheme X.

Then we define the torsor of paths in X from b to x as

$$\pi_1(X, b, x) \cong \mathrm{Isom}(e_b, e_x)$$

We can prove, in a manner identical to the topological case, that this is a left torsor for the fundamental group at b.

Next, we return our attention to the universal cover of X. We will develop this theory only in the algebraic case although, as before, an analogous theory holds in the topological case as well.

For this chapter, we let X be a geometrically connected, separated Noetherian scheme of finite type over a field k, and let b and x be geometric points on X. Also, let $\tilde{\tilde{X}}$ be the universal cover of X as in chapter 2.

Lemma 3.3. *Fix a basepoint $\tilde{b} \in \tilde{\tilde{X}}_b$ over b in the universal cover. Then the map*

$$\pi_1(X, b, x) \longrightarrow \tilde{\tilde{X}}_x$$

given by $p \to p(\tilde{b})$ is an isomorphism.

Proof. It is clear that $\pi_1(X, b, x)$ is also a right torsor for $\pi_1(X, x)$. Then, by [20] 5.5.1 we can fix a choice of $p \in \pi_1(X, b, x)$, and use it to produce an isomorphism (by definition 14)

$$\pi_1(X, b, x) \cong \pi_1(X, x)$$

defined by $p_1 \to p^{-1}p_1$. Then , for any $\tilde{x} \in \tilde{\tilde{X}}_x$, lemma 2.16 gives an isomorphism

$$\pi_1(X, x) \cong \tilde{\tilde{X}}_x$$

by $\gamma \to \gamma(\tilde{x})$.

We compose these two maps to obtain an isomorphism as required. □

We can also use these paths-torsors to create isomorphisms between the fundamental groups associated to X with different basepoints.

Lemma 3.4. *Let X, b, and x be as before. Then there is a non-canonical isomorphism*

$$\pi_1(X, b) \cong \pi_1(X, x)$$

Proof. Choose $p_0 \in \mathrm{Isom}(e_b, e_x)$. Then

$$\pi_1(X, b) \longrightarrow \pi_1(X, b, x)$$

given by $\gamma \to \gamma p_0$ and

$$\pi_1(X, b, x) \longrightarrow \pi_1(X, x)$$

given by $p \to p_0^{-1}p$ are both isomorphisms. Composing them gives the required map. □

We note that two such fundamental groups cannot be canonically isomorphic, since this map naturally factors through a set, and a group cannot be canonically isomorphic to a set.

Indeed, this map is simply the algebraic analogy of the the standard change-of-basepoint map used in topology. In the topological case too, one can think of the group homomorphism as factoring through a torsor, so it is not canonical. In the next chapter, we will make use of the non-canonicality of this map.

Specifically, we shall use the fact that it does not preserve extra Galois- and Hodge-theoretic structures.

3.2 A Classification Theorem for Torsors

We have now defined torsors, and have studied paths-torsors, which are the source of most of the torsors we shall see. This section is devoted to a result on the classification of torsors. Lemmata 3.5 and 3.6 follow the treatment of [19], I.5.2.

Let G be a group and let T be a left G torsor. Let Γ be a group acting on both G and T on the right in a manner compatible with the torsor action. That is, for $\gamma \in \Gamma$, $g \in G$, and $t \in T$, we insist that

$$(gt)^{\gamma} = g^{\gamma} t^{\gamma}$$

For a fixed $t_0 \in T$, the action of Γ on T yields a map

$$\Gamma \longrightarrow T$$

given by $\gamma \to t_0^{\gamma}$. On the other hand, the action of G on T yields a map

$$T \longrightarrow G$$

where $t \to (g : gt_0 = t)$. This is well-defined by the torsor axiom.

Composing these two maps gives a map ξ_0 from Γ to G given by $\xi_0(\gamma) = (g|gt_0 = t_0^{\gamma})$. Furthermore, we note that

Lemma 3.5. *The map ξ_0 described above is a 1-cocycle for Γ with coefficients in G.*

Proof. We verify the cocycle condition by direct calculation.

$$\begin{aligned} \xi_0(\gamma)^{\gamma'}\xi_0(\gamma') &= \left(g^{\gamma'}h|gt_0 = t_0^{\gamma} \text{ and } ht_0 = t_0^{\gamma'}\right) \\ &= \left(g^{\gamma'}h|g^{\gamma'}t_0^{\gamma'} = t_0^{\gamma\gamma'} \text{ and } ht_0 = t_0^{\gamma'}\right) \\ &= \xi_0(\gamma\gamma') \end{aligned}$$

□

In fact, we can go further and say that

Lemma 3.6. *The cohomology class of the cocyle ξ_0 is not dependent on the choice of $t_0 \in T$.*

Proof. Let $t_1 \in T$. There exists a unique $g_1 \in G$ such that $g_1 t_1 = t_0$. Let ξ_1 be the cocycle associated to t_1. Then

$$\begin{aligned}\xi_0(\gamma) &= \left(h \in G | h t_0 = t_0^\gamma\right) \\ &= (h | h g_1 t_1 = (g_1 t_1)^\gamma) \\ &= \left(h | h g_1 t_1 = g_1^\gamma t_1^\gamma\right)\end{aligned}$$

whence

$$\begin{aligned}\xi_0(\gamma) g_1 t_1 &= g_1^\gamma t_1^\gamma \\ &= g_1^\gamma \xi_1(\gamma) t_1 \\ \Rightarrow \xi_0(\gamma) g_1 &= g_1^\gamma \xi_1(\gamma) \\ \Rightarrow \xi_0(\gamma) &= g_1^\gamma \xi_1(\gamma) g_1^{-1} \\ \Rightarrow \xi_0(\gamma) &\equiv \xi_1(\gamma)\end{aligned}$$

as cocycles. □

Since the cohomology class of the cocycle arising from an element in a torsor depends not on the choice of the element, but only on the torsor itself, we can talk about the cocycle associated to a torsor. For a torsor T, from now on, we will write ξ_T to mean the class of ξ_t for any $t \in T$. We have therefore defined a map

$$\{G\text{-torsors with a compatible } \Gamma\text{-action}\} \to H^1(\Gamma, G)$$

We observe that this map sends G, the trivial G-torsor, to the class of coboundaries. Indeed, for $g_0 \in G$, we have

$$\begin{aligned}\xi_G(\gamma) &= \left(g | g g_0 = g_0^\gamma\right) \\ \Rightarrow \xi_G(\gamma) &= g_0^\gamma g_1^{-1} \qquad \forall \gamma \in \Gamma\end{aligned}$$

It will turn out that this map is injective and, with certain extra conditions, surjective. We can therefore interpret this map as a classification of G-torsors with compatible Γ-action.

3.3 The Rational Universal Cover

The second idea that we need to introduce in this chapter is the rational universal cover of a scheme, which we will denote by $\tilde{X}$. In this section we let X be Noetherian, separated, of finite type, and geometrically connected, as before, and also quasi-projective. Let b, and x be geometric points, and let the points of X underlying b and x be k-rational. We begin with the following observation.

Lemma 3.7. *Suppose X/k is quasi-projective. Then $\tilde{\tilde{X}}$ is the base-change of a pro-scheme defined over k.*

Proof. We will use the notation of [22], theorem 3. Let $\sigma, \tau \in G$. Then we have the following diagram.

$$\begin{tikzcd}
& \sigma^*\tilde{\tilde{X}} \arrow[dr, "\phi_\sigma"] & \\
\tau^*\sigma^*\tilde{\tilde{X}} \arrow[ur, "\sigma\phi_\tau"] \arrow[rr, "\phi_{\sigma\tau}"] & & \tilde{\tilde{X}}
\end{tikzcd}$$

where $\sigma^*\tilde{\tilde{X}}$ is defined to be the inverse limit over the system defined by applying σ^* (as in [22]) to every scheme and morphism in the system defining $\tilde{\tilde{X}}$. The rational basepoint $\tilde{b} \in \tilde{\tilde{X}}$ is fixed by G, so the triangle above must commute since, by lemma 2.13, $\tilde{\tilde{X}}$ is initial among pointed covers.

By the definition of a morphism of $\tilde{\tilde{X}}$, we know that, for any (Y, y) in the system defining $(\tilde{\tilde{X}}, \tilde{b})$, there is some (Y', y') covering (Y, y) such that the descent datum for $(\tilde{\tilde{X}}, \tilde{b})$ defines a descent datum for (Y', y'). We conclude that the corresponding diagrams for Y' commute. Since X is quasi-projective, so is Y'. We conclude that Y' is the base change of a cover defined over k, and since such (Y', y') are cofinal in $\tilde{\tilde{X}}$, we are done.

□

Definition 16. We define the pointed *rational universal cover* of a scheme over a field k to be

$$(\tilde{X}, \tilde{x}, \theta_k) := \varprojlim (Y, y, \phi)$$

where this limit is taken over all pointed etale covers $\phi : (Y, y) \to (X, x)$ such that (Y, y) and ϕ are defined over k.

Once again, the commutativity of all triangles in this system follows from lemma 2.8. As for $\tilde{\tilde{X}}$, we can prove that $\tilde{X}$ has the following properties. We assume that X is again quasi-projective.

Lemma 3.8. *1. Let $\tilde{b} \in \tilde{X}_b$. Then $(\tilde{X}, \tilde{b})$ is initial among rationally pointed rational covers of (X, b).*

2. $\tilde{X} \times_k \bar{k} = \tilde{\tilde{X}}$. That is, the base change of the rational universal cover is the universal cover. Here $\tilde{X} \times \bar{k}$ means $\varprojlim(Y \times K)$ where Y is an etale cover of X that is defined over k and K is a finite extension of k. This limit is again over pointed maps of pointed schemes.

Proof. The proof of the first statement is nearly identical to lemma 2.13.

For the second, let Z be a cover appearing in $\tilde{\tilde{X}}$. (We ignore points for clarity.) By lemma 3.7, it is covered by the base-change of a cover defined over k, say $Z' \times_X K$. Then Z' appears in the system $\tilde{X}$, so $Z' \times K$ appears in $\tilde{X} \times \bar{k}$. The identity map from the copy of $Z' \times K$ in $\tilde{X} \times K$ to the copy in $\tilde{\tilde{X}}$ defines a map from $\tilde{X} \times \bar{k}$ to $\tilde{\tilde{X}}$.

Conversely, let $Z \times K$ be a cover appearing in $\tilde{X}$. Then Z appears in $\tilde{\tilde{X}}$, and $Z \times K$ is a finite cover of Z, so $Z \times K$ is a finite cover of X and appears in $\tilde{\tilde{X}}$. The identity map from the copy of $Z \times K$ in $\tilde{\tilde{X}}$ to the copy in $\tilde{X} \times \bar{k}$ defines a map $\tilde{\tilde{X}}$ to $\tilde{X} \times \bar{k}$.

One composition of these maps is an endomorphism of $\tilde{\tilde{X}}$ which is the identity on the system $Z \times K$ where Z is rational. This system is cofinal by lemma 3.7, so this composition is $Id_{\tilde{\tilde{X}}}$. The other composition is, by a similar observation, $Id_{\tilde{X} \times \bar{k}}$.

□

We are now in a position to summarise, in a visually appealing form, the main results that are of interest to us.

Lemma 3.9. *Let K be a finite separable extension of k. We have the following canonical isomorphisms.*

1. $\overline{\widetilde{\mathrm{Spec}(k)}} \cong \mathrm{Spec}(\bar{k})$

2. $\overline{\widetilde{(X \times K)}} \cong \tilde{\bar{X}}$

Proof. 1. The connected etale covers of $\mathrm{Spec}\, k$ are simply the spectra of finite separable extensions of k. Let $Y = \mathrm{Spec}\, K$ be such a scheme. A geometric point y of Y is a map $\mathrm{Spec}\, \bar{k} \to Y$. It is therefore clear that the geometric points of Y correspond to the maps from $(\mathrm{Spec}\, \bar{k}, Id)$ to Y. In other words, $(\mathrm{Spec}\, \bar{k}, Id)$ satisfies the universal property of the pointed universal cover. Then the result follows by the uniqueness property.

2. We first give a map from $\tilde{\bar{X}}$ to $\overline{\widetilde{(X \times K)}}$. A general cover of $X \times K$ is, by base-change and composition, also a cover of X. So we map the copy in $\tilde{\bar{X}}$ to that in $\overline{\widetilde{X \times K}}$ by the identity. Conversely, covers of the form $Y \times K$ (where Y covers X) are cofinal in $\tilde{\bar{X}}$ by base-change, and are also covers of $X \times K$ by the property of the fibre product. Thus we can define a map from $\overline{\widetilde{X \times K}}$ to $\tilde{\bar{X}}$ by sending such covers in the former to themselves in the latter by the identity. These maps compose to give the identity on a cofinal subsystem of each inverse system, so they are mutually inverse.

□

We end this section with a result that will allows us to facilitate the computation of the Galois actions on fundamental groups. Let b be a rational basepoint of X, and let $\bar{b} \in \bar{X}_b$.

Lemma 3.10. $\tilde{X}_b \cong \tilde{\bar{X}}_{\bar{b}}$

Proof. We first claim that we can identify $\mathrm{Aut}_{\bar{X}}(\tilde{\bar{X}})$ with $\mathrm{Aut}_X(\tilde{X})$.

Indeed, to give an automorphism of $\tilde{\bar{X}}$ that preserves $\bar{X}$ is to give a compatible collection of automorphisms of each cover in $\tilde{\bar{X}}$ that act as the identity on maps of the form $X \times K \to X$.

Since the system $Y \times K \to X$, where Y is a rational cover of X, is cofinal in $\tilde{\bar{X}}$, this amounts to giving automorphisms of $Y \times K$ that are K-invariant. By the properties of fibre products, this is the same as giving a compatible collection of automorphisms of $Y \to X$ defined over k. Such a collection is precisely an automorphism of $\tilde{X}$ over X.

Now we conclude that

$$\tilde{\bar{X}}_{\bar{b}} \cong \mathrm{Aut}_{\bar{X}}(\tilde{\bar{X}}) \cong \mathrm{Aut}_X(\tilde{X}) \cong \tilde{X}_b$$

The first equality relies on the universal property of the pointed universal cover, the second follows from the claim above, and the third follows from the universal property of the pointed rational universal cover. □

We can use the identification above to calculate the Galois action of $G := Gal(\bar{k}/k)$ on $\pi_1(\bar{X}, \bar{b})$. Combining lemmata 2.16 and 3.10, we obtain

$$\pi_1(\bar{X}, \bar{b}) \cong \tilde{\bar{X}}_{\bar{b}} \cong \tilde{X}_b$$

G acts on the category of rational etale covers of (X, b). This yields a map

$$G \to \mathrm{Aut}(\tilde{X}_b)$$

and thence an action on $\pi_1(\bar{X}, \bar{b})$, which, we hope, is more tractable than following the original definition via the action on each cover and thence on the fibre functor and its automorphisms.

Explicitly, we can describe the action in the following terms. Firstly, if $b \in X(k)$, then the data of $\bar{b} \in \bar{X}_b$ includes a morphism $\bar{k} = k(\bar{b}) \to \bar{k}$. This will be affected by G, so that $\bar{b}$ is not G-invariant. However, b itself includes only a morphism $k = k(b) \to \bar{k}$, so is G-invariant.

Let

$$\Omega : \pi_1(\bar{X}, \bar{b}) \to \tilde{\bar{X}}_{\bar{b}} \to \tilde{X}_b$$

be the identification above, given by $\Omega(\gamma) = R(\gamma(\bar{b}))$. The map Ω itself is then acted on by G, and we can calculate the action of $g \in G$ on $\gamma \in \pi_1$ by

$$\gamma^g = \{\sigma : \Omega(\sigma) = \Omega(\gamma)^g\}$$

In the language of the topological fundamental group, we are lifting loops to the universal cover and sending each loop to the end-point of this lift. If the start-point, $\tilde{b}$, of the lift is rational, then we can lift γ^g to the path that ends at the image, under g, of the end-point of the lift of γ.

3.4 Two Examples

The final section in this chapter is devoted to the construction of two simple examples illustrating the ideas developed so far.

3.4.1 The Twice Punctured Projective Line

Our first example will be the scheme $X := \mathbb{P}^1_{\mathbb{Q}} \setminus \{0, \infty\}$. We choose to work with the basepoint 1 for reasons which will be made clear later. Define $\bar{X} := X \times \bar{\mathbb{Q}} = \mathbb{P}^1_{\bar{\mathbb{Q}}} \setminus \{0, \infty\}$.

We know that the cyclic covers

$$\phi_n : \mathbb{P}^1_{\mathbb{C}} \setminus \{0, \infty\} \to \mathbb{P}^1_{\mathbb{C}} \setminus \{0, \infty\}$$

given by $\phi_n : z \to z^n$ are surjective and everywhere non-trivial on tangent planes. For a curve, this is equivalent to being etale.

Consider also the manifold $X^{an} := (\mathbb{P}^1_{\mathbb{C}} \setminus \{0, \infty\})^{an}$. We can analytify each cover ϕ_n to give a map to this manifold which is surjective and a tangent plane isomorphism. By the local isomorphism theorem, this is the same a topological covering map.

Furthermore, X^{an} is homotopic to S^1, and so has fundamental group $\mathbb{Z}$. Since finite covering maps correspond to finite quotients of $\mathbb{Z}$, we deduce that the ϕ^{an} are (up to homeomorphism) all of the covering maps of X^{an}. Then, since any other etale cover of $\mathbb{P}^1_{\mathbb{C}} \setminus \{0, \infty\}$ would analyitify to yield a new covering map of X^{an}, we conclude that the ϕ_n are (up to biholomorphism) all of the etale covers of $\mathbb{P}^1_{\mathbb{C}} \setminus \{0, \infty\}$.

Next, we observe that all of these covers can be defined over $\bar{\mathbb{Q}}$, and even over $\mathbb{Q}$. That is, there are covers $\theta_n : X \to X$ given by $\theta_n : z \to z^n$ such that $\bar{\theta}_n := \theta_n \times \bar{\mathbb{Q}}_p$ give etale covers of $\bar{X}$, and $\bar{\theta}_n \times \mathbb{C} = \phi_n$. Again, there cannot be (up to isomorphism) any more etale covers of $\bar{X}$, as any such covers would base change to give etale covers of $\mathbb{P}^1_{\mathbb{C}} \setminus \{0, \infty\}$, and we know that the covers ϕ_n are cofinal here.

We observe that the preimage of the basepoint 1 under the cover θ_n is the set μ_n of n^{th} roots of unity in $\bar{Q}$. Let $\bar{1}$ be some lift of this basepoint to $\bar{X}$. We can use lemma 3.10 to identify

$$\tilde{\bar{X}}_{\bar{1}} \cong \tilde{X}_1 \cong \varprojlim \mu_n$$

The action of $G := Gal(\bar{Q}/Q)$ on $\varprojlim \mu_n$ is given by the cyclotomic character, and we can therefore use lemma 3.10 to write

$$\pi_1(\bar{X}, \bar{1}) \cong \varprojlim \mu_n$$

as groups with G-action.

3.4.2 An Elliptic Curve

Let $E/\mathbb{Q}$ be an elliptic curve. Let $Y \xrightarrow{\phi} \bar{E}$ be any etale cover of $\bar{E} := E \times \bar{\mathbb{Q}}$ and let $\bar{0}$ lie over 0. By the Riemann-Hurwitz Theorem, we have

$$2g_Y - 2 = deg(\phi)(2g_{\bar{E}} - 2) + \sum[\text{ramification terms}]$$

The genus of $\bar{E}$ is 1, and we can ignore the ramification terms since ϕ is etale, whence we conclude that $g_Y = 1$.

If we now choose any $y \in \phi^{-1}(\bar{0})$, we can give (Y, y) the structure of an elliptic curve. Then ϕ becomes a non-zero isogeny, and so there exists some n and a dual isogeny

$$\phi^\vee : (\bar{E}, \bar{0}) \to (Y, y)$$

such that $\phi^\vee\phi = [n]$, multiplication by n on $\bar{E}$. By [14], theorem 8.2 or similar, we know that $[n]$ itself is etale, and we have just shown that it covers the (aritrary) cover ϕ. Hence the system

$$[n] : \bar{E} \to \bar{E}$$

is cofinal in the system of all etale covers of $\bar{E}$, and we can use it to study $\tilde{\bar{E}}$.

For E to be defined over $\mathbb{Q}$ as an abelian variety, we must have $0 \in E(\mathbb{Q})$. Clearly the system $[n]$ on $\bar{E}$ descends to $[n]$ on E. Thus we can identify

$$\pi_1(\bar{E}, \bar{0}) \cong \tilde{\bar{E}}_{\bar{0}} \cong \tilde{E}_0$$

and, again, this identification is compatible with the action of G.

Now we write $([n])^{-1}(0) \cong E[n]$ for the n-torsion elements, so that

$$\tilde{E}_0 \cong \varprojlim E[n] \cong T(E)$$

Thus studying the G-structure on $\pi_1(\bar{E}, \bar{0})$ is the same as studying the G-structure on $T(E)$.

Chapter 4

On Certain Properties of Twists

4.1 On Twists

We begin this section by introducing the second of our main ingredients.

Let Π be a group and let G be a group acting on Π. A G-twist of Π, roughly speaking, is an alternative action of G on Π. Alternatively, we can consider it to be a group with an action of G that is isomorphic to Π in the category of groups, but is not necessarily so in the category of G-groups.

Formally, we have the following definition.

Definition 17. Let Π be a group. Let G be a group acting on Π.

A G-twist of Π is a group T, with an action of G, such that there exists a group isomorphism

$$\phi : T \longrightarrow \Pi$$

We note that for a homomorphism ϕ as above, we must in general distinguish between pre- and post-composition with the action of an element of G.

The former takes data from only the action of G on T; and the latter takes data from only the action of G on Π.

Since ϕ is a homomorphism relating Π and T, it is natural to let G act on ϕ by conjugation, thus capturing the data of both actions above. We define

$$\phi^g := g\phi g^{-1} : T \to \Pi$$

for each $g \in G$.

Our first aim in this chapter is to discuss an algebraic description of these twists. We begin by associating a cocycle to a pair (T, ϕ) as above, of a twist and an isomorphism describing it as a twist.

Lemma 4.1. *Let G, Π, and T be as above. Then the map*

$$G \longrightarrow \mathrm{Aut}(\Pi)$$

given by $g \to \phi_g := \phi^g \phi^{-1}$ is a 1-cocycle of G.

Proof. Let $g, h \in G$. We have

$$\begin{aligned} g(\phi_h)\phi_g &= g\phi_h g^{-1}\phi_g \\ &= (gh\phi h^{-1}\phi^{-1}g^{-1})(g\phi g^{-1}\phi^{-1}) \\ &= gh\phi h^{-1}g^{-1}\phi^{-1} \\ &= \phi_{gh} \end{aligned}$$

□

In fact, the cocycle produced is independent, up to coboundary, of the choice of isomorphism ϕ used to express the twisting relationship.

That is, if $\theta : T \to \Pi$ is another isomorphism expressing the twist, then the cocyle $g \to \theta_g$ differs from the cocycle $g \to \phi_g$ only by a coboundary. Formally, we have the following lemma.

Lemma 4.2. *Let G, Π, T, ϕ, and θ be as above. Then the cohomology classes of $g \to \phi_g$ and $g \to \theta_g$ agree.*

Proof. We have a commutative triangle as follows.

$$\begin{tikzcd} & T \arrow[dl, "\theta"'] \arrow[dr, "\phi"] & \\ \Pi \arrow[rr, "\phi\theta^{-1}"'] & & \Pi \end{tikzcd}$$

The cocycle associated to θ is

$$g \to \theta_g = g\theta g^{-1}\theta^{-1}$$

while the cocycle associated to $\phi = \phi\theta^{-1}\theta$ is

$$\begin{aligned} g \to \phi_g &= g\phi g^{-1}\phi^{-1} \\ &= g\phi\theta^{-1}\theta g^{-1}\theta^{-1}\theta\phi^{-1} \\ &= (g\phi\theta^{-1}g^{-1})(g\theta g^{-1}\theta^{-1})(\theta\phi) \\ &= (\phi\theta^{-1})^g\theta_g(\phi\theta)^{-1} \end{aligned}$$

Since $\phi\theta^{-1} \in \mathrm{Aut}(\Pi)$, we see that ϕ_g is related to θ_g by a coboundary. □

We can interpret this result as allowing us to define a map from the set of G-twists of Π to the set $H^1(G, \mathrm{Aut}\,\Pi)$.

Note that, the cocycles produced by this process express the difference between the actions of G on two groups related by any twisting isomorphism. In particular, it follows that an automorphism of Π itself yields the trivial cohomology class, even if it is not G-equivariant.

It is reasonable to ask if this map is injective or surjective. However, as we shall only be concerned with a specific subset of these twists, such questions are not immediately relevant here.

Indeed, we shall concern ourselves mostly with the set of 'geometric' twists; that is, twists which arise geometrically. Formally, we make the following definition.

Definition 18. Let $G := Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. Let b be a chosen geometric basepoint on X, tangential or otherwise. Let $\Pi := \pi_1(X, b)$.

Then a geometric twist of Π is a G-twist T of Π such that there exists a geometric point x on X with

$$T \cong_G \pi_1(X, x)$$

as G-groups.

For any geometric point x on X, and for any path $p \in \pi_1(X, x, b)$, there is an isomorphism

$$\pi_1(X, x) \longrightarrow \pi_1(X, b)$$

given by $\gamma \to p\gamma p^{-1}$. We make two observations.

1. The map above factors as

$$\begin{tikzcd} \pi_1(X,x) \arrow[r, "\gamma\to\gamma p^{-1}"] \arrow[d, "\gamma\to p\gamma"'] & \pi_1(X,b,x) \arrow[d, "\gamma\to\gamma p"] \\ \pi_1(X,x,b) \arrow[r, "\gamma\to\gamma p^{-1}"'] & \pi_1(X,b) \end{tikzcd}$$

   Either route from $\pi_1(X, b)$ to $\pi_1(X, x)$ factors through a torsor set. Since a set cannot be canonically isomorphic to a group, we do not expect these two fundamental groups to be canonically isomorphic. That is, while they are isomorphic as groups, we ought not to expect them to have identical G-actions. They are, in fact, G-twists.

   Indeed, our main theorem may be interpreted as a statement on the injectivity of the set of geometric points of X into the set of G-twists of $\pi_1(X, b)$.

2. There are many choices of path $p \in \pi_1(X, x, b)$, and none of them need be G-invariant.

   However, for any path p, we get a map expressing a twisting relationship between fundamental groups. Hence any path p yields a cocycle, with coefficients in $\mathrm{Aut}(\Pi)$, associated to $\pi_1(X, x)$, and hence to the point x.

   An obvious corollary of lemma 4.2 is that the cohomology class of the resulting cocycle is independent of the choice of p.

   Thus we have produced a map

$$X(\mathbb{Q}_p) \longrightarrow H^1(G, \mathrm{Aut}(\Pi))$$

   The next section will involve the study of an algebraic description of these geometric twists.

4.2 Inner Twists

We summarise and review the two main structures established so far.

To a geometric point x on X we have associated a G-torsor of Π by

$$x \longrightarrow \pi_1(X,x,b)$$

and also a G-twist of Π by

$$x \longrightarrow \pi_1(X,x)$$

To the former we can associate a 1-G-cocycle with coefficients in Π. Though this cocycle depends on the choice of a path from x to b, its cohomology class does not.

To the latter we can associate a 1-G-cocycle with coefficients in $\operatorname{Aut}\Pi$. Though this cocycle depends on a choice of an isomorphism of fundamental groups, which can be specified by a choice of a path from x to b, its class does not.

Geometrically, we can relate the torsor associated to x and the twist associated to x by

$$\begin{array}{ccc} \pi_1(X,x,b) & \longrightarrow & \pi_1(X,x) \\ \gamma & \longrightarrow & p\gamma \end{array}$$

for any path p.

$$\begin{tikzcd} & x \arrow[dl] \arrow[dr] & \\ \pi_1(X,x,b) \arrow[rr, "\gamma\to p\gamma"'] & & \pi_1(X,x) \end{tikzcd}$$

However, since we also have cohomology descriptions of the torsor and the twist associated to x, it is natural to ask whether we can find an algebraic map, acting on cohomology, relating these objects.

$$\begin{tikzcd} & x \arrow[dl] \arrow[dr] & \\ \{g \to \gamma | \gamma p = p^g\} \arrow[rr, dashed, "?"'] & & \{g \to \phi_g\} \end{tikzcd}$$

(ϕ, as before, expressing the twisting relationship.)

In fact, we claim that the required map arises from conjugation in Π, in the following way. Let

$$c : \Pi \longrightarrow \operatorname{Aut}\Pi$$

be the conjugation map, given by $\gamma \to (\sigma \to \gamma\sigma\gamma^{-1})$. This functorially yields a map, defined by post-composition with c,

$$H^1(c) : H^1(G, \Pi) \longrightarrow H^1(G, \operatorname{Aut}\Pi)$$

that we can think of as taking torsors to twists. Indeed, we verify that this is the map that we require: that it takes the geometric torsor associated to x to the geometric twist associated to x.

Lemma 4.3. *Let x be a geometric point on X. The map $H^1(c)$ defined above carries the class of the cocycle of $\pi_1(X, x, b)$ to the class of the cocycle of $\pi_1(X, x)$.*

Proof. We have established in lemmata 3.6 and 4.2 that we can use any isomorphism

$$\phi : \pi_1(X, x) \longrightarrow \pi_1(X, b)$$

and any path

$$p \in \pi_1(X, x, b)$$

to define the associated cocycles. So we choose a path p and use the isomorphism defined by $\phi(\gamma) := p\gamma p^{-1}$.

Then the cocycle associated to $\pi_1(X, x)$ sends $g \in G$ to ϕ_g. This acts on a loop $\tau \in \pi_1(X, b)$

as

$$\begin{aligned}
(\phi^g \phi^{-1})(\tau) &= (g\phi g^{-1}\phi^{-1})(\tau) \\
&= g\phi g^{-1}(p^{-1}\tau p) \\
&= g\phi(g^{-1}(p^{-1})g^{-1}(\tau)g^{-1}(p)) \\
&= g(pg^{-1}(p^{-1})g^{-1}(\tau)g^{-1}(p)p^{-1}) \\
&= g(p)p^{-1}\tau p g(p^{-1}) \\
&= \{\sigma p p^{-1}\tau p(\sigma p)^{-1} | \sigma p = p^g\} \\
&= \{\sigma\tau\sigma^{-1} | \sigma p = p^g\} \\
&= \{H^1(c)(\sigma) | \sigma p = p^g\}(\tau)
\end{aligned}$$

Since this holds for all $\tau \in \pi_1(X, b)$, we can identify the functions

$$\phi_g \cong \left(H^1(c)\right)(\sigma p = p^g)$$

where we recognise the argument on the right as the cocycle associated to $\pi_1(X, x, b)$. □

In summary, we have asserted that the lower square in the following diagram commutes. Here the top square represents the functor $H^1(G, -)$. The bottom arrow from the set of 'geometric torsors' to 'geometric twists' carries the torsor associated to a rational basepoint to the twist associated to the same basepoint.

$$\begin{tikzcd}
\Pi \arrow[rr, "c:\gamma\to(\tau\to\gamma\tau\gamma^{-1})"] \arrow[d, dashed, "H^1"'] \arrow[drr, phantom, "{\downarrow H^1}"] & & \mathrm{Aut}\,\Pi \arrow[d, dashed, "H^1"] \\
H^1(G, \Pi) \arrow[rr, "H^1(c)"'] & & H^1(G, \mathrm{Aut}\,\Pi) \\
\{\text{Geometric Torsors}\} \arrow[u] \arrow[rr, "\pi_1(X,x,b)\to\pi_1(X,x)"'] & & \{\text{Geometric Twists}\} \arrow[u]
\end{tikzcd}$$

Chapter 5

Previous Results

Overview

5.1 The Work of Nakamura, Tamagawa, and Mochizuki

A slightly related class of problems was studied by Nakamura, Tamagawa, and Mochizuki, as outlined in [17]. Specifically, for various fields k, they considered the 'augmented π_1' of hyperbolic schemes U/k. (Here, $\pi_1(U)$ is the fundamental group based at the generic point of U, which is isomorphic to $Gal(k(U))$.) By constructing from this data certain invariants of the field $k(U)$, they were able to prove various theorems on the rigidity of this profinite fundamental group.

For example, in [15], Mochizuki proved a result which includes the following statement. For any smooth algebraic variety S and a hyperbolic X, both defined over a sub-p-adic field k, the natural map

$$\mathrm{Hom}_k^{dom}(S, X) \to \mathrm{Hom}_{Gal(k)}^{open}(\pi_1(S), \pi_1(X))/c(\pi_1(\bar{U}))$$

is a bijection. Here Hom^{dom} denotes the set of dominant morphisms. The 'open' superscript on the right denotes the set of open homomorphisms (using the profinite topology), while the $Gal(k)$ subscript denotes the restriction that these morphisms are compatible with the given augmentation maps. These homomorphisms are considered modulo conjugation by elements of $\pi_1(\bar{U})$, the geometric fundamental group.

This establishes the strong, (Hom) form of Grothendieck's anabelian conjecture for curves. By restricting to isomorphisms on both sides, we obtain a classification of hyperbolic curves by their fundamental groups.

5.2 The Work of Hain

5.2.1 Analogy

Let M be a differentiable manifold. For any points b and x we can define the topological fundamental groups $\pi_1(M, b)$ and $\pi_1(M, x)$ and the paths torsor $\pi_1(M, x, b)$ as in Chapter 2.

By conjugating a (class of) loops in $\pi_1(M, b)$ with a path from x to b, we obtain a (class of) loops at x.

This association is clearly invertible, and can easily be seen to be a group isomorphism. Hence, any two fundamental groups on M are 'intrinsically' isomorphic. (That is, they are isomorphic as groups.)

However, a differentiable manifold has more structure than the underlying topological space. It is reasonable to ask if this extra structure can descend to the fundamental group; and, if it can, to ask whether this additional structure is sufficient to distinguish the different fundamental groups.

This section follows the development in [7].

5.2.2 Hodge Strucure on π_1

We can attempt to use the Hodge filtration on $H^1(M)$ to induce a Hodge filtration on $\pi_1(X, b)$. However, the usual line integral, sending a loop γ to the map $\omega \to \int_\gamma \omega$ can only 'see' those elements of $\pi_1(M, b)$ visible in $H_1(M)$. Indeed, this map must factor through the abelianisation of $\pi_1(M, b)$. We note that $H_1(M)$ has a basepoint-free definition, so we cannot use line integrals to distinguish the fundamental groups associated to different basepoints.

We can, however, use the iterated integrals introduced by Chen for this purpose. In the formulation introduced here, iterated integrals may be viewed as generalisations of the usual line integrals which are capable of seeing many elements of π_1 that vanish in H_1. This allows us to put a mixed Hodge structure on π_1 and on its derived groups which lifts the Hodge structure on H_1. We can then hope that this provides sufficient structure on π_1 to allow us to distinguish the fundamental groups associated to different basepoints.

5.2.3 What is Possible

We refer the reader to [4], section 2, for a review of Deligne's theory of Mixed Hodge Strucutres and extensions in this category.

With this construction in place, Hain formulates the first main theorem of [7] as follows. Let $J(M,t)$ denote the augmentation ideal of the group ring $\mathbb{Z}[\pi_1(M,t)]$. We denote it by J alone where V and t are understood.

Theorem (Hain)**.** *If $V := \mathbb{P}^1 \backslash \{a_1, ..., a_n\}$, then the polarised mixed Hodge structure on $J(V,t)/J^3$ determines (V,t) up to biholomorphism.*

For $n = 1$ or $n = 2$, the result is trivial. Indeed, for any (V,t_1) and (V,t_2), there is a Mobius transformation carrying t_1 to t_2 and preserving a_1 (and a_2). This invertible map of differentiable manifolds must induce an invertible map of fundamental groups with all additional structures, and hence an invertible map from the mixed Hodge structure on $J(V,t_1)/J^3$ with the mixed Hodge structure on $J(V,t_2)/J^3$. The case of $n \geq 4$ follows trivially from the case of $n = 3$. We therefore outline only the main case, in which $n = 3$.

Hain begins with the assertion that the sequence

$$0 \longrightarrow J/J^2 \otimes J/J^2 \xrightarrow{i} J/J^3 \xrightarrow{p} J/J^2 \longrightarrow 0$$

is exact, for any basepoint t. Here i is given by $i(a \otimes b) = a \times b$ (well-defined up to J^3) and p is projection. Dualising, we obtain the following exact sequence.

$$0 \longrightarrow (J/J^2)^\vee \xrightarrow{p^*} (J/J^3)^\vee \xrightarrow{i^*} (J/J^2)^\vee \otimes (J/J^2)^\vee$$

We can identify J/J^2 with the singular homology group $H_1(V,\mathbb{Z})$, and hence $(J/J^2)^\vee$ with $H^1(V,\mathbb{Z})$. Now the image of i^* may be identified with the kernel of the first cup product on

$H^*(V,\mathbb{Z})$, and since $H^2(V,\mathbb{Z}))$ is trivial, we conclude that i^* is surjective. We can thus assert that the following sequence is exact.

$$0 \longrightarrow H^1(V,\mathbb{Z}) \longrightarrow \mathrm{Hom}(J/J^3,\mathbb{Z}) \longrightarrow H^1(V) \otimes H^1(V,\mathbb{Z}) \longrightarrow 0$$

This is therefore an extension of mixed Hodge structures. Moreover, it is a separated extension of mixed Hodge structures. We recall the following definitions, following [4].

Definition 19. A separated extension of mixed Hodge structures is an exact sequence

$$0 \longrightarrow A \longrightarrow X \longrightarrow B \longrightarrow 0$$

of mixed Hodge structures, where A is pure of weight m, B is pure of weight n, and where $n > m$.

Definition 20. Two separated extensions of mixed Hodge structures are congruent if there exists an isomorphism of mixed Hodge structures $\phi : X_1 \to X_2$ such that the following diagram commutes.

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, equal] & X_1 \arrow[r] \arrow[d, "\phi"] & B \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & A \arrow[r] & X_2 \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$

Note that separatedness is a condition on A and B only, so that the set of (congruence classes of) separated extensions of B by A is the same as the set of (congruence classes of) extensions of B by A.

We note also that mixed Hodge structures form an abelian category. Thus for fixed mixed Hodge structures A and B, congruence classes of extensions of B by A naturally form a group under Baer sum, as outlined in [21], Corollary 3.4.5.

The importance to us of separatedness lies in the following result of Carlson (See [4].)

Lemma 5.1. *Let A, B be as above. Then there is a canonical, functorial group isomorphism*

$$\phi : Ext^1_F(B,A) \cong \frac{\mathrm{Hom}_{\mathbb{C}}(B,A)}{F^0\,\mathrm{Hom}_{\mathbb{C}}(B,A) + \mathrm{Hom}_{\mathbb{Z}}(B,A)}$$

Here $\mathrm{Hom}_{\mathbb{Z}}$ means morphisms respecting the integral lattice underlying the Hodge structure, and $F^0\,\mathrm{Hom}$ means morphisms respecting the Hodge filtration of the Hodge structure. The subscript F indicates that we consider the extensions in the category of mixed Hodge structures.

The proof of this lemma uses separatedness to show that any extension is congruent to some 'normalised' extension, that is, an extension such that

$$X_{\mathbb{Z}} \cong A_{\mathbb{Z}} \oplus B_{\mathbb{Z}}$$

ϕ may be defined as follows.

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "i"'] & X \arrow[l, bend right, "r_{\mathbb{Z}}"'] \arrow[r, "p"'] & B \arrow[l, bend right, "s_F"'] \arrow[r] & 0 \end{tikzcd}$$

If X as above is an extension, choose an integral retraction $r_{\mathbb{Z}}$ of i and a Hodge filtration-preserving splitting s_F of p. The composition of these two maps will produce a map from B to A well-defined up to $F^0\,\mathrm{Hom}_{\mathbb{C}}(B,A)+\mathrm{Hom}_{\mathbb{Z}}(B,A)$. If we restrict our attention to only normalised extensions, it is possible to show that the map ϕ in the lemma above is an isomorphism.

The proof of Hain's theorem now proceeds as follows. We are given the data of $J(V,t)/J^3$ with its polarised Hodge structure.

From the product in J/J^3, we can recover the sequence

$$0 \longrightarrow H^1(V) \longrightarrow \mathrm{Hom}(J/J^3,\mathbb{Z}) \longrightarrow H^1(V)\otimes H^1(V) \longrightarrow 0$$

which we know to be exact. The cohomology group $H^1(V)$ may be defined without regard to the basepoint t. We can therefore view the association

$$(V,t) \longrightarrow \left\{0 \to H^1 \to (J/J^3)^\vee \to H^1\otimes H^1 \to 0\right\}$$

as a map from the points of V to the group $\mathrm{Ext}^1(H^1\otimes H^1, H^1)$

$$V(\mathbb{C}) \longrightarrow \mathrm{Ext}^1_F(H^1\otimes H^1, H^1)$$

We stress again that the subscript F indicates that the extensions are considered in the category of mixed Hodge structures. Indeed, our earlier observation that all of the fundamental groups on V are intrinsically isomorphic may be reinterpreted in this formulation as saying that the composition

$$V(\mathbb{C}) \longrightarrow \mathrm{Ext}^1_F(B, A) \longrightarrow \mathrm{Ext}^1(B, A)$$

where the second Ext is in the category of $\mathbb{C}$-algebras on integral lattices or anything coarser, is trivial.

We now proceed with the outline of Hain's theorem.

The polarisation on J/J^3 allows us to pick out an integral basis for $(J/J^3)^\vee$ and for H^1. This enables us to construct the integral retraction $r_\mathbb{Z}$ expicitly.

Hain then applies Chen's π_1 theorem and his previous results on the Hodge structure of J/J^3 to construct the splitting s_F.

Combining these yields a map μ from which Hain is able to recover the cross ratio of the points $\{a_1, a_2, a_3, t\}$. This proves the theorem in the case $n = 3$.

Indeed, as the biholomorphisms of $\mathbb{P}^1$ are mobius transformations, the biholomorphisms of $\mathbb{P}^1 \setminus \{a_1, a_2, a_3\}$ are the six mobius transformations that permute the set $\{a_1, a_2, a_3\}$. Let ϕ be one such map. Then $\pi_1(\phi) : \pi_1(V, t) \to \pi_1(V, \phi(t))$ induces a morphism of Hodge structures from $J(t)/J^3$ to $J(\phi(t))/J^3$. This is invertible because ϕ itself is. The six possible choices for $\phi(t)$ are the points such the the cross ratio $< a_1, a_2, a_3, \phi(t) >$ agrees with the cross ratio $< a_1, a_2, a_3, t >$.

For such $\phi(t)$, we cannot hope to distinguish the fundamental groups $\pi_1(V, \phi(t))$ from one another, even by considering additional structures. If, therefore, we can distinguish such $\phi(t)$ from all other points, it may be viewed as the best possible result.

5.2.4 What is Not Possible

It would seem reasonable to attempt a similar theorem in the arithmetic case.

We can reduce the problem to considering only $(a_1, a_2, a_3) = (0, 1, \infty)$, as for any other triple, there is a Möbius map carrying it to $(0, 1, \infty)$. Let $X := \mathbb{P}^1_{\bar{\mathbb{Q}}_p} \setminus \{0, 1, \infty\}$.

In adapting the proof given by Hain for the analytic case above, we can again prove that the sequence

$$0 \longrightarrow J/J^2 \otimes J/J^2 \xrightarrow{i} J/J^3 \xrightarrow{p} J/J^2 \longrightarrow 0$$

is exact, where J is now the augmentation ideal of, say, the $\mathbb{Q}_p$-algebra of the unipotent fundamental group $\pi_1^u(X,t)$.

We can dualise and proceed exactly as above, and we find that the sequence

$$0 \longrightarrow H^1_{et}(V,\mathbb{Q}_p) \longrightarrow \mathrm{Hom}(J/J^3,\mathbb{Q}_p) \longrightarrow H^1_{et}(V,\mathbb{Q}_p) \otimes H^1_{et}(V,\mathbb{Q}_p) \longrightarrow 0$$

is exact. We now encounter two problems.

Firstly, in constructing the unipotent group, we have applied the Malcev functor $\otimes\mathbb{Q}$. As described, this generalises the standard tensorisation functor. This has the effect of destroying the integral structure of the original group. Thus there is no clear substitute for the integral retraction $r_{\mathbb{Z}}$.

Secondly, our (perhaps rather naive) substitute for the Hodge structure on the topological fundamental group π_1^{top} of a manifold is the Galois structure of the unipotent etale fundamental group π_1^u on X. Then the natural analogue for the Hodge filtration preserving splitting s_F above would be a Galois equivariant splitting s_G of this new p^*. It is a consequence of one of our later results that such a splitting cannot exist for general basepoints.

Chapter 6

The Unipotent Fundamental Group

Overview

The full, profinite, fundamental group of even a simple scheme can be an extremely intractable and mysterious object.

For example, Grothendieck famously called $\pi_1^{et}(\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\})$ 'the most interesting object in mathematics'.

It is an extension of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ by $\widehat{\mathbb{F}_2}$ (the completion of the free group on two generators), and Belyi proved in [1] that this extension is sufficiently non-trivial that even the natural outer representation is injective.

Fix a prime p. We shall be concerned with just the fundamental group of $\mathbb{P}^1_{\bar{\mathbb{Q}}_p} \setminus \{0, 1, \infty\}$, for various basepoints. The Galois theory of the local field $\mathbb{Q}_p$ is better understood, which simplifies the task of understanding the Galois action.

As even this simpler fundamental group is quite hard to deal with, we shall attempt to replace it with a 'linearised' version which is, on one hand, simpler to study and, on the other hand, still sufficiently rich for our needs.

We also consider in this chapter the maximal pro-p quotient of the profinite etale fundamental group. In particular, we wish to relate the structure of this group to that of the $\mathbb{Q}_p$-unipotent completion.

6.1 Construction

In this section, we provide a construction of the $\mathbb{Q}_p$-unipotent completion, U, of $\pi_1^{et}(\bar{X})$. We also review some basic properties of this object. We follow here the treatments in [8], Appendix A, and [18], Appendix A.3.

We make the following definitions.

Definition 21. Let Γ be a group. The unipotent completion of Γ over $\mathbb{Q}$ consists of a pro-unipotent algebraic $\mathbb{Q}$-group $\Gamma^{un}_{/\mathbb{Q}}$ and a group homomorphism $\theta : \Gamma \to \Gamma^{un}_{/\mathbb{Q}}(\mathbb{Q})$. These have the universal property of being initial among all pairs (W, θ) of pro-unipotent $W/\mathbb{Q}$ and $\theta \to W(\mathbb{Q})$.

There is a natural extension of this definition to topological groups and topological fields. See [8], section A.2.

Definition 22. Let Γ be a profinite group, and $W/\mathbb{Q}_p$ an algebraic group. This implies that, in particular, the $\mathbb{Q}_p$-points of W form a group. We call a group homomorphism $\Gamma \to W(\mathbb{Q}_p)$ continuous if it is continuous with respect to the profinite topology on Γ and the topology on $W(\mathbb{Q}_p)$ induced by that on $\mathbb{Q}_p$.

Extending this, we define a group homomorphism $\theta : \Gamma \to W(\mathbb{Q}_p)$ for a pro-algebraic group W as follows. Such a map is, by definition, a compatible collection of maps $\theta_\alpha : \Gamma \to W_\alpha(\mathbb{Q}_p)$ for some inverse system $\{W_\alpha\}$ of algebraic groups defining W. We call θ continuous when each θ_α is continuous.

We can now make the following definition:

Definition 23. The p-adic unipotent completion of Γ consists of a pro-unipotent $\mathbb{Q}_p$-group $\Gamma^{un}_{/\mathbb{Q}_p}$ and a continuous map $\theta^{un} : \Gamma \to \Gamma^{un}_{/\mathbb{Q}_p}(\mathbb{Q}_p)$. These have the universal property of being initial among all pairs (W, θ) of pro-unipotent $W/\mathbb{Q}_p$ and $\theta : \Gamma \to W(\mathbb{Q}_p)$.

The p-adic unipotent completion of a profinite group, Γ, may be seen to exist, by construction:

$$\Gamma^{un}_{/\mathbb{Q}_p} := \varprojlim U_\rho$$

where this limit is taken over the inverse system of all pairs of unipotent algebraic group $U_\rho/\mathbb{Q}_p$ and Zariski-dense maps $\Gamma \to U_\rho(\mathbb{Q}_p)$. Furthermore, the universal mapping property ensures that the p-adic unipotent completion is unique (up to unique isomorphism).

We quote without proof the following comparison theorem ([8], theorem A.4).

Lemma 6.1. *If Γ is a finitely generated group with pro-p completion $\Gamma^{(p)}$ and profinite completion $\hat{\Gamma}$, then*

$$\Gamma^{un}_{/\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong (\Gamma^{(p)})^{un}_{/\mathbb{Q}_p} \cong \hat{\Gamma}^{un}_{/\mathbb{Q}_p}$$

Proof. This is [8], theorem A.4. □

For the rest of this work, we will denote the p-adic unipotent completion of $\pi_1^{et}(\bar{X})$ by U when the basepoint is clear, or otherwise by $\pi_1^{un}(\bar{X}, x)$. We will also need to understand the structure of U^{ab}.

First, recall that we can also express the abelianisation of a group H in terms of a universal mapping property. Indeed, every map from H to an abelian group factors uniquely through the abelianisation. Now we observe that both $(\Gamma^{un})^{ab}$ and $(\Gamma^{ab})^{un}$ have the same universal mapping property. Indeed, they both have the property that they uniquely factor any map from Γ to an abelian unipotent algebraic group. By uniqueness, we conclude that $U^{ab} \cong (\pi_1^{et}(\bar{X})^{ab})^{un}$.

Recall that the maximal pro-p quotient of the fundamental group satisfies $\left(\pi_1^{et}(\bar{X})^{(p)}\right)^{ab} \cong \mathbb{Z}_p^2$ as groups, and observe that the inclusion $\mathbb{Z}_p^2 \hookrightarrow \mathbb{Q}_p^2$ has the required universal mapping property to be the p-adic unipotent completion of $\mathbb{Z}_p^2$. We conclude that $U^{ab} \cong (\mathbb{Z}_p^2)^{un} \cong \mathbb{Q}_p^2$.

Note that this does not describe the Galois structure at all. By [5] or 3.4.1, we know that the Galois action on the loop γ_0 of $\pi_1^{et}(\bar{X})$, based at $\vec{t}$ and going clockwise once around 0 is by the cyclotomic character. Thus the action of G on the image of γ_0 in $\pi_1^{et}(\bar{X})^{ab}$ is also by the cyclotomic character. Recall that this abelianisation may be defined as the dual of the etale cohomology group which has a basepoint-free definition. This implies that the G-action on γ_1, the clockwise loop once around 1, is also by the cyclotomic character. Thus we have $\pi_1^{et}(\bar{X})^{(p)} \cong \mathbb{Z}_p(1)^2$ as G-groups.

(We could also have obtained this result from a direct application of lemma 6.1. Indeed, take Γ to be the (finitely generated) topological fundamental group of the thrice-punctured projective line over $\mathbb{C}$, so that $\hat{\Gamma}$ is isomorphic to the profinite etale fundamental group of the thrice-punctured projective line over $\mathbb{Q}_p$.)

Now, since the Galois action on $(\pi_1^{et})^{ab}$ is by the cyclotomic character, and since taking the unipotent completion is functorial, we conclude that the Galois action on U^{ab} is also by the cyclotomic character. We can thus write $U^{ab} \cong \mathbb{Q}_p(1)^2$ as G-groups.

In general, it is more difficult to understand the action of G on larger quotients of U. This action is an object of interest in the subsequent chapters.

6.2 Observations

We make two final observations. Firstly, we recall that every affine group scheme is a linear group scheme. Thus we conclude that we have functorially created from π_1^{et} a linear group. Thus we are justified in describing this as a 'linearisation'.

A second important reason for introducing the unipotent completion is the following well-known fact (see, for example [9], page 1), of which we shall make use in the next chapters.

Lemma 6.2. *The category of unipotent affine algebraic groups over $\mathbb{Q}_p$ (alternatively $\mathbb{Q}$) is equivalent to the category of finite dimensional nilpotent Lie algebras over $\mathbb{Q}_p$ (respectively $\mathbb{Q}$).*

Explicitly, we can pass from groups to algebras by the logarithm map and from algebras to groups by exponentiation. The Baker-Campbell-Hausdorff formula tells us the effect of the group multiplication in the algebra.

In fact, the equivalence above holds for any field of characteristic zero.

Chapter 7

First Result

7.1 Previous Results and Aims

7.1.1 The Full Fundamental Group

We are now ready to state our main aim, which we will formulate more precisely in our main theorem. From the rest of this work, we require that $p > 2$. This is necessary, in particular, for lemma 7.7 and for the calculation in section 7.2.1.

We have seen that the fundamental groups associated to a scheme via different basepoints are non-canonically isomorphic. That is, they are isomorphic as groups, but need not be isomorphic as groups with, say, the action by G induced by the action of G on the scheme, where G is the Galois group of the base field.

Nakamura proved in [16] that the fundamental group $\pi_1(X, x)$ contains sufficient data to recover the basepoint x. That, the map

$$\Omega_\infty : X(\mathbb{Q}_p) \longrightarrow \{\text{Groups with } G-\text{action}\}$$

defined by $x \to \pi_1(X, x)$ is injective, even though

$$X(\mathbb{Q}_p) \longrightarrow \{\text{Groups}\}$$

defined by $x \to \pi_1(X, x)$ sends the entire domain to the same point.

7.1.2 The Quotient of π_1 by the first derived group

On the other hand, we have the identity, in the category of groups with G-actions

$$\left(\pi_1(X,x)^{(p)}\right)^{ab} \cong H_1^{et}(X,\mathbb{Z}_p)$$

Here the right-hand group may be identified with the dual of the first etale cohomology group, again as groups with G-actions. Observe that the right hand side thus has a basepoint-free definition. Hence we conclude that the map

$$\Omega_1 : X(\mathbb{Q}_p) \longrightarrow \{\text{Groups with } G - \text{action}\}$$

given by $x \to \left(\pi_1(X,x)^{(p)}\right)^{ab}$ sends the entire domain to a single point.

This result could be expected by a believer in Grothendieck's Anabelian philosophy. By ignoring the non-commutativity of the fundamental group, we produce only the direct sum of two abelian fundamental groups , say those of $\pi_1(\mathbb{P}^1 \setminus \{0,\infty\},x)$ and $\pi_1(\mathbb{P}^1 \setminus \{1,\infty\},x)$.

Then the map Ω_1 factors through the equivalent maps for each of the component abelian fundamental groups, which, according to Grothendieck, should have no data about the basepoint.

7.1.3 The Quotients of π_1 by higher derived groups

We therefore turn our attention to the second derived group and the associated quotient of the fundamental group.

Basepoint dependence at the level of this quotient would yield a result analogous to the result of Hain discussed earlier, in section 5.2.

In fact, we wish to avail ourselves of the richer structure of the unipotent completion of the fundamental group, for reasons that will become clear. We have therefore evolved the following question.

Question When is the map

$$\Omega_n : X(\mathbb{Q}_p) \longrightarrow \{\text{Groups with } G - \text{action}\}$$

given by $x \to \pi_1^{un}(X, x)_n$, injective?

It is clear that the maps Ω_n, as n varies, form a tower, and it is therefore clear that, if Ω_N is injective for some N, then any higher map must also be so.

Since the unipotent fundamental group may be constructed from the full profinite group, it must contain at most as much information; so we can once again dismiss the case $n = 1$.

For larger n, our approach will be as follows. Recall that a tangential basepoint is a map $\operatorname{Spec} \bar{k}((t)) \to X$. We let b be a rational tangential basepoint corresponding to the map $z \to t$ where z is the coordinate on X, then factor the map from points to fundamental groups as follows.

$$X(\mathbb{Q}_p) \to \{U\text{-Torsors}\} \to \{U\text{-twists}\}$$

sending $x \to \pi_1^{un}(\bar{X}, x, b) \to \pi_1^{un}(\bar{X}, b)$. We study each of these two maps to understand how injective the composition is.

7.2 Points to Torsors

We consider first the map from points of $\bar{X}$ to torsors. To do this, we will start by studying the map from points to torsors in the simpler case of the scheme $\mathbb{P}^1_{\bar{\mathbb{Q}}_p} \setminus \{0, \infty\}$.

Let $\bar{X}^1 := \mathbb{P}^1_{\bar{\mathbb{Q}}_p} \setminus \{0, \infty\}$ with the basepoint 1. As discussed in chapter 2, the p-covers of $\bar{X}^1$ are

$$\phi_n : \bar{X}^1 \to \bar{X}^1$$

given by $\phi_n(z) = z^{p^n}$. In each cover, 1 lies over the basepoint, so we can take $\tilde{1} := (1)_{n\in\mathbb{N}}$ to be a G-invariant point in $\tilde{\bar{X}}^1_1$. Let q be a rational point on $\tilde{\bar{X}}^1$. As discussed in chapter 2, we can use any point $\tilde{q} \in \tilde{\bar{X}}^1_q$ to define a path $\tilde{Q} \in \pi_1(\bar{X}^1, 1, q)$. This is the unique element in $\operatorname{Isom}(e_1, e_q)$ taking $\tilde{1}$ to $\tilde{q}$.

We can calculate the action of G on $\tilde{Q}$ as follows.

$$\begin{aligned}(\tilde{Q}^g)(\tilde{1}) &= g\tilde{Q}g^{-1}(\tilde{1}) \\ &= g\tilde{Q}(\tilde{1}) \\ &= g\tilde{q} \\ &= \tilde{q}^g\end{aligned}$$

so that $\tilde{Q}^g$ is the unique element of $\mathrm{Isom}(e_1, e_q)$ taking $\tilde{1}$ to $\tilde{q}^g$. This simple description allows the following calculation. Consider the short exact sequence of G-groups

$$1 \longrightarrow \mu_{p^n} \longrightarrow \bar{\mathbb{Q}}_p^\times \xrightarrow{p^n} \bar{\mathbb{Q}}_p^\times \longrightarrow 1$$

Taking a part of the associated long exact sequence in cohomology for each n yields a tower like

$$\begin{tikzcd} \mathbb{Q}_p^\times \arrow[r, "p^n"] & \mathbb{Q}_p^\times \arrow[r, "\delta_n"] & H^1(G, \mu_{p^n}) \arrow[r] & H^1(G, \bar{\mathbb{Q}}_p^\times) \\ \mathbb{Q}_p^\times \arrow[r] \arrow[u, "p"] & \mathbb{Q}_p^\times \arrow[r, "\delta_{n+1}"] \arrow[u, "1"] & H^1(G, \mu_{p^{n+1}}) \arrow[r] \arrow[u, "H^1(p)"] & H^1(G, \bar{\mathbb{Q}}_p^\times) \end{tikzcd}$$

The right-hand objects are 1 by Hilbert's Theorem 90. We check that the diagram commutes. The commutativity of the first square is clear. For the second, let $x \in \mathbb{Q}_p^\times$. We have

$$\begin{aligned}H^1(G, p)(\delta_{n+1})(x) &= H^1(G, p)(g \to y^g y^{-1}) \\ &= (g \to (y^p)^g (y^p)^{-1})\end{aligned}$$

for any y such that $y^{p^{n+1}} = x$. On the other hand, we have

$$\begin{aligned}(\delta_n)(1)(x) &= \delta_n(x) \\ &= (g \to z^g z^{-1})\end{aligned}$$

for any z such that $z^{p^n} = x$. Since y^p satisfies this condition, and since we know that we can use any z to compute the bockstein, we are done.

Now $\mathbb{Q}_p^\times$ maps to each member of the system $(H^1(G, \mu_{p^n}))_{n \in N}$ in a manner compatible with the connecting maps $(H^1(G, p))_{n \in N}$ in the system. We can therefore use the inverse limit of this system to define a map

$$\mathbb{Q}_p^\times \to \varprojlim H^1(G, \mu_{p^n})$$

Such a system of maps gives rise (for example, by [21] Theorem 2.6.10) to a map

$$\delta_\infty : \mathbb{Q}_p^\times \to H^1(G, Z_p(1))$$

This map is given by $\delta_\infty(x) = (g \to (y_n^g y_n^{-1})_n)$ where $y_n^{p^n} = x$. The kernel of this map is the set of points in $\mathbb{Q}_p^\times$ with a rational $(p^n)^{th}$ root for all n.

Lemma 7.1. *The cocycle associated to the paths torsor $\pi_1(\bar{X}^1, 1, x)$ agrees with $\delta_\infty(x)$.*

Proof. Let Y be the p^n-fold cyclic etale cover of $\bar{X}^1$. Then we can identify Y_p with $\{y : y^{p^n} = x\}$. Thus

$$\tilde{\bar{X}}_p^1 \cong \{(y_n) : y_n^{p^n} = x\}$$

Choose some such (y_n), and let Q be the path sending $\tilde{1}$ to (y_n). We know that Q^g sends $\tilde{1}$ to (y_n^g), and Q^{-1} must be the unique path carrying (y_n) to $\tilde{1}$.

Combining these, we see that the cocycle associated to x, which is $g \to Q^g Q^{-1}$, must send $\tilde{1}$ to $(y_n^g y_n^{-1})$.

This agrees with δ_∞. □

7.2.1 A Calculation

We claim that the map from the $\mathbb{Q}_p$-points of $\bar{X}$ to G-torsors for $U_1 := U^{ab}$, the abelianised p-adic unipotent completion of $\pi_1^{et}(\bar{X})$ is finite-to-one. We denote by $\pi_1^{(p)}(\bar{X})$ the maximal pro-p quotient of the fundamental group. Since we know that $\pi_1^{(p)}(\bar{X})^{ab} \cong \mathbb{Z}_p(1)^2$ and $U_1 \cong \mathbb{Q}_p(1)^2$, we can factorise this map as

$$\begin{tikzcd}
\bar{X}(\mathbb{Q}_p) \arrow[r, "f"] & \{\text{torsors for } \pi_1^{(p)}(\bar{X})^{ab}\} \arrow[r, "g"] \arrow[d, equal] & \{\text{torsors for } U_1\} \arrow[d, equal] \\
& H^1(G, \mathbb{Z}_p(1)^2) & H^1(G, \mathbb{Q}_p(1)^2)
\end{tikzcd}$$

We can further decompose the map f by noting that $\pi_1^{et}(\bar{X})^{(p)} \cong \pi_1^{(p)}(\mathbb{P}\setminus\{0,1\})\oplus\pi_1^{(p)}(\mathbb{P}\setminus\{0,\infty\})$. Applying the functor $H^1(G,-)$ to this, we can write

$$f(x) = (\delta_\infty(x), \delta_\infty(1-x))$$

To show that f is finite-to-one, it will suffice to show that δ_∞ is finite-to-one, so we first consider the kernel of this homomorphism. We saw that the kernel of this map is the set of elements y such that, for all n, there exists z_n with $(z_n)^{p^n} = y$. We claim that for any such y, we have $y^{p-1} = 1$. First note that, if $|y| = \lambda$, then λ must have a p^n-th root for all n, from which we conclude that $\lambda = 1$, so that $y \in \mathbb{Z}_p^\times$. We know that $y^p \equiv y$ modulo p, and we will show that $y^p \equiv y$ modulo p^n for all n, by induction. Assume this is true for $n = k$.

There is some z satisfying $z^{p^k} \equiv y$ modulo p^{k+1}, so that also z^{p^k}, whence $y \equiv z$ modulo p^k. So modulo p^{k+1} we have

$$\begin{aligned} y &\equiv z^{p^k} \\ &\equiv (y+mp^k)^{p^k} \\ &\equiv y^{p^k} \end{aligned}$$

On the other hand, we must have $y \equiv y^{p^{k+1}}$ modulo p^{k+1}, so that

$$\begin{aligned} y^{p^{k+1}} &\equiv y \equiv y^{p^k} \\ \Rightarrow (y^{p^k})^p &\equiv y^{p^k} \\ \Rightarrow y^p &\equiv y \end{aligned}$$

We conclude that $y^{p-1} = 1$ in $\mathbb{Z}_p$, so that δ_∞ is p-to-one. An immediate consequence of this is that f is finite-to-one.

We now study the map g, carrying torsors for the abelianised profinite fundamental group to the abelianised unipotent fundamental group. Consider the following short exact sequence.

$$1 \longrightarrow \mathbb{Z}_p(1) \longrightarrow \mathbb{Q}_p(1) \longrightarrow \mathbb{Q}_p(1)/\mathbb{Z}_p(1) \longrightarrow 1$$

Recall that, for the scheme $\mathbb{P}^1 \setminus \{0,1\}$, passing from the profinite fundamental group to the unipotent fundamental group can be identified with tensoring with $\mathbb{Q}$. We can thus identify the map from {torsors for the profinite fundamental group} to {torsors for the unipotent fundamental group} with the second map in the sequence

$$H^0(\mathbb{Q}_p(1)/\mathbb{Z}_p(1)) \longrightarrow H^1(\mathbb{Z}_p(1)) \longrightarrow H^1(\mathbb{Q}_p(1))$$

coming from the long exact sequence of Galois cohomology associated to the short exact sequence above. We have

$$\begin{aligned}
\mathbb{Q}_p(1)/\mathbb{Z}_p(1) &:= \frac{\mathbb{Q} \otimes_{\mathbb{Z}} \varprojlim \mu_{p^n}}{\varprojlim \mu_{p^n}} \\
&\cong \frac{\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z}_p \otimes_{\mathbb{Z}_p} \varprojlim \mu_{p^n})}{\varprojlim \mu_{p^n}} \\
&\cong \frac{(\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \varprojlim \mu_{p^n}}{\varprojlim \mu_{p^n}} \\
&\cong \frac{\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim \mu_{p^n}}{\varprojlim \mu_{p^n}} \\
&\cong \mu_{p^\infty}
\end{aligned}$$

The kernel of our map on torsors is therefore the image of the Galois invariants of $\mathbb{Q}_p(1)/\mathbb{Z}_p(1) \cong \mu_{p^\infty}$, the set of all p-power roots of unity. Since $p > 2$, we know by Eisenstein that $\mathbb{Q}_p$ has no p-power roots, so this image is trivial. Thus the following sequence is exact.

$$1 = H^0(\mu_{p^\infty}) \longrightarrow \{\text{torsors for } \pi_1^{(p)}(\bar{X})^{ab}\} \longrightarrow \{\text{torsors for } \pi_1^{un}(\bar{X})^{ab}\}$$

We conclude that distinct torsors for the abelianised profinite group $\pi_1^{et}(\bar{X})^{ab}$ must produce distinct torsors for the abelianised unipotent group $\pi_1^{u}(\bar{X})^{ab}$. We summarise this as follows.

Lemma 7.2. *The map from $\mathbb{Q}_p$-rational points of X to torsors for the abelianised unipotent fundamental group, U_1, is finite-to-one.*

The remainder of this work therefore concerns the fibres of the map from torsors to twists.

7.3 General Background on Non-Abelian Group Cohomology

As outlined in the previous chapter, we can factorise the map Ω_n into two maps, the first taking points to torsors, and the second taking torsors to twists. The second map was given an algebraic description in terms of cohomology, and so to study its fibre sets, we shall need to introduce some elementary but non-standard results on non-abelian cohomology.

Let

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

be a short exact sequence of (possibly) non-abelian groups. Then

$$H^0(G,C) \to H^1(G,A) \xrightarrow{j} H^1(G,B)$$

is exact, and we assert that $H^0(G,C)$ acts on the fibres of j in the following way.

Let $\xi \in H^1(G,A)$, and let $c \in C^G$. Define ξ^c by

$$\xi^c : g \to \tilde{c}^g \xi_g \tilde{c}^{-1}$$

for some $b \in B$ lifting c.

We observe that

Lemma 7.3. *This construction is well-defined. Furthermore, if we let f denote the map $H^1(i)$: $H^1(G,A) \to H^1(G,B)$, we have*

$$H^0(G,C) \times \xi = f^{-1} f(\xi)$$

for any $\xi \in H^1(G,A)$. That is, the fibre sets of f are precisely the orbits of the action of C^G.

Proof. We first check that the cocycle ξ^c is independent of the choice of a lift of c. Indeed, we write $C \cong A \setminus B$, so that for any other lift, b' of c, we have $b' = ab$ for some $a \in A$. Then ξ^c defined via b' sends $g \in G$ to $(b')^g \xi_g (b')^{-1}$. We can write this as $a^g b^g \xi_g b^{-1} a^{-1}$, which is cohomologous to the definition of ξ_c via b.

Secondly, we verify that ξ^c is indeed a cocycle. Let g and h be in G. We have

$$\begin{aligned}(\xi^c_g)^h\xi^c_h &= (b^g\xi_g b^{-1})^h(b^h\xi_h b^{-1})\\ &= b^{gh}\xi^h_g(b^{-1})^h b^h\xi_h b^{-1}\\ &= b^{gh}\xi_{gh}b^{-1} = \xi^c_{gh}\end{aligned}$$

Thirdly, we check that ξ^c does have coefficients in A. Indeed, A is normal in B, so $b\xi_g b^{-1} \in A$ for each g. Further, under the projection $B \to C$, $b^g b^{-1}$ goes to $c^g c{-}1 = 1$ since c is G-invariant. So we write $\xi^c_g = (b^g b^{-1})(b\xi_g b^{-1})$ which is in A.

Fourthly, we check that ξ^c has the same image under f as ξ itself. Indeed, by definition we have the existence of $b \in B$ such that, for each g, $\xi^c_g = b^g\xi_g b^{-1}$, which is equivalent to saying that these cocycles are cohomologous in B. That is, ξ and ξ^c are in the same fibre set of the map f.

So we have shown that the action of C^G on the fibre sets of $H^1(G, A)$ is well-defined, and that, for any $\xi \in H^1(G, A)$, we have

$$H^0(G, C) \times \xi \subseteq f^{-1}f(\xi)$$

and we wish to obtain the reverse inclusion. Let ξ and ζ be two cocyles in the same fibre of f. This means that there exists some $b \in B$ such that $\xi_g = b^g\zeta_g b^{-1}$ for all g. Now $\xi_g \in A$ and $b\zeta_g b^{-1} \in A$ by normality, so that $b^g b^{-1} \in A$ for all g. Then $p(b^g b^{-1}) \in p(A) = 1$. Hence $p(b)^g = p(b)$ for all g, which says that $p(b) \in C^G$. That is, $\xi = \zeta^{p(b)}$. □

7.3.1 Notes

1. Lemma 7.3 is merely a restatement of [19], I, Propositions 38 and 39. We include full proofs here because we will need to carry out explicit calculations using the action described.

2. Since the conjugation map $U_2 \to \mathrm{Aut}(U_2)$ factors as $U_2 \to U_1 \to \mathrm{Aut}(U_2)$, we will interest ourselves in the injectivity of the map $H^1(G, U_1) \to H^1(G, \mathrm{Aut}(U_2))$ instead.

U is centre-free; thus the conjugation map $U_1 \to \operatorname{Aut} U_2$ is injective, and yields an associated long exact sequence in cohomology. Thus we can study the fibres of $H^1(U_1) \to H^1(\operatorname{Aut} U_2)$ more easily than we could study the fibres of $H^1(U_2) \to H^1(\operatorname{Aut} U_2)$.

7.4 Level 2 - Non-Torelli

This section will use the tools developed so far to construct our first important theorem. We aim to show that

Theorem 1. *The map*

$$\Omega_2 : X(\mathbb{Z}_p) \longrightarrow \{Groups\ with\ G - action\}$$

given by $x \to \pi_1^{un}(X,x)_2$ is constant. Thus we cannot recover an integral basepoint from the Galois structure on (the isomorphism class of) the associated fundamental group.

Here $\pi_1^{un}(X,x)_2$ means the quotient of the $\mathbb{Q}_p$-unipotent fundamental group by the third member of its lower central series.

Some Notation: From here onwards, we will let z denote the standard coordinate on X, and let b denote the tangential basepoint corresponding under definition 7 to $z \to t$. We let U denote the unipotent completion $\pi_1^{un}(X,b)$ of the fundamental group at b. $U^{(n)}$ will be the n^{th} member of the lower central series, and U_n will be the quotient U/U^{n+1}, indexed so that U_1 is the abelianisation of U.

We wish to study the map $H^1(c)$, where $c : U_2 \to \operatorname{Aut}(U_2)$ is the conjugation map. This is simply an algebraic description of the map from G-torsors of U_2 to G-twists of U_2 that carries $\pi_1^{un}(X,x,b)$ to $\pi_1^{un}(X,b)$.

We first make the following observation.

Lemma 7.4. *For each natural number n, there is a natural surejction* $\operatorname{Aut} U_{n+1} \to \operatorname{Aut} U_n$.

Proof. We define the image of an automorphism ϕ of U_{n+1} as ϕ restricted to U_n. This is well-defined because the elements of the lower central series are characteristic subgroups, so that ϕ must induce an automorphism of $U^{(n+1)}/U^{(n+2)} \subset U_{n+1}$.

The map is surjective because U is the unipotent completion of (the profinite completion of) a free group. □

To study $H^1(c)$, we will fit the map c into an intelligible short exact sequence, using the lemma above.

Lemma 7.5. *The sequence of G-groups*

$$0 \to U_1 \to \mathrm{Aut}(U_2) \to \mathrm{Aut}(U_1) \to 0$$

is exact.

Proof. For each n, we can consider the elements of U_n as inner automorphisms of U_n, acting by conjugation, and so we see that

$$0 \to Z(U_n) \to U_n \to \mathrm{Aut}(U_n) \to \mathrm{Out}\ (U_n) \to 0$$

is exact. U itself is centre-free, so that $Z(U_n) \cong U^n/U^{n+1}$. Thus

$$0 \to U_1 \to \mathrm{Aut}(U_2) \to \mathrm{Out}\ (U_1) \to 0$$

is exact. This says that the conjugation action of U_1 on U_2 is well-defined.

Let K be the kernel of the projection $\mathrm{Aut}(U_2) \to \mathrm{Aut}(U_1)$. The conjugation action of U_1 on U_2 projects to the trivial action on U_1, so that $U_1 \to \mathrm{Aut}(U_2)$ must factor through K.

This yields maps $U_1 \to K$ and $\mathrm{Out}\ (U_2) \to \mathrm{Aut}(U_1)$, so that the following diagram commutes.

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & & U_1 \arrow[dl, "\theta"'] \arrow[d] & & \\
0 \arrow[r] & K_2^1 \arrow[r] & \mathrm{Aut}(U_2) \arrow[r] \arrow[d] & \mathrm{Aut}(U_1) \arrow[r] & 0 \\
 & & \mathrm{Out}\ (U_2) \arrow[ur] \arrow[d] & & \\
 & & 0 & &
\end{tikzcd}$$

Here the exactness of the horizontal sequence follows from an application of lemma 7.4 with $n = 2$. We aim to show that θ is an isomorphism.

As $\mathbb{Q}_p$ vector spaces, we can write

$$U_2 \cong U_1 \oplus U^2/U^3$$

Thus we can represent an automorphism ϕ of U_2 as a matrix

$$\phi = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}$$

where $M_11 \in \mathrm{Aut}(U_1)$, $M_{12} \in \mathrm{Hom}(U^2/U^3, U_1)$, $M_{21} \in \mathrm{Hom}(U_1, U^2/U^3)$, and $M_{22} \in \mathrm{Aut}(U^2/U^3)$.

Let $\phi \in K$. Then we must have $M_{11} = 1$.

Since ϕ is a group morphism, M_{22} is fully determined by M_{11}, so that $M_{22} = 1$.

Again, since ϕ is a group morphism, it must preserve the lower central series, so that $M_{12} = 0$.

However, the condition $\phi \in K$ places no restrictions on M_{21}, so we can identify K with $\mathrm{Hom}(U_1, U^2/U^3)$. U_1 is generated by the images A and B of the single loops around 1 and 0, and U^2/U^3 is generated by $ABA^{-1}B^{-1}$. Thus, as $\mathbb{Q}_p$ vector spaces, $\mathrm{Hom}(U_1, U^2/U^3) \cong \mathrm{Hom}(\mathbb{Q}_p^2, \mathbb{Q}_p) \cong \mathbb{Q}_p^2$.

Now $U_1 \to \mathrm{Aut}(U_2)$ is injective, so $U_1 \to K$ must be injective. It is an injective map between vector spaces of dimension 2, so it is an isomorphism. It follows that the quotient map Out $(U_2) \to \mathrm{Aut}(U_1)$ is also an isomorphism.

We can therefore identify the two short exact sequences in the diagram above, so that

$$0 \to U_1 \to \mathrm{Aut}(U_2) \to \mathrm{Aut}(U_1) \to 0$$

is exact, as claimed. □

By the factorisation of the conjugation map, discussed in the preceeding lemma, we obtain the factorisation

$$\begin{tikzcd} & H^1(G, U_n) \arrow[dr] & \\ H^1(G, U_{n+1}) \arrow[ur] \arrow[rr] & & H^1(G, \mathrm{Aut}\, U_{n+1}) \end{tikzcd}$$

We have seen that $X(\mathbb{Q}_p)$ maps to $H^1(G, U_i)$ with finite fibres for any $i \geq 1$, so that we are reduced to studying the fibres of $H^1(G, U_n) \to H^1(G, \mathrm{Aut}\, U_{n+1})$ to understand our problem.

By considering the long exact sequence associated to the short exact sequence in lemma 7.5, we see that

$$H^0(G, \mathrm{Aut}\, U_2) \to H^0(G, \mathrm{Aut}\, U_1) \to H^1(G, U_1) \to H^1(G, \mathrm{Aut}\, U_2)$$

is exact. By lemma 7.3, we conclude that $H^0(G, \mathrm{Aut}\, U_1)$ acts on the fibres of the level two torsor-to-twist map.

To better understand the structure of $H^0(G, \mathrm{Aut}\, U_1)$, we introduce the following two lemmata.

Lemma 7.6. $H^0(G, \mathrm{Aut}\, U_1) \cong \mathrm{Aut}\, U_1 \cong GL_2(\mathbb{Q}_p)$

Proof. Let α and β be the single loops around 0 and 1 in $\pi_1^{un}(X, b)$. We know that G acts on α by χ, the cyclotomic character, and that any $g \in G$ acts on β by sending it to a conjugate of $\beta^{\chi(g)}$.

Thus, in $U_1 \cong \pi_1^{un}(X, b)^{ab}$, G acts on the images of α and β by χ; hence it acts by χ on all of U_1.

Therefore, as G-groups, we can write

$$U_1 \cong \mathbb{Q}_p(1)^2$$

By the calculation

$$\begin{aligned} \mathrm{Hom}(\mathbb{Q}_p(1)^2, \mathbb{Q}_p(1)^2) &\cong (\mathbb{Q}_p(1)^2)^* \otimes \mathbb{Q}_p(1)^2 \\ &\cong \mathbb{Q}_p(-1)^2 \otimes \mathbb{Q}_p(1)^2 \\ &\cong \mathbb{Q}_p^4 \end{aligned}$$

we can identify $\mathrm{Hom}(U_1, U_1)$ with $\mathrm{Hom}(\mathbb{Q}_p^2, \mathbb{Q}_p^2)$ as G-groups. This essentially says that, since G acts homogeneously on U_1, the automorphisms of U_1 are G-equivariant.

The invertible elements on each side must be identified too, yielding

$$\begin{aligned} \mathrm{Aut}\, U_1 &\cong \mathrm{Aut}(\mathbb{Q}_p^2) \\ &\cong GL_2(\mathbb{Q}_p) \end{aligned}$$

Finally, we have $(\mathrm{Aut}\, U_1)^G \cong (GL_2(\mathbb{Q}_p))^G \cong GL_2(\mathbb{Q}_p)$ □

This is a full description of the automorphisms of U_1 on its own, as a G-group. To understand it in relation to $\mathrm{Aut}\, U_2$, we have the following lemma.

Lemma 7.7. *Let $\mathcal{L}_2$ be the nilpotent Lie algebra associated by the Baker-Campbell-Hausdorff equivalence to U_2, and similarly for $\mathcal{L}_1$ and U_1. Then there exists a G-equivariant splitting*

$$\begin{tikzcd} \mathcal{L}_2 \arrow[r] & \mathcal{L}_1 \arrow[l, bend right, "s_G"'] \arrow[r, "p"] & 0 \end{tikzcd}$$

of the surjection p corresponding to the surjection $U_2 \to U_1$.

Proof. This may be proved in a manner identical to the proof of Lemma 1.1 of [12], except for the following simple ammendment. The involution map i used in [12] may be replaced with the map $x \to \frac{x}{x-1}$, which is the Mobius transformation which swaps 1 and ∞ and fixes 0. The construction given in [12] to construct a G-invariant path from $-b$ to b gives us a G-invariant path from $(-\vec{t})$ to $(\vec{t})$.

This proof requires us to find a rational system of pre-images of the basepoint $-1 \in \mathbb{P}^1_{\bar{\mathbb{Q}}_p} \setminus \{0, \infty\}$ in every etale cover that is visible in the unipotent fundamental group. By lemma 6.1, these are only the covers having degree equal to a power of p. Since $p > 2$, then -1 is such a system of basepoints. □

Corollary. *The induced map*

$$(\mathrm{Aut}\, U_2)^G \to (\mathrm{Aut}\, U_1)^G$$

is surjective.

Proof. By the Baker-Campbell-Hausdorff equivalence, it suffices to prove the equivalent result for the Lie algebras associated to these groups.

Let $\phi \in (\operatorname{Aut}\mathcal{L}_1)^G$. Let A and B generate $\mathcal{L}_1$. Lift these to $\tilde{A}$ and $\tilde{B}$; then $\tilde{A}$, $\tilde{B}$, and $\tilde{C} := [\tilde{A}, \tilde{B}]$ generate $\mathcal{L}_2$.

Define $\tilde{\phi} \in \operatorname{Aut}\mathcal{L}_2$ by $\tilde{\phi}(\tilde{A}) = s_G \phi p(\tilde{A})$, and $\tilde{\phi}(\tilde{B}) = s_G \phi p(\tilde{B})$. For $\tilde{\phi}$ to be a Lie algebra morphism, we must have $\tilde{\phi}(\tilde{C}) = [\tilde{\phi}(\tilde{A}), \tilde{\phi}(\tilde{B})]$, so that $\tilde{\phi}$ is defined on all of $\mathcal{L}_2$ by linearity.

We check that $\tilde{\phi}$ is G-invariant.

Indeed, we have $\tilde{A}$, we have $\tilde{\phi}^g(\tilde{A}) = s_G^g \phi^g p^g(\tilde{A})$, but each component morphism is G-invariant, so their composition must be; and similiarly for $\tilde{B}$. For $\tilde{C}$, since the action of G must preserve the Lie bracket, and we have defined $\tilde{\phi}$ so that it also does, we have

$$\begin{aligned}
\tilde{\phi}^g(\tilde{C}) &= (g\tilde{\phi}g^{-1})[\tilde{A}, \tilde{B}] \\
&= [(g\tilde{\phi}g^{-1})(\tilde{A}), (g\tilde{\phi}g^{-1})(\tilde{B})] \\
&= [\tilde{\phi}(\tilde{A}), \tilde{\phi}(\tilde{B})] \\
&= \tilde{\phi}(\tilde{C})
\end{aligned}$$

□

We note that this corollary allows us to lift G-equivariant automorphisms of U_1 to G-equivariant automorphisms of U_2. We make use of this in studying explicitly the action of $(\operatorname{Aut} U_1)^G$ on $H^1(G, U_1)$.

Lemma 7.8. *Let $\xi \in H^1(G, U_1)$ and let $\phi \in (\operatorname{Aut} U_1)^G$. The action of $(\operatorname{Aut} U_1)^G$ on $H^1(G, U_1)$ is given by $\xi_g^{\phi} = \phi(\xi_g)$.*

Proof. We identify $U_1 \cong \operatorname{Inn} U_2$ to understand the action of $\phi \in (\operatorname{Aut} U_1)^G$. The automorphism

ϕ acts on $c(\xi)$ in the following way.

$$\begin{aligned} c(\xi)_g^\phi &= \tilde{\phi}^g c(\xi_g)\tilde{\phi}^{-1} \\ &= c(\phi(\xi_g))\tilde{\phi}^g\tilde{\phi}^{-1} \\ &\simeq c(\phi(\xi_g))\tilde{\phi}\tilde{\phi}^{-1} \\ &\simeq c(\phi(\xi_g)) \end{aligned}$$

This says that $\xi^\phi = \phi(\xi)$. Here $c(x)$ means conjugation in U_2 by the element x of U_1, and $\tilde{\phi}$ is a lift of ϕ to Aut U_2, which, by the corollary to lemma 7.7, we can insist is also G-equivariant. □

We are now ready to assemble the proof of our first important theorem.

Proof of Theorem 1.

$$\begin{tikzcd} & & X(\mathbb{Z}_p) \arrow[d] \arrow[dr] & \\ (\mathrm{Aut}\, U_2)^G \arrow[r] & (\mathrm{Aut}\, U_1)^G \arrow[r] & H^1(G, U_1) \arrow[r] & H^1(G, \mathrm{Aut}\, U_2) \end{tikzcd}$$

We know that the set of integral points of X maps to the two rightmost sets in the diagram above. We call the images of these maps **'geometric'** torsors and twists, respectively. We will consider the map from the geometric U_1-torsors to geometric U_2-twists. We know from lemma 7.5 that the fibres of this map are the orbits of the action of $(\mathrm{Aut}\, U_1)^G$. Lemma 7.6 identifies $(\mathrm{Aut}\, U_1)^G$ with GL_2, and lemma 7.8 gives us an explicit description of this action.

As in [3] definition 3.7.2, we define the restricted cohomolgy set $H^1_g(G, V)$ of a G-representation to be the kernel of the map $H^1(G, V) \to H^1(G, V \otimes B_{DR})$. We defer further discussion of this object until section 8.5.2.

[10], Proposition 5, tells us that, in fact, the 'geometric' torsors lie within the subset $H^1_g(G, U_1)$. We choose a basis, $\{A, B\}$ of U_1, and write $H^1_g(G, U_1) \cong H^1_g(G, \mathbb{Q}_p(1)) \oplus H^1_g(G, \mathbb{Q}_p(1))$. $H^1_g(G, \mathbb{Q}_p(1))$ is a subspace of $H^1(G, \mathbb{Q}_p(1)) = \mathbb{Q}_p^2$ cut out by a non-trivial linear form, so it must be one-dimensional. Hence $H^1_g(G, U_1)$ is two-dimensional and contains all geometric torsors. Thus the basis of U_1 yields a basis for $H^1_g(G, U_1)$.

We want to check that the action of any $\phi \in (\mathrm{Aut}\, U_1)^G$ preserves this Selmer condition; this would imply that $(\mathrm{Aut}\, U_1)^G$ acts on the subset $H^1_g(G, U_1)$. Let $\xi \in H^1_g(G, U_1)$. This means that there exists some $b \in U_1 \otimes B_{DR}$ such that $\xi_g \otimes 1_{B_{DR}} = b^g b^{-1}$ for all g. Define $\Phi \in \mathrm{Aut}(U_1 \otimes B_{DR})$ by $\Phi(u \otimes b) = \phi(u) \otimes b$, so Φ is G-equivariant. Then we know from lemma 7.8 that ϕ simply sends the cocyle ξ to the cocyle $g \to \phi(\xi_g)$, so we have

$$\begin{aligned} \xi_g^\phi \otimes 1 &= \phi(\xi_g) \otimes 1 \\ &= \Phi(\xi_g \otimes 1) \\ &= \Phi(b^g b^{-1}) \\ &= \Phi(b)^g \Phi(b)^{-1} \end{aligned}$$

which says that, in $H^1(G, U_1 \otimes B_{DR})$, the image ξ^ϕ is trivialised by $\Phi(b)$, so that ξ^ϕ also satisfies the Selmer conditions.

We can decompose any geometric cocycle as $\xi = (\rho, \sigma)$, where $\rho \in H^1_f(G, \pi_1(\bar{X}^1)_1$ and $\sigma \in H^1_f(G, \pi_1(\bar{X}^0)_1$. Let $\zeta \in H^1_f(G, U_1)$ be another geometric torsor, which we decompose similarly as $\zeta = (\tau, \upsilon)$. Recall that, by lemma 7.1, such geometric cocycles corresponding to torsors are non-trivial.

Considering ξ and ζ as elements of $\mathbb{Q}_p^2$ with the basis given by $\{A, B\}$, we find a matrix M such that $\xi \simeq M\zeta$. This is possible since ξ and ζ are both non-trivial. Note that, although $M \in GL_2(\mathbb{Q}_p)$ also acts on U_1, it does not necessarily follow that $\xi_g = M\zeta_g$ pointwise. Now let ϕ be the automorphism of U_1 given by the matrix M with respect to the basis $\{A, B\}$. By lemma 7.6, this is G-equivariant, and by lemma 7.8, we see that the action of ϕ moves ξ to ζ.

This argument allows us to move any non-trivial geometric torsor to any other by the action of some element of $(\mathrm{Aut}\, U_1)^G$. Since these orbits coincide with fibres of the map $H^1(c)$, we conclude that all geometric torsors lie in the same fibre set. This means that the map $\{G-$ torsors of $U_1\} \longrightarrow \{G-$ twists of $U_2\}$ is trivial on geometric torsors.

In other words, for any two rational points, x and y, the fundamental groups $\pi_1^{un}(\bar{X}, x)_2$ and $\pi_1^{un}(\bar{X}, y)_2$ are identical G-twists of U_2. Thus they are isomorphic as G-groups. □

Chapter 8

Higher Levels

This chapter will extend the methods introduced in the previous chapter and apply them to higher levels of the unipotent fundamental group; that is, to the quotients of U by higher derived groups.

Some notation: Let $\mathcal{X}$ be $\mathbb{P}^1_{\mathbb{Z}_p} \setminus \{0, 1, \infty\}$, so we recover X as the base-change of $\mathcal{X}$ to $\mathbb{Q}_p$. A $\mathbb{Z}_p$-point, x, of $\mathcal{X}$ includes the data of a $\mathbb{Q}_p$-point of X, so to this point we can associate elements of $H^1(G, U_n)$ and in $H^1(G, \mathrm{Aut}\, U_{n+1})$. By a slight abuse of notation, we write $x \in X(\mathbb{Z}_p)$ for this point.

8.1 Construction

We begin by considering the following construction as an analogy, at the n^{th} level, of theorem 7.5.

Let K_n^m be the kernel of the natural map from $\mathrm{Aut}\, U_n$ to $\mathrm{Aut}\, U_m$, for $n > m$. For each n, we have a short exact sequence of the form

$$0 \longrightarrow U_{n-1} \longrightarrow \mathrm{Aut}\, U_n \longrightarrow \mathrm{Out}\, U_n \longrightarrow 0$$

given by considering elements of U_{n-1} as inner automorphisms on U_n. Since U_1 is abelian and has no inner automorphisms, it is clear that every inner automorphism of U_n must lie in the kernel K_n^1. Hence the following diagram commutes. The exactness of the horizontal sequence again follows from lemma 7.4.

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & & U_{n-1} \arrow[d] \arrow[dl] & & \\
0 \arrow[r] & K_n^1 \arrow[r] & \mathrm{Aut}\, U_n \arrow[r] \arrow[d] & \mathrm{Aut}\, U_1 \arrow[r] & 0 \\
 & & \mathrm{Out}\, U_n \arrow[d] \arrow[ur] & & \\
 & & 0 & &
\end{tikzcd}$$

While it is no longer true, for $n > 2$, that the map $U_{n-1} \to K_n^1$ is an isomorphism, we can aim to use this construction to study the map $U_{n-1} \to \mathrm{Aut}\, U_n$. Indeed, the construction yields a decomposition of the torsors-to-twists map as

$$H^1(G, U_{n-1}) \longrightarrow H^1(G, K_n^1) \longrightarrow H^1(G, \mathrm{Aut}\, U_n)$$

Our mains aims will thus be to understand the kernels of these two component maps. We will also consider a geometric interpretation for the set in the middle, of G-cocycles with coefficients in $\mathrm{Aut}^1 U_n$.

8.2 The First Map

We consider first the map $H^1(U_{n-1}) \to H^1(K_n^1)$. We observe that the surjection $\mathrm{Aut}\, U_m \to \mathrm{Aut}\, U_n$ for each $m > n$ induces commutative squares like

$$\begin{tikzcd}
U_n \arrow[r] \arrow[d] & K_{n+1}^1 \arrow[d] \\
U_{n-1} \arrow[r] & K_n^1
\end{tikzcd}$$

which fit into a tower indexed over all n.

By functoriality, this extends to a tower

$$\begin{tikzcd}
 & H^1(U_{n+2}) \arrow[r] \arrow[d] & H^1(K^1_{n+1}) \arrow[d] \\
X(\mathbb{Q}_p) \arrow[ur] \arrow[r, "f"] \arrow[dr, "g"'] \arrow[ddr] & H^1(U_{n+1}) \arrow[r, "\alpha"] \arrow[d, "\beta"] & H^1(K^1_{n+2}) \arrow[d, "\gamma"] \\
 & H^1(U_n) \arrow[r, "\delta"] \arrow[d] & H^1(K^1_{n+1}) \arrow[d] \\
 & H^1(U_{n-1}) \arrow[r] & H^1(K^1_n)
\end{tikzcd}$$

which is commutative. g has finite fibres because the composition

$$X(\mathbb{Q}_p) \to H^1(U_n) \to H^1(U_1)$$

has finite fibres by lemma 7.2. Similarly, f is injective.

We observe that

$$\begin{aligned} \delta g &= \delta\beta f \\ &= \gamma\alpha f \end{aligned}$$

We recall that the map $H^1(U_1) \to H^1(K^1_2)$ is an isomorphism by lemma 7.5, and observe that this map is simply δ for $n = 1$. To show that α is injective on the image of f for $n = k$, we can therefore proceed inductively, assuming that δ is injective on the image of g for $n = k$.

However, the fibres of the map αf cannot be bigger than those of the map $\gamma\alpha f$. We know that g injects, and δ injects on the image of g. The fibres of $\gamma\alpha f = \delta g$ are thus trivial, and hence so are the fibres of αf.

We conclude that α injects on the image of f for $n = k$, which is equivalent to δ injecting on the image of g for $n = k + 1$.

We have thus proved

Theorem 2. *The map of sets*

$$H^1(G, U_n) \longrightarrow H^1(G, K^1_{n+1})$$

is injective on the set of 'geometric' torsors.

8.3 The Second Map

Our attention for this section will be focused on the properties of the Second map of section 8.1, $S_n : H^1(K_n^1) \to H^1(\mathrm{Aut}\, U_n)$.

We consider the difference between the profinite and unipotent cases, and this leads us to a geometric interpretation of the set $H^1(K_n^1)$ of cocycles with coefficients in K_n^1. We observe that the difference between K_n^1 and $\mathrm{Aut}\, U_n$ is the main obstruction to our theorem.

We can compare the kernels of the maps S_n and S_{n+1} in the following way. Let K_j^i be defined as the kernel of the natural projection from $\mathrm{Aut}\, U_j$ to $\mathrm{Aut}\, U_i$. We observe that

Lemma 8.1. *K_{n+1}^n is naturally isomorphic to the kernel of the map from K_{n+1}^1 to K_n^1.*

Proof. Indeed, we call the latter kernel K. We define a map f from K to K_{n+1}^n as follows. Compose the map α from K to K_{n+1}^1 with the map β from K_{n+1}^1 to $\mathrm{Aut}\, U_{n+1}$. We observe that, since every element of K maps to 1 in K_n^1, the image of $\beta\alpha$ must lie in K_{n+1}^n. We can therefore take this to be the map f.

$$\begin{tikzcd}
 & K \arrow[r, "f"] \arrow[d, "\alpha"] & K_{n+1}^n \arrow[d, "\gamma"] & & \\
1 \arrow[r] & K_{n+1}^1 \arrow[r, "\beta"] \arrow[d, "\epsilon"] & \mathrm{Aut}\, U_{n+1} \arrow[r, "\delta"] \arrow[d] & \mathrm{Aut}\, U_1 \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & K_n^1 \arrow[r] & \mathrm{Aut}\, U_n \arrow[r] & \mathrm{Aut}\, U_1 \arrow[r] & 1
\end{tikzcd}$$

Let $\phi \in K_{n+1}^n$. By definition, ϕ acts trivially on $\mathrm{Aut}\, U_n$, so it certainly acts trivially on U_1. That is, $\delta\gamma(\phi) = 1$, so that $\gamma(\phi) \in K_{n+1}^1$. Again, since ϕ acts trivially on U_n, we have $\gamma(\phi) \in ker(\epsilon)$, so $\gamma(\phi) \in K$. It follows that f surjects. Finally, β and α are individually injective, so it follows that f injects. □

8.3.0.1 Graded Pieces

Write $V_n(x)$ for $\pi_1^u(\bar{X}, x)_n$ for each rational basepoint x. If x is the tangential basepoint b, we of course have $U_n = V_n(x)$. Our first tool will involve the use of the individual graded pieces of the graded group associated to $V_3(x)$.

As G-groups, we know that $V_1 \cong \mathbb{Q}_p(1)^2$. That is, G acts on the generators of V_1 by the cyclotomic character, χ. It does not follow that G acts on the generators of $V_n(x)$ by the cyclotomic character.

Indeed, for $n = 2$, the content of lemma 7.7 is that the action of G on the generators of U is by χ, at least modulo $U^{(3)}$. Then, by theorem 1, this cannot be true for any other basepoint (where we identify basepoints up to geometric morphisms). Indeed, one part of the content of the theorem is that the map from U_1-torsors to U_2-twists is injective on the privileged point. Hence, for any other point x, we conclude that G cannot act on $V_2(x)$ in the same way that it acts on U_2. Since the action of G on $V_2(x)$ is specified by its action on the two generators, G cannot act on both generating loops by χ.

However, for any x, we observe that G must act on the generator of $V(x)^{(2)}/V(x)^{(3)}$ by χ^2. We aim to make use of the simple G-structure of these graded pieces of $V_n(x)$ in general. Our first step towards generalising this is

Lemma 8.2. *There is an isomorphism*

$$K^n_{n+1} \cong \mathrm{Hom}(U_{n+1}, Z_{n+1})$$

where Z_{n+1} is the kernel of the surjection $U_{n+1} \to U_n$.

Proof. For $f \in K^n_{n+1}$, we define $h_f : U_{n+1} \to Z_{n+1}$ by $h_f(u) := f(u)u^{-1}$. We claim that this is a well-defined homomorphism, and that is induces an isomorphism h from K^n_{n+1} to $\mathrm{Hom}(U_{n+1}, Z_{n+1})$.

Let f and u be as above. To see that h_f is well-defined, we reduce modulo $U^{(n+1)}$, to get $\overline{h_f(u)} = \overline{f(u)u^{-1}} = \overline{uu^{-1}} = 1$. Hence $h_f(u) \in Z_{n+1}$.

Next we check that, for a fixed f, h_f is an homomorphism. Observe that Z_{n+1} is central in U_{n+1}. We let $u \in U + n + 1$ and $z \in Z_{n+1}$, so that $v \in V^{(n+1)}/V^{(n+2)}$, whence $[u, v] =$

$V^{(n+2)}/V^{(n+2)} = 1$. Now let $u, v \in U_{n+1}$. We have

$$\begin{aligned} h_f(u)h_f(v) &= f(u)u^{-1}(f(v)v^{-1}) \\ &= f(u)f(v)v^{-1}u^{-1} \\ &= f(uv)(uv)^{-1} \\ &= h_f(uv) \end{aligned}$$

Next, we show that h itself is an homomorphism. The group law in K^n_{n+1} is composition, while the group law on $\mathrm{Hom}(U_{n+1}, Z_{n+1})$ comes from the group law on Z_{n+1}. Thus we have $h_{fg}(u) = (fg)(u)u^{-1}$, while $(h_f h_g)(v) = h_f(v)h_g(v) = f(u)u^{-1}g(u)u^{-1}$. It will thus suffice to show that $(fg)(u) = f(u)u^{-1}g(u)$. We compute

$$\begin{aligned} [(fg)(u)][f(u)u^{-1}g(u)]^{-1} &= (fg)(u)[g(u)^{-1}u]f(u^{-1}) \\ &= (fg)(u)f(u)^{-1}g(u)^{-1}u \\ &= f(g(u)u^{-1})(g(u)u^{-1})^{-1} \\ &= h_f(g(u)u^{-1}) = h_f(h_g(u)) \end{aligned}$$

(Here we use the facts that Z_{n+1} is central, and that $[g(u), u^{-1}] = 1$.) But $h_g(u)$ lies in Z_{n+1} by the note above, so that $h_f(h_g(u)) = 1$.

Finally, we check that h is an isomorphism. Suppose that there exist f, g such that $h_f = h_g$. That is, $\forall u \in U_{n+1}$, we have $f(u)u^{-1} = g(u)u^{-1}$. Then $f(u) = g(u)$ for all $u \in U_{n+1}$, so that $f \equiv g$.

On the other hand, let $\phi \in \mathrm{Hom}(U_{n+1}, Z_{n+1})$. Since U_{n+1} is (a quotient of the unipotent completion of) the free group on two generators u_1 and u_2, it follows that ϕ is uniquely specified by $\phi(u_1)$ and $\phi(u_2)$, and, conversely, that any two such choices will give rise to an homomorphism ϕ. For surjectivity, we wish to find some f such that

$$h_f(u_i) = f(u_i)u_i^{-1} = \phi(u_i) \qquad i = 1, 2$$

We can choose to define f by $f(u_i) = \phi(u_i)u_i$ (with inverse $f^{-1} = (-\phi)(u) \times u$), and, as above, this uniquely and completely specifies $f \in \mathrm{Aut}(U_{n+1})$. It is then clear that $h_f = \phi$. □

Furthermore, we note that Z_{n+1} is abelian, and we recall that there is a correspondence between maps from U_{n+1} to Z_{n+1} and maps from the abelianisation of U_{n+1} to Z_{n+1}. Indeed, we have the following corollary.

Corollary. *There is an isomorphism*

$$K^n_{n+1} \cong \mathrm{Hom}(U_1, Z_{n+1})$$

where Z_{n+1} is the kernel of the surjection $U_{n+1} \to U_n$.

8.4 On the Central Obstruction to our Aim

Our aim at the beginning of this work was to be able recover the geometric point x from the G-group $\pi_1^u(\bar{X}, x)_n$.

This hope was made more precise and elaborated on in the previous chapters; and was shown to be false for $n = 2$.

We now attempt to make precise an observation into the obstruction that caused this failure. We first recall our earlier definitions of K^i_j as the kernel of the natural surjection $\mathrm{Aut}\, U_j \to \mathrm{Aut}\, U_i$, and $\mathrm{Aut}^1 U_n := K^1_n$. Recall also that we can interpret the set $H^1(G, U_n)$ as the set of G-twists of U_n. That is, the two associated cocycles with coefficients in $\mathrm{Aut}\, U_n$ are cohomologous if there is an automorphism of U_n (as a group only) relating the two corresponding G-actions.

In a similar light, we can view $H^1(G, \mathrm{Aut}^1 U_n)$ as follows. A cocycle corresponds to a G-action on U_n, and two cocycles are cohomologous exactly when there is an automorphism ϕ of U_n relating the actions; such that ϕ induces 1 on U_1.

We know that the set of $\mathbb{Q}_p$-points of X maps with finite fibres to $H^1(\mathrm{Aut}^1 U_N)$. This says that only finitely many 'geometric' cocycles with coefficients in $\mathrm{Aut}\, U_n$ can be related by automorphisms in $(\mathrm{Aut}^1 U_n)^G$. Concretely, for a fixed x, there are only finitely many y such that $\exists$ a G-equivariant isomorphism $\theta : \pi_1^u(\bar{X}, x)_n \to \pi_1^u(\bar{X}, y)_n$ such that $\theta|_1 : \pi_1^u(\bar{X}, x)_1 \to \pi_1^u(\bar{X}, y)_1$ is 1. (Here we canonically identify both of these abelian groups with $H_1^{et}(\bar{X}, \mathbb{Q}_p)$.)

However, theorem 1 tells us that, for any $x, y \in \bar{X}(\mathbb{Q}_p)$, there is some G-equivariant isomorphism $\theta : \pi_1^u(\bar{X}, x)_2 \to \pi_1^u(\bar{X}, y)_2$. Having understood $H^1(\mathrm{Aut}^1 U_n)$ in this way, a natural question related to our theorem is whether, for larger n, U_n has 'too many' G-equivariant automorphisms. The corollary to lemma 7.7 proves that U_2 has too many G equivariant automorphisms. Indeed, in this case, every automorphism of U_1 is G-equivariant, and every G-equivariant automorphism of U_1 lifts to a G-equivariant automorphism of U_2. This viewpoint motivates further questions about the G-structure of Aut U_n, Aut^1 U_n, and K_n^1.

We begin by noting the following generalisation of lemma 8.2, the proof of which is very similar to the proof of the latter.

Lemma 8.3. *Let $i \leq n$. Then*

$$K_n^i / K_n^{i+1} \cong \mathrm{Hom}(U_1, U^{(i+1)}/U^{(i+2)})$$

Proof. Let $\phi \in K_n^i/K_n^{i+1}$. Define $h_\phi : U_n \to U^{i+1}/U^{i+2}$ by $h_\phi(u) = \phi(u)u^{-1}$. We verify the many assumptions that are implicit in this definition.

We first check that this map is well-defined. Indeed, since ϕ acts trivially on U_{i+1}, we have $\phi(u) = u$ modulo U^{i+1}. Thus $\phi(u)u^{-1} \in U^{i+1}$. And if we use some other $\psi = \phi$ modulo K_n^{i+1}, we have $\phi(u) = \psi(u)$ modulo U^{i+2}, whence $h_\phi(u) = \phi(u)u^{-1} = \psi(u)u^{-1} = h_\psi(u)$.

Secondly, we check that $h(\phi)$ is actually a homomorphism. We have

$$\begin{aligned} h(\phi)(uv) &= \phi(uv)(uv)^{-1} \\ &= \phi(u)\phi(v)v^{-1}u^{-1} \\ &= (\phi(u)u^{-1})(u\phi(v)v^{-1}u^{-1}) \\ &= (\phi(u)u^{-1})(\phi(v)v^{-1}) \end{aligned}$$

The last line holds $\phi(v)v^{-1} \in U^{i+1}$, which implies $u\phi(v)v^{-1}u^{-1} = \phi(v)v^{-1}$, all modulo U^{i+2}.

Thirdly, since $h(\phi)$ is an homomorphism from U_n to an abelian group, it must factor through $U_1 = U_n^{ab}$. Abusing notation, we have a map

$$h : K_n^i/K_n^{i+1} \to \mathrm{Hom}(U_1, U^{i+1}/U^{i+2})$$

Fourthly, we check that h itself is an homomorphism. Let ψ and ϕ be any two elements of K_n^i/K_n^{i+1}. We have

$$\begin{aligned} h_{\phi\psi}(u) &= (\phi\psi)(u)\phi(u)^{-1}\phi(u)u^{-1} \\ &= \phi(\psi(u)u^{-1})\phi(u)u^{-1} \\ &= \phi(\psi(u)u^{-1})(\psi(u)u^{-1})^{-1}(\psi(u)u^{-1})(\phi(u)u^{-1}) \\ &= h_\phi(h_\psi(u))h_\psi(u)h_\phi(u) \end{aligned}$$

However, we know that $h(\psi)(u) \in U^{i+1}$. We write it as $[v, w]$. Then, since $h(\phi)$ is an homomorphism, we have

$$\begin{aligned} h\phi(h_\psi(u)) &= h_\phi([v, w]) \\ &= [h_\phi(v), h_\phi(w)] \end{aligned}$$

which lies in U^{i+2}, since we may assume that $v \in U^{i+1}$. Therefore, modulo U^{i+2}, we have

$$\begin{aligned} h_{\phi\psi}(u) &= h_\phi(h_\psi(u))h_\psi(u)h_\phi(u) \\ &= 1 \times h_\phi(u)h_\psi(u) \end{aligned}$$

Here we have swapped the last two factors because U^{i+1}/U^{i+2} is abelian. We can thus conclude that h is an homomorphism.

We check that h is injective. Indeed, suppose $h(\phi) = 1$. Then $\phi(u)u^{-1}$ vanishes modulo U^{i+2}, for all u. This is equivalent to the statement that $\phi \in K_n^{i+1}$.

To check that h is surjective, we work at the level of the lie algebras associated to each group by the Baker-Campbell-Hausdorff formula. Indeed, let $\bar{f} : \mathcal{L}_n \to \mathcal{L}^{i+1}/\mathcal{L}^{i+2}$. Since $h(\phi)$ is defined as $u \to \phi(u) - u$, we simply have to find some $\bar{f}$ such that $\phi(u) = u + \bar{f}(u)$. Let u_1, u_2 generate $\mathcal{L}_n$ as an algebra. We simply define $\bar{f}(u_i) := \phi(u_i) - u_i$. This produces a well-defined morphism $\bar{f}$ because $\mathcal{L}_n$ is a quotient of a free Lie algebra. Then ϕ defined as above will yield $h(\phi) = \bar{f}$. □

We recover lemma 8.2 in the case where $i = n-1$. The usefulness of this structure theorem is revealed when we combine it with the following observation of Serre.

Lemma 8.4. *Let*

$$1 \to A \to B \to C \to 1$$

be a short exact sequence of G-groups. Let A be central in B. Then $H^1(A)$ acts naturally on $H^1(B)$ and the fibres of $H^1(B \to C)$ are exactly the orbits of this action.

Proof. Let $\chi \in H^1(A)$ and $\xi \in H^1(B)$. We define the action by $\chi : \xi \to (g \to \chi(g)\xi(g))$.

We first check that this is a cocylce. Indeed, we have

$$\begin{aligned} (\chi\xi)(g) &= \chi(gh)\xi(gh) \\ &= \chi(g)\chi(h)^g\xi(g)\xi(h)^g \\ &= \chi(g)^h\xi(g)^h\chi(h)\xi(h) \\ &= (\chi\xi)(g)^h(\chi\xi)(h) \end{aligned}$$

where the third line follows from the centrality of A.

It is clear that each orbit of this action is contained in a fibre. We check that the fibres coincide with orbits. So let ξ and ζ lie in the same fibre. That is, there exists some $c \in C$ such that $\xi(g) = c^g\zeta(g)c^{-1}$ for all g. Lift c to some $b \in B$, and define $\chi(g) := b^g\zeta(g)b^{-1}\xi(g)^{-1}$. We check that this is a cocycle:

$$\begin{aligned} \chi(gh) &= b^{gh}\zeta(gh)b^{-1}\xi(gh) \\ &= b^{gh}\zeta(g)^h\zeta(h)b^{-1}\xi(h)^{-1}(\xi(g)^h)^{-1} \\ &= [b^{gh}\zeta(g)^h(b^{-1})^h\xi(g)^h][\xi(g)^hb^h)][\zeta(h)b^{-1}\xi(h)^{-1}(\xi(g)^h)^{-1}] \\ &= [b^g\zeta(g)b^{-1}\xi(g)]^h[b^h\zeta(h)b^{-1}\xi(h)] \end{aligned}$$

since $\left(b^h\zeta(h)b^{-1}\xi(h)^{-1}\right)(\xi(g)^h)^{-1} = (\xi(g)^h)^{-1}\left(b^h\zeta(h)b^{-1}\xi(h)^{-1}\right)$, again by the centrality of A. $\square$

Applying this lemma to the first vertical exact sequence in lemma 8.1 yields the stronger result

Lemma 8.5. *$H^1(K^i_{i+1})$ acts freely on $H^1(Aut^1 U_{i+1})$, and the orbits of this action are the fibres of the map $H^1(Aut^1 U_{i+1}) \to H^1(Aut^1 U_i)$.*

Proof. Identifying unipotent groups with their associated Lie algebras, we first check that K^i_{i+1} is central in $\mathrm{Aut}^1 U_{i+1}$. Choose a $\mathbb{Q}_p$-linear splitting of the surjection $\mathcal{L}_{i+1} \to \mathcal{L}_i$, We can then write any $u \in \mathcal{L}_{i+1}$ as (u_i, v), where u_i lies in the image of the splitting map and $v \in \mathcal{L}^{i+1}/\mathcal{L}^{i+2}$. Let $\theta \in K^i_{i+1}$ and let $\phi \in \mathrm{Aut}\,\mathcal{L}_{i+1}$. By the structure theorem, and the fact that ϕ and θ are both group homomorphisms, we can write them as $\phi = \begin{pmatrix} \phi_{11} & 0 \\ \phi_{12} & \phi_{22} \end{pmatrix}$ and $\theta = \begin{pmatrix} 1 & 0 \\ \theta_{12} & 1 \end{pmatrix}$. θ is a group homomorphism, and the generators for $\mathcal{L}_{i+1}/\mathcal{L}_{i+2}$ must come from Lie brackets of the generators of $\mathcal{L}_i$. Hence $\theta_{11} = \theta|_{\mathcal{L}_i} = 1$ implies that $\theta_{22} = 1$. Then we have

$$\begin{aligned}
\theta\phi\theta^{-1}(u) &= \theta\phi(u_n, -\theta_{12}(u_n) + v) \\
&= \theta(\phi_{11}(u_n), \phi_{12}(u_n) - \phi_{22}(\theta_{12}(u_n)) + \phi_{22}(v)) \\
&= (\phi_{11}(u_n), \theta_{12}\phi_{11}(u_n) + \phi_{12}(u_n) - \phi_{22}\theta_{12}(u_n) + \phi_{22}(v)) \\
&= (\phi_{11}(u_n), \phi_{12}(u_n) + \phi_{22}(v)) + (0, \theta_{12}\phi_{11}(u_n) - \phi_{22}\theta_{12}(u_n)) \\
&= \phi(u)
\end{aligned}$$

by the relation $\theta_{12}\phi_{11}(u_n) = \phi_{22}\theta_{12}(u_n)$, which follows from the fact that ϕ is a group homomorhpism. This establishes the centrality of K^n_{n+1} in $\mathrm{Aut}\, U_{n+1}$, so that it is necessarily central in $\mathrm{Aut}^1 U_{n+1}$.

Next, suppose $\chi \in H^1(K^i_{I+1})$ fixes $\xi \in H^1(\mathrm{Aut}^1 U_{i+1})$. Then there is some $\phi \in \mathrm{Aut}^1 U_{i+1}$ such that $\chi(g)\xi(g) = \phi^g \xi(g)\phi^{-1}$. Reducing to $\mathrm{Aut}^1 U_i$, this becomes $\bar{\xi(g)} = \bar{\phi}^g \bar{\xi(g)}\bar{\phi}^{-1}$, whence $\bar{\phi}^g = \bar{\xi(g)}\bar{\phi}\bar{\xi(g)}^{-1}$. By induction and by lemma 8.3, $\bar{\phi}$ is trivial. Then $\chi(g) = \phi^g \xi(g)\phi^{-1}\xi(g)^{-1} = \phi^g\phi^{-1}$ is a coboundary. $\square$

8.4.1 A Finiteness Result of Nakamura

For comparison, we recall here a result of Nakamuara on the outer G-automorphisms of the profinite fundamental group of $U := \mathbb{P}^1_k \setminus \{0, 1, \infty\}$, for k an number field. This is the main result of [16].

Fixing an odd prime l, Nakamura defines J_l to be the kernel of the natural projection $\pi_1(U_{\bar{k}}) \to \pi_1^l(U_{\bar{k}})$, and $\pi_1'(U) := \pi_1(U)/J_l$. That is, $\pi_1'(U)$ contains all the Galois-theoretic structure of $\pi_1(U)$, but only the pro-l part of the geometric fundamental group.

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(U_{\bar{k}}) \arrow[r] \arrow[d, two heads] & \pi_1(U) \arrow[r] \arrow[d, two heads] & G_k \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \pi_1^l(U_{\bar{k}}) \arrow[r] & \pi_1'(U) \arrow[r] & G_k \arrow[r] & 1
\end{tikzcd}$$

Then [16], theorem 1 states that

$$\frac{\mathrm{Aut}_{G_k}(\pi_1'(U))}{\mathrm{Inn}\,\pi_1^l(U_{\bar{k}})} \cong \underset{k}{\mathrm{Aut}}(U)$$

and we know that $\mathrm{Aut}_k(U) \cong S_3$ is simply the group of Mobius transformations fixing the set $\{0, 1, \infty\}$. We conclude that (Out $\pi_1^l(U_{\bar{k}})$ is finite. Hence, by the construction of 7.5, we conclude the finiteness of the map

$$H^1(G, \pi_1^l) \to H^1(G, \mathrm{Aut}\,\pi_1^l)$$

sending paths-torsors to fundamental groups.

This result highlights again the extra rigidity possessed by the profinite fundamental group (and, indeed, even by its pro-l quotients), which the unipotent completion lacks.

8.5 Main Theorem

This section is devoted to the proof that the second map in section 8.1 is finite-to-one.

Theorem 3. *Let $p \geq 7$. The map from $\mathbb{Z}_p$-points of X to groups with Galois action given by*

$$x \longrightarrow \pi_1^{un}(\bar{X}, x)$$

is finite-to-one.

8.5.1 Representability

An important step in this proof is to view the set $H^1(\mathrm{Aut}^1 U_n)$ as the $\mathbb{Q}_p$-points of a scheme, which we will, by slightly abusing notation, also refer to $H^1(\mathrm{Aut}^1 U_n)$. To this end, we have

Lemma 8.6. *Let R be a $\mathbb{Q}_p$-algebra. Then the functor*

$$H^1(Aut^1 U_n) : R \longrightarrow H^1(Aut^1 U_n(R))$$

is representable.

Proof. We prove this in a manner similar to Kim's proof of this statement for $H^1(U_n)$ ([10], Proposition 2). The proof is by induction on n, and relies on lemma 8.3, which may be interpreted as saying that $\mathrm{Aut}^1 U_{n+1}$ is an n-fold extension of vector groups.

It is clear that the result is true for $n = 1$. Indeed, $H^1_f(\mathrm{Aut}^1 U_1)$ is represented by $\mathrm{Spec}\,\mathbb{Q}_p$. So we inductively assume that the result is true for $H^1(\mathrm{Aut}^1 U_n)$.

We first need to know that $H^0(L^i_{i+1}) = 0$ for all i, where L^i_{i+1} is the kernel of the map from $\mathrm{Aut}^1 U_{i+1}$ to $\mathrm{Aut}^1 U_i$. But lemma 8.1 tells us that $L^i_{i+1} \cong K^i_{i+1}$, and lemma 8.3 gives us an explicit understanding of the structure of the graded quotients of these kernels. Indeed, we have $L^i_{i+1} \cong \mathrm{Hom}(U_1, U^{i+1}/U^{i+2}) \cong \mathrm{Hom}(\mathbb{Q}_p(1)^2, \mathbb{Q}_p(i+1)^{r(i)})$, for some $r(i)$. This is then just a product of $\mathbb{Q}_p(i)$'s, and consequently has trivial H^0.

It follows that $H^0(L^i_{i+1})(R) = 0$ for any $\mathbb{Q}_p$-algebra R with trivial G-action. Indeed, we have $L^i_{i+1}(R) = \mathrm{Hom}(R, L^i_{i+1})$, the G-invariants of which must come from the G-invariants of L^i_{i+1}.

Next, we observe that $H^0(G, \mathrm{Aut}^1 U_i) = 0$ for all i. Indeed, this is true for $i = 1$, and for $i \geq 2$ we have the following short exact sequence.

$$1 \longrightarrow H^0(K^{i-1}_i)(R) \longrightarrow H^0(\mathrm{Aut}^1 U_i)(R) \longrightarrow H^0(\mathrm{Aut}^1 U_{i-1})(R)$$

Thirdly, we claim that $H^1(L^i_{i+1})$ is representable. Indeed, we have seen that L^i_{i+1} is a vector group, and lemma 6 of [10] shows us that H^1 of a vector group is representable.

Since the sequence $1 \rightarrow L^i_{i+1} \rightarrow \mathrm{Aut}^1 U_{i+1} \rightarrow \mathrm{Aut}^1 U_i \rightarrow 1$ is exact, we can realise $\mathrm{Aut}^1 U_{i+1}$ as a L^i_{i+1} torsor over $\mathrm{Aut}^1 U_i$. Since $\mathrm{Aut}^1 U_i$ is affine, this torsor must split. We choose an algebraic splitting

$$s : \mathrm{Aut}^1 U_i \longrightarrow \mathrm{Aut}^1 U_{i+1}$$

to the natural projection map. This gives us splittings $\mathrm{Aut}^1 U_i(X) \rightarrow \mathrm{Aut}^1 U_{i+1}(X)$ for each X, functorial in X.

Similarly, the surjectivity of the map $Z^1(\mathrm{Aut}^1 U_i) \rightarrow H^1(\mathrm{Aut}^1 U_i)$ gives us surjective maps $Z^1(\mathrm{Aut}^1 U_i)(X) \rightarrow H^1(\mathrm{Aut}^1 U_i)(X)$ for each X. In particular, we must have a surjection from $Z^1(\mathrm{Aut}^1 U_i)(H^1(\mathrm{Aut}^1 U_i)$ to $H^1(\mathrm{Aut}^1 U_i)(H^1(\mathrm{Aut}^1 U_i)$, under which a pre-image of the identity yields a splitting, t, of the the original surjection.

We compose this map t with $s_* : Z^1(\mathrm{Aut}^1 U_i) \rightarrow Z^1(\mathrm{Aut}^1 U_{i+1})$ and the boundary map $d : C^1(\mathrm{Aut}^1 U_{n+1}) \rightarrow C^2(K^i_{i+1})$. Recall that d is defined by

$$d(c) : (g_1, g_2) \longrightarrow c(g_1 g_2)(c(g_2)^{g_1})^{-1} c(g_1)^{-1}$$

The image of $Z^1(\mathrm{Aut}^1 U_i)$ need not lie in $Z^1(\mathrm{Aut}^1 U_{i+1})$. However, it is clear that dsi composed with the quotient map $q : Z^2(K) \rightarrow H^2(K)$ is yields the bockstein, δ.

Now q and dsi are natural maps, and so are algebraic by lemma 8.7. $B^2(K) = q^{-1}(1)$ is thus a closed subscheme of $Z^2(K)$. Then $(dsi)^{-1}(B^2(K))$ is a closed subscheme of $H^1(\mathrm{Aut}^1 U_i)$.

Since, by [10], lemma 6, we know that $C^1(K)(X) = C^1(K(X))$ and $B^2(K(X)) = B^2(K)(X)$, we can choose a linear splitting $a_B : B^2(G, K(B)) \rightarrow C^1(G, K(B))$ of the boundary map, which yields a functorial splitting $a : B^2(G, K) \rightarrow C^1(G, K)$.

We proceed with the construction of the map $b : x \rightarrow (si)(x) \times (adsi)(x)^{-1}$ exactly as in [10], Proposition 2. Then we have a square like

$$\begin{tikzcd}
I(\mathrm{Aut}^1 U_n) \arrow[r, "b"] \arrow[d] & Z^1(\mathrm{Aut}^1 U_{n+1}) \arrow[d] \\
H^1(\mathrm{Aut}^1 U_n) & H^1(\mathrm{Aut}^1 U_{n+1}) \arrow[l]
\end{tikzcd}$$

The lower arrow here comes from the map $\mathrm{Aut}^1 U_{n+1} \to \mathrm{Aut}^1 U_n$ constructed above. Its codomain is $I(\mathrm{Aut}^1 U_n) \subseteq H^1(\mathrm{Aut}^1 U_n)$ because $I(\mathrm{Aut}^1 U_n) := \delta^{-1}(1)$.

Now we have a short exact sequence

$$1 \longrightarrow H^1(K^n_{n+1}) \longrightarrow H^1(\mathrm{Aut}^1 U_{n+1}) \longrightarrow H^1(\mathrm{Aut}^1 U_n) \longrightarrow 1$$

By lemma 8.5, and since $H^0(\mathrm{Aut}^1 U_n) = 1$, there is a free action of $H^1(K^n_{n+1})$ on $H^1(\mathrm{Aut}^1 U_{n+1})$, and the orbits of this action are the fibres of the the second map.

This free action allows us to construct an isomorphism

$$H^1(K^n_{n+1}) \times I(\mathrm{Aut}^1 U_n) \cong H^1(\mathrm{Aut}^1 U_{n+1})$$

given by $(\xi, \zeta) \to \xi S(\zeta)$.

$H^1(K^n_{n+1})$ is representable because it is H^1 of a vector group, while $I(\mathrm{Aut}^1 U_n)$ is a closed subscheme of the scheme $H^1(\mathrm{Aut}^1 U_n)$. We conclude that $H^1(\mathrm{Aut}^1 U_{n+1})$ is representable. □

Observe that the initial step, that $H^1(\mathrm{Aut}^1 U_n)$ is representable (because it is a vector group), fails if we replace Aut^1 by Aut.

By the same argument, we can show that the functor $R \to H^1(\mathrm{Aut}^1(U_n(R \otimes B)))$ is representable. From [10], Proposition 2, we already know that the functor $H^1(U_n)$ is representable, so we turn our attention to the map

$$H^1(U_n) \to H^1(\mathrm{Aut}^1 U_n)$$

now understood to be a map between two representable functors. We need the following technical lemma

Lemma 8.7. *Let X and Y be k-schemes. Suppose that we have a functor morphism*

$$\phi : \mathrm{Hom}(-, X) \to \mathrm{Hom}(-, Y)$$

Then there is a scheme morphism $\Phi : X \to Y$ inducing ϕ.

Proof. This functor map must include a map $\phi(X) : X(X) \to Y(X)$. Let Φ be the image of Id_X. We check that $\Phi_* : \mathrm{Hom}(-, X) \to \mathrm{Hom}(-, Y)$ is equal to ϕ. Let Z/k be a scheme, and let $\theta \in X(Z)$. There is a map $f : X(X) \to X(Z)$, carrying $\alpha : X \to X$ to $\alpha\theta : Z \to X$, which takes Id_x to θ. We consider the application of ϕ to this map:

$$\begin{tikzcd} X(X) \arrow[r, "f"] \arrow[d, "\phi(Z)"'] & X(Z) \arrow[d, "\phi(X)"] \\ Y(X) \arrow[r, "\phi(f)"'] & Y(Z) \end{tikzcd}$$

Here we have $F(Id_X) = \theta$, and $\phi(X)(Id_X) = \Phi$, so that, by the commutativity of this square, we must have $\phi(f)(\Phi) = \phi(Z)(\theta)$. But $\phi(f)$ carries Φ to $\Phi\theta = \Phi_*(\theta)$, so that $\Phi_* = \phi$. □

Note that this result may be viewed as merely an interpretation of the Yoneda Lemma.

We now apply this lemma repeatedly. First, observe that $H^1(U_n)$ satisfies the hypotheses, as does $H^1(U_n(B))$, where B is any $\mathbb{Q}_p$-algebra, and by a slight abuse of notation we write $U_n(B)$ to mean $U_n \times \mathrm{Spec}\, B$. In particular, we can take B to be B_{DR} as defined in [3], definition 1.15.

$$H^1_f(U_n) := ker[H^1(U_n) \to H^1(U_n(B))]$$

must, as a closed subscheme of $H^1(U_n)$, also be representable. Secondly, $H^1(\mathrm{Aut}^1 U_n)$ and $H^1_f(\mathrm{Aut}^1 U_n(B))$ satisfy the hypotheses, so that

$$H^1_f(\mathrm{Aut}^1 U_n) := ker[H^1(\mathrm{Aut}^1 U_n) \to H^1(\mathrm{Aut}^1 U_n(B))]$$

must also be representable.

Thirdly, we apply the lemma to $H^1(U_n)$ and $H^1(\mathrm{Aut}^1 U_n)$, and conclude that the map

$$H^1(U_n) \longrightarrow H^1(\mathrm{Aut}^1 U_n)$$

is algebraic. Finally, since the squares

$$\begin{tikzcd} H^1(U_n)(R) \arrow[r] \arrow[d] & H^1(\mathrm{Aut}^1 U_n)(R) \arrow[d] \\ H^1(U_n)(R \otimes B) \arrow[r] & H^1(\mathrm{Aut}^1 U_n)(R \otimes B) \end{tikzcd}$$

commute, we can conclude that there is an algebraic map $H^1_f(U_n) \to H^1_f(\mathrm{Aut}^1 U_n)$.

We also have a natural action of $H^0(\mathrm{Aut}\, U_1)$ on $H^1(\mathrm{Aut}^1 U_n)$, given by the connecting homomorphism of the long exact sequence associated to the horizontal short exact sequence in 8.1.

Coupled with the identification

Lemma 8.8. *$H^0(\mathrm{Aut}\, U_1) \cong GL_2$ as group schemes.*

Proof. Let R be a $\mathbb{Q}_p$-algebra. By lemma 8.7, we need only show that $H^0(\mathrm{Aut}\, U_1)(R) \cong GL_2(R)$ functorially.

Indeed, we have $GL_2(R) = \mathrm{Hom}(\mathrm{Spec}\, R, GL_2)$, while on the other hand

$$\begin{aligned}
H^0(\mathrm{Aut}\, U_1) &= H^0(\mathrm{Aut}\, \mathrm{Hom}(\mathrm{Spec}\, R, U_1)) \\
&= H^0(\mathrm{Aut}\, \mathrm{Hom}(\mathbb{Q}_p(1)^2 \otimes R)) \\
&= H^0(\mathrm{Aut}(\mathbb{Q}_p(1)^2)^* \otimes R) \\
&= H^0(\mathrm{Aut}(\mathbb{Q}_p(-1)^2 \otimes R) \\
&= H^0(\mathrm{Aut}(\mathbb{Q}_p(-1) \otimes R)^2) \\
&= \{\phi \in \mathrm{Aut}((\mathbb{Q}_p(-1) \otimes R)^2) | g\phi g^{-1} = \phi\} \\
&= GL_2(R)
\end{aligned}$$

Since this equality is functorial in R, we are done. □

This allows us to conclude that there is a geometric action of GL_2 on the scheme $H^1_f(\mathrm{Aut}^1 U_n)$ such that the orbits of the action on the set $H^1_f(G, \mathrm{Aut}^1 U_n)(\mathbb{Q}_p)$ are the fibres of the map $H^1_f(G, U_n)(\mathbb{Q}_p) \to H^1(G, \mathrm{Aut}^1 U_n)(\mathbb{Q}_p)$, which is the 'second map' from 8.1.

8.5.2 De Rham realisations

We make the following definitions.

Definition 24. Let B be the crystalline period ring B_{cr} defined in [3], definition 1.10, and let W be a G representation.

We define $\mathcal{D}(W) := (W \otimes B)^G$. In particular, we will often have cause to refer to $\mathcal{D}(U_n) := (U_n \otimes B)^G$, which we will denote by U_n^{DR}.

We are concentrating our attention here on $H^1_f(G, U_n)$ because of the following observation. Recall the definition of 'geometric' U_n-torsors as torsors that arise from rational points on X.

Lemma 8.9. *Let $\mathcal{P}$ be a 'geometric' torsor for U_n. Then the corresponding class $[\xi] \in H^1(U_n)$ lies in $H^1_f(U_n)$.*

Proof. Following [10], we know that 'geometric' torsors are of De Rham type, and [10], Proposition 5 tells us that De Rham torsors lie in H^1_f. □

We will also make use of the following construction of Kim (the 'level-n Albanese map').

$$H^1_f(U_n) \cong U_n^{DR}$$

The map here may be defined, from left to right, as follows. As in [10], lemma 8, we specify this map of affine schemes on the sets of R points, for arbitrary R - this is sufficient by lemma 8.7. Let $[\xi] \in H^1_f(U_n(R))$ be represented by $\xi : G \to U_n(R)$. By the definition of H^1_f, this must be trivialised by some $a \in U_n(B \otimes R)$. Indeed, consider the set

$$\Omega := \{a \in U_n(B \otimes R) | g(a)a^{-1} = \xi(g)\}$$

There is a natural map $\Omega \times (U_n(B \otimes R))^G \to \Omega$ given by $(\omega, u) \to \omega u$. We know that Ω is non-empty, and we observe that, for any $\omega \in \Omega$, the induced map $\{\omega\} \times (U_n(B \otimes R))^G \to \Omega$ is an isomorphism. Hence we can conclude that Ω is a $(U_n(B \otimes R))^G$-torsor.

By the argument of Besser ([2], corollary 3.2), there is a unique $\gamma_F \in \Omega^{\phi=1}$, and by the argument of Kim ([10]), there is a unique $\gamma_{DR} \in F^0\Omega$. We map $[\xi]$ to '$\gamma_{DR}\gamma_F^{-1}$'. Since Ω is a set, we mean by this the unique transporter from γ_F to γ_{DR}.

The following proof, (a near verbatim reproduction of a proof due to Kim, with $\mathrm{Aut}^1 U_n$ replacing U_n), interprets De Rham torsors in terms of the De Rham fundamental group.

Lemma 8.10.

$$H^1_f(Aut^1 U_n) \cong Aut^1(U_n^{DR})$$

The proof follows immediately from the following four lemmata. First, note that the functor $\mathcal{D}$ commutes with the functor Aut^1. Indeed we have

Lemma 8.11.

$$\mathcal{D}(Aut^1 U_n) \cong Aut^1(\mathcal{D})$$

Proof. Let $\phi \in (\mathrm{Aut}^1 U_n \otimes B)^G$, and $\gamma \in U_n^{DR}$. We have

$$\begin{aligned} \phi(\gamma)^g &= g\phi(g^{-1}\gamma) \quad \text{since } \gamma^{g^{-1}} = g \\ &= (g\phi g^{-1})(\gamma) \\ &= \phi^g(\gamma) \\ &= \phi(\gamma) \quad \text{since } \phi^g = \phi \end{aligned}$$

Thus $\phi(\gamma)$ is G-invariant whenever γ is G-invariant. Hence $\phi \in \mathrm{Aut}^1(U_n \otimes B)^G$, and we have shown that

$$(\mathrm{Aut}^1 U_n \otimes B)^G \hookrightarrow \mathrm{Aut}^1((U_n \otimes B)^G)$$

We note that $\mathrm{Aut}^1((U_n \otimes B)^G)$ should mean $ker(\mathrm{Aut}(U_n^{DR}) \to \mathrm{Aut}(U_1^{DR}))$, so that, in particular, $\mathrm{Aut}^1(U_1 \otimes B)^G = 1$; while on the other hand, $(\mathrm{Aut}^1 U_1 \otimes B)^G$ should mean $ker(\mathrm{Aut}(U_n \otimes B) \to \mathrm{Aut}(U_1 \otimes B))^G$, so that $(\mathrm{Aut}^1 U_1 \otimes B)^G = 1$.

Inductively, we will suppose that $(\mathrm{Aut}^1 U_n \otimes B)^G \cong \mathrm{Aut}^1((U_n \otimes B)^G)$, for some n. We also note that the map set up above will also induce an inclusion

$$(\mathrm{Aut}^n U_{n+1} \otimes B)^G \hookrightarrow \mathrm{Aut}^n((U_{n+1} \otimes B)^G)$$

Passing via the associated Lie algebras

$$\begin{aligned}(\mathrm{Aut}^n(U_{n+1}\otimes B))^G &\cong (\mathrm{Aut}^n(\mathcal{L}_{n+1}\otimes B))^G\\ &\cong \left(\mathrm{Hom}(\mathcal{L}_1\otimes B, \frac{\mathcal{L}^{n+1}}{\mathcal{L}^{n+2}}\otimes B)\right)^G\\ &\cong \mathrm{Hom}\left((\mathcal{L}_1\otimes B)^G, (\frac{\mathcal{L}^{n+1}}{\mathcal{L}^{n+2}}\otimes B)^G\right)\\ &\cong \mathrm{Aut}^n((\mathcal{L}_{n+1}\otimes B)^G)\end{aligned}$$

so we are done by the equality of the dimensions of these objects. □

We need the following technical lemma equating the three restricted cohomology sets of [3].

Lemma 8.12. *We have the following (in)equalities, where H^1_e, H^1_f, and H^1_g are the restricted cohomology sets defined as in [3], definition 3.7.2.*

$$H^1_e(Aut^1U_n) \cong H^1_f(Aut^1U_n) \subseteq H^1_g(Aut^1U_n)$$

Proof. Recall that, by definition, $B_{cr}^{\phi=1} \subseteq B_{cr} \subseteq B_{DR}$. We also know that these restricted cohomology sets all lie naturally inside the set $H^1(\mathrm{Aut}^1U_n)$. For any rings $A_1 \subseteq A_2$, a cocycle with coefficients in Aut^1U_n that is trivialised by base-changing to A_1 is clearly trivialised over A_2, so we conclude that

$$H^1_e(\mathrm{Aut}^1U_n) \subseteq H^1_f(\mathrm{Aut}^1U_n) \subseteq H^1_g(\mathrm{Aut}^1U_n)$$

By the corollary to lemma 8.2, we know that $K^n_{n+1} \cong \mathrm{Hom}(U_1, Z_{n+1})$, which is $\mathrm{Hom}(\mathbb{Q}_p(1)^2, \mathbb{Q}_p(n+1)^{d_n})$ for some d_n. Thus, as in the calculation of lemma 7.6, K^n_{n+1} may be written as a direct sum of copies of $\mathbb{Q}_p(n)$.

By [3], example 3.9, we know that the dimensions of $H^1_e(G,\mathbb{Q}_p(n))$ and $H^1_f(G,\mathbb{Q}_p(n))$ agree for all $n >= 1$. Since $\mathrm{Aut}^1(U_1)$ is trivial, we have $H^1_*(G,\mathrm{Aut}^1U_1) = 1$ for $* = e, f$. We proceed by induction. Suppose the equality holds for $n = k$. Then, since $dim(H^1_*(G,\mathrm{Aut}^1U_{k+1})) = dim(H^1_*(G,\mathrm{Aut}^1U_k)) + dim(H^1_*(G,K^k_{k+1}))$, and since the right hand side of this equation takes the same value for $* = e, f$, we conclude that the equality holds for $n = k+1$. □

Lemma 8.13. *There is an isomorphism*

$$Exp : Aut^1(U_n^{DR}) \longrightarrow H_f^1(Aut^1 U_n)$$

Proof. Recall the following fundamental exact sequence.

$$1 \longrightarrow \mathbb{Q}_p \longrightarrow B_{cr}^{\phi=1} \longrightarrow B_{DR}/B_{DR}^+ \longrightarrow 1$$

from which we obtain the exactness of

$$1 \longrightarrow \mathrm{Aut}^1 U_n \longrightarrow \mathrm{Aut}^1 U_n(B_{cr}^{\phi=1}) \longrightarrow \mathrm{Aut}^1 U_n(B_{DR}/B_{DR}^+) \longrightarrow 1$$

The connecting homomorphism of the associated long exact sequence yields a surjection of $(\mathrm{Aut}^1 U_n(B_{DR}/B_{DR}^+))^G$ surjects onto $H_e^1(\mathrm{Aut}^1 U_n)$, which coincides with $H_g^1(\mathrm{Aut}^1 U_n)$ by lemma 8.12.

Now the inclusion $B_{DR}^+ \hookrightarrow B_{DR}$ yields the exact sequence

$$1 \longrightarrow \mathrm{Aut}^1 U_n \otimes B_{DR}^+ \longrightarrow \mathrm{Aut}^1 U_n \otimes B_{DR} \longrightarrow \mathrm{Aut}^1 U_n \otimes (B_{DR}/B_{DR}^+) \longrightarrow 1$$

B_{DR} is flat and these objects are all De Rham, so the following two rows are identical short exact sequences.

$$\begin{tikzcd}
1 \arrow[r] & (\mathrm{Aut}^1 U_n(B_{DR}^+)) \otimes B_{DR} \arrow[r] \arrow[d, equal] & (\mathrm{Aut}^1 U_n(B_{DR})) \otimes B_{DR} \arrow[r] \arrow[d, equal] & (\mathrm{Aut}^1 U_n(\frac{B_{DR}}{B_{DR}^+})) \otimes B_{DR} \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & (\mathrm{Aut}^1 U_n(B_{DR}^+))^G \otimes B_{DR} \arrow[r] & (\mathrm{Aut}^1 U_n(B_{DR}))^G \otimes B_{DR} \arrow[r] & (\mathrm{Aut}^1 U_n(\frac{B_{DR}}{B_{DR}^+}))^G \otimes B_{DR} \arrow[r] & 1
\end{tikzcd}$$

Since B_{DR} is faithfully flat, we can 'un-tensor'. Furthermore, we recall that the Hodge filtration on U_n, and hence on $\mathrm{Aut}^1 U_n$, is trivial, so that

$$\begin{aligned}
H^0(\mathrm{Aut}^1 U_n \otimes B_{DR}^+) &= H^0(\mathrm{Aut}^1 U_n \otimes F^0 B_{DR}) \\
&= F^0 H^0(\mathrm{Aut}^1 U_n \otimes B_{DR}) \\
&= F^0 \mathrm{Aut}^1 U_n^{DR} = 1
\end{aligned}$$

Combining our results so far, we have surjections

$$\mathrm{Aut}^1 U_n^{DR} = (\mathrm{Aut}^1 U_n \otimes (B_{DR}/B_{DR}^+))^G \to H_g^1(\mathrm{Aut}^1 U_n)$$

for each n. These maps fit into a tower like

$$\begin{tikzcd}
\mathrm{Aut}^1 U_{n+1}^{DR} \arrow[r, two heads] \arrow[d] & H^1_g(\mathrm{Aut}^1 U_{n+1}) \arrow[d] \\
\mathrm{Aut}^1 U_n^{DR} \arrow[r, two heads] & H^1_g(\mathrm{Aut}^1 U_n)
\end{tikzcd}$$

so that we can deduce the surjectivity of the right-hand map. Our understanding of the structure of $\mathrm{Aut}^1 U_n$, expressed in lemma 8.2, shows that $H^0(\mathrm{Aut}^1 U_n) = 1$, so we know that the left-hand map on the bottom row of

$$\begin{tikzcd}
1 \arrow[r] & (K^n_{n+1})^{DR} \arrow[r] \arrow[d] & \mathrm{Aut}^1 U_{n+1}^{DR} \arrow[r] \arrow[d] & \mathrm{Aut}^1 U_n^{DR} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & H^1_g(K^n_{n+1}) \arrow[r] & H^1_g(\mathrm{Aut}^1 U_{n+1}) \arrow[r] & H^1_g(\mathrm{Aut}^1 U_n) \arrow[r] & 1
\end{tikzcd}$$

is injective. By considering dimensions (see [3], corollary 3.8.4), we see that the left-hand vertical map is an isomorphism. By inductively applying the 5-lemma, we can conclude that the middle vertical map is also an isomorphism, and we are done. □

We make the following two observations about this construciton. Firstly, the map Exp may be regarded as simply the projection from $\mathrm{Aut}^1(U_n^{DR})$ to $\mathrm{Aut}^1(U_n(B_{DR}/B^+_{DR}))$, followed by the connecting homomorphism to $H^1(\mathrm{Aut}^1(B^+_{DR}))$.

Secondly, the isomorphism Exp in the last lemma is inverse to the map, D, from $H^1_f(\mathrm{Aut}^1 U_n)$ to $\mathrm{Aut}^1 U_n^{DR}$ described before the statement of lemma 8.10. We prove this in

Lemma 8.14.

$$Exp \circ D = 1$$

Proof. Having defined the isomorphism Exp, we will show that the composition $Exp \circ D$ is the identity, so that D is an isomorphism.

Indeed, we see from the construction above that $H^1_e = H^1_f$, so that an element of H^1_f is already trivialised in $\mathrm{Aut}^1 U_n \otimes B_{cr}^{\phi=1}$. By the same process as above, we can then associate a

$(\mathrm{Aut}^1 U_n \otimes B_{cr}^{\phi=1})^G$-torsor to the class $[\xi]$. But since ϕ acts trivially on $\mathrm{Aut}^1 U_n$, we have

$$\begin{aligned}(\mathrm{Aut}^1 U_n \otimes B_{cr}^{\phi=1})^G &= ((\mathrm{Aut}^1 U_n \otimes B_{cr})^{\phi=1})^G \\ &= ((\mathrm{Aut}^1 U_n \otimes B_{cr})^G)^{\phi=1} \\ &\subseteq (\mathrm{Aut}^1 U_n^{DR})^{\phi=1} \\ &= \{1\}\end{aligned}$$

by the uniqueness of Frobenius-invariance. A $(\mathrm{Aut}^1 U_n \otimes B_{cr}^{\phi})$-torsor, therefore, must be a single element $u_0 \in \mathrm{Aut}^1 U_n \otimes B_{cr}$ satisfying $\xi(g) = g(u_0)u^{-1}$.

Recall that $[\xi] \in H_f^1(\mathrm{Aut}^1 U_n) \subseteq H^1(\mathrm{Aut}^1 U_n)$ may be explicitly identified with the $\mathrm{Aut}^1 V_n$-torsor given by the underlying set $\mathrm{Aut}^1 U_n$ and the twisted G action

$$g : u \longrightarrow \xi(g)^{-1} g(u)$$

(where $g(u)$ means the G-action in $\mathrm{Aut}^1 U_n$). So to say that u_0 trivialises the class of ξ is to say that $\xi(g) = g(u_0)u_0^{-1}$, which in turn may be re-written as $u_0 = \xi(g)^{-1}g(u_0)$, which is equivalent to saying that u_0 is the unique G-invariant element of $\mathrm{Aut}^1 U_n(\xi)$ with the twisted action corresponding to ξ.

Then $D([\xi])$ must be the transporter from $\gamma_{DR} = 1$ (since F_0 is trivial) to $\gamma_F = u_0$, so that $D([\xi]) = u_0$.

We can therefore write

$$\begin{aligned}Exp \circ D([\xi]) &= Exp(u_0) \\ &= \delta(\bar{u}_0)\end{aligned}$$

where δ is the connecting homomorphism from $(\mathrm{Aut}^1 U_n \otimes B_{DR}/B_{DR}^+)^G$ to $H^1(\mathrm{Aut}^1 U_n)$ and $\bar{u}_0$ is the image of u_0 in $(U_n \otimes B/B^+)^G$. But this connecting homomorphism may be realised as sending $\bar{u}_0$ to $\{g \to g(u_0)u_0^{-1}\}$. By the construction of u_0, this is just $\{g \to \xi(g)\}$, so that $Exp \circ D([\xi]) = [\xi]$ as required. □

8.5.3 Proof

Proof of theorem 3.

$$\begin{tikzcd}
 & U_n^{DR} \arrow[r, hook] \arrow[d, equal] & \mathrm{Aut}^1(U_{n+1}^{DR}) \arrow[d, equal] \\
\Omega(\mathbb{Z}_p) \arrow[ur, dashed] \arrow[r] \arrow[drr] & H^1_f(U_n) \arrow[r] & H^1_f(\mathrm{Aut}^1 U_{n+1}) \arrow[d, "/GL_2"] \\
 & & H^1(\mathrm{Aut}\, U_{n+1})
\end{tikzcd}$$

We are now ready to assemble our proof. As discussed earlier in the chapter, let $\mathcal{X}$ be the scheme $\mathbb{P}^1_{\mathbb{Z}_p} \setminus \{0, 1, \infty\}$, so that we recover X as the base-change of $\mathcal{X}$ to $\mathbb{Q}_p$. A $\mathbb{Z}_p$-integral point of $\mathcal{X}$ includes the data of a $\mathbb{Q}_p$ point of X, so to such an integral point we can associate points in $H^1(U_n)$ and in $H^1(\mathrm{Aut}^1 U_n)$ as we can to a rational point of X. Let $x \in \mathcal{X}(\mathbb{Z}_p)$. We denote by $P_n(x)$, $U_n^1(x)$, and $U_n(x)$ the images of x in $H^1(U_n)$, $H^1(\mathrm{Aut}^1 U_{n+1})$, and $H^1(\mathrm{Aut}\, U_{n+1})$ respectively.

Let $y \in \mathcal{X}(\mathbb{Z}_p)$ be any point with $U_n(y) \cong_G U_n(x)$. We know, by lemma 8.9, that $U_n^1(x)$ and $U_n^1(y)$ lie in $H^1_f(\mathrm{Aut}^1 U_{n+1})$. Since they map to the same point in $H^1(\mathrm{Aut}\, U_{n+1})$, we know that these torsors lie in the same $H^0(\mathrm{Aut}\, U_1)$-orbit, by lemma 7.3.

Recall also that $H^1_f(\mathrm{Aut}^1 U_{n+1})$ is representable by lemma 8.6, that $H^0(\mathrm{Aut}\, U_1) \cong GL_2$, and that by lemma 8.7 the action of the latter on the former is algebraic. The orbits of this action are locally closed, so that this orbit is contained in some closed subscheme Z with $U_n^1(x) \in Z \subseteq H^1_f(\mathrm{Aut}^1 U_{n+1})$ such that any y with $U_n(y) \cong_G U_n(x)$ satisfies $U_n(y) \in Z$.

The pre-image, W, of Z in $H^1_f(U_n)$ is also a closed subscheme, since the map $H^1_f(U_n) \to H^1_f(\mathrm{Aut}^1 U_{n+1})$ is algebraic. That is, $W \subseteq H^1_f(U_n)$ is a closed subscheme containing $P_n(y)$ for all y with $U_n(y) \cong_G U_n(x)$.

W is the pre-image of an orbit of GL_2 under the map $H^1_f(U_n) \to H^1_f(\mathrm{Aut}^1 U_{n+1})$. By the identifications $H^1_f(U_n) \cong U_n^{DR}$ and $H^1_f(\mathrm{Aut}^1 U_{n+1}) \cong \mathrm{Aut}^1 U_{n+1}^{DR}$, we identify this map with the injection (since U is centre-free) $U_n^{DR} \to \mathrm{Aut}^1 U_{n+1}^{DR}$. It follows that the dimension of W is not greater than $dim(GL_2) = 4$, so that whenever $dim(U_n^{DR}) > 4$, W must be a proper closed subscheme. This happens if $n \geq 3$.

Now set $n = 3$. Let $p \geq 7$, so that $(p-1)/2 \geq (n+1)$, satisfying the hypotheses of the main theorem of [10].Let f be any non-zero function on U_n^{DR} that vanishes on W. Following [11], we know that the map from the $\mathbb{Z}_p$-points of $\mathcal{X}$ to U_n^{DR} is analytic, and that the function f pulls back to a non-constant analytic function on each residue disc of $X(\mathbb{Q}_p)$. This therefore has only finitely many zeroes, from which we conclude that only finitely many points of $X(\mathbb{Z}_p)$ can map to Z.

We conclude that, whenever $p \geq 7$, every W as above must be contained in a proper closed subscheme. Then $W \cap im(X(\mathbb{Z}_p))$ is finite, so the map from integral points to $H^1(G, \mathrm{Aut}\, U_3)$ is finite to one. The fibres of the map to $H^1(G, \mathrm{Aut}\, U_m)$ for any $m > 3$, or the map to $H^1(G, \mathrm{Aut}\, U)$, cannot be larger; so these must also be finite. $\square$

References

[1] G. V. Belyi. On Galois Extensions of a Maximal Cyclotomic Field. *Izv. Akad. Nauk SSSR*, 8:267–276, 1979. English translation in Math. USSR Izv. 14 (1980) no. 2, pp 247-256.

[2] A. Besser. Coleman Integration Using The Tannakian Formalism. *Math. Ann.*, 322(1):19–48, 2002.

[3] S. Bloch and K. Kato. L-Functions and Tamagawa numbers of Motives. *Grothendieck Festschrift*, I:333–400, 1990.

[4] J. Carlson. Extensions of Mixed Hodge Structures. *Journees de Geometrie Algebrique d'Angers*, pages 77–105, 1980.

[5] P. Deligne. Le Groupe Fondamental de la Droite Projective Moins Trois Points. *Galois Groups over $\mathbb{Q}$ MSRI Publ*, 16:79–298, 1989.

[6] A. Grothendieck et al. *Revetments Etales et Groupe Fondamental*, volume 224 of *Lecture Notes in Mathematics*. Springer-Verlag, 1971.

[7] R. M. Hain. The Geometry of the Mixed Hodge Structure on the Fundamental Group. *Proc. Symp. Pure Math*, 46:247–282, 1987.

[8] R. M. Hain and M. Matsumoto. Weighted Completion of Galois Groups and Galois Actions on the Fundamental Group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. *Compositio Math.*, 139(2):119–167, 2003.

[9] G. Hochschild. Note on Algebraic Lie Algebras. *Proceedings of the American Mathematical Society*, 29(1):10–16, June 1971.

[10] M. Kim. The Motivic Fundamental Group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the Theorem of Siegel. *Invent. Math*, 161(3):629–656, 2005.

[11] M. Kim. The Unipotent Albanese Map and Selmer Varieties for Curves. *Publ. RIMS*, 45:89–133, 2009.

[12] M. Kim. Massey Products for Elliptic Curves of Rank 1. *J. Amer. Math. Soc.*, 23:725–747, 2010.

[13] J. S. Milne. *Etale Cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, 1980.

[14] Milne, J. S. Abelian varieties. *Arithmetic Geometry*, pages 103–150, 1985. ed. Silverman, J. H. and Cornell, G.

[15] S.. Mochizuki. The Local pro-p Anabelian Geometry of Curves. *RIMS pre-print 1097*, 1996. Kyoto University.

[16] H. Nakamura. On Galois Automorphisms of the Fundamental Group of the Projective Line Minus Three Points. *Math. Z.*, 206(4):617–622, 1991.

[17] H. Nakamura, A. Tamagawa, and S. Mochizuki. The Grothendieck Conjecture on the Fundamental Groups of Algebraic Curves [Translation of Sugaku 50]. *Sugaku Expositions*, 14(1):31–53, 2001.

[18] D. Quillen. Rational Homotopy Theory. *Annals of Mathematics*, 90(2):205–295, 1969.

[19] J-P Serre. *Galois Cohomology*. Springer Monographs in Mathematics. Springer, 2002.

[20] T. Szamuely. *Galois Groups and Fundamental Groups*, volume 117 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2009.

[21] C. A. Weibel. *An Introduction to Homological Algebra*. Cambridge, 1994.

[22] A. Weil. The Field of Definition of a Variety. *American Journal of Mathematics*, 78:509–524, 1956.