Galois actions on non-abelian finite groups and applications

Junghwan Lim

Merton College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Michaelmas 2017

Statement of Originality

I declare that the work in this thesis is, to the best of my knowledge, original and my own work, except where otherwise indicated, cited, or commonly known. This thesis has not been submitted for a degree at another university.

Junghwan Lim
Oxford, 17 October 2017

Acknowledgements

The little understanding I have acquired over the course of my study is entirely due to the company of several people who I wish to thank here.

First and foremost, it has been a wonderful privilege to be a student of Minhyong Kim. I have benefited mathematically and personally from his generosity, patience and encouragement and from many inspiring conversations. This thesis is a poor reflection of the assistance and guidance I have received from him over the past four years.

I am very grateful to Francesca Balestrieri, Alexander Betts, Netan Dogra, and Jan Vonk for providing great times in Mathematical Institute.

I thank all the people that have given colour to my life during my time in Oxford. In particular, I thank Seung Hoon Chae, Jiwoong Choi, Joon Son Chung, Seungchan Ko, and Joonkyung Lee for sharing plenty of enjoyable moments.

Finally, I thank my family for the countless things they have done for me. They mean the world to me, and this thesis is dedicated to them.

Abstract

In this thesis, we consider the Galois actions on some finite characteristic quotients of the geometric fundamental groups of once-punctured elliptic curves. In particular, those of which can be naturally regarded as *non-abelian* lifts of usual mod ℓ Galois representations attached to elliptic curves. We also find its applications to some questions in the realm of Diophantine geometry.

Contents

List of Figures

Chapter 1

Introduction

In his letter [8] to Faltings, Grothendieck has pointed out the importance of the study of Galois actions on geometric fundamental groups of hyperbolic curves over number fields.

Even though Grothendieck's suggestion may be the first moment for emphasising the study of how Galois groups act on *full* fundamental groups, the study of Galois actions on *abelian* (characteristic) quotients of fundamental groups has already been taking a central position in the world of arithmetic geometry for several decades. For example, for a given elliptic curve E over a number field K with zero-section O, Serre [21] has studied the ℓ-adic Galois representations

$$T_\ell E = \varprojlim_n E[\ell^n]$$

attached to E, for (varying) primes ℓ, where each $T_\ell E$ may be viewed as the maximal abelian pro-ℓ quotient of the geometric fundamental group of $E^\circ := E - O$.

In fact, it is already hard to get a satisfactory understanding of Galois actions on abelian quotients of fundamental groups, so working with full fundamental groups might be a forbidding task. One reason that the problem gets harder is ignorance of expected information which can be extracted from there. Nevertheless, it is believed that there should exist much interesting information living in Galois actions on full fundamental groups, we hardly know what is in there and how to obtain it.

In a series of papers [12], [13], and [14], Kim has achieved really fascinating results on finiteness of integral points on some hyperbolic curves.

Also, in a recent paper [2], Brown has obtained a really striking result saying that the motivic fundamental group of thrice-punctured projective line generates the category of mixed Tate motives over Spec$\mathbb{Z}$.

In this thesis, we are going to study

(A) Galois actions on finite *non-abelian* quotients of geometric fundamental groups of once-punctured elliptic curves,

(B) some applications of (A).

1.1 Main results: direction (A)

To give the statements of main results, we firstly need to set up some basic facts. Let E be an elliptic curve over a number field K with the zero-section O. Let I_O be the sheaf of ideals defining the zero-section. If we are given a nowhere vanishing invariant differential ω, forming a K-basis of

$$\underline{\omega}_{E/K} := f_*(\Omega^1_{E/K})$$

where $f : E \to \mathrm{Spec}K$ is the structure morphism, then, as explained in [17, §2.1], there exists a *unique* basis $\{1, x, y\}$ of $f_*(I_O^{-3})$ and *uniquely* determined elements $g_2, g_3 \in K$ such that

(1) $g_2^3 - 27g_3^2 \neq 0$,

(2) the affine ring $H^0(E - O, \mathscr{O}_E) = \varinjlim_n H^0(E, I_O^{-n})$ is of the form

$$K[x, y]/(y^2 - (4x^3 - g_2x - g_3)),$$

and

(3) $\omega = \frac{\mathrm{d}x}{y}$.

Definition 1.1.1. The invariant $\Delta_{\mathrm{mod}} := g_2^3 - 27g_3^2$ is called the *modular discriminant* of E.

Remark 1.1.2. As one may see in the above, Δ_{mod} depends on the choice of a nowhere vanishing invariant differential ω. So, Δ_{mod} is well-defined only when ω is fixed.

From now on, we fix a pair (E, ω) of an elliptic curve E over a fixed number field K with zero-section O and K-basis ω of $\underline{\omega}_{E/K}$.

Let $\bar{E}^\circ$ be the base change of $E^\circ := E - O$ along $\mathrm{Spec}\bar{K} \to \mathrm{Spec}K$, where $\bar{K}$ is a fixed algebraic closure of K. From given ω, by following [5, §15], we can define a functor

$$v : \mathfrak{Fet}(\bar{E}^\circ) \to \mathfrak{fset}$$

from the category of schemes which are finite étale over $\bar{E}^\circ$ to the category of finite sets so that the automorphism group

$$\pi_1^{\text{ét}}(\bar{E}^\circ) := \mathrm{Aut}(v),$$

known to be a profinite group, admits a continuous action by the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ of K. The Galois action on $\pi_1^{\text{ét}}(\bar{E}^\circ)$ is sufficiently interesting in the following sense: for any prime ℓ, the ℓ-adic Tate module $T_\ell E$ of E is canonically the maximal abelian pro-ℓ quotient of $\pi_1^{\text{ét}}(\bar{E}^\circ)$ so that the $\mathrm{Gal}(\bar{K}/K)$-action on $T_\ell E$ inherited from the $\mathrm{Gal}(\bar{K}/K)$-action on $\pi_1^{\text{ét}}(\bar{E}^\circ)$ produces usual ℓ-adic Galois representation

$$\mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}(T_\ell E)$$

attached to E.

For a given odd prime ℓ, we consider two finite characteristic quotients $Q_s[\ell]$, $s = 2, 3$ of $\pi_1^{\text{ét}}(\bar{E}^\circ)$ satisfying the following properties:

(a) under the $\mathrm{Gal}(\bar{K}/K)$-action on $Q_2[\ell]$ inherited from $\pi_1^{\text{ét}}(\bar{E}^\circ)$, we have Galois equivariant isomorphisms

$$Z(Q_2[\ell])^1 = \mu_\ell \text{ and } Q_2[\ell]/Z(Q_2[\ell]) = E[\ell].$$

(b) under the $\mathrm{Gal}(\bar{K}/K)$-action on $Q_3[\ell]$ inherited from $\pi_1^{\text{ét}}(\bar{E}^\circ)$, we have Galois equivariant isomorphisms

$$Z(Q_3[\ell]) = E[\ell] \otimes \mu_\ell \text{ and } Q_3[\ell]/Z(Q_3[\ell]) = Q_2[\ell].$$

[1] As usual, for a given abstract group G, its centre is denoted by $Z(G)$.

From (a) and (b), we obtain Galois representations

$$\varrho_s[\ell] : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathrm{gp}}(Q_s[\ell])$$

for $s = 2, 3$ such that, when $\varrho_s[\ell]$ is composed with the natural group homomorphism

$$\mathrm{Aut}_{\mathrm{gp}}(Q_s[\ell]) \to \mathrm{Aut}_{\mathrm{gp}}(E[\ell]),$$

we obtain the mod-ℓ Galois representation

$$\mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathrm{gp}}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$$

attached to E. Hence we may view both $\varrho_2[\ell]$ and $\varrho_3[\ell]$ as *non-abelian* lifts of the mod ℓ Galois representation attached to E.

Definition 1.1.3. For each $s = 2, 3$, we set $K_s[\ell]$ to be the subfield of $\bar{K}$ fixed by $\ker(\varrho_s[\ell])$, i.e.

$$\mathrm{Gal}(\bar{K}/K_s[\ell]) = \ker(\varrho_s[\ell]).$$

With this definition, our first goal is to find generators of $K_s[\ell]$ over K.

Theorem 1.1.4. *We have*

(i) $K_2[\ell] = K(E[\ell])$ *for any odd prime* ℓ*,*

(ii) $K_3[\ell] = K(E[\ell])(\Delta_{\mathrm{mod}}^{1/\ell})$ *for any prime* $\ell > 3$ *(note that we are given a nowhere vanishing invariant differential* ω*, so* Δ_{mod} *is well-defined).*

1.2 Main results: direction (B)

1.2.1 First application

Let us further assume that our elliptic curve E has a K-rational non-torsion point α. For each prime ℓ, we consider the Galois extension

$$K_{\alpha,\ell}$$

of K generated by all $z \in E(\bar{K})$ such that $\ell \cdot z = \alpha$. It is known that $K_{\alpha,\ell}$ is a Galois extension of $K(E[\ell])$.

Under this setting, we can define a group homomorphism

$$\varphi_\ell : \mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell])) \to E[\ell]$$

in the following way: take any $z \in E(\bar{K})$ such that $\ell \cdot z = \alpha$. Define

$$\varphi_\ell(g) = g(z) - z.$$

Then it can be easily check that φ_ℓ is an injective group homomorphism.

In [20], Ribet has studied this homomorphism φ_ℓ:

Theorem 1.2.1 (Ribet)**.** *When E has complex multiplication, the homomorphism*

$$\varphi_\ell : \mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell])) \to E[\ell]$$

defined in the above is an isomorphism for almost all prime ℓ.

Remark 1.2.2. In fact, Ribet proved similar theorems for all CM abelian varieties.

Before we consider *non-abelian* generalisations of Ribet's theorem, we firstly consider the non-CM generalisation:

Theorem 1.2.3. *Even when E has no complex multiplication, the homomorphism*

$$\varphi_\ell : \mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell])) \to E[\ell]$$

is an isomorphism for almost all primes ℓ.

To find the right non-abelian generalisation of the work of Ribet, we need the following lemma:

Lemma 1.2.4. *For each prime ℓ, there is a homomorphism*

$$\Phi_\ell : \mathrm{Gal}(\bar{K}/K(E[\ell])) \to E[\ell]$$

describing how the Galois group $\mathrm{Gal}(\bar{K}/K(E[\ell]))$ *acts on "the set of étale $E[\ell]$-paths from v to α on $\bar{E}^\circ$" so that Ribet's thereom is equivalent to surjectivity of Φ_ℓ for almost all primes ℓ.*

The phrase "the set of ..." in the above lemma will be defined properly later in the thesis (chapter 4), and was omitted so as not to over-complicate the exposition.

To introduce our first application in a simple form, we make an ad hoc definition:

Definition 1.2.5. A prime ℓ is called an *R-prime* if the map

$$\Phi_\ell : \mathrm{Gal}(\bar{K}/K(E[\ell])) \to E[\ell]$$

in Lemma 1.2.4 is surjective.

Theorem 1.2.6. *For each prime ℓ and each $s = 2, 3$, there is a homomorphism*

$$\Psi_{s,\ell} : \mathrm{Gal}(\bar{K}/K_s[\ell]) \to Q_s[\ell]$$

which describes the $\mathrm{Gal}(\bar{K}/K_s[\ell])$*-action on "the set of étale $Q_s[\ell]$-paths from v to α on $\bar{E}^\circ$". Moreover, we have*

(i) $\Psi_{2,\ell}$ *is surjective for every R-prime ℓ,*

(ii) $\Psi_{3,\ell}$ *is surjective for any R-prime ℓ such that the modular discriminant Δ_{mod} of E admits an ℓ-th root in $K(E[\ell])$.*

1.2.2 Second application

Recall that for any integer $N \geq 1$, a level-N-structure on E is defined to be an isomorphism

$$E[N] \simeq \mathbb{Z}/N \times \mathbb{Z}/N.$$

Since $E[N]$ is naturally regarded as a quotient of $\pi_1^{\text{ét}}(\bar{E}^\circ)$, a level-$N$-structure on E may be considered as a surjective homomorphism

$$\pi_1^{\text{ét}}(\bar{E}^\circ) \twoheadrightarrow \mathbb{Z}/N \times \mathbb{Z}/N.$$

One may generalise this picture to any finite group G admitting a surjective homomorphism from F_2 (the free group of rank 2). In fact, in the (very) recent paper [3], William Y. Chen has succeeded to establish this idea very precisely. He defined the notion of *G-structures* on elliptic curves E over connected schemes S for any finite group G which can be generated by two elements. For such group G, a G-structure on an elliptic curve E over a connected scheme S is represented by an element of

$$\mathrm{Hom}^{\text{sur-ext}}(F_2, G) := \mathrm{Hom}^{\text{sur}}(F_2, G)/\mathrm{Inn}(G)$$

where F_2 is the free group of rank 2 and $\mathrm{Hom}^{\mathrm{sur}}(F_2, G)$ is the set of surjective homomorphisms $F_2 \twoheadrightarrow G$ and $\mathrm{Inn}(G)$ is the group of inner automorphisms of G.

After giving the definition of G-structures, he considered the moduli stack

$$\mathscr{M}(G)$$

of elliptic curves with G-structures. It is proven that $\mathscr{M}(G)$ is a smooth and separated Deligne–Mumford stack over $\mathbb{Z}[\frac{1}{\#G}]$.

Theorem 1.2.7 (Chen). *(i) When $G = \mathbb{Z}/N \times \mathbb{Z}/N$ for some integer $N \geq 1$, the G-structures on an elliptic curve E over a connected scheme S agree with the usual level-N-structures on E.*

(ii) Let G be a finite group which can be generated by two elements. If $f : G \twoheadrightarrow G'$ is a surjective homomorphism of groups, then f induces a surjective finite étale morphism

$$f_* : \mathscr{M}(G) \to \mathscr{M}(G').$$

Our second application concerns rational points on some $\mathscr{M}(G)$: for $s = 2, 3$ and a prime ℓ, we define abstract groups $G_s[\ell]$ by

- $G_2[\ell]$ is a group such that $Z(G_2[\ell]) \simeq \mathbb{Z}/\ell$ and $G_2[\ell]/Z(G_2[\ell]) \simeq \mathbb{Z}/\ell \times \mathbb{Z}/\ell$,
- $G_3[\ell]$ is a group such that $Z(G_3[\ell]) \simeq \mathbb{Z}/\ell \times \mathbb{Z}/\ell$ and $G_3[\ell]/Z(G_3[\ell]) \simeq G_2[\ell]$.

The reader may already notice that these groups $G_s[\ell]$ are modelled by the quotients $Q_s[\ell]$ of $\pi_1^{\text{ét}}(\bar{E}^\circ)$.

Theorem 1.2.8. *Let ℓ be a prime greater than* 3.

(a) Let F be a number field. Then any F-rational point z of $\mathscr{M}(\mathbb{Z}/\ell \times \mathbb{Z}/\ell)$ lifts to $\mathscr{M}(G_2[\ell])$:

$$\begin{tikzcd} & \mathscr{M}(G_2[\ell]) \arrow[d] \\ \mathrm{Spec} F \arrow[r, "z"'] \arrow[ur, dashed] & \mathscr{M}(\mathbb{Z}/\ell \times \mathbb{Z}/\ell) \end{tikzcd}$$

(b) *Let F be a number field. Let z be a F-rational point of $\mathscr{M}(\mathbb{Z}/\ell \times \mathbb{Z}/\ell)$. If the underlying elliptic curve E_z of z admits a nowhere vanishing invariant differential ω such that the modular discriminant Δ_{mod} determined by ω has a F-rational ℓ-th root, then z lifts to $\mathscr{M}(G_3[\ell])$.*

$$\begin{tikzcd} & \mathscr{M}(G_3[\ell]) \arrow[d] \\ \mathrm{Spec} F \arrow[r, "z"'] \arrow[ur, dashed] & \mathscr{M}(\mathbb{Z}/\ell \times \mathbb{Z}/\ell) \end{tikzcd}$$

1.3 Outline

In chapter 2 we review general definition of étale fundamental groups. After that we see how the absolute Galois group of the base field acts on geometric fundamental groups with particular base points. In the following section, we see how to make precise the notion of étale paths and prove some foundational results, which are possibly well-known to experts, for later usage.

In the next chapter we study Galois actions on the finite groups $Q_2[\ell]$ and $Q_3[\ell]$. We firstly see how the preliminary theories are applied to our setting. After giving the constructions of $Q_s[\ell]$, we develop some necessary theories for the study of Galois actions. In the last section of chapter 3, we see how the theory of elliptic polylogarithms of Beilinson and Levin is particularly helpful for the study of Galois action on $Q_3[\ell]$.

The last two chapters are devoted to the study of some applications of the contents in chapter 3. In chapter 4, we review the classical result of Ribet and see how it can be interpreted in terms of our language. This interpretation enables us to find a generalisation of Ribet's work which we study in the last section. In chapter 5, we briefly review the theory of G-structures recently developed by W. Y. Chen, and we see how our study can be used for the study of the set of rational points of moduli stack of elliptic curves with G-structures.

Conventions

For a scheme X over a field K, its base change to a (fixed) algebraic closure $\bar{K}$ of K is denoted by $\bar{X}$, i.e. $\bar{X} = X \times_{\mathrm{Spec}K} \mathrm{Spec}\bar{K}$. When X_1 and X_2 are schemes over $\bar{K}$, we denote their fibred product over Spec$\bar{K}$ simply by

$$X_1 \times_{\bar{K}} X_2.$$

For any scheme X, its underlying set is denoted by $|X|$.

The category of finite sets is denoted by $\mathfrak{fset}$. If π is a topological group, then the category of finite discrete sets endowed with continuous (left) π-actions is denoted by π-$\mathfrak{fset}$. For a scheme X, the category of schemes over X is denoted by

$$\mathfrak{Sch}_X.$$

For a connected scheme X, we denote by

$$\mathfrak{Sch}_{X,\text{ét}}$$

the big étale site of X.

For any group G, we use the convention for the commutator of two elements g, h of G that $[g,h] = ghg^{-1}h^{-1}$. Also, for any topological group G, each subgroup occurring in the lower central series

$$G = G_1 \supset G_2 = [G, G_1] \supset \ldots \supset G_{n+1} = [G, G_n] \supset \ldots$$

of G is always considered as the minimal *closed* subgroup generated by iterated commutators. For example, $G_3 = [G,[G,G]]$ is the minimal closed subgroup G generated by $[g_1,[g_2,g_3]]$ for all $g_1, g_2, g_3 \in G$.

If $f : X \to Y$ is a map of mathematical objects (for example, sets, groups, modules, etc.) equipped with actions by a group G, we say that f is G-*equivariant* if

$$f(g \cdot x) = g \cdot f(x)$$

holds for any $g \in G$ and $x \in X$.

Chapter 2

Preliminaries

In this chapter we review some foundational theories related with étale fundamental groups. The first section is devoted to a recap of the theory of Galois categories. In section 2 we see that how one can define Galois actions on étale fundamental groups, which is the central theme of our study. In the last section we review some basic theory of equivariant torsors and prove some properties of étale path torsors and their push-outs which are used in the analysis of the Galois actions on some finite quotients of the geometric fundamental groups of once-punctured elliptic curves.

2.1 Abstract theory of Galois categories

The theory of Galois categories was developed by Grothendieck [7] in an effort to define for schemes an analogue of the correspondence between finite covering spaces of a connected topological space X and finite sets equipped with actions by the usual topological fundamental group of X. Instead of Grothendieck's original formalism, we closely follow the article [15] by Lenstra.

Definition 2.1.1. Let $\mathfrak{C}$ be a category and F a covariant functor from $\mathfrak{C}$ to $\mathfrak{fset}$. We say that $\mathfrak{C}$ is a *Galois category* with *fundamental functor* F if it satisfies the following conditions:

(a) $\mathfrak{C}$ has a terminal object and fibred products,

(b) $\mathfrak{C}$ has finite sums, and for any object in $\mathfrak{C}$ the quotient by a finite group of automorphisms exists,

(c) any morphism f in $\mathfrak{C}$ factorises as $f = f' \circ f''$ where f'' is an epimorphism and f' is a monomorphism, and any monomorphism $m : X \to Y$ in $\mathfrak{C}$ is an isomorphism of X with a direct summand of Y,

(d) the functor F preserves terminal objects and commutes with fibred products,

(e) the functor F commutes with finite sums, preserves epimorphisms, and commutes with passage to the quotient by a finite group of automorphisms,

(f) if f is a morphism in $\mathfrak{C}$ such that $F(f)$ is an isomorphism, then f is an isomorphism.

If $\mathfrak{C}$ is a Galois category with fundamental functor F, the automorphism group $\mathrm{Aut}(F)$ of F is known to be a profinite group. For any object X in $\mathfrak{C}$, the profinite group $\mathrm{Aut}(F)$ acts continuously on the finite set $F(X)$, where $F(X)$ is viewed as a topological space endowed with the discrete topology. In other words, the stabiliser in $\mathrm{Aut}(F)$ of any element of $F(X)$ is open. Moreover, we can see that, for any morphism f in $\mathfrak{C}$, $F(f)$ is a morphism of $\mathrm{Aut}(F)$-sets. Hence we find a functor

$$\mathfrak{C} \to \mathrm{Aut}(F)\text{-}\mathfrak{fset}$$

arising naturally from F. Let us call this functor by $\tilde{F}$.

The following theorem is one of main theorems in the theory of Galois categories.

Theorem 2.1.2 ([15, 3.5])**.** *Let $\mathfrak{C}$ be an essentially small Galois category with fundamental functor F. Let $\tilde{F} : \mathfrak{C} \to \mathrm{Aut}(F)\text{-}\mathfrak{fset}$ be the functor as defined in the above. Then we have:*

(a) the functor $\tilde{F}$ is an equivalence of categories,

(b) if π is a profinite group such that the categories $\mathfrak{C}$ and $\pi\text{-}\mathfrak{fset}$ are equivalent by an equivalence that, when composed with the forgetful functor $\pi\text{-}\mathfrak{fset} \to \mathfrak{fset}$, yields the functor F, then π is canonically isomorphic to $\mathrm{Aut}(F)$,

(c) if F' is a second fundamental functor on $\mathfrak{C}$, then F and F' are isomorphic,

(d) if π is a profinite group such that the categories $\mathfrak{C}$ and π-$\mathfrak{fset}$ are equivalent, then there is an isomorphism of profinite groups $\pi \simeq \mathrm{Aut}(F)$ that is canonically determined up to an inner automorphism of $\mathrm{Aut}(F)$.

We will see some examples of Galois categories in the following section.

2.2 Étale fundamental groups and Galois actions

2.2.1 Étale fundamental groups

Let X be a scheme. A pair (Y, f) of a scheme Y and a finite étale morphism $f : Y \to X$ is called an *étale covering* of X. A *morphism* $\varphi : (Y_1, f_1) \to (Y_2, f_2)$ of étale coverings of X is a morphism $Y_1 \to Y_2$ of schemes compatible with f_1 and f_2, i.e. a dotted arrow making the following diagram commute:

$$\begin{tikzcd} Y_1 \arrow[rr, dotted] \arrow[dr, "f_1"'] & & Y_2 \arrow[dl, "f_2"] \\ & X & \end{tikzcd}$$

Obviously, the collection of étale coverings of a scheme X forms a category and we denote this category of étale coverings of X by $\mathfrak{Fet}(X)$. For simplicity, an étale covering (Y, f) of X is usually denoted by Y. Also, we denote a morphism $\varphi : (Y_1, f_1) \to (Y_2, f_2)$ of étale coverings of X simply by $\varphi : Y_1 \to Y_2$.

Definition 2.2.1. Let η be a geometric point of a scheme X. We define a functor

$$F_\eta : \mathfrak{Fet}(X) \to \mathfrak{fset}$$

by setting $F_\eta(Y)$ as the underlying set of Y_η. The functor F_η is called the *fibre functor* at η.

Theorem 2.2.2 ([15, 3.6])**.** *Let X be a connected scheme and η a geometric point of X. The category $\mathfrak{Fet}(X)$ is a Galois category with fundamental functor F_η.*

Definition 2.2.3. Let X be a connected scheme and η a geometric point of X. The *étale fundamental group* $\pi_1^{\text{ét}}(X, \eta)$ of X with base point η is defined to be the profinite group $\mathrm{Aut}(F_\eta)$.

Example 2.2.4. Let F be a number field with a fixed algebraic closure $\bar{F}$ and $X = \mathrm{Spec}F$. Let $\eta : \mathrm{Spec}\bar{F} \to X$ be the geometric point induced by the inclusion $F \hookrightarrow \bar{F}$. Then $\mathfrak{Fet}(X)$ is a Galois category with fundamental functor $F_\eta : \mathfrak{Fet}(X) \to \mathfrak{fset}$. In this case, the étale fundamental group $\pi_1^{\text{ét}}(X, \eta)$ of X with base point η is the same as the absolute Galois group $\mathrm{Gal}(\bar{F}/F)$ of F. For details, we refer to [15, 2.9].

Example 2.2.5. Let F be a number field with a fixed algebraic closure $\bar{F}$. By applying the Riemann–Hurwitz formula, one can see that every étale covering of $\mathbf{G}_{m,\bar{F}}$ may be expressed in the form

$$\mathbf{G}_{m,\bar{F}} \xrightarrow{(\cdot)^s} \mathbf{G}_{m,\bar{F}}$$

for some integer $s \geq 1$. With this observation, from the discussion given later in §2.2.5, we see that

$$\pi_1^{\text{ét}}(\mathbf{G}_{m,\bar{F}}, 1) \simeq \widehat{\mathbb{Z}}(1)$$

where 1 in the left hand side is the geometric point $1 \in \mathbf{G}_{m,\bar{K}}(\bar{K})$.

Remark 2.2.6. When X is a geometrically connected scheme over a field K, the étale fundamental group $\pi_1^{\text{ét}}(\bar{X}, \eta)$ of $\bar{X}$ with base point by some geometric point η of $\bar{X}$ is usually called the *geometric fundamental group* of X.

In general, it is quite hard to give any explicit description of the étale fundamental group of a given connected scheme. However, we can sometimes find presentations of étale fundamental groups by the following theorem:

Theorem 2.2.7 ([7, Exposé XII Corollaire 5.2])**.** *Let X be a connected scheme of finite type over $\mathbb{C}$. Let X^{an} be the complex analytic space associated to X. For any $\eta : \mathrm{Spec}\mathbb{C} \to X$, there is an isomorphism*

$$\pi_1\widehat{(X^{\text{an}}, \eta^{\text{an}})} \simeq \pi_1^{\acute{e}t}(X, x)$$

where the left hand side is the profinite completion of the topological fundamental group of X^{an} with base point η^{an} associated to η.

2.2.2 Rational geometric points

Let K be a number field with a fixed algebraic closure $\bar{K}$.

Definition 2.2.8. Let X be a scheme over K. A geometric point η of X is called *rational* if it is of the form

$$\mathrm{Spec}\bar{K} \to \mathrm{Spec}K \xrightarrow{x} X$$

for $x \in X(K)$.

Remark 2.2.9. Let X be a scheme over K. If $\eta : \mathrm{Spec}\bar{K} \to X$ is a geometric point of X, it naturally produces a geometric point of $\bar{X}$ (a unique dashed arrow given by the universal property of the fibred products):

$$\begin{tikzcd} & \mathrm{Spec}\bar{K} \\ \mathrm{Spec}\bar{K} \arrow[ur, equal] \arrow[r, dashed] \arrow[dr, "\eta"'] & \bar{X} \arrow[u] \arrow[d] \\ & X \end{tikzcd}$$

where the vertical arrows are natural projections. By abuse of notation, we write η for this geometric point of $\bar{X}$. Also, we say that a geometric point $\eta : \mathrm{Spec}\bar{K} \to \bar{X}$ is *rational* if it is produced from a rational geometric point of X as in the above diagram.

2.2.3 Rational tangential points

Let K be a number field with a fixed algebraic closure $\bar{K}$. Recall that a *hyperbolic curve* U over K is a curve over K of the form $X \setminus D$ where X is a smooth projective curve over K of genus g and D is a divisor over K with $r := \#D(\bar{K}) < \infty$ such that $2g - 2 + r > 0$[1]. Since we are particularly interested in the case $r > 0$, we always assume this unless specified.

Definition 2.2.10. Let X be a smooth projective curve over K. We define the *tangent space* $T_{\bar{X},x}$ at $x \in \bar{X}(\bar{K})$ to be

$$T_{\bar{X},x} = \mathrm{Spec}\left(\bigoplus_{i \geq 0} \mathfrak{m}_x^i / \mathfrak{m}_x^{i+1}\right)$$

[1]When $g = 0$, we only consider the case $r \geq 3$. Also, when $g = 1$, we should have $r \geq 1$. Lastly, if $g \geq 2$, then r can be arbitrary non-negative integer.

where $\mathfrak{m}_x$ is the maximal ideal of the local ring $\mathscr{O}_{\bar{X},x}$. Here, by convention, we define $\mathfrak{m}_x^0 = \mathscr{O}_{\bar{X},x}$. We also set, so-called *the punctured tangent space*, $T^{\circ}_{\bar{X},x} = \operatorname{Spec}\left(\bigoplus_{i\in\mathbb{Z}} \mathfrak{m}_x^i/\mathfrak{m}_x^{i+1}\right)$.

Remark 2.2.11. Let X be a smooth projective curve over K. Let $x \in \bar{X}(\bar{F})$. Then, by a choice of uniformiser of the local ring $\mathscr{O}_{\bar{X},x}$, one can define an isomorphism

$$T^{\circ}_{\bar{X},x} \simeq \mathbf{G}_{m,\bar{K}}$$

of schemes over $\bar{K}$.

Let U be a geometrically connected hyperbolic curve over K. Let $x \in \bar{D}(\bar{K})$. In [5], Deligne has introduced a functor

$$\mathrm{res}_x : \mathfrak{Fet}(\bar{U}) \to \mathfrak{Fet}(T^{\circ}_{\bar{X},x}).$$

For the construction of this functor with details, we refer to [5, §15].

Definition 2.2.12 (Deligne)**.** Let U be a geometrically connected hyperbolic curve over K. Let $x \in \bar{D}(\bar{K})$. A *tangential point* v_x of $\bar{U}$ at x is a composite

$$\mathfrak{Fet}(\bar{U}) \xrightarrow{\mathrm{res}_x} \mathfrak{Fet}(T^{\circ}_{\bar{X},x}) \xrightarrow{\sim} \mathfrak{Fet}(\mathbf{G}_{m,\bar{K}}) \to \mathfrak{fset}$$

where the middle equivalence is defined by an isomorphism $T^{\circ}_{\bar{X},x} \simeq \mathbf{G}_{m,\bar{K}}$ given by a choice of uniformiser of the local ring $\mathscr{O}_{\bar{X},x}$ and the last functor $\mathfrak{Fet}(\mathbf{G}_{m,\bar{K}}) \to \mathfrak{fset}$ is a fibre functor at some $\bar{K}$-point of $\mathbf{G}_{m,\bar{K}}$.

Remark 2.2.13. Let U be a geometrically connected hyperbolic curve over K and $x \in \bar{D}(\bar{K})$. When we say that v_x is a tangential point of $\bar{U}$ at x, we always implicitly assume that its defining data is given, i.e. we are assuming that there is a given choice of uniformiser of $\mathscr{O}_{\bar{X},x}$ and a fibre functor $\mathfrak{Fet}(\mathbf{G}_{m,\bar{K}}) \to \mathfrak{fset}$ at some $\bar{K}$-point of $\mathbf{G}_{m,\bar{K}}$.

The following proposition follows directly from the definition of tangential points:

Proposition 2.2.14. *Let U be a geometrically connected hyperbolic curve over K. Let $v_x : \mathfrak{Fet}(\bar{U}) \to \mathfrak{fset}$ be a tangential point of $\bar{U}$ at some $x \in \bar{D}(\bar{K})$. Then $\mathfrak{Fet}(\bar{U})$ is a Galois category with fundamental functor v_x.*

As before, when U is a geometrically connected hyperbolic curve over K and v_x is a tangential point of $\bar{U}$ at some $x \in \bar{D}(\bar{K})$, the étale fundamental group $\pi_1^{\text{ét}}(\bar{U}, v_x)$ of $\bar{U}$ with base point v_x is defined to be the automorphism group $\mathrm{Aut}(v_x)$ of the functor $v_x : \mathfrak{Fet}(\bar{U}) \to \mathfrak{fset}$.

Remark 2.2.15. In [5, §15], Deligne has given topological realisations of tangential points. So one may guess a natural analogue of Theorem 2.2.7 for the étale fundamental groups of hyperbolic curves with tangential points as base points.

To speak about Galois actions, we need a special type of tangential points – *rational* tangential points. For that, we need to make some observations: let U be a geometrically connected hyperbolic curve over K. Let us suppose that there exists an element x of $D(K)$. We see that x gives a rational geometric point $\bar{x}$ of X which gives also a rational geometric point $\bar{x}$ of $\bar{X}$ as explained in Remark 2.2.9:

$$\begin{tikzcd} & & \bar{X} \arrow[d] \\ \mathrm{Spec}\bar{K} \arrow[r] \arrow[urr, "\bar{x}"] & \mathrm{Spec}K \arrow[r, "x"'] & X \end{tikzcd}$$

In this situation, we see that there is a natural local isomorphism of local rings

$$\mathscr{O}_{\bar{X},\bar{x}} \simeq \mathscr{O}_{X,x} \otimes_K \bar{K},$$

i.e. a local homomorphism which is an isomorphism. Hence we may take a uniformiser of $\mathscr{O}_{\bar{X},\bar{x}}$ from that of $\mathscr{O}_{X,x}$, and such a choice gives an isomorphism

$$T^{\circ}_{\bar{X},\bar{x}} \simeq \mathbf{G}_{m,K} \times_{\mathrm{Spec}K} \mathrm{Spec}\bar{K}$$

of schemes over $\bar{K}$.

Definition 2.2.16. Let U be a geometrically connected hyperbolic curve over K with $D(K) \neq \emptyset$. Let $\bar{x}$ be a rational geometric point of $\bar{X}$ given by some $x \in D(K)$. A *rational tangential point* $v_{\bar{x}}$ of $\bar{U}$ at $\bar{x}$ is a tangential point $v_{\bar{x}}$ of $\bar{U}$ at $\bar{x}$ where

(a) the isomorphism $T^{\circ}_{\bar{X},\bar{x}} \simeq \mathbf{G}_{m,\bar{K}}$ is defined by a choice of uniformiser of $\mathscr{O}_{X,x}$

(b) the functor $\mathfrak{Fet}(\mathbf{G}_{m,\bar{K}}) \to \mathfrak{fset}$ is a fibre functor at some rational geometric point given by some K-rational point of $\mathbf{G}_{m,K}$.

Example 2.2.17. Let $U = \mathbf{P}^1_K \setminus \{0, 1, \infty\}$. We regard U as a thrice-punctured t-line. Then there is a canonical isomorphism

$$T^{\circ}_{\mathbf{P}^1_{\bar{K}}, \bar{0}} \simeq \mathrm{Spec}\bar{K}[t, 1/t]$$

of schemes where $\bar{0}$ is the rational geometric point of $\mathbf{P}^1_{\bar{K}}$ given by $0 \in \mathbf{P}^1_K(K)$. By identifying $\mathrm{Spec}\bar{K}[t, 1/t]$ with $\mathbf{G}_{m,\bar{K}}$, we obtain a rational tangential point

$$\vec{01} : \mathfrak{Fet}(\bar{U}) \to \mathfrak{Fet}(\mathbf{G}_{m,\bar{K}}) \xrightarrow{F_{\bar{1}}} \mathfrak{fset}$$

of $\bar{U}$ at $\bar{0}$ where $F_{\bar{1}}$ is the fibre functor at the rational geometric point $\bar{1}$ of $\mathbf{G}_{m,\bar{K}}$ given by $1 \in \mathbf{G}_{m,K}(K)$.

This (rational) tangential point $\vec{01}$ of $\bar{U}$ plays a crucial role in [5] for the study of motivic fundamental group of $U = \mathbf{P}^1_K \setminus \{0, 1, \infty\}$.

Remark 2.2.18. There is another way for defining rational tangential points of hyperbolic curves. Let $\Omega := \bar{K}\{\{T\}\}$ be the field of Puiseux series over $\bar{K}$. It is known that the field Ω is an algebraically closed field.

Let U be a geometrically connected hyperbolic curve over K with $x \in D(K)$. If $v_{\bar{x}}$ is a rational tangential point of $\bar{U}$ at $\bar{x}$ (the rational geometric point of $\bar{X}$ given by x), there is a way for interpreting $v_{\bar{x}}$ as a fibre functor

$$F_{\eta_{\bar{x}}} : \mathfrak{Fet}(\bar{U}) \to \mathfrak{fset}$$

at some Ω-geometric point $\eta_{\bar{x}}$ of $\bar{U}$. More precisely, one can take a geometric point $\eta_{\bar{x}} : \mathrm{Spec}\Omega \to \bar{U}$, so that there is a canonical isomorphism

$$F_{\eta_{\bar{x}}} \simeq v_{\bar{x}}$$

of functors. For details, we refer to [16, §1].

2.2.4 Galois actions on étale fundamental groups

Let K be a number field with a fixed algebraic closure $\bar{K}$. Let U be a geometrically connected hyperbolic curve over K with either $U(K) \neq \emptyset$ or $D(K) \neq \emptyset$. We consider a functor

$$\eta : \mathfrak{Fet}(\bar{U}) \to \mathfrak{fset}$$

which is

(i) a fibre functor $F_{\bar{x}}$ at some rational geometric point $\bar{x}$ of $\bar{U}$ given by $x \in U(K)$ if $U(K) \neq \emptyset$, or

(ii) a rational tangential point $v_{\bar{x}}$ at some rational geometric point $\bar{x}$ of $\bar{X}$ given by $x \in D(K)$ if $D(K) \neq \emptyset$.

For any such functor $\eta : \mathfrak{Fet}(\bar{U}) \to \mathfrak{fset}$, we can define a continuous $\mathrm{Gal}(\bar{K}/K)$-action on the étale fundamental group $\pi_1^{\text{ét}}(\bar{U}, \eta)$.

Before we explain the way for defining the Galois action, we need to introduce some notation to simplify the discussion. For any scheme Z over $\bar{K}$ and $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we set Z^σ to be the base change of Z by the morphism ${}^a\sigma : \mathrm{Spec}\bar{K} \to \mathrm{Spec}\bar{K}$ associated to σ. Also, if $f : Z' \to Z$ is a morphism of schemes over $\bar{K}$, its base change by ${}^a\sigma$ is denoted by

$$f^\sigma : (Z')^\sigma \to Z^\sigma.$$

Note that we have

$$Z^{\sigma\tau} = (Z^\sigma)^\tau \text{ and } f^{\sigma\tau} = (f^\sigma)^\tau$$

for any scheme Z over $\bar{K}$, morphism f of schemes over $\bar{K}$, and $\sigma, \tau \in \mathrm{Gal}(\bar{K}/K)$.

Now, we proceed to define a $\mathrm{Gal}(\bar{K}/K)$-action on $\pi_1^{\text{ét}}(\bar{U}, \eta)$. Let $w \in \pi_1^{\text{ét}}(\bar{U}, \eta)$ and $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Note that w is an automorphism of the functor η, i.e. w is a compatible family of bijections

$$w_V : \eta(V) \xrightarrow{\sim} \eta(V)$$

of finite sets for all étale coverings V of $\bar{U}$. To define σw, it suffices to specify a bijection

$$(\sigma w)_V : \eta(V) \xrightarrow{\sim} \eta(V)$$

for each étale covering V of $\bar{U}$. To define such a bijection, let us observe the following commutative diagram given by the base change via ${}^a\sigma : \mathrm{Spec}\bar{K} \to \mathrm{Spec}\bar{K}$ of an étale covering (V, f) of $\bar{U}$:

$$\begin{tikzcd} V^\sigma \arrow[rr, "\sim"] \arrow[dr, "f^\sigma"'] & & V \arrow[dl, "f"] \\ & \bar{U}^\sigma \simeq \bar{U} & \end{tikzcd}$$

where $\bar{U}^\sigma \simeq \bar{U}$ is canonical since U is a scheme over K. Hence we may view V^σ as an étale covering of $\bar{U}$. Also, there is a bijection

$$\eta(V^\sigma) \simeq \eta(V)$$

of finite sets induced from ${}^a\sigma$. Under these observations, for each étale covering V of $\bar{U}$ we define $(\sigma w)_V$ to be the composite

$$\eta(V) \simeq \eta(V^\sigma) \xrightarrow{w_{V^\sigma}} \eta(V^\sigma) \simeq \eta(V).$$

Then it can be easily checked that the bijections $(\sigma w)_V$ form a compatible family such that

$$(\sigma\tau)w = \sigma(\tau w)$$

for any $\sigma, \tau \in \mathrm{Gal}(\bar{K}/K)$. In other words, we have defined a $\mathrm{Gal}(\bar{K}/K)$-action on $\pi_1^{\text{ét}}(\bar{U}, \eta)$. Continuity of this action can be seen immediately from its construction.

2.2.5 Galois actions on Galois coverings

Let U be a geometrically connected hyperbolic curve over K such that either $U(K) \neq \emptyset$ or $D(K) \neq \emptyset$. Let η be a fundamental functor considered in §2.2.4. Recall that a connected étale covering V of $\bar{U}$ is called a *Galois covering* if the natural $\mathrm{Aut}(V/\bar{U})$-action on $\eta(V)$ is transitive, i.e. for any $v \in \eta(V)$, the map

$$\mathrm{Aut}(V/\bar{U}) \to \eta(V) : g \mapsto g(v)$$

is bijective. For a given finite group Q, a Galois covering V of $\bar{U}$ with $\mathrm{Aut}(V/\bar{U}) \simeq Q$ is called a *Galois Q-covering*. Note that if V is a Galois Q-covering of $\bar{U}$ for some finite group Q, then there is a projection

$$\pi_1^{\text{ét}}(\bar{U}, \eta) \twoheadrightarrow Q.$$

Let N be a closed normal subgroup of $\pi_1^{\text{ét}}(\bar{U}, \eta)$ of finite index which is stable under the G_K-action on $\pi_1^{\text{ét}}(\bar{U}, \eta)$, i.e. for any $n \in N$ and $\sigma \in G_K$, we have $\sigma n \in N$. Then the G_K-action on $\pi_1^{\text{ét}}(\bar{U}, \eta)$ induces a G_K-action on Q. By applying the theory of Galois descent, for example, found in [23], one sees from the general theory of Galois categories that

(a) the Galois covering V admits a K-model, i.e. there exists a scheme V_0 over K such that $V \simeq V_0 \times_{\mathrm{Spec}K} \mathrm{Spec}\bar{K}$,

(b) there exists an element v_0 of $\eta(V)$ fixed by the natural G_K-action on $\eta(V)$ so that the bijection

$$Q \xrightarrow{\sim} \eta(V) : g \mapsto g(v_0)$$

is G_K-equivariant,

(c) if one regards v_0 as a geometric point of V, the fibre functor $F_{v_0} : \mathfrak{Fet}(V) \to \mathfrak{fset}$ at v_0 has the same type as η, i.e. if η arises from a rational geometric point of $\bar{U}$, then v_0 is a rational geometric point of V. Similarly, if η is a rational tangential point of $\bar{U}$, then F_{v_0} is a rational tangential point of V (recall that every rational tangential point can be regarded as a fibre functor at some geometric point, see Remark 2.2.18), and

(d) let v_0 be as in (c) which is regarded as a geometric point of V, then $N = \pi_1^{\text{ét}}(V, v_0)$

2.3 Étale path torsors

Throughout this section, we fix a number field K and its algebraic closure $\bar{K}$. The absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ is simply denoted by G_K.

2.3.1 Equivariant torsors

Let G be a profinite group and π a profinite group endowed with a continuous left G-action.

Definition 2.3.1. A *G-equivariant π-torsor* P is a non-empty topological set such that

(i) π acts on P continuously from the right,

(ii) G acts on P continuously from the left, and this G-action is compatible with the G-action on π, i.e. for any $\gamma \in P$, $w \in \pi$, and $\sigma \in G$, we have

$$\sigma(\gamma w) = (\sigma\gamma)(\sigma w),$$

(iii) for any two elements γ_1, γ_2 of P, there exists a unique element $w_{12} \in \pi$ such that

$$\gamma_2 = \gamma_1 w_{12}.$$

Example 2.3.2. Let P_0 be the underlying set of the profinite group π. We view P as a right π-set whose continuous right π-action is given by multiplication. Then P_0 is naturally a G-equivariant π-torsor. This G-equivariant π-torsor P_0 is called the *trivial* torsor.

Definition 2.3.3. A *morphism* $\varphi : P_1 \to P_2$ of π-torsors is a π-equivariant map of sets, i.e. φ is a map of sets such that

$$\varphi(\gamma w) = \varphi(\gamma) w$$

for any $\gamma \in P_1$ and $w \in \pi$.

A morphism $\varphi : P_1 \to P_2$ of π-torsors is called an *isomorphism* if it is also G-equivariant, i.e. we have

$$\varphi(\sigma\gamma) = \sigma\varphi(\gamma)$$

for any $\gamma \in P$ and $\sigma \in G$.

Definition 2.3.4. A G-equivariant π-torsor P is called *trivial* if it is isomorphic to the trivial torsor P_0.

Lemma 2.3.5. *A G-equivariant π-torsor P is trivial if and only if there exists an element γ of P fixed by G.*

Proof. ($\Rightarrow$) Let $\varphi : P_0 \xrightarrow{\sim} P$ be an isomorphism. Then the image $\varphi(e)$ of the identity element e of π is fixed by G.

($\Leftarrow$) Let $\gamma_0 \in P$ be an element fixed by G. For any $\gamma \in P$, there uniquely exists $w_\gamma \in \pi$ such that $\gamma = \gamma_0 w_\gamma$. Then the map

$$P \to P_0 : \gamma \mapsto w_\gamma$$

gives an isomorphism. $\square$

Definition 2.3.6. For a G-equivariant π-torsor P, any element of P fixed by the G-action is called a *trivialisation* of P.

Recall that the first non-abelian cohomology set $H^1(G, \pi)$ is defined to be the set of equivalence classes of 1-cocycles of G in π.

Proposition 2.3.7 ([22, Proposition 33])**.** *There is a bijection between the set of isomorphism classes of G-equivariant π-torsors and the set $H^1(G, \pi)$ sending the class of the trivial torsor P_0 to the class of the trivial 1-cocycle.*

2.3.2 Étale path torsors

Definition 2.3.8. Let X be a connected scheme and $F_1, F_2 : \mathfrak{Fet}(X) \to \mathfrak{fset}$ fundamental functors. An isomorphism $F_1 \xrightarrow{\sim} F_2$ of functors is called an *étale path* from F_1 to F_2 on X.

If F_i is the fibre functor at some geometric point η_i of X for $i = 1, 2$, as a convention, an isomorphism $F_1 \xrightarrow{\sim} F_2$ of functors is called an étale path from η_1 to η_2 on X, and we denote it by $\eta_1 \rightsquigarrow \eta_2$.

Remark 2.3.9. For a connected scheme X and fundamental functors F_1, F_2 : $\mathfrak{Fet}(X) \to \mathfrak{fset}$, there always exists an étale path from F_1 to F_2 on X by Theorem 2.1.2.(c).

Let U be a geometrically connected hyperbolic curve over K such that either $U(K) \neq \emptyset$ or $D(K) \neq \emptyset$. Let $\eta_1, \eta_2 : \mathfrak{Fet}(\bar{U}) \to \mathfrak{fset}$ be fundamental functors considered in §2.2.4. Then, by the virtue of profinite-ness of étale fundamental groups, the set

$$P^{\text{ét}}(\bar{U}; \eta_1, \eta_2)$$

of étale paths from η_1 to η_2 on $\bar{U}$ is a profinite set. Moreover, by following the exactly same procedure we have conducted in §2.2.4, one can see that there exists a continuous (left) G_K-action on the profinite set $P^{\text{ét}}(\bar{U}; \eta_1, \eta_2)$.

The following proposition is obvious.

Proposition 2.3.10. *Under the natural right $\pi_1^{ét}(\bar{U}, \eta_1)$-action, the set $P^{ét}(\bar{U}; \eta_1, \eta_2)$ is a G_K-equivariant $\pi_1^{ét}(\bar{U}, \eta_1)$-torsor.*

2.3.3 More on étale fundamental groups

Let X be a connected scheme. For any geometric points η_1, η_2 of X, an étale path $\gamma : \eta_1 \rightsquigarrow \eta_2$ defines an isomorphism

$$\pi_1^{\text{ét}}(X, \eta_1) \xrightarrow{\sim} \pi_1^{\text{ét}}(X, \eta_2) : w \mapsto \gamma w \gamma^{-1}.$$

In general, two distinct étale paths from η_1 to η_2 induce different isomorphisms between $\pi_1^{\text{ét}}(X, \eta_1)$ and $\pi_1^{\text{ét}}(X, \eta_2)$.

Contrary to this phenomenon, one can determine quotients of two étale fundamental groups with distinct base points in a way that is independent of choices of étale paths. For more precise statement, let η_1 and η_2 be distinct geometric points of X. Let N_1 be a closed normal subgroup of $\pi_1^{\text{ét}}(X, \eta_1)$ and $Q_1 = \pi_1^{\text{ét}}(X, \eta_1)/N_1$. An étale path $\gamma : \eta_1 \rightsquigarrow \eta_2$ determines a closed normal subgroup N_2 of $\pi_1^{\text{ét}}(X, \eta_2)$ by

$$N_2 = \gamma N_1 \gamma^{-1},$$

hence a quotient

$$Q_2 = \pi_1^{\text{ét}}(X, \eta_2)/N_2$$

of $\pi_1^{\text{ét}}(X, \eta_2)$. We claim that the construction of Q_2 is independent of the choice of $\gamma : \eta_1 \rightsquigarrow \eta_2$. In fact, if $\nu : \eta_1 \rightsquigarrow \eta_2$ is another étale path, we have

$$\gamma N_1 \gamma^{-1} = \nu N_1 \nu^{-1}$$

since N_1 is normal in $\pi_1^{\text{ét}}(X, \eta_1)$. The discussion we have done so far motivates the following definition:

Definition 2.3.11. Let X be a connected scheme and η a geometric point of X. For a given closed normal subgroup N of $\pi_1^{\text{ét}}(X, \eta)$, the *universal quotient* determined by the pair $(\pi_1^{\text{ét}}(X, \eta), N)$ is the family of quotients $\pi_1^{\text{ét}}(X, \eta')/N'$ of all geometric points η' of X as defined in the above. If we write Q for the quotient $\pi_1^{\text{ét}}(X, \eta)/N$, we usually denote the universal quotient simply by

$$\pi_1^{\text{ét}}(X) \twoheadrightarrow Q.$$

When we say that $\pi_1^{\text{ét}}(X) \twoheadrightarrow Q$ is a universal quotient, we implicitly assume that there exists a geometric point η of X and a closed normal subgroup N of $\pi_1^{\text{ét}}(X, \eta)$ such that $\pi_1^{\text{ét}}(X, \eta)/N = Q$.

2.3.4 Push-out torsors

Let G be a profinite group and π a profinite group endowed with a continuous left G-action.

In the following, every finite group is regarded as a topological group provided with the discrete topology.

Definition 2.3.12. Let Q be a finite group equipped with a continuous left G-action. Let $\phi : \pi \to Q$ be a G-equivariant continuous homomorphism of topological groups. For a G-equivariant π-torsor P, the *push-out* $P \times^{\phi} Q$ of P by ϕ is defined to be the set

$$\{(\gamma, q) \in P \times Q\}/\sim$$

of equivalence classes where the equivalence relation $\sim$ is given by

$$(\gamma w, q) \sim (\gamma, \phi(w)^{-1} q)$$

for any $\gamma \in P$, $w \in \pi$, and $q \in Q$. When there is no danger of confusion, we write $P \times^{\pi} Q$ instead of $P \times^{\phi} Q$.

Lemma 2.3.13. *Let Q be a finite G-group and $\phi : \pi \to Q$ a continuous G-equivariant homomorphism. For a G-equivariant π-torsor P, the push-out $P \times^{\pi} Q$ has a natural structure of a G-equivariant Q-torsor.*

Proof. Let us denote by $[\gamma, q]$ the class of $(\gamma, q) \in P \times Q$. We define a continuous left G-action by setting

$$\sigma[\gamma, q] = [\sigma\gamma, \sigma q]$$

for every $\sigma \in G$ and a continuous right Q-action by setting

$$[\gamma, q]q' = [\gamma, qq']$$

for every $q' \in Q$. Then one obviously has $\sigma([\gamma, q]q') = (\sigma[\gamma, q])\sigma q'$ for any $\sigma \in G$, $\gamma \in P$, and $q, q' \in Q$. Also, from the equalities

$$\begin{aligned} [\gamma', q'] &= [\gamma w, q'] \\ &= [\gamma, \phi(w) q'] \\ &= [\gamma, qq^{-1}\phi(w) q'] \\ &= [\gamma, q](q^{-1}\phi(w) q') \end{aligned}$$

where $w \in \pi$ such that $\gamma' = \gamma w$, we see that $P \times^{\pi} Q$ is a G-equivariant Q-torsor. $\square$

Proposition 2.3.14. *Let Q be a finite G-group with a continuous G-equivariant homomorphism $\phi : \pi \to Q$. Under the natural map*

$$H^1(G, \pi) \to H^1(G, Q)$$

of sets, the class of a G-equivariant π-torsor P maps to the class of $P \times^{\pi} Q$.

Proof. This is a direct consequence of Proposition 2.3.7. □

2.3.5 Galois actions on push-out torsors

Let U be a geometrically connected hyperbolic curve over K such that either $U(K) \neq \emptyset$ or $D(K) \neq \emptyset$. Let $\eta_1, \eta_2 : \mathfrak{Fet}(\bar{U}) \to \mathfrak{fset}$ be fundamental functors considered in §2.2.4.

For a closed normal subgroup N of $\pi_1^{\text{ét}}(\bar{U}, \eta_1)$ of finite index, we set $Q = \pi_1^{\text{ét}}(\bar{U}, \eta)/N$. Then we obtain a G_K-equivariant Q-torsor

$$P^{\text{ét}}(\bar{U}; \eta_1, \eta_2) \times^{\pi_1^{\text{ét}}(\bar{U}, \eta_1)} Q$$

which may be viewed as the set of bijections $\eta_1(V) \xrightarrow{\sim} \eta_2(V)$ commuting with the action of $\mathrm{Aut}(V/U)$ where V is the Galois Q-covering of $\bar{U}$ as in §2.2.5. Moreover, if we take $v_0 \in \eta_1(V)$ as in §2.2.5.(b), then the map

$$P^{\text{ét}}(\bar{U}; \eta_1, \eta_2) \times^{\pi_1^{\text{ét}}(\bar{U}, \eta_1)} Q \to \eta_2(V) : h \mapsto h(v_0)$$

is a G_K-equivariant bijection of sets, where the set $\eta_2(V)$ is equipped with the natural G_K-action.

Chapter 3

Galois actions on non-abelian finite groups

In the first section, we establish the basic setting of rational tangential points on once-punctured elliptic curves. In the second section, we explain topological realisations of the geometric fundamental groups of once-punctured elliptic curves under the setting established in the first section. The third section is devoted to the construction of finite groups whose attached Galois actions are our main interest of study. We investigate these Galois actions in the fourth section. In the first half of the final section, we briefly review the theory of elliptic polylogarithms by Beilinson and Levin which allows us to pursue more delicate studies on Galois actions performed in the second half.

Throughout this chapter, we fix a number field K with an algebraic closure $\bar{K} \subset \mathbb{C}$. As before, the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ of K is sometimes written by G_K.

3.1 Rational tangential points on elliptic curves

3.1.1 Basics on elliptic curves

Let $f : E \to \mathrm{Spec}K$ be an elliptic curve with the zero-section $O \in E(K)$. The formal completion $\widehat{E}$ of E along the zero-section O admits an isomorphism

$$\widehat{E} \simeq \mathrm{Spf}K[\![T]\!]$$

called a *formal parameterisation* at zero and T is called a *formal parameter* at zero. Once we have fixed such an isomorphism, we can find a *unique* K-basis ω of

$$\underline{\omega}_{E/K} := f_*\Omega^1_{E/K}$$

whose formal expansion along the zero-section is

$$\omega = (1 + \text{higher terms}) \cdot \mathrm{d}T.$$

Conversely, once we are given a K-basis ω of $\underline{\omega}_{E/K}$, there exists a formal parameter T at zero (unique up to $T \mapsto T + \text{higher terms}$) so that $\widehat{E} \simeq \mathrm{Spf} K[\![T]\!]$ and ω is expressed as in the above.

Recall that if I is the sheaf of ideals defining O, then $f_*(I^{-n})$ is a n-dimensional K-vector space for each integer $n \geq 1$. Once we have fixed a K-basis ω of $\underline{\omega}_{E/K}$, we can find a basis $\{1, x\}$ of $f_*(I^{-2})$ such that x is uniquely determined up to $x \mapsto x + a$ by the normalisation

$$x \sim \frac{1}{T^2}(1 + \text{higher terms})$$

at zero for *any* formal parameter T at zero taken from the choice of ω. Similarly, we can find a basis $\{1, x, y\}$ where x is fixed as in the above and y is uniquely determined up to $y \mapsto y + ax + b$ by the normalisation

$$y \sim \frac{-2}{T^3}(1 + \text{higher terms})$$

at zero for any formal parameter T at zero. We call these x and y by *parameters* of E.

Let us pick and fix a K-basis ω of $\underline{\omega}_{E/K}$ which is nothing other than a nowhere vanishing invariant differential. Then, as explained in [17, §2.1], we can find *unique* parameters x and y of E (independent of the choice of a local parameter T at zero) such that

(i) the affine ring $H^0(E - O, \mathscr{O}_E) = \varinjlim_n H^0(E, I^{-n})$ has the form

$$K[x, y]/(y^2 - (4x^3 - g_2 x - g_3))$$

where $g_2, g_3 \in K$ are uniquely determined (independently of the choice of a local parameter T at zero) and $\Delta_{\mathrm{mod}} := g_2^3 - 27g_3^2 \in K^\times$,

(ii) $\omega = \frac{\mathrm{d}x}{y}$.

The element $\Delta_{\mathrm{mod}} \in K^{\times}$ is called the *modular discriminant* of E.

Remark 3.1.1. The modular discriminant Δ_{mod} of E depends only on the choice of a K-basis ω of $\underline{\omega}_{E/K}$. So, it is well-defined only when the choice of ω is fixed.

3.1.2 Construction of base points

For a given elliptic curve E over K, let

$$E^{\circ} := E - O.$$

We fix a nowhere vanishing invariant differential ω, i.e. a K-basis of $\underline{\omega}_{E/K}$. We then are given a (unique) affine equation $y^2 = 4x^3 - g_2 x - g_3$ for E such that $\omega = \frac{\mathrm{d}x}{y}$. Under this affine equation, we see that the rational function

$$\varpi := \frac{-2x}{y}$$

is a uniformiser of the local ring $\mathscr{O}_{E,O}$. Hence one may also consider ϖ as a uniformiser of the local ring $\mathscr{O}_{\bar{E},O} = \mathscr{O}_{E,O} \otimes_K \bar{K}$. Then the choice of ϖ induces an isomorphism

$$T^{\circ}_{\bar{E},O} \simeq \mathbf{G}_{m,K} \times_{\mathrm{Spec}K} \mathrm{Spec}\bar{K},$$

and, hence, an equivalence

$$\mathfrak{Fet}(T^{\circ}_{\bar{E},O}) \simeq \mathfrak{Fet}(\mathbf{G}_{m,\bar{K}})$$

of categories.

We define a rational tangential point $v : \mathfrak{Fet}(\bar{E}^{\circ}) \to \mathfrak{fset}$ of $\bar{E}^{\circ}$ at O to be the composite

$$\mathfrak{Fet}(\bar{E}^{\circ}) \to \mathfrak{Fet}(T^{\circ}_{\bar{E},O}) \simeq \mathfrak{Fet}(\mathbf{G}_{m,\bar{K}}) \xrightarrow{F_{\bar{1}}} \mathfrak{fset}.$$

where the functor $F_{\bar{1}} : \mathfrak{Fet}(\mathbf{G}_{m,\bar{K}}) \to \mathfrak{fset}$ is the fibre functor at rational geometric point $\bar{1}$ of $\mathbf{G}_{m,\bar{K}}$ given by $1 \in \mathbf{G}_{m,K}(K)$.

Remark 3.1.2. For a given elliptic curve E over K, from [5, 15.20], one sees that giving a nowhere vanishing invariant differential ω on $\bar{E}$ is equivalent to giving a tangential point of $\bar{E}^{\circ}$. The rational tangential point $v : \mathfrak{Fet}(\bar{E}^{\circ}) \to \mathfrak{fset}$ we have constructed in the above is exactly the tangential point obtained from the given ω under this equivalence.

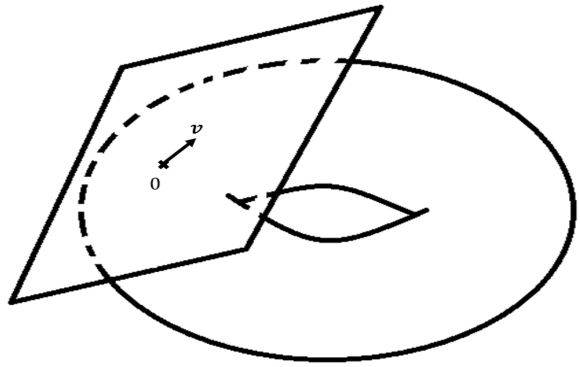

Figure 3.1: Topological realisation of v

3.2 Geometric fundamental group of E°

Until the end of this chapter, we fix an elliptic curve E over K and a nowhere vanishing invariant differential ω on E. Also, we let $v : \mathfrak{Fet}(\bar{E}^\circ) \to \mathfrak{fset}$ be the rational tangential point of $\bar{E}^\circ$ as constructed in §3.1.2.

3.2.1 Topological realisations

Let L be a lattice of $\mathbb{C}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/L$. Then the rational tangential point v is realised as a tangent vector at $O \in \mathbb{C}/L$ as depicted in Figure 3.1. By abuse of notation, let us use the symbol v for this tangent vector at $O \in \mathbb{C}/L$. We explain how one can think of the topological fundamental group $\pi_1(E(\mathbb{C}), v)$ of $E(\mathbb{C})$ with base point v by explaining a way of giving a set of generators of $\pi_1(E(\mathbb{C}), v)$.

Let T_O be the tangent space at $O \in \mathbb{C}/L$. There exists a germ of a pointed isomorphism $\varphi : (T_O, 0) \to (\mathbb{C}/L, O)$ such that $\varphi'(0) = 1$. Take a non-zero tangent vector $v' \in T_O$ in the direction of v which is very close to $0 \in T_O$. By the map φ, the tangent vector v' maps to a point $\varphi(v')$ on $\mathbb{C}/L$ which takes a close position with $O \in \mathbb{C}/L$. We firstly define a set $\{a', b'\}$ of generators of the topological fundamental group $\pi_1(E^\circ(\mathbb{C}), \varphi(v'))$ through the loops described in Figure 3.2 where D_L is the fundamental parallelogram of L.

Secondly, we consider a topological path γ from $v \in T_O$ to $\varphi(v') \in \mathbb{C}/L$ which

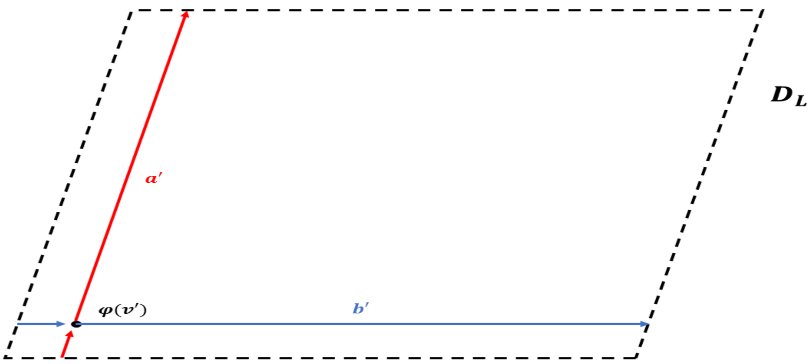

Figure 3.2: Generators of $\pi_1(E^\circ(\mathbb{C}), \varphi(v'))$

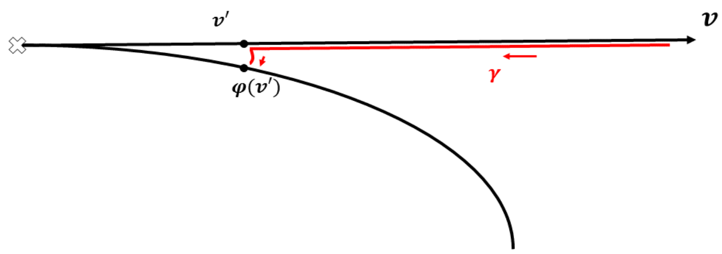

Figure 3.3: Topological path from v to $\varphi(v')$

is a composite

$$\gamma : v \rightsquigarrow v' \xrightarrow{\varphi} \varphi(v')$$

where $v \rightsquigarrow v'$ is a topological path on the tangent space T_O, see Figure 3.3. Then we define a set of generators $\{a, b\}$ of $\pi_1(E^\circ(\mathbb{C}), v)$ by

$$a = \gamma^{-1} a' \gamma \text{ and } b = \gamma^{-1} b' \gamma,$$

then we obtain the following presentation

$$\pi_1(E^\circ(\mathbb{C}), v) = \langle a, b, c \mid [a, b]c = 1 \rangle.$$

A pictorial summary of the procedure choosing generators a and b of $\pi_1(E^\circ(\mathbb{C}), v)$ is given in Figure 3.4.

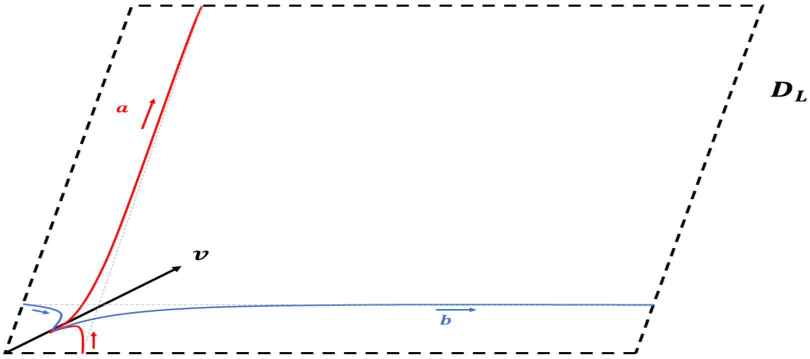

Figure 3.4: Generators of $\pi_1(E^\circ(\mathbb{C}), v)$

3.2.2 Set up of topological generators

Once we have fixed a presentation of the topological fundamental group $\pi_1(E^\circ(\mathbb{C}), v)$ as in §3.2.1, by applying the comparison isomorphism between topological and étale fundamental groups

$$\pi_1(\widehat{E^\circ(\mathbb{C})}, v) \simeq \pi_1^{\text{ét}}(\bar{E}^\circ, v),$$

we find a set of topological generators $\{a, b, c\}$ of $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$ so that

$$\pi_1^{\text{ét}}(\bar{E}^\circ, v) \simeq \langle a, b, c \mid [a, b]c = 1 \rangle^\wedge$$

where $(-)^\wedge$ in the right hand side means the profinite completion. We keep using these elements a, b, c for the generators of $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$ in the following discussion.

3.3 Construction of finite quotients

Let ℓ be an odd prime. Let Π be the maximal pro-ℓ quotient of the geometric fundamental group $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$ of E° with base point v. Let $\{\Pi_n\}_{n\geq 1}$ be the lower central series with the normalisation $\Pi_1 = \Pi$.

Definition 3.3.1. Let $[\Pi_2, \Pi_2]$ be the minimal closed subgroup generated by $[w_1, w_2]$ for $w_1, w_2 \in \Pi_2$. We define

$$\bar{\Pi} = \Pi/[\Pi_2, \Pi_2].$$

Let $\{\bar{\Pi}_n\}_{n\geq 1}$ be the lower central series of $\bar{\Pi}$ with the normalisation $\bar{\Pi}_1 = \bar{\Pi}$. For each integer $n \geq 1$, we call the quotient

$$\bar{\Pi}/\bar{\Pi}_{n+1}$$

by the *n-step quotient* of Π.

Remark 3.3.2. The group $\bar{\Pi}$ is a characteristic quotient of $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$. Hence it is equipped with a G_K-action inherited from the G_K-action on $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$. For a similar reason, all groups $\bar{\Pi}_m$, $\bar{\Pi}_m/\bar{\Pi}_n$ for integers $n > m \geq 1$ are naturally endowed with G_K-actions inherited from the G_K-action on $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$.

Note that, by definition, for each integer $n \geq 2$ the n-step quotient $\bar{\Pi}/\bar{\Pi}_{n+1}$ is a central extension of the $(n-1)$-step quotient $\bar{\Pi}/\bar{\Pi}_n$ by $\bar{\Pi}_n/\bar{\Pi}_{n+1}$. In fact, the centre of $\bar{\Pi}/\bar{\Pi}_{n+1}$ is exactly $\bar{\Pi}_n/\bar{\Pi}_{n+1}$. We call the exact sequence

$$1 \to \bar{\Pi}_n/\bar{\Pi}_{n+1} \to \bar{\Pi}/\bar{\Pi}_{n+1} \to \bar{\Pi}/\bar{\Pi}_n \to 1$$

by the *n-step exact sequence* of Π.

3.3.1 2-step finite quotients

Let us first observe that the 1-step quotient $\bar{\Pi}/\bar{\Pi}_2$ of Π is isomorphic to the ℓ-adic Tate module

$$T_\ell E = \varprojlim_m E[\ell^m]$$

of E. So the 2-step exact sequence of Π can be rewritten as

$$1 \to \bar{\Pi}_2/\bar{\Pi}_3 \to \bar{\Pi}/\bar{\Pi}_3 \to T_\ell E \to 0.$$

Lemma 3.3.3. *There exists a G_K-equivariant isomorphism*

$$\bar{\Pi}_2/\bar{\Pi}_3 \xrightarrow{\sim} \mathbb{Z}_\ell(1).$$

Proof. We firstly claim that the map

$$\bar{\Pi}/\bar{\Pi}_2 \wedge \bar{\Pi}/\bar{\Pi}_2 \to \bar{\Pi}_2/\bar{\Pi}_3 : \bar{g} \wedge \bar{h} \mapsto \overline{[g,h]}$$

is a G_K-equivariant isomorphism (here, $\bar{g}$ means the image of $g \in \bar{\Pi}$ under the natural projection to $\bar{\Pi}/\bar{\Pi}_2$. $\overline{[g,h]}$ is defined similarly). To check whether the map is well-defined, let us take an element h_1 of $\bar{\Pi}$ such that $\bar{h} = \bar{h}_1$. By symmetry of the map, it suffices to check that if the equality $\overline{[g,h]} = \overline{[g,h_1]}$ holds. Equivalently, we need to show that $\overline{[g,h][h_1,g]} = \bar{1}$. To show this, let us observe that $h^{-1}h_1 \in$

$\bar{\Pi}_2$ and $[g,h][h_1,g] = gh[g^{-1},h^{-1}h_1]h^{-1}g^{-1}$. Since $[g^{-1},h^{-1}h_1] \in \bar{\Pi}_3$, we have $\overline{[g,h][h_1,g]} = \overline{ghh^{-1}g^{-1}} = \bar{1}$. Hence, the map is well-defined.

Once well-defined-ness of the map is checked, G_K-equivariance follows directly by the definition of the map: for $\sigma \in G_K$, we have $\sigma\overline{[g,h]} = \overline{\sigma[g,h]} = \overline{[\sigma g, \sigma h]}$.

Now, the lemma follows from the Weil pairing by identifying $\bar{\Pi}/\bar{\Pi}_2$ with $T_\ell E$:

$$\mathbb{Z}_\ell(1) \xleftarrow{\sim} \bar{\Pi}/\bar{\Pi}_2 \wedge \bar{\Pi}/\bar{\Pi}_2 \xrightarrow{\sim} \bar{\Pi}_2/\bar{\Pi}_3.$$

$\square$

From the G_K-equivariant isomorphism $\bar{\Pi}_2/\bar{\Pi}_3 \simeq \mathbb{Z}_\ell(1)$, we may rewrite the 2-step exact sequence of Π by

$$0 \to \mathbb{Z}_\ell(1) \to \bar{\Pi}/\bar{\Pi}_3 \to T_\ell E \to 0.$$

Lemma 3.3.4. *Let G be a topological group. Let H_1 and H_2 be characteristic subgroups of G. Then the minimal closed subgroup H of G generated by H_1 and H_2 is also a characteristic subgroup of G.*

Proof. This is obvious since given H_1 and H_2 are characteristic subgroups. $\square$

Definition 3.3.5. Let $\bar{\Pi}^\ell$ be the minimal closed subgroup of $\bar{\Pi}$ generated by w^ℓ for all $w \in \bar{\Pi}$, hence $\bar{\Pi}^\ell$ is a characteristic subgroup of $\bar{\Pi}$. We define

$$Q_2[\ell] = \bar{\Pi}/(\bar{\Pi}_3 \cdot \bar{\Pi}^\ell)$$

where $\bar{\Pi}_3 \cdot \bar{\Pi}^\ell$ is the minimal closed subgroup of $\bar{\Pi}$ generated by $\bar{\Pi}_3$ and $\bar{\Pi}^\ell$.

Recall that we have chosen topological generators a, b, c of the geometric fundamental group $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$ of E°. We let a_2, b_2, c_2 be images of a, b, c respectively in $Q_2[\ell]$ under the natural projection

$$\pi_1^{\text{ét}}(\bar{E}^\circ, v) \twoheadrightarrow Q_2[\ell].$$

Then every element of $Q_2[\ell]$ is expressed in the form

$$a_2^{e_a} b_2^{e_b} c_2^{e_c}$$

for some $e_a, e_b, e_c \in \{0, 1, \ldots, \ell - 1\}$ by applying

$$\begin{aligned} b_2 a_2 &= b_2 a_2 b_2^{-1} a_2^{-1} a_2 b_2 \\ &= c_2 a_2 b_2 \\ &= a_2 b_2 c_2 \end{aligned}$$

successively[1].

Proposition 3.3.6. *The group $Q_2[\ell]$ is a central extension of $E[\ell]$ by μ_ℓ in the category of finite G_K-groups, whose centre is exactly μ_ℓ.*

Proof. Recall that the 2-step exact sequence of Π can be written by

$$0 \to \mathbb{Z}_\ell(1) \xrightarrow{i} \bar{\Pi}/\bar{\Pi}_3 \xrightarrow{j} T_\ell E \to 0.$$

We firstly claim that the push-forward of the natural projection $\mathrm{pr}_2 : \bar{\Pi}/\bar{\Pi}_3 \to Q_2[\ell]$ along $j : \bar{\Pi}/\bar{\Pi}_3 \to T_\ell E$ is the natural projection $T_\ell E \to E[\ell]$. In fact, this is quite obvious since the push-forward is exactly the quotient of $T_\ell E$ by image of $\bar{\Pi}^\ell$ in $T_\ell E$.

We also claim that the pull-back of $\mathrm{pr}_2 : \bar{\Pi}/\bar{\Pi}_3 \to Q_2[\ell]$ along $i : \mathbb{Z}_\ell(1) \to \bar{\Pi}/\bar{\Pi}_3$ is the natural projection $\mathbb{Z}_\ell(1) \to \mu_\ell$. Note that, here, the pull-back operation is equivalent to taking maximal ℓ-torsion quotient of $\mathbb{Z}_\ell(1) \simeq \bar{\Pi}_2/\bar{\Pi}_3$, which is obviously $\mathbb{Z}_\ell(1) \twoheadrightarrow \mu_\ell$.

Therefore, we obtain the following commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}_\ell(1) \arrow[r] \arrow[d] & \bar{\Pi}/\bar{\Pi}_3 \arrow[r] \arrow[d] & T_\ell E \arrow[r] \arrow[d] & 0 \\ 1 \arrow[r] & \mu_\ell \arrow[r] & Q_2[\ell] \arrow[r] & E[\ell] \arrow[r] & 0 \end{tikzcd}$$

whose rows are exact sequences and vertical maps are natural projections. Every arrow in the diagram is G_K-equivariant by the constructions.

Finally, we obtain $Z(Q_2[\ell]) = \mu_\ell$ form the equality $Z(\bar{\Pi}/\bar{\Pi}_3) = \mathbb{Z}_\ell(1)$, which holds by the definition of $\bar{\Pi}/\bar{\Pi}_3$. $\square$

[1]Note that $Z(\bar{\Pi}/\bar{\Pi}_3) = \bar{\Pi}_2/\bar{\Pi}_3$ is generated by the image of c in $\bar{\Pi}/\bar{\Pi}_3$ under the natural projection $\pi_1^{\text{ét}}(\bar{E}^\circ, v) \twoheadrightarrow \bar{\Pi}/\bar{\Pi}_3$. Hence, c_2 generates the centre of $Q_2[\ell]$.

3.3.2 3-step finite quotients

Lemma 3.3.7. *There is a G_K-equivariant isomorphism*

$$\bar{\Pi}_3/\bar{\Pi}_4 \simeq T_\ell E(1)$$

where $T_\ell E(1) := T_\ell E \otimes \mathbb{Z}_\ell(1)$.

Proof. We consider the map

$$\bar{\Pi}/\bar{\Pi}_2 \otimes \bar{\Pi}_2/\bar{\Pi}_3 \to \bar{\Pi}_3/\bar{\Pi}_4 : \bar{w}_1 \otimes \bar{w}_2 \mapsto \overline{[w_1, w_2]}.$$

We are firstly required to check whether this map is well-defined. Since we have already conducted similar computations in the proof of Lemma 3.3.3, at here, we omit the tedious computations for proving well-defined-ness. Also, this map is G_K-equivariant and surjective from the construction.

To show that injectivity of the map, let us denote by $\bar{a}, \bar{b}, \bar{c}$ the images of a, b, c in $\bar{\Pi}$, respectively. Then we see that $\bar{\Pi}_3/\bar{\Pi}_4$ is a $\mathbb{Z}_\ell$-module generated by $[\bar{a}, \bar{c}]$ and $[\bar{b}, \bar{c}]$.

Let us define a map

$$\bar{\Pi}/\bar{\Pi}_2 \otimes \bar{\Pi}_2/\bar{\Pi}_3 \leftarrow \bar{\Pi}_3/\bar{\Pi}_4$$

by $\mathbb{Z}_\ell$-linearly extending the assignments

$$\begin{cases} \bar{a} \otimes \bar{c} & \mapsfrom [\bar{a}, \bar{c}] \\ \bar{b} \otimes \bar{c} & \mapsfrom [\bar{b}, \bar{c}] \end{cases}.$$

Then, by its construction, we see that this map is a G_K-equivariant $\mathbb{Z}_\ell$-module homomorphism. Moreover, again by the constructions, the composition

$$\bar{\Pi}/\bar{\Pi}_2 \otimes \bar{\Pi}_2/\bar{\Pi}_3 \to \bar{\Pi}_3/\bar{\Pi}_4 \to \bar{\Pi}/\bar{\Pi}_2 \otimes \bar{\Pi}_2/\bar{\Pi}_3$$

is the identity map. So, we have the desired injectivity.

Now, we get the lemma as we know $\bar{\Pi}_2/\bar{\Pi}_3 \simeq \mathbb{Z}_\ell(1)$ from Lemma 3.3.3. □

By the G_K-equivariant isomorphism $\bar{\Pi}_3/\bar{\Pi}_4 \simeq T_\ell E(1)$, we may rewrite the 3-step exact sequence of Π by

$$0 \to T_\ell E(1) \to \bar{\Pi}/\bar{\Pi}_4 \to \bar{\Pi}/\bar{\Pi}_3 \to 1.$$

Definition 3.3.8. Let $\bar{\Pi}^\ell$ be as in definition of $Q_2[\ell]$. We define

$$Q_3[\ell] = \bar{\Pi}/(\bar{\Pi}_4 \cdot \bar{\Pi}^\ell)$$

where $\bar{\Pi}_4 \cdot \bar{\Pi}^\ell$ is the minimal closed subgroup of $\bar{\Pi}$ generated by $\bar{\Pi}_4$ and $\bar{\Pi}^\ell$.

Proposition 3.3.9. *For any prime $\ell > 3$, the group $Q_3[\ell]$ is a central extension of $Q_2[\ell]$ by $E[\ell](1) := E[\ell] \otimes \mu_\ell$ in the category of finite G_K-groups, whose centre is exactly $E[\ell](1)$.*

Proof. By taking appropriate push-forward and pull-back of the natural projection $\bar{\Pi}/\bar{\Pi}_4 \to Q_3[\ell]$ along the 3-step exact sequence

$$0 \to T_\ell E(1) \to \bar{\Pi}/\bar{\Pi}_4 \to \bar{\Pi}/\bar{\Pi}_3 \to 1$$

of Π, we obtain the following commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & T_\ell E(1) & \longrightarrow & \bar{\Pi}/\bar{\Pi}_4 & \longrightarrow & \bar{\Pi}/\bar{\Pi}_3 & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E[\ell](1) & \longrightarrow & Q_3[\ell] & \longrightarrow & Q_2[\ell] & \longrightarrow & 1
\end{array}$$

whose rows are exact sequences and every vertical map is natural projections. Moreover, every arrow is G_K-equivariant by the construction. □

As in the case of $Q_2[\ell]$, there is a natural G_K-equivariant projection

$$\pi_1^{\text{ét}}(\bar{E}^\circ, v) \twoheadrightarrow Q_3[\ell].$$

If we write by a_3, b_3, c_3 images of a, b, c respectively in $Q_3[\ell]$ under this projection, from the above proposition, we see that the centre $Z(Q_3[\ell])$ is generated by $[a_3, c_3]$ and $[b_3, c_3]$. Then we see that every element of $Q_3[\ell]$ can be expressed in the form

$$a_3^{e_a} b_3^{e_b} c_3^{e_c} [a_3, c_3]^{e_s} [b_3, c_3]^{e_t}$$

for some $e_a, e_b, e_c, e_s, e_t \in \{0, \ldots, \ell - 1\}$: if $\alpha \in Q_3[\ell]$. Then the image of α in $Q_2[\ell]$ is expressed in the form $a_2^{e'_a} b_2^{e'_b} c_2^{e'_c}$ for some $e'_a, e'_b, e'_c \in \{0, \ldots, \ell - 1\}$. Hence, α is same with $a_3^{e'_a} b_3^{e'_b} c_3^{e'_c}$ upto an element of $Z(Q_3[\ell])$.

3.4 Galois actions on non-abelian finite groups

Let ℓ be an odd prime (we assume $\ell > 3$ when we work with $Q_3[\ell]$). Note that the finite groups $Q_2[\ell]$ and $Q_3[\ell]$ we have constructed in the previous section arise as characteristic quotients of $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$. Hence, as aforementioned, the continuous action by $G_K = \mathrm{Gal}(\bar{K}/K)$ on $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$ induces continuous G_K-actions on $Q_2[\ell]$ and $Q_3[\ell]$, i.e. we obtain Galois representations

$$\varrho_n[\ell] : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathrm{gp}}(Q_n[\ell])$$

for $n = 2, 3$. Moreover, since $Q_2[\ell]$ may be regarded as a characteristic quotient of $Q_3[\ell]$, the composite

$$\mathrm{Gal}(\bar{K}/K) \xrightarrow{\varrho_3[\ell]} \mathrm{Aut}_{\mathrm{gp}}(Q_3[\ell]) \to \mathrm{Aut}_{\mathrm{gp}}(Q_2[\ell])$$

coincides with $\varrho_2[\ell]$. By the same reason, the composites

$$\mathrm{Gal}(\bar{K}/K) \xrightarrow{\varrho_n[\ell]} \mathrm{Aut}_{\mathrm{gp}}(Q_n[\ell]) \to \mathrm{Aut}_{\mathrm{gp}}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$$

for $n = 2, 3$ coincide with the mod ℓ Galois representation attached to E.

Therefore, one may regard both $\varrho_2[\ell]$ and $\varrho_3[\ell]$ as *non-abelian* lifts of the mod ℓ Galois representation attached to E.

3.4.1 Some auxiliary results

Recall that we have constructed a rational tangential point

$$v : \mathfrak{Fet}(\bar{E}^\circ) \xrightarrow{\mathrm{res}_O} \mathfrak{Fet}(\mathbf{G}_{m,\bar{K}}) \xrightarrow{F_{\bar{1}}} \mathfrak{fset}$$

from the information extracted from the given nowhere vanishing invariant differential ω on E.

We consider the composite

$$-v : \mathfrak{Fet}(\bar{E}^\circ) \xrightarrow{\mathrm{res}_O} \mathfrak{Fet}(\mathbf{G}_{m,\bar{K}}) \xrightarrow{F_{-\bar{1}}} \mathfrak{fset}$$

where res_O is the same functor used for constructing v and $F_{-\bar{1}}$ is the fibre functor at the rational geometric point of $\mathbf{G}_{m,\bar{K}}$ given by $-1 \in \mathbf{G}_{m,K}(K)$.

Lemma 3.4.1. *Let $\iota : \bar{E} \xrightarrow{\sim} \bar{E}$ be the involution on $\bar{E}$. Then ι naturally transforms v into $-v$. More precisely, when the equivalence $\iota^* : \mathfrak{Fet}(\bar{E}^\circ) \xrightarrow{\sim} \mathfrak{Fet}(\bar{E}^\circ)$ induced from ι is composed with v, the resulting functor is exactly $-v$.*

Proof. Recall that we are given an affine equation $y^2 = 4x^3 - g_2 x - g_3$ for E uniquely determined by given nowhere vanishing invariant differential ω. Then, in terms of affine coordinates, the involution ι is expressed by

$$(x, y) \mapsto (x, -y).$$

This observation directly derives the lemma. □

Note that the functor $-v$ is also a rational tangential point of $\bar{E}^\circ$. Hence one can equip a continuous (left) G_K-action to the geometric fundamental group $\pi_1^{\text{ét}}(\bar{E}^\circ, -v)$ of $\bar{E}^\circ$ with base point $-v$ through the exactly same procedure we have explained in §2.2.4.

The next proposition directly follows from the fact that the involution is defined over K.

Proposition 3.4.2. *The involution $\iota : \bar{E} \xrightarrow{\sim} \bar{E}$ on $\bar{E}$ naturally induces a G_K-equivariant isomorphism*

$$\iota^* : \pi_1^{\acute{e}t}(\bar{E}^\circ, v) \xrightarrow{\sim} \pi_1^{\acute{e}t}(\bar{E}^\circ, -v).$$

To express the G_K-equivariant isomorphism $\iota^* : \pi_1^{\text{ét}}(\bar{E}^\circ, -v) \xrightarrow{\sim} \pi_1^{\text{ét}}(\bar{E}^\circ, v)$ in a more explicit way, it might be helpful to find topological generators of $\pi_1^{\text{ét}}(\bar{E}^\circ, -v)$. Instead of repeating all the detailed procedures, we give a pictorial summary in Figure 3.5. From the comparison isomorphism between topological and étale fundamental groups, we have

$$\pi_1^{\text{ét}}(\bar{E}^\circ, -v) \simeq \langle a', b', c' \mid [a', b']c' = 1 \rangle^\wedge.$$

Under this choice of topological generators of $\pi_1^{\text{ét}}(\bar{E}^\circ, -v)$, we can explicitly write the isomorphism ι^*:

$$\begin{array}{rcl} \pi_1^{\text{ét}}(\bar{E}^\circ, v) & \xrightarrow{\iota^*} & \pi_1^{\text{ét}}(\bar{E}^\circ, -v) \\ a & \mapsto & (a')^{-1}, \\ b & \mapsto & (b')^{-1}. \end{array}$$

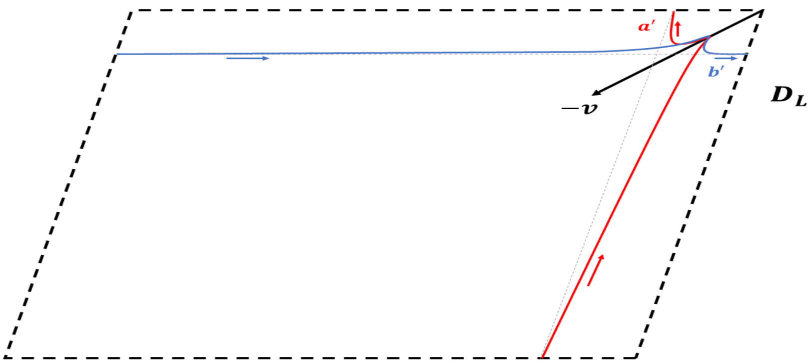

Figure 3.5: Generators of $\pi_1(E^\circ(\mathbb{C}), -v)$

Definition 3.4.3. For simplicity, we define

$$P^{(\ell)}(\bar{E}^\circ; v, -v)$$

to be the push-out of $P^{\text{ét}}(\bar{E}^\circ; v, -v)$ by the natural projection $\pi_1^{\text{ét}}(\bar{E}^\circ, v) \twoheadrightarrow \Pi$ (recall that we have defined Π as the maximal pro-ℓ quotient of $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$), i.e.

$$P^{(\ell)}(\bar{E}^\circ; v, -v) = P^{\text{ét}}(\bar{E}^\circ; v, -v) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} \Pi.$$

Then $P^{(\ell)}(\bar{E}^\circ; v, -v)$ is a G_K-equivariant Π-torsor.

Lemma 3.4.4. *$P^{(\ell)}(\bar{E}^\circ; v, -v)$ is a trivial G_K-equivariant Π-torsor .*

Proof. By Lemma 2.3.5, it is enough to show that $P^{(\ell)}(\bar{E}^\circ; v, -v)$ has an element fixed by the G_K-action. Then, by definition of $-v$, we see that it suffices to check that whether there exist K-rational solutions to the equations

$$X^{\ell^s} = -1$$

for all integers $s \geq 0$. Obviously, we have a K-rational solution $X = -1$ for each $s \geq 0$ since ℓ is given to be an odd prime. $\square$

Let λ be the trivialisation of $P^{(\ell)}(\bar{E}^\circ; v, -v)$. Then λ defines an isomorphism

$$\Pi' \xrightarrow{\sim} \Pi : w \mapsto \lambda^{-1} w \lambda$$

where Π' is the maximal pro-ℓ quotient of $\pi_1^{\text{ét}}(\bar{E}^\circ, -v)$. Moreover, this isomorphism is G_K-equivariant since λ is fixed by the G_K-action on $P^{(\ell)}(\bar{E}^\circ; v, -v)$.

3.4.2 Galois actions on $Q_2[\ell]$

Recall that we have constructed various quotients of $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$ in §3.3. We consider quotients of $\pi_1^{\text{ét}}(\bar{E}^\circ, -v)$ obtained through the exactly same procedure we have applied to construct the quotients of $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$ in §3.3. The quotients of $\pi_1^{\text{ét}}(\bar{E}^\circ, -v)$ are distinguished by attaching the upper index $'$. For example, Π' is the maximal pro-ℓ quotient $\pi_1^{\text{ét}}(\bar{E}^\circ, -v)$. Similarly,

$$\bar{\Pi}' = \Pi'/[\Pi'_2, \Pi'_2],$$

et cetera.

Also, we write by a'_2, b'_2, c'_2 for the images of a', b', c' in $Q'_2[\ell]$ through the natural projection

$$\pi_1^{\text{ét}}(\bar{E}^\circ, -v) \twoheadrightarrow Q'_2[\ell].$$

Lemma 3.4.5. *The involution ι on $\bar{E}^\circ$ induces a G_K-equivariant isomorphism*

$$\iota_2^* : Q_2[\ell] \xrightarrow{\sim} Q'_2[\ell]$$

which is expressed explicitly by

$$\begin{array}{rcl} a_2 & \mapsto & (a'_2)^{-1}, \\ b_2 & \mapsto & (b'_2)^{-1}, \\ c_2 & \mapsto & c'_2. \end{array}$$

Proof. The isomorphism $\iota^* : \pi_1^{\text{ét}}(\bar{E}^\circ, v) \xrightarrow{\sim} \pi_1^{\text{ét}}(\bar{E}^\circ, -v)$ induces naturally an isomorphism $Q'_2[\ell] \xrightarrow{\sim} Q_2[\ell]$ which we denote by ι_2^*. The explicit descriptions are obvious except for c_2. The image of c_2 under ι_2^* is computed as follows:

$$\begin{array}{rcl} \iota_2^*(c_2) & = & \iota_2^*([b_2, a_2]) \\ & = & (b'_2)^{-1}(a'_2)^{-1}b'_2a'_2 \\ & = & (b'_2)^{-1}(a'_2)^{-1}b'_2a'_2(b'_2)^{-1}(a'_2)^{-1}a'_2b'_2 \\ & = & (b'_2)^{-1}(a'_2)^{-1}c'_2a'_2b'_2 \\ & = & c'_2 \end{array}$$

where the last equality follows from the fact that c'_2 generates the centre of $Q'_2[\ell]$. □

Similarly, the G_K-equivariant isomorphism

$$\Pi' \xrightarrow{\sim} \Pi : w \mapsto \lambda^{-1} w \lambda$$

given by an trivialisation λ of $P^{(\ell)}(\bar{E}^\circ; v, -v)$ also induces a G_K-equivariant isomorphism

$$\Lambda : Q_2'[\ell] \xrightarrow{\sim} Q_2[\ell].$$

Lemma 3.4.6. *We have* $\Lambda(c_2') = \Lambda(\iota_2^*(c_2)) = c_2$.

Proof. Let a_1, b_1 be images of $a, b \in \pi_1^{\text{ét}}(\bar{E}^\circ, v)$ under the natural projection, we see that the diagram

$$\begin{tikzcd} Q_2'[\ell] \arrow[rr, "\Lambda"] \arrow[dr] & & Q_2[\ell] \arrow[dl] \\ & E[\ell] & \end{tikzcd}$$

commutes, where the two diagonal arrows are the natural projections. Moreover, every arrow in this diagram is G_K-equivariant. From this, we see that

$$\Lambda(a_2') = a_2 c_2^\alpha \text{ and } \Lambda(b_2') = b_2 c_2^\beta$$

for some $\alpha, \beta \in \{0, 1, \ldots, \ell - 1\}$. Hence we have

$$\begin{aligned} \Lambda(c_2') &= \Lambda([b_2', a_2']) \\ &= \Lambda(b_2')\Lambda(a_2')\Lambda((b_2')^{-1})\Lambda((a_2')^{-1}) \\ &= b_2 a_2 b_2^{-1} a_2^{-1} \\ &= c_2 \end{aligned}$$

since c_2 generates the centre $Z(Q_2[\ell])$. $\square$

Recall that we have set a Galois representation

$$\varrho_2[\ell] : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathrm{gp}}(Q_2[\ell]).$$

Definition 3.4.7. Let us set $K_2[\ell]$ as the subfield of $\bar{K}$ fixed by $\ker(\varrho_2[\ell])$.

Theorem 3.4.8. $K_2[\ell] = K(E[\ell])$.

Proof. Recall that $Q_2[\ell]$ is a central extension of $E[\ell]$ by μ_ℓ with $Z(Q_2[\ell]) = \mu_\ell$. We claim that the exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mu_\ell \arrow[r] & Q_2[\ell] \arrow[r] & E[\ell] \arrow[r] \arrow[l, bend right, dotted, "\mathbf{s}"'] & 0 \end{tikzcd}$$

of finite G_K-groups admits a splitting

$$\mathbf{s} : E[\ell] \to Q_2[\ell]$$

as a sequence of *finite* G_K*-sets*, i.e. $\mathbf{s}$ is a G_K-equivariant map of G_K-sets. If the claim is true, we have a bijection

$$Q_2[\ell] \simeq E[\ell] \times \mu_\ell$$

of sets and the theorem is proved.

Let a_1, b_1 be images of a_2, b_2 respectively in $E[\ell]$ under the natural projection $Q_2[\ell] \twoheadrightarrow E[\ell]$. We define such a splitting $\mathbf{s}$ as follows: for any $s, t \in \{0, 1, \ldots, \ell-1\}$, take

$$\mathbf{s}(a_1^s b_1^t) = (a_2^s b_2^t \Lambda(\iota_2^*(a_2^{-s} b_2^{-t})))^{\frac{1-\ell}{2}}$$

where $\Lambda : Q_2'[\ell] \xrightarrow{\sim} Q_2[\ell]$ is the map defined previously. It can be directly checked that the composition of $\mathbf{s}$ with the natural projection

$$Q_2[\ell] \to E[\ell]$$

is the identity map $\mathrm{id} : E[\ell] \to E[\ell]$. Moreover, by applying Lemma 3.4.6, we see that $\mathbf{s}$ is G_K-equivariant since both $\Lambda : Q_2'[\ell] \xrightarrow{\sim} Q_2[\ell]$ and $\iota_2^* : Q_2[\ell] \xrightarrow{\sim} Q_2'[\ell]$ are G_K-equivariant. $\square$

Remark 3.4.9. After we found a proof of the equality $K_2[\ell] = K(E[\ell])$, we realise that there was a study along this line in [13]. In there, Kim studied the Galois action on the pro-unipotent pro-$\mathbb{Q}_\ell$ completion $\mathcal{U}$ of Π. Through a highly abstract method, he showed that the Galois group $\mathrm{Gal}(\bar{K}/K(T_\ell E))$ acts trivially on $\mathcal{U}/\mathcal{U}_3$. From this result, one may reasonably suspect that our result should hold. However, there is no evident way for deducing our result from the Kim's argument.[2]

[2]Moreover, our argument is substantially explicit so that it gives a more concrete understanding of $Q_2[\ell]$ as a "Galois representation".

3.4.3 Galois actions on $Q_3[\ell]$

($*$) Until the end of this section, we freely use various discussions we have made in §2.3.5 and §2.2.5.

Recall that the centre $Z(Q_3[\ell]) = E[\ell](1)$ of $Q_3[\ell]$ is generated by $[a_3, c_3]$ and $[b_3, c_3]$.

Lemma 3.4.10. *Let κ be the kernel of the natural projection $Q_3[\ell] \to E[\ell]$. Then κ is an abelian subgroup fixed by the* $\mathrm{Gal}(\bar{K}/K(E[\ell]))$*-action on $Q_3[\ell]$, i.e. for any $k \in \kappa$ and $\sigma \in \mathrm{Gal}(\bar{K}/K(E[\ell]))$ we have $\sigma k = k$.*

Proof. Since κ is the subgroup generated by $c_3, [a_3, c_3], [b_3, c_3]$, it is obviously an abelian subgroup.

Recall that $Q_3[\ell]$ is a central extension of $Q_2[\ell]$ by $E[\ell](1)$ in the category of finite G_K-groups. By Theorem 3.4.8, we see that $\mathrm{Gal}(\bar{K}/K(E[\ell]))$ acts trivially on $Q_2[\ell]$. If we take an element $\sigma \in \mathrm{Gal}(\bar{K}/K(E[\ell]))$, from the fact that the natural projection $Q_3[\ell] \to Q_2[\ell]$ is G_K-equivariant, then we see that

$$\begin{aligned} \sigma(a_3) &= a_3[a_3, c_3]^{u_1}[b_3, c_3]^{v_1} \\ \sigma(b_3) &= b_3[a_3, c_3]^{u_2}[b_3, c_3]^{v_2} \end{aligned}$$

for some $u_1, v_1, u_2, v_2 \in \{0, 1, \ldots, \ell - 1\}$. Then direct computation shows us that

$$\sigma(c_3) = c_3, \ \ \sigma([a_3, c_3]) = [a_3, c_3], \ \text{ and } \ \sigma([b_3, c_3]) = [b_3, c_3].$$

Therefore, every element of κ is fixed by the $\mathrm{Gal}(\bar{K}/K(E[\ell]))$-action. $\square$

Note that, since $Q_3[\ell]$ and $E[\ell]$ are (characteristic) quotients of $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$, there are Galois coverings V_3 and V_1 of $\bar{E}^\circ$ corresponding to $Q_3[\ell]$ and $E[\ell]$ respectively. Moreover, we see that V_3 is a Galois κ-covering of V_1:

$$\begin{tikzcd} V_3 \arrow[d] \arrow[d, bend right, dashed, dash, "\kappa"'] \arrow[dd, bend left=60, dashed, dash, "Q_3[\ell]"] \\ V_1 \arrow[d] \arrow[d, bend right, dashed, dash, "E[\ell]"'] \\ \bar{E}^\circ \end{tikzcd}$$

In fact, V_1 is nothing but the base change of $E \setminus E[\ell]$ by $\mathrm{Spec}\bar{K} \to \mathrm{Spec}K$.

To simplify the following discussion, we fix a level structure

$$E[\ell] \simeq \mathbb{Z}/\ell \times \mathbb{Z}/\ell$$

by setting

$$a_1^{\alpha} b_1^{\beta} \leftrightarrow (\alpha, \beta)$$

where a_1, b_1 are, as before, images of $a, b \in \pi_1^{\text{ét}}(\bar{E}^{\circ}, v)$ in $E[\ell]$. Under this level structure, we also write by

$$R_{\alpha,\beta}$$

the ℓ-torsion point of E corresponding to $(\alpha, \beta) \in \mathbb{Z}/\ell \times \mathbb{Z}/\ell$ and by

$$T_{\alpha,\beta} : V_1 \to V_1$$

the addition-by-$R_{\alpha,\beta}$ map, i.e. $T_{\alpha,\beta}(R) = R + R_{\alpha,\beta}$. We regard $T_{\alpha,\beta} : V_1 \to V_1$ as an element of $\mathrm{Aut}(V_1/\bar{E}^{\circ}) \simeq E[\ell]$.

From §2.2.5.(d), we know that there exist a fibre $v_{0,0}$ in V_1 over v, i.e. an element in $v(V_1)$, so that κ arises as a quotient of $\pi_1^{\text{ét}}(V_1, v_{0,0})$ (kernel of $\pi_1^{\text{ét}}(\bar{E}^{\circ}, v) \twoheadrightarrow E[\ell]$). Moreover, the following diagram commutes

$$\begin{tikzcd} \pi_1^{\text{ét}}(V_1, v_{0,0}) \arrow[r] \arrow[d, two heads] & \pi_1^{\text{ét}}(\bar{E}^{\circ}, v) \arrow[d, two heads] \\ \kappa \arrow[r] & Q_2[\ell] \end{tikzcd} .$$

We extract some information of the finite étale morphism $V_3 \to V_1$ from the natural projection

$$\pi_1^{\text{ét}}(V_1, v_{0,0}) \to \kappa.$$

To achieve this purpose, we are required to find topological generators of $\pi_1^{\text{ét}}(V_1, v_{0,0})$. Since we have already explained a similar procedure before, we omit the details. As a subgroup of $\pi_1^{\text{ét}}(\bar{E}^{\circ}, v)$, we have the presentation

$$\pi_1^{\text{ét}}(V_1, v_{0,0}) \simeq \langle a^{\ell}, b^{\ell}, \{\gamma_{i,j}\}_{0 \leq i,j < \ell} \mid [a^{\ell}, b^{\ell}] \prod_{i,j} \gamma_{i,j} = 1 \rangle^{\wedge}$$

where $\gamma_{i,j} = a^i b^j c a^{-i} b^{-j}$[3][4]: this presentation is merely the presentation of the topological fundamental group of $(E \setminus E[\ell])(\mathbb{C})$. Then the isomorphism above is the isomorphism obtained by the comparison isomorphism of étale and topological fundamental groups, i.e. Theorem 2.2.7.

Lemma 3.4.11. *The map $\pi_1^{\acute{e}t}(V_1, v_{0,0}) \twoheadrightarrow \kappa$ is $\mathrm{Gal}(\bar{K}/K(E[\ell]))$-equivariant. It can be explicitly written by*

$$\begin{aligned} a^\ell, b^\ell &\mapsto 1 \\ \gamma_{i,j} &\mapsto c_3[a_3, c_3]^i [b_3, c_3]^j. \end{aligned}$$

Proof. The first part follows since $\pi_1^{\text{ét}}(\bar{E}^\circ, v) \twoheadrightarrow Q_3[\ell]$ is G_K-equivariant. The explicit description is just a concrete computation using the definition of $\gamma_{i,j}$. $\square$

Let us identify κ with $\mathbb{Z}/\ell \times \mathbb{Z}/\ell \times \mathbb{Z}/\ell$ by the map

$$\kappa \xrightarrow{\sim} \mathbb{Z}/\ell \times \mathbb{Z}/\ell \times \mathbb{Z}/\ell : c_2^i [a_2, c_2]^j [b_2, c_2]^k \mapsto (i, j, k).$$

Then, by composing $\pi_1^{\text{ét}}(V_1, v_{0,0}) \twoheadrightarrow \kappa$ with the projections $\kappa \to \mathbb{Z}/\ell$ to s-th component for $s = 1, 2, 3$, we obtain three different $\mathrm{Gal}(\bar{K}/K(E[\ell])$-equivariant surjective homomorphisms

$$\mathrm{pr}_s : \pi_1^{\text{ét}}(V_1, v_{0,0}) \twoheadrightarrow \mathbb{Z}/\ell.$$

We observe that each map pr_s corresponds to a Galois $\mathbb{Z}/\ell$-covering W_s of V_1.

Proposition 3.4.12. *Let $\Delta : V_1 \to V_1 \times_{\bar{K}} V_1 \times_{\bar{K}} V_1$ be the diagonal map. Then V_3 is canonically identified with the fibre product of $W_1 \times_{\bar{K}} W_2 \times_{\bar{K}} W_3$ and V_1 over $V_1 \times_{\bar{K}} V_1 \times_{\bar{K}} V_1$, i.e. the following diagram is Cartesian:*

$$\begin{tikzcd} V_3 \arrow[r] \arrow[d] & W_1 \times_{\bar{K}} W_2 \times_{\bar{K}} W_3 \arrow[d] \\ V_1 \arrow[r, "\Delta"] & V_1 \times_{\bar{K}} V_1 \times_{\bar{K}} V_1 \end{tikzcd}$$

[3]As an element of topological fundamental group, each $\gamma_{i,j}$ is the homotopy class of the loop $R_{i,j} + \epsilon e^{2\pi i \theta}$ $(0 \leq \theta \leq 1)$ where $\epsilon > 0$ is small enough so that there is no puncture other than $R_{i,j}$ inside of the loop.

[4]Here we do not specify the order of the product $\prod_{i,j} \gamma_{i,j}$. This is not really an important issue for the following discussion. Hence we just want to notice that there is some way for establishing that everything makes sense.

Proof. Recall that for a given good[5] topological space X, any finite index subgroup H of $\pi_1(X)$ corresponds to a finite covering space $X_H \to X$. This correspondence generalises to the setting of étale fundamental groups.

Let us observe that we have the following exact sequence

$$0 \to \mathbb{Z}/\ell \times \mathbb{Z}/\ell \times \mathbb{Z}/\ell \simeq \kappa \to Q_3[\ell] \to E[\ell] \to 0.$$

So, the étale covering corresponding to $\ker(\pi_1^{\text{ét}}(\bar{E}^\circ, v) \twoheadrightarrow Q_3[\ell])$ is the étale covering of $V_1 = (E \setminus E[\ell]) \otimes \bar{K}$ associated to $\ker(\pi_1^{\text{ét}}(V_1, v_{0,0}) \to \kappa)$. Now, the proposition directly follows from the construction of W_s. $\square$

Remark 3.4.13. In fact, by its construction, one can see that W_1 is the Galois $Q_2[\ell]$-covering of $\bar{E}^\circ$ corresponding to the natural projection $\pi_1^{\text{ét}}(\bar{E}^\circ, v) \to Q_2[\ell]$.

After identifying V_3 and $W_1 \times_{\bar{K}} W_2 \times_{\bar{K}} W_3$, we see that for any geometric point η of V_1 there is a canonical bijection

$$|(V_3)_\eta| \simeq |(W_1 \times_{\bar{K}} W_2 \times_{\bar{K}} W_3)_{\eta\times\eta\times\eta}|$$

of finite sets.

Recall that our main interest is the Galois representation

$$\varrho_3[\ell] : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathrm{gp}}(Q_3[\ell]).$$

Definition 3.4.14. We set $K_3[\ell]$ to be the subfield of $\bar{K}$ fixed by $\ker(\varrho_3[\ell])$.

Since $Q_3[\ell]$ is a central extension of $Q_2[\ell]$ by $E[\ell](1)$ and $\mathrm{Gal}(\bar{K}/K(E[\ell]))$ acts trivially on $Q_2[\ell]$[6], we only need to figure out how the Galois group $\mathrm{Gal}(\bar{K}/K(E[\ell]))$ acts on $Q_3[\ell]$.

Now, we observe that there is a G_K-equivariant bijection

$$Q_3[\ell] \simeq |(V_3)_v|$$

of finite G_K-sets. Similarly, we also have G_K-equivariant bijection

$$E[\ell] \xrightarrow{\sim} |(V_1)_v| : T_{i,j} \mapsto T_{i,j}(v_{0,0}).$$

[5]For example, path-connected, locally path-connected, and semilocally simply connected
[6]by Theorem 3.4.8

If we set

$$v_{i,j} := T_{i,j}(v_{0,0}),$$

then the finite set $|(V_3)_v|$ may be decomposed as

$$|(V_3)_v| = \bigsqcup_{0 \leq i,j < \ell} |(V_3)_{v_{i,j}}|$$

where V_3 is regarded as an étale covering of V_1. In conclusion, we have a bijection

$$Q_3[\ell] \simeq \bigsqcup_{0 \leq i,j < \ell} |(V_3)_{v_{i,j}}|$$

of finite sets. Moreover, this bijection is $\mathrm{Gal}(\bar{K}/K(E[\ell]))$-equivariant and the Galois action on the right hand side preserves disjoint union, i.e. if $w \in |(V_3)_{v_{i,j}}|$, then σw is also an element of $|(V_3)_{v_{i,j}}|$ for any $\sigma \in \mathrm{Gal}(\bar{K}/K(E[\ell]))$.

Now, our task is to analyse the $\mathrm{Gal}(\bar{K}/K(E[\ell]))$-action on the finite sets $|(V_3)_{v_{i,j}}|$ for all $0 \leq i, j < \ell$. We can go slightly further by remembering that $Q_3[\ell]$ is generated by a_3, b_3. This implies that, instead of considering every $|(V_3)_{v_{i,j}}|$, it suffices to study the $\mathrm{Gal}(\bar{K}/K(E[\ell]))$-actions on the two sets

$$|(V_3)_{v_{1,0}}| \text{ and } |(V_3)_{v_{0,1}}|,$$

or, the two sets

$$|(W_1 \times_{\bar{K}} W_2 \times_{\bar{K}} W_3)_{v_{1,0} \times v_{1,0} \times v_{1,0}}| \text{ and } |(W_1 \times_{\bar{K}} W_2 \times_{\bar{K}} W_3)_{v_{0,1} \times v_{0,1} \times v_{0,1}}|.$$

Lemma 3.4.15. *For each $s = 1, 2, 3$, let $Y_s \to \bar{E}$ be the smooth completion of the finite étale morphism $W_s \to V_1$.*

(i) $Y_1 \to \bar{E}$ is totally ramified over every $R_{i,j} \in E[\ell]$.

(ii) $Y_2 \to \bar{E}$ is totally ramified over $R_{i,j} \in E[\ell]$ with $i \neq 0$.

(iii) $Y_3 \to \bar{E}$ is totally ramified over $R_{i,j} \in E[\ell]$ with $j \neq 0$.

The morphisms $Y_s \to \bar{E}$ are unramified otherwise for all $s = 1, 2, 3$.

Proof. Note that $Y_s \to \bar{E}$ is a ramified Galois $\mathbb{Z}/\ell$-covering. It's ramification can occur only over some $R_{i,j} \in \bar{E}[\ell]$. If $y_1, \ldots, y_t$ are fibres over $R_{i,j} \in \bar{E}[\ell]$ with ramification indices $e_1, \dots, e_t$, respectively, then we have $e := e_1 = \ldots = e_t$[7] and $e_1 + \cdots + e_t = te = \ell$.[8] Also, the order of the image of $\gamma_{i,j}$ in $\mathbb{Z}/\ell$ under pr_s is exactly e. With these observations, the lemma follows from the explicit description given in Lemma 3.4.11. $\square$

Note that we have

$$\begin{aligned} |(W_1 \times_{\bar{K}} W_2 \times_{\bar{K}} W_3)_{v_{1,0} \times v_{1,0} \times v_{1,0}}| &= |(W_1)_{v_{1,0}}| \times |(W_2)_{v_{1,0}}| \times |(W_3)_{v_{1,0}}| \\ |(W_1 \times_{\bar{K}} W_2 \times_{\bar{K}} W_3)_{v_{0,1} \times v_{0,1} \times v_{0,1}}| &= |(W_1)_{v_{0,1}}| \times |(W_2)_{v_{0,1}}| \times |(W_3)_{v_{0,1}}| \end{aligned}$$

and the Galois actions on the right hand sides preserve products, i.e. if $w \in |(W_s)_{v_\bullet}|$, then we have $\sigma w \in |(W_s)_{v_\bullet}|$ for any $\sigma \in \mathrm{Gal}(\bar{K}/K(E[\ell]))$ and $\bullet \in \{(1,0),(0,1)\}$.

Proposition 3.4.16. *Let F be a number field with $\mu_\ell \subset F$. Let $V = X \setminus D$ be a geometrically connected hyperbolic curve over F such that $2 \leq \#D(F)$. Let $\bar{v}$ be a rational tangential point of $\bar{V}$ at some rational geometric point $v \in D(F)$. We suppose that $\mathbb{Z}/\ell$ (with trivial Galois action) arises as a characteristic quotient of $\pi_1^{\acute{e}t}(\bar{V}, \bar{v})$ such that the smooth completion $Y \to \bar{X}$ of the Galois $\mathbb{Z}/\ell$-covering $W \to \bar{V}$ corresponding to $\pi_1^{\acute{e}t}(\bar{V}, \bar{v}) \twoheadrightarrow \mathbb{Z}/\ell$ is totally ramified over some $v' \in D(F)$. Furthermore, we assume that there exists an automorphism f of X so that $v' = f(v)$. If we denote by F' the minimal Galois extension of F such that the* $\mathrm{Gal}(\bar{F}/F')$*-action on*

$$P^{\acute{e}t}(\bar{V}; \bar{v}, \bar{v}') \times^{\pi_1^{\acute{e}t}(\bar{V}, \bar{v})} \mathbb{Z}/\ell$$

is trivial where $\bar{v}'$ is the rational tangential point obtained from $\bar{v}$ via f, then there exists a non-zero element ξ of F such that $F' = F(\xi^{1/\ell})$.

Proof. For simplicity, we may assume that the defining data of v consists of

(i) a uniformiser ϖ of $\mathscr{O}_{\bar{X},v}$ defined over F,

(ii) $\mathfrak{Fet}(\bar{\mathbf{G}}_{m,\bar{F}}) \to \mathfrak{fset}$ is the fibre functor at $\bar{1} \in \mathbf{G}_{m,\bar{F}}(\bar{F})$.

[7] Recall that $Y_s \to \bar{E}$ is Galois.

[8] Note that, here, we are working over an algebraically closed field.

By assumption, Y admits an F-model Y_0, i.e. $Y \simeq Y_0 \times_F \bar{F}$. Also, there exists a unique F-rational point w' of Y_o over $v' \in X(F)$ from the given ramification condition. Note that the inverse of f induces a pointed isomorphism

$$(\bar{X}, v') \xrightarrow{\sim} (\bar{X}, v).$$

If we set ϖ' as the image of ϖ in $\mathscr{O}_{\bar{X},v'}$ under the isomorphism

$$\mathscr{O}_{\bar{X},v} \xrightarrow{\sim} \mathscr{O}_{\bar{X},v'}$$

induced from the inverse of f, then ϖ' is a uniformiser of $\mathscr{O}_{\bar{X},v'}$ defined over F.

Let us take a uniformiser π of $\mathscr{O}_{Y,w'}$ defined over F. Then the local homomorphism

$$\mathscr{O}_{\bar{X},v'} \to \mathscr{O}_{Y,w'}$$

is explicitly written by

$$\varpi' \mapsto \xi\pi^{\ell} + (\text{higher terms in } \pi)$$

for some $\xi \in F$. Then this ξ is the element of F we are looking for. Indeed, from §2.3.5 and (general) definition of tangential points given by Deligne, we see that the $\mathrm{Gal}(\bar{F}/F')$-action on $P^{\text{ét}}(\bar{V}; \bar{v}, \bar{v}') \times^{\pi_1^{\text{ét}}(\bar{V},\bar{v})} \mathbb{Z}/\ell$ is trivial if and only if ξ admits an ℓ-th root in F'. By the minimality condition given to F', we see that $F' = F(\xi^{1/\ell})$. □

We apply this proposition to the $\mathrm{Gal}(\bar{K}/K(E[\ell]))$-actions on sets

$$P^{\text{ét}}(V_1; v_{0,0}, v_\bullet) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell \simeq |(W_s)_{v_\bullet}|$$

for $s = 1, 2, 3$ and $\bullet \in \{(1,0), (0,1)\}$.

Lemma 3.4.17. *The group* $\mathrm{Gal}(\bar{K}/K(E[\ell]))$ *acts trivially on both* $|(W_1)_{v_{1,0}}|$ *and* $|(W_1)_{v_{0,1}}|$.

Proof. This lemma has nothing to do with Proposition 3.4.16. This is a direct consequence of Theorem 3.4.8 since W_1 is the Galois $Q_2[\ell]$-covering of $\bar{E}^\circ$ as pointed out in Remark 3.4.13. □

Theorem 3.4.18. *There are four non-zero elements, not necessarily distinct, $\xi_1, \xi_2, \xi_3, \xi_4$ of $K(E[\ell])$ such that*

$$K_3[\ell] = K(E[\ell])(\xi_i^{1/\ell} \mid i = 1, 2, 3, 4).$$

Proof. From the given projections $\mathrm{pr}_s : \pi_1^{\text{ét}}(V_1, v_{0,0}) \to \mathbb{Z}/\ell$ for $s = 1, 2, 3$, we may consider universal quotients determined by pr_s. By abuse of notation, we keep using the notation pr_s for the quotient

$$\mathrm{pr}_s : \pi_1^{\text{ét}}(V_1, \eta) \twoheadrightarrow \mathbb{Z}/\ell$$

for each $s = 1, 2, 3$ and any geometric point η of V_1. So we may think of the push-out

$$P^{\text{ét}}(V_1; \eta, \eta') \times^{\mathrm{pr}_s} \mathbb{Z}/\ell$$

for any rational geometric/tangential points η and η' of V_1.

Let $\underline{i} = (i_1, i_2)$ and $\underline{j} = (j_1, j_2)$ be elements of $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$ such that

(i) $i_1, i_2, j_1, j_2 \neq 0$,

(ii) the subgroup of $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$ generated by $\underline{i}$ and $\underline{j}$ is the same as $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$.

By Lemma 3.4.15 and Proposition 3.4.16, we see that there exist non-zero elements $\xi_{s,\bullet}$ of $K(E[\ell])$ for $s = 2, 3$, $\bullet \in \{\underline{i}, \underline{j}\}$ so that $K(E[\ell])(\xi_{s,\bullet}^{1/\ell})$ is minimal among the Galois extensions F of $K(E[\ell])$ such that the group $\mathrm{Gal}(\bar{K}/F)$ acts trivially on $P^{\text{ét}}(V_1; v_{0,0}, v_\bullet) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell$.

We claim that

$$K_3[\ell] = K(E[\ell])(\xi_{2,\underline{i}}^{1/\ell}, \xi_{2,\underline{j}}^{1/\ell}, \xi_{3,\underline{i}}^{1/\ell}, \xi_{3,\underline{j}}^{1/\ell}).$$

The later is obviously a subfield of the former.

Before we give a proof of the reverse inclusion, let us set

$$K' = K(E[\ell])(\xi_{2,\underline{i}}^{1/\ell}, \xi_{2,\underline{j}}^{1/\ell}, \xi_{3,\underline{i}}^{1/\ell}, \xi_{3,\underline{j}}^{1/\ell})$$

and $G_{K'} = \mathrm{Gal}(\bar{K}/K')$ for convenience. Note that there are non-zero integers A, B, C, D such that

$$\begin{aligned} A\underline{i} + B\underline{j} &= (1, 0), \\ C\underline{i} + D\underline{j} &= (0, 1) \end{aligned}$$

since $\underline{i}$, $\underline{j}$ generate $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$. Observe that there exists a $\mathrm{Gal}(\bar{K}/K(E[\ell]))$-equivariant isomorphism

$$P^{\text{ét}}(V_1; v_{0,0}, v_{\underline{i}}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell \simeq P^{\text{ét}}(V_1; v_{\underline{i}}, v_{2\underline{i}}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell$$

induced from $T_{\underline{i}} \in \mathrm{Aut}(V_1/\bar{E}^\circ)$. Hence $G_{K'}$ acts trivially on both sides, and this implies that $G_{K'}$ acts trivially on

$$P^{\text{ét}}(V_1; v_{0,0}, v_{2\underline{i}}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell.$$

Inductively, we see that $G_{K'}$ acts trivially on

$$P^{\text{ét}}(V_1; v_{0,0}, v_{d\underline{i}}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell$$

for any integer d.

In a similar manner, we can show that the group $G_{K'}$ acts trivially on

$$P^{\text{ét}}(V_1; v_{0,0}, v_{e\underline{j}}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell$$

for any integer e. Then we see from the $\mathrm{Gal}(\bar{K}/K(E[\ell]))$-equivariant isomorphism

$$P^{\text{ét}}(V_1; v_{0,0}, v_{B\underline{j}}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell \simeq P^{\text{ét}}(V_1; v_{A\underline{i}}, v_{A\underline{i}+B\underline{j}}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell$$

induced from $T_{A\underline{i}}$ that $G_{K'}$ acts trivially on

$$P^{\text{ét}}(V_1; v_{A\underline{i}}, v_{A\underline{i}+B\underline{j}}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell.$$

Now, since $G_{K'}$ acts trivially on both $P^{\text{ét}}(V_1; v_{0,0}, v_{A\underline{i}}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell$ and $P^{\text{ét}}(V_1; v_{A\underline{i}}, v_{A\underline{i}+B\underline{j}}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell$, we see that it also trivially acts on

$$P^{\text{ét}}(V_1; v_{0,0}, v_{1,0}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell \simeq |(W_s)_{v_{1,0}}|.$$

Through a similar procedure, one also can show that $G_{K'}$ acts trivially on

$$P^{\text{ét}}(V_1; v_{0,0}, v_{0,1}) \times^{\mathrm{pr}_s} \mathbb{Z}/\ell \simeq |(W_s)_{v_{0,1}}|.$$

Hence we have the inclusion

$$K_3[\ell] \subset K' = K(E[\ell])(\xi_{2,\underline{i}}^{1/\ell}, \xi_{2,\underline{j}}^{1/\ell}, \xi_{3,\underline{i}}^{1/\ell}, \xi_{3,\underline{j}}^{1/\ell})$$

which proves the theorem. $\square$

3.5 Elliptic polylogarithms

The theory of elliptic polylogarithms was originated by Beilinson and Levin in [1]. This theory may be regarded as an elliptic generalisation of Deligne's theory of (classical) polylogarithms [5]. Beilinson and Levin have constructed mixed sheaves called *elliptic polylogarithm extensions*. Because of its motivic nature, it is too complicated to be explained in any accessible and short form. So if the reader really wants to grasp the theory, then we recommend that they should go to Beilinson and Levin's original paper [1] where the theory was born. Appendix A in the paper [9] might possibly be a nice replacement.

Here we only explain how the theory of elliptic polylogarithms fits into our study.

Let $\mathcal{U}$ be the $\mathbb{Q}_\ell$-pro-unipotent étale fundamental group of $\bar{E}^\circ$ with base point v. We denote its Lie algebra by $\mathcal{L}$. Some details on $\mathcal{U}$ and $\mathcal{L}$ can be found in [4, §2]. For more general reference, we refer to [19, Appendix A].

We consider the lower central series

$$\mathcal{L} = \mathcal{L}_1 \supset \mathcal{L}_2 = [\mathcal{L}, \mathcal{L}_1] \supset \ldots \supset \mathcal{L}_{n+1} = [\mathcal{L}, \mathcal{L}_n] \supset \ldots$$

of $\mathcal{L}$ and the exact sequence

$$0 \to [\overline{\mathcal{L}}, \overline{\mathcal{L}}] \to \overline{\mathcal{L}} \to \mathcal{L}/[\mathcal{L}, \mathcal{L}] \to 0$$

where

$$\overline{\mathcal{L}} = \mathcal{L}/[\mathcal{L}_2, \mathcal{L}_2].$$

Note that we have the identification

$$\mathcal{L}/[\mathcal{L}, \mathcal{L}] \simeq V_\ell := T_\ell E \otimes \mathbb{Q}_\ell$$

of Galois representations.

Lemma 3.5.1. *The left adjoint action of $\overline{\mathcal{L}}$ on $[\overline{\mathcal{L}}, \overline{\mathcal{L}}]$ factors through V_ℓ. Moreover, we have an isomorphism*

$$[\overline{\mathcal{L}}, \overline{\mathcal{L}}] \simeq \prod_{i \geq 0} \mathrm{Sym}^i(V_\ell)(1)$$

of Galois representations where $\mathrm{Sym}^i(V_\ell)$ *is the* i*-th symmetric power of* V_ℓ *and* $\mathrm{Sym}^i(V_\ell)(1)$ *is the Tate twist of* $\mathrm{Sym}^i(V_\ell)$*, i.e.* $\mathrm{Sym}^i(V_\ell) \otimes \mathbb{Q}_\ell(1)$.

Proof. The first assertion is obvious. For the second assertion, we see that there exists a map

$$\mathbb{Q}_\ell(1) \to \mathcal{U}$$

of Galois representations which comes from the rational tangential point v of $\bar{E}^\circ$ as in [5, 16.1.1]. Then we obtain the desired isomorphism of Galois representations since $[\overline{\mathcal{L}}, \overline{\mathcal{L}}]$ is a free $\prod_{i>0} \mathrm{Sym}^i(V_\ell)$-module of rank 1 by the first assertion (image of the generator of $\mathbb{Q}_\ell(1)$ in $\mathcal{U}$ is a generator of $[\overline{\mathcal{L}}, \overline{\mathcal{L}}]$ as a $\prod_{i>0} \mathrm{Sym}^i(V_\ell)$-module). $\square$

3.5.1 Galois actions on $Q_3[\ell]$: revisited

$(*)$ From now on, we assume that ℓ is a prime not only odd but also greater than 3.[9] Also, in what following, Ext^1 is taken in the category of representations of G_K unless specified.

As we have pointed out in the above, $\overline{\mathcal{L}}$ determines a class in

$$\mathrm{Ext}^1(V_\ell, [\overline{\mathcal{L}}, \overline{\mathcal{L}}]) = \mathrm{Ext}^1(V_\ell, \prod_i \mathrm{Sym}^i(V_\ell)(1)).$$

Then, by pushing-out the exact sequence $0 \to [\overline{\mathcal{L}}, \overline{\mathcal{L}}] \to \overline{\mathcal{L}} \to \mathcal{L}/[\mathcal{L}, \mathcal{L}] \to 0$ through the natural projection

$$[\overline{\mathcal{L}}, \overline{\mathcal{L}}] \twoheadrightarrow \mathrm{Sym}^1(V_\ell)(1) \times \mathrm{Sym}^0(V_\ell)(1) = V_\ell(1) \times \mathbb{Q}_\ell(1),$$

we obtain a class in

$$\mathcal{E}_3 \in \mathrm{Ext}^1(V_\ell, V_\ell(1) \times \mathbb{Q}_\ell(1)).$$

Through the natural maps

$$\begin{tikzcd} & \mathrm{Ext}^1(V_\ell, V_\ell(1) \times \mathbb{Q}_\ell(1)) \arrow[dl] \arrow[dr] & \\ \mathrm{Ext}^1(V_\ell, V_\ell(1)) & & \mathrm{Ext}^1(V_\ell, \mathbb{Q}_\ell(1)) \end{tikzcd},$$

the class $\mathcal{E}_3$ produces

$$\begin{aligned} \mathcal{E}_3^1 &\in \mathrm{Ext}^1(V_\ell, \mathbb{Q}_\ell(1)), \\ \mathcal{E}_3^2 &\in \mathrm{Ext}^1(V_\ell, V_\ell(1)). \end{aligned}$$

[9] Through this assumption, we can guarantee that $\frac{1}{12}$ is a unit in $\mathbb{Z}_\ell$, which is the fact will be used later.

Theorem 3.5.2. *We have* $K_3[\ell] = K(E[\ell])(\Delta_{\mathrm{mod}}^{1/\ell})$.

Proof. By following [1], we see that the elliptic polylogarithm extension (shortly, EPE) gives a class

$$\mathcal{E}_{\mathrm{pol}} \in \mathrm{Ext}^1(V_\ell, V_\ell(1)).$$

From the construction of EPE given in [1, §1], it is known that one can prove that $\mathcal{E}_{\mathrm{pol}}$ is exactly the same as $\mathcal{E}_3^2$.[10] What is claimed by Beilinson and Levin [1, §2.1.6] is as follows: let us set $L = K(E[\ell])$ and G_L the Galois group $\mathrm{Gal}(\bar{K}/L)$. Let us consider the natural map

$$H^1(G_L, \mathbb{Q}_\ell(1)) \simeq \mathrm{Ext}^1_{G_L}(\mathbb{Q}_\ell, \mathbb{Q}_\ell(1)) \to \mathrm{Ext}^1_{G_L}(V_\ell, V_\ell(1)).$$

Then the image of $\frac{1}{12} \cdot kumm(\Delta_{\mathrm{mod}})$ in $\mathrm{Ext}^1_{G_L}(V_\ell, V_\ell(1))$ is exactly $\mathcal{E}_{\mathrm{pol}}$ (regarded as a representation of G_L via $G_L \hookrightarrow G_K$) where $kumm(\Delta_{\mathrm{mod}})$ is the Kummer class of $\Delta_{\mathrm{mod}} \in K^\times \subset L^\times$ in $H^1(G_L, \mathbb{Z}_\ell(1))$.

It is well-known that the maximal pro-ℓ quotient Π of $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$ can be regarded as a $\mathbb{Z}_\ell$-lattice of $\bar{\mathcal{L}}$. Hence, its image in $\mathcal{E}_3$ produces a $\mathbb{Z}_\ell$-lattice of $\mathcal{E}_3$. Now, we observe that the exact sequence

$$1 \to \kappa \to Q_3[\ell] \to E[\ell] \to 0$$

in Lemma 3.4.10 may be rewritten by

$$1 \to E[\ell](1) \times \mu_\ell \to Q_3[\ell] \to E[\ell] \to 0.$$

So, we may look $Q_3[\ell]$ as the "mod ℓ quotient" of the $\mathbb{Z}_\ell$-lattice of $\mathcal{E}_3$ determined by Π. Under these observations, $K_3[\ell]$ is the minimal Galois extension of K such that $\mathrm{Gal}(\bar{K}/K_3[\ell])$ acts trivially on the mod ℓ quotient of the $\mathbb{Z}_\ell$-lattice of $\mathcal{E}_3$ determined by Π. To determine $K_3[\ell]$, it suffices to consider the G_K-representations $\mathcal{E}_3^1$ and $\mathcal{E}_3^2$.[11] By the similar reason for $Q_3[\ell]$, we may regard $Q_2[\ell]$ as the mod ℓ quotient of the $\mathbb{Z}_\ell$-lattice $\mathcal{E}_3^1$ determined by Π, and we have seen that $\mathrm{Gal}(\bar{K}/K(E[\ell]))$ acts trivially on $Q_2[\ell]$ which means $K_3[\ell] \supset K(E[\ell])$.[12] Now, we need to care about

[10] In fact, the construction of EPE given by Beilinson and Levin is in motivic nature. In [1], they proved the Betti realisation version of the equality $\mathcal{E}_{\mathrm{pol}} = \mathcal{E}_3^2$. What we need here is the ℓ-adic realisation version whose proof is found in [9, Appendix].

[11] More precisely, mod ℓ quotients of their lattices determined by Π.

[12] In fact, $K(E[\ell])$ is the minimal among the Galois extensions K' of K such that $\mathrm{Gal}(\bar{K}/K')$ acts trivially on $Q_2[\ell]$.

$\mathcal{E}_3^2$. By the aforementioned result of Beilinson and Levin, we only need to care about the Kummer class of Δ_{mod} in $H^1(G_L, \mu_\ell)$,[13] and we see that its image in $H^1(\mathrm{Gal}(K_3[\ell]/L), \mu_\ell)$ is trivial if and only if $K_3[\ell]$ contains $\Delta_{\mathrm{mod}}^{1/\ell}$. In conclusion, we see that $K_3[\ell] = K(E[\ell])(\Delta_{\mathrm{mod}}^{1/\ell})$. $\square$

[13] We remark that $\frac{1}{12}$ is a unit in $\mathbb{Z}_\ell$ by our assumption on ℓ.

Chapter 4

Application I: non-abelian torsors

In this chapter, we study the variation of the Galois action on the geometric fundamental group of once-punctured elliptic curve over a number field when the base point varies. In the first section, we review a classical result of Ribet which may be regarded as a study in this direction. In section 2, we see how the work of Ribet can be interpreted in terms of Galois actions on torsors. This sheds light on a way for non-abelian generalisations of Ribet's work. Prior to the study of the non-abelian generalisations in the last section, we see the non-CM generalisation of the work of Ribet.

As in the previous chapter, we assume that K is a number field with a fixed algebraic closure $\bar{K}$. The absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ is sometimes abbreviated by G_K.

Furthermore, when we say that E is an elliptic curve over K, we always assume that we are given a nowhere vanishing invariant differential ω on E and accompanying information explained in §3.1.1. So, we use various notations given in §3.1.1 without further explanation.

Lastly, when E is an elliptic curve over K and z is a K-rational point of E, for any integer $n \geq 1$, any $z' \in E(\bar{K})$ is called a *n-th root* of z if $nz' = z$.

4.1 Review of classical results

Let E be an elliptic curve over K. We suppose that

(i) E has complex multiplication,

(ii) E has a non-torsion K-rational point α.

For a given prime ℓ, we let

$$K_{\alpha,\ell}$$

be the Galois extension of K generated by all ℓ-th roots of α. Then it is known that $K_{\alpha,\ell}$ is a Galois extension of $K(E[\ell])$.

One can define an injective group homomorphism

$$\mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell])) \hookrightarrow E[\ell]$$

in the following way: take any ℓ-th root of α, say z. Define

$$\mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell])) \to E[\ell] : g \mapsto (g(z) - z).$$

Then, since the multiplication-by-ℓ map on E commutes with every element of $\mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell]))$, it can be easily checked that this is a well-defined injective group homomorphism.

Lemma 4.1.1. *Let ℓ be a prime and*

$$\nu_\ell : \mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell])) \to E[\ell]$$

be the map as in the above. Then the image $\mathrm{im}(\nu_\ell)$ *is a subgroup of* $E[\ell]$ *stable under the* $\mathrm{Gal}(K(E[\ell])/K)$*-action, i.e. for any* $x \in \mathrm{im}(\nu_\ell)$ *and* $\sigma \in \mathrm{Gal}(K(E[\ell])/K)$ *we have* $\sigma(x) \in \mathrm{im}(\nu_\ell)$.

Proof. Indeed, this lemma follows from the following formula:

$$\sigma\nu_\ell(\tau) = \nu_\ell(\sigma\tau\sigma^{-1})$$

for any $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and $\tau \in \mathrm{Gal}(\bar{K}/K(E[\ell]))$. □

Remark 4.1.2. The map $\mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell])) \hookrightarrow E[\ell]$ defined in the above is independent of the choice of an ℓ-th root of α.

Theorem 4.1.3 (Ribet [20]). *Under the above circumstance, the homomorphism*

$$\mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell])) \hookrightarrow E[\ell]$$

is surjective for almost all primes ℓ.

4.2 Formulation in terms of torsors

As in the previous section, let us consider a CM elliptic curve E over K having a non-torsion K-rational point α. Let us also fix a prime ℓ.

Note that $E[\ell]$ is naturally considered as a characteristic quotient of $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$.

Lemma 4.2.1. *The automorphism group of the $E[\ell]$-torsor*

$$P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} E[\ell]$$

is isomorphic to $E[\ell]$.

Proof. We define a map

$$\Xi : \mathrm{Aut}(P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} E[\ell]) \to E[\ell]$$

in the following way: firstly pick an element γ of $P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} E[\ell]$. Note that, if f is an automorphism of $P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} E[\ell]$, there uniquely exists an element $w_f \in E[\ell]$ such that

$$f(\gamma) = \gamma w_f.$$

We define

$$\Xi(f) = w_f.$$

Uniqueness of w_f explains injectivity of the map Ξ. Moreover, from the equality

$$w_{f \circ g} = w_f w_g$$

for any automorphisms f, g of $P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} E[\ell]$, we see that Ξ is indeed a group homomorphism.

To define an inverse of Ξ, we firstly claim that any automorphism f of

$$P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} E[\ell]$$

is completely determined its value at γ (the chosen element). Indeed, if γ' is an element of $P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} E[\ell]$, there exists $w \in E[\ell]$ uniquely such that

$$\gamma' = \gamma w.$$

Then $f(\gamma') = f(\gamma w) = f(\gamma)w$, hence, the claim is proved. Now, we define a map

$$\Psi : E[\ell] \to \mathrm{Aut}(P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} E[\ell])$$

by

$$w \mapsto (f : \gamma \mapsto \gamma w).$$

We can check that Ψ is an injective group homomorphism: let us set $\Psi(w) = f_w$ for simplicity. Then $f_w = f_v$ implies that $\gamma w = \gamma v$ for any element γ of $P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} E[\ell]$. By definition of torsor, we should have $w = v$. Also, we have $f_{wv}(\gamma) = \gamma wv = (\gamma w)v = f_v(\gamma w) = f_v(f_w(\gamma))$, which implies the association $w \mapsto f_w$ is a group homomorphism.

Finally, the maps Ξ and Ψ are inverses to each other, so the proof is finished. $\square$

We see that the G_K-action on $P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} E[\ell]$ naturally induces a group homomorphism

$$\mathrm{Gal}(\bar{K}/K(E[\ell])) \to \mathrm{Aut}(P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} E[\ell]).$$

Hence, by using the isomorphism in Lemma 4.2.1, we obtain a group homomorphism

$$\varphi_\ell : \mathrm{Gal}(\bar{K}/K(E[\ell])) \to E[\ell].$$

Proposition 4.2.2. *The theorem of Ribet is equivalent to saying that φ_ℓ is surjective for almost all prime ℓ.*

Proof. This equivalence is a direct consequence of the bijection we have explained in §2.3.5.[1] $\square$

Under this equivalence, one may naturally ask about the Galois actions on

$$P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} Q_s[\ell]$$

for $s = 2, 3$ where $Q_s[\ell]$ are non-abelian finite G_K-groups constructed in the previous chapter.

[1] This equivalence might be well-known to experts, but we could not find any literature specifying it.

Definition 4.2.3. Let P be a G-equivariant π-torsor for profinite groups G and π where G acts continuously on π from the left. We say that P is *abelian* (resp. *non-abelian*) if π is an abelian (resp. a non-abelian) group.

Remark 4.2.4. When P is a G-equivariant π-torsor for some profinite groups G and π, the G-action on P gives a homomorphism

$$G \to \mathrm{Aut}_{\mathrm{set}}(P)$$

where $\mathrm{Aut}_{\mathrm{set}}(P)$ is the group of automorphisms of P as a set. If we denote by $\mathrm{Aut}(P)$ the group of automorphisms of P as a π-torsor, then not every element of G takes value in $\mathrm{Aut}(P)$ under $G \to \mathrm{Aut}_{\mathrm{set}}(P)$. Only the elements of the subgroup $\ker(G \to \mathrm{Aut}_{\mathrm{gp}}(\pi))$ of G take values in $\mathrm{Aut}(P)$.

4.3 Non-CM generalisation

Before we get into the study of Galois actions on non-abelian torsors, we generalise the theorem of Ribet for non-CM elliptic curves.

Throughout this section, we let E be a non-CM elliptic curve over K and $\alpha \in E(K)$ a non-torsion point.

Lemma 4.3.1. *Let ℓ be a prime. Let us consider $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$ as a $\mathrm{GL}_2(\mathbb{F}_\ell)$-group under the natural left action. If H is a subgroup of $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$ stable under the $\mathrm{GL}_2(\mathbb{F}_\ell)$-action, then H is either the trivial subgroup or $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$.*

Proof. Let H be a non-trivial subgroup of $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$ stable under the $\mathrm{GL}_2(\mathbb{F}/\ell)$-action. We write every element of $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$ in the column form. Let $\begin{bmatrix} u \\ v \end{bmatrix}$ be a non-zero element of H. We claim that there exists an element $M \in \mathrm{GL}_2(\mathbb{F}_\ell)$ such that

$$M \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Indeed, without loss of generality we may assume that $u \neq 0$. Then we have

$$M = \begin{pmatrix} u^{-1} & 0 \\ -vu^{-1} & 1 \end{pmatrix}$$

Also, we have

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Therefore, H is the same as the whole group $\mathbb{Z}/\ell \times \mathbb{Z}/\ell$. □

Theorem 4.3.2. *For almost all prime ℓ the map*

$$\mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell])) \to E[\ell]$$

in the theorem of Ribet is surjective, hence, it is an isomorphism.

Proof. We have already seen that the image of $\mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell]))$ in $E[\ell]$ is a $\mathrm{Gal}(K(E[\ell])/K)$-stable subgroup. Moreover, from [10, Lemma 3.7], we see that $\mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell]))$ is non-trivial for almost all prime ℓ. By the work of Serre [21], we know that

$$\mathrm{Gal}(K(E[\ell])/K) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$$

for almost all prime ℓ since our elliptic curve has no complex multiplication. Therefore, we have

$$\mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell])) \simeq E[\ell]$$

for almost all prime ℓ by the above lemma. □

4.4 Non-abelian torsors and Galois representations

Throughout this section we fix an elliptic curve E over K having a non-torsion K-rational point α.

Recall that $Q_2[\ell]$ is a central extension of $E[\ell]$ by μ_ℓ in the category of finite G_K-groups. The G_K-action on $Q_2[\ell]$ gives the Galois representation

$$\varrho_2[\ell] : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathrm{gp}}(Q_2[\ell])$$

whose kernel is denoted by

$$\mathrm{Gal}(\bar{K}/K_2[\ell]) = \ker(\varrho_2[\ell]).$$

Then we have a group homomorphism

$$\mathrm{Gal}(\bar{K}/K_2[\ell]) \to \mathrm{Aut}(P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} Q_2[\ell])$$

where the later group is the automorphism group of $Q_2[\ell]$-tosor $P^{\text{ét}}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\text{ét}}(\bar{E}^\circ, v)} Q_2[\ell]$.

Lemma 4.4.1. *There is a (non-canonical) isomorphism*

$$\mathrm{Aut}(P^{ét}(\bar{E}^{\circ}; v, \alpha) \times^{\pi_1^{ét}(\bar{E}^{\circ}, v)} Q_2[\ell]) \xrightarrow{\sim} Q_2[\ell]$$

of finite groups.

Proof. Exactly the same method used in proof of Lemma 4.2.1 is applied to derive the isomorphism. □

Definition 4.4.2. Let us call a prime ℓ an *R-prime* if the map

$$\mathrm{Gal}(K_{\alpha,\ell}/K(E[\ell])) \to E[\ell]$$

in the theorem of Ribet is surjective.

Theorem 4.4.3. *For any R-prime ℓ, the composite*

$$\varphi : \mathrm{Gal}(\bar{K}/K_2[\ell]) \to \mathrm{Aut}(P^{ét}(\bar{E}^{\circ}; v, \alpha) \times^{\pi_1^{ét}(\bar{E}^{\circ}, v)} Q_2[\ell]) \simeq Q_2[\ell]$$

is surjective.

Before we give the proof of this theorem, we prove the following group theoretical fact:

Proposition 4.4.4. *Let $1 \to C \to G \xrightarrow{\pi} Q \to 1$ be a central extension of finite groups with the property that C is generated by commutators in G. Then any homomorphism of groups $\theta : G' \to G$ is surjective if and only if the composition homomorphism $\pi \circ \theta$ is surjective.*

Proof. The only non-trivial part is the 'if' part. To show the 'if' part, let $c_1, \ldots, c_n$ be generators of C such that $c_i = [g_{i1}, g_{i2}]$ for some $g_{i1}, g_{i2} \in G$. Let us take $g'_{ij} \in G'$ such that $\pi \circ \theta(g'_{ij}) = \pi(g_{ij})$. Then we have $\theta(g'_{ij}) = g_{ij} c_1^{u_1} \cdots c_n^{u_n}$ for some integers u_k. So, we have $\theta([g'_{i1}, g'_{i2}]) = [g_{i1}, g_{i2}] = c_i$. Hence, c_i's are contained in the image of θ.

Now, let us take a set $\{g_1, \ldots, g_m\}$ of generators of G. Then we can find $g'_i \in G'$ such that $\pi \circ \theta(g'_i) = \pi(g_i)$, which implies that $\theta(g'_i)$ and g_i differ by an element of C. Therefore, we see that g_i's are contained in the image of θ, i.e. θ is surjective. □

Proof of Theorem 4.4.3. We have seen that $K_2[\ell] = K(E[\ell])$ for any odd prime ℓ, see Theorem 3.4.8.

Note that the composite

$$\mathrm{Gal}(\bar{K}/K(E[\ell])) \to Q_2[\ell] \twoheadrightarrow E[\ell]$$

is the same as the homomorphism $\mathrm{Gal}(\bar{K}/K(E[\ell])) \to E[\ell]$ in the theorem of Ribet. So, the theorem is obtained by applying Proposition 4.4.4. $\square$

We repeat the similar procedure for $Q_3[\ell]$. It is a central extension of $Q_2[\ell]$ by $E[\ell](1)$ in the category of finite G_K-groups. It has generators a_3, b_3, c_3 inherited from the topological generators of $\pi_1^{\text{ét}}(\bar{E}^\circ, v)$, and the centre $Z(Q_3[\ell]) = E[\ell](1)$ is generated by $[a_3, c_3]$ and $[b_3, c_3]$.

Lemma 4.4.5. *The group of automorphisms of the G_K-equivariant $Q_3[\ell]$-torsor $P^{\acute{e}t}(\bar{E}^\circ; v, \alpha) \times^{\pi_1^{\acute{e}t}(\bar{E}^\circ, v)} Q_3[\ell]$ is isomorphic to $Q_3[\ell]$.*

Proof. Omitted. $\square$

Recall that we have set

$$\mathrm{Gal}(\bar{K}/K_3[\ell])) = \ker(\mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathrm{gp}}(Q_3[\ell])).$$

Theorem 4.4.6. *Let ℓ be an R-prime. The homomorphism*

$$\mathrm{Gal}(\bar{K}/K_3[\ell])) \to Q_3[\ell]$$

is surjective when the modular discriminant Δ_{mod} of E admits a $K(E[\ell])$-rational ℓ-th root.

Proof. Under the given condition, we have $K_3[\ell] = K(E[\ell])$. Then one can apply Proposition 4.4.4 to obtain this theorem. $\square$

Chapter 5

Application II: rational points on moduli stacks

In this chapter, we study some questions on the sets of rational points on moduli stacks of elliptic curves with non-abelian level structures. In the first section, we start with a brief historical review and preliminary theories. After reviewing some preliminary theories, we explain Chen's idea for defining non-abelian level structures on elliptic curves. In the second section, we explain some parts of Chen's paper [3] which are required for our applications achieved in the final section.

5.1 Teichmüller structures (or G-structures)

In [6], Deligne and Mumford introduced the notion of *Teichmüller structures* on curves. After it was introduced, Pikaart and de Jong [18] studied Teichmüller structures for proper curves of genus greater than 1. Recently, William Y. Chen [3] has introduced Teichmüller structures (or G-structures in his terminology) for elliptic curves and studied various interesting questions related with the topic.

To get into the theory of Chen, we are required to review some necessary theories of relative fundamental groups. Before we start, we firstly set up some notations: for a connected scheme S, we let $\mathbb{L}_S$ be the set of primes invertible on S.

For an elliptic curve E over a connected scheme S with zero-section $O : S \to E$, we set $E^\circ = E - O(S)$.

Lastly, a finite group G is called 2-*generated* if it can be generated by two elements.

5.1.1 Relative fundamental groups

Proposition 5.1.1 ([3, Proposition 2.1.4]). *Let E be an elliptic curve over a connected scheme S. Let us assume that either*

(i) $\mathbb{L} := \mathbb{L}_S \neq \emptyset$ *or*

(ii) the structure morphism $E^\circ \to S$ admits a section $g : S \to E^\circ$.

Let s be a given geometric point of S. For a geometric point η of E°_s, by abuse of notation, we use the symbol η for the geometric points of E° and of S induced from η. Then we have an exact sequence

$$1 \to \pi_1^{\mathbb{L}}(E^\circ_s, \eta) \to \pi_1'(E^\circ, \eta) \to \pi_1^{\acute{e}t}(S, \eta) \to 1$$

where

- $\pi_1^{\mathbb{L}}(E^\circ_s, \eta)$ *is the maximal pro-$\mathbb{L}$ quotient of* $\pi_1^{\acute{e}t}(E^\circ_s, \eta)$ *and*
- $\pi_1'(E^\circ, \eta) = \pi_1^{\acute{e}t}(E^\circ, \eta)/M$ *where M is defined to be the smallest subgroup of* $\ker(\pi_1^{\acute{e}t}(E^\circ, \eta) \to \pi_1^{\acute{e}t}(S, \eta))$ *such that the quotient*

$$\ker(\pi_1^{\acute{e}t}(E^\circ, \eta) \to \pi_1^{\acute{e}t}(S, \eta))/M$$

is a pro-$\mathbb{L}$ group.

Let us suppose that E is an elliptic curve over a connected scheme S. We also suppose that there is a given geometric point s of S. If the structure morphism $E^\circ \to S$ admits a section $g : S \to E^\circ$, from [7, Exposé V Proposition 5.2], we see that there exists a pro-object, denoted by

$$\pi_1^{\mathbb{L}_S}(E^\circ/S, g, s),$$

of the category of finite étale group schemes over S. This pro-object is called the *relative fundamental group* of E°.

Proposition 5.1.2 ([7, Exposé XIII 4.5]). *For the triples E, s, and $g : S \to E^\circ$ as in the above, we have*

(i) the formulation of $\pi_1^{\mathbb{L}_S}(E^\circ/S, g, s)$ commutes with arbitrary base change.

(ii) for any geometric point ξ of S, there is a canonical isomorphism

$$\pi_1^{\mathbb{L}_S}(E^\circ/S, g, s)_\xi \simeq \pi_1^{\mathbb{L}_S}(E^\circ_\xi, g(\xi))$$

where $g(\xi)$ is the geometric point of E°_ξ given by the (unique) dotted arrow in the following commutative diagram:

$$\begin{tikzcd}
\xi \arrow[drr, bend left] \arrow[ddr, dotted] \arrow[dddr, equal, bend right] & & \\
& & S \arrow[d, "g"] \\
& E^\circ_\xi \arrow[r] \arrow[d] & E^\circ \arrow[d] \\
& \xi \arrow[r] & S
\end{tikzcd}$$

(iii) if s' is a geometric point of S distinct to s, then the pro-object $\pi_1^{\mathbb{L}_S}(E^\circ/S, g, s')$ is canonically isomorphic to $\pi_1^{\mathbb{L}_S}(E^\circ/S, g, s)$.

From the canonical isomorphism

$$\pi_1^{\mathbb{L}_S}(E^\circ/S, g, s') \simeq \pi_1^{\mathbb{L}_S}(E^\circ/S, g, s)$$

in the above proposition, it makes sense to simply write

$$\pi_1^{\mathbb{L}_S}(E^\circ/S, g)$$

instead of $\pi_1^{\mathbb{L}_S}(E^\circ/S, g, s)$.

5.1.2 G-structures

Until the end of this section, let S be a connected scheme with $\mathbb{L}_S \neq \emptyset$. We let G be a finite 2-generated group whose order is invertible on S. By abuse of notation, we write G for the constant group scheme over S defined by G. We also write G for the sheaf on $\mathfrak{Sch}_{S,\text{ét}}$ determined by the constant group scheme G over S.

Note that if E is an elliptic curve over S such that the structure morphism $E^\circ \to S$ admits a section $g : S \to E^\circ$, then we may consider the pro-object $\pi_1^{\mathbb{L}_S}(E^\circ/S, g)$ as a sheaf on $\mathfrak{Sch}_{S,\text{ét}}$.

Proposition 5.1.3 ([3, Proposition 2.2.1 and Proposition 2.2.2])**.** *Let E be an elliptic curve over S such that the structure morphism $E^\circ \to S$ admits a section $g : S \to E^\circ$. Let*

$$\mathscr{H}om_S^{\mathrm{sur}}(\pi_1^{\mathbb{L}_S}(E^\circ/S, g), G)$$

be the sheaf $\mathscr{H}om$ of surjective homomorphisms

$$\pi_1^{\mathbb{L}_S}(E^\circ/S, g) \to G$$

of sheaves on $\mathfrak{Sch}_{S,ét}$. Then $\mathscr{H}om_S^{\mathrm{sur}}(\pi_1^{\mathbb{L}_S}(E^\circ/S, g), G)$ is finite locally constant on $\mathfrak{Sch}_{S,ét}$.

If $h : S \to E^\circ$ is another section of the structure morphism $E^\circ \to S$, there is a canonical isomorphism

$$\mathscr{H}om_S^{\mathrm{sur}}(\pi_1^{\mathbb{L}_S}(E^\circ/S, g), G) \xrightarrow{\sim} \mathscr{H}om_S^{\mathrm{sur}}(\pi_1^{\mathbb{L}_S}(E^\circ/S, h), G)$$

of sheaves on $\mathfrak{Sch}_{S,ét}$.

Under the situation in the above proposition, let us define

$$\mathscr{H}om^{\text{sur-ext}}(\pi_1(E^\circ/S), G) := \mathscr{H}om_S^{\mathrm{sur}}(\pi_1^{\mathbb{L}_S}(E^\circ/S, g), G)/\mathrm{Inn}(G)$$

This notation does make sense from the canonical isomorphism

$$\mathscr{H}om_S^{\mathrm{sur}}(\pi_1^{\mathbb{L}_S}(E^\circ/S, g), G) \xrightarrow{\sim} \mathscr{H}om_S^{\mathrm{sur}}(\pi_1^{\mathbb{L}_S}(E^\circ/S, h), G)$$

in the above proposition.

Definition 5.1.4 (Chen)**.** Let E be an elliptic cure over S. For a finite 2-generated group G, the *sheaf of G-structures* on E/S is defined to be the sheaf associated to the following presheaf on $\mathfrak{Sch}_{S,\text{ét}}$:

$$(T \to S) \mapsto \begin{cases} \mathscr{H}om^{\text{sur-ext}}(\pi_1(E^\circ/S), G)(T) & \text{if } E_T^\circ/T \text{ admits a section over } T, \\ \emptyset & \text{otherwise} \end{cases}.$$

By abuse of notation, this sheaf is also denoted by

$$\mathscr{H}om^{\text{sur-ext}}(\pi_1(E^\circ/S), G).$$

A global section of $\mathscr{H}om^{\text{sur-ext}}(\pi_1(E^\circ/S), G)$ is called a *G-structure* on E/S.

Proposition 5.1.5 ([3, Proposition 2.2.4]). *Let E be an elliptic curve over S. The sheaf $\mathscr{H}om^{\text{sur-ext}}(\pi_1(E^\circ/S), G)$ of G-structures on E/S is finite locally constant, representable by a finite étale scheme over S. If $\tilde{s}$ is a geometric point of E_s° where $s \in S$, then we have*

$$\mathscr{H}om^{\text{sur-ext}}(\pi_1(E^\circ/S), G)_s = \mathrm{Hom}^{\text{sur-ext}}(\pi_1^{\mathbb{L}_S}(E_s^\circ, \tilde{s}), G) \simeq \mathrm{Hom}^{\text{sur-ext}}(\widehat{F}_2, G)$$

where $\widehat{F}_2$ is the profinite completion of the free group of rank 2.

Remark 5.1.6. In fact, Chen gave some explicit descriptions of G-structures. Since this is not really required for our study, for the reader who is interested, we refer to [3, Proposition 2.2.6].

Recall that for an elliptic curve E over S and an integer $N \geq 1$, the $\Gamma(N)$-*structure* on E/S is an isomorphism

$$(\mathbb{Z}/N \times \mathbb{Z}/N)_S \simeq E[N]$$

of group schemes over S, see [11, Chapter 3].

Proposition 5.1.7 ([3, Proposition 2.2.12]). *Let N be an integer $N \geq 1$. For an elliptic curve E over S, there is a bijection between the set of $(\mathbb{Z}/N \times \mathbb{Z}/N)$-structures on E/S and the set of $\Gamma(N)$-structures on E/S.*

5.2 Moduli stacks of G-structures

Throughout this section we fix a finite 2-generated group G whose order is denoted by N.

It is well-known that the moduli stack $\mathscr{M}(1)$ of elliptic curves is a connected noetherian smooth separated Deligne–Mumford stack over $\mathrm{Spec}\mathbb{Z}$.

We consider the functor

$$P_G : \mathscr{M}(1)_{\mathbb{Z}[\frac{1}{N}]} \to \mathfrak{fset}$$

given by

$$(E \to S) \mapsto \{\text{global sections of } \mathscr{H}om^{\text{sur-ext}}(\pi_1(E^\circ/S), G)\}.$$

Proposition 5.2.1 ([3, Proposition 3.1.2])**.** *The functor $P_G : \mathscr{M}(1)_{\mathbb{Z}[\frac{1}{N}]} \to \mathfrak{fset}$ is a sheaf on $\mathscr{M}(1)_{\mathbb{Z}[\frac{1}{N}]}$. Moreover, P_G is a finite étale relatively representable moduli problem in the sense of [11, Chapter 4].*

Definition 5.2.2 (Chen)**.** A fibred category $\mathscr{M}(G)$ over $\mathfrak{Sch}_{\mathrm{Spec}\mathbb{Z}[\frac{1}{N}]}$ is defined as follows: for a connected scheme S over $\mathbb{Z}[\frac{1}{N}]$, the objects over S are pairs $(E/S, \alpha)$ where $\alpha \in P_G(E/S)$, and a morphism between $(E/S, \alpha)$ and $(E'/S', \alpha')$ is a Cartesian diagram

$$\begin{tikzcd} (E')^\circ \arrow[r, "\phi"] \arrow[d] & E^\circ \arrow[d] \\ S' \arrow[r] & S \end{tikzcd}$$

such that $\phi^*\alpha = \alpha'$.

Proposition 5.2.3 ([3, Proposition 3.1.4])**.** *$\mathscr{M}(G)$ is a Deligne–Mumford stack, finite étale over $\mathscr{M}(1)_{\mathbb{Z}[\frac{1}{N}]}$, smooth and separated over $\mathbb{Z}[\frac{1}{N}]$.*

Now, we see the last proposition required for the study in the next section.

Proposition 5.2.4 ([3, Proposition 3.2.8])**.** *Let $f : G \to G'$ be a surjective group homomorphism. Then f induces a surjective finite étale morphism*

$$f_* : \mathscr{M}(G) \to \mathscr{M}(G').$$

5.3 Rational points on moduli stacks

Let us consider the following (abstract) groups which are modelled by $Q_2[\ell]$ and $Q_3[\ell]$ in Chapter 3: for a prime ℓ, we let $G_2[\ell]$ be a group such that

(i) $Z(G_2[\ell]) \simeq \mathbb{Z}/\ell$,

(ii) $G_2[\ell]/Z(G_2[\ell]) \simeq \mathbb{Z}/\ell \times \mathbb{Z}/\ell$.

We also let $G_3[\ell]$ be a group such that

(i′) $Z(G_3[\ell]) \simeq \mathbb{Z}/\ell \times \mathbb{Z}/\ell$,

(ii′) $G_3[\ell]/Z(G_3[\ell]) \simeq G_2[\ell]$.

Then, for any odd prime ℓ, there always exist such groups $G_s[\ell]$ for $s = 2, 3$. Moreover, both $G_2[\ell]$ and $G_3[\ell]$ are finite and generated by 2-elements.

Theorem 5.3.1. *Let ℓ be an odd prime greater than 3. For $s = 2, 3$, let $G_s[\ell]$ be finite groups as in the above.*

(a) Let K be a number field. Then any K-rational point z of $\mathscr{M}(\mathbb{Z}/\ell \times \mathbb{Z}/\ell)$ lifts to $\mathscr{M}(G_2[\ell])$:

$$\begin{tikzcd} & \mathscr{M}(G_2[\ell]) \arrow[d] \\ \mathrm{Spec}K \arrow[r, "z"'] \arrow[ur, dashed] & \mathscr{M}(\mathbb{Z}/\ell \times \mathbb{Z}/\ell) \end{tikzcd}$$

(b) Let K be a number field. Let z be a K-rational point of $\mathscr{M}(\mathbb{Z}/\ell \times \mathbb{Z}/\ell)$. If the underlying elliptic curve E_z of z admits a nowhere vanishing invariant differential ω such that the modular discriminant Δ_{mod} determined by ω has a K-rational ℓ-th root, then z lifts to $\mathscr{M}(G_3[\ell])$.

$$\begin{tikzcd} & \mathscr{M}(G_3[\ell]) \arrow[d] \\ \mathrm{Spec}K \arrow[r, "z"'] \arrow[ur, dashed] & \mathscr{M}(\mathbb{Z}/\ell \times \mathbb{Z}/\ell) \end{tikzcd}$$

Proof. (a) Note that $\mathscr{M}(\mathbb{Z}/\ell \times \mathbb{Z}/\ell)$ is the same as the moduli stack of elliptic curves with level-ℓ-structures. Let E_z be the underlying elliptic curve of $z \in \mathscr{M}(\mathbb{Z}/\ell \times \mathbb{Z}/\ell)$. As Chen pointed out in [3, §1.2.2], a $G_2[\ell]$-structure on $E_z/\mathrm{Spec}K$ is precisely a principal $G_2[\ell]$-bundle on $\bar{E}_z^\circ$ whose isomorphism class is fixed by $\mathrm{Gal}(\bar{K}/K)$. Hence, to check that whether the given K-rational point z of $\mathscr{M}(\mathbb{Z}/\ell \times \mathbb{Z}/\ell)$ lifts, we are required to check that if there exists a principal $G_2[\ell]$-bundle satisfying the above mentioned condition. The elliptic curve E_z is defined over K, so we can take a nowhere vanishing invariant differential ω_z defined over K. Its dual gives a tangential point v_z on $\bar{E}_z^\circ$ as constructed in Chapter 3. If we consider the Galois $Q_2[\ell]$-covering of $\bar{E}_z^\circ$ associated to $\pi_1^{\text{ét}}(\bar{E}_z^\circ, v_z) \twoheadrightarrow Q_2[\ell]$, we see that it is a principal $G_2[\ell]$-bundle[1] whose isomorphism class is fixed by $\mathrm{Gal}(\bar{K}/K)$ since we know that $\mathrm{Gal}(\bar{K}/K)$ acts trivially on $Q_2[\ell]$ from Theorem 3.4.8. In conclusion, we see that the K-rational point z lifts as claimed in the theorem.

(b) By a similar argument to (a), this follows from Theorem 3.5.2. $\square$

[1]Recall that the abstract group $G_2[\ell]$ is modelled by $Q_2[\ell]$.

Bibliography

[1] A. Beilinson and A. Levin. The elliptic polylogarithm. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 123–190. Amer. Math. Soc., Providence, RI, 1994.

[2] F. Brown. Mixed Tate motives over $\mathbb{Z}$. *Ann. of Math. (2)*, 175(2):949–976, 2012.

[3] W. Y. Chen. Moduli Interpretations for Noncongruence Modular Curves. *arXiv:1510.05687v5 [math.NT]*, October 2015.

[4] J. Coates and M. Kim. Selmer varieties for curves with CM Jacobians. *Kyoto J. Math.*, 50(4):827–852, 2010.

[5] P. Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois groups over* $\mathbf{Q}$ *(Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 79–297. Springer, New York, 1989.

[6] P. Deligne and D. Mumford. The irreducibility of the space of curves of given genus. *Inst. Hautes Études Sci. Publ. Math.*, (36):75–109, 1969.

[7] A. Grothendieck. *Revêtements étales et groupe fondamental. Fasc. I: Exposés 1 à 5*, volume 1960/61 of *Séminaire de Géométrie Algébrique*. Institut des Hautes Études Scientifiques, Paris, 1963.

[8] A. Grothendieck. Brief an G. Faltings. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 49–58. Cambridge Univ. Press, Cambridge, 1997. With an English translation on pages. 285–293.

[9] A. Huber and G. Kings. Degeneration of l-adic Eisenstein classes and of the elliptic polylog. *Invent. Math.*, 135(3):545–594, 1999.

[10] R. Jones and J. Rouse. Galois theory of iterated endomorphisms. *Proc. Lond. Math. Soc. (3)*, 100(3):763–794, 2010. Appendix A by Jeffrey D. Achter.

[11] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[12] M. Kim. The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[13] M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23(3):725–747, 2010.

[14] M. Kim. p-adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication. *Ann. of Math. (2)*, 172(1):751–759, 2010.

[15] H. W. Lenstra. Galois theory for schemes. *http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf*, 2008.

[16] H. Nakamura. Tangential base points and Eisenstein power series. In *Aspects of Galois theory (Gainesville, FL, 1996)*, volume 256 of *London Math. Soc. Lecture Note Ser.*, pages 202–217. Cambridge Univ. Press, Cambridge, 1999.

[17] H. Nakamura. On arithmetic monodromy representations of Eisenstein type in fundamental groups of once punctured elliptic curves. *Publ. Res. Inst. Math. Sci.*, 49(3):413–496, 2013.

[18] M. Pikaart and A. J. de Jong. Moduli of curves with non-abelian level structure. In *The moduli space of curves (Texel Island, 1994)*, volume 129 of *Progr. Math.*, pages 483–509. Birkhäuser Boston, Boston, MA, 1995.

[19] D. Quillen. Rational homotopy theory. *Ann. of Math. (2)*, 90:205–295, 1969.

[20] K. A. Ribet. Dividing rational points on abelian varieties of CM-type. *Compositio Math.*, 33(1):69–74, 1976.

[21] J. P. Serre. *Abelian l-adic representations and elliptic curves.* McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[22] J. P. Serre. *Galois cohomology.* Springer-Verlag, Berlin, 1997. Translated from the French by Patrick Ion and revised by the author.

[23] A. Weil. The field of definition of a variety. *Amer. J. Math.*, 78:509–524, 1956.