University of Nottingham

School of Mathematical Sciences

Anabelian Geometry of Punctured Elliptic Curves

Wojciech Porowski

A thesis submitted to the University of Nottingham for the degree of
Doctor of philosophy

March 2020

To my parents

Abstract

Anabelian geometry of hyperbolic curves has been studied in detail for the last thirty years, culminating in proofs of various versions of Grothendieck Anabelian Conjectures. These results are usually stated as fully faithfulness of a certain functor, which to a hyperbolic curve X associates some type of fundamental group Π_X. Careful inspection of the proofs reveals that in fact quite often we proceed by establishing various reconstruction algorithms, which to a fundamental group Π_X associate some other type of data related to the curve X. In other words, we recover information about the curve X from the topological group Π_X. This algorithmic approach is sometimes called *mono-anabelian*.

In this thesis we concentrate on the special case when the hyperbolic curve X is a smooth and proper curve of genus one over a p-adic local field K with one K-rational point removed i.e., elliptic curve E punctured at the origin. We consider the problem of reconstructing the local height of a rational point on an elliptic curve from the fundamental group Π_X equipped with a section of the absolute Galois group G_K determined by this point. We provide such construction for the full étale fundamental group of X as well as for its maximally geometrically pro-p quotient in the case when the elliptic curve E has potentially good reduction.

Another problem we consider is determining the reduction type of the elliptic curve E from the maximal geometrically pro-p fundamental group of X, equipped with an additional data of the set of discrete tangential sections. Our main result provides such reconstruction when the residue characteristic p is greater than three. Moreover, we study the tempered fundamental group of a Tate curve and prove that a particular torsor of cohomology classes of theta functions admits a natural trivialization, well defined up to a sign, which is compatible with the integral structure coming form the stable model of the Tate curve. Finally, in the last chapter we shift our attention to studying G_K-equivariant automorphisms of various multiplicative submonoids of the monoid $(K^{\mathrm{alg}})^{\times}$ and describe their structure.

Acknowledgements

I am deeply grateful to my advisor Professor Ivan Fesenko for his guidance, motivation and encouragement during the time of my graduate studies, as well as his numerous comments which vastly improved the structure of this thesis.

Moreover, I would like to express my sincere gratitude to Professor Shinichi Mochizuki for many hours of stimulating discussion and sharing with me his insights about anabelian geometry.

I have greatly benefited from various conversations with Yuichiro Hoshi, Emmanuel Lepage and Arata Minamide, to whom I am really thankful.

I would like to thank Weronika Czerniawska, Paolo Dolce, Christopher Hall, Wester van Urk and Raven Waller, for all the time we spent together sharing an office through our PhD studies.

Special thanks go to the organizers and participants of various Number Theory Study Groups in which I participated: Richard Hatton, Andreea Mocanu, Michalis Neururer, Sergey Oblezin, Darya Schedrina, Frederick Strömberg and Chris Wuthrich, for many interesting topics which I learned from them.

Finally, I would like to thank Research Institute of Mathematical Sciences in Kyoto, Japan, for supporting me for six months during my stay in Kyoto, where I finished my thesis.

Last but not least, I would like to acknowledge the constant support of my wife Justyna, without which this work would not have been possible.

Contents

Introduction

This introduction provides a more detailed overview of the topics presented in this thesis. In addition, every chapter starts with its own introduction.

Let K be a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers. Recall that a hyperbolic curve X over K is a smooth variety of dimension one obtained as an open subscheme of a proper smooth curve $\overline{X}$ of genus g such that the reduced divisor $D = \overline{X} \setminus X$ satisfies the inequality $2g - 2 + \deg(D) > 0$. After base changing to some fixed algebraic closure K^{alg} the divisor D becomes a set of r rational points and the above condition translates into $2g - 2 + r > 0$. Consider now the étale fundamental group $\pi_1(X_{K^{\mathrm{alg}}})$ of the curve $X_{K^{\mathrm{alg}}}$. Then, the condition of being hyperbolic given by the previous inequality is equivalent to the property that the group $\pi_1(X_{K^{\mathrm{alg}}})$ is *not* abelian. In fact, when X is hyperbolic and $r > 0$, then the étale fundamental group of $X_{K^{\mathrm{alg}}}$ is a free profinite group on $2g + r - 1$ generators, hence it is, in some sense, very far from being abelian. This is exactly the property expressed by the adjective *anabelian*.

Grothendieck formulated a few conjectures about expected properties of anabelian varieties. For example, let X and Y be two hyperbolic curves over some base field K and consider the map

$$\mathrm{Mor}_K(X, Y) \to \mathrm{Hom}_{G_K}(\pi_1(X), \pi_1(Y)),$$

from the set of dominant K-morphisms $X \to Y$ to the set of open continuous homomorphisms of étale fundamental groups $\pi_1(X) \to \pi_1(Y)$ compatible with surjections to G_K and considered up to conjugation by elements from the geometric fundamental group $\pi_1(Y_{K^{\mathrm{alg}}})$. Then, the Hom-version of relative Grothendieck Conjecture over K says that this map should be a bijection, in other words the functor associating to a hyperbolic curve X its fundamental group $\pi_1(X)$ equipped with the surjection to the absolute Galois group of the base field G_K is fully faithful in appropriate categories. This conjecture was proved by Mochizuki when K is a sub-p-adic field.

We call this result relative since étale fundamental groups are equipped with fixed surjections to the absolute Galois group G_K of the base field and homomorphisms are required to commute with them. On the other hand, one may also consider absolute version of Grothendieck Conjecture by removing this fixed surjection and considering all open continuous group homomorphisms $\pi_1(X) \to \pi_1(Y)$. When K is a number field and we consider only isomorphisms of schemes and fundamental groups, then this relative Isom-version is in fact equivalent to the absolute one due to the Neukirch-Uchida theorem. This theorem says that all open continuous homomorphisms between absolute Galois groups of number fields come from morphisms of underlying fields. However, when K is a p-adic local field, then the absolute Isom-version is indeed more general since the naive extension of the Neukirch-Uchida theorem from number fields to local fields is false. In general, the Absolute Grothendieck Conjecture is still an open problem.

A very common situation appearing in anabelian geometry may be presented in the following form. Suppose that we start from the fundamental group $\pi_1(X)$ of hyperbolic curve, treated as an object in the category of topological groups, and then we try to reconstruct some information related to the geometry of the curve X. This approach is called *mono-anabelian* to emphasize that we start with only one group. On the other hand, we may also start from two topological groups $\pi_1(X) \to \pi_1(Y)$ together with a homomorphism between them and ask whether we may infer some relations between X and Y. This second approach is called *bi-anabelian*.

Then, one can formulate theorems in anabelian geometry using both these approaches. For example, a mono-anabelian version would state that certain property A of the curve X may be determined group theoretically from the topological group $\pi_1(X)$. On the other hand, a bi-anabelian version would say that if we have an isomorphism of topological groups $\pi_1(X) \cong \pi_1(Y)$, then X has the property A if and only if Y has. Hence we see that in general a mono-anabelian results may be considered slightly stronger than their bi-anabelian versions. Therefore, it is usually the case that they are more difficult to obtain. For example, the original proof of the Neukirch-Uchida theorem did not provide a method of reconstructing a number field K from its fundamental group G_K.

In this thesis we study the mono-anabelian geometry of once punctured elliptic curve X over a p-adic local field K. In other words, we are interested in group theoretic reconstructions of properties of the elliptic curve E from various versions of the étale fundamental group $\pi_1(X)$. As we will see, the properties that we are especially interested in are the local height of rational points of E

as well as determining whether the elliptic curve E has good reduction over K.

In Chapter 1 we will consider the following situation. Let E be an elliptic curve over a p-adic local field K and let $\pi_1(X)$ be the étale fundamental group of the hyperbolic curve $X = E \setminus \{O\}$. Then, we have a surjection $\pi_1(X) \twoheadrightarrow G_K$, where G_K is the absolute Galois group of the local field K. Every K-rational point $P \in X(K)$ determines a section $s_P \colon G_K \hookrightarrow \pi_1(X)$ of the surjection $\pi_1(X) \twoheadrightarrow G_K$. Characterizing sections of the form s_P for some K-rational point P among all sections of the above surjection is a difficult open problem. Indeed, description of sections coming from rational points is the content of another anabelian conjecture of Grothendieck, so-called Section Conjecture. On the other hand, assuming that we are given the section s_P, we may try to recover some information about the point P from the section s_P. The main result we prove in Chapter 1 says that in certain cases we may reconstruct the local Néron-Tate height of the point P, from the data of the étale fundamental group $\pi_1(X)$ together with the section s_P.

Theorem 1. *Assume that E has potentially good reduction. Let $\pi_1(X) \twoheadrightarrow G_K$ be the natural surjection and let $s \colon G_K \hookrightarrow \pi_1(X)$ be a section determined by a K-rational point P. Then, one can recover the local Néron-Tate height of the point P from the diagram $G_K \hookrightarrow \pi_1(X) \twoheadrightarrow G_K$ of two homomorphisms of topological groups.*

In fact, one can prove a version of the above theorem also in the case when the point P is an L-rational point, for some finite field extension L/K. Moreover, Chapter 1 also serves as an introduction of basic techniques that we are going to use in Chapters 2 and 3, namely group theoretic Kummer theory and elliptic cuspidalization.

In Chapter 2 we consider a slight variation of the étale fundamental group of X which is called the maximal geometrically pro-p fundamental group, denoted by Π_X. This group classifies all finite étale covers Y of X whose Galois closure $Z \to X$ is a composition of a base change morphism $X_L \to X$, for some finite field extension L/K, and a geometrically connected finite étale cover $Z \to X_L$ of p-power degree. Then, we may ask which properties of the elliptic curve E may be recovered from the group Π_X. For example, we may try to determine whether E has good reduction over K. This question is motivated by the work of Hoshi (see [16]), as well as by the p-adic nonabelian criterion of good reduction of Andreatta, Iovita and Kim (see [4]).

The main difficulty of the problem we consider lies in the fact that various classes of p-adic representations used in p-adic Hodge Theory, e.g., crystalline

or semistable, may not be preserved under the automorphisms of the absolute Galois group G_K of a local field K. This is precisely the reason why results from p-adic Hodge Theory have rather limited applications to problems in absolute anabelian geometry over p-adic local fields. On the other hand, certain facts and theorems can still be used. For example, we will see that the potential type of reduction of E may be group theoretically reconstructed from the fundamental group Π_X, without any assumptions on the residue characteristic p. Moreover, when $p > 2$ and E has potentially good ordinary reduction, then we may in fact determine the reduction type over K. Thus, in Chapter 2 we will be focused mainly on the case of elliptic curves E with potentially good supersingular reduction.

In our main result we consider the group Π_X endowed with certain additional data, namely the set of all discrete tangential sections. These sections do not come from rational points of the curve X, rather they are associated to cotangent vectors at the unique cusp of X. Then, we prove that if we further restrict the residue characteristic of the base field K, then we may determine the reduction type of E from this augmented data.

Theorem 2. *Assume that the residue characteristic p is at least five. Then, from the topological group Π_X equipped with the set of all discrete tangential sections, we may recover the reduction type of the elliptic curve E.*

Moreover, in the last section we consider a pro-p version of the main theorem of Chapter 1, reconstructing local height of a rational point from the corresponding section of the surjection $\Pi_X \twoheadrightarrow G_K$. Let P be a nonzero K-rational point on the elliptic curve E. Hence, the point P determines a section $s_P \colon G_K \hookrightarrow \Pi_X$ of the surjection $\Pi_X \twoheadrightarrow G_K$. Then, the strongest result we are currently able to prove is the following theorem.

Theorem 3. *Assume that the elliptic curve E has potentially good reduction. Then, we can determine group theoretically from the diagram $G_K \hookrightarrow \Pi_X \twoheadrightarrow G_K$ whether the local height of the rational point P is equal to zero. Moreover, if we assume additionally that we are given the canonical rigidity isomorphism*

$$M_X^{(p)} \cong \mathbb{Z}_p(G_K),$$

then we may in fact reconstruct the local height of the point P.

The canonical rigidity isomorphism $M_X^{(p)} \cong \mathbb{Z}_p(G_K)$ used in the statement will be defined in Section 2.6. It is likely that the two previous results could be strengthened. For example, the author hopes that the rigidity isomorphism

mentioned in the statement of the previous theorem can be in fact reconstructed from the topological group Π_X, which would allow us to remove it from the assumptions. Similarly, one may investigate whether the set of discrete tangential sections may be reconstructed group theoretically. These two questions are closely related and require further study.

In Chapter 3 we use another type of fundamental group of the hyperbolic curve X called the tempered fundamental group Π_X^{tp}, introduced by André in [3]. This group in not profinite in general, as it classifies not only finite étale covers but also some infinite analytic covers. We consider the case when E is a Tate curve with Tate parameter $q \in K^\times$ and analyse cohomology class of certain analytic theta function $\ddot{\Theta}$ on an infinite analytic cover $\ddot{Y}$ of X, introduced by Mochizuki in [29]. This function is given by the formula

$$\ddot{\Theta}(\ddot{U}) = \ddot{U} \prod_{n\geq 0}(1 - q^n\ddot{U}^2) \prod_{n>0}(1 - q^n\ddot{U}^{-2}).$$

One can prove that the $\mathcal{O}_K^\times$-torsor of multiples of Kummer classes of Θ may be reconstructed group theoretically from the topological group Π_X^{tp}. The result we prove is that this $\mathcal{O}_K^\times$-torsor admits a group theoretic trivialization, well defined up to a sign.

Theorem 4. *Assume that K contains all 12th roots of unity as well as coordinates of all 2-torsion points. Then, there exists a group theoretic construction of a trivialization of the $\mathcal{O}_K^\times$-torsor of multiples of theta function Θ, well defined up to a sign. Moreover, this trivialization is constructed by evaluating theta function at a lift of a certain 6th torsion point.*

This construction slightly improves some results from [29] and positively answers the question asked in 2016 at IUT summit organized at RIMS, Kyoto, about extending the theory of [29] to local fields with even residue characteristic.

Finally, in the last section of Chapter 3, we come back to discussing the reconstruction of the local height of a rational point on a Tate curve from its section, this time using the tempered fundamental group Π_X^{tp}. We consider section $s_P\colon G_K \hookrightarrow \Pi_X^{\mathrm{tp}}$ of the surjection $\Pi_X^{\mathrm{tp}} \twoheadrightarrow G_K$ coming from a nonzero rational point P of the elliptic curve E. Then, we prove the following theorem

Theorem 5. *Assume that E is a Tate curve. Then, there exists a group theoretic reconstruction of the local height of the point P from the diagram $G_K \hookrightarrow \Pi_X^{\mathrm{tp}} \twoheadrightarrow G_K$ of topological groups.*

This theorem may be considered as a complement to analogous results we obtain in Chapters 1 and 2 regarding the problem of reconstructing the local height.

Chapter 4 is the last part of this thesis and is essentially independent of the first three chapters. Let us first provide some motivation for the results of we are going to state. Fix an algebraic closure K^{alg} of the p-adic local field K and let $G_K = \mathrm{Gal}(K^{\mathrm{alg}}/K)$ be the absolute Galois group of K. We write $G_K \curvearrowright K^{\mathrm{alg}}$ for the pair of the topological group G_K acting on the field K^{alg}. Consider now the group of automorphisms $\mathrm{Aut}(G_K \curvearrowright K^{\mathrm{alg}})$ of this pair, which consists of a group automorphism of G_K and a field automorphism of K^{alg}. It is easy to check that every such automorphism must be in fact inner. Thus, the image of the restriction map

$$\mathrm{Aut}(G_K \curvearrowright K^{\mathrm{alg}}) \to \mathrm{Aut}(G_K) \tag{1}$$

is equal to the group of inner automorphisms of G_K, moreover the map is injective since the group G_K has trivial center. Therefore, since the group G_K admits automorphisms which are not inner, the restriction map (1) is not surjective.

Consider now a multiplicative monoid $\mathcal{O}^{\triangleright}_{K^{\mathrm{alg}}} = \mathcal{O}^{\times}_{K^{\mathrm{alg}}} \setminus \{0\}$ of nonzero integral elements of the field K^{alg}. Similarly as before we may consider the group $\mathrm{Aut}(G_K \curvearrowright \mathcal{O}^{\triangleright}_{K^{\mathrm{alg}}})$ of automorphisms of the pair of a group acting on a monoid. Then, it is proved in [30] that the restriction map

$$\mathrm{Aut}(G_K \curvearrowright \mathcal{O}^{\triangleright}_{K^{\mathrm{alg}}}) \to \mathrm{Aut}(G_K)$$

is in fact a bijection. In other words, when we consider only multiplicative structure of K^{alg}, then it is possible to lift every automorphism of the group G_K to an automorphism of a pair. As we have seen, this is not true if we want to respect both multiplicative and additive structure of K^{alg}.

Motivated by this results, we consider the following situation: let L/K be a Galois extension of K with the Galois group G, and let $\mathcal{O}^{\triangleright}_L = \mathcal{O}_L \setminus \{0\}$ be the multiplicative monoid of nonzero integral elements of the field L. As previously, we have the restriction map

$$\mathrm{Aut}(G \curvearrowright \mathcal{O}^{\triangleright}_L) \to \mathrm{Aut}(G), \tag{2}$$

which in general may not be injective. The question to determine Galois field extensions L/K for which the map (2) is an isomorphism was asked to Prof. Fesenko by Prof. Mochizuki.

Our main focus is to analyse the kernel of this map, which is equal to the group $\mathrm{Aut}_G(\mathcal{O}^{\triangleright}_L)$ of G-equivariant automorphisms of the monoid $\mathcal{O}^{\triangleright}_L$. We also introduce the group $\mathrm{Aut}_G(\mathcal{O}^{\times}_L)$ of G-equivariant automorphisms of the group of

units $\mathcal{O}_L^\times$. To state our main result, denote by $V_L = \mathcal{O}_L^\triangleright/\mathcal{O}_L^\times$ the value monoid of L. Moreover, let $V(L/K) = \varprojlim_M \mathbb{Z}/e(M/K)\mathbb{Z}$, where M runs through all finite subextensions of L/K and $e(M/K)$ is the ramification degree of a field extension M/K. We prove that they form a part of the following exact sequence.

Theorem 6. *Let L/K be a Galois field extension with the Galois group G. Then, there exists an exact sequence of group homomorphisms*

$$1 \to \mathrm{Hom}(V_L, \mathcal{O}_K^\times) \to \mathrm{Aut}_G(\mathcal{O}_L^\triangleright) \to \mathrm{Aut}_G(\mathcal{O}_L^\times) \to V(L/K)^\times \to 1.$$

Using this result, we give a few examples of field extensions L/K when the restriction map (2) is not injective. On the other hand, the question whether there exists a non algebraically closed field extension L/K such that the map (2) is injective remains open. Finally, in the last section of Chapter 4 we discuss briefly the issue of surjectivity of the restriction map.

We use standard notation $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Q}_p$ for sets of integers, rational numbers, real numbers and p-adic numbers. Furthermore, we denote the set of prime numbers by $\mathbb{P}$. The only type of base field K we use in this thesis is a finite extension of $\mathbb{Q}_p$, therefore we will simply say that K is a local field, or p-adic local if we want to indicate the residue characteristic p.

Chapter 1

Anabelian construction of local height

1.1 Introduction

Let E be an elliptic curve of over the field K which is a finite extension of the p-adic field $\mathbb{Q}_p$. Let X be the hyperbolic curve obtained by removing from E a K-rational point given by the origin O of the elliptic curve E. Thus, X is an affine curve over K.

Consider the étale fundamental group $\pi_1(X)$ of X. We do not specify base-points for various fundamental groups of curves as we will only consider them as abstract topological groups. Then, one has the following short exact sequence

$$1 \to \pi_1(X_{K^{\mathrm{alg}}}) \to \pi_1(X) \to G_K \to 1, \tag{1.1}$$

where G_K is the absolute Galois group of the local field K. For a finite field extension L/K, every L-rational point S of X determines a section $s : G_L \to \pi_1(X)$ over the open subgroup $G_L \subset G_K$ of the surjection $\pi_1(X) \twoheadrightarrow G_K$. Hence we have a commutative diagram

$$\begin{array}{ccc} & & G_L \\ & \overset{s}{\swarrow} & \big\downarrow \\ \pi_1(X) & \longrightarrow\!\!\!\!\!\rightarrow & G_K. \end{array} \tag{1.2}$$

Then, the result we are going to prove is the following theorem.

Theorem 1.1.1. *Assume that E has potentially good reduction. Let $\pi_1(X) \twoheadrightarrow G_K$ be the natural surjection and let $s\colon G_L \hookrightarrow \pi_1(X)$ a splitting over an open subgroup determined by an L-rational point S. Then, one can recover the local Néron-Tate height of the point S from the diagram* (1.2)*, i.e., from the data of two homomorphisms of topological groups.*

We recall the notion of the Néron-Tate local height of a rational point in the next section. Moreover, in the following by "recovering" certain data we will mean the description of an appropriate group theoretic algorithmic construction which determines the data under consideration.

For elliptic curves over a number field there is a notion of the global Néron-Tate height, which is in fact an appropriate sum of local heights. Then, one can consider analogous statement as in Theorem 1.1.1 replacing the field K by a number field. In this case, it is known that one can reconstruct the global height of a rational point from its corresponding section. In fact, one has a much stronger result of Mochizuki (see [30], Theorem 1.9) which essentially says that the whole curve X can be reconstructed from the topological group $\pi_1(X)$.

Moreover, a similar result is known also in the case where K is a p-adic local field, see [28], Corollary 3.8 and Remark 3.8.1, together with [30], Appendix, (CM5). Although the result of [28] is stated in a bi-anabelian fashion, in fact the content of the proof is entirely mono-anabelian. On the other hand, the method which we use in this chapter may be adapted to the maximal geometrically pro-p étale fundamental group which we consider in Chapter 2.

The structure of this chapter is as follows: in Section 1.2 we recall the definition of the local height; in Sections 1.3 and 1.4 we recall basic properties of absolute Galois groups of local fields and étale fundamental groups of hyperbolic curves over local fields; in Sections 1.5 to 1.7 we present a few results of Mochizuki considering the anabelian constructions of Kummer classes and elliptic cuspidalizations; finally in Section 1.8 we use these results to prove Theorem 1.1.1.

1.2 Néron-Tate local height function

In this section we briefly recall the definition and some properties of the local height function. Let K be a p-adic local field and let $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ be a multiplicative valuation which we uniquely extend to some fixed algebraic closure K^{alg} of K. For $x \in K^{\mathrm{alg}}$, we define $v(x) = -\log|x|$, hence v is an additive valuation on K^{alg} with $v(x) \geq 0$ if and only if x is an integral element of K^{alg}. It will be convenient to use two different normalizations of this additive valuation. We will write $v_K\colon K \to \mathbb{Z}$ for the additive valuation such that $v_K(\pi_K) = 1$, where π_K is a uniformizer of K. Moreover, we will write $v\colon K^{\mathrm{alg}} \to \mathbb{Q}$ for the additive valuation satisfying $v(p) = 1$. Then, it is clear that we have $v_K = ev$, where e is the ramification degree of the field extension $K/\mathbb{Q}_p$.

Consider an elliptic curve E over K and choose a Weierstrass equation of E

$$y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_2x + a_6. \tag{1.3}$$

Then, we have the following classical theorem, see [37], Chapter VI, Theorem 1.1.

Theorem 1.2.1. *There exists a unique function*

$$\lambda\colon E(K) \setminus \{O\} \to \mathbb{R}$$

satisfying the following properties:

1. *λ is continuous and is bounded on the complement of every v-adic neighbourhood of O.*

2. *The limit*

$$\lim_{P \to O} (\lambda(P) + \tfrac{1}{2}v(x(P)))$$

   exists.

3. *For all $P \in E(K)$ with $2P \neq O$,*

$$\lambda(2P) = 4\lambda(P) + v((2y + a_1x + a_3)(P)) - \tfrac{1}{4}v(\Delta).$$

Moreover, the function λ is independent on the choice of a Weierstrass equation representing E and is invariant under field extensions.

The function constructed in the above theorem is called the local Néron-Tate height function. In this chapter we are especially interested in the case when E has good reduction. Then, we have a more explicit formula (see [37], Chapter VI, Theorem 4.1).

Proposition 1.2.2. *Suppose that E has good reduction over K and let*

$$y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_2x + a_6$$

be a minimal Weierstrass equation of E. Then, the local height is given by the formula

$$\lambda(P) = \tfrac{1}{2}\max\{-v(x(P)), 0\}.$$

In particular, if $v(x(P)) \geq 0$, then the local height $\lambda(P)$ is equal to zero. Therefore, in the case of good reduction, one can think informally of the function λ as measuring the size of the denominator of $x(P)$.

We also discuss the explicit formula in the case of bad reduction, as it will be needed in Chapter 2. First, we introduce some notation. For $q \in K^\times$ with $|q| < 1$, denote by E_q the Tate curve corresponding to the parameter q (see [37], V, §3). Then, we have a Galois equivariant isomorphism $(K^{\mathrm{alg}})^\times/q^{\mathbb{Z}} \cong E_q(K^{\mathrm{alg}})$ as well as an isomorphism $K^\times/q^{\mathbb{Z}} \cong E_q(K)$. Every split multiplicative elliptic curve over K is K-isomorphic to a unique Tate curve E_q for some $q \in K^\times$.

We also introduce the following infinite product

$$\theta(u) = (1-u)\prod_{n\geq 1}(1-q^n u)(1-q^n u^{-1}).$$

The series $\theta(u)$ is convergent for all $u \in (K^{\mathrm{alg}})^\times$ and satisfies the functional equation

$$\theta(qu) = -u^{-1}\theta(u).$$

Finally, denote by $B_2(T)$ the polynomial $T^2 - T + \frac{1}{6}$. In the next proposition we identify $E(K)$ with $K^\times/q^{\mathbb{Z}}$ using Tate parametrization and we consider the local height function as a function defined on the group $K^\times/q^{\mathbb{Z}}$.

Proposition 1.2.3. *Suppose that E has split multiplicative reduction and let $E \cong E_q$ for $q \in K^\times$. Then, the local height function $\lambda\colon K^\times/q^{\mathbb{Z}} \to \mathbb{R}$ at the point $\bar{u} \in K^\times/q^{\mathbb{Z}}$ is given by the formula*

$$\lambda(\bar{u}) = \tfrac{1}{2}B_2\left(\frac{v(u)}{v(q)}\right)v(q) + v(\theta(u)),$$

where $u \in K^\times$ is a lift of $\bar{u}$. The value $\lambda(\bar{u})$ is independent of the choice of this lift.

In fact, in what follows, we will not need the definition of the local height given in Theorem 1.2.1, as will only use the explicit formula recalled above in the case of good and split multiplicative reduction. Moreover, for future reference, we recall the following simple lemma.

Lemma 1.2.4. *Assume that E has good reduction over K and fix a minimal Weierstrass equation* (1.3) *of E. For a natural number n, define the function*

$$F_n = n^2 \prod_{T\in E[n]\setminus\{O\}}(x - x(T)).$$

Then, we have the following formula

$$\lambda(nP) = n^2\lambda(P) + \frac{1}{2}v(F_n(P)),$$

for every K-rational point P with $nP \neq O$.

Proof. See [37], Chapter VI, Exercise 6.4.(e). □

1.3 Absolute Galois group of a local field

Here we recall a few basic facts concerning the absolute Galois group of a local field of characteristic zero that are important from the point of view of anabelian geometry. All the statements in this section are well known, see, e.g., [34] or [13].

First we need to introduce some notation. Let $\Sigma \subset \mathbb{P}$ be a nonempty set of prime numbers. We say that a natural number n is a Σ-*integer* if all of its prime divisors are contained in Σ. We denote the set of Σ-integers by $\mathbb{N}(\Sigma)$. Let A be an abelian group. We define its Σ-*completion* by the formula

$$\widehat{A}^{\Sigma} = \varprojlim_{n \in \mathbb{N}(\Sigma)} A/nA.$$

When the set Σ is equal to the set of all prime numbers we simply write $\widehat{A}$.

Let K be a finite extension of $\mathbb{Q}_p$ and denote by e and d the absolute ramification index of K and the degree of the field extension $K/\mathbb{Q}_p$, respectively. Moreover, let k be the residue field of K and denote by $q = p^f$ its cardinality. The absolute Galois group G_K of K fits in the short exact sequence

$$1 \to I_K \to G_K \to \widehat{\mathbb{Z}} \to 1,$$

where I_K is the inertia subgroup. The quotient $G_K/I_K \cong \widehat{\mathbb{Z}}$ corresponds to the maximal unramified extension K^{ur} of the local field K and has the canonical generator given by the Frobenius element. The inertia group I_K has a unique normal pro-p Sylow subgroup I_K^{wild} called the wild inertia subgroup and the quotient

$$1 \to I_K^{\mathrm{wild}} \to I_K \to I_K^{\mathrm{tm}} \to 1$$

is called the tame inertia group. By pushing out the quotient $I_K \twoheadrightarrow I_K^{\mathrm{tm}}$ we obtain a quotient $G_K \twoheadrightarrow G_K^{\mathrm{tm}}$ and the Galois field extension corresponding to this quotient is the maximal tamely ramified extension K^{tm} of K.

Let $\mu_n \subset (K^{\mathrm{alg}})^{\times}$ be the subgroup of nth roots of unity. Consider the projective system of G_K-modules μ_n indexed by natural numbers n, where the morphisms $\mu_{mn} \to \mu_n$ in this system are given by raising to the mth power for all natural numbers m, n. Define $\widehat{\mathbb{Z}}(\mu) = \varprojlim \mu_n$ be the limit of this projective system over all natural numbers n. Here we diverge from the standard notation $\widehat{\mathbb{Z}}(1)$ to emphasise the construction of $\widehat{\mathbb{Z}}(\mu)$ from the group of roots of unity. Thus, in the following by $\widehat{\mathbb{Z}}(1)$ we will mean a free $\widehat{\mathbb{Z}}$-module of rank one with a fixed generator $1 \in \widehat{\mathbb{Z}}(1)$, equipped with an action of G_K given by the cyclotomic character. Therefore, the module $\widehat{\mathbb{Z}}(\mu)$ is a G_K-module isomorphic

(noncanonically) to the G_K-module $\widehat{\mathbb{Z}}(1)$. Similarly, by taking limit over all natural numbers n which are Σ-integers we obtain

$$\widehat{\mathbb{Z}}^{\Sigma}(\mu) = \varprojlim_{n \in \mathbb{N}(\Sigma)} \mu_n.$$

When $\Sigma = \mathbb{P} \setminus \{p\}$, we will write $\widehat{\mathbb{Z}}^{(p')}(\mu)$ for simplicity, which is a Galois module isomorphic (again noncanonically) to the module $\widehat{\mathbb{Z}}^{(p')}(1) = \prod_{l \neq p} \mathbb{Z}_l(1)$. Then, it is well known that the tame inertia group I_K^{tm} is canonically isomorphic to the group $\widehat{\mathbb{Z}}^{(p')}(\mu)$, in particular it is an abelian group. In fact, this is an isomorphism of $\mathrm{Gal}(K^{\mathrm{ur}}/K)$-modules, where the action of $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ on I_K is obtained by lifting the Frobenius element to the group G_K and acting by conjugation on the inertia group I_K. This action descends to an action on the quotient I_K^{tm}, which is independent of the choice of the lift since the group I_K^{tm} is abelian.

Let $G_K \twoheadrightarrow G_K^{\mathrm{ab}}$ be the abelianization map and denote the images of I_K and I_K^{wild} in G_K^{ab} with the upper index a. Therefore we have the exact sequence

$$1 \to I_K^a \to G_K^{\mathrm{ab}} \to \widehat{\mathbb{Z}} \to 1,$$

as well as the sequence

$$1 \to I_K^{a,\mathrm{wild}} \to I_K^a \to I_K^{a,\mathrm{tm}} \to 1,$$

where $I_K^{a,\mathrm{tm}}$ is defined to make the last sequence exact. The filtration

$$I_K^{a,\mathrm{wild}} \subset I_K^a \subset G_K^{\mathrm{ab}}$$

is closely related to the filtration $U_K \subset \mathcal{O}_K^{\times} \subset K^{\times}$, where U_K is the subgroup of principal units, via the reciprocity map $\kappa\colon K^{\times} \to G_K^{\mathrm{ab}}$ from the local class field theory. Indeed, recall that κ is an injection with dense image which induces isomorphisms $\mathcal{O}_K^{\times} \cong I_K^a$ and $U_K \cong I_K^{a,\mathrm{wild}}$. Moreover, the induced injection

$$\mathbb{Z} = K^{\times}/\mathcal{O}_K^{\times} \hookrightarrow G_K^{\mathrm{ab}}/I_K^a \cong \widehat{\mathbb{Z}}$$

maps the canonical generator $1 \in \mathbb{Z}$ to the Frobenius element.

Using the results recalled above we may prove the following well-known fact.

Proposition 1.3.1. *The subgroups I_K and I_K^{wild} of the group G_K, together with the natural numbers d, e, f and p, may be reconstructed group theoretically from the topological group G_K. Moreover, we may also reconstruct the canonical generator of the quotient G_K/I_K determined by the Frobenius element.*

Proof. For every prime number we consider the (finite) dimension

$$d_l = \dim_{\mathbb{Q}_l} G_K^{\mathrm{ab}} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l.$$

Because the group U_K is a pro-p group we easily see that $d_l = 1$ for $l \neq p$. On the other hand, since the p-adic logarithm determines an isomorphism of the open subgroup of U_K with the group $\mathbb{Z}_p^d$, we obtain $d_p = d + 1$. Thus, we may recover the residue characteristic p as the unique prime number l such that $d_l > 1$. Then, since the prime to p torsion in G_K^{ab} has the cardinality $q - 1$, we may easily recover the degree f of the residue field extension $k/\mathbb{F}_p$. Finally, we can determine the degree d simply as $d_p - 1$ and then the ramification degree as $e = d/f$.

We now apply the same method to every open normal subgroup $H \subset G$. If the subgroup H corresponds to the Galois field extension L/K, then we may determine the relative degrees $d(L/K), e(L/K)$ and $f(L/K)$ as quotients of the corresponding absolute degrees. In particular, we may characterise all the open subgroups $H \subset G$ such that the corresponding field extension is unramified. Then, the inertia subgroup I_K may be determined as the intersection of all open subgroups corresponding to unramified extensions. Similarly, the group I_K^{wild} can be determined by considering open subgroups H corresponding to tamely ramified extensions (or as the unique p-Sylow subgroup of I_K).

Consider now the action of $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ on the group I_K^{tm}. From the isomorphism $I_K^{\mathrm{ur}} \cong \widehat{\mathbb{Z}}^{(p')}(\mu)$ recalled above we see that the Frobenius element is the unique element of $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ which acts as the multiplication by q on the group I_K^{tm} (written additively). □

Therefore, from the topological group G_K, one can naturally reconstruct the Galois module $K^\times$ as the preimage of the subgroup $\mathbb{Z} \subset \widehat{\mathbb{Z}}$, generated by the Frobenius element, along the surjection $G_K \twoheadrightarrow \widehat{\mathbb{Z}}$. Moreover, from well-known functorial properties of the residue map in the local class field theory, for every finite field extension L/K the inclusion $K^\times \subset L^\times$ corresponds to the transfer morphism $G_K^{\mathrm{ab}} \to G_L^{\mathrm{ab}}$. By taking the colimit over all open subgroups $G_L \subset G_K$ with connecting homomorphisms given by the transfer map we obtain a group theoretic reconstruction of the Galois module $(K^{\mathrm{alg}})^\times$. We will denote this G_K-module by $K^{\mathrm{alg}}(G_K)^\times$ to emphasise the group theoretic construction implicit in its definition. In particular, by considering the torsion subgroup we recover subgroups corresponding to the groups of nth roots of unity, which we similarly denote by $\mu_n(G_K)$. Finally, by taking the limit of the Galois modules $\mu_n(G_K)$ with connecting homomorphisms given by raising to an appropriate power we

obtain the Galois module

$$\widehat{\mathbb{Z}}(G_K) = \varprojlim_{n\in\mathbb{N}} \mu_n(G_K),$$

noncanonically isomorphic to the module $\widehat{\mathbb{Z}}(1)$. Similarly, for every nonempty subset Σ of the set of prime numbers we may define the G_K-module

$$\widehat{\mathbb{Z}}^{\Sigma}(G_K) = \varprojlim_{n\in\mathbb{N}(\Sigma)} \mu_n(G_K)$$

which is noncanonically isomorphic to the module $\widehat{\mathbb{Z}}^{\Sigma}(1)$.

Consider now the Kummer sequence associated to the group theoretical G_K-module $K^{\mathrm{alg}}(G_K)^{\times}$

$$1 \to \mu_n(G_K) \to K^{\mathrm{alg}}(G_K)^{\times} \to K^{\mathrm{alg}}(G_K)^{\times} \to 1,$$

which induces, by the Hilbert's Satz 90 (see [34], Theorem 6.2.1), the isomorphism

$$K(G_K)^{\times}/K(G_K)^{\times n} \cong H^1(G_K, \mu_n(G)),$$

where by $K(G_K)^{\times}$ we simply mean the group of G_K-invariants of the G_K-module $K^{\mathrm{alg}}(G_K)^{\times}$. Since the inclusion $K(G_K)^{\times} \hookrightarrow G^{\mathrm{ab}}$ induces an isomorphism

$$K(G_K)^{\times}/K(G_K)^{\times n} \cong G_K^{\mathrm{ab}}/(G_K^{\mathrm{ab}})^n,$$

we get the canonical isomorphism

$$G_K^{\mathrm{ab}}/(G_K^{\mathrm{ab}})^n \cong H^1(G_K, \mu_n(G)).$$

By taking the limit over all natural numbers n, we construct a group theoretical isomorphism

$$G_K^{\mathrm{ab}} \cong H^1(G_K, \widehat{\mathbb{Z}}(G_K)). \tag{1.4}$$

This isomorphism is a group theoretic analogue of the classical Kummer isomorphism

$$\widehat{K^{\times}} \cong H^1(G_K, \widehat{\mathbb{Z}}(\mu))$$

Here by $\widehat{K^{\times}}$ we mean the limit $\varprojlim K^{\times}/K^{\times n}$ with respect to the natural quotient homomorphisms. In particular, by composing the isomorphism (1.4) with the surjection $G_K^{\mathrm{ab}} \twoheadrightarrow \widehat{\mathbb{Z}}$, we obtain the homomorphism

$$H^1(G_K, \widehat{\mathbb{Z}}(G_K)) \twoheadrightarrow \widehat{\mathbb{Z}}. \tag{1.5}$$

Then, it follows immediately from the construction that the composition of the isomorphism $\widehat{\mathbb{Z}}(\mu) \cong \widehat{\mathbb{Z}}(G_K)$, induced by the residue homomorphism κ, with

the isomorphism $\widehat{K^\times} \cong H^1(G_K, \widehat{\mathbb{Z}}(\mu))$ gives rise to the following commutative diagram

$$\begin{array}{ccccc} \widehat{K^\times} & \xrightarrow{\simeq} & H^1(G_K, \widehat{\mathbb{Z}}(\mu)) \cong H^1(G_K, \widehat{\mathbb{Z}}(G_K)) & \twoheadrightarrow & \widehat{\mathbb{Z}} \\ \uparrow & & & & \uparrow \\ K^\times & & \twoheadrightarrow & & \mathbb{Z} \end{array}$$

where the bottom horizontal map is simply the additive valuation $K^\times \twoheadrightarrow \mathbb{Z}$. Therefore, the group homomorphism (1.5) may be thought of as a group theoretic profinite valuation map.

In the similar manner, we have a pro-Σ version of the valuation homomorphism

$$H^1(G_K, \widehat{\mathbb{Z}}^\Sigma(G_K)) \twoheadrightarrow \widehat{\mathbb{Z}}^\Sigma, \tag{1.6}$$

which has analogous compatibility property induced by the canonical isomorphism $\widehat{\mathbb{Z}}^\Sigma(G_K) \cong \widehat{\mathbb{Z}}^\Sigma(\mu)$.

Remark 1.3.2. When we use group cohomology of a profinite group G with coefficients in a topological G-module A we always mean the continuous group cohomology $H^i(G, A) = H^i_{cts}(G, A)$, as defined for example in [34]. We need to relate this group cohomology to the group cohomology with discrete coefficient groups. Assume that A is (topologically) isomorphic to the limit $\varprojlim A_n$, where every G-module A_n is a finite group with discrete topology. Moreover, suppose that for every natural number n the cohomology groups $H^{i-1}(G, A_n)$ are finite. Then, we have the natural isomorphism $H^i(G, A) \cong \varprojlim H^i(G, A_n)$. For a proof, see [34], Corollary 2.7.6. The finiteness assumption from this statement will be satisfied in all our applications.

Remark 1.3.3. Proposition 1.3.1 can also be found in [17], Lemma 1.3. Here we remark that in general it is not possible to recover the additive structure on the set $K^{\mathrm{alg}}(G_K)^\times \cup \{0\}$, together with the multiplicative structure on $K^{\mathrm{alg}}(G_K)^\times$ corresponding to the field structure on K^{alg}. Indeed, it follows from the fact that there exist two nonisomorphic local fields K_1 and K_2 such that their absolute Galois groups G_{K_1} and G_{K_2} are isomorphic as topological groups (see [34], remark preceding Theorem 12.2.7).

1.4 Fundamental group of a hyperbolic curve

In this section we recall basic properties of fundamental groups of hyperbolic curves together with group theoretic characterization of the geometric fundamental group and inertia subgroups associated to cusps. The reference for the notion of the étale fundamental group is [1].

Let X by a smooth separated geometrically connected curve over a p-adic local field K. Moreover, let $X \subset \overline{X}$ be the unique smooth compactification of the curve X. Denote by g be the genus of $\overline{X}$ and by r the cardinality of the finite set $\overline{X}_{K^{\mathrm{alg}}} \setminus X_{K^{\mathrm{alg}}}$. We will then say that the curve X is *hyperbolic* if $2g + r - 2 > 0$, moreover the curve X is hyperbolic *of type* (g, r) if X is hyperbolic and the numbers g and r are defined as above. Every point lying in the complement of the curve X inside the compactification $\overline{X}$ will be referred as a *cusp*. Therefore, the number r is equal to the number of geometric cusps. We emphasise the possibly confusing point that with this terminology all cusps are in fact smooth points.

Denote by $\pi_1(X)$ the étale fundamental group of X and by $\pi_1(X_{K^{\mathrm{alg}}})$ the étale fundamental group of $X_{K^{\mathrm{alg}}}$. Then, the morphisms of schemes $X \to \operatorname{Spec} K$ and $X_{K^{\mathrm{alg}}} \to X$ induce the homomorphisms of fundamental groups $\pi_1(X) \to G_K$ and $\pi_1(X_{K^{\mathrm{alg}}}) \to \Pi_X$, which give rise to the following short exact sequence of fundamental groups

$$1 \to \pi_1(X_{K^{\mathrm{alg}}}) \to \pi_1(X) \to G_K \to 1.$$

This exact sequence induces naturally the outer representation

$$G_K \to \mathrm{Out}(\pi_1(X_{K^{\mathrm{alg}}})).$$

It is constructed by lifting an element $\sigma \in G_K$ to an element $\tilde{\sigma} \in \pi_1(X)$ and considering the automorphism of $\pi_1(X_{K^{\mathrm{alg}}})$ induced by the conjugation $\tau \mapsto \tilde{\sigma}\tau\tilde{\sigma}^{-1}$ for $\tau \in \pi_1(X_{K^{\mathrm{alg}}})$. The dependence on the choice of lifting vanishes after taking the quotient $\mathrm{Aut}(\pi_1(X_{K^{\mathrm{alg}}})) \twoheadrightarrow \mathrm{Out}(\pi_1(X_{K^{\mathrm{alg}}}))$.

There is a well-known group theoretic presentation of the profinite group $\pi_1(X_{K^{\mathrm{alg}}})$. First, for every nonnegative integers g, r we define the following discrete group

$$\Gamma(g, n) = \langle a_1, b_1, \ldots, a_g, b_g, c_1, \ldots, c_r \mid [a_1, b_1] \ldots [a_g, b_g] c_1 \ldots c_r = 1 \rangle,$$

which is a quotient of a free group on $2g + r$ letters by one relation. The group $\Gamma(g, n)$ is isomorphic to the topological fundamental group of the Riemann surface $X(\mathbb{C})$ of genus g punctured at r points. The elements a_i and b_i correspond to the standard loops on the compactification $\overline{X}(\mathbb{C})$ of $X(\mathbb{C})$ generating the first singular homology, whereas the elements c_i correspond to the loops around the points on the boundary. Let $\Gamma^{\wedge}(g, n)$ be the profinite completion of $\Gamma(g, n)$, more explicitly $\Gamma^{\wedge}(g, n) = \varprojlim \Gamma(g, n)/N$ where the inverse limit runs through all normal subgroups N of finite index. Then, the geometric étale fundamental group $\pi_1(X_{K^{\mathrm{alg}}})$ is noncanonically isomorphic to the profinite group $\Gamma^{\wedge}(g, r)$,

where g and r are equal to the genus and the number of cusps of X. This is true over every algebraically closed field of characteristic zero. For a proof, see [1], Exposé X. It uses specialization theorems to reduce to the case over the complex numbers where one can use topological methods.

We need to introduce a pro-Σ version of the fundamental group of a hyperbolic curve X. Let Σ be fixed nonempty subset of the set of prime numbers. Denote by $\pi_1(X_{K^{\mathrm{alg}}}) \twoheadrightarrow \Delta_X$ the maximal pro-Σ quotient of the geometric fundamental group $\pi_1(X_{K^{\mathrm{alg}}})$. It is defined as the inverse limit of all finite discrete quotients $\pi_1(X_{K^{\mathrm{alg}}}) \twoheadrightarrow Q$ whose orders are Σ-integers. Thus, this quotient classifies all finite étale covers of $X_{K^{\mathrm{alg}}}$ whose degree is a Σ-integer. Moreover, we define the maximal geometrically pro-Σ fundamental group of X to be the topological group Π_X fitting the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(X_{K^{\mathrm{alg}}}) & \longrightarrow & \pi_1(X) & \twoheadrightarrow & G_K & \longrightarrow & 1 \\ & & \downarrow\!\!\downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \Delta_X & \longrightarrow & \Pi_X & \longrightarrow & G_K & \longrightarrow & 1. \end{array}$$

From now on, we fix a nonempty subset Σ as above and we consider the topological groups Δ_X and Π_X.

We need to describe the Galois module structure of the abelian group Δ_X^{ab}. The quotient $\Delta_X \twoheadrightarrow \Delta_X^{\mathrm{ab}}$ induces a homomorphism $\mathrm{Out}(\Delta_X) \to \mathrm{Aut}(\Delta_X^{\mathrm{ab}})$, therefore we have a well defined action of G_K on the abelianization Δ_X^{ab}. Let now J be the Jacobian variety of $\overline{X}$ and denote by $J[n]$ be the kernel of the multiplication by n isogeny $[n]\colon J \to J$. Define the (pro-Σ) Tate module $T^{\Sigma}(J)$ of J by the usual formula

$$T^{\Sigma}(J) = \varprojlim_{n \in \mathbb{N}(\Sigma)} J[n](K^{\mathrm{alg}}),$$

where the map $J[mn](K^{\mathrm{alg}}) \to J[n](K^{\mathrm{alg}})$ in this projective system is defined as multiplication by m. Then $T^{\Sigma}(J)$ is a free $\widehat{\mathbb{Z}}^{\Sigma}$-module of rank $2g$. Using the fact that every abelian finite étale cover of X comes from the finite étale cover of J (see [12], Chapter VII, Proposition 9.1), together with a well-known isomorphism $\pi_1(J_{K^{\mathrm{alg}}}) \cong T(J)$ (see [33], §18), we obtain a natural isomorphism of G_K-modules

$$\Delta_{\overline{X}}^{\mathrm{ab}} \cong T^{\Sigma}(J).$$

The morphism of schemes $X_{K^{\mathrm{alg}}} \to \overline{X}_{K^{\mathrm{alg}}}$ induces the surjection $\Delta_X \twoheadrightarrow \Delta_{\overline{X}}$ which again induces the surjection $\Delta_X^{\mathrm{ab}} \twoheadrightarrow \Delta_{\overline{X}}^{\mathrm{ab}}$ on abelianizations. Obviously, if $r = 0$ then it is the identity, and in the case when $r > 0$ we have the following

short exact sequence of G_K-modules

$$1 \to \widehat{\mathbb{Z}}^{\Sigma}(1) \to \bigoplus_{x \in \text{cusps}} \widehat{\mathbb{Z}}^{\Sigma}(1)_x \to \Delta_X^{\text{ab}} \to T^{\Sigma}(J) \to 1.$$

The direct product in the formula above runs through the finite set of geometric cusps.

The group Δ_X is a normal closed subgroup of the topological group Π_X. Moreover, there exists a purely group theoretic characterization of this subgroup.

Theorem 1.4.1. *Let X be a hyperbolic curve and let Π_X be its étale fundamental group. Then the subgroup $\Delta_X \subset \Pi_X$ may be reconstructed group theoretically.*

Proof. When $\Sigma = \mathbb{P}$, this is the content of [23], Lemma 1.1.4, (ii), however the same proof works under the assumption that $\{p, l\} \subset \Sigma$, for some prime number $l \neq p$. We give an idea of the proof. The crucial observation is the fact that the function

$$\mathbb{P} \ni l \mapsto \dim_{\mathbb{Q}_l}(\Pi_X^{\text{ab}} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l) - \dim_{\mathbb{Q}_l}(G_K^{\text{ab}} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l) \in \mathbb{Z}$$

is constant, where $\mathbb{P}$ is the set of prime numbers. In particular, applying it to every open subgroup of Π_X and every prime number in Σ one can characterize the subgroup Δ_X in a similar way as we did in the case of inertia group I_K in the proof of Proposition 1.3.1. The remaining cases when $p \in \Sigma$ or when $\Sigma = \{p\}$ may be proved using [26], Lemma 1.17. We discuss the case $\Sigma = \{p\}$ in Chapter 2 in Proposition 2.4.1. □

We also recall the definition of decomposition groups associated to rational points and inertia groups associated to cusps (see, e.g., [1], Exposé V).

For a finite field extension L/K, let x be an L-rational point on X and fix a geometric point $\bar{x}$ over x. For every connected finite étale cover $Y \to X$ we may consider the geometric fibre $Y_{\bar{x}}$ over the geometric point $\bar{x}$. Choose now the universal pro-system of étale covers $\varprojlim X_i \to X$ and consider the limit of sets $\varprojlim X_{i,\bar{x}}$. Each element it this set is called a pro-point lying over $\bar{x}$. In other words, a pro-point is a system of compatible geometric points lying over $\bar{x}$ for every finite étale cover of X. Pick one pro-point $\tilde{x}$ lying over $\bar{x}$. The étale fundamental group $\pi_1(X)$ acts naturally on the set of pro-points and we may consider the stabilizer of the chosen pro-point $\tilde{x}$. It is a closed subgroup of $\pi_1(X)$ called a decomposition group of x. Choosing a different pro-point lying over $\bar{x}$ results in conjugating the decomposition group by some

element of $\pi_1(X)$. Therefore, the conjugacy class of decomposition subgroup is independent of any choices. We will write D_x for a decomposition group of x, well defined up to conjugation. Through the surjection $\pi_1(X) \twoheadrightarrow G_K$, the group D_x maps isomorphically onto the open subgroup G_L of G_K.

Let now x be a cusp, hence it is an L-rational point on $\overline{X}$ for some finite field extension L/K. Every connected finite étale cover $Y \to X$ extends uniquely to a connected (possibly ramified) finite cover $\overline{Y} \to \overline{X}$, where $\overline{Y}$ is the smooth compactification of Y. Therefore, we may consider as previously the pro-fibre and pro-point over $\bar{x}$ and define a decomposition group D_x of x as an appropriate stabilizer. We then define an inertia group I_x of x as the intersection $D_x \cap \pi_1(X)$. Equivalently, inertia group of x it is equal to the decomposition group of the unique lift of the point x to the base-changed curve $X_{K^{\mathrm{alg}}}$. Inertia group is a subgroup of $\pi_1(X)$ defined up to conjugation by $\pi_1(X)$. When we fix a decomposition group D_x, then we have a short exact sequence

$$1 \to I_x \to D_x \to G_L \to 1.$$

Finally, we look at the local structure of the ramification. Fix a cusp x and let R be the completion of the local ring at x on the curve $\overline{X}_{K^{\mathrm{alg}}}$. The ring R is noncanonically isomorphic to the power series ring $K^{\mathrm{alg}}[[T]]$. Covers of $\overline{X}$ ramified at x are étale locally of the form $S = R[X]/(X^n - T)$. Every automorphism of the cover $R \to S$ is given by $X \to \zeta X$ for some n-th root of unity ζ, which does not depend on the choice of the parameter T. On the other hand, this group is equal to I_x/nI_x by the definition of an inertia subgroup, hence we have a natural isomorphism $I_x/nI_x \cong \mu_n$. Therefore, by taking limit over all natural numbers, we obtain the canonical isomorphism $I_x \cong \varprojlim \mu_n = \widehat{\mathbb{Z}}(\mu)$.

Subgroups of Δ_X obtained as images of inertia groups by the surjection $\pi_1(X_{K^{\mathrm{alg}}}) \twoheadrightarrow \Delta_X$ will be called inertia groups as well, similarly for decomposition groups. One easily checks that every inertia group I in Δ_X is isomorphic to the group $\widehat{\mathbb{Z}}^{\Sigma}(1)$, moreover we also have the canonical isomorphism $I \cong \widehat{\mathbb{Z}}^{\Sigma}(\mu)$.

Theorem 1.4.2. *For a nonempty set of prime numbers Σ, inertia groups in Δ_X associated to the cusps of X can be reconstructed group theoretically from the topological group Π_X^{Σ}.*

Proof. When Σ is equal to the set of all prime numbers, see [23], Lemma 1.3.9. For the general case, we refer to [27], Corollary 2.7. □

Finally, we discuss another relation between the inertia group and the decomposition group of a cusp. For this purpose we need to recall the definition

of a commensurator. Let $H \subset G$ be a closed subgroup of a topological group G. Consider the set of all elements $g \in G$ such that the intersection $H \cap gHg^{-1}$ has finite index in H, as well as in gHg^{-1}. This set is in fact a group containing H which is called the *commensurator* of H in G and is denoted by $C_G(H)$. Then, we have the following theorem.

Theorem 1.4.3. *Fix an inertia group $I \subset \Delta_X$ of a cusp x. Then, the commensurator $C_{\Pi_X}(I)$ of the inertia group in the étale fundamental group Π_X is equal to a decomposition group D_x of the cusp x. In particular, an inertia group of a cusp determines its decomposition group.*

Proof. In the pro-l case, see [23], Lemma 1.3.7. The same proof works for every nonempty set of primes Σ. □

1.5 Kummer classes of rational functions

In this section we present the anabelian construction of Kummer classes of certain rational functions on X, as presented in [24], §4 (for a pro-Σ version, see [26], §2). We assume that X is a hyperbolic curve over a local field K with the smooth compactification $\overline{X}$. We use the same notation as in previous section. The following lemma identifies étale cohomology of certain curves with the group cohomology of their étale fundamental group.

Lemma 1.5.1. *Suppose that the genus $g(\overline{X})$ is nonzero. Let A be a finite $\pi_1(\overline{X})$-module. Then, there exists a natural isomorphism*

$$H^i(\pi_1(\overline{X}), A) \cong H^i_{\acute{e}t}(\overline{X}_{K^{\mathrm{alg}}}, A).$$

Proof. See [26], Proposition 1.1 for the case $g \geq 2$, the same proof works in our case. □

By taking inverse limits and using Remark 1.3.2 we see that similar statement holds in the case when $A = \mathbb{Z}_l$ or $A = \mathbb{Z}_l(1)$ for a prime number l.

Let $n \geq 1$ be a natural number and consider the short exact sequence of étale sheaves

$$1 \to \mu_n \to \mathbb{G}_m \to \mathbb{G}_m \to 1.$$

Taking the long exact sequence in cohomology we obtain a coboundary map

$$\mathcal{O}(X)^\times / \mathcal{O}(X)^{\times n} \hookrightarrow H^1_{\text{ét}}(X, \mu_n)$$

Identifying the étale cohomology with the group cohomology we obtain an injection

$$\mathcal{O}(X)^\times / \mathcal{O}(X)^{\times n} \hookrightarrow H^1(\pi_1(X), \mu_n).$$

This map is given explicitly by assigning to a regular function $f \in \mathcal{O}(X)^\times$ the finite étale cover obtained by taking nth root of f. We may now consider the inverse limit of these maps over all natural numbers n. Denote by

$$\widehat{\mathcal{O}(X)^{\times\Sigma}} = \varprojlim_{n\in\mathbb{N}(\Sigma)} \mathcal{O}(X)^\times/\mathcal{O}(X)^{\times n}$$

the limit of the modules $\mathcal{O}(X)^\times/\mathcal{O}(X)^{\times n}$ with respect to the natural quotient homomorphisms. Then, by taking limits we obtain an injective homomorphism

$$\widehat{\mathcal{O}(X)^{\times\Sigma}} \hookrightarrow H^1(\Pi_X, \widehat{\mathbb{Z}}^\Sigma(\mu)).$$

We will call this homomorphism the (pro-Σ) Kummer map and the image of a rational function f under the Kummer map will be called the (pro-Σ) Kummer class of f.

On the other hand, the exact sequence $1 \to \Delta_X \to \Pi_X \to G_K \to 1$ induces the inflation to restriction sequence

$$1 \to H^1(G_K, \mu_n) \to H^1(\Pi_X, \mu_n) \to H^1(\Delta_X, \mu_n)^{G_K}.$$

Since Δ_X acts trivially on the group μ_n, the last group may be replaced by the group of G_K-equivariant homomorphisms

$$\mathrm{Hom}_{G_K}(\Delta_X, \mu_n) = \mathrm{Hom}_{G_K}(\Delta_X^{\mathrm{ab}}, \mu_n).$$

Using the isomorphism $K^\times/K^{\times n} \cong H^1(G_K, \mu_n)$ and taking limit over all Σ-integers n we obtain the exact sequence

$$1 \to \widehat{K^{\times\Sigma}} \to H^1(\Pi_X, \widehat{\mathbb{Z}}^\Sigma(\mu)) \to \mathrm{Hom}_{G_K}(\Delta_X^{\mathrm{ab}}, \widehat{\mathbb{Z}}^\Sigma(\mu)). \tag{1.7}$$

Here the group of homomorphisms actually mean the group of continuous homomorphisms. Let $I \subset \Delta_X^{\mathrm{ab}}$ be the subgroup generated by the inertia subgroups I_x for all cusps $x \in \overline{X}_{K^{\mathrm{alg}}} \setminus X_{K^{\mathrm{alg}}}$, which has a direct sum decomposition $I = \oplus_x I_x$. Because the quotient of Δ_X^{ab} determined by the subgroup I is equal to the quotient $\Delta_X^{\mathrm{ab}} \twoheadrightarrow \Delta_{\overline{X}}^{\mathrm{ab}}$, we obtain the exact sequence

$$1 \to \mathrm{Hom}_{G_K}(\Delta_{\overline{X}}^{\mathrm{ab}}, \widehat{\mathbb{Z}}^\Sigma(\mu)) \to \mathrm{Hom}_{G_K}(\Delta_X^{\mathrm{ab}}, \widehat{\mathbb{Z}}^\Sigma(\mu)) \to \mathrm{Hom}_{G_K}(I, \widehat{\mathbb{Z}}^\Sigma(\mu))$$

Lemma 1.5.2. *The group* $\mathrm{Hom}_{G_K}(\Delta_{\overline{X}}^{\mathrm{ab}}, \widehat{\mathbb{Z}}^\Sigma(\mu))$ *of* G_K*-equivariant homomorphisms is trivial.*

Proof. See [24], Lemma 4.6. Here we give a sketch of the proof for the convenience of the reader. The group $\Delta_{\overline{X}}^{\mathrm{ab}}$ is isomorphic to the Σ-adic Tate module of the Jacobian $J(\overline{X})$ of the curve $\overline{X}$, which is self dual with respect to the

Cartier duality. Hence, it would be enough to show that the Tate module of an abelian variety A over a p-adic field K has a trivial submodule of G_K-invariant elements. But $A(K)$ is a p-adic Lie group, thus has an open neighbourhood of identity isomorphic to the group $\mathbb{Z}_p^d$ for some natural number d, which is obviously torsion-free. Since $A(K)$ is compact, the subgroup of torsion elements must be finite, which implies that the G_K-invariant part of the Tate module of A is trivial. □

Therefore, using the above lemma, we obtain the injection

$$\mathrm{Hom}_{G_K}(\Delta_X^{\mathrm{ab}}, \widehat{\mathbb{Z}}^\Sigma(\mu)) \hookrightarrow \mathrm{Hom}_{G_K}(I, \widehat{\mathbb{Z}}^\Sigma(\mu)),$$

which together with the sequence (1.7) gives the following exact sequence

$$1 \to \widehat{K^{\times\Sigma}} \to H^1(\Pi_X, \widehat{\mathbb{Z}}^\Sigma(\mu)) \to \mathrm{Hom}_{G_K}(I, \widehat{\mathbb{Z}}^\Sigma(\mu)).$$

Using the natural identification $I_x \cong \widehat{\mathbb{Z}}^\Sigma(\mu)$ recalled at the end of Section 1.4 we obtain a canonical isomorphism

$$\mathrm{Hom}_{G_K}(I, \widehat{\mathbb{Z}}^\Sigma(\mu)) \cong \bigoplus_{x \in cusps} \widehat{\mathbb{Z}}^\Sigma,$$

which gives us the exact sequence

$$1 \to \widehat{K^{\times\Sigma}} \to H^1(\Pi_X, \widehat{\mathbb{Z}}^\Sigma(\mu)) \to \bigoplus_{x \in cusps} \widehat{\mathbb{Z}}^\Sigma. \tag{1.8}$$

The next lemma relates this sequence to the Kummer homomorphism.

Lemma 1.5.3. *We have a commutative diagram with exact rows*

$$\begin{array}{ccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & \mathcal{O}(X)^\times & \xrightarrow{div} & \oplus_{x \in cusps} \mathbb{Z} \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \widehat{K^{\times\Sigma}} & \longrightarrow & H^1(\Pi_X, \widehat{\mathbb{Z}}^\Sigma(\mu)) & \longrightarrow & \oplus_{x \in cusps} \widehat{\mathbb{Z}}^\Sigma, \end{array}$$

where the map div is the divisor map. Moreover, when Σ is equal to the set of all prime numbers, then all vertical arrows are injective.

Proof. The commutativity of the left square is obvious from the functoriality of Kummer sequence. The commutativity of the right square follows easily from the construction of the canonical isomorphism $I_x \cong \widehat{\mathbb{Z}}^\Sigma(\mu)$. The injectivity in the case $\Sigma = \mathbb{P}$ follows from the fact that for every p-adic local field K the subgroup $\bigcap_{n \geq 1} K^\times/(K^\times)^n$ of divisible elements is trivial. □

Let x be an L-rational point on the curve X, for some finite field extension L/K. Choose a decomposition group D_x of this point and consider the restriction map

$$s^*\colon H^1(\Pi_{X_L}, \widehat{\mathbb{Z}}^\Sigma(\mu)) \to H^1(D_x, \widehat{\mathbb{Z}}^\Sigma(\mu)) \cong H^1(G_L, \widehat{\mathbb{Z}}^\Sigma(\mu)),$$

where the last isomorphism is induced by the isomorphism $D_x \cong G_L$. Then, we have the following diagram

$$\begin{array}{ccccc} \mathcal{O}(X_L)^\times & \hookrightarrow & \widehat{\mathcal{O}(X_L)^{\times\Sigma}} & \hookrightarrow & H^1(\Pi_{X_L}, \widehat{\mathbb{Z}}^\Sigma(\mu)) \\ \vdots & & \downarrow & & \downarrow{\scriptstyle s^*} \\ L^\times & \hookrightarrow & \widehat{L^{\times\Sigma}} & \xrightarrow{\simeq} & H^1(G_L, \widehat{\mathbb{Z}}^\Sigma(\mu)) \end{array}$$

where the existence and description of the dotted arrow follows from the next lemma.

Lemma 1.5.4. *The restriction map $H^1(\Pi_{X_L}, \widehat{\mathbb{Z}}^\Sigma(\mu)) \to H^1(G_L, \widehat{\mathbb{Z}}^\Sigma(\mu))$ induces the homomorphism $\mathcal{O}(X_L)^\times \to L^\times$ which is equal to the evaluation map $f \mapsto f(x)$.*

Proof. This follows immediately from the functoriality of the Kummer homomorphism with finite coefficients μ_n applied to the morphism $\operatorname{Spec} L \to X$ given by the rational point x. □

To turn the above construction into a group theoretical algorithm we will need to replace the Galois module $\widehat{\mathbb{Z}}^\Sigma(\mu)$ and a canonical isomorphism $I_x \cong \widehat{\mathbb{Z}}^\Sigma(\mu)$ by a corresponding group theoretical object.

1.6 Rigidification of cyclotomes

In this section we provide a group theoretic version of the canonical isomorphism $I_x \cong \widehat{\mathbb{Z}}^\Sigma(\mu)$ that was used to construct the sequence (1.8). First, we explain the terminology used in the title of this section. Following Mochizuki, by a *cyclotome* we mean a topological G_K-module isomorphic (noncanonically) to the topological G_K-module $\widehat{\mathbb{Z}}^\Sigma(1)$, for some nonempty set of prime numbers Σ. Thus, an inertia group I_x of a cusp x and the module $\widehat{\mathbb{Z}}^\Sigma(\mu)$ are examples of cyclotomes. The topic of this section is to construct certain canonical isomorphisms between those cyclotomes.

Let C be a proper curve over K of nonzero genus and let n be a Σ-integer. From the Poincaré duality in étale cohomology (e.g., [20], VI, §11), expressed as a cup product in group cohomology

$$H^0(\Delta_C, \mu_n) \times H^2(\Delta_C, \mathbb{Z}/n\mathbb{Z}) \to H^2(\Delta_C, \mu_n) \cong \mathbb{Z}/n\mathbb{Z},$$

we obtain a natural isomorphism $\mathrm{Hom}(H^2(\Delta_C, \mathbb{Z}/n\mathbb{Z}), \mathbb{Z}/n\mathbb{Z}) \cong \mu_n$. Following [26], we introduce the following definition.

Definition 1.6.1. Let X be a hyperbolic curve with positive genus $g(\overline{X})$. We define the G_K-module M_X^Σ by the formula

$$M_X^\Sigma = \mathrm{Hom}(H^2(\Delta_{\overline{X}}, \widehat{\mathbb{Z}}^\Sigma), \widehat{\mathbb{Z}}^\Sigma)$$

where, as previously, $X \subset \overline{X}$ is the smooth compactification of X.

From the short discussion preceding the definition together with a limit argument it follows that M_X^Σ is naturally isomorphic to the G_K-module $\widehat{\mathbb{Z}}^\Sigma(\mu)$, thus M_X^Σ is a cyclotome. Composing the natural isomorphisms $M_X^\Sigma \cong \widehat{\mathbb{Z}}^\Sigma(\mu)$ and $\widehat{\mathbb{Z}}^\Sigma(\mu) \cong I_x$ we obtain, for every cusp x, the canonical isomorphism $M_X \cong I_x$. In what follows, we are going to reconstruct this canonical isomorphism between the module M_X^Σ and the inertia group I_x of a cusp x group theoretically.

Let x be a K-rational point on X and define U to be the open subscheme $\overline{X} \setminus \{x\}$. Then, we have open immersions $X \hookrightarrow U \hookrightarrow \overline{X}$ which induce surjections $\Delta_X \twoheadrightarrow \Delta_U \twoheadrightarrow \Delta_{\overline{X}}$. The quotient $\Delta_X \twoheadrightarrow \Delta_U$ is obtained by dividing by the smallest normal subgroup of Δ_X generated by all inertia groups of cusps excluding the cusp x. On the other hand, the quotient $\Delta_U \twoheadrightarrow \Delta_{\overline{X}}$ is obtained by dividing by the normal subgroup generated by the inertia group of the cusp x. Moreover, the quotient $\Delta_X \twoheadrightarrow \Delta_U$ maps every inertia group of the cusp x in X isomorphically onto an inertia subgroup of the same cusp x in U, thus we may identify them canonically. Therefore, we are reduced to consider the surjection $\Delta_U \twoheadrightarrow \Delta_{\overline{X}}$. Let H be the kernel of this homomorphism. Consider the topological commutator subgroup $[\Delta_U, H]$ of H. It is also a normal subgroup of Δ_U, hence by taking quotient by $[\Delta_U, H]$ we obtain a commutative diagram with short exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \longrightarrow & \Delta_U & \longrightarrow & \Delta_{\overline{X}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & I & \longrightarrow & Q & \longrightarrow & \Delta_{\overline{X}} & \longrightarrow & 1. \end{array}$$

From the above description of the group H we easily see that the group I is isomorphic to $\widehat{\mathbb{Z}}^\Sigma(1)$. Moreover, for every choice of an inertia subgroup $I_x \subset H$ the quotient $H \twoheadrightarrow I$ induces an isomorphism $I_x \cong I$. Therefore it is enough to construct the induced isomorphism $I \cong M_X^\Sigma$. The subquotient

$$\Delta_U \twoheadrightarrow Q \twoheadrightarrow \Delta_{\overline{X}}$$

will be called the *maximal centrally cuspidal subquotient* of the quotient $\Delta_U \twoheadrightarrow \Delta_{\overline{X}}$.

Consider now the inflation-restriction exact sequence associated to the group extension $1 \to I \to Q \to \Delta_{\overline{X}} \to 1$ with the coefficient module equal to I equipped with a trivial group action. In particular, we have the coboundary map:

$$\mathrm{Hom}(I, I) = H^1(I, I)^{\Delta_{\overline{X}}} \to H^2(\Delta_{\overline{X}}, I^I) = H^2(\Delta_{\overline{X}}, I)$$

On the other hand, we have canonical isomorphisms

$$\mathrm{Hom}(M_X^\Sigma, I) \cong \mathrm{Hom}(M_X^\Sigma, \widehat{\mathbb{Z}}^\Sigma) \otimes I \cong H^2(\Delta_{\overline{X}}, \widehat{\mathbb{Z}}^\Sigma) \otimes I \cong H^2(\Delta_{\overline{X}}, I).$$

Therefore, composing those isomorphisms with the coboundary map mentioned previously we obtain a homomorphism

$$\mathrm{Hom}(I, I) \to \mathrm{Hom}(M_X^\Sigma, I).$$

Now, consider the image of the identity map $I \to I$ under this homomorphism, which is a homomorphism $M_X^\Sigma \to I$.

Proposition 1.6.2. *The homomorphism $M_X^\Sigma \to I$ just constructed is in fact an isomorphism which is equal to the natural isomorphism $M_X^\Sigma \cong I$.*

Proof. When Σ is the set of all prime numbers, see [30], Proposition 1.4,(ii), this also implies the general case. □

In this way we construct canonical isomorphisms between the G_K-module M_X^Σ and an inertia group $I_x \subset \Delta_X$ of a cusp x compatible with the natural identifications with $\widehat{\mathbb{Z}}^\Sigma(\mu)$.

In Section 1.3 we introduced another cyclotome $\widehat{\mathbb{Z}}(G_K)$, canonically isomorphic to $\widehat{\mathbb{Z}}(\mu)$ by the local reciprocity map. Therefore, by composing canonical isomorphisms $M_X \cong \widehat{\mathbb{Z}}(\mu)$ and $\widehat{\mathbb{Z}}(\mu) \cong \widehat{\mathbb{Z}}(G_K)$ we obtain the canonical isomorphism $M_X \cong \widehat{\mathbb{Z}}(G_K)$. Then, in the case when the set Σ is equal to the set of all prime numbers, we have the following lemma.

Lemma 1.6.3. *Assume that $\Sigma = \mathbb{P}$. Then, the natural isomorphism $M_X \cong \widehat{\mathbb{Z}}(G_K)$ can be reconstructed group theoretically from the topological group $\Pi_X = \pi_1(X)$.*

Proof. See [30], Corollary 1.10, (ii), (c). □

We now need to discuss the group theoretic version of the Kummer exact sequence and the Kummer classes of functions. Recall the exact sequence

$$1 \longrightarrow H^1(G_K, \widehat{\mathbb{Z}}^\Sigma(\mu)) \longrightarrow H^1(\Pi_X, \widehat{\mathbb{Z}}^\Sigma(\mu)) \longrightarrow \bigoplus_{x \in cusps} \widehat{\mathbb{Z}}^\Sigma.$$

We may apply exactly the same construction as in Section 1.5, replacing the cyclotome $\widehat{\mathbb{Z}}^\Sigma(\mu)$ with the cyclotome M_X^Σ, to obtain the exact sequence

$$1 \longrightarrow H^1(G_K, M_X^\Sigma) \longrightarrow H^1(\Pi_X, M_X^\Sigma) \longrightarrow \bigoplus_{x \in cusps} \mathrm{Hom}_{G_K}(I_x, M_X^\Sigma).$$

Using the natural (and group theoretic) isomorphism $M_X^\Sigma \cong I_x$, the last group of homomorphisms is identified with a direct sum of copies of the group $\widehat{\mathbb{Z}}^\Sigma$. Moreover, since the natural isomorphism $M_X^\Sigma \cong \widehat{\mathbb{Z}}^\Sigma(\mu)$ is compatible with the natural isomorphisms $\widehat{\mathbb{Z}}^\Sigma(\mu) \cong I_x$ and $M_X^\Sigma \cong I_x$, it induces a commutative diagram

$$\begin{array}{ccccc} H^1(G_K, \widehat{\mathbb{Z}}^\Sigma(\mu)) & \longrightarrow & H^1(\Pi_X, \widehat{\mathbb{Z}}^\Sigma(\mu)) & \longrightarrow & \bigoplus_{x \in cusps} \widehat{\mathbb{Z}}^\Sigma \\ \downarrow \simeq & & \downarrow \simeq & & \| \\ H^1(G_K, M_X^\Sigma) & \longrightarrow & H^1(\Pi_X, M_X^\Sigma) & \longrightarrow & \bigoplus_{x \in cusps} \widehat{\mathbb{Z}}^\Sigma. \end{array} \tag{1.9}$$

The cohomology module $H^1(\Pi_X, M_X^\Sigma)$, constructed group theoretically, serves as an analogue of the group $H^1(\Pi_X, \widehat{\mathbb{Z}}^\Sigma(\mu))$ and the above diagram provides the compatibility between the Kummer classes of regular functions.

1.7 Elliptic cuspidalization

We now come back to the original situation introduced in Section 1.1. Namely, we have an elliptic curve E over the p-adic local field K and we consider the hyperbolic curve X of type $(1,1)$ obtained by removing the K-rational point given by the origin O from the curve E. We also denote by $X_n = E \setminus E[n]$ the open subscheme of E obtained by removing the subgroup of n-torsion points. In this section we assume that the residue characteristic p is contained in the set Σ.

Consider the maximal geometrically pro-Σ étale fundamental group Π_X of the hyperbolic curve X. The main result in this section is a group theoretic construction of decomposition groups of nonzero torsion points of the elliptic curve E, as subgroups of the group Π_X. In fact, the construction will give even more, as it produces a fundamental group of the curve E with certain torsion points removed. More precisely, for every natural number n, we are going to construct (from the fundamental group Π_X) another topological group Π_U together with a surjective homomorphism $\Pi_U \twoheadrightarrow \Pi_X$ such that Π_U is the étale fundamental group of a scheme U and the group homomorphism $\Pi_U \twoheadrightarrow \Pi_X$ comes from the open immersion $U \hookrightarrow X$ which identifies U with the subscheme X_n. This construction is usually called the *elliptic cuspidalization* and is introduced in [24] in the case when $\Sigma = \mathbb{P}$.

From the definition of X_n, for every natural number n, we have a cartesian diagram

$$\begin{array}{ccc} X_n & \hookrightarrow & E \\ \downarrow & & \downarrow n \\ X & \hookrightarrow & E, \end{array}$$

where the vertical arrows are finite étale morphisms obtained by the multiplication by n isogeny on the elliptic curve E.

Lemma 1.7.1. *The open subgroups Π_{X_n} of Π_X corresponding to the finite étale covers $X_n \to X$ can be characterised group theoretically.*

Proof. First we claim that we may determine all the open subgroups of $\Pi_U \subset \Pi_X$ such that the corresponding finite étale cover $U \to X$ is unramified over the unique cusp of X, equivalently that the cover $U \to X$ extends to the finite étale cover of the proper curve E. Indeed, we easily observe that the quotient $\Pi_X \twoheadrightarrow \Pi_E$ corresponding to the open immersion $X \hookrightarrow E$ is determined group theoretically as the pushout of the following diagram

$$\begin{array}{ccc} \Delta_X & \hookrightarrow & \Pi_X \\ \downarrow & & \\ \Delta_X^{\mathrm{ab}}. & & \end{array}$$

Thus, the étale covers of X which extend to étale covers of E correspond to the open subgroups of Π_X which are the preimages of open subgroups of Π_E under the quotient map $\Pi_X \twoheadrightarrow \Pi_E$.

Therefore, we are reduced to characterise the multiplication by n isogeny among all étale covers of E, where n is a Σ-integer. Let H be a normal open subgroup of Π_E generated by the image of the decomposition group of the cusp and the subgroup $n\Delta_E \subset \Delta_E$ (written additively). Then one easily checks that H corresponds to the étale cover $[n]\colon E \to E$. □

The above lemma constructs the group Π_{X_n} as an open subgroup of Π_X, whereas we want to construct the surjection $\Pi_{X_n} \twoheadrightarrow \Pi_X$. This is the content of the next proposition which is in fact the most nontrivial part of the whole construction since it uses the main result of [22].

Proposition 1.7.2. *From the topological group Π_X we may reconstruct the surjection $\Pi_{X_n} \twoheadrightarrow \Pi_X$ corresponding to the open immersion $X_n \hookrightarrow X$. Moreover, we may also reconstructs the set of conjugacy classes of decomposition groups of torsion points (as subgroups of the topological group Π_X) together with the group structure on the set of decomposition groups corresponding to the group structure on the elliptic curve E.*

Proof. Take the open subgroup $\Pi_{X_n} \subset \Pi_X$ constructed in the previous lemma. The curve X_n has n^2 cusps. Using the results of Section 1.4 we may reconstruct the inertia groups of those cusps and, by considering commensurators, also their decomposition groups. Pick one of the cusps which is K-rational, equivalently its decomposition group surjects onto the Galois group G_K, and call it P. Define the quotient $\Delta_{X_n} \twoheadrightarrow \Delta_P$ whose kernel is the normal subgroup generated by the inertia subgroups of Π_{X_n} of all cusps excluding the cusp P. Finally, let Π_P be a quotient of Π_{X_n} obtained by pushing out the quotient $\Delta_{X_n} \twoheadrightarrow \Delta_P$ along the map $\Delta_{X_n} \hookrightarrow \Pi_{X_n}$

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_{X_n} & \longrightarrow & \Pi_{X_n} & \longrightarrow & G_K & \longrightarrow & 1 \\ & & \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow & & \| & & \\ 1 & \longrightarrow & \Delta_P & \longrightarrow & \Pi_P & \longrightarrow & G_K & \longrightarrow & 1. \end{array}$$

By construction, the quotient Π_P is isomorphic to the étale fundamental group Π_U of the curve $U = E \setminus \{P\}$. Moreover, we may choose the isomorphism $\Pi_P \cong \Pi_U$ to commute with the natural surjections to G_K. Therefore, the above discussion may be summarized by the following diagram of curves and their fundamental groups

$$\begin{array}{ccc} \Pi_{X_n} & \twoheadrightarrow & \Pi_P \cong \Pi_U \\ \downarrow & & \\ \Pi_X & & \end{array} \qquad \begin{array}{ccc} X_n & \hookrightarrow & U \\ \downarrow\!\!\downarrow & & \\ X. & & \end{array} \tag{1.10}$$

The K-curves X and U are isomorphic as schemes over K. Moreover, since every fundamental group in the above diagram is endowed with the fixed surjection to the group G_K and the maps between them are morphisms over G_K, we may choose an isomorphism $\Pi_P \cong \Pi_X$ lying over G_K. Now it follows from the p-adic Grothendieck Conjecture (see [22], Theorem A) that this isomorphism of fundamental groups comes from the isomorphism of K-schemes $U \cong X$ (this is the point where we use that $p \in \Sigma$). Therefore, the surjection $\Pi_{X_n} \twoheadrightarrow \Pi_X$ obtained as the composition

$$\Pi_{X_n} \twoheadrightarrow \Pi_P \cong \Pi_X$$

comes from the morphism of schemes, which can be identified (up to an automorphism of K-schemes) with the open immersion $X_n \hookrightarrow X$. This proves the first part of the proposition.

Consider now the conjugacy classes of decomposition groups of cusps in Π_{X_n}. We map them to Π_X by the surjection $\Pi_{X_n} \twoheadrightarrow \Pi_X$. Then, it follows easily from the construction that this image consists of conjugacy classes of

decomposition groups of n-torsion points. To recover the group structure on the decomposition groups we use the natural isomorphism

$$E[n](K^{\mathrm{alg}}) \cong \mathrm{Gal}(E_{K^{\mathrm{alg}}} \to E_{K^{\mathrm{alg}}})$$

between geometric torsion points of E and the Galois group of the finite étale cover $E_{K^{\mathrm{alg}}} \to E_{K^{\mathrm{alg}}}$ given by the multiplication by n isogeny. Indeed, we may map all decomposition groups of torsion points to the quotient $\Pi_X \twoheadrightarrow \Pi_E$ and consider the permutations of their images under the action of the Galois group of the cover $[n]\colon E \to E$. □

In fact, we may obtain a slightly stronger statement as a corollary of the above proof. Let P be a nonzero point of E with a decomposition group $D \subset \Pi_X$ and let n be a Σ-integer. Let $X_n \hookrightarrow X$ be the open subscheme obtained by removing n-torsion points. Therefore, the previous proposition constructs the corresponding surjection $\Pi_{X_n} \twoheadrightarrow \Pi_X$. Consider the set A of rational points Q on the elliptic curve E such that $nQ = P^\tau$, for some automorphism τ of the elliptic curve E. Hence the points from the set A are rational points on the curve X_n.

Lemma 1.7.3. *With the notation as above, suppose we are given a decomposition group D of the point P as a subgroup of the group Π_X. Then, from the inclusion $D \subset \Pi_X$, we may reconstruct conjugacy classes of decomposition groups of rational points Q belonging to the set A as conjugacy classes of subgroups of Π_{X_n}.*

Proof. Indeed, we look again at the diagram (1.10). Intersecting the conjugacy class of a decomposition group D with an open subgroup Π_{X_n} produces n^2 conjugacy classes of subgroups in Π_{X_n}, corresponding to points Q satisfying $nQ = P$. Therefore, using G_K-equivariant isomorphism $\Pi_P \cong \Pi_X$, the set of conjugacy classes of subgroups that we obtain in Π_{X_n} is equal to the desired set of decomposition groups. □

1.8 Reconstruction of the local height

In this final section we give the proof of Theorem 1.1.1. Observe that, when $\Sigma \neq \{p\}$, having good reduction is a group theoretic property due to the following lemma.

Lemma 1.8.1. *Assume that the set Σ contains a prime number $l \neq p$. Then, from the topological group Π_X one can determine whether the elliptic curve E has good reduction.*

Proof. We have seen that the subgroup $\Delta_X \subset \Pi_X$ can be recovered group theoretically. Therefore, for a prime number $l \neq p$ belonging to Σ we may consider the G_K-module $\Delta_X^{(l)} = \Delta_X \otimes_{\widehat{\mathbb{Z}}^\Sigma} \mathbb{Z}_l$. On the other hand, $\Delta_X^{(l)}$ is isomorphic as a G_K-module to the l-adic Tate module $T_l(E)$. It follows immediately from a well-known criterion of Serre-Tate (see [36]), that E has good reduction if and only if the action of the inertia group I_K on $\Delta_X^{(l)}$ is trivial. Since the subgroup $I_K \subset G_K$ is group theoretic, the lemma follows. □

We now start proving Theorem 1.1.1. Because the Néron-Tate local height function is invariant under field extensions, we may reduce to the case when E has good reduction. Indeed, for a finite extension L/K, the fundamental group of X_L is equal to the preimage of G_L under the group theoretic surjection $\Pi_X \twoheadrightarrow G_K$. Then, at least in the case when $\Sigma \neq \{p\}$, we may restrict to a subgroup G_L and use Lemma 1.8.1 to finish the reduction step. On the other hand, recall that there exists a finite field extension F/K such that every elliptic curve over K acquires split semi-abelian reduction after the base change to F. Indeed, it follows from a well-known property of local fields that for every integer d there exist only finitely many field extensions L/K with degree $[L : K] \leq d$. Thus, we may simply restrict to the open subgroup G_F to acquire good reduction, without any assumption on the set Σ.

Therefore, we will now assume that E has good reduction. Recall that for an elliptic curve E over K with good reduction there exists a model $\mathcal{E}$ over $\mathcal{O}_K$ described by a minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_2x + a_6$$

where $a_i \in \mathcal{O}_K$ with discriminant Δ being a p-adic unit. This expression is unique up to the change of coordinates given by the formula

$$x \mapsto u^2x + r, \quad y \mapsto u^3y + u^2sx + t,$$

where $r, s, t \in \mathcal{O}_K$ and $u \in \mathcal{O}_K^\times$ (see [38]). In the following we fix some minimal Weierstrass equation of E.

We will call a K^{alg}-rational point P on the elliptic curve E *integral* if

$$v_K(x(P)) \geq 0,$$

where x is the function chosen in the minimal Weierstrass equation above. We easily see from the transformation formula recalled above that this property does not depend on the choice of the function x and is therefore well defined. Because the group scheme $\mathcal{E}[n]$ is étale over $\operatorname{Spec} \mathcal{O}_K$ for every natural number

n prime to p, one easily checks that every n-torsion point (for $(n,p)=1$) is integral. Moreover, the set of K^{alg}-points which are not integral is equal to the preimage of the origin O of the reduced elliptic curve $\mathcal{E}_k$ under the reduction map $E(K^{\mathrm{alg}}) = \mathcal{E}(\mathcal{O}_{K^{\mathrm{alg}}}) \to \mathcal{E}_k(k^{\mathrm{alg}})$ (see, e.g., [38], Chapter VII, §2).

Let P be now a nonzero n-torsion point on the elliptic curve E. Consider the set of rational functions on E having double pole at the origin O and simple zero at the point P. It follows immediately from the Riemann-Roch formula that this set is a $K^{\times}$-torsor and every function in this set is equal to $u(x-x(P))$ for some $u \in K^{\times}$. We introduce the following useful definition.

Definition 1.8.2. For every algebraic extension L/K we define the $L^{\times}$-torsor of *standard* functions associated to the point P as the set of functions f of the form $f = u(x - x(P))$, for some $u \in L^{\times}$. Moreover, we define the $\mathcal{O}_L^{\times}$-torsor of *integral* standard functions associated to the point P as the set of all functions of the form $u(x - x(P))$, where $u \in \mathcal{O}_L^{\times}$.

Observe that the definition of the $\mathcal{O}_K^{\times}$-torsor of integral functions does not depend on the choice of a minimal Weierstrass equation over K. Indeed, for any other choice of minimal Weierstrass equation with coordinate functions x' and y' we have $x'-x'(P) = v(x-x(P))$, for some unit $v \in \mathcal{O}_K^{\times}$. Therefore, any minimal Weierstrass equation determines the same reduction of the group structure from $K^{\times}$ to $\mathcal{O}_K^{\times}$, i.e., canonically determines the $\mathcal{O}_K^{\times}$-torsor of integral functions. Moreover, we easily see that the construction of this torsor is compatible with every algebraic extension of the base field, as the good reduction property is stable under base change.

Lemma 1.8.3. *Assume that Σ is the set of all prime numbers and E has good reduction. Let n be a natural number prime to p and suppose that $K = K(E[n])$. Then, the set of $\mathcal{O}_K^{\times}$-torsors of integral standard functions associated to all nonzero n-torsion points can be constructed group theoretically from the group Π_X.*

Proof. Let P be a nonzero n-torsion point on E. We use the elliptic cuspidalization (Proposition 1.7.2) to construct the topological group Π_U together with a surjection $\Pi_U \twoheadrightarrow \Pi_X$ coming from the open immersion of schemes $U = X \setminus \{P, -P\} \hookrightarrow X$ if $n > 2$, and $U = X \setminus \{P\} \hookrightarrow X$ if $n = 2$. Next, we recall the exact sequence (1.9)

$$1 \to H^1(G_K, M_X) \to H^1(\Pi_U, M_X) \to \bigoplus_{x \in cusps} \widehat{\mathbb{Z}},$$

which we constructed group theoretically. By the definition of U, the set of standard functions associated to the point P is contained in the set of regular

functions on U. Then, using the above exact sequence and considering the divisor of zeroes and poles associated to classes in $H^1(\Pi_U, M_X)$, we may choose those classes whose divisor has double pole at the cusp of X and zero at the point P. This set of classes is a $\widehat{K^\times}$-torsor, informally it consists of all functions f of the form $f(x) = u(x - x(P))$ for $u \in \widehat{K^\times}$. Therefore, to obtain the $\mathcal{O}_K^\times$-torsor of integral standard functions, we need to reduce the indeterminacy from $\widehat{K^\times}$ to $\mathcal{O}_K^\times$. We achieve this by evaluating these functions at various torsion points.

Recall that by applying elliptic cuspidalization we also obtain the set of decomposition groups of torsion points, as subgroups of Π_U, together with a group structure coming from the group structure on elliptic curve E. Thus, if D_Q is a decomposition group of a m-torsion point Q, we may consider the evaluation map

$$H^1(\Pi_U, M_X) \to H^1(D_Q, M_X) \cong H^1(G_K, M_X) \cong H^1(G_K, \widehat{\mathbb{Z}}(G_K)) \twoheadrightarrow \widehat{\mathbb{Z}} \quad (1.11)$$

where the first isomorphism is induced by surjection $\Pi_U \twoheadrightarrow G_K$, the second comes from the canonical isomorphism $M_X \cong \widehat{\mathbb{Z}}(G_K)$ and the last surjection is the valuation map (1.5) constructed in Section 1.3.

To specify the $\mathcal{O}_K^\times$-torsor of integral standard functions f, we impose the following condition:

> $(*)$ *for all natural numbers m prime to p and all m-torsion points $Q \neq \pm P$, the value $f(Q)$ of the function f at the point Q is a p-adic unit.*

We claim that f satisfies the above property if and only if f is an integral standard function. Indeed, since $f(Q) = u(x(Q) - x(P))$, it is equivalent to check that $x(Q) - x(P)$ belongs to $\mathcal{O}_{K^{\mathrm{alg}}}^\times$. But it clearly belongs to $\mathcal{O}_{K^{\mathrm{alg}}}$ since both points P and Q are integral. Hence it is enough to prove that the only m-torsion points Q, for $(m, p) = 1$, satisfying $\overline{x(Q)} = \overline{x(P)}$ are given by $\pm P$. Here by $\overline{x(Q)}$ we mean the image of $x(Q)$ under the reduction map $\mathcal{O}_{K^{\mathrm{alg}}} \twoheadrightarrow k^{\mathrm{alg}}$. On the other hand, this statement follows easily from the injectivity of the reduction map $E(K^{\mathrm{alg}})[m] \to \mathcal{E}_k(k^{\mathrm{alg}})$, when restricted to m-torsion points. Finally, we easily observe that the condition $(*)$ is group theoretic since it is equivalent to the triviality of the homomorphism (1.11) for the point Q. $\square$

Finally, we may prove the main theorem of this chapter.

Proof of Theorem 1.1.1. Let s be a section over an open subgroup G_L of the surjection $\Pi_X \twoheadrightarrow G_K$ coming from a rational point S. We may assume that S

is a nontorsion point. Choose natural number n prime to p and let $X_n \hookrightarrow X$ be the subscheme obtained by removing all n-torsion points. Let A be the set of all rational points Q such that $nQ = S^\tau$, for some automorphism $\tau \in \mathrm{Aut}(E)$. By restricting to an open subgroup of G_K we may assume that all n-torsion points as well as all points Q contained in A are K-rational.

The section s determines a decomposition group of the point S in Π_X. Using Lemma 1.7.3 we may reconstruct conjugacy classes of decomposition groups of all points Q from the set A as subgroups of the group Π_{X_n}. We fix one point $Q \in A$ and its decomposition group $D_Q \subset \Pi_{X_n}$. The group D_Q determines a section $s_0 \colon G_K \to \Pi_{X_n}$ of the surjection $\Pi_{X_n} \twoheadrightarrow G_K$, hence also a restriction map

$$s_0^* \colon H^1(\Pi_{X_n}, M_X) \to H^1(G_K, M_X) \cong H^1(G_K, \widehat{\mathbb{Z}}(G_K)),$$

which we may compose with the group theoretic absolute value map (1.5)

$$v \colon H^1(G_K, \widehat{\mathbb{Z}}(G_K)) \twoheadrightarrow \widehat{\mathbb{Z}}.$$

Then, for every regular function $f \in \mathcal{O}(X_n)^\times$, from the functorial properties of Kummer sequence we obtain the equality $v \circ s_0^*(f) = v(f(Q))$. Moreover, since the section comes from the rational point, this image actually lies in the subgroup $\mathbb{Z} \subset \widehat{\mathbb{Z}}$.

Let P be a nontrivial n-torsion point. By using Lemma 1.8.3 we may reconstruct cohomology classes of a integral standard functions $f = u(x - x(P))$, where u is a p-adic unit, associated an n-torsion point P. These classes are in fact elements of the group $H^1(\Pi_{X_n}, M_X)$. Thus, by the previous discussion, we may evaluate these classes at the point Q to obtain the integer

$$v \circ s_0^*(f) = v(f(S)) = v(x(Q) - x(P)) \in \mathbb{Z}.$$

This integer is nonnegative if and only if Q is integral which implies that its local height is equal to zero. On the other hand, if $v(f(Q)) < 0$, then in fact $v(f(Q))$ is already equal to $v(x(Q))$ from which we immediately obtain the local height $\lambda(Q)$ of the point Q.

Moreover, observe that the cohomology class of the function F_n appearing in Lemma 1.2.4 may also be reconstructed group theoretically, up to a p-adic unit, as a cohomology class in $H^1(\Pi_{X_n}, M_X)$. Indeed, we easily see that F_n is, up to the factor n^2, equal to the product of integral standard functions associated to n-torsion points. Therefore, by evaluating the Kummer class of F_n at Q, we may reconstruct the integer $v(F_n(Q))$. Finally, Lemma 1.2.4 implies that this data determines the local height $\lambda(nQ) = \lambda(S)$, which finishes the proof. $\square$

Remark 1.8.4. In fact, in the case of potentially good reduction it is also possible to prove a pro-Σ version of Theorem 1.1.1, for every subset Σ of prime numbers containing the prime number p. Namely, we replace the étale fundamental group $\pi_1(X)$ by maximal geometric pro-Σ quotient Π_X and consider sections of the surjection $\Pi_X^{\Sigma} \twoheadrightarrow G_K$ coming from rational points. We come back to this problem at the end of the next chapter.

Chapter 2

Anabelian criteria of good reduction

2.1 Introduction

Let E be an elliptic curve over a p-adic local field K. Consider, as in the previous chapter, a hyperbolic curve X obtained by removing from E the K-rational point given by the origin O of the elliptic curve E. Let $\pi_1^{(p)}(X)$ be the maximal geometrically pro-p étale fundamental group of the hyperbolic curve X. Thus, we have a short exact sequence of topological groups

$$1 \to \pi_1^{(p)}(X_{K^{\mathrm{alg}}}) \to \pi_1^{(p)}(X) \to G_K \to 1,$$

where $\pi_1^{(p)}(X_{K^{\mathrm{alg}}})$ is defined as the maximal pro-p quotient of the geometric fundamental group $\pi_1(X_{K^{\mathrm{alg}}})$.

In this chapter we consider the following problem. Given the topological group $\pi_1^{(p)}(X)$, is it possible to determine the reduction type of the elliptic curve E over K? In this context, the strongest result we can prove is the following theorem.

Theorem 2.1.1. *Assume that $p \geq 5$. Then, from the topological group $\pi_1^{(p)}(X)$ equipped with the set of all discrete tangential sections, we may recover the reduction type of the elliptic curve E.*

For a definition of the notion of a discrete tangential section, see Section 2.5. In fact, we will see that even when p is smaller than five we may recover the reduction type is certain special cases.

The problem considered in this chapter is motivated by the results of [16], where it is proved that for a proper hyperbolic curve X one can determine, from the fundamental group $\pi_1^{(p)}(X)$, whether the curve X has good ordinary

reduction. Here, good ordinary reduction of a curve X means that the curve X has good reduction and that the reduction of the Jacobian $J(X)$ of X is an ordinary abelian variety.

Remark 2.1.2. Let Σ be a nonempty set of prime numbers. One can consider analogous problem where instead of $\pi_1^{(p)}(X)$ we take the maximal geometrically pro-Σ fundamental group Π_X of the curve X. When the set Σ contains a prime number $l \neq p$, then we have already seen this characterization in Lemma 1.8.1. On the other hand, we will explain below why we are cannot use the p-adic criterion of good reduction to determine the reduction type of E.

Recall that, for an abelian variety A over K, we know that the variety A has good reduction if and only if the p-adic representation $V_p(A) = T_p(A) \otimes \mathbb{Q}_p$ of the Galois group G_K is crystalline (we will recall the notion of crystalline representation in the next section). Thus, one may try to characterise good reduction of E using this theorem applied as previously to the p-adic representation $\pi_1^{p,\mathrm{ab}}(X_{K^{\mathrm{alg}}})$. However, this may not be possible. Indeed, the fundamental group $\pi_1^{(p)}(X)$ is considered just as a topological group, without any fixed surjection to the absolute Galois group G_K. Therefore, the quotient $\pi_1^{(p)}(X) \twoheadrightarrow G_K$, whose kernel may be reconstructed group theoretically, is determined only up to an automorphism of topological groups. On the other hand, the category of crystalline representations (considered as a full subcategory of all p-adic representations) is not necessarily preserved by the equivalence of categories induced by automorphisms of the topological group G_K. For example, it is known that there exist Hodge-Tate representations $G_K \to \mathrm{GL}(V)$ and an automorphism $G_K \cong G_K$ such that the composition $G_K \cong G_K \to \mathrm{GL}(V)$ is *not* a Hodge-Tate representation. This problem did not arise in the l-adic case simply because the subcategory of unramified representations is preserved by every automorphism of G_K. See also the discussion in [16]. Nevertheless, in the following we will use certain results from p-adic Hodge theory which will not be affected by the group of automorphisms of G_K and therefore are purely group theoretic.

Let us fix the notation used in this chapter. When X is a hyperbolic curve and Σ is a nonempty set of prime numbers, we have defined in Section 1.4 the maximally geometrically pro-Σ étale fundamental group Π_X of X. For the rest of this chapter, we will consider only the pro-p case hence we assume that $\Sigma = \{p\}$. Thus, we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(X_{K^{\mathrm{alg}}}) & \longrightarrow & \pi_1(X) & \longrightarrow & G_K & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \Delta_X & \longrightarrow & \Pi_X & \longrightarrow & G_K & \longrightarrow & 1, \end{array}$$

obtained as the pushout by the maximal pro-p quotient $\pi_1(X_{K^{\mathrm{alg}}}) \twoheadrightarrow \Delta_X$.

Let K be a local field. We denote by $\widehat{K^{\times p}}$ the inverse limit

$$\widehat{K^{\times p}} = \varprojlim_{n \geq 1} K^\times/(K^\times)^{p^n}.$$

Note that by Kummer theory we have

$$K^\times/(K^\times)^{p^n} \cong H^1(G_K, \mu_{p^n}),$$

therefore by taking the inverse limit over all natural numbers n we obtain

$$\widehat{K^{\times p}} \cong H^1(G_K, \mathbb{Z}_p(\mu)).$$

The kernel of the natural homomorphism of groups $K^\times \to \widehat{K^{\times p}}$ is equal to the group $\mu_K^{p'}$ of roots of unity of order prime to p contained in K. For every local field L we denote

$$L^{\times \mu} = L^\times/\mu_L^{p'},$$

the quotient of $L^\times$ by the subgroup of p'-roots of unity. Moreover, we have a natural isomorphism $U_L \cong \mathcal{O}_L^\times/\mu_L^{p'}$, where U_L denotes the group of principal units. Hence, we obtain injections $U_L \hookrightarrow L^{\times \mu} \hookrightarrow \widehat{L^{\times p}}$.

2.2 Reminder on p-adic Hodge Theory

In this section we recall a few basic facts from the theory of p-adic representations that we will use later.

Let k be a perfect field of characteristic p and denote by $W(k)$ the ring of Witt vectors over k. Let K be a finite totally ramified extension of the nonarchimedean complete field $W(k)[1/p]$. Let V be a finite dimensional vector space over $\mathbb{Q}_p$ equipped with a linear continuous G_K-action, where G_K is the absolute Galois group of K. We will simply say that V is a representation of G_K. Moreover, for every integer $n \in \mathbb{Z}$, we will denote by $V(n)$ the nth Tate twist of the representation V.

The general formalism of rings of periods is given as follows. Let B be a $\mathbb{Q}_p$-algebra domain equipped with a continuous and linear action of G_K. Then one can consider the functor $D_B : V \mapsto (B \otimes_{\mathbb{Q}_p} V)^{G_K}$ from the category of G_K-representations to the category of B^{G_K} modules. It naturally induces the G_K-equivariant comparison morphism of B-modules

$$\alpha : D_B(V) \otimes_{B^{G_K}} B \to V \otimes_{\mathbb{Q}_p} B$$

Assume now additionally that B is $(\mathbb{Q}_p, G_K)$-regular. This means that we have the equality $B^{G_K} = \mathrm{Frac}(B)^{G_K}$ and for every nonzero $b \in B$ such that the line

$\mathbb{Q}_p b$ is G_K-stable we have $b \in B^\times$. This obviously implies that the $\mathbb{Q}_p$-algebra B^{G_K} is a field, hence $D_B(V)$ is a vector space over B^{G_K}. Then, using the assumption of $(\mathbb{Q}_p, G_K)$-regularity, one proves that the morphism α is injective, in particular $\dim_{B^{G_K}} D_B(V) \leq \dim_K V$. Therefore, one defines a representation V to be B-admissible when the morphism α is an isomorphism, which is in fact equivalent to the equality $\dim_{B^{G_K}} D_B(V) = \dim_K V$. Every subrepresentation and every quotient of a B-admissible representation is also B-admissible. Moreover, the category of B-admissible representations in closed under the formation of tensor product and operation of taking the dual representation.

In the following we use three period rings, $\mathbf{B}_{\mathrm{cris}}$, $\mathbf{B}_{\mathrm{st}}$ and $\mathbf{B}_{\mathrm{dR}}$, whose admissible representations are called crystalline, semistable and de Rham, respectively (see, e.g., [14]). One has inclusions $\mathbf{B}_{\mathrm{cris}} \subset \mathbf{B}_{\mathrm{st}} \subset \mathbf{B}_{\mathrm{dR}}$, hence every crystalline representation is also semistable and every semistable representation is also de Rham. Moreover, a representation V is crystalline (semistable, de Rham) if and only if its restriction to the inertia subgroup $I_K \subset G_K$ is crystalline (semistable, de Rham, respectively), in particular every unramified representation is crystalline. The ring $\mathbf{B}_{\mathrm{dR}}$ is equipped with a decreasing filtration $\mathbf{B}_{\mathrm{dR}}^i$ for $i \in \mathbb{Z}$, in addition it satisfies the equality $\mathbf{B}_{\mathrm{dR}}^{G_K} = K$. Therefore, for every representation V the K-vector space $D_{\mathrm{dR}}(V)$ has the induced decreasing filtration of K-vector subspaces $D_{\mathrm{dR}}(V)^i$, for $i \in \mathbb{Z}$. Moreover, if the representation V is de Rham then V is also a Hodge-Tate representation and the dimension of the i-graded subquotient

$$D_{\mathrm{dR}}(V)^i / D_{\mathrm{dR}}^{i+1}(V)$$

is equal to the multiplicity of the weight i in the Hodge-Tate decomposition of V. Finally, the cyclotomic character $\mathbb{Q}_p(1)$ is a crystalline representation. The main property of these representations we are going to use is the following theorem which we have already mentioned in the introduction (see [11] for the good reduction case and [10] for the semi-stable case).

Theorem 2.2.1. *Let E be an elliptic curve over a p-adic local field K. Then, E has good reduction over K if and only if the representation $V_p(E)$ is crystalline. Moreover, when $p > 2$, then E has semi-abelian reduction over K if and only if the p-adic representation $V_p(E)$ is semistable.*

We also recall, following [7], the definition of crystalline, and semistable cohomology classes. Let V be a finite dimensional p-adic representation of G_K. The cohomology group $H^1(G_K, V)$ is a finite dimensional $\mathbb{Q}_p$-vector space. For a ring of periods B, we may consider the kernel of the natural map

$$H^1(G_K, V) \to H^1(G_K, V \otimes_{\mathbb{Q}_p} B).$$

When $B = \mathbf{B}_{\text{cris}}$, then cohomology classes lying the kernel of the above map are called crystalline and the kernel is denoted by $H^1_f(G_K, V)$. Similarly, when $B = \mathbf{B}_{\text{st}}$ then the kernel is denoted by $H^1_{\text{st}}(G_K, V)$ and a cohomology class lying in the kernel is called semistable. Consider now a cohomology class $\alpha \in H^1(G_K, V)$ and let

$$1 \to V \to W \to \mathbb{Q} \to 1$$

be the extension of representations corresponding to α, via the identification $H^1(G_K, V) = \text{Ext}^1_{\mathbb{Q}_p[G_K]}(\mathbb{Q}_p, V)$. Suppose now that the representation V is crystalline (semistable). Then, the representation W is crystalline (semistable) if and only if the cohomology class α is crystalline (semistable).

Lemma 2.2.2. *Let V be a two-dimensional p-adic representation fitting in the following exact sequence of G_K-modules*

$$1 \to \mathbb{Q}_p(1) \to V \to \mathbb{Q}_p \to 1.$$

Then, the representation V is semistable.

Proof. Consider the cohomology group $H^1(G_K, \mathbb{Q}_p(1))$. By Kummer theory, it is a $\mathbb{Q}_p$-vector space of dimension $[K : \mathbb{Q}_p] + 1$. From the computation of [7] (see the table in Example 3.9), we know that the subspace $H^1_f(G_K, \mathbb{Q}_p(1))$ of crystalline cohomology classes is a $\mathbb{Q}_p$-vector space of dimension $[K : \mathbb{Q}_p]$. Moreover, the extension of $\mathbb{Q}_p$ by $\mathbb{Q}_p(1)$ constructed from the Tate module of a Tate curve over K (which we will recall in the next section) is a semistable extension which is not crystalline (by Theorem 2.2.1). Therefore, the cohomology class of this extension generates a one dimensional $\mathbb{Q}_p$-vector subspace of the vector space $H^1(G_K, \mathbb{Q}_p(1))$, consisting of semistable classes, which is not contained in $H^1_f(G_K, \mathbb{Q}_p(1))$. Since the subspace of crystalline classes is of codimension one this implies that every class is semistable. □

In fact, we have a slightly stronger result.

Lemma 2.2.3. *Let V be a two-dimensional p-adic representation such that there exist one-dimensional unramified representations V' and V'' and an exact sequence of G_K-modules*

$$1 \to V'(1) \to V \to V'' \to 1.$$

Then, the representation V is semistable.

Proof. By tensoring with the dual of the character V'' we may assume that $V'' = \mathbb{Q}_p$. Moreover, by the previous lemma we may assume that the unramifed

character V' is nontrivial. We prove that in this case the representation V is in fact crystalline, hence also semistable.

For a p-adic representation W we write $h^i(W) = \dim_{\mathbb{Q}_p} H^1(G_K, W)$, similarly $h^i_f(W) = \dim_{\mathbb{Q}_p} H^1_f(G_K, V)$. Recall (see [34], Corollary 7.3.8), that the Euler characteristic of the representation W is equal to

$$h^0(W) - h^1(W) + h^2(W) = -[K : \mathbb{Q}_p] \dim_{\mathbb{Q}_p} W.$$

Moreover, it we denote by

$$W^* = \mathrm{Hom}_{\mathbb{Q}_p}(W, \mathbb{Q}_p)$$

the $\mathbb{Q}_p$-linear dual representation of W, then it follows from local Tate duality (see [34], Theorem 7.2.6), that

$$h^i(W) = h^{2-i}(W^*(1)), \text{ for } 0 \leq i \leq 2.$$

Since V' is a nontrivial unramified character we have $h^0(V'(1)) = 0$ and

$$h^2(V'(1)) = h^0((V')^*) = 0,$$

therefore $h^1(V'(1)) = [K : \mathbb{Q}_p]$. On the other hand, using [7], Corollary 3.8.4, for every de Rham representation W we have the equality

$$h^1_f(W) = h^0(W) + \dim_{\mathbb{Q}_p}(D_{\mathrm{dR}}(V)/D_{\mathrm{dR}}(V)^0).$$

The second term on the right hand side of the above formula is equal to the sum of negative Hodge-Tate weights of the representation W. In particular, it is invariant under twisting by unramified characters. Thus, for the unramified character V' we have

$$h^1_f(V'(1)) = h^1_f(\mathbb{Q}_p(1)) = [K : \mathbb{Q}_p].$$

Therefore, we obtain $h^1_f(V'(1)) = h^1(V'(1))$ which implies that

$$H^1_f(G_K, V'(1)) = H^1(G_K, V'(1)).$$

Thus, every cohomology class is crystalline and V is a crystalline representation.

□

2.3 Structure of p-adic Tate module

In this section we will recall basic properties of the p-adic Tate module of an elliptic curve over a p-adic field. Similar discussion would be valid in the more general case of abelian varieties. All the results are well known, e.g., see [39].

Let E be an elliptic curve over a p-adic local field K. We assume that E has split semi-abelian reduction over K i.e., the Néron model $\mathcal{E}$ of E, which is a smooth flat scheme over $\mathrm{Spec}(\mathcal{O}_K)$, has the special fibre $\mathcal{E}_k$ isomorphic to either an elliptic curve or to a split torus. Equivalently, the special fibre of the minimal Weierstrass model of E over $\mathcal{O}_K$ is either an elliptic curve or a split nodal pointed curve. In each case we are going to describe a G_K-module structure of the p-adic Tate module $T_p(E)$.

Suppose first that E has bad reduction. Since it also has split semi-abelian reduction we know that E is a Tate curve. Thus, there exists a unique element $q \in K^\times$ with $|q| < 1$ and an isomorphism $E \cong E_q$. Hence we also have a G_K-equivariant isomorphism $E(K^{\mathrm{alg}}) \cong (K^{\mathrm{alg}})^\times/q^{\mathbb{Z}}$. In particular, the group of n-torsion points is isomorphic to the subgroup of $(K^{\mathrm{alg}})^\times/q^{\mathbb{Z}}$ generated by the elements

$$\zeta_n^i q_n^j, \quad \text{for} \quad 0 \leq i, j \leq n-1,$$

where ζ_n is a primitive nth root of unity and q_n is an nth root of q. The elements ζ_n^i form a cyclic subgroup of $E[n](K^{\mathrm{alg}})$ which is G_K-invariant, hence we have a short exact sequence of G_K-modules

$$1 \to \langle \zeta_n \rangle \to E[n] \to E[n]/\langle \zeta_n \rangle \to 1.$$

Since for every $\sigma \in G_K$ we have $\sigma(q_n) = \zeta_n^i q_n$ for some natural number i, we see that the quotient $E[n]/\langle \zeta_n \rangle$ has trivial G_K-action. Moreover, the above short exact sequence is compatible with the multiplication map $E[nm] \to E[m]$. Therefore, by taking $n = p^k$, for every $k \geq 1$ and considering the inverse system with morphisms given by multiplication by p we obtain a short exact sequence

$$1 \to \varprojlim_{n \geq 1} \mu_n \to T_p(E) \to \varprojlim_{n \geq 1} \mathbb{Z}/n\mathbb{Z} \to 1.$$

The exactness on the right follows from finiteness of groups μ_n. Hence, by tensoring with $\mathbb{Q}_p$ we see that there exists a short exact sequence of p-adic representations of G_K

$$1 \to \mathbb{Q}_p(1) \to V_p(E) \to \mathbb{Q}_p \to 1.$$

Next, we are going to describe the good reduction case. Here we have two possibilities, either the elliptic curve E has ordinary reduction or it has supersingular reduction. Let $\mathcal{E}$ be the Néron model of E. Consider the p^i-torsion group scheme $\mathcal{E}[p^i]$, which is defined as the kernel of the homomorphism $p^i \colon \mathcal{E} \to \mathcal{E}$. It is a finite flat group scheme of order p^{2i} over $\mathrm{Spec}(\mathcal{O}_K)$, which is a local henselian scheme, therefore its connected component of identity $\mathcal{E}[p^i]^\circ$

is naturally a subgroup scheme. Then, we have a short exact sequence of finite flat group schemes

$$1 \to \mathcal{E}[p^i]^\circ \to \mathcal{E}[p^i] \to \mathcal{E}[p^i]^{\text{ét}} \to 1,$$

where the quotient $\mathcal{E}[n]^{\text{ét}}$ is étale over $\text{Spec}(\mathcal{O}_K)$. Here by a short exact sequence of finite flat group schemes over $\text{Spec}(\mathcal{O}_K)$ we mean the short exact sequence of corresponding sheaves in the flat topology. Thus, essentially by definition, for every natural number i the finite flat group scheme $\mathcal{E}[p^i]^{\text{ét}}$ has order p^i (is trivial) if and only if E has ordinary (supersingular) reduction. By looking at K^{alg}-points we obtain a short exact sequence of G_K-modules

$$1 \to \mathcal{E}[p^i]^\circ(K^{\text{alg}}) \to \mathcal{E}[p^i](K^{\text{alg}}) \to \mathcal{E}[p^i]^{\text{ét}}(K^{\text{alg}}) \to 1.$$

As the group $\mathcal{E}[p^i]^{\text{ét}}$ is finite étale, we have $\mathcal{E}[p^i]^{\text{ét}}(K^{\text{alg}}) = \mathcal{E}_k[p^i](k^{\text{alg}})$. Hence the subgroup $\mathcal{E}[p^i]^\circ(K^{\text{alg}}) \subset E(K^{\text{alg}})$ consists exactly of all p^i-torsion points such that their reduction to the special fibre $\mathcal{E}_k$ is equal to the origin O of the reduced elliptic curve $\mathcal{E}_k$. The above short exact sequence is compatible with the multiplication map on elliptic curve E. Therefore, since the groups $\mathcal{E}[p^i]^\circ(K^{\text{alg}})$ are finite for every $i \in \mathbb{N}$, after taking inverse limit we obtain a short exact sequence of G_K-modules

$$1 \to T_p(E)^\circ \to T_p(E) \to T_p(E)^{\text{ét}} \to 1.$$

Here we use the notation $T_p(E)^\circ = \varprojlim_{i\geq 1} \mathcal{E}[p^i]^\circ(K^{\text{alg}})$, similarly $T_p(E)^{\text{ét}} = \varprojlim_{i\geq 1} \mathcal{E}[p^i]^{\text{ét}}(K^{\text{alg}})$. After tensoring with $\mathbb{Q}_p$ we have a short exact sequence of G_K representations

$$1 \to V_p(E)^\circ \to V_p(E) \to V_p(E)^{\text{ét}} \to 1. \tag{2.1}$$

Because the p-divisible group $\mathcal{E}[p^i]^{\text{ét}}$ is étale over $\text{Spec}(\mathcal{O}_K)$, the action of G_K on the module $T_p(E)^{\text{ét}}$ is unramified.

Assume now that E has good ordinary reduction. Then, both G_K-modules $T_p(E)^\circ$ and $T_p(E)^{\text{ét}}$ are free $\mathbb{Z}_p$-modules of rank one. On the other hand, it follows easily from the Cartier duality together with the self-duality of elliptic curves that there exist a G_K-equivariant isomorphism

$$T_p(E)^\circ \cong \text{Hom}_{\mathbb{Z}_p}(T_p(E)^{\text{ét}}, \mathbb{Z}_p(1)).$$

Therefore, we obtain that in the ordinary case the short exact sequence (2.1) is of the form

$$1 \to \mathbb{Q}_p(\chi^{-1})(1) \to V_p(E) \to \mathbb{Q}_p(\chi) \to 1,$$

where χ is some unramified character.

Finally, we assume that the elliptic curve E has good supersingular reduction. Here, the only fact concerning the p-adic Tate module that we are going to use is the following lemma (see also [21], Lemma 8.1).

Lemma 2.3.1. *Suppose that E has good supersingular reduction. Then, there are no nontrivial I_K-equivariant homomorphisms $V_p(E) \to \mathbb{Q}_p$.*

Proof. Since the construction of connected-to-étale exact sequence is functorial with respect to unramified field extension we may assume that $I_K = G_K$. Let $V_p(E) \to \mathbb{Q}_p$ be any G_K-equivariant homomorphism. By replacing the elliptic curve E with some isogenous elliptic curve we may assume that the homomorphism $V_p(E) \to \mathbb{Q}_p$ of $\mathbb{Q}_p$-vector spaces comes from the homomorphism $T_p(E) \to \mathbb{Z}_p$ of $\mathbb{Z}_p$-modules. Since the functor from the category of p-divisible groups over $\mathrm{Spec}(K)$ to the category of $\mathbb{Z}_p[G_K]$-modules given by the Tate module is fully faithful we obtain a homomorphism $E[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p$ of p-divisible groups over the field K. Now, by the theorem of Tate (see [39], Theorem 4), it comes from a unique homomorphism

$$\mathcal{E}[p^\infty]_{\mathcal{O}_K} \to (\mathbb{Q}_p/\mathbb{Z}_p)_{\mathcal{O}_K}$$

of p-divisible groups over $\mathrm{Spec}(\mathcal{O}_K)$. On the other hand, a homomorphism from a connected group scheme to a constant group scheme must be trivial. Hence, the homomorphism $E[p^\infty] \to (\mathbb{Q}_p/\mathbb{Z}_p)_K$ of p-divisible groups over the generic fibre $\mathrm{Spec}(K)$ is trivial as well. Then, it follows that the map $T_p(E) \to \mathbb{Z}_p$ is also trivial. □

2.4 Potential type of reduction

In this section we are going to determine the potential type of reduction of the elliptic curve E from the topological group Π_X. This means determining whether the curve E has potentially good reduction or essentially bad reduction (i.e., has bad reduction after every finite field extension). Recall that the elliptic curve has essentially bad reduction if and only if after some finite field extension it is isomorphic to a Tate curve. To obtain the desired group theoretic description we will look at the Galois action on the p-adic Tate module.

Before we start, we discuss the following proposition which we have already mentioned in Chapter 1.

Proposition 2.4.1. *The prime number p together with a subgroup $\Delta_X \subset \Pi_X$ may be reconstructed group theoretically from the topological group Π_X.*

Proof. Consider the set S of all closed, normal subgroups H of Π_X which are topologically finitely generated pro-p groups. This set contains the subgroup Δ_X and is partially ordered by inclusion. We claim that the group Δ_X is in fact the greatest element in the partially ordered set S, which will provide the desired characterisation. Indeed, let H be any subgroup contained in the set S. Since for every two subgroups H_1 and H_2 from the set S their product H_1H_2 also belongs to S, we may assume that $\Delta_X \subset H$. Consider now the image $M \subset G_K$ of H by the surjection $\Pi_X \twoheadrightarrow G_K$. The group M is also closed, normal and topologically finitely generated pro-p subgroup of G_K. Let K^{tm} be the maximal tamely ramified extension of K and let $G_K^{\mathrm{tm}} = \mathrm{Gal}(K^{\mathrm{tm}}/K)$ be the Galois group of this extension. From the well-known structure of the group G_K^{tm} (see, [34], Theorem 7.5.3) it easily follows that the image of M by the quotient map $G_K \twoheadrightarrow G_K^{\mathrm{tm}}$ is trivial, therefore K must be contained in the wild inertia subgroup $G_K^{\mathrm{wild}} \subset G_K$. On the other hand, the group G_K^{wild} is a free pro-p group of infinite rank (see, [34], Proposition 7.5.1), hence it has no nontrivial closed normal subgroups which are topologically finitely generated. Thus, the group M is trivial, hence $H = \Delta_X$. □

Proposition 2.4.2. *The potential type of reduction of the elliptic curve E (i.e., potentially good or essentially bad) may be recovered group theoretically from the topological group Π_X.*

Proof. Let F be a field extension of K such that every elliptic curve over K acquires split semi-abelian reduction after the base change to F, as in the discussion after Lemma 1.8.1. Thus, by extending the base field K to F (which is independent of the curve E), we may assume that the elliptic curve E has split semi-abelian reduction. Now, we observe that E has bad reduction if and only if there exists a G_K-equivariant surjection $V_p(E) \twoheadrightarrow \mathbb{Q}_p$. Indeed, if E has bad reduction then the description of the Tate module given previously provides us with such homomorphism. On the other hand, assume that E has good reduction and let φ a G_K-equivariant homomorphism $\varphi\colon V_p(E) \to \mathbb{Q}_p$. We are going to prove that every such homomorphism is trivial. If the reduction is supersingular then we have already seen in Lemma 2.3.1 that the homomorphism φ must be trivial. Suppose now that the reduction is ordinary. Then, as we have seen in Section 2.3, there exists a short exact sequence

$$1 \to \mathbb{Q}_p(\chi^{-1})(1) \to V_p(E) \to \mathbb{Q}_p(\chi) \to 1$$

of G_K-modules, where χ is an unramified character. After restricting to the inertia subgroup $I_K \subset G_K$ we have a short exact sequence

$$1 \to \mathbb{Q}_p(1) \to V_p(E) \to \mathbb{Q}_p \to 1$$

of I_K-modules. Since the restriction of p-adic cyclotomic character to the inertia subgroup is nontrival, every homomorphism $V_p(E) \to \mathbb{Q}_p$ must be trivial on the submodule $\mathbb{Q}_p(\chi^{-1})(1)$, hence it factorizes through the quotient $\mathbb{Q}_p(\chi)$. Thus, φ is trivial if and only if the character χ is nontrivial. Since $\mathbb{Q}_p(\chi)$ is isomorphic to the Tate module of the reduced curve E_k we see that this action must be nontrivial, otherwise it would imply the existence of infinitely many p-power torsion points defined over the finite field k, which is absurd. □

Proposition 2.4.3. *Assume that the elliptic curve E has potentially good reduction. Then, from the topological group Π_X we may determine whether the potential reduction of E is supersingular or ordinary.*

Proof. As previously, we may extend the base field and assume that the elliptic curve E has good reduction. Then we observe that the reduction is ordinary if and only if there exists a surjective homomorphism $T_p(E) \twoheadrightarrow \mathbb{Z}_p$ of I_K-modules. Indeed, if the reduction is ordinary then it follows from the description of the p-adic Tate module of E. On the other hand, if the reduction is supersingular we have seen that every homomorphism to the trivial representation must be trivial. □

Proposition 2.4.4. *Assume that $p > 2$ and E has potentially good ordinary reduction. Then, we may determine from the topological group Π_X whether the elliptic curve E has good reduction over the field K.*

Proof. We claim that E has good reduction over K if and only if there exists of short exact sequence of G_K-modules

$$1 \to W(1) \to V_p(E) \to V \to 1, \tag{2.2}$$

where W and V are unramified representations. As we have seen, this condition is necessary. We now prove that it is also sufficient. Suppose that we have a sequence of representations as in (2.2). Then, using Corollary 2.2.3 we obtain that the p-adic representation $V_p(E)$ is semistable. Moreover, by Theorem 2.2.1, this implies that the elliptic curve E has semi-abelian reduction over the field K. Finally, it is easy to see that potentially good reduction and semi-abelian reduction over K together imply good reduction over K. □

Summarizing, by looking at the Tate module of E, we were able to determine group theoretically the potential reduction type of E, i.e, the reduction type of the curve E_F with F/K as in the proof of Proposition 2.4.2. Moreover, in the case when the curve E_F does have good ordinary reduction and $p > 2$, we were able to distinguish when the good model of E_F descends to the good model of

E over K. Therefore, we have reduced the original problem to the problem of finding a group theoretic criterion for a descent of the good model from F to K in the case of good supersingular reduction.

2.5 Tangential sections

In this section we recall the notion of a tangential section associated to a cusp of a hyperbolic curve and its relation to the integral model of the curve.

First we consider the following elementary situation arising in group theory. Let G be a group, A an abelian group and suppose that we have a short exact sequence of groups

$$1 \to A \to \Pi \xrightarrow{p} G \to 1.$$

Then, the conjugaction by Π determines an action $\Pi \to \mathrm{Aut}(A)$ descending to a natural action $G \to \mathrm{Aut}(A)$. Therefore the abelian group A in naturally a G-module. Denote by $Sect(\Pi, G)$ the set of all sections of the surjection $\Pi \twoheadrightarrow G$. This set has a natural left action of the group A given by conjugating sections by elements from A. Let $A \setminus Sect(\Pi, G)$ be the quotient of the set of sections by this action. Finally, denote by C the subset of all cohomology classes in $H^1(\Pi, A)$ such that their image under the restriction map

$$H^1(\Pi, A) \to H^1(A, A) = \mathrm{Hom}(A, A)$$

is equal to the identity homomorphism. Then, we have the following well-known lemma.

Lemma 2.5.1. *There is a natural bijection of sets $C \simeq A \setminus Sect(\Pi, G)$ given explicitly by as follows.*

- *If $[a_\pi] \in C \subset H^1(\Pi, A)$ is a cohomology class, then we define the corresponding section $s\colon G \to \Pi$ by the formula $g \mapsto (a_\pi)^{-1}\pi$, where $\pi \in \Pi$ is any element such that $p(\pi) = g$.*
- *If $s\colon G \to \Pi$ is a section of the surjection $\Pi \twoheadrightarrow G$, then we define the corresponding cocycle a_π by the formula $a_\pi = \pi s(p(\pi^{-1}))$.*

Proof. We include the proof for convenience of the reader. Let s be a section and for every $\pi \in \Pi$ we define $a_\pi \in A$ by the formula $\pi = a_\pi s(p(\pi))$. By definition, we have

$$a_{\pi\pi'} s(p(\pi\pi')) = \pi\pi' = a_\pi s(p(\pi)) a_{\pi'} s(p(\pi')).$$

Since s is a homomorphism we obtain

$$a_{\pi\pi'} s(p(\pi)) = a_\pi s(p(\pi)) a_{\pi'},$$

thus $a_{\pi\pi'} = a_\pi a_{\pi'}^\pi$ and $\pi \mapsto a_\pi$ is a cocycle. It is obvious that a_π is the identity on homomorphism A. For $\alpha \in A$, consider the conjugated section $s' = s^\alpha$ with the corresponding cocycle b_π. We compute

$$\pi = b_\pi s'(p(\pi)) = b_\pi \alpha s(p(\pi)) \alpha^{-1} = b_\pi a_\pi^{-1} \alpha \pi \alpha^{-1},$$

therefore $a^\pi a^{-1} = b_\pi a_\pi^{-1}$, hence the classes $[a_\pi] = [b_\pi]$ are equal.

Let now $[a_\pi]$ be a cohomology class in $H^1(\Pi, A)$ defined by a cocycle $\pi \mapsto a_\pi$ such that its restriction to A induces the identity homomorphism. Define the section $s\colon G \to \Pi$ as $s(g) = a_\pi^{-1}\pi$, where π is a lift of g to Π. It is well defined since if π' is another lift of g then we have $\pi' = \alpha\pi$ for some $\alpha \in A$, hence

$$a_{\pi'}^{-1}\pi' = a_\pi^{-1}\alpha^{-1}\alpha\pi = a_\pi^{-1}\pi.$$

We need to check that s is a group homomorphism. Fix $g, g' \in G$ with lifts π and π' respectively, then

$$s(gg') = a_{\pi\pi'}^{-1}\pi\pi' = (a_{\pi'}^{-1})^\pi a_\pi^{-1}\pi\pi' = \pi a_{\pi'}^{-1}\pi^{-1} s(g)\pi'.$$

Hence using that $\pi^{-1}s(g) \in A$ we obtain after rearranging $s(g)s(g')$.

Moreover, let a cocycle b_π be cohomologous to a_π, thus we may write $b_\pi = a_\pi \alpha^\pi \alpha^{-1}$. Let s' be a section obtained from the cocycle b_π, then we compute

$$s'(g) = \alpha(\alpha^{-1})^\pi a_\pi^{-1}\pi = \alpha\pi\alpha^{-1}\pi^{-1}s(g) = \alpha s(g)\alpha.$$

Therefore s' is a conjugate section of s. It is now easy to check that the both maps constructed above are inverses of each other. □

After this preliminary discussion, we recall the local structure of fundamental groups at the cusps. Let X be an affine hyperbolic curve over a local field K and let $\overline{X}$ be the unique smooth compactification of X. Therefore, we have a surjection of pro-p fundamental groups $\Delta_X \twoheadrightarrow \Delta_{\overline{X}}$ as well as a surjection of geometrically pro-p fundamental groups $\Pi_X \twoheadrightarrow \Pi_{\overline{X}}$.

Let x be a (K-rational) cusp of the hyperbolic curve X over K, denote by $D \subset \Pi_X$ its decomposition group and by $I = D \cap \Delta_X$ its inertia group. Then, we have a short exact sequence

$$1 \to I \to D \to G_K \to 1.$$

The group I is isomorphic to $\mathbb{Z}_p(1)$ as a G_K-module. Here we recall the definition of a tangential section.

Definition 2.5.2. We say that a section s of the surjection $\Pi_X \twoheadrightarrow G_K$ is *tangential* at the cusp x if its image lies in some decomposition group of the cusp x, i.e., if s comes (up to conjugation) from the section of the surjection $D \twoheadrightarrow G_K$.

Therefore, the set of tangential sections at the cusp x is a torsor over the group $H^1(G_K, I) \cong \widehat{K^{\times p}}$.

Let $\mathcal{O}_{\overline{X},x}$ be the local ring at the point x with the maximal ideal $\mathfrak{m}_x$. Define K_x to be the fraction field of the completion of $\mathcal{O}_{\overline{X},x}$ with respect to $\mathfrak{m}_x$-adic topology

$$K_x = \mathrm{Frac}(\widehat{\mathcal{O}_{\overline{X},x}}).$$

From the Cohen structure theorem, the field K_x is (noncanically) isomorphic to the field of Laurent series $K((T))$ with coefficients in K. In fact, K_x has the structure of a two dimensional local field. Let G_x be the absolute Galois group of the field K_x (defined with respect to some algebraic closure K_x^{alg}). The natural inclusion $K \hookrightarrow K_x$ induces a surjection $G_x \twoheadrightarrow G_K$. Define Δ_x to be the kernel of this surjection, hence we have a short exact sequence of groups

$$1 \to \Delta_x \to G_x \to G_K \to 1.$$

The group Δ_x may be identified with the absolute Galois group of the tensor product $F_x = K_x \otimes_K K^{\mathrm{alg}}$ and is (again, noncanonically) isomorphic as a G_K-module to the group $\widehat{\mathbb{Z}}(1)$. Then, the group D may be identified with the quotient of the absolute Galois group G_x such that the induced quotient $\Delta_x \twoheadrightarrow I$ is equal to the maximal pro-p quotient, i.e. we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_x & \longrightarrow & G_x & \longrightarrow & G_K & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & I & \longrightarrow & D & \longrightarrow & G_K & \longrightarrow & 1 \end{array}$$

The quotient $G_x \twoheadrightarrow D$ corresponds to the Galois group of the field extension L_x/K_x, where L_x is the maximal pro-p extension of the field F_x. Therefore, sections of the surjection $D \twoheadrightarrow G_K$ may be identified with field subextensions $K_x \subset M \subset L_x$ satisfying $\mathrm{Gal}(L_x/M) \cong G_K$.

Extensions of this form can be easily constructed as follows. Let $t \in \mathfrak{m}_x \setminus \mathfrak{m}_x^2$, choose a compatible system t^{1/p^i} of p-power roots of t and define the field

$$M_t = \bigcup_{i \geq 1} K_x(t^{1/p^i}).$$

One easily checks that this field satisfies $\mathrm{Gal}(L_x/M_t) \cong G_K$, hence it defines a tangential section $s_t \colon G_K \to D$. Moreover, different choices of a compatible

system of roots of t correspond to conjugating the section s_t by the elements of the group I. Therefore, the conjugacy class of the section s_t does not depend on this choice.

Let U_x be the multiplicative group $1+\widehat{\mathfrak{m}}_x$, where $\widehat{\mathfrak{m}}_x$ is the maximal ideal $\mathfrak{m}_x\widehat{\mathcal{O}_{\overline{X},x}}$ of the local ring $\widehat{\mathcal{O}_{\overline{X},x}}$. We easily observe that the group U_x is divisible. Thus, for any two uniformizers satisfying $t \equiv t' \mod \widehat{\mathfrak{m}}_x^2$ we have $M_t = M'_t$, for some choice of a compatible system of roots. This implies that the sections s_t and $s_{t'}$ are in the same conjugacy class. Therefore, the conjugacy class of a section s_t depends only on the cotangent vector $\bar{t} \in \widehat{\mathfrak{m}}_x/\widehat{\mathfrak{m}}_x^2$. Let

$$T_K^\vee = \widehat{\mathfrak{m}}_x/\widehat{\mathfrak{m}}_x^2 = \mathfrak{m}_x/\mathfrak{m}_x^2$$

denotes the cotangent space at the point x. For a nonzero vector ω from the one dimensional K-vector space $T_K^\vee$, we define a conjugacy class of tangential section s_ω as conjugacy class of a section s_t, where t is a lift of ω to the maximal ideal $\mathfrak{m}_x$. Thus, we obtain a well defined map of sets

$$T_K^\vee \setminus \{0\} \longrightarrow \{\text{conjugacy classes of sections of } D \twoheadrightarrow G_K\}.$$

Definition 2.5.3. We say that the tangential section $s\colon G_K \to D$ is *discrete* if its conjugacy class is equal to a conjugacy class of a section s_ω for some nonzero cotangent vector ω in $T_K^\vee$.

The set of sections of the surjection $D \twoheadrightarrow G_K$ is a torsor over the group $\widehat{K^{\times p}} \cong H^1(G_K, I)$, whereas the set of nonzero differentials ω is a $K^\times$-torsor. One easily observes that these torsor structures are compatible with the natural map $K^\times \to \widehat{K^{\times p}}$, in other words for every $a \in K^\times$ and $w \in T_K^\vee$ we have $as_\omega = s_{a\omega}$. Indeed, the description of the torsor structure of tangential sections is given as follows. Let a be an element of $\widehat{K^{\times p}}$ which defines a sequence of elements $a_i \in K^\times/(K^\times)^{p^i}$ satisfying $a_j = a_i \mod (K^\times)^{p^i}$ for $j \geq i$. Moreover, let t be a uniformizer with the corresponding section s_t. Then, consider the field extension

$$L_a = \bigcup_{i\geq 1} K_x(b_i t^{1/p^i}),$$

where $b_i^{p^i} = a_i$. By construction, this field extension defines the section s_t^a, hence the compatibility follows. Therefore the set of discrete sections is naturally a $K^{\times\mu}$-torsor.

Suppose now that the hyperbolic curve X has stable reduction over K and denote by $\mathcal{X}$ the stable model of X over $\mathcal{O}_K$. Then, the one dimensional cotangent space $T_K^\vee$ has a canonical $\mathcal{O}_K$-submodule $T_{\mathcal{O}_K}^\vee$ of rank 1 determined by the stable model $\mathcal{X}$ at x. Thus, the set of generators of this $\mathcal{O}_K$-submodule is a $\mathcal{O}_K^\times$-torsor.

Definition 2.5.4. Assume that the curve X has stable reduction over K (see [18]). We say that the tangential section $s\colon G_K \to D$ is *integral* if it is equal to a discrete section s_ω for a cotangent vector ω contained in the $\mathcal{O}_K^\times$-torsor of generators of the $\mathcal{O}_K$-module $T^\vee_{\mathcal{O}_K}$. We say that a uniformizer $t \in \mathfrak{m}_x$ is *integral* if the section s_t is integral. Similarly, we say that a differential $\omega \in T^\vee_K$ is *integral* if the section s_ω is integral.

Obviously the set of integral sections is a U_K-torsor. For a tangential section s we may consider its restriction to an open subgroup $G_L \subset G_K$ which determines a tangential section s_L at the unique lift of the cusp x to the curve X_L. Then we have the following lemma.

Lemma 2.5.5. *Assume that the curve X has stable reduction over $\mathcal{O}_K$. Then, the section s is integral if and only if the section s_L is integral.*

Proof. When s is integral then the section s_L is integral as well. Indeed, it follows immediately from the compatibility of stable models with base change. Suppose now that the section s_L is integral. Choose any integral section s' of $D \twoheadrightarrow G_K$ and let s'_L be its restriction to G_L, which is also integral. Then, we have $s = as'$ for some $a \in \widehat{K^{\times p}}$, as well as $s_L = bs'_L$ for some $b \in U_L$, since both sections s_L and s'_L are integral. Therefore, by restricting the first equality to G_L we obtain $a = b$. On the other hand, it is easy to check that $U_L \cap \widehat{K^{\times p}} = U_K$, therefore a belongs to U_K. It implies that s is an integral section. □

We will need to compare the cohomology class associated to a cuspidal section with certain Kummer classes. First, fix a cotangent vector ω in $T^\vee_K$ and let s_ω be a discrete tangential section associated to ω. Denote by α the cohomology class in $H^1(D, I)$ determined by s_ω using bijection from Lemma 2.5.1. On the other hand, using the differential ω we may construct another cohomology class in the following way. Choose a regular function f on U, where U is an open subscheme of X, with simple zero at the cusp x and inducing the cotangent vector ω. Hence we obtain the Kummer class $\eta_f \in H^1(\Pi_U, \mathbb{Z}_p(\mu))$ of the function f. Consider now the following composition

$$H^1(\Pi_U, \mathbb{Z}_p(\mu)) \to H^1(D, \mathbb{Z}_p(\mu)) \cong H^1(D, I),$$

where the first map is the restriction and the second comes from the natural isomorphism $\mathbb{Z}_p(\mu) \cong I$. Let β be the image in $H^1(D, I)$ of the Kummer class η_f by this composition.

Lemma 2.5.6. *The cohomology classes α and β are equal.*

Proof. This follows easily from the construction, once we recall all the definitions. Indeed, let t be a uniformizing element lifting the cotangent vector ω. Then the restriction of the Kummer class of f to the cohomology group $H^1(D, \mathbb{Z}_p(\mu))$ is equal to the cohomology class associated to the projective limit of cocycles

$$D \ni \pi \mapsto \frac{\pi(t^{1/n})}{t^{1/n}} \in \mu_n.$$

On the other hand, let s be the tangential section determined by the cotangent vector ω. Then, by definition, the cohomology class in $H^1(D, I)$ associated to s is represented by the cocycle $\pi \mapsto a_\pi$ where a_π satisfies the equality $\pi = a_\pi s(p(s))$. Here, p denotes the projection $p\colon D \twoheadrightarrow G$. Recall that the section s was constructed using certain quotient of the absolute Galois group of the field $M_t = \bigcup_{i\geq 1} K_x(t_\omega^{1/p^i})$ for some choice of a compatible system of roots of t. In particular, by replacing s by some conjugate section we may assume that the image of s acts trivially on the field M_t. Therefore, we obtain the equality

$$\frac{\pi(t^{1/n})}{t^{1/n}} = \frac{a_\pi(t^{1/n})}{t^{1/n}}.$$

Moreover, by the construction of the natural isomorphism $I \cong \mathbb{Z}_p(\mu)$ we see that the element on the right hand side of the above equality corresponds to the image of a_π in the quotient I/nI. Therefore, by taking inverse limit we obtain that the cohomology class of β is represented by the cocycle $\pi \mapsto a_\pi$, hence it is equal to the class determined by α. □

Remark 2.5.7. We easily observe that results analogous to those stated in this section remain valid also in the case of the full fundamental group $\pi_1(X)$ and its tangential sections. Indeed, instead of considering the quotient $\Delta_x \twoheadrightarrow I$, we may simply work with the full group $\Delta_x \cong \widehat{\mathbb{Z}}(1)$.

2.6 Cohomology classes of integral functions

To analyse the case of potentially good reduction we will need to introduce cohomology classes of certain special functions.

Let E be an elliptic curve over the local field K and X be the hyperbolic curve $E \setminus \{O\}$. Let $v\colon (K^{\mathrm{alg}})^\times \to \mathbb{Q}$ be the standard additive valuation with $v(p) = 1$. Choose a minimal Weierstarss equation of E over K

$$y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_2x + a_6, \tag{2.3}$$

thus the coefficients a_i are integral. We fix the minimal Weierstrass equation (2.3) and when we refer to the function x it is always understood the be the chosen coordinate function.

Let P be a nonzero torsion point of p-power order and denote by $K(P)$ the field extension of K obtained by adding coordinates of the point P. Finally, let L be any field extension containing $K(P)$. Similarly as in the previous chapter, we consider the $L^\times$-torsor of standard functions associated to the point P as the set of all rational functions on E_L with only one pole of order two at the origin and with single zero at the point P. Moreover, recall that in the case when E has stable reduction we have also defined the $\mathcal{O}_L^\times$-torsor of integral standard functions associated to the point P, as the set of all functions of the form $u(x - x(P))$, where $u \in \mathcal{O}_L^\times$.

Assume that the point P has order p^n and let X_n be the open subscheme of E obtained by removing all p^n-torsion points. Let L/K be a field extension such that all p^n-torsion points are L-rational. Using elliptic cuspidalization from Section 1.7 in the pro-p case we may reconstruct the surjection $\Pi_{X_n} \twoheadrightarrow \Pi_X$ of topological groups. Then, by applying Kummer theory as in the proof of Lemma 1.8.3, we reconstruct the $H^1(G_L, M_X^{(p)})$-orbit of the set of cohomology classes of standard functions associated to p^n-torsion points, as a subset of the cohomology group $H^1(\Pi_{X_n}, M_X^{(p)})$. This orbit is a torsor over the cohomology group

$$H^1(G_L, M_X^{(p)}) \cong \widehat{L^{\times p}}$$

and may be thought of as a set of functions of the form $a(x - x(P))$, where $a \in \widehat{L^{\times p}}$. Cohomology classes contained in this $\widehat{L^{\times p}}$-torsor will be called *profinite*, we will also call them profinite standard functions. Classes corresponding to the image of standard functions under the Kummer map will be called *standard* classes, they form a $L^{\times \mu}$-torsor. Similarly, when E has stable reduction, then classes corresponding to the image of integral standard function will be called *integral*, they form a U_L-torsor.

It will be convenient to introduce certain colimit of cohomology groups which contains Kummer classes of all standard functions associated to p-power torsion points. Observe that for each pair of natural numbers $m \geq n$, elliptic cuspidalization also constructs the surjection $\Pi_{X_m} \twoheadrightarrow \Pi_{X_n}$ coming from the open immersion $X_n \hookrightarrow X_m$. Therefore, by using the injective inflation map

$$H^1(\Pi_{X_n}, M_X^{(p)}) \hookrightarrow H^1(\Pi_{X_m}, M_X^{(p)}),$$

we may always consider cohomology classes in $H^1(\Pi_{X_n}, M_X^{(p)})$ as elements of $H^1(\Pi_{X_m})$. Next, for every finite field extension L/K we write $\Pi_{X_n,L}$ for the preimage of G_L under the surjection $\Pi_{X_n} \twoheadrightarrow G_K$. Then, observe that the restriction map

$$H^1(\Pi_{X_n}, M_X^{(p)}) \hookrightarrow H^1(\Pi_{X_n,L}, M_X^{(p)})$$

is in fact injective, hence we may consider $H^1(\Pi_{X_n}, M_X^{(p)})$ as a subgroup of the group $H^1(\Pi_{X_n,L}, M_X^{(p)})$. Finally, we introduce the following colimit

$$C(X) = \varinjlim_{L/K} \varinjlim_{n\in\mathbb{N}} H^1(\Pi_{X_n,L}, M_X^{(p)})$$

over all natural numbers and finite extensions L/K. Therefore, it follows from the construction that we may regard the Kummer class of every rational function on X with divisor supported at the set of p-power torsion points as an element of $C(X)$. Moreover, by considering colimit of $\widehat{L^{\times p}}$-torsors of profinite standard functions associated to p-power torsion points over all finite extensions L/K we obtain a $K^{\wedge\infty}$-torsor of profinite standard functions in $C(X)$, where

$$K^{\wedge\infty} = \varinjlim_{L/K} \widehat{L^{\times p}}.$$

Similarly, defining

$$K^{\infty} = \varinjlim_{L/K} L^{\times p}, \quad U^{\infty} = \varinjlim_{L/K} U_L$$

and taking colimits of corresponding torsors we obtain a K^{∞}-torsor of discrete classes as well as U^{∞}-torsor of integral classes of standard functions, both contained in $C(X)$.

Let P and Q be two nonzero p-power torsion points and let $f = a(x - x(P))$ and $g = b(x - x(Q))$, for some $a, b \in (K^{\mathrm{alg}})^{\times}$, be two standard functions associated to points P and Q, respectively. We say that f and g are *equivalent* if the element $ab^{-1} \in (K^{\mathrm{alg}})^{\times}$ is a root of unity. We easily see that this notion does not depend on the choice of minimal Weierstrass equation and indeed it is an equivalence relation. Similarly, when $f = a(x - x(P))$ and $g = b(x - x(Q))$, for some $a, b \in K^{\wedge\infty}$, are two profinite classes associated to P and Q we say that the classes f and g are *equivalent* if the element $ab^{-1} \in K^{\wedge\infty}$ is torsion. Observe that the Kummer classes of two standard functions are equivalent if and only if these two functions are equivalent. Indeed, it follows from the fact that for every local field L the kernel of the map $L^{\times} \to \widehat{L^{\times p}}$ is contained in the group of roots of unity. Moreover, it is easy to see that for $P \neq Q$, profinite classes f and g are equivalent if and only if $f(Q)g(P)^{-1}$ is a torsion element in the group $K^{\wedge\infty}$. The next lemma shows that the above notion of equivalence is group theoretical.

Lemma 2.6.1. *From the topological group Π_X we may reconstruct equivalence classes of profinite standard functions, considered as cohomology classes inside the colimit $C(X)$.*

Proof. Pick any two torsion points P and Q as above and two profinite standard function f_P and f_Q associated to these two points. We need to determine whether they are equivalent. Fix some decomposition groups D_P and D_Q of points P and Q. For m large enough, consider the evaluation maps

$$H^1(\Pi_{X_m}, M_X^{(p)}) \to H^1(D_P, M_X^{(p)}) \cong H^1(G_L, M_X^{(p)})$$

and

$$H^1(\Pi_{X_m}, M_X^{(p)}) \to H^1(D_Q, M_X^{(p)}) \cong H^1(G_L, M_X^{(p)}),$$

for some sufficiently large finite field extension L/K.

By evaluating the functions f_P and f_Q at points Q and P we obtain two elements $f_P(Q)$ and $f_Q(P)$ of the group $H^1(G_L, M_X^{(p)}) \cong \widehat{L^{\times p}}$. Then, as we have seen, f_P is equivalent to f_Q if and only if the element $f_P(Q)f_Q(P)^{-1}$ is torsion in the group $H^1(G_L, M_X^{(p)})$. □

To compute the evaluations of standard functions, we need to use pro-p version of the group theoretical valuation homomorphism (1.6). Recall, that we have the natural isomorphisms

$$M_X^{\Sigma} \cong \widehat{\mathbb{Z}}^{\Sigma}(\mu) \cong \widehat{\mathbb{Z}}^{\Sigma}(G),$$

thus in the pro-p case we obtain the isomorphisms

$$M_X^{(p)} \cong \mathbb{Z}_p(\mu) \cong \mathbb{Z}_p(G_K).$$

We refer to the above isomorphism $M_X^{(p)} \cong \mathbb{Z}_p(G_K)$ of topological G_K-modules as *canonical rigidity isomorphism*. It induces a homomorphism

$$H^1(G_K, M_X^{(p)}) \cong H^1(G_K, \mathbb{Z}_p(G_K)) \twoheadrightarrow \mathbb{Z}_p,$$

where the second map has a group theoretical construction. When L/K is a finite extension, then the inclusion $G_L \subset G_K$ induces a natural isomorphism $\mathbb{Z}_p(G_L) \cong \mathbb{Z}_p(G_K)$ of G_L-modules. Thus, we may consider the following colimit

$$K^{\wedge\infty}(G_K) = \varinjlim_{L/K} H^1(G_L, \mathbb{Z}_p(G_L)),$$

as well as

$$K^{\wedge\infty}(M_X) = \varinjlim_{L/K} H^1(G_L, M_X^{(p)}).$$

Thus, by taking colimit of over finite extensions L/K we obtain homomorphisms

$$K^{\wedge\infty}(M_X) \cong K^{\wedge\infty}(G_K) \twoheadrightarrow \mathbb{Q}_p. \tag{2.4}$$

We will refer to the above diagram as valuation map. Observe that the set of all isomorphisms $\alpha\colon M_X^{(p)} \cong \mathbb{Z}_p(G_K)$ of G_K-modules has a natural torsor structure under the group $\mathbb{Z}_p^\times$, with a trivialization given by the canonical rigidity isomorphism. In particular, the knowledge of the canonical rigidity isomorphism is equivalent to the knowledge of the above valuation map.

We now assume that the elliptic curve E has good supersingular reduction over K. Let $P \in E(K^{\mathrm{alg}})$ be a torsion point of p-power order. Since the p-divisible group of the reduced curve is connected, it has no nontrival field-valued points, hence the image of P under the reduction map

$$E(K^{\mathrm{alg}}) = E(\mathcal{O}_{K^{\mathrm{alg}}}) \to E_k(k^{\mathrm{alg}})$$

is trivial. In other words, using the equation (2.3), if P is represented in homogeneous coordinates by

$$[X_P\colon Y_P\colon Z_P],$$

where X_P, Y_P and Z_P are integral and are not all contained in the maximal ideal of $\mathcal{O}_K$, then we have $v(X_P) < 0$ and $v(Z_P) < 0$, while $v(Y_P) = 0$. Therefore, going back to inhomogeneous coordinates $P = (x(P), y(P))$ one obtains $v(x(P)) < 0$. Moreover, by comparing absolute values in the equation (2.3) we also obtain $v(y(P)) < 0$, in fact $v(x(P)) = -2a$ and $v(y(P)) = -3a$ for some positive rational number a. Therefore, it follows from the transformation formula for Weierstrass equation that the value $v(x(P))$ is in fact independent of the choice of a minimal Weierstarss equation.

We are going to use a result from [38], which bounds the value $v(x(P))$ from below. The formulation we will need is the following lemma, which is a key technical fact in the theory of this chapter.

Lemma 2.6.2. *Let $P = (x(P), y(P))$ be a torsion point on the elliptic curve (2.3) of the exact order p^n, for some natural number n. Then, we have the following inequality*

$$0 > v(x(P)) \geq -\frac{2}{p^n - p^{n-1}}.$$

Proof. We have already seen that the first inequality holds. The second one is just a reformulation of [38] Chapter VII, Theorem 3.4, once we compare our notation. Let $L = K(E[p^n])$ be the field extension obtained by adding coordinates of all torsion points of E of order p^n. Let π be the uniformizing element of L and let $e = e(L/\mathbb{Q}_p)$ be the absolute ramification degree of the field L. Then, [38] says that we have $\pi^{2r}x(P) \in \mathcal{O}_L$, where

$$r = \left\lfloor \frac{e}{p^n - p^{n-1}} \right\rfloor$$

Since $v(\pi) = 1/e$, it is equivalent to $2r/e + v(x(P)) \geq 0$. On the other hand,

$$\frac{2r}{e} \leq \frac{2e}{e(p^n - p^{n-1})} = \frac{2}{p^n - p^{n-1}},$$

which is exactly the statement of the lemma. □

We immediately obtain the following corollary which is crucial for our recovery of the reduction type in the supersingular case.

Corollary 2.6.3. *Let E be an elliptic curve with good supersingular reduction. For every natural number n, let P_n be a torsion point on the elliptic curve E of exact order p^n. Then, we have*

$$\lim_{n\to\infty} v(x(P_n)) = 0,$$

where x is a rational function from the minimal Weierstrass equation (2.3).

We now go back to the discussion of the canonical rigidity isomorphism. Let $\mathbb{Q}^\times_{(p)}$ be a subgroup of the group $\mathbb{Q}^\times$ consisting of all rational numbers a/b, where a, b are nonzero and relatively prime, such that ab is not divisible by p. The group $\mathbb{Q}^\times_{(p)}$ may be considered as a subgroup of the group $\mathbb{Z}_p^\times$. The next proposition reflects the difference between the profinite and pro-p cases.

Proposition 2.6.4. *Assume that the elliptic curve E has good supersingular reduction. Then, the $\mathbb{Q}^\times_{(p)}$-orbit of the canonical rigidity isomorphism of cyclotomes $M_X^{(p)} \cong \mathbb{Z}_p(G_K)$ may be reconstructed group theoretically.*

Proof. Observe that for any choice of an isomorphism $\alpha\colon M_X^{(p)} \cong \mathbb{Z}_p(G_K)$ inducing an isomorphism $\alpha_*\colon K^{\wedge\infty}(M_X) \to K^{\wedge\infty}(G_K)$, the kernel of the composition

$$K^{\wedge\infty}(M_X) \xrightarrow{\alpha_*} K^{\wedge\infty}(G_K) \twoheadrightarrow \mathbb{Q}_p$$

does not depend on the choice of the isomorphism α. Indeed, it follows from the fact that the set of isomorphisms α as above is a torsor under the group $\mathbb{Z}_p^\times$ and the subgroup $U_K \subset \widehat{K^{\times p}}$ is preserved by this action.

Let n be sufficiently large natural number, which we will specify later. Pick a torsion point P_n of exact order p^n and a standard function f_n associated to this point. Denote by $L = K(E[p^n])$ the field extension obtained by adjoining coordinates of all p^n-torsion points. Moreover, choose another nontrivial p^n-torsion point Q such that $Q \neq \pm P$. Using any automorphism α, we may normalize the function f_n by requiring that the p-adic valuation of the evaluation $f_n(Q)$

$$v_\alpha\colon H^1(\Pi_{X_n}, M_X^{(p)}) \to H^1(G_L, M_X^{(p)}) \xrightarrow{\cong} H^1(G_L, \mathbb{Z}_p(G_L)) \twoheadrightarrow \mathbb{Z}_p$$

is trivial. This defines f_n uniquely, up to an element from U_L, more precisely $f_n = u(x - x(P_n))$ with an element $u \in L^{\times p}$ satisfying $v(u) = -v(x(Q) - x(P_n))$. Moreover, as we have seen, this normalization of f_n does not depend on the choice of an automorphism $\alpha : M_X^{(p)} \cong \mathbb{Z}_p(G_K)$. We now consider the set A of absolute values $v_\alpha(f_n(R))$ of all nontrivial p^n-torsion points R such that $R \neq \pm P$. It follows from Corollary 2.6.3 that for n large enough, the set A generates a free $\mathbb{Z}$-submodule of rank one of the group $\mathbb{Z}_p$.

Finally, observe that when the submodule A is contained in the submodule of integers $\mathbb{Z} \subset \mathbb{Z}_p$, then the automorphism α is equal, up to a $\mathbb{Q}_{(p)}^\times$-action, to the canonical rigidity isomorphism $M_X^{(p)} \cong \mathbb{Z}_p(G_L)$. Indeed, it follows from the fact that the only elements of $\mathbb{Z}_p^\times$ which preserve the line $\mathbb{Q} \subset \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Q}$ belong to $\mathbb{Q} \cap \mathbb{Z}_p^\times = \mathbb{Q}_{(p)}^\times$. □

Remark 2.6.5. In particular, the valuation map (2.4) can be constructed group theoretically up to multiplication by some rational number from $\mathbb{Q}_{(p)}^\times$. We will see soon that this $\mathbb{Q}_{(p)}^\times$ indeterminacy may by reduced further to the subgroup $\mathbb{Q}_{(p)}^\times \cap \mathbb{Q}_{>0}$ of positive rational numbers contained in $\mathbb{Q}_{(p)}^\times$. However, we are currently unable to remove this indeterminacy completely and this is the reason why in various statements in this chapter we need to assume that we are given the canonical rigidity isomorphism. On the other hand, observe that if we knew in advance all valuations $v(x(P))$ of all p-torsion points P, then in fact we would be able to reconstruct the canonical rigidity isomorphism $M_X^{(p)} \cong \mathbb{Z}_p(G_K)$. Indeed, in that case we would also know the index of the submodule $A \subset \mathbb{Z}$ from the proof of the previous proposition, which would reduce the indeterminacy.

Lemma 2.6.6. *Assume that we are given the canonical rigidity isomorphism $M_X^{(p)} \cong \mathbb{Z}_p(G_K)$ and suppose that $K = K(E[p^n])$ for some natural number $n \geq 1$. Then, for every p^n-torsion point P, the $L^{\times\mu}$ torsor of standard functions associated to P may be reconstructed group theoretically.*

Proof. Let P be a nonzero p^n-torsion point. Since we assume that the canonical rigidity isomorphism is given, for every p^n-torsion point $Q \neq \pm P$ we obtain the valuation map

$$H^1(\Pi_{X_n}, M_X^{(p)}) \to H^1(G_L, M_X^{(p)}) \twoheadrightarrow \mathbb{Z}_p,$$

defined as $f \mapsto v(f(Q))$, without any indeterminacies. Then, a profinite standard function f associated to the point P is standard if and only if the image $v(f(Q))$ lies in the submodule $\mathbb{Z} \subset \mathbb{Z}_p$. □

Proposition 2.6.7. *Assume that the elliptic curve E has good supersingular reduction. Then, for every nonzero torsion point P of p-power order the U^∞-torsor of integral standard functions can be reconstructed group theoretically.*

Proof. Let $v\colon K^{\wedge\infty}(M_X) \twoheadrightarrow \mathbb{Q}_p$ be the p-adic valuation, which by Proposition 2.6.4 may be reconstructed group theoretically up to multiplication by some rational number. For every P as in the proposition, choose a cohomology class of a profinite standard function $f_P \in H^1(\Pi_{X_n}, M_X^{(p)})$. Using Lemma 2.6.1, we may assume that they lie in the same equivalence class. Moreover, we may also assume that the value $v(f_P(Q))$ lies in the subgroup $\mathbb{Q} \subset \mathbb{Q}_p$, for all p-power torsion points P and Q such that $Q \neq \pm P$. Pick now a sequence of p-power torsion points P_i, for $i \geq 0$, with $P = P_0$ and such that the exact orders of points P_i go to infinity as $i \to \infty$. To ease the notation, we write $f_j = f_{P_j}$. Finally, for every pair of natural numbers i, j consider the absolute value

$$v_{i,j} = v(f_j(P_i)) \in \mathbb{Q}$$

of the evaluation of the Kummer class of f_j at the point P_i. Then, the set $\{v_{i,j}\}$ of rational numbers can be reconstructed group theoretically, up to multiplication by some rational number r.

Consider now the double limit

$$\lim_{i\to\infty} \lim_{j\to\infty} v_{i,j} \in \mathbb{R},$$

here the limit is taken with respect to archimedean topology. We claim that this limit exists and moreover it is equal to $0 \in \mathbb{R}$ if and only if the chosen equivalence class of functions f_j consists of integral standard functions. Moreover, since multiplication by $r \in \mathbb{Q}$ on $\mathbb{R}$ is continuous and fixes the point 0, this characterization is not affected by the indeterminacy in the construction of the valuation v. Therefore, it will provide the desired group theoretic reconstruction.

To prove the claim, observe that if we fix the index i, then the sequence $v_{i,j}$ of rational numbers becomes constant for sufficiently large j. Indeed, if we denote $f_j = u_j(x - x(P_j))$, then since the functions f_j are in the same equivalence class the valuation $v(u_j)$ does not depend on j. Denote this constant value by $a = v(u_j)$. Then, from Corollary 2.6.3 we see that for sufficiently large index j we have

$$v_{i,j} = v(u_j(x(P_i) - x(P_j))) = v(u_j) + v(x(P_i)) = a + v(x(P_i)).$$

Therefore, for fixed i, the sequence $(v_{i,j})_j$ is eventually constant and we obtain

$$\lim_{j\to\infty} v_{i,j} = a + v(x(P_i)).$$

Therefore, again applying Corollary 2.6.3 we compute

$$\lim_{i\to\infty} \lim_{j\to\infty} v_{i,j} = a.$$

This proves the first part of our claim. Moreover, as we have seen, $a = 0$ is equivalent to $v(u_j) = 0$, which is equivalent to the fact that u_j is a Kummer class of a p-adic unit. This is exactly the definition of being an integral standard function. $\square$

Observe that the proof of the above proposition also slightly reduces the indeterminacy in the reconstruction of the canonical rigidity isomorphism, as we see in the next corollary.

Corollary 2.6.8. *Assume that the elliptic curve E has good supersingular reduction. Then, the canonical rigidity isomorphism $M_X^{(p)} \cong \mathbb{Z}_p(G_K)$ may be reconstructed up to an element from the group $\mathbb{Q}_{(p)}^{\times} \cap \mathbb{Q}_{>0}$.*

Proof. Let $f_i = u(x - x(P_i))$ be the integral standard function used in the proof of the previous proposition. Observe that for every p-torsion point Q the value $v(f_i(Q))$ is negative for all sufficiently large natural numbers i. Therefore, by requiring that an isomorphism $\alpha\colon M_X^{(p)} \cong \mathbb{Z}_p(G_K)$ from the proof of Proposition 2.6.4 preserves this sign reduces the indeterminacy to positive rational numbers in $\mathbb{Q}_{(p)}^{\times}$. $\square$

In other words, the above corollary says that the sign of the valuation homomorphism is determined group theoretically.

2.7 Criterion in the supersingular case

In this section we are going to give the proof of Theorem 2.1.1. Let E be an elliptic curve over K and let $X = E \setminus \{O\}$. First, we will need a few simple results.

Lemma 2.7.1. *Suppose that we are given the set of all discrete tangential sections of the surjection $\Pi_X \twoheadrightarrow G_K$. Then, we may reconstruct the $\{\pm 1\}$-orbit of the canonical rigidity isomorphism $M_X^{(p)} \cong \mathbb{Z}_p(G_K)$.*

Proof. Recall that discrete section have a structure of a $K^{\times\mu}$-torsor. Therefore, the set of all discrete sections of the surjection determines a subgroup of the group $H^1(G_K, I)$, where I is an inertia group of the cusp, corresponding to the subgroup $K^{\times\mu} \subset \widehat{K^{\times p}}$. This in turn determines, by applying a group theoretic isomorphism $M_X^{(p)} \cong I$, a subgroup J_K of the cohomology group $H^1(G_K, M^{(p)})$. Let $\alpha\colon M_X^{(p)} \cong \mathbb{Z}_p(G_K)$ be an isomorphism of G_K-modules and consider the induced map

$$v_\alpha\colon H^1(G_L, M_X^{(p)}) \to H^1(G_L, \mathbb{Z}_p(G_K)) \twoheadrightarrow \mathbb{Z}_p.$$

Then, the image of the subgroup J_K under the map v_α is equal to the subgroup $\mathbb{Z} \subset \mathbb{Z}_p$ if and only if the isomorphism α is equal, up to ± 1, to the canonical rigidity isomorphism. Indeed, it follows from the fact that the only elements of $\mathbb{Z}_p^\times$ which preserve the subgroup $\mathbb{Z} \subset \mathbb{Z}_p$ are equal to ± 1. $\square$

Lemma 2.7.2. *Suppose that we are given the set of all discrete tangential sections of the surjection $\Pi_X \twoheadrightarrow G_K$. Then, for every finite field extension L/K we may reconstruct the set of all discrete tangential sections of the surjection $\Pi_{X_L} \twoheadrightarrow G_L$.*

Proof. Observe that restriction of a discrete section is also discrete. Since the set of discrete sections of $\Pi_{X_L} \to G_L$ is a $L^{\times\mu}$-torsor, it is enough to reconstruct the subgroup $L^{\times\mu}$. By the previous lemma, from the set of discrete sections, we may reconstruct the canonical rigidity isomorphism, up to ± 1. Thus, it uniquely determines a subgroup J_L of the cohomology group $H^1(G_L, M_X^p)$ corresponding to the subgroup $L^{\times\mu} \subset \widehat{L^{\times p}}$. $\square$

Using the theory developed so far we may prove the following proposition, which may be regarded as pro-p version of Lemma 1.8.3 in the case of supersingular reduction.

Proposition 2.7.3. *Assume that E is an elliptic curve with good supersingular reduction. Suppose that we are given the set of all discrete tangential sections of the surjection $\Pi_X \twoheadrightarrow G_K$ Then, we may reconstruct group theoretically the $\mathcal{O}_K^\times$-torsor of integral tangential sections.*

Proof. Fix any nonzero torsion point P of p-power order. By using Proposition 2.6.7 we may recover the U^∞-torsor of Kummer classes of integral standard functions associated to P inside the group $C(X)$. In particular, for sufficiently large finite field extension L/K and some positive integer $m \in \mathbb{N}$ we have constructed U_L-torsor of integral classes inside the cohomology group $H^1(\Pi_{U_m}, M_X^{(p)})$. Since the elliptic curve E has good reduction, by Lemma 2.5.5 together with Lemma 2.7.2 we may assume that $L = K$.

Denote by c the cusp determined by the origin of E and let $\omega \in T^\vee_{c,K}$ be an integral cotangent vector. We claim that there exists a lift $t \in K_c$ of ω such that for every integral standard function f associated to P we have the equality $f = vt^2$ for some $v \in \mathcal{O}_K^\times$. Indeed, recall that integral functions f are of the form $f = u(x - x(P))$, where u belongs to $\mathcal{O}_K^\times$. Since our fixed Weierstrass equation is minimal we know that the function $z = x/y$ determines an integral uniformizer at the cusp c. Moreover, in the field K_c we have the equality

$$x = 1/z^2 + \text{higher order terms.}$$

Thus, we obtain

$$f^{-1} = u^{-1}(x - x(P))^{-1} = u^{-1}z^2(1 + \text{higher order terms}) = u^{-1}(zs)^2,$$

for some $s \in 1 + \mathfrak{m}_c$. Hence we may take $t = zs$.

Fix a decomposition group D of the cusp c, hence we have a short exact sequence

$$1 \to I \to D \to G_K \to 1.$$

Consider inverses η_f^{-1} of the Kummer classes of integral standard functions f associated to the point P. Restrict these classes to the decomposition group D. We denote this set of classes by B, it is a U_K-torsor contained in the cohomology group $H^1(D, M_X^p)$. Applying the canonical isomorphism $M_X^{(p)} \cong I$ we may treat B as a U_K-torsor contained in the cohomology group $H^1(D, I)$. By the discussion in the previous paragraph, the torsor B is determined by Kummer classes of functions ut^2, where $u \in \mathcal{O}_K^\times$ and t is an integral uniformizer. By assumption, we have a $K^{\times\mu}$-torsor of cohomology classes in $H^1(D, I)$ corresponding to discrete sections, every class in this torsor will be called discrete.

Let A be a subset of $H^1(D, I)$ consisting of all discrete cohomology classes α in $H^1(D, I)$ such that $2\alpha \in B$, here we use the additive notation for cohomology classes. From the short exact sequence

$$1 \to H^1(G_K, I) \to H^1(D, I) \to \mathrm{Hom}(I, I) \to 1$$

we easily observe that A is determined by Kummer classes of functions ut, for all $u \in U_K$. In particular, for every $\alpha \in A$ its restriction to $H^1(I, I) = \mathrm{Hom}(I, I)$ is the identity. Therefore, the U_K-torsor A defines the torsor of integral tangential sections. □

Proposition 2.7.4. *Assume that E has potentially good supersingular reduction. Then, from the topological group Π_X equipped with the set of all discrete tangential sections, we may determine whether the absolute value of the minimal discriminant $v_K(\Delta)$ of E/K is divisible by* 12.

Proof. Choose a decomposition group $D_K \subset \Pi_X$ of the unique cusp of X, hence we have a short exact sequence

$$1 \to I \to D_K \to G_K \to 1.$$

Let L/K be a finite field extension such that E has good reduction over the field L. By pulling back the above short exact sequence along the inclusion $G_L \hookrightarrow G_K$ we obtain the restricted sequence

$$1 \to I \to D_L \to G_L \to 1.$$

By the previous proposition, applied to the fundamental group Π_L, we may reconstruct the U_L-torsor of integral tangential sections s_L of the surjection $D_L \to G_L$. Consider now the following diagram

$$\begin{array}{ccc} & \overset{s_L}{\curvearrowleft} & \\ D_L & \longrightarrow & G_L \\ \downarrow & & \downarrow \\ D_K & \longrightarrow & G_K. \\ & \underset{s_K}{\curvearrowright} & \end{array}$$

We are going to prove that the value $v_K(\Delta)$ is divisible by 12 if and only if there exists an integral tangential section s_L which extends to a discrete section $s_K \colon G_K \to D_K$ of the surjection $D_K \twoheadrightarrow G_K$. This group theoretic description will finish the proof.

Let $T_L^\vee = T_K^\vee \otimes L$ be the cotangent L-vector space of the unique cusp on X_L and let $S \subset T_L^\vee$ be the $\mathcal{O}_L^\times$-torsor of integral differentials. We have the following diagram

$$\begin{array}{ccc} S & \hookrightarrow & T_L^\vee \\ \uparrow & & \uparrow \\ S \cap T_K^\vee & \hookrightarrow & T_K^\vee. \end{array}$$

We claim that there exists a tangential integral section s_L which extends to a discrete section over G_K if and only if the intersection $S \cap T_K^\vee$ is nonempty. Indeed, choose any integral tangential section s_L of the surjection $D_L \twoheadrightarrow G_L$ corresponding to the cotangent vector $\omega_L \in T_L^\vee$. Moreover, choose any discrete tangential section s of the surjection $D_K \twoheadrightarrow G_K$ corresponding to a cotangent vector $\omega_K \in T_K^\vee$. Then, the section s_L extends to a section of the surjection $D_K \twoheadrightarrow G_K$ if and only if there exists an element $a \in K^{\times\mu}$ such that the restriction of as to G_L is equal to s_L. Using the correspondence between discrete sections and cotangent vectors we see that this equality of restrictions is equivalent to the equality $a\omega_K = b\omega_L$, for some $a \in K^\times$ and $b \in \mathcal{O}_L^\times$. This finishes the proof of the claim.

Let now x' and y' be some fixed coordinates of a minimal Weierstrass equation over K, similarly let x and y be coordinates of a minimal equation over L. Then we have

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t$$

for some $u \in L^\times$ and $r, s, t \in L$. Let $\omega_K \in T_K^\vee$ be the cotangent vector determined by the rational function x'/y', similarly let $\omega_L \in T_L^\vee$ be the cotangent vector determined by x/y. We easily check that $u\omega_K = \omega_L$, as elements of $T_L^\vee$. Moreover, if Δ and Δ' denote the discriminants of the corresponding minimal

Weierstrass equations, then we know that $u^{12}\Delta' = \Delta$. Therefore we obtain $v(u^{12}) = v(\Delta)$, since Δ' is a unit.

Assume now that the intersection $S \cap T_K^{\vee}$ is nonempty. Then, we have the equality $a\omega_K = b\omega_L$, for some $a \in K^{\times}$ and $b \in \mathcal{O}_L^{\times}$. Thus, we obtain $a\omega_K = bu\omega_L$, which implies that $a = bu$, hence comparing valuations we have $v(a) = v(u)$. Therefore, we finally compute that $v(\Delta) = v(a^{12})$ for some $a \in K$, which proves that 12 divides $v_K(\Delta)$.

On the other hand, if we assume this divisibility it is easy to run the argument backwards and see that we obtain the existence of $a \in K$ and $b \in \mathcal{O}_L^{\times}$ as before, which proves that $S \cap T_K^{\vee}$ is nonempty. □

Finally, as a corollary we obtain the proof of the main result of this chapter.

Proof of Theorem 2.1.1. As we have seen in Section 2.4, when the elliptic curve E does not have a potentially good supersingular reduction, then in fact we may determine the reduction type of E by analysing the p-adic Tate module of E; moreover in this case the proof is valid for every residue characteristic $p > 2$ and does not need additional data consisting of the set of discrete sections.

When E has potentially good supersingular reduction, we have shown in Proposition 2.7.4 that we can determine group theoretically whether the p-adic absolute value $v_K(\Delta)$ of the minimal discriminant Δ over K is divisible by 12. On the other hand, it is well known that, for an elliptic curve over K with potentially good reduction, we have the following estimate

$$v_K(\Delta) < 12 + 12v_K(2) + 6v_K(3).$$

In particular, if $p \geq 5$, then $v_K(E) < 12$. Therefore, in this case, having good reduction is equivalent to the divisibility condition we have obtained and this finishes the proof. □

2.8 Pro-p reconstruction of local height

In this section we prove a pro-p version of Theorem 1.1.1. To state it precisely, we recall our assumptions. Let E be an elliptic curve over a local field K and let X be a hyperbolic curve $E \setminus \{O\}$. Consider the maximal pro-p geometric fundamental group $\Delta_X = \pi_1^{(p)}(X_{K^{\mathrm{alg}}})$ of X, hence we have a pushout diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(X_{K^{\mathrm{alg}}}) & \longrightarrow & \pi_1(X) & \longrightarrow & G_K & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \Delta_X & \longrightarrow & \Pi_X & \longrightarrow & G_K & \longrightarrow & 1. \end{array}$$

Let P be an L-rational point of the curve X, for some finite field extension L/K. The point P determines a section over an open subgroup G_L of the surjection $\pi_1(X) \twoheadrightarrow G_K$. Therefore, by composing this section with the surjctive homomorphism $\pi_1(X) \twoheadrightarrow \Pi_X$ we obtain a commutative diagram

$$\begin{array}{ccc} & & G_L \\ & \overset{s}{\swarrow} & \big\downarrow \\ \Pi_X & \twoheadrightarrow & G_K. \end{array} \tag{2.5}$$

Hence s is a section over an open subgroup of the surjection $\Pi_X \twoheadrightarrow G_K$ determined by a L-rational point P. Then, we have the following pro-p version of Theorem 1.1.1 in the case of potentially good reduction.

Theorem 2.8.1. *With the notation as above, assume moreover that the elliptic curve E has potentially good reduction. Then, we can determine group theoretically from the diagram* (2.5) *whether the local height of the rational point P is equal to zero. Moreover, if we assume additionally that we are given the canonical rigidity isomorphism $M_X^{(p)} \cong \mathbb{Z}_p(G_K)$, then we may in fact reconstruct the local height of the point P.*

The proof of the above theorem is almost identical to the proof of Theorem 1.1.1, namely we are going to reconstruct classes of integral standard function and use group theoretic valuation map to compute the height. The additional difficulty comes from the fact that in the pro-p case elliptic cuspidalization constructs only torsion points of p-power order.

Since the local height is invariant under field extensions, in order to prove Theorem 2.8.1 we may assume that E has good reduction. Fix a minimal Weiestrass equation (2.3) of the elliptic curve E. Recall, that in Chapter 1 we defined the notion of integral point on the hyperbolic curve $X = E \setminus \{O\}$. Namely, an L-rational point $P \neq O$ is integral when $v(x(P)) \geq 0$, for some finite extension L/K. Similarly, we say that a point $P \neq O$ is *nonintegral* when $v(x(P)) < 0$. These notions are independent of the choice of a minimal Weierstrass equiation. Moreover, we have seen that the set of nonintegral points together with the origin O is equal to the preimage of O under the reduction map

$$E(K^{\mathrm{alg}}) = \mathcal{E}(\mathcal{O}_{K^{\mathrm{alg}}}) \to \mathcal{E}_k(k^{\mathrm{alg}}).$$

In particular, it is a subgroup of the group of all rational points. When E has supersingular reduction then every nonzero torsion point of p-power order is nonintegral. For a rational point P on the elliptic curve E we will write $\bar{P}$ for the reduction of P.

Assume now that the elliptic curve E has good ordinary reduction and consider the set of nonzero m-torsion points, for some $m = p^\alpha$. Then, it follows from our discussion in Section 2.4 that we have a short exact sequence of abelian groups

$$1 \to \mathcal{E}[m]^\circ(K^{\mathrm{alg}}) \to \mathcal{E}[m](K^{\mathrm{alg}}) \to \mathcal{E}[m]^{\text{ét}}(K^{\mathrm{alg}}) \to 1,$$

recall that $\mathcal{E}$ is a good model of E over $\mathrm{Spec}(\mathcal{O}_K)$. Since E has ordinary reduction, the group $\mathcal{E}[m]^{\text{ét}}(K^{\mathrm{alg}})$ has order m. Therefore, the set of nonzero nonintegral m-torsion points has cardinality $m-1$, hence the set of nonzero integral m-torsion points has cardinality $m^2 - m$.

We now take $m = p$ for $p > 3$, $m = 9$ if $p = 3$ and $m = 8$ if $p = 2$. Moreover, choose any s from the set $(\mathbb{Z}/m\mathbb{Z})^\times \setminus \{1, -1\}$, which is nonempty by the choice of m. Therefore, if P is a point of exact order m, then the point sP also has exact order m and $sP \neq \pm P$. Moreover, P is integral if and only if sP is integral. For every nonzero torsion point P of exact order m we write

$$A_P = E[m](K^{\mathrm{alg}}) \setminus \{O, P, -P\},$$

which is a set of cardinality $m^2 - 3$. Consider a function $\varphi_P \colon A_P \to \mathbb{Q}$ defined by the formula

$$\varphi_P(Q) = v(x(Q) - x(P)) - v(x(sP) - x(P)).$$

Let P be any nonzero torsion point of exact order m. Then, we have the following technical lemma.

Lemma 2.8.2. *With the notation as above, the following statements hold.*

1. *Suppose that P is an integral point such that $s\bar{P} \neq \pm\bar{P}$ and $\bar{P} \neq -\bar{P}$. Then, the set $\varphi_P^{-1}(\mathbb{Q}_{<0})$ is of cardinality $m-1$, the set $\varphi_P^{-1}(\{0\})$ is of cardinality $m^2 - 3m$ and the set $\varphi_P^{-1}(\mathbb{Q}_{>0})$ is of cardinality $2m-2$.*

2. *Suppose that P is an integral point such that $s\bar{P} \neq \pm\bar{P}$ and $\bar{P} = -\bar{P}$. Then, the set $\varphi_P^{-1}(\mathbb{Q}_{<0})$ is of cardinality $m-1$, the set $\varphi_P^{-1}(\{0\})$ is of cardinality $m^2 - 2m$ and the set $\varphi_P^{-1}(\mathbb{Q}_{>0})$ is of cardinality $m-2$.*

3. *Suppose that P is an integral point and $s\bar{P} = \pm\bar{P}$. Then, the set $\varphi_P^{-1}(\mathbb{Q}_{<0})$ has cardinality at least $m^2 - 2m + 1$.*

4. *Suppose that P is a nonintegral point. Then, at least one of the sets*

$$\varphi_P^{-1}(\mathbb{Q}_{<0}),\ \varphi_P^{-1}(\{0\}),\ \varphi_P^{-1}(\mathbb{Q}_{>0}),$$

has cardinality greater than or equal to $m^2 - m$.

Proof. Assume first that P is an integral point and $s\bar{P} \neq \pm\bar{P}$. Then, we have $v(x(sP) - x(P)) = 0$ and it follows that

$$\varphi_P(Q) = v(x(Q) - x(P)).$$

When Q is a nonintegral point, then $v(x(Q)) < 0$ and we obtain $\varphi_P(Q) < 0$. Suppose now that Q is integral so we have $x(Q) \geq 0$, hence $\varphi_P(Q) \geq 0$. Thus, it is enough to count points Q such that $\varphi_P(Q) > 0$. On the other hand, $x(\bar{Q}) = x(\bar{P})$ if and only if $\bar{Q} = \pm\bar{P}$. When $\bar{P} \neq -\bar{P}$, then this equation has $2m-2$ solutions Q in the set A_P and when $\bar{P} = -\bar{P}$, then it has $m-2$ solutions. This proves statements (1) and (2).

Assume now that the point P is integral and $s\bar{P} = \pm\bar{P}$. Then, we have

$$v(x(s(P)) - x(P)) > 0,$$

and it follows that

$$\varphi_P(Q) < v(x(Q) - x(P)).$$

Therefore, we may repeat the computation from the previous paragraph to obtain that $\varphi_P(Q) < 0$ for at least $(m-1) + (m^2 - 3m) = m^2 - 2m - 1$ points Q from the set A_P. This proves statement (3).

Finally, assume that P is a nonintegral point, hence $v(x(P)) < 0$. Therefore, for every integral point Q we have

$$\varphi_P(Q) = v(x(P)) - v(x(sP) - x(P)).$$

For clarity, we distinguish three cases.

- Suppose that $v(x(P)) \neq v(x(sP))$. Therefore

  $$v(x(sP) - x(P)) = \min\{v(x(sP)), v(x(P))\}$$

  and for every integral point Q we compute

  $$\varphi_P(Q) = v(x(P)) - \min\{v(x(sP)), v(x(P))\} > 0.$$

- Suppose that $v(x(P)) = v(x(sP)) = v(x(sP) - x(P))$. Then, for every integral point Q we obtain

  $$\varphi_P(Q) = v(x(P)) - v(x(sP) - x(P)) = 0,$$

- Finally, suppose that $v(x(P)) = v(x(sP)) \neq v(x(sP) - x(P))$, hence $v(x(sP) - x(P)) > v(x(P)) = v(x(sP))$. Therefore, for every integral point Q we have

  $$\varphi_P(Q) = v(x(P)) - v(x(sP) - x(P)) < 0.$$

This finishes the proof, since the set of integral points in A has cardinality $m^2 - m$. □

We will say a nonzero integral torsion point P of exact order m is a *good* integral point if $s\bar{P} \neq \pm\bar{P}$. Therefore, when the integral point P is good, we have seen in the proof of the previous lemma that $\varphi_P(Q) = v(x(Q) - x(P))$, for every point $Q \in A_P$.

In the next three lemmas, we assume that E has good ordinary reduction over K.

Lemma 2.8.3. *The $\mathbb{Q}_{(p)}^{\times}$-orbit of the canonical rigidity isomorphism may be reconstructed group theoretically from the group Π_X.*

Proof. Observe that to prove this lemma we may apply exactly the same argument as in the proof of Proposition 2.6.4. Indeed, the only place we needed the assumption that E has good supersingular reduction was to prove that the module A is nontrivial, which is clear in the case of good ordinary reduction as the sets of integral and nonintegral points are both nonempty. □

In particular, the valuation map $H^1(G_K, M_X^{(p)}) \twoheadrightarrow \mathbb{Z}_p$ may be reconstructed up to multiplication by some rational number. Recall that elliptic cuspidalization reconstructs from the group Π_X the set of decomposition groups of p-power torsion points. Next lemma says that we may determine whether a specific decomposition group comes from an integral point.

Lemma 2.8.4. *Let $D \subset \Pi_X$ be a decomposition group of a nonzero torsion point S of p-power order. Then, we may determine group theoretically whether the point S is integral or not. Moreover, we may also reconstruct the canonical rigidity isomorphism up to an element from $\mathbb{Q}_{(p)}^{\times} \cap \mathbb{Q}_{>0}$.*

Proof. Let m and s be as in Lemma 2.8.2 and consider set $B = E[m] \setminus \{O\}$ of nonzero m-torsion points. We may assume that all m-torsion points are rational. Let P be a torsion point of exact order m. Fix a profinite standard function f_P associated to the point P satisfying $v(f_P(sP)) = 0$. This condition is group theoretic, moreover f_P is in fact a standard function $f_P = u(x - x(P))$, for some $u \in K^{\times\mu}$ satisfying $v(u) = -v(x(sP) - x(P))$. Hence, for every torsion point Q from the set A_P we have the equality $v(f_P(Q)) = \varphi_P(Q)$. Then, it follows from Lemma 2.8.3 that the function $\varphi_P \colon A_P \to \mathbb{Q}$ may be reconstructed group theoretically form the group Π_X, up to multiplication by some nonzero rational number.

Observe that by Lemma 2.8.2 this information suffices to determine if the point P is a good integral point. Moreover, when P is in fact a good integral point we may use Lemma 2.8.2 again to reduce the indeterminacy in the reconstruction of canonical rigidity isomorphism to positive rational numbers. Indeed, it follows from the fact that sets $\varphi_P^{-1}(\mathbb{Q}_{<0})$ and $\varphi_P^{-1}(\mathbb{Q}_{>0})$ have different cardinalities. Therefore, we may now reconstruct the value $v(f_P(S))$ group theoretically up to multiplication by some positive rational number. Finally, observe that when P is a good integral point of exact order m, then $v(f_P(S)) = v(x(S) - x(P))$ is nonnegative if and only if the point S is integral. Therefore, it follows that we may determine whether the point S is integral or not. □

Lemma 2.8.5. *Let S be a nonzero p-power torsion point. Then, we may reconstruct U^∞-torsor of integral standard functions associated to the point S.*

Proof. Fix a nonzero good integral torsion point P or exact order m. Let f_P be the function used in the proof of the previous lemma, normalized by the condition $v(f_P(sP)) = 0$. Since $v(x(sP) - x(P)) = 0$, it implies that the function f_P is already integral. Then, it follows from Lemma 2.6.1 that we may also reconstruct integral standard functions associated to the point S. □

Corollary 2.8.6. *Suppose that E has good reduction. Then, from the group Π_X, we may reconstruct group theoretically U^∞-torsor of integral standard function associated to all nonzero p-power points.*

Proof. This is simply Proposition 2.6.7 and Lemma 2.8.5. □

Proof of Theorem 2.8.1. We proceed as in the proof of Theorem 1.1.1. Let $s\colon G_L \to \Pi_X$ be a section over an open subgroup G_L of the surjection $\Pi_X \twoheadrightarrow G_K$ coming from the L-rational point. We may extend the base field K so that s becomes a real section and all p-torsion points are K-rational. Moreover, we may assume that the point P is not a p-power torsion point. Using elliptic cuspidalization, we obtain the surjection $\Pi_{X_1} \twoheadrightarrow \Pi_X$ determined by the open immersion $X_1 = E\backslash E[p] \hookrightarrow X$. The image of the section s determines a decomposition group $D_P \subset \Pi_X$ of the point P. Using Lemma 1.7.3 we reconstruct conjugacy classes of decomposition groups $D_Q \subset \Pi_{X_1}$ of points Q satisfying $pQ = P^\tau$, for some automorphism τ of the elliptic curve E. We choose one of those classes corresponding to a point Q and a decomposition group D_Q from this class.

Let S be a nontrivial p-torsion point and let f_S be an integral standard function associated to the point S. Thus, we have $f_S = u(x - x(S))$ for some

unit $u \in \mathcal{O}_K^\times$. By Corollary 2.8.6, the cohomology class of the function f_S may be reconstructed group theoretically, up to a p-adic unit, as an element of the cohomology group $H^1(\Pi_{X_1}, M_X^{(p)})$.

Observe now that we may determine whether the rational point Q is integral or not. Indeed, we evaluate the class f_S at the decomposition group D_Q and consider the p-valuation $v(f_S(Q)) \in \mathbb{Q}$. Then, the rational point Q is integral if and only if there exists an integral p-torsion point S such that the number $v(f_S(Q))$ is nonnegative. On the other hand, when the point Q is not integral, then the value $v(f_S(Q))$ for an integral p-torsion point S computes the local height of the point Q. Therefore, we may reconstruct the height of the point Q, up to multiplication by some rational number r.

Moreover, the cohomology class of the function F_p from Lemma 1.2.4 may be reconstructed as well, as a product of integral standard function associated to p-torsion points normalized by p^2. By restricting the cohomology class of the function F_p to decomposition group D_Q and taking valuations we may compute $v(F_p(Q))$, up to multiplication by the same rational number r. Thus, by Lemma 1.2.4, we may determine whether the local height of P is equal to zero. Suppose now that we are given the canonical rigidity isomorphism, in particular the valuation map is defined without any indeterminacy. Then, using the above computation we recover the local height of the point P. $\square$

Chapter 3

Anabelian geometry of Tate curve

3.1 Introduction

In this chapter we continue studying anabelian geometry of punctured elliptic curve $X = E \setminus \{O\}$ over a local field K, this time under the assumption that E is a Tate curve. In this case, we will consider the tempered fundamental group Π_X^{tp} of X, which is no longer a profinite group. This group allows us to consider certain infinite analytic covers, like the Tate uniformization $\mathbb{G}_m \to \mathbb{G}_m/q^{\mathbb{Z}}$ in terms of fundamental groups. In particular, one can consider Kummer classes of theta functions, as introduced in [29].

To explain our main result, we need to introduce some notation which will be defined in the following sections. We write $Y \to X$ for a $\mathbb{Z}$-cover determined by the Tate uniformization and $\ddot{Y} \to Y$ for certain étale cover of degree two. On the curve $\ddot{Y}$ we introduce the following theta function

$$\ddot{\Theta}(\ddot{U}) = \ddot{U} \prod_{n\geq 0}(1 - q^n\ddot{U}^2) \prod_{n>0}(1 - q^n\ddot{U}^{-2}).$$

The preimage of the cusp O determines the set of cusps on the curve $\ddot{Y}$ and the function $\ddot{\Theta}(\ddot{U})$ has single zero at each of these cusps. Moreover, it also possesses certain well-known symmetries with respect to transformations $\ddot{U} \mapsto -\ddot{U}$ and $\ddot{U} \mapsto \ddot{U}^{-1}$. It is shown in [29] that these symmetries, together with the property of having single zeroes at cusps, allows us to reconstruct group theoretically a $K^\times$-torsor of Kummer classes of the function $\ddot{\Theta}(\ddot{U})$, as a subset of certain cohomology group $H^1(\Pi_{\ddot{Y}}^{\mathrm{tp}}, \Delta_\Theta)$.

Since X has stable model over K, we have the notion of an integral tangential section of the surjection $\Pi_X^{\mathrm{tp}} \twoheadrightarrow G_K$, introduced in Section 2.5. Therefore,

one can further reduce the $K^\times$-torsor structure to obtain a $\mathcal{O}_K^\times$-torsor of classes compatible with the integral structure at cusps. Assume now that the field K contains 12th roots of unity as well as coordinates of all 2-torsion points of E. Then, our main result in this chapter is the following theorem (for a more detailed statement, see Theorem 3.4.5 and Corollary 3.4.11).

Theorem 3.1.1. *There exists a group theoretic construction of a trivialization of the $\mathcal{O}_K^\times$-torsor of Kummer classes of theta functions compatible with integral structure at the cusp, which is well defined up to a sign.*

More precisely, this trivialization is constructed by normalizing the above $\mathcal{O}_K^\times$-torsor at certain special point.

Finally, in the last section we consider a variant of the problem discussed in Chapter 1. Assume that E is an elliptic curve without potentially good reduction. Let P be a nonzero rational point on E and consider the diagram

$$\begin{array}{ccc} & & G_L \\ & \overset{s}{\swarrow} & \downarrow \\ \Pi_X^{\mathrm{tp}} & \longrightarrow & G_K, \end{array}$$

where s is a section over an open subgroup G_L induced by the point P. Then, in Proposition 3.5.1, we prove the following result.

Theorem 3.1.2. *The local Néron-Tate height of the point P may be reconstructed group theoretically from the above diagram of topological groups.*

Throughout this chapter we assume that the set Σ introduced in Chapter 1 is equal to the set of all prime numbers. To simplify the notation, we will still write $\Pi_X = \pi_1(X)$ and $\Delta_X = \pi_1(X_{K^{\mathrm{alg}}})$ for étale fundamental groupsof X.

3.2 Tate curve

In this section we recall a few basic facts surrounding the geometry of the Tate curve. For more details, see [32], Section 5 and [15], Section 5.1, as well as [35], II.5.

Let E be an elliptic curve over K with split multiplicative reduction and let $X = E \setminus \{O\}$ be the hyperbolic curve obtained by removing the origin of E. As in the previous chapters, we will refer to the point O as the cusp of X. By Tate's uniformization, there is an element $q \in K^\times$ of norm $|q| < 1$ and a G_K-equivariant isomorphism of groups $E(K^{\mathrm{alg}}) \cong (K^{\mathrm{alg}})^\times / q^{\mathbb{Z}}$. In particular,

we have an isomorphism $E(K) \cong K^\times/q^{\mathbb{Z}}$. The quotient map $K^\times \twoheadrightarrow K^\times/q^{\mathbb{Z}}$ corresponds to a rigid analytic morphism

$$\mathbb{G}_{m,K}^{\mathrm{an}} \to \mathbb{G}_{m,K}^{\mathrm{an}}/q^{\mathbb{Z}} \cong E.$$

The preimages of the cusp O in $\mathbb{G}_{m,K}^{\mathrm{an}}$ define the set of cusps on $\mathbb{G}_{m,K}^{\mathrm{an}}$, corresponding to the set of points q^i, for all $i \in \mathbb{Z}$. Denote by Y the analytic curve $\mathbb{G}_{m,K}^{\mathrm{an}}$ punctured at these cusps, by restriction we have the analytic cover $Y \to X$. It is a Galois cover with the Galois group $\mathrm{Aut}(Y/X)$ isomorphic to $\mathbb{Z}$. This group acts on the set of cusps of Y and in fact the set of cusps of Y is an $\mathrm{Aut}(Y/X)$-torsor. Hence, by choosing generator of the group $\mathrm{Aut}(Y/X)$ and a trivialization of this torsor we may identify the set of cusps of the curve Y with the set of integers $\mathbb{Z}$. We fix this bijection and we will say that an integer corresponding to a cusp is its *label*.

Let $\mathcal{X}$ be the stable model of the curve X over the ring of integers $\mathcal{O}_K$. Then, using the language of formal schemes, the cover $Y \to X$ may be described as a morphism of formal schemes $\mathfrak{Y} \to \mathfrak{X}$ as follows:

$$\begin{array}{ccccc} \mathcal{Y} & \rightsquigarrow & \mathfrak{Y} & \dashrightarrow & \mathfrak{Y}_K = Y \\ & & \downarrow & & \downarrow \\ \mathcal{X} & \rightsquigarrow & \mathfrak{X} & \dashrightarrow & \mathfrak{X}_K = X. \end{array}$$

Here, curved arrows represent the completion of stable models over $\mathcal{O}_K$ along the special fibre and dotted arrows express the Raynaud's generic fibre functor (see [8], Chapter 8). The scheme $\mathcal{Y}$ is given explicitly as

$$\mathcal{Y} = \mathbf{Proj}(\mathcal{O}_K[\ldots,\ q^{k^2+k}U^{2k+1}\mathbf{t},\ q^{k^2}U^{2k}\mathbf{t},\ q^{k^2-k}U^{2k-1}\mathbf{t}, \ldots]_{k\in\mathbb{Z}}),$$

where the symbol $\mathbf{t}$ indicates degree 1. Let us describe the standard affine open subschemes covering this scheme. For every $k \in \mathbb{Z}$ and $\varepsilon \in \{-1, 0, 1\}$, we denote by $U_{k,\varepsilon}$ the affine scheme obtained by inverting the element $q^{k^2+\varepsilon k}X^{2k+\varepsilon}\mathbf{t}$. Hence we have $U_{k,1} = U_{k+1,-1}$, moreover we see that

$$U_{i,0} = \operatorname{Spec} \mathcal{O}_K[q^i X, q^{-i}X^{-1}]$$

and

$$U_{i,1} = \operatorname{Spec} \mathcal{O}_K[q^{i+1}X, q^{-i}X^{-1}], \quad U_{i,-1} = \operatorname{Spec} \mathcal{O}_K[q^i X, q^{-i+1}X^{-1}].$$

Therefore, introducing new variables $X_i = q^i X$ for all $i \in \mathbb{Z}$, we may write

$$U_{i,0} = \operatorname{Spec} \mathcal{O}_K[X_i, X_i^{-1}]$$

and

$$U_{i,1} = \operatorname{Spec} \mathcal{O}_K[X_{i+1}, X_i^{-1}]/(X_{i+1}X_i^{-1} - q).$$

Thus, we easily see that the generic fibre $\mathcal{Y}_K$ of $\mathcal{Y}$ is the multiplicative group scheme $\mathbb{G}_{m,K}$. On the other hand, the special fibre $\mathcal{Y}_k$ of $\mathcal{Y}$ has the structure of an infinite chain of projective lines with labels $i \in \mathbb{Z}$. They are glued together by identifying the point ∞ on the line with label i with the point 0 on the line with label $i+1$. In fact, when q is a uniformizer of K, the smooth locus of the morphism $\mathcal{Y} \to \operatorname{Spec}(\mathcal{O}_K)$ may be considered as a Néron lft-model of the multiplicative group scheme $\mathbb{G}_{m,K}$ (see [9], Chapter 10). The scheme $\mathcal{Y}$ is endowed with the action of the group $\mathbb{Z}$ of integers

$$(n, X) \mapsto q^n X$$

$$(n, \mathbf{t}) \mapsto q^{n^2} X^{2n} \mathbf{t}$$

which maps the open subscheme $U_{i,\epsilon}$ isomorphically onto the subscheme $U_{i+n,\epsilon}$. On the special fibre of $\mathcal{Y}$ this action corresponds to the "translation by n" in the chain of projective lines.

The rigid analytic space $\mathbb{G}_{m,K}$ has an admissible cover determining a cover of the multiplicative group $(K^{\mathrm{alg}})^\times$ by the open annuli A_i, defined as follows:

$$A_i = \{x \in (K^{\mathrm{alg}})^\times : \ |q^{i+1}| \leq |x| \leq |q^i|\}.$$

This covering corresponds to the decomposition of the special fibre of the scheme $\mathcal{Y}$ as a sum of projective lines, under the Raynaud's generic fibre functor. For example, K-rational points on the generic fibre $\mathcal{Y}_K$ which reduce to k rational points lying in the smooth locus of the special fibre $\mathcal{Y}_k$ belong to the set $B = \bigcup_i B_i$, where $B_i = A_i \cap A_{i-1}$ is the "boundary" of the annulus. On the other hand, points reducing to the singular points of the special fibre $\mathcal{Y}_k$ belong to the set $C = \bigcup_i C_i$, where $C_i = A_i \setminus (B_i \cup B_{i+1})$ is the"interior" of the annulus A_i. Therefore, we obtain bijection between the set of cusps on Y and the set of irreducible components of the special fibre of $\mathcal{Y}$. Hence we may define a label of a projective line in the special fibre $\mathcal{Y}_k$ as the label of its corresponding cusp.

In the following, we are going to use the notion of the tempered fundamental group of a curve C. Here we briefly recall the definition, for a detailed explanation see [3] and [2]. Let C^{an} be the analytification of the curve C, in the sense of Berkovich spaces. The topological space C^{an} is locally contractible and locally path connected hence has a universal topological covering. On the other hand, unlike in the complex case, the analytification $C'^{\mathrm{an}} \to C^{\mathrm{an}}$ of a finite étale cover $C' \to C$ is not necessarily a topological covering. A tempered cover of

C^{an} is defined to be a cover $T \to C^{\mathrm{an}}$ of K-manifolds which is a quotient of the cover $T' \to D^{\mathrm{an}} \to C^{\mathrm{an}}$, where $D \to C$ is a finite étale cover and $T' \to D^{\mathrm{an}}$ is a topological cover. Then, the tempered fundamental group Π_C^{tp} of C is a prodiscrete topological group classifying tempered covers of C^{an}, namely open subgroups of Π_C^{tp} correspond to tempered covers. More precisely, one defines Π_C^{tp} as an automorphism group of a fibre functor associated to a chosen base point, similarly as in the case of the étale fundamental group. In particular, since we are not using base points in our notation, we treat the group Π_C^{tp} as a topological group defined up to an inner automorphism. Since algebraic covers are tempered, have a natural homomorphism $\Pi_C^{\mathrm{tp}} \to \Pi_C$ from the tempered fundamental group of C to its algebraic fundamental group.

Equivalently, one can define Π_C^{tp} as follows. Let $(C_i \to C)_{i \in I}$ be the universal pro-étale cover of C, i.e., inductive limit of all finite Galois étale covers $C_i \to C$. Write $C_i^{\infty} \to C_i^{\mathrm{an}}$ to be the universal topological cover of the analytification C_i^{an} of C_i. It is easy to check that every cover $C_i^{\infty} \to C^{\mathrm{an}}$ is Galois as well. Then, one can define Π_C^{tp} to be the inverse limit

$$\Pi_C^{\mathrm{tp}} = \varprojlim_{i \in I} \mathrm{Gal}(C_i^{\infty} \to C^{\mathrm{an}})$$

Here we give a few examples. Recall that for a stable curve C over K the homotopy type of its Berkovich analytification C^{an} is equal to the homotopy type of the dual graph of the special fibre of the stable model of C (see [6]). In particular, if C has good reduction then C^{an} has no nontrivial topological coverings. Moreover, for every curve C, the homomorphism $\Pi_C^{\mathrm{tp}} \to \Pi_C$ is injective and induces an isomorphism $\widehat{\Pi}_C^{\mathrm{tp}} \cong \Pi_X$ of profinite completions. Therefore, when E is an elliptic curve with good reduction then we have an isomorphism $\Pi_E^{\mathrm{tp}} \cong \Pi_X$. Indeed, morphisms $[n] : E \to E$ are cofinal in the family of all étale covers of E, hence all tempered coverings are algebraic and the natural map $\Pi_E^{\mathrm{tp}} \to \Pi_E$ is an isomorphism. One example of a nontrivial tempered cover is given by the Tate uniformization $G_m^{\mathrm{an}} \to E^{\mathrm{an}}$, where E is an elliptic curve with split multiplicative reduction. This cover gives a surjection $\Pi_E^{\mathrm{tp}} \twoheadrightarrow \mathbb{Z}$, hence also an example of an infinite discrete quotient. In fact, one can show that when K is algebraically closed, the tempered fundamental group of a Tate curve E is isomorphic to the product $\widehat{\mathbb{Z}} \times \mathbb{Z}$.

Similarly as in the case of étale fundamental group, for every rational point P on the curve C we have a decomposition group $D_P \subset \Pi_C^{\mathrm{tp}}$ of the point P, determined up to conjugation by Π_C^{tp}. Moreover, for every cusp x of C we also have inertia and decomposition groups. Then, every such decomposition group is in fact compact and its image under the inclusion map $\Pi_C^{\mathrm{tp}} \hookrightarrow \Pi_C$ is equal to

corresponding decomposition group in Π_C, similarly for inertia groups of cusps. Therefore, the theory of tangential sections recalled in Section 2.5 immediately extends to tempered tangential sections. Furthermore, when Σ is the set of all prime numbers, the statements of Theorem 1.4.2 and Theorem 1.4.3 remain valid also in the tempered case. See, e.g., [25], Section 6. This implies that the elliptic cuspidalisation algorithm introduced in Section 1.7 is applicable also in the case of tempered fundamental group.

3.3 Theta function

Let us now recall the definition of the *basic theta function* (see, e.g., [15], Definition 5.1.8)

$$\Theta(U) = \prod_{n\geq 0}(1-q^nU)\prod_{n>0}(1-q^nU^{-1}).$$

We check that $\Theta(U)$ is a global section of a structure sheaf of the formal scheme $\mathfrak{Y}$, for instance using the classical Jacobi triple product formula (see [5], Theorem 14.6)

$$\prod_{n\geq 1}(1-q^n)\prod_{n\geq 0}(1-q^nU)\prod_{n>0}(1-q^nU^{-1}) = \sum_{n\in\mathbb{Z}}(-1)^n q^{n(n-1)/2}U^n,$$

together with the fact that $\prod_{n\geq 1}(1-q^n)$ is a unit in $\mathcal{O}_K$. As a meromorphic function on Y, the function $\Theta(U)$ has simple zeroes at all cusps of Y and no poles. Moreover, just from the definition, we easily obtain that the theta function $\Theta(U)$ has the following properties

$$\Theta(U^{-1}) = -U^{-1}\Theta(U), \quad \Theta(q^{-1}U) = -q^{-1}U\Theta(U).$$

The operation $U \mapsto q^{-1}U$ corresponds to"translation by one line" on the underlying topological space of the special fibre of $\mathfrak{Y}$, hence also to translation by one on the set of labels $\mathbb{Z}$. Similarly, the operation $U \mapsto U^{-1}$ defines an automorphism of $\mathfrak{Y}$ coming from the automorphism $[-1] : E \to E$ of the elliptic curve E. On the special fibre $\mathfrak{Y}_k$ this automorphism corresponds to changing the order of projective lines given by multiplication by -1 on the set of labels $\mathbb{Z}$.

Assume that q has a square root in K. We consider another cover $\ddot{\mathcal{Y}} \to \mathcal{Y}$ of formal schemes of degree 2 by taking square root $\ddot{U} = U^{1/2}$ of the function U. The scheme $\ddot{\mathcal{Y}}$ may be defined using the **Proj** functor by the same formula as $\mathcal{Y}$, where we replace U by $\ddot{U}$ and change q to $q^{1/2}$. Thus, the special fibre of $\ddot{\mathcal{Y}}$ is also a chain of projective lines and the map $\ddot{\mathcal{Y}} \to \mathcal{Y}$ defines a bijection between sets of irreducible components in the special fibre. Analytically, it

gives rise to a cover $\ddot{Y} \to Y$ of rigid spaces corresponding to the square map $(\cdot)^2 : K^\times \to K^\times$. Similarly as before, we define the set of cusps of $\ddot{Y}$ as the preimage of the unique cusp of X under the composition $\ddot{Y} \to Y \to X$. Thus, cusps on $\ddot{Y}$ correspond to the set $\{\pm q^{i/2}\}_{i\in\mathbb{Z}}$. When the residue characteristic p is different than two, then the scheme $\ddot{\mathcal{Y}}$ defines a stable model of $\ddot{Y}$, in the sense that reductions of cusps (corresponding to points $\pm q^{i/2}$, for all $i \in \mathbb{Z}$) to the special fibre lie in the smooth locus and are pairwise distinct. On the other hand, when the residue characteristic $p = 2$, then the stable model has additional lines coming from blowups performed at each line (cf. Lemma 3.4.6). Summarizing, we have the following picture of models and formal schemes

$$\begin{array}{ccccc}
\ddot{\mathcal{Y}} & \rightsquigarrow & \ddot{\mathfrak{Y}} & \dashrightarrow & \ddot{Y} \\
\downarrow & & \downarrow & & \downarrow \\
\mathcal{Y} & \rightsquigarrow & \mathfrak{Y} & \dashrightarrow & Y \\
\downarrow & & \downarrow & & \downarrow \\
\mathcal{X} & \rightsquigarrow & \mathfrak{X} & \dashrightarrow & X
\end{array}
\qquad
\begin{array}{c}
(K^{\mathrm{alg}})^\times \\
\downarrow{\scriptstyle (\cdot)^2} \\
(K^{\mathrm{alg}})^\times \\
\downarrow \\
(K^{\mathrm{alg}})^\times/q^{\mathbb{Z}}.
\end{array}$$

Following [29], we introduce another function, which we will be our main object of interest

$$\ddot{\Theta}(\ddot{U}) = \ddot{U}\Theta(\ddot{U}^2) = \ddot{U}\prod_{n\geq 0}(1-q^n\ddot{U}^2)\prod_{n>0}(1-q^n\ddot{U}^{-2}).$$

The theta function $\ddot{\Theta}(\ddot{U})$ is a global section of the structure sheaf on the formal scheme $\ddot{\mathfrak{Y}}$ and defines a meromorphic function on the analytic curve $\ddot{Y}$. The set of zeroes of $\ddot{\Theta}(\ddot{U})$ is equal to the set of cusps $\{\pm q^{i/2}\}_{i\in\mathbb{Z}}$ of $\ddot{Y}$ and every zero occurs with multiplicity one. We easily check that $\ddot{\Theta}(\ddot{U})$ satisfies the following symmetry relations

$$\ddot{\Theta}(\ddot{U}^{-1}) = -\ddot{\Theta}(\ddot{U}), \quad \ddot{\Theta}(-\ddot{U}) = -\ddot{\Theta}(\ddot{U}),$$

together with the "translation" relation:

$$\ddot{\Theta}(q^{-i/2}\ddot{U}) = (-1)^i q^{-i^2/2}\ddot{U}^{2i}\ddot{\Theta}(\ddot{U}), \quad \text{for all } i \in \mathbb{Z}.$$

We are going to give a group theoretic construction of the Kummer class of the theta function $\ddot{\Theta}(\ddot{U})$. First, following [29], we define certain subquotients of the tempered fundamental group Π_X^{tp}. There is a canonical quotient $\Pi_X^{\mathrm{tp}} \twoheadrightarrow \mathbb{Z}$ corresponding to the analytic cover $Y \to X$. Define the kernel of this quotient to be Π_Y^{tp}, so we have a short exact sequence

$$1 \to \Pi_Y^{\mathrm{tp}} \to \Pi_X^{\mathrm{tp}} \to \mathbb{Z} \to 1.$$

Similarly, we define groups Δ_X^{tp} and Δ_Y^{tp} to fit in the following diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_Y^{\mathrm{tp}} & \longrightarrow & \Pi_Y^{\mathrm{tp}} & \longrightarrow & G_K & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \Delta_X^{\mathrm{tp}} & \longrightarrow & \Pi_X^{\mathrm{tp}} & \longrightarrow & G_K & \longrightarrow & 1. \end{array}$$

We define Π_X and Δ_X to be the profinite completions of Π_X^{tp} and Δ_X^{tp} and identify them with the étale fundamental group and the geometric étale fundamental group of X, respectively. Thus, we have the usual short exact sequence

$$1 \to \Delta_X \to \Pi_X \to G_K \to 1.$$

When G is a topological group we write, $[G, G]$ for the topological commutator subgroup which is defined as the closure of the usual commutator subgroup of G. Next, we define the following quotients of the geometric fundamental group

$$\Delta_X^{\mathrm{ell}} = \Delta_X/[\Delta_X, \Delta_X], \qquad \Delta_X^{\Theta} = \Delta_X/[\Delta_X, [\Delta_X, \Delta_X]].$$

The notation is explained as follows: superscript ell corresponds to all étale covers of X which extend to étale covers of the underlying elliptic curve E, and superscript Θ describes, as we will see later, étale covers needed to define the Kummer class of the function $\Theta(U)$. Moreover, since the group Δ_X is a free profinite group on two generators, we know that the theta quotient Δ_X^{Θ} has noncanonically the structure of the Heisenberg group:

$$\begin{bmatrix} 1 & \widehat{\mathbb{Z}} & \widehat{\mathbb{Z}} \\ 0 & 1 & \widehat{\mathbb{Z}} \\ 0 & 0 & 1 \end{bmatrix}.$$

Define Δ_Θ to be the kernel of the natural surjection $\Delta_X^{\Theta} \twoheadrightarrow \Delta_X^{\mathrm{ell}}$, it gives us the short exact sequence

$$1 \to \Delta_\Theta \to \Delta_X^{\Theta} \to \Delta_X^{\mathrm{ell}} \to 1,$$

which similarly may be represented in a matrix group form

$$1 \longrightarrow \begin{bmatrix} 1 & 0 & \widehat{\mathbb{Z}} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & \widehat{\mathbb{Z}} & \widehat{\mathbb{Z}} \\ 0 & 1 & \widehat{\mathbb{Z}} \\ 0 & 0 & 1 \end{bmatrix} \longrightarrow \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}} \longrightarrow 1.$$

Observe, that when X is a punctured elliptic curve the quotient Δ_X^{Θ} is equal to the maximal cuspidally central quotient introduced in Section 1.6. This can be seen, for example, from the explicit group presentation of the group Δ_X given by

$$\Delta_X \cong \langle a, b, c \mid [a, b]c = 1 \rangle.$$

In particular, for every inertia group $I \subset \Delta_X$ of the cusp, the surjection $\Delta_X \twoheadrightarrow \Delta_X^{\Theta}$ rectricted to I induces a natural isomorphism $I \cong \Delta_{\Theta}$.

Going back to the tempered case, we define quotients

$$\Delta_X^{\mathrm{tp}} \twoheadrightarrow (\Delta_X^{\mathrm{tp}})^{\Theta} \twoheadrightarrow (\Delta_X^{\mathrm{tp}})^{\mathrm{ell}}$$

by pushing out the following quotients

$$\Delta_X \twoheadrightarrow \Delta_X^{\Theta} \twoheadrightarrow \Delta_X^{\mathrm{ell}}.$$

Thus, we obtain two exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_{\Theta} & \longrightarrow & (\Delta_X^{\mathrm{tp}})^{\Theta} & \longrightarrow & (\Delta_X^{\mathrm{tp}})^{\mathrm{ell}} & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \Delta_{\Theta} & \longrightarrow & \Delta_X^{\Theta} & \longrightarrow & \Delta_X^{\mathrm{ell}} & \longrightarrow & 1. \end{array}$$

Again, the upper row can be noncanonically represented in a matrix group form

$$1 \longrightarrow \begin{bmatrix} 1 & 0 & \widehat{\mathbb{Z}} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & \widehat{\mathbb{Z}} & \widehat{\mathbb{Z}} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{bmatrix} \longrightarrow \widehat{\mathbb{Z}} \times \mathbb{Z} \longrightarrow 1,$$

which shows the difference between the group Δ_X and Δ_X^{tp} coming from the analytic $\mathbb{Z}$-cover $Y \to X$.

Similarly, we define quotients

$$\Delta_Y^{\mathrm{tp}} \twoheadrightarrow (\Delta_Y^{\mathrm{tp}})^{\Theta} \twoheadrightarrow (\Delta_Y^{\mathrm{tp}})^{\mathrm{ell}} \quad \text{and} \quad \Pi_Y^{\mathrm{tp}} \twoheadrightarrow (\Pi_Y^{\mathrm{tp}})^{\Theta} \twoheadrightarrow (\Pi_Y^{\mathrm{tp}})^{\mathrm{ell}},$$

by pushing out the following quotients

$$\Delta_X^{\mathrm{tp}} \twoheadrightarrow (\Delta_X^{\mathrm{tp}})^{\Theta} \twoheadrightarrow (\Delta_X^{\mathrm{tp}})^{\mathrm{ell}}.$$

Hence we have a short exact sequence

$$1 \to \Delta_{\Theta} \to (\Delta_Y^{\mathrm{tp}})^{\Theta} \to (\Delta_Y^{\mathrm{tp}})^{\mathrm{ell}} \to 1,$$

which may be represented as

$$1 \longrightarrow \begin{bmatrix} 1 & 0 & \widehat{\mathbb{Z}} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & \widehat{\mathbb{Z}} & \widehat{\mathbb{Z}} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 1$$

Finally, we define quotients

$$\Delta_{\ddot{Y}}^{\mathrm{tp}} \twoheadrightarrow (\Delta_{\ddot{Y}}^{\mathrm{tp}})^{\Theta} \twoheadrightarrow (\Delta_{\ddot{Y}}^{\mathrm{tp}})^{\mathrm{ell}} \quad \text{and} \quad \Pi_{\ddot{Y}}^{\mathrm{tp}} \twoheadrightarrow (\Pi_{\ddot{Y}}^{\mathrm{tp}})^{\Theta} \twoheadrightarrow (\Pi_{\ddot{Y}}^{\mathrm{tp}})^{\mathrm{ell}},$$

by pushing out the quotients

$$\Delta_{Y}^{\mathrm{tp}} \twoheadrightarrow (\Delta_{Y}^{\mathrm{tp}})^{\Theta} \twoheadrightarrow (\Delta_{Y}^{\mathrm{tp}})^{\mathrm{ell}}.$$

Thus, we have a short exact sequence

$$1 \to \Delta_{\Theta} \to (\Delta_{\ddot{Y}}^{\mathrm{tp}})^{\Theta} \to (\Delta_{\ddot{Y}}^{\mathrm{tp}})^{\mathrm{ell}} \to 1,$$

which again may be represented as

$$1 \longrightarrow \begin{bmatrix} 1 & 0 & \widehat{\mathbb{Z}} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 2\widehat{\mathbb{Z}} & \widehat{\mathbb{Z}} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \longrightarrow 2\widehat{\mathbb{Z}} \longrightarrow 1.$$

After these preparations, we will consider Kummer classes of theta functions $\Theta(U)$ and $\ddot{\Theta}(\ddot{U})$. It follows from [29], Proposition 1.1 and Lemma 1.2 that all covers of Y needed to define cohomology classes of these functions come from the quotient $(\Pi_{Y}^{\mathrm{tp}})^{\Theta}$. Therefore, we obtain two Kummer classes

$$\eta_{\Theta} \in H^1((\Pi_{Y}^{\mathrm{tp}})^{\Theta}, \widehat{\mathbb{Z}}(\mu)) \quad \text{and} \quad \ddot{\eta}_{\Theta} \in H^1((\Pi_{\ddot{Y}}^{\mathrm{tp}})^{\Theta}, \widehat{\mathbb{Z}}(\mu)).$$

We remark here our notation of these cohomology classes slightly differs from the notation used in [29]. We have seen that the quotient $\Delta_X \twoheadrightarrow \Delta_X^{\Theta}$ induces a natural isomorphism between an inertia group I of the cusp and the cyclotome Δ_{Θ}. Hence, by composing with the canonical isomorphism $I \cong \widehat{\mathbb{Z}}(\mu)$, we obtain an isomorphism $\widehat{\mathbb{Z}}(\mu) \cong \Delta_{\Theta}$, which we will call canonical as well. Therefore, we have two cohomology classes (denoted in the same way)

$$\eta_{\Theta} \in H^1((\Pi_{Y}^{\mathrm{tp}})^{\Theta}, \Delta_{\Theta}) \quad \text{and} \quad \ddot{\eta}_{\Theta} \in H^1((\Pi_{\ddot{Y}}^{\mathrm{tp}})^{\Theta}, \Delta_{\Theta}).$$

To characterize the Kummer class of the theta function $\ddot{\Theta}(\ddot{U})$ we will use the following two exact sequences

$$1 \to H^1(G_K, \Delta_\Theta) \to H^1((\Pi_{\ddot{Y}}^{\mathrm{tp}})^\Theta, \Delta_\Theta) \to \mathrm{Hom}((\Delta_{\ddot{Y}}^{\mathrm{tp}})^\Theta, \Delta_\Theta) \to 1$$

and

$$1 \to \mathrm{Hom}((\Delta_{\ddot{Y}}^{\mathrm{tp}})^{\mathrm{ell}}, \Delta_\Theta) \to \mathrm{Hom}((\Delta_{\ddot{Y}}^{\mathrm{tp}})^\Theta, \Delta_\Theta) \to \mathrm{Hom}(\Delta_\Theta, \Delta_\Theta) \to 1.$$

We are going to specify a subset of cohomology classes in $H^1((\Pi_{\ddot{Y}}^{\mathrm{tp}})^\Theta, \Delta_\Theta)$ satisfying certain properties. Recall our choice of bijection between the set of cusps on Y and the set of integers $\mathbb{Z}$. We choose an automorphism ι_Y of Π_Y^{tp} corresponding to multiplication by -1 on the set of labels $\mathbb{Z}$. This can be defined group theoretically, it is the unique (up to inner automorphisms) involution fixing the label 0 and lying over the automorphisms of Π_X^{tp} induced by multiplication by -1 on the level of elliptic curve E. Using the model $\mathcal{Y}$ it corresponds to a morphism defined by $U \mapsto U^{-1}$. Let now η be a cohomology class in the group $H^1((\Pi_{\ddot{Y}}^{\mathrm{tp}})^\Theta, \Delta_\Theta)$. We impose two conditions, as follows.

1. We require that the restriction of η to $\mathrm{Hom}(\Delta_\Theta, \Delta_\Theta)$ is equal to the identity map. This property comes from the fact that the theta function $\ddot{\Theta}(\ddot{U})$ has simple zeroes at all cusps (recall the choice of the canonical isomorphism $\Delta_\Theta \cong \widehat{\mathbb{Z}}(\mu)$).

2. We further require that the restriction of η to $\mathrm{Hom}((\Delta_{\ddot{Y}}^{\mathrm{tp}})^\Theta, \Delta_\Theta)$ is invariant with respect to the action of ι_Y. This property corresponds to the invariance of $\ddot{\Theta}(\ddot{U})$, up to a sign, with respect to operations $\ddot{U} \mapsto \ddot{U}^{-1}$ and $\ddot{U} \mapsto -\ddot{U}$.

Observe that the set of cohomology classes satisfying both conditions as above is a $\widehat{K^\times}$-torsor generated by the Kummer class of the theta function $\ddot{\Theta}(\ddot{U})$. Indeed, the classes η_Θ and η_U form a $\widehat{\mathbb{Z}}$-basis of the free $\widehat{\mathbb{Z}}$-module $\mathrm{Hom}((\Pi_{\ddot{Y}}^{\mathrm{tp}})^\Theta, \Delta_\Theta)$ and we have the following commutative diagram of groups

$$\begin{array}{ccccc}
\mathrm{Hom}((\Pi_{\ddot{Y}}^{\mathrm{tp}})^\Theta, \Delta_\Theta) & \xrightarrow{\cong} & \mathrm{Hom}(\widehat{\mathbb{Z}} \oplus 2\widehat{\mathbb{Z}}, \widehat{\mathbb{Z}}) & \xrightarrow{\cong} & \widehat{\mathbb{Z}}\eta_\Theta \oplus \frac{1}{2}\widehat{\mathbb{Z}}\eta_U \\
\uparrow & & \uparrow & & \uparrow \\
\mathrm{Hom}((\Pi_{\ddot{Y}}^{\mathrm{tp}})^\Theta, \Delta_\Theta) & \xrightarrow{\cong} & \mathrm{Hom}(\widehat{\mathbb{Z}}^2, \widehat{\mathbb{Z}}) & \xrightarrow{\cong} & \widehat{\mathbb{Z}}\eta_\Theta \oplus \widehat{\mathbb{Z}}\eta_U.
\end{array}$$

Similarly, the classes $\eta_{\ddot{\Theta}} = \eta_\Theta + \frac{1}{2}\eta_U$ and $\eta_{\ddot{U}} = \frac{1}{2}\eta_U$ form a basis of the free $\widehat{\mathbb{Z}}$-module $\mathrm{Hom}((\Pi_{\ddot{Y}}^{\mathrm{tp}})^\Theta, \Delta_\Theta)$. Let $\eta = a\eta_{\ddot{\Theta}} + b\eta_{\ddot{U}}$ be any class in $\mathrm{Hom}((\Pi_{\ddot{Y}}^{\mathrm{tp}})^\Theta, \Delta_\Theta)$, for some $a, b \in \widehat{\mathbb{Z}}$. Because the theta function $\ddot{\Theta}(\ddot{U})$ has a simple zero at each

cusp we see that the cohomology class η satisfies the condition (1) if and only if $a = 1$. Moreover, from the transformation formula, the class $\eta_{\ddot{\Theta}}$ is invariant with respect to the action of ι_Y whereas the Kummer class $\eta_{\ddot{U}}$ is an eigenvector with eigenvalue -1. Hence, the class η satisfies the condition (2) if and only if $b = 0$. Therefore, we obtain a group theoretic construction of the $\widehat{K^\times}$-torsor generated by the Kummer class of the function of $\ddot{\Theta}(\ddot{U})$.

The above computation explains the necessity of introducing the double cover $\ddot{Y} \to Y$. Indeed, up to a constant, Kummer classes of meromorphic functions on Y satisfying the condition (1) are those of the form $a\eta_U + \eta_\Theta$. Then, invariance with respect to the automorphism ι_Y forces $a = 1 - a$, hence $a = 1/2$. Finally, we observe that the reconstruction is independent on the choice of a generator of the group $\mathrm{Gal}(Y/X)$. Indeed, it follows from the invariance of $\ddot{\Theta}(\ddot{U})$ (up to a constant) under the automorphism $\ddot{U} \mapsto \ddot{U}^{-1}$.

3.4 Evaluation points

So far we have seen that we may recover the Kummer class of the theta function $\ddot{\Theta}(\ddot{U})$ up to a constant from $\widehat{K^\times}$, i.e., arbitrary cohomology class in $H^1(G_K, \widehat{\mathbb{Z}}(\mu))$. We may reduce this indeterminacy further from $\widehat{K^\times}$ to $K^\times$ by evaluating Kummer classes on decomposition groups of rational points. Indeed, let P be an L-rational point on $\ddot{Y}$ which is not a cusp, for some finite extension L/K, and let D_P be a decomposition group of P. Recall the valuation map already used in previous two chapters

$$H^1(\Pi^{\mathrm{tp}}_{\ddot{Y}}, \Delta_\Theta) \to H^1(D_P, \Delta_\Theta) \cong H^1(G_L, \Delta_\Theta) \cong H^1(G_L, \widehat{\mathbb{Z}}(G_L)) \twoheadrightarrow \widehat{\mathbb{Z}}.$$

Then, if $\eta = \eta_u + \ddot{\eta}_\Theta$ is a cohomology class for some $u \in \widehat{L^\times}$, then the valuation of $\eta(P)$ lies in the subset $\mathbb{Z} \subset \widehat{\mathbb{Z}}$ if and only if $u \in L^\times$. Therefore, we easily obtain a $K^\times$-torsor of multiples of the theta function $\ddot{\Theta}(\ddot{U})$.

Definition 3.4.1. Any function θ of the form $\theta = u\ddot{\Theta}$ for some $u \in (K^{\mathrm{alg}})^\times$ will be called a *standard* theta function.

The above definition is analogous to Definition 1.8.2. Observe that a cohomology class of a standard theta function θ determines a discrete tangential section of the surjection $\Pi^{\mathrm{tp}}_X \twoheadrightarrow G_K$ at the cusp x, as defined in Section 2.5. Indeed, let Q be one of two cusps of the curve $\ddot{Y}$ with label 0. Since the function θ has a single pole at the cusp Q, using the construction from Lemma 2.5.1 we obtain conjugacy class of tangential sections of the surjection $\Pi^{\mathrm{tp}}_{\ddot{Y}} \twoheadrightarrow G_K$. Thus, by composing with the inclusion $\Pi^{\mathrm{tp}}_{\ddot{Y}} \hookrightarrow \Pi^{\mathrm{tp}}_X$, we obtain a conjugacy class

of tangential sections s_θ of the surjection $\Pi_X^{\mathrm{tp}} \twoheadrightarrow G_K$, which does not depend on the choice of the cusp Q.

Moreover, recall from Section 2.5, that the $\mathcal{O}_K$-module structure provided by the stable model $\mathcal{X}$ gives rise to the notion of an integral tangential section. Hence, we may introduce the following definition.

Definition 3.4.2. We say that a standard theta function θ is *integral* if the tangential section s_θ is integral.

Hence the set of integral theta functions is a $\mathcal{O}_K^\times$-torsor. Moreover, we have the following lemma.

Lemma 3.4.3. *Let $\theta = u\ddot{\Theta}$ be a standard theta function. Then, the function θ is integral if and only if u is a p-adic unit.*

Proof. Let $a = (\prod_{n\geq 1}(1-q^n))^{-1}$, which is a p-adic unit. Using Jacobi triple product formula we have

$$\Theta(U) = a\sum_{n\in\mathbb{Z}}(-1)^n q^{n(n-1)/2}U^n,$$

hence

$$\ddot{\Theta}(\ddot{U}) = a\sum_{n\in\mathbb{Z}}(-1)^n q^{n(n-1)/2}\ddot{U}^{2n+1}.$$

Observe that every coefficient of $\ddot{\Theta}(\ddot{U})$ is an integral element of K. Moreover, the reduction of $\ddot{\Theta}$ modulo the maximal ideal of $\mathcal{O}_K$ is nonzero as it is equal to $a(\ddot{U}^{-1} - \ddot{U})$. Since $\ddot{\Theta}(\ddot{U})$ has simple zero at every cusp, these two properties imply that the theta function $\ddot{\Theta}$ is integral, in the sense of Definition 3.4.2. Indeed, it follows from the fact that the formal scheme $\mathfrak{X}$ is equal to the quotient of the formal scheme $\mathfrak{Y}$ and that the stable model $\mathcal{X}$ is obtained as the algebraization of the formal scheme $\mathfrak{X}$. Therefore, any integral theta function is of the form $u\ddot{\Theta}$ for some p-adic unit u. □

We will need one more definition.

Definition 3.4.4. Let P be a K-rational point on the curve $\ddot{Y}$ which is not a cusp. We say that a standard theta function θ is *normalized* at P if its value $\theta(P)$ at the point P is equal to one.

The condition of being normalized at P is obviously group theoretic. Indeed, let $D_P \subset \Pi_{\ddot{Y}}^{\mathrm{tp}}$ be a decomposition group of the point P, hence we have the restriction map

$$H^1(\Pi_{\ddot{Y}}^{\mathrm{tp}}, M_X) \to H^1(D_P, M_X).$$

Then θ is normalized at P if and only of the restriction of η_f along the above map is equal to the trivial element of the group $H^1(D_P, M_X) \cong \widehat{K^\times}$.

We denote by Γ the group of automorphisms of $\ddot{Y}$ generated by the automorphisms $\ddot{U} \mapsto \ddot{U}^{-1}$ and $\ddot{U} \mapsto -\ddot{U}$. Thus, we have $\Gamma \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Finally, we may state the main theorem of this chapter.

Theorem 3.4.5. *There exists a rational point P on the curve $\ddot{Y}$ having the following two properties:*

1. *There exists a group theoretic reconstruction, from the topological group Π_X and a chosen automorphism i_Y of Π_Y, of the Γ-orbit of the conjugacy class of decomposition groups D_P of the point P,*

2. *After extending the base field to $K(P)$, the theta function normalized at the point P is integral.*

In fact, the point P is given explicitly as a lift of a certain 6th torsion point on E.

To prove the above theorem, we first observe that the theta function $\theta = u\ddot{\Theta}$ normalized at the point P is integral if and only if $\ddot{\Theta}(P)$ is a p-adic unit. Indeed, we have seen in Lemma 3.4.3 that θ is integral if and only if u is a p-adic unit. Since θ is normalized at P we have $\theta(P) = u\ddot{\Theta}(P) = 1$, hence u is a unit if and only if $\ddot{\Theta}(P) \in \mathcal{O}_K^\times$.

Before we continue, we need to recall the notion of a dual semi-graph of a stable marked curve C (see [23], Appendix). Let C_k be the special fibre of the (marked) stable model of C. Then, we have the usual notion of a dual graph (see [19], Chapter X), whose vertices v correspond to irreducible components Z_v and edges correspond to intersection between components. Moreover, for every marked point x lying in the smooth locus of the component Z_v we attach an open edge e_v abutting to the vertex v. In this way we obtain a semi-graph which we call a dual semi-graph of the stable curve C.

To construct the decomposition group of the point P from Theorem 3.4.5 we are going to use [23], Lemma 2.3 which says that if C is a hyperbolic curve over a local field K with a stable reduction over $\mathcal{O}_K$, then we may recover the dual graph $\mathbb{G}_C$ of the special fibre of the stable model of the curve C. Moreover, this algorithm also gives a bijection between the set of cusps and the the set of open edges of the semi-graph $\mathbb{G}_C$. We are going to apply this theorem to identify some "special" torsion points of the elliptic curve E.

Take a natural number n and let X_n be a marked curve over $K(E[n])$ obtained from the Tate curve E, with the divisor of marked points given by all

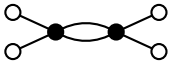
n-torsion points. The next lemma describes the structure of special fibres of stable models of some of those curves.

Lemma 3.4.6.

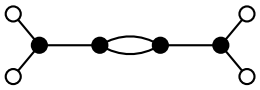
Assume that n is a prime number. Then the graph of the special fibre of the stable model of the marked curve X_n is equal to

- *$(n \neq p)$ a standard n-gon with n open edges attached to each vertex of the n-gon;*
- *$(n = p)$ a modified standard n-gon, where to each vertex v from the standard n-gon we attach a semi-graph consisting of one vertex v', one closed edge $[v, v']$ connecting v' to v together with n open edges attached to the vertex v'.*

For example, for $n = 2$ it is one of the following:

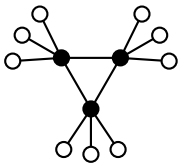


$p \neq 2$

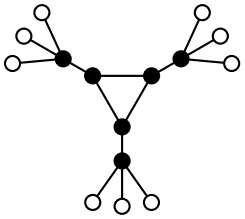


$p = 2$

For $n = 3$ is one of the following:



$p \neq 3$



$p = 3$

Proof. This follows from a well-known computation of a blowup of the scheme $\operatorname{Spec} R[X, Y]/(XY - a)$ at the point (X, Y, π), where R is a discrete valuation ring and a belongs to the maximal ideal of R (see Chapter 8, Example 3.53 in [19]). We blow up the model $\mathcal{X}$ at the cusp n times after which we obtain another model $\mathcal{X}'$ with the special fibre equal to the n-gon of projective lines and with the property that all marked points of X_n reduce to the smooth locus of $\mathcal{X}'_k$. When $n \neq p$, then then this model is already a stable model since reductions of torsion points $\{\zeta_n^i,\ 0 \leq i \leq n-1\}$ to the special fibre are pairwise distinct. Indeed, it follows from the fact that the product

$$\prod_{1 \leq i \leq n-1} (1 - \zeta_n^i) = n$$

is a p-adic unit.

Suppose now that $n = p$. Then, for a fixed integer $0 \leq j \leq n-1$, all n-torsion points from the set

$$T_j = \{\zeta_n^i q^{j/n},\ 0 \leq i \leq n-1\}$$

reduce to the same point s_j on the special fibre of $\mathcal{X}'$. However, observe that the p-adic valuations of numbers $1-\zeta_n^i$, for all $1 \leq i \leq p-1$, are equal. Indeed, modulo the maximal ideal of $\mathcal{O}_K$ we have the equality

$$\frac{1-\zeta_n^i}{1-\zeta} = \sum_{0 \leq j \leq i-1} \zeta_n^j \equiv i$$

which is a p-adic unit. Therefore, after blowing up the model $\mathcal{X}'$ again at points s_j we obtain new projective lines L_j such that the reduction of the points from the set S_j lie on the smooth locus of L_j and are pairwise distinct. □

Remark 3.4.7. A similar description may be obtained as well in the case of n-torsion, for every natural number n. In the following, we will need only torsion points of order two and three.

Corollary 3.4.8. *Consider the subgroups $S_2 = \{1, -1\} \subset E[2](K^{\mathrm{alg}})$ and $S_3 = \{1, \zeta_3, \zeta_3^2\} \subset E[3](K^{\mathrm{alg}})$. Then, the conjugacy classes of decomposition groups of rational points belonging to S_2 and S_3 can be reconstructed group theoretically from the topological group Π_X.*

Proof. As we have discussed in Section 3.2, by applying the tempered version of elliptic cuspidalization we may reconstruct decomposition groups of torsion points together with the surjection $\Pi_{X_n}^{\mathrm{tp}} \twoheadrightarrow \Pi_X^{\mathrm{tp}}$ of topological groups, for every natural number n. Then, using the reconstruction of the dual graph of the special fibre of the stable model, applied to profinite completions of groups $\Pi_{X_n}^{\mathrm{tp}}$ for $n = 2$ and $n = 3$, we may distinguish decomposition group corresponding to subgroups S_2 and S_3. Indeed, from Lemma 3.4.6, these subgroups are precisely the subsets of marked points lying on the same irreducible component as the origin of the elliptic curve E. □

In particular, the above corollary provides a method to find the conjugacy class of decomposition groups of the 2-torsion point determined by -1, which is a normalization point used in [29].

Corollary 3.4.9. *Let $\zeta_6 \in K^{\mathrm{alg}}$ be a primitive 6th root of unity. Then the decomposition groups of torsion points $\zeta_6, \zeta_6^{-1} \in E[6](K^{\mathrm{alg}})$ may be reconstructed group theoretically from the topological group Π_X^{tp}, as subgroups of Π_X^{tp},*

Proof. Recall that the group structure on the set of decomposition groups of torsion points may be constructed group theoretically. Therefore, since we have already obtained ζ_2 and ζ_3, we may construct the subgroup of the group of 6th torsion points generated by ζ_2 and ζ_3. Then, ζ_6 and ζ_6^{-1} are obtained as generators of this subgroup. □

Finally, we come back to the proof of the main theorem.

Proof of Theorem 3.4.5. First, we lift points ζ_6 and ζ_6^{-1} from the curve X to Y. In terms of decomposition groups, we intersect a conjugacy class of decomposition groups with the subgroup $\Pi_Y^{\mathrm{tp}} \subset \Pi_X^{\mathrm{tp}}$ to obtain a $\mathrm{Aut}(Y/X)$-torsor of conjugacy classes of preimages of points ζ_6 and ζ_6^{-1} to the cover $Y \to X$. These preimages correspond to sets of points

$$\{\zeta_6 q^k\}_{k\in\mathbb{Z}} \quad \text{and} \quad \{\zeta_6^{-1} q^k\}_{k\in\mathbb{Z}}.$$

Using again the anabelian reconstruction of the dual graph applied to all finite subcovers of $Y \to X$ we may choose the preimages corresponding to the label 0, namely the points ζ_6, ζ_6^{-1} on the curve Y. Lifting them further to the cover $\ddot{Y} \to Y$ (which corresponds to the map $x \mapsto x^2$), we obtain the following set of four points on the curve $\ddot{Y}$

$$\{\zeta_{12}, \zeta_{12}^{-1}, -\zeta_{12}, -\zeta_{12}^{-1}\}.$$

It is an orbit of the point $P = \zeta_{12}$ under the action of the group Γ. Because our construction was entirely group theoretical, the point P satifies the first condition from the statement of Theorem 3.4.5.

We claim that the point P satisfies also the second condition. Indeed, we observe from the product formula

$$\ddot{\Theta}(\ddot{U}) = \ddot{U}\Theta(\ddot{U}^2) = \ddot{U}\prod_{n\geq 0}(1-q^n\ddot{U}^2)\prod_{n>0}(1-q^n\ddot{U}^{-2})$$

that $\ddot{\Theta}(P)$ is a p-adic unit if and only if $1-\zeta_6$ is a p-adic unit. Since $\Phi_6(x) = x^2 - x + 1$, we see that

$$(1-\zeta_6)(1-\zeta_6^{-1}) = \Phi_6(1) = 1,$$

which finishes the proof. □

Remark 3.4.10. In fact, for every natural number n, we may use the same method to reconstruct decomposition groups of the subgroup of n-torsion points generated by ζ_n. Then, it is interesting to note that among all these points the only choice of a point P satisfying both conditions in Theorem 3.4.5 comes from $n = 6$. Indeed, the properties of the natural number n that we use are $\varphi(n) \leq 2$ and $\Phi_n(1) = 1$, which occurs only for $n = 6$.

Therefore, we have the following immediate corollary.

Corollary 3.4.11. *Assume that the field K contains 12th roots of unity. Then, the $\mathcal{O}_K^\times$-torsor of Kummer classes of integral theta functions has a group theoretic trivialization, well defined up to a sign.*

Proof. Indeed, using Theorem 3.4.5 we reconstruct the Γ-orbit of the point P and we may trivialize this $\mathcal{O}_K^\times$-torsor by normalizing at a point P. Since we have $\ddot{\Theta}(P) = \pm\ddot{\Theta}(\gamma P)$ for every $\gamma \in \Gamma$, this trivialization is well defined up to multiplication by -1. □

3.5 Local height on Tate curve

In this section we are going to prove another version of Theorem 1.1.1. Let E be an elliptic curve over K with essentially bad reduction and consider the hyperbolic curve $X = E \setminus \{O\}$. Moreover, let P be a nonzero L-rational, point of E, for some finite extension L/K. The point P defines a section over an open subgroup of the surjection $\Pi_X^{\mathrm{tp}} \twoheadrightarrow G_K$. In other words, we have a commutative diagram of topological groups

$$\begin{array}{ccc} & & G_L \\ & \overset{s}{\swarrow} & \big\downarrow \\ \Pi_X^{\mathrm{tp}} & \longrightarrow & G_K. \end{array} \tag{3.1}$$

Then, we have the following proposition.

Proposition 3.5.1. *There exists a group theoretic reconstruction of the local height of the point P from the diagram* (3.1) *of topological groups.*

Observe that for the proof of this proposition we may extend the base field by any finite extension, by the invariance of the local height. Therefore, we assume that K contains 12th roots of unity, coordinates of all 2-torison points as well as coordinates of the point P and all its 2-division points. Moreover, we may assume that E has stable reduction over K. Hence, E is a Tate curve E_q for some $q \in K^\times$. Let $\ddot{q}$ be a square root of q, which belongs to K by the above assumptions.

Recall, that we have a group theoretic valuation map

$$v\colon H^1(G_K, M_X) \cong H^1(G_K, \widehat{\mathbb{Z}}(G_K)) \twoheadrightarrow \mathbb{Z}_p$$

induced by the isomorphism $M_X \cong \widehat{\mathbb{Z}}(G_K)$ from Lemma 1.6.3. Therefore, by restricting Kummer classes of standard theta functions θ to decomposition

group of the rational point P we may compute group theoretically the absolute value $v(\theta(P)) \in \mathbb{Q}$.

Lemma 3.5.2. *The absolute value $v(q)$ of the q-parameter of E may be recovered group theoretically from the topological group Π_X^{tp}.*

Proof. Let P be a rational point on $\ddot{Y}$ from the proof of Theorem 3.4.5 and let θ be a theta function normalized at P. Thus we have $\theta = u\ddot{\Theta}$ for some $u \in \mathcal{O}_K^\times$. Consider the orbit of the point P under the action of the group $\mathrm{Aut}(\ddot{Y}/X)$. This orbit of points corresponds to the set $\{\pm\zeta_{12}^{\pm} q^{i/2}\}_{i\in\mathbb{Z}}$. By restricting the Kummer class of θ to decomposition groups of points from this set and computing valuations we construct the following set of values

$$\{v(\theta(\pm\zeta_{12}^{\pm} q^{i/2}))\}_{i\in\mathbb{Z}} = \{i^2 v(\ddot{q})\}_{i\in\mathbb{Z}}.$$

This equality of sets comes from the transformation formula of the theta function Θ. Clearly, this set of integers determines the value $v(q)$. □

Using the uniformization isomorphism $K^\times/q^{\mathbb{Z}} \cong E(K)$, every K-rational point P of E may by uniquely represented by some $u \in K^\times$, satisfying

$$0 \leq v(u) < v(q).$$

We will say that the point P is *integral* if $v(u) = 0$.

Lemma 3.5.3. *With the notation as above, from the diagram* (3.1) *we may determine whether the point P is integral. Moreover, when the point P is not integral, we may reconstruct the set of values $\{v(u), v(q) - v(u)\}$.*

Proof. We lift the point P to the curve Y, hence we obtain a set of points S corresponding to the set $\{uq^i\}_{i\in\mathbb{Z}}$. Since the set S is a torsor over the group $\mathrm{Aut}(Y/X) \cong \mathbb{Z}$, it may be naturally regarded as a sequence of elements, in particular in the set S we have a notion of consecutive points. Next, we may lift points from S to the curve $\ddot{Y}$ to obtain another set of points S' corresponding to the set $\{\pm wq^{i/2}\}_{i\in\mathbb{Z}}$, where $w^2 = u$. Over each element of S lies a pair of elements in S', thus the set S' may be regarded as a sequence of pairs of points.

Let θ be an integral theta function on $\ddot{Y}$. By restricting the cohomology class of θ to decomposition groups of points from S' we may compute the set V of valuations

$$V = \{v(\theta(s'))\}_{s'\in S'}.$$

Since $v(\theta(wq^{i/2})) = v(\theta(-wq^{i/2}))$, the set V may be regarded as a sequence of integers. We may compute this set directly using the transformation formula of the theta function

$$v_i = v(\theta(wq^{i/2})) = -i^2 v(\ddot{q}) - iv(u) + v(\ddot{\Theta}(w)).$$

If we choose an "orientation" of the set V (more precisely, a generator of the group $\mathrm{Aut}(Y/X) \cong \mathbb{Z}$), then we may consider the set V_2 of differences between consecutive elements of V

$$v_{i+1} - v_i = -(2i+1)v(\ddot{q}) - v(u).$$

Finally, we observe that the set V_2 is contained in the set of odd multiples of $v(\ddot{q})$ if and only if we have $v(u) = 0$. Indeed, it follows from the inequality

$$0 \leq v(u) < 2v(\ddot{q}),$$

moreover this characterization does not depend on the choice of orientation of V. Hence, by using Lemma 3.5.2 we may determine group theoretically whether $v(u)$. Furthermore, when $v(u) \neq 0$, then the set V_2 of rational numbers uniquely determines the set $\{v(u), v(q) - v(u)\}$, independently of the choice of an orientation on V. □

Proof of Proposition 3.5.1. When P is not an integral point, then by using Lemma 3.5.3 together with Lemma 3.5.2 we may determine the value $v(q)$ as well as the set

$$\left\{\frac{v(u)}{v(q)}, 1 - \frac{v(u)}{v(q)}\right\}.$$

This uniquely determines the height of the point P, by Proposition 1.2.3 (observe that $B_2(x) = B_2(1-x)$).

Suppose now that P is an integral point, thus $v(u) = 0$. Observe that the set of values V that we computed in the proof of Lemma 3.5.3 is equal to the set of rational numbers

$$\{-i^2 v(\ddot{q}) + v(\ddot{\Theta}(w))\}_{i \in \mathbb{Z}}.$$

Therefore the set V has a unique maximal element equal to $v(\ddot{\Theta}(w))$. Moreover, as $v(u) = 0$, we use the product formula

$$\ddot{\Theta}(\ddot{U}) = \ddot{U} \prod_{n \geq 0} (1 - q^n \ddot{U}^2) \prod_{n > 0} (1 - q^n \ddot{U}^{-2})$$

to compute that $v(\ddot{\Theta}(w)) = v(1-u)$. Thus, we have determined the value $v(1-u)$ and again using Proposition 1.2.3 we may compute the height of P. □

Remark 3.5.4. The statement of Proposition 3.5.1 uses section of the tempered fundamental group Π_X^{tp}, whereas in the Theorem 1.1.1 we used sections of the étale fundamental group Π_X. Obviously, every section of the tempered fundamental group determines a section of the étale fundamental group. One

may ask if it is possible to prove another version of Proposition 3.5.1, where we replace the group Π_X^{tp} by its étale version Π_X. This is indeed possible, here we give a sketch of the proof. Recall that using [23], Lemma 2.3 we may reconstruct the dual graph of the stable model of a hyperbolic curve X from its étale fundamental group Π_X. Applying this reconstruction to all étale covers of X we may distinguish covers coming from topological covers of the dual graph of the stable model. Therefore, one can recover Π_X^{tp} as a subgroup (not topological) of Π_X, determined up to conjugation. Moreover, using [31], Corollary 2.5, we obtain that the image of some conjugate of the section s is contained Π_X^{tp} and is in fact equal to a decomposition group in Π_X^{tp} of the point P. Thus, this reduces the problem to the tempered case already discussed in Proposition 3.5.1.

Chapter 4

Automorphisms of Galois monoids

4.1 Introduction

Let K be a finite extension of $\mathbb{Q}_p$ with the ring of integral elements $\mathcal{O}_K$. For every algebraic field extension L/K we denote by $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L and by $\mathcal{O}_L^\times$ the group of units of the ring $\mathcal{O}_L$. Let $\mathcal{O}_L^\triangleright = \mathcal{O}_L \setminus \{0\}$ be the set of nonzero integral elements, which is a monoid with respect to multiplication. In what follows, we will always consider $\mathcal{O}_L^\triangleright$ as a monoid. If we assume additionally that L/K is a Galois extension with the Galois group $G = \mathrm{Gal}(L/K)$, then we obtain a natural action of G on the monoid $\mathcal{O}_L^\triangleright$. Denote by $G \curvearrowright M$ a pair consisting of a monoid M and a group G acting on M by monoid automorphisms. Consider the group of automorphisms $\mathrm{Aut}(G \curvearrowright M)$ of this pair. Every such automorphism consists of an automorphism α of G and an automorphism β of the monoid M satisfying the following compatibility property

$$\begin{array}{ccc} G \times M & \longrightarrow & M \\ \downarrow{\scriptstyle \alpha\times\beta} & & \downarrow{\scriptstyle \beta} \\ G \times M & \longrightarrow & M, \end{array}$$

where the horizontal arrows correspond to the action of the group G. In this chapter we will be interested in the case when G is the Galois group of a field extension L/K and M is equal ether to the monoid $\mathcal{O}_L^\triangleright$ or to the group $\mathcal{O}_L^\times$.

Consider now the following restriction map

$$\mathrm{Aut}(G \curvearrowright M) \to \mathrm{Aut}(G). \tag{4.1}$$

Its kernel is equal to the group $\mathrm{Aut}_G(M)$ of G-equivariant automorphisms of the monoid M. Then, we have the following theorem of Mochizuki (see [30],

Proposition 3.2 and Proposition 3.3), which motivates theory developed in this chapter.

Theorem 4.1.1. *Suppose that M is equal to the monoid $\mathcal{O}^{\triangleright}_{K^{\mathrm{alg}}}$ where K^{alg} is an algebraic closure of K and G is the Galois group G_K of the field extension K^{alg}/K. Then the restriction map*

$$\mathrm{Aut}(G_K \curvearrowright \mathcal{O}^{\triangleright}_{K^{\mathrm{alg}}}) \to \mathrm{Aut}(G_K)$$

is an isomorphism. Moreover, when M is equal to the group of units $\mathcal{O}^{\times}_{K^{\mathrm{alg}}}$ of p-adic algebraic integers, then the restriction map

$$\mathrm{Aut}(G_K \curvearrowright \mathcal{O}^{\times}_{K^{\mathrm{alg}}}) \to \mathrm{Aut}(G_K)$$

is surjective with kernel naturally isomorphic to the group $\widehat{\mathbb{Z}}^{\times}$.

In particular, the above theorem computes the groups $\mathrm{Aut}_{G_K}(\mathcal{O}^{\triangleright}_{K^{\mathrm{alg}}})$ and $\mathrm{Aut}_{G_K}(\mathcal{O}^{\times}_{K^{\mathrm{alg}}})$, as the trivial group and $\widehat{\mathbb{Z}}^{\times}$, respectively. In this chapter we are going to consider more generally the groups $\mathrm{Aut}_G(\mathcal{O}^{\triangleright}_L)$ and $\mathrm{Aut}_G(\mathcal{O}^{\times}_L)$, for a Galois field extension L/K with $G = \mathrm{Gal}(L/K)$. The main result we prove is the following theorem.

Theorem 4.1.2. *Let L/K be a Galois extension with the Galois group $G = \mathrm{Gal}(L/K)$. Then, there exists an exact sequence of group homomorphisms*

$$1 \to \mathrm{Hom}(V_L, \mathcal{O}^{\times}_K) \to \mathrm{Aut}_G(\mathcal{O}^{\triangleright}_L) \to \mathrm{Aut}_G(\mathcal{O}^{\times}_L) \to V(L/K)^{\times} \to 1.$$

Here, $V_L = \mathcal{O}^{\triangleright}_L/\mathcal{O}^{\times}_L$ and $V(L/K) = \varprojlim_M \mathbb{Z}/e(M/K)\mathbb{Z}$, where M runs through all finite subextensions of L/K and $e(M/K)$ is the ramification degree.

This theorem is proved as Corollary 4.4.17. As a special case we will see that when $V_L \cong \mathbb{Q}$, then the group $\mathrm{Aut}_G(\mathcal{O}^{\triangleright}_L)$ is trivial if and only if the group $\mathrm{Aut}_G(\mathcal{O}^{\times}_L)$ is isomorphic to $\widehat{\mathbb{Z}}^{\times}$. We also give a few applications and examples.

Finally, in the last section we briefly discuss the problem when the restriction map

$$\mathrm{Aut}_G(G \curvearrowright \mathcal{O}^{\triangleright}_L) \to \mathrm{Aut}(G)$$

is surjective. To understand the difficulty of this question it is useful to make the following remark. Denote by $\mathrm{Inn}(G)$ the subgroup of the group of automorphisms $\mathrm{Aut}(G)$ consisting of all inner automorphisms and by $\mathrm{Inn}(G \curvearrowright M)$ the preimage of $\mathrm{Inn}(G)$ under the restriction map (4.1). Then, the map

$$\mathrm{Inn}(G \curvearrowright M) \to \mathrm{Inn}(G)$$

is obviously surjective. Indeed, for every inner automorphism $g \mapsto \sigma g \sigma^{-1}$ we may consider the automorphism $m \mapsto \sigma m$ of M and they together define an automorphism of the pair $G_K \curvearrowright M$. In other words, we have the following commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Aut}_G(M) & \longrightarrow & \mathrm{Inn}(G \curvearrowright M) & \longrightarrow & \mathrm{Inn}(G) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{Aut}_G(M) & \longrightarrow & \mathrm{Aut}(G \curvearrowright M) & \longrightarrow & \mathrm{Aut}(G) & & \end{array}$$

Hence the real difficulty for determining the cokernel of the map (4.1) comes from the fact that the Galois group $\mathrm{Gal}(L/K)$ may have nontrivial outer automorphisms. For example, this is the case when $L = K^{\mathrm{alg}}$.

4.2 Notation

From now on K is a fixed finite extension of $\mathbb{Q}_p$. We recall our convention that a finite extension of a p-adic field $\mathbb{Q}_p$ is called a local field. We write K^{ur} and K^{tm} for the maximal unramified extension and the maximal tamely ramified extension of K, respectively, both contained in a fixed algebraic closure K^{alg}. Moreover, let q be the cardinality of the residue field of K.

For every algebraic field extension L/K define the value monoid V_L as the quotient monoid

$$1 \to \mathcal{O}_L^\times \to \mathcal{O}_L^\triangleright \to V_L \to 1.$$

Hence, V_L is isomorphic to the additive monoid $\mathbb{N}$ of natural numbers if and only if $LK^{\mathrm{ur}}/K^{\mathrm{ur}}$ is finite. Obviously $V_L = \varinjlim_M V_M$, where M runs over all finite subextensions of the extension L/K. We may identify V_L with a submonoid of the additive monoid $\mathbb{Q}_{\geq 0}$ by sending the image of a uniformizer of K to 1. Usually, when the field extension L/K is assumed to be Galois, we will write G as the Galois group of this extension.

Moreover, for every extension L/K, we denote by $\mathfrak{m}_L$ the maximal ideal of $\mathcal{O}_L$. We also have the following subgroups of $\mathcal{O}_L^\times$: the group of principal units $U_L = 1 + \mathfrak{m}_L\mathcal{O}_L$, the subgroup μ_L of all roots of unity in L, the subgroup μ_L^p of roots of unity of p-power order and the subgroup $\mu_L^{p'}$ consisting of roots of unity of order prime to p. Elements of the group μ_L^p and $\mu_L^{p'}$ will also be called p-roots of unity and p'-roots of unity, respectively. When L/K is finite then all these subgroups of $\mathcal{O}_L^\times$ are characteristic subgroups of the monoid $\mathcal{O}_L^\triangleright$. Similarly, when the field extension L/K is Galois with the Galois group G, then they are characteristic subgroups of the pair $G \curvearrowright \mathcal{O}_L^\triangleright$.

To indicate G-invariance we always use the lower subscript $(\cdot)_G$, as for example in the group $\mathrm{Aut}_G(\mathcal{O}_L^{\triangleright})$ of G-equivariant automorphisms.

4.3 General properties

We will consider short exact sequences of commutative monoids, not necessarily abelian groups. Let A, B and C be commutative monoids. We say that the diagram

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1 \tag{4.2}$$

is a short exact sequence if the following conditions are satisfied: the monoid A is in fact an abelian group, the morphism f is injective, the morphism g is surjective and finally the image of f is equal to the kernel of g. In other words, the morphism g induces an isomorphism of the monoid C with the quotient monoid B/A. Here we remark that this quotient is well defined and has a monoid structure since we have assumed that A is an abelian group. Similarly, if all the monoids A, B, C are equipped with an action of a group G and the morphisms f and g are G-equivariant, then the short exact sequence considered above is said to be a short exact sequence of G-monoids.

Suppose now that the group A is a characteristic subgroup of B. Then, by restriction we obtain a natural group homomorphism $\mathrm{Aut}(B) \to \mathrm{Aut}(A)$. Similarly, taking quotient we get another group homomorphism $\mathrm{Aut}(B) \to \mathrm{Aut}(C)$, denoted $\varphi \mapsto \varphi_C$ for any $\varphi \in \mathrm{Aut}(B)$. Moreover, when (4.2) is a short exact sequence of G-monoids we obviously obtain G-equivariant versions of the restriction homomorphism $\mathrm{Aut}_G(B) \to \mathrm{Aut}_G(A)$ and the quotient homomorphism $\mathrm{Aut}_G(B) \to \mathrm{Aut}_G(C)$.

Recall the following well-known fact.

Lemma 4.3.1. *The kernel of the homomorphism* $\mathrm{Aut}(B) \to \mathrm{Aut}(A) \times \mathrm{Aut}(C)$ *is naturally isomorphic to the group* $\mathrm{Hom}(C, A)$. *Moreover, when the short exact sequence* (4.2) *is in fact a short exact sequence of* G*-monoids, then the kernel of the morphism* $\mathrm{Aut}_G(B) \to \mathrm{Aut}_G(A) \times \mathrm{Aut}_G(C)$ *is naturally isomorphic to the group* $\mathrm{Hom}_G(C, A)$.

Proof. Let φ be an element from the kernel D of the map $\mathrm{Aut}(B) \to \mathrm{Aut}(A) \times \mathrm{Aut}(C)$. Denote by $\overline{b}$ the image of the element $b \in B$ under the map g. Then, for each b from B we obtain $\overline{\varphi(b)} = \varphi_C(\overline{b}) = \overline{b}$, hence $\varphi(b) = ab$ for some $a \in A$. Thus, we may define a unique homomorphism $\varphi_0 \colon B \to A$ such that $\varphi(b) = \varphi_0(b)b$. Since φ is the identity on A we have $\varphi_0(a) = 1$ for every a from A. Therefore, the map φ_0 factorizes through a homomorphism $\varphi_0 \colon C \to A$,

denoted in the same way. Hence we obtain a map $D \to \mathrm{Hom}(C, A)$, which is obviously injective and we need to prove that it is also surjective.

Let now $\varphi_0 \colon C \to A$ be a homomorphism and define the endomorphism φ of B by the formula $\varphi(b) = \varphi_0(\overline{b})b$ for all b in B. We need to check that the endomorphism φ is in fact an isomorphism. It is injective, since if $\varphi(x) = \varphi_0(\overline{x})x = 1$ for some $x \in B$, then $x = \varphi_0(\overline{x})^{-1}$ belongs to A. Hence $\varphi_0(\overline{x}) = 1$, which implies $x = 1$. For the surjectivity we easily check that for every $b \in B$, if we put $x = b\varphi_0(\overline{b})^{-1}$, then we obtain $\varphi(x) = b$.

The G-module case follows immediately from the same argument as every morphism appearing above would be G-equivariant. □

We now fix a Galois field extension L/K with the Galois group $G = \mathrm{Gal}(L/K)$. We have a short exact sequence of G-monoids

$$1 \to \mathcal{O}_L^{\times} \to \mathcal{O}_L^{\triangleright} \to V_L \to 1.$$

Lemma 4.3.2. *Let φ be a G-equivariant automorphism of $\mathcal{O}_L^{\triangleright}$. Then, φ induces the identity on the value monoid V_L.*

Proof. Since φ is G-equivariant, it also induces the G-equivariant automorphism of a monoid $\mathcal{O}_M^{\triangleright}$, for every finite Galois field subextension M/K. Hence, it also induces the automorphism of the value monoid $V_M \cong \mathbb{N}$, which must be the identity homomorphism. The result follows from the fact that $V_L = \varinjlim_M V_M$. □

The above lemma implies that every G-equivariant automorphism φ of the monoid $\mathcal{O}_L^{\triangleright}$ is of the form $\varphi(x) = \varphi_0(x)x$, for some $\varphi_0 \in \mathrm{Hom}_G(\mathcal{O}_L^{\triangleright}, \mathcal{O}_L^{\times})$ and for every $x \in \mathcal{O}_L^{\triangleright}$.

Lemma 4.3.3. *Consider the natural restriction map $\mathrm{Aut}_G(\mathcal{O}_L^{\triangleright}) \to \mathrm{Aut}_G(\mathcal{O}_L^{\times})$. Then, the kernel of this homomorphism is naturally isomorphic to the group $\mathrm{Hom}_G(V_L, \mathcal{O}_L^{\times}) = \mathrm{Hom}(V_L, \mathcal{O}_K^{\times})$.*

Proof. We apply Lemma 4.3.1 to the short exact sequence

$$1 \to \mathcal{O}_L^{\times} \to \mathcal{O}_L^{\triangleright} \to V_L \to 1.$$

together with the previous observation that every G-equivariant automorphism of $\mathcal{O}_L^{\triangleright}$ induces the identity homomorphism on the quotient V_L. Moreover, the last equality follows since the action of G on V_L is trivial and $(\mathcal{O}_L^{\times})^G = \mathcal{O}_K^{\times}$. □

Lemma 4.3.4. *The group $\mathrm{Hom}(V_L, \mathcal{O}_K^{\times})$ is trivial if and only if the monoid V_L is $p(q-1)$-divisible.*

Proof. Assume first that the group V_L is p-divisible. Since the only p-divisible elements of the group $\mathcal{O}_K^\times$ are p'-roots of unity we easily see that every homomorphism $\mathrm{Hom}(V_L, \mathcal{O}_K^\times)$ has its image contained in $\mu_K^{p'}$. Moreover, when the group V_L is $(q-1)$ divisible then this image must be in fact trivial since $q-1$ is the order of the group $\mu_K^{p'}$. This proves the sufficiency of our condition.

Suppose now that the group V_L is not p-divisible, we want to construct a nonzero homomorphism in the group $\mathrm{Hom}(V_L, \mathcal{O}_K^\times)$. Recall that V_L may be identified with a submonoid of the additive monoid $\mathbb{Q}_{\geq 0}$. Since we assume that V_L is not p-divisible, the powers of p appearing in the denominator must be bounded. It follows that V_L is contained in some submonoid S_n consisting of all nonnegative rational numbers of the form $a/p^n b$ for some natural numbers a, b and n such that b is not divisible by p. Then, we easily produce a map $S_n \to U_K$ by declaring $1/p^n \mapsto u$, using any element u of U_K. It is well defined since raising to the power b for b prime to p defines an automorphism of the group U_L. Thus, in this case the group $\mathrm{Hom}(V_L, \mathcal{O}_K^\times)$ is nontrivial.

Suppose now that the group V_L is not $(q-1)$-divisible. In particular, there exist a prime l dividing $q-1$ such that V_L is not l-divisible. Arguing as previously we see that the monoid V_L is contained in some set L_n which consists of all nonzero rational numbers of the form $a/l^n b$ where a, b and n are rational numbers such that b is not divisible by l. Moreover, we may choose the smallest n satisfying $V_K \subset L_n$. Consider now the group $\mu_l \subset \mu_K$ of all lth roots of unity. We may define a homomorphism $L_n \to \mu_l$ by declaring $1/l^n \mapsto \zeta$ for some primitive lth root of unity ζ. It is well defined since raising to the power b for b prime to l is an automorphism of the group μ_l. Moreover, by the minimality of L_n the homomorphism $V_L \to \mu_l$ obtained by composition is nonzero. This proves nontrivialty of the group $\mathrm{Hom}(V_L, \mathcal{O}_K^\times)$ and finishes the proof. □

Recall that a supernatural number is a formal product $\prod p_i^{\alpha_i}$ over all prime numbers p_i where α_i is either a nonnegative integer or $+\infty$. The set of supernatural number has an obvious monoid structure as well as a relation of divisibility. If n_i is a sequence of supernatural numbers such that $n_i | n_j$ for $i \leq j$, then we write $\lim_{i\to\infty} n_i$ for the least common multiple of the numbers n_i.

We use this notion in the following situation. Let L/K be an algebraic extension and write $L = \varinjlim_{i\in\mathbb{N}} M_i$ as a colimit of a directed set of finite extensions M_i/K. Define the ramification index $e(L/K)$ of the extension L/K as the supernatural number $\lim_{i\to\infty} e(M_i/K)$, where $e(M_i/K)$ is the usual ramification index of the finite field extension M_i/K. It is easy to see that this definition does not depend on the choice of the collection of fields M_i. Using

this terminology, we have a restatement of the previous corollary.

Corollary 4.3.5. *Let L/K be a Galois field extension with Galois group G such that $p^\infty(q-1)^\infty$ does not divide the ramification number $e(L/K)$. Then, the group $\mathrm{Aut}_G(\mathcal{O}_L^\triangleright)$ is nontrivial.*

Definition 4.3.6. Let L/K be a Galois extension with the Galois group G and let $M \in \{\mathcal{O}_L^\triangleright, \mathcal{O}_L^\times\}$. Hence, for each $\varphi \in \mathrm{Aut}_G(M)$ we may write $\varphi(x) = \varphi_0(x)x$ for some $\varphi_0 \in \mathrm{Hom}_G(M, \mathcal{O}_L^\times)$.

1. Define the subgroup $\mathrm{Aut}_G^{p'}(M)$ of the group $\mathrm{Aut}_G(M)$ as the set of all automorphisms $\varphi \in \mathrm{Aut}_G(M)$ such that $\varphi_0(x)$ is a p'-root of unity for every $x \in M$.

2. Define the subgroup $\mathrm{Aut}_G^0(M)$ of the group $\mathrm{Aut}_G(M)$ as the set of all automorphisms φ of M such that $\varphi_0(x) \in U_L$ for every $x \in M$.

We have a natural isomorphism of groups

$$\mathcal{O}_L^\times \cong \mu_L^{p'} \times U_L. \tag{4.3}$$

This decomposition is in fact a characteristic decomposition of the monoid $\mathcal{O}_L^\times$. Indeed, it follows from the fact that the group U_L can be characterised as the subgroup of all l-divisible elements for any prime $l \neq p$.

Lemma 4.3.7. *We have a natural group isomorphism*

$$\mathrm{Aut}_G(\mathcal{O}_L^\times) \cong \mathrm{Aut}_G^{p'}(\mathcal{O}_L^\times) \times \mathrm{Aut}_G^0(\mathcal{O}_L^\times)$$

which to every automorphism $\varphi \in \mathrm{Aut}(\mathcal{O}_L^\times)$ associates pair of automorphisms (φ', φ'') defined as $\varphi'(x) = \varphi_0'(x)x$ and $\varphi''(x) = \varphi_0''(x)x$, where

$$\varphi_0(x) = \varphi_0'(x)\varphi_0''(x)$$

is the decomposition induced by the isomorphism (4.3).

Proof. Observe first that the restriction maps

$$\mathrm{Aut}^{p'}(\mathcal{O}_L^\times) \to \mathrm{Aut}(\mu_L^{p'}) \quad \text{and} \quad \mathrm{Aut}^0(\mathcal{O}_L^\times) \to \mathrm{Aut}(U_L)$$

are isomorphisms. Indeed, for every automorphisms $\varphi \in \mathrm{Aut}^{p'}(\mathcal{O}_L^\times)$ its restriction to U_L is the identity. Therefore, we easily see that the first homomorphism in the statement must be an isomorphism. Similarly, the restriction of every automorphism $\varphi \in \mathrm{Aut}^0(\mathcal{O}_L^\times)$ to the group $\mu_L^{p'}$ is the identity, hence the second map is an isomorphism as well. This, together with the isomorphism (4.3), finishes the proof. □

4.4 Cohomology classes of automorphisms

In this section we are going to construct certain cohomology classes measuring the obstruction to the existence of a lift of a G-equivariant automorphism of $\mathcal{O}_L^\times$ to a G-equivariant automorphism of $\mathcal{O}_L^\triangleright$. This method will enable us to characterise the cokernel of the restriction map $\mathrm{Aut}_G(\mathcal{O}_L^\triangleright) \to \mathrm{Aut}_G(\mathcal{O}_L^\times)$.

Observe first that when we do not require G-equivariance, then for every finite extension L/K the map $\mathrm{Aut}(\mathcal{O}_L^\triangleright) \to \mathrm{Aut}(\mathcal{O}_L^\times)$ is surjective. Indeed, pick any uniformizing element π of $\mathcal{O}_L^\triangleright$. Then, if φ is any automorphism of the group $\mathcal{O}_L^\times$, we may simply define $\tilde{\varphi}(u\pi^n) = \varphi(u)\pi^n$, for a unit u and natural number n. This defines an endomorphism of $\mathcal{O}_L^\triangleright$, which is in fact an automorphism.

Fix a finite Galois extension L/K and let φ be a G-equivariant automorphism of $\mathcal{O}_L^\times$. Take any lift $\tilde{\varphi}$ of φ to an (not necessary G-equivariant) automorphism of $\mathcal{O}_L^\triangleright$ and choose a uniformizer π_L of $\mathcal{O}_L^\triangleright$. Then, we may define for every $\sigma \in G$ the element a_σ by the following formula

$$a_\sigma = \frac{\tilde{\varphi}(\sigma(\pi_L))}{\sigma(\tilde{\varphi}(\pi_L))}.$$

It is easy to see that a_σ is a unit in the p-adic field L. We then have the following basic lemma.

Lemma 4.4.1. *The function $\sigma \mapsto a_\sigma$ is a cocycle, in other words we have $a_{\sigma\tau} = a_\sigma \sigma(a_\tau)$. Moreover, the construction of a_σ does not depend on the choice of an uniformizer π_L. Furthermore, choosing a different lift $\tilde{\varphi} \in \mathrm{Aut}(\mathcal{O}_L^\triangleright)$ changes the cocycle a_σ by a coboundary (i.e. a map $\sigma \mapsto \sigma(b)/b$, for some unit b). Together it implies that we obtain a well defined map of sets*

$$\mathrm{Aut}_G(\mathcal{O}_L^\times) \to H^1(G, \mathcal{O}_L^\times).$$

Proof. We start by proving that a_σ is independent of the choice of a uniformizer of $\mathcal{O}_L^\triangleright$. Obviously the map

$$\mathcal{O}_L^\triangleright \ni x \mapsto \frac{\tilde{\varphi}(\sigma(x))}{\sigma(\tilde{\varphi}(x))} \in \mathcal{O}_L^\times$$

is multiplicative, moreover it vanishes on units $\mathcal{O}_L^\times$ as φ is assumed to be G-equivariant. Thus, if $\pi_L' = u\pi_L$ is another uniformizer then we have

$$a_\sigma' = \frac{\tilde{\varphi}(\sigma(\pi_L'))}{\sigma(\tilde{\varphi}(\pi_L'))} = \frac{\tilde{\varphi}(\sigma(u))}{\sigma(\tilde{\varphi}(u))}\frac{\tilde{\varphi}(\sigma(\pi_L))}{\sigma(\tilde{\varphi}(\pi_L))} = \frac{\tilde{\varphi}(\sigma(\pi_L))}{\sigma(\tilde{\varphi}(\pi_L))} = a_\sigma.$$

Now we will prove the cocycle relation. We have

$$a_{\sigma\tau} = \frac{\tilde{\varphi}(\sigma\tau(\pi_L))}{\sigma\tau(\tilde{\varphi}(\pi_L))} = \frac{\tilde{\varphi}(\sigma\tau(\pi_L))}{\sigma(\frac{\varphi(\tau(\pi_L))}{a_\tau})} = \frac{\tilde{\varphi}(\sigma(\tau(\pi_L)))}{\sigma(\tilde{\varphi}(\tau(\pi_L)))}\sigma(a_\tau) = a_\sigma\sigma(a_\tau),$$

where the last equality follows from the fact that $\tau(\pi_L)$ is also a uniformizer.

Finally, let φ_2 be some other extension of φ to an automorphism of $\mathcal{O}_L^{\triangleright}$. Then we have $\varphi_2(\pi_L) = \tilde{\varphi}(\pi_L)u$, for some unit u. Moreover, for every $\sigma \in G$ we have

$$\varphi_2(\sigma(\pi_L)) = \varphi_2\left(\frac{\sigma(\pi_L)}{\pi_L}\pi_L\right) = \varphi\left(\frac{\sigma(\pi_L)}{\pi_L}\right)\tilde{\varphi}(\pi_L)u = \tilde{\varphi}(\sigma(\pi_L))u.$$

We now compute the cocycle using the lift φ_2

$$\frac{\varphi_2(\sigma(\pi_L))}{\sigma(\varphi_2(\pi_L))} = \frac{\tilde{\varphi}(\sigma(\pi_L)u)}{\sigma(\tilde{\varphi}(\pi_L)u)} = \frac{\tilde{\varphi}(\sigma(\pi_L))}{\sigma(\tilde{\varphi}(\pi_L))}\frac{u}{\sigma(u)} = a_\sigma\frac{u}{\sigma(u)}.$$

hence two computations of a_σ differ by a cocycle $\sigma(u)/u$, which finishes the proof. □

The map just constructed will be denoted by κ_L, we also use the notation $\kappa_L(\varphi)_\sigma$ to denote a cocycle in the cohomology class $\kappa_L(\varphi)$.

$$\begin{aligned}\kappa_L\colon \operatorname{Aut}_G(\mathcal{O}_L^\times) &\to H^1(G, \mathcal{O}_L^\times)\\ \varphi &\mapsto [\sigma \mapsto \kappa_L(\varphi)_\sigma]\end{aligned}$$

Observe that the group $\operatorname{Aut}_G(\mathcal{O}_L^\times)$ acts naturally on the group $H^1(G, \mathcal{O}_L^\times)$. Indeed, if φ is any G-equivariant automorphism of $\mathcal{O}_L^\times$ and $\sigma \mapsto a_\sigma$ is a cocycle, then we may compose a_σ with φ to get a map $\sigma \mapsto \varphi(a_\sigma) = b_\sigma$. Then it follows from the G-equivariance of φ that b_σ is a cocycle

$$b_{\sigma\tau} = \varphi(a_{\sigma\tau}) = \varphi(a_\sigma\sigma(a_\tau)) = \varphi(a_\sigma)\sigma(\varphi(a_\tau)) = b_\sigma\sigma(b_\tau).$$

Similarly, again by G-equivariance, composing with φ preserves the set of coboundaries, hence the action of φ descends to the action on the group $H^1(G, \mathcal{O}_L^\times)$.

Lemma 4.4.2. *The map κ_L is a crossed homomorphism. In other words, we have $\kappa_L(\varphi\psi) = \kappa_L(\varphi)\varphi(\kappa_L(\psi))$ for every two automorphisms φ and ψ.*

Obviously, a crossed homomorphism is the same as a cocycle, however we choose this terminology to avoid any confusion with cocylces representing cohomology classes in the group $H^1(G, \mathcal{O}_L^\times)$.

Proof. We want to compute the cocycle associated to the morphism $\varphi\psi$. Choose extensions $\tilde{\varphi}$ and $\tilde{\psi}$, moreover as an extension of $\varphi\psi$ we may simply take $\tilde{\varphi}\tilde{\psi}$. To ease the notation, denote the cocycles corresponding to $\tilde{\varphi}$ and $\tilde{\psi}$ by a_σ and b_σ, respectively. Then we have

$$\frac{\tilde{\varphi}\tilde{\psi}(\sigma(\pi_L))}{\sigma(\tilde{\varphi}\tilde{\psi}(\pi_L))} = a_\sigma\frac{\tilde{\varphi}(b_\sigma\sigma(\tilde{\psi}(\pi_L)))}{\tilde{\varphi}(\sigma(\tilde{\psi}(\pi_L)))} = a_\sigma\varphi(b_\sigma),$$

hence the lemma follows. □

Every crossed homomorphism $G \to A$ from a group G to a G-module group has a well defined kernel which is a subgroup of G (however, it may not be a normal subgroup of G).

We are now able to describe the relation between the map κ_L and the group of G-equivariant automorphisms of $\mathcal{O}_L^{\triangleright}$.

Proposition 4.4.3. *Let L/K be a finite Galois extension with the Galois group G. Then, the following sequence is exact*

$$1 \longrightarrow \mathrm{Hom}(V_L, \mathcal{O}_K^{\times}) \longrightarrow \mathrm{Aut}_G(\mathcal{O}_L^{\triangleright}) \longrightarrow \mathrm{Aut}_G(\mathcal{O}_L^{\times}) \xrightarrow{\kappa_L} H^1(G, \mathcal{O}_L^{\times}) \tag{4.4}$$

More precisely, the kernel of the crossed homomorphism κ_L is equal to the image of the group $\mathrm{Aut}_G(\mathcal{O}_L^{\triangleright})$ in the group $\mathrm{Aut}_G(\mathcal{O}_L^{\times})$.

Proof. Put $\kappa = \kappa_L$. By Lemma 4.3.3 we only need to check exactness at $\mathrm{Aut}_G(\mathcal{O}_L^{\times})$. Let φ be a G-equivariant automorphism of $\mathcal{O}_L^{\times}$. Suppose first that φ lies in the image of $\mathrm{Aut}_G(\mathcal{O}_L^{\triangleright})$. Hence we may assume that the lift $\tilde{\varphi}$ chosen in the construction of the class $\kappa(\varphi)$ is G-equivariant. Thus, directly from the definition of the map κ, we obtain $\kappa(\varphi) = 1$.

Suppose now that $\kappa(\varphi) = 1$. Choose any extension $\tilde{\varphi}$ of φ to the automorphism of $\mathcal{O}_L^{\triangleright}$. Triviality of $\kappa(\varphi)$ means that the cocycle constructed from $\tilde{\varphi}$ is a coboundary, in other words there exist a unit v and a uniformizer π_L such that for every $\sigma \in G$ we have

$$\frac{\tilde{\varphi}(\sigma(\pi_L))}{\sigma(\tilde{\varphi}(\pi_L))} = \frac{\sigma(v)}{v}.$$

We may now define an automorphism $\hat{\varphi}$ of $\mathcal{O}_L^{\triangleright}$ by putting

$$\hat{\varphi}(u\pi^i) = v\varphi(u)\tilde{\varphi}(\pi_L)$$

for every unit u. Then we have

$$\hat{\varphi}(\sigma(\pi_L)) = \hat{\varphi}(\frac{\sigma(\pi_L)}{\pi_L}\pi_L) = \hat{\varphi}(\frac{\sigma(\pi_L)}{\pi_L})\hat{\varphi}(\pi_L) = \tilde{\varphi}(\frac{\sigma(\pi_L)}{\pi_L})v\tilde{\varphi}(\pi_L) = v\tilde{\varphi}(\sigma(\pi_L))$$

and similarly

$$\sigma(\hat{\varphi}(\pi_L)) = \sigma(v\tilde{\varphi}(\pi_L)) = \sigma(v)\sigma(\tilde{\varphi}(\pi_L)),$$

hence comparing both sides we get $\hat{\varphi}(\sigma(\pi_L)) = \sigma(\hat{\varphi}(\pi_L))$. Since π_L and units generate the monoid $\mathcal{O}_L^{\triangleright}$, it shows that $\hat{\varphi}$ is in fact a G-equivariant automorphism extending φ, which finishes the proof. □

The natural isomorphism $\mathcal{O}_L^{\times} \cong \mu_L^{p'} \times U_L$ induces a splitting

$$H^1(G, \mathcal{O}_L^{\times}) \cong H^1(G, \mu_L^{p'}) \times H^1(G, U_L),$$

moreover, from Lemma 4.3.7, we have a similar product decomposition for the group of automorphisms.

$$\mathrm{Aut}_G(\mathcal{O}_L^\times) \cong \mathrm{Aut}_G^{p'}(\mathcal{O}_L^\times) \times \mathrm{Aut}_G^0(\mathcal{O}_L^\times)$$

The next lemma shows that the map κ_L respects these product decompositions.

Lemma 4.4.4. *There exist dotted arrows (also denoted by κ_L), which are crossed homomorphisms, fitting in the following commutative diagram with exact rows.*

$$\begin{array}{ccccccc}
1 & \longrightarrow & \mathrm{Hom}(V_L, \mu_K^{p'}) & \longrightarrow & \mathrm{Aut}_G^{p'}(\mathcal{O}_L^\triangleright) & \longrightarrow & \mathrm{Aut}_G^{p'}(\mathcal{O}_L^\times) \overset{\kappa_L}{\dashrightarrow} H^1(G, \mu_L^{p'}) \\
 & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \mathrm{Hom}(V_L, \mathcal{O}_K^\times) & \longrightarrow & \mathrm{Aut}_G(\mathcal{O}_L^\triangleright) & \longrightarrow & \mathrm{Aut}_G(\mathcal{O}_L^\times) \overset{\kappa_L}{\longrightarrow} H^1(G, \mathcal{O}_L^\times) \\
 & & \uparrow & & \uparrow & & \uparrow \\
1 & \longrightarrow & \mathrm{Hom}(V_L, U_K) & \longrightarrow & \mathrm{Aut}_G^0(\mathcal{O}_L^\triangleright) & \longrightarrow & \mathrm{Aut}_G^0(\mathcal{O}_L^\times) \overset{\kappa_L}{\dashrightarrow} H^1(G, U_L)
\end{array}$$

Proof. We will only consider the upper row, the proof for the bottom one is analogous. Let φ be a G-equivariant p'-automorphism of $\mathcal{O}_L^\times$. Choose a uniformizer π_L of L. Observe that the extension $\tilde{\varphi}$ defined by $\tilde{\varphi}(u\pi_L^n) = \varphi(u)\pi_L^n$ is also a p'-automorphism. Write $\varphi(x) = \varphi_0(x)x$ and $\sigma(x) = \sigma_0(x)x$, for every $x \in \mathcal{O}_L^\triangleright$. We compute the cocycle a_σ using the lift $\tilde{\varphi}$

$$a_\sigma = \frac{\tilde{\varphi}(\sigma(\pi_L))}{\sigma(\tilde{\varphi}(\pi_L))} = \frac{\tilde{\varphi}_0(\sigma_0(\pi_L))}{\sigma_0(\tilde{\varphi}_0(\pi_L))}.$$

Therefore we see that a_σ belongs to the set $\mu_L^{p'}$ of p'-roots of unity. Choosing a different p'-automorphism extending φ changes the cocycle a_σ by a coboundary, hence it gives a well defined cohomology class in $H^1(G, \mu_L^{p'})$. This defines the dotted arrow, also denoted by κ_L. Moreover, by the same computation as previously, we see that it is a crossed homomorphism. □

Lemma 4.4.5. *For every finite Galois extension L/K with $G = \mathrm{Gal}(L/K)$ there exist natural isomorphisms*

$$H^1(G, \mathcal{O}_L^\times) \cong V_L/V_K \cong \mathbb{Z}/e\mathbb{Z}$$

where $e = e(L/K)$ is the ramification index. Moreover, if $L'/L/K$ is a tower of Galois extensions with Galois group $G' = \mathrm{Gal}(L'/K)$, then the following diagram

$$\begin{array}{ccc}
H^1(G', \mathcal{O}_{L'}^\times) & \xrightarrow{\simeq} & \mathbb{Z}/e(L'/L)\mathbb{Z} \\
\downarrow{\scriptstyle e(L'/L)} & & \downarrow \\
H^1(G, \mathcal{O}_L^\times) & \xrightarrow{\simeq} & \mathbb{Z}/e(L/K)\mathbb{Z}
\end{array}$$

is commutative. Here, the left vertical arrow is a multiplication by $e(L'/L)$ and the right vertical arrow is the natural projection.

Proof. Consider the following exact sequence of G-modules

$$1 \to \mathcal{O}_L^\times \to L^\times \to V_L \to 1.$$

Taking the long exact sequence in cohomology associated to this short exact sequence we obtain

$$1 \to \mathcal{O}_K^\times \to K^\times \to V_L \to H^1(G, \mathcal{O}_L^\times) \to H^1(G, L^\times).$$

The group $H^1(G, L^\times)$ vanishes by Hilbert's Theorem 90 and the image of $K^\times$ in V_L is identified with V_K. That finishes the proof of the first part of the lemma.

For the second part, since the isomorphism $H^1(G, \mathcal{O}_L^\times) \cong V_L/V_K$ obtained above is functorial, applying the restriction map we have a commutative diagram

$$\begin{array}{ccc} V_{L'}/V_K & \xrightarrow{\simeq} & H^1(G', \mathcal{O}_{L'}^\times) \\ \uparrow & & \uparrow \\ V_L/V_K & \xrightarrow{\simeq} & H^1(G, \mathcal{O}_L^\times), \end{array}$$

hence also a commutative diagram

$$\begin{array}{ccc} H^1(G', \mathcal{O}_{L'}^\times) & \xrightarrow{\simeq} & V_{L'}/V_K \\ \downarrow{\scriptstyle e(L'/L)} & & \downarrow{\scriptstyle e(L'/L)} \\ H^1(G, \mathcal{O}_L^\times) & \xrightarrow{\simeq} & V_L/V_K. \end{array}$$

Then it is enough to observe the commutativity of the diagram

$$\begin{array}{ccc} V_{L'}/V_K & \xrightarrow{\simeq} & \mathbb{Z}/e(L'/K)\mathbb{Z} \\ \downarrow{\scriptstyle e(L'/L)} & & \downarrow \\ V_L/V_K & \xrightarrow{\simeq} & \mathbb{Z}/e(L/K)\mathbb{Z}, \end{array}$$

which is obvious. □

Remark 4.4.6. We may write down explicitly the formula of the above isomorphism. Let n be an element of the group V_L/V_K and take any lift of n to an element a of $L^\times$. Then, the cohomology class corresponding to the element n is given by the cocyle $\sigma \mapsto \sigma(a)/a$. In particular, the canonical generator $1 \in \mathbb{Z}/e\mathbb{Z}$ corresponds to the cocycle $\sigma \mapsto \sigma(\pi)/\pi$, where π is a uniformizer of L.

Remark 4.4.7. Observe that one can define the map κ_L even without choosing a lift $\tilde{\varphi}$. Indeed, let $\varphi \in \mathrm{Aut}_G(\mathcal{O}_L^\times)$ be a G-equivariant automorphism of $\mathcal{O}_L^\times$. We write $\varphi_0(x) = \varphi(x)x^{-1}$ for all $x \in \mathcal{O}_L^\times$, similarly let $\sigma_0(x) = \sigma(x)x^{-1}$ for every $\sigma \in G$. Then, one easily checks that the cohomology class $\kappa_L(\varphi)$ is represented by the cocycle $\sigma \mapsto \varphi_0(\sigma_0(\pi_L))$, where π_L is a uniformizer of L.

In the next lemma we observe that we may replace the crossed homomorphism κ_L by another map which is a group homomorphism.

Lemma 4.4.8. *The map* $\kappa_L \colon \mathrm{Aut}_G(\mathcal{O}_L^\times) \to H^1(G, \mathcal{O}_L^\times)$ *factorizes as the following composition*

$$\mathrm{Aut}_G(\mathcal{O}_L^\times) \to \mathrm{Aut}(H^1(G, \mathcal{O}_L^\times)) \to H^1(G, \mathcal{O}_L^\times)$$

where the first map is a natural group homomorphism induced by the functoriality of group cohomology. The second map is a map of sets given by

$$(\mathbb{Z}/e\mathbb{Z})^\times \ni n \mapsto n - 1 \in \mathbb{Z}/e\mathbb{Z},$$

here we use the natural isomorphism $H^1(G, \mathcal{O}_L^\times) \cong \mathbb{Z}/e\mathbb{Z}$ *from Lemma 4.4.5.*

Proof. Let φ be an G-equivariant automorphism of $\mathcal{O}_L^\times$ and π a uniformizer of L. Then, we have seen in Remark 4.4.7 that the class κ_L is represented by the cocycle $\kappa_L(\varphi)_\sigma = \varphi(\sigma_0(\pi))/\sigma_0(\pi)$. On the other hand, $\sigma_0(\pi)$ is a canonical generator of $H^1(G, \mathcal{O}_L^\times)$ identified with $1 \in \mathbb{Z}/e\mathbb{Z}$. Therefore, if φ induces an automorphism of $H^1(G, \mathcal{O}_L^\times)$ identified with $b \in (\mathbb{Z}/e\mathbb{Z})^\times$, then $\kappa_L(\varphi)$ corresponds to $b - 1$. □

Therefore we may modify Corollary 4.4 to obtain the next result.

Corollary 4.4.9. *Using the natural identification* $\mathrm{Aut}(H^1(G, \mathcal{O}_L^\times)) \cong (\mathbb{Z}/e\mathbb{Z})^\times$ *we have a short exact sequence of group homomorphisms*

$$1 \longrightarrow \mathrm{Hom}(V_L, \mathcal{O}_K^\times) \longrightarrow \mathrm{Aut}_G(\mathcal{O}_L^\triangleright) \longrightarrow \mathrm{Aut}_G(\mathcal{O}_L^\times) \longrightarrow (\mathbb{Z}/e\mathbb{Z})^\times.$$

Next we describe functorial behaviour of the map κ_L with respect to field extensions.

Lemma 4.4.10. *Let* $L'/L/K$ *be a tower of Galois extensions with Galois groups* $G' = \mathrm{Gal}(L'/K)$ *and* $G = \mathrm{Gal}(L/K)$*. Then we have the following commutative diagram*

$$\begin{array}{ccccc}
\mathrm{Aut}_{G'}(\mathcal{O}_{L'}^\times) & \xrightarrow{\kappa_{L'}} & H^1(G', \mathcal{O}_{L'}^\times) & & \\
\downarrow & & & \searrow^{e(L'/L)} & \\
\mathrm{Aut}_G(\mathcal{O}_L^\times) & \xrightarrow{\kappa_L} & H^1(G, \mathcal{O}_L^\times) & \hookrightarrow & H^1(G', \mathcal{O}_{L'}^\times),
\end{array}$$

where the inclusion $H^1(G, \mathcal{O}_L^\times) \hookrightarrow H^1(G', \mathcal{O}_{L'}^\times)$ *is the inflation map and* $e(L'/L)$ *denotes the multiplication by the ramification index* $e(L'/L)$ *of the field extension* L'/L.

Proof. Choose a uniformizer $\pi_{L'}$ of L' and denote $e = e(L'/L)$. Then, we have $\pi_{L'}^e = u\pi_L$ for some uniformizer π_L of L and some unit $u \in \mathcal{O}_{L'}^\times$. Let φ be a G-equivariant automorphism of $\mathcal{O}_{L'}^\times$. Then, by Remark 4.4.7, we may compute the eth power of the cocycle $\kappa_{L'}(\varphi)_\sigma$ as follows

$$\kappa_{L'}(\varphi)_\sigma^e = \varphi_0(\sigma_0(\pi_{L'}))^e = \varphi_0(\sigma_0(u\pi_L)) = \sigma_0(\varphi_0(u))\varphi_0(\sigma_0(\pi_L)),$$

where the last equality uses G-equivariance of φ. Therefore, the right hand side of the above equality is a cocycle cohomologous to $\kappa_L(\varphi)_\sigma$, which finishes the proof. □

Corollary 4.4.11. *For every tower of Galois field extensions* $L'/L/K$ *as in Lemma 4.4.10 we have a commutative diagram of group homomorphisms*

$$\begin{array}{ccc} \mathrm{Aut}_{G'}(\mathcal{O}_{L'}^\times) & \longrightarrow & (\mathbb{Z}/e(L'/K)\mathbb{Z})^\times \\ \downarrow & & \downarrow \\ \mathrm{Aut}_G(\mathcal{O}_L^\times) & \longrightarrow & (\mathbb{Z}/e(L/K)\mathbb{Z})^\times, \end{array}$$

where the right vertical arrow is the natural projection.

Proof. This compatibility follows immediately from Lemma 4.4.10, together with statements of Lemma 4.4.8 and Lemma 4.4.5. □

We are going to describe the relation between the product decomposition $\mathcal{O}_L^\times \cong \mu_L^{p'} \times U_L$ and the group homomorphism $\mathrm{Aut}_G(\mathcal{O}_L^\times) \to (\mathbb{Z}/e(L/K)\mathbb{Z})^\times$. First we recall a well-known computation of certain Galois cohomology modules.

Lemma 4.4.12. *Write* $e = e(L/K)$ *as the product* $p^\alpha e'$, *where* $(e', p) = 1$. *Then, we have natural isomorphisms,*

$$H^1(G, \mu_L^{p'}) \cong \mathbb{Z}/e'\mathbb{Z}, \quad H^1(G, U_L) \cong \mathbb{Z}/p^\alpha\mathbb{Z},$$

which are compatible with the product decomposition $\mathcal{O}_L^\times \cong \mu_L^{p'} \times U_L$.

Proof. Let $G^{\mathrm{wild}} \subset G$ be the wild inertia subgroup and let $G \twoheadrightarrow G^{\mathrm{tm}} \twoheadrightarrow G^{\mathrm{ur}}$ be the maximal tamely ramified and unramified quotient, respectively. Hence we have short exact sequences

$$1 \to G^{\mathrm{wild}} \to G \to G^{\mathrm{tm}} \to 1$$

and

$$1 \to G^{\mathrm{tr}} \to G^{\mathrm{tm}} \to G^{\mathrm{ur}} \to 1.$$

They correspond to the following tower of intermediate field extensions

$$K \subset F^{\mathrm{ur}} \subset F^{\mathrm{tm}} \subset L.$$

First we are going to prove that the cohomology groups $H^1(G^{\mathrm{tm}}, U_{F^{\mathrm{tm}}})$ and $H^2(G^{\mathrm{tm}}, U_{F^{\mathrm{tm}}})$ vanish. Consider the Hochschild-Serre spectral sequence

$$H^p(G^{\mathrm{ur}}, H^q(G^{\mathrm{tr}}, U_{F^{\mathrm{tm}}})) \Rightarrow H^{p+q}(G^{\mathrm{tm}}, U_{F^{\mathrm{tm}}}),$$

associated to the group extension

$$1 \to G^{\mathrm{tr}} \to G^{\mathrm{tm}} \to G^{\mathrm{ur}} \to 1.$$

Since the order of G^{tr} is prime to p we see that for every $q > 0$ cohomology groups $H^q(G^{\mathrm{tr}}, U_{F^{\mathrm{tm}}})$ are trivial. Hence, the spectral sequence degenerates and we get isomorphisms $H^n(G^{\mathrm{ur}}, U_{F^{\mathrm{ur}}}) \cong H^n(G^{\mathrm{tm}}, U_{F^{\mathrm{tm}}})$, for every $n \geq 0$. Consider now the short exact sequence of G^{ur}-modules

$$1 \to \mathcal{O}_{F^{\mathrm{ur}}}^{\times} \to (F^{\mathrm{ur}})^{\times} \to V_{F^{\mathrm{ur}}} \to 1$$

and the associated long exact sequence in cohomology

$$K^{\times} \to V_{F^{\mathrm{ur}}} \to H^1(G^{\mathrm{ur}}, \mathcal{O}_{F^{\mathrm{ur}}}^{\times}) \to H^1(G^{\mathrm{ur}}, (F^{\mathrm{ur}})^{\times}).$$

The first map is surjective since the extension F^{ur}/K is unramified and the last group vanishes by Hibert's Theorem 90. Therefore, the cohomology group $H^1(G^{\mathrm{ur}}, \mathcal{O}_{F^{\mathrm{ur}}}^{\times})$ is trivial which implies that $H^1(G^{\mathrm{ur}}, U_{F^{\mathrm{ur}}})$ is trivial as well. Hence, we obtain that the group $H^1(G^{\mathrm{tm}}, U_{F^{\mathrm{tm}}})$ is trivial.

To compute the second cohomology group we may use periodicity of Tate cohomology (see [34], Proposition 1.7.1), since the group G^{ur} is cyclic. Therefore, we obtain

$$H^2(G^{\mathrm{tm}}, U_{F^{\mathrm{tm}}}) \cong H^2(G^{\mathrm{ur}}, U_{F^{\mathrm{ur}}}) \cong \hat{H}^0(G^{\mathrm{ur}}, U_{F^{\mathrm{ur}}}) = U_K/\mathrm{Nm}(U_{F^{\mathrm{ur}}}) = 1,$$

since for unramified extensions the norm map $\mathrm{Nm}\colon U_{F^{\mathrm{ur}}} \to U_K$ is surjective.

Going back to the proof of the lemma, observe that we have a sequence of isomorphisms

$$H^1(G, \mu_L^{p'}) \cong H^1(G^{\mathrm{tr}}, \mu_L^{p'}) \cong H^1(G^{\mathrm{tr}}, \mathcal{O}_L^{\times}) \cong \mathbb{Z}/e'\mathbb{Z}.$$

Indeed, the first isomorphism comes from inflation map since G^{wild} is a p-group, the second follows from triviality of cohomology group $H^1(G^{\mathrm{tm}}, U_L)$ and the last one come from Lemma 4.4.5. This finishes the proof of the first isomorphism.

For the second isomorphism, we consider the spectral sequence

$$H^p(G^{\mathrm{tm}}, H^q(G^{\mathrm{wild}}, U_L)) \Rightarrow H^{p+q}(G, U_L),$$

associated to the short exact sequence

$$1 \to G^{\mathrm{wild}} \to G \to G^{\mathrm{tm}} \to 1$$

Then, we obtain the exact sequence

$$1 \to H^1(G^{\mathrm{tm}}, U_{F^{\mathrm{tm}}}) \to H^1(G, U_L) \to H^1(G^{\mathrm{wild}}, U_L)^{G^{\mathrm{tm}}} \to H^2(G^{\mathrm{tm}}, U_{F^{\mathrm{tm}}}),$$

hence the middle arrow is an isomorphism. Moreover,

$$H^1(G^{\mathrm{wild}}, U_L) \cong H^1(G^{\mathrm{wild}}, \mathcal{O}_L^\times) \cong \mathbb{Z}/p^\alpha\mathbb{Z}$$

and the action of G^{tm} on $H^1(G^{\mathrm{wild}}, U_L)$ is trivial, therefore finally we obtain $H^1(G, U_L) \cong \mathbb{Z}/p^\alpha\mathbb{Z}$. Compatibility with the product decomposition is obvious. □

Corollary 4.4.13. *The map* $\mathrm{Aut}_G(\mathcal{O}_L^\times) \to (\mathbb{Z}/e(L/K)\mathbb{Z})^\times$ *is compatible with the decomposition* $\mathcal{O}_L^\times \cong \mu_L^{p'} \times U_L$. *More precisely, we have the following commutative diagram of group homomorphisms with exact rows*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Hom}(V_L, \mu_K^{p'}) & \longrightarrow & \mathrm{Aut}_G^{p'}(\mathcal{O}_L^\triangleright) & \longrightarrow & \mathrm{Aut}_G^{p'}(\mathcal{O}_L^\times) & \longrightarrow & (\mathbb{Z}/e'\mathbb{Z})^\times \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \mathrm{Hom}(V_L, \mathcal{O}_K^\times) & \longrightarrow & \mathrm{Aut}_G(\mathcal{O}_L^\triangleright) & \longrightarrow & \mathrm{Aut}_G(\mathcal{O}_L^\times) & \longrightarrow & (\mathbb{Z}/e\mathbb{Z})^\times \\
 & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\
1 & \longrightarrow & \mathrm{Hom}(V_L, U_K) & \longrightarrow & \mathrm{Aut}_G^0(\mathcal{O}_L^\triangleright) & \longrightarrow & \mathrm{Aut}_G^0(\mathcal{O}_L^\times) & \longrightarrow & (\mathbb{Z}/p^\alpha\mathbb{Z})^\times.
\end{array}$$

Proof. This follows from Lemma 4.4.4 together with Lemma 4.4.12. □

We would like to extend Corollary 4.4.9 to the case of infinite Galois extensions. Let L/K be a fixed Galois extension (not necessarily finite) with the Galois group G. Write $L = \varinjlim_{i \in I} L_i$, where every L_i is a finite Galois subextension of L/K and denote for simplicity $e_i = e(L_i/K)$. Moreover, let G_i be the quotient of G given by the Galois group of the field extension L_i/K.

Definition 4.4.14. With the notation as above, we define

$$V(L/K) = \varprojlim_{i \in I} \mathbb{Z}/e_i\mathbb{Z},$$

where the maps in the inverse system are given by the natural projections. Similarly, we define

$$V(L/K)^\times = \varprojlim_{i \in I} (\mathbb{Z}/e_i\mathbb{Z})^\times.$$

For every L_i we have constructed a map $\mathrm{Aut}_{G_i}(\mathcal{O}_{L_i}^\times) \to (\mathbb{Z}/e_i\mathbb{Z})^\times$ and as i varies they form an inverse system with respect to natural restrictions and projections, by Corollary 4.4.11. Taking limit over $i \in I$ we obtain a group homomorphism

$$\mathrm{Aut}_G(\mathcal{O}_L^\times) = \varprojlim_{i\in I} \mathrm{Aut}_{G_i}(\mathcal{O}_{L_i}^\times) \to V(L/K)^\times.$$

Lemma 4.4.15. *The following sequence of group homomorphisms*

$$1 \to \mathrm{Hom}(V_L, \mathcal{O}_K^\times) \to \mathrm{Aut}_G(\mathcal{O}_L^\triangleright) \to \mathrm{Aut}_G(\mathcal{O}_L^\times) \to V(L/K)^\times \tag{4.5}$$

is exact.

Proof. We only need to check exactness at $\mathrm{Aut}_G(\mathcal{O}_L^\times)$. One inclusion is immediate, since if φ is a G-equivariant automorphism of $\mathcal{O}_L^\triangleright$, then from the finite degree case its image in $(\mathbb{Z}/e_i\mathbb{Z})^\times$ is trivial for every i, hence its image in $V(L/K)^\times$ is trivial as well.

Suppose now that we have a G-equivariant automorphism of $\mathcal{O}_L^\times$ which vanishes in $V(L/K)^\times$, which is equivalent to vanishing in every $V(L_i/K)^\times$. By the finite degree case this is equivalent to the existence of a lift of φ to a G_i-equivariant automorphism of $\mathcal{O}_{L_i}^\triangleright$. However, since those lifts are not unique, it is not immediate that they lift to a G-equivariant automorphism of $\mathcal{O}_L^\triangleright$.

Let S_i be the subset of those lifts, more precisely S_i is a subset of $\mathrm{Aut}_{G_i}(\mathcal{O}_{L_i}^\triangleright)$ consisting of all G_i-equivariant automorphisms which coincide with φ after restricting to $\mathcal{O}_{L_i}^\times$. For every two fields $L_i \subset L_j$ we have a natural restriction map $S_j \to S_i$ and we need to prove that the inverse limit $\varprojlim_{i\in I} S_i$ is nonempty. We are going to prove it by defining a topology on every set S_i which makes it into a compact topological space and such that the restriction maps $S_j \to S_i$ are continuous. That will finish the proof since the inverse limit of compact topological spaces is always nonempty.

We define the topology on S_i to be the topology of uniform convergence. Here, a basis of neighbourhoods of an automorphism φ is given by the sets U_ε of automorphisms ψ such that $|\varphi(x)/\psi(x) - 1| < \varepsilon$ for every $x \in \mathcal{O}_{L_i}^\triangleright$, where $\varepsilon > 0$. Then, it is immediate that with respect to this topology the restriction maps $S_j \to S_i$ are continuous. Therefore, we need to check that the topological spaces S_i are compact. Since the field extension L_i/K is finite, the monoid V_{L_i} is isomorphic to $\mathbb{N}$. Therefore we have an isomorphism $\mathrm{Hom}(V_{L_i}, \mathcal{O}_K^\times) \simeq \mathcal{O}_K^\times$. Moreover, as the set S_i is a torsor over the group $\mathrm{Hom}(V_{L_i}, \mathcal{O}_K^\times) \cong \mathcal{O}_K^\times$, we may fix a trivialization t and get a bijection $\mathrm{Hom}(V_{L_i}, \mathcal{O}_K^\times) \simeq S_i$, defined by $s \mapsto st$. Together we obtain a bijection $\mathcal{O}_K^\times \simeq S_i$ which is a homeomorphism,

by the definition of the topology on S_i. Hence the compactness of the group $\mathcal{O}_K^\times$ finishes the proof. □

In the following we are going to show that the rightmost arrow in the exact sequence (4.5) is in fact surjective. To achieve this we will construct explicitly certain homomorphism $\widehat{\mathbb{Z}}^\times \to \mathrm{Aut}_G(\mathcal{O}_L^\times)$ of groups, describe its action on $H^1(G, \mathcal{O}_L^\times)$ and prove that the composition $\widehat{\mathbb{Z}}^\times \to V(L/K)^\times$ is surjective.

Fix a Galois extension L/K and let M/K be a finite subextension. Then the field M is also a local field, in particular it is locally compact and we have a natural isomorphism

$$\mathcal{O}_M^\times \cong \varprojlim_{n\in\mathbb{N}} \mathcal{O}_M^\times/(\mathcal{O}_M^\times)^n.$$

The maps in this inverse system are given by the natural projections

$$\mathcal{O}_M^\times/(\mathcal{O}_M^\times)^{mn} \twoheadrightarrow \mathcal{O}_M^\times/(\mathcal{O}_M^\times)^n.$$

For every natural number n and for every element α_n of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ we may define a map $\mathcal{O}_M^\times/(\mathcal{O}_M^\times)^n \to \mathcal{O}_M^\times/(\mathcal{O}_M^\times)^n$ given by raising to the power α_n. It is easy to check that this is well defined an that the constructed map (denoted also by α_n) is an isomorphism. Now consider any element

$$\alpha = (\alpha_n)_n \in \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}.$$

For any two natural numbers n, m the automorphisms of $\mathcal{O}_M^\times/(\mathcal{O}_M^\times)^{nm}$ and $\mathcal{O}_M^\times/(\mathcal{O}_M^\times)^n$ given by α_{mn} and α_n are compatible with the natural projection $\mathcal{O}_M^\times/(\mathcal{O}_M^\times)^{mn} \twoheadrightarrow \mathcal{O}_M^\times/(\mathcal{O}_M^\times)^n$. Therefore, the element $\alpha \in \widehat{\mathbb{Z}}$ defines an automorphism of the inverse limit of those projection, hence an automorphism of $\mathcal{O}_M^\times$. Moreover, it is immediate from the construction that when the field M is Galois over K with the Galois group $\mathrm{Gal}(M/K) = H$ then the automorphism $\alpha\colon \mathcal{O}_M^\times \to \mathcal{O}_M^\times$ is H-equivariant. Write $\mathcal{O}_L^\times = \varinjlim_M \mathcal{O}_M^\times$ as the colimit over all finite subextensions M/K with respect to the natural inclusion maps. The automorphism α constructed for every finite extension M/K is compatible with inclusions hence it defines an automorphism of the colimit $\mathcal{O}_L^\times$. This defines the map $\widehat{\mathbb{Z}}^\times \to \mathrm{Aut}_G(\mathcal{O}_L^\times)$, which is obviously a group homomorphism.

It is easy to see that the automorphism α could also be defined in another way as follows. Pick a sequence of integers $a_i \in \mathbb{Z}$ converging to α (as $\mathbb{Z} \subset \widehat{\mathbb{Z}}$ is a dense subset). Let x be any element of the group of units $\mathcal{O}_L^\times$, we may then define $\alpha(x) = \lim_{i\to\infty} x^{a_i}$. As x lies in some finite subextension M/K the sequence converges and gives the same automorphism of $\mathcal{O}_L^\times$ as constructed previously.

We also easily see that the homomorphism $\widehat{\mathbb{Z}}^\times \to \mathrm{Aut}_G(\mathcal{O}_L^\times)$ respects the product decomposition $\mathcal{O}_L^\times \cong \mu_L^{p'} \times U_L$. Namely, let $\mathbb{Z}_{p'} = \prod_{l \neq p} \mathbb{Z}_l$, thus we have a canonical isomorphism $\widehat{\mathbb{Z}}^\times = \mathbb{Z}_p^\times \times \mathbb{Z}_{p'}^\times$. Then, we have the natural commutative diagram

$$\begin{array}{ccccc} \mathbb{Z}_p^\times & \hookrightarrow & \widehat{\mathbb{Z}}^\times & \hookleftarrow & \mathbb{Z}_{p'}^\times \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Aut}_G(U_L) & \hookrightarrow & \mathrm{Aut}_G(\mathcal{O}_L^\times) & \hookleftarrow & \mathrm{Aut}_G(\mu_L^{p'}), \end{array}$$

here we use the natural isomorphisms from Lemma 4.3.7. We easily see that the left vertical arrow is injective whereas the right vertical arrow is surjective.

Lemma 4.4.16. *Let L/K be a finite Galois field extension with the Galois group G and ramification index $e = e(L/K)$. Then, the composition of homomorphisms*

$$\widehat{\mathbb{Z}}^\times \to H^1(G, \mathcal{O}_L^\times) \to \mathrm{Aut}(H^1(G, \mathcal{O}_L^\times)) \cong (\mathbb{Z}/e\mathbb{Z})^\times$$

is equal to the natural projection homomorphism $\widehat{\mathbb{Z}}^\times \twoheadrightarrow (\mathbb{Z}/e\mathbb{Z})^\times$.

Proof. Let $N \in \widehat{\mathbb{Z}}^\times$, for any unit $x \in \mathcal{O}_L^\times$ we will use the notation x^N for the image of x under the automorphism corresponding to N. We may uniquely write $N = n + eN'$ for a natural number n satisfying $0 \leq n \leq e-1$ and some $N' \in \widehat{\mathbb{Z}}$. Then, we also have $x^N = x^{n+eN'} = x^n x^{eN'}$.

Take any uniformizer π of the local field L. The canonical generator of $H^1(G, \mathcal{O}_L^\times)$ is given by the class of a cocycle $\sigma(\pi)/\pi$. Therefore, by Lemma 4.4.8, the image by the action of N is given by the class of a cocycle

$$\left(\frac{\sigma(\pi)}{\pi}\right)^N = \left(\frac{\sigma(\pi)}{\pi}\right)^n \left(\frac{\sigma(\pi)}{\pi}\right)^{eN'}.$$

Since the group $H^1(G, \mathcal{O}_L^\times)$ is e-torsion, the e-power of the cocycle $(\frac{\sigma(\pi)}{\pi})^{N'}$ has trivial cohomology class. Therefore, the action of N is determined by the natural number n which obviously coincides with the image under the projection map. □

Corollary 4.4.17. *Let L/K be a Galois extension. Then the following sequence of group homomorphisms is exact*

$$1 \to \mathrm{Hom}(V_L, \mathcal{O}_K^\times) \to \mathrm{Aut}_G(\mathcal{O}_L^\triangleright) \to \mathrm{Aut}_G(\mathcal{O}_L^\times) \to V(L/K)^\times \to 1. \tag{4.6}$$

Moreover, when the value group V_L is $p(q-1)$-divisible,then we have the following short exact sequence

$$1 \to \mathrm{Aut}_G(\mathcal{O}_L^\triangleright) \to \mathrm{Aut}_G(\mathcal{O}_L^\times) \to V(L/K)^\times \to 1.$$

Proof. Surjectivity follows immediately from the definition of $V(L/K)^\times$ together with Lemma 4.4.16. When V_L is $p(q-1)$-divisible, then the group $\mathrm{Hom}(V_L, \mathcal{O}_K^\times)$ vanishes by Lemma 4.3.4. □

To state the next corollary, we need to introduce some notation. Let L/K be an algebraic extension and $\mu_L \subset L$ the subgroup of roots of unity. Then, we may define a supernatural number r_L as the order of the group μ_L. More precisely, write $\mu_L = \varinjlim_M \mu_M$, where M/K runs through all finite extensions M/K, and define r_L to be the limit of r_M. Similarly, when we consider only the group of roots of unity $\mu_L^{p'}$ of order prime to p, then we will denote its order by $r_L^{(p')}$. Moreover, we write $e'(L/K)$ for the supernatural number equal to the prime to p component of the supernatural number $e(L/K)$.

Another corollary we obtain from the exact sequence (4.6) is the following characterization of the triviality of the group $\mathrm{Aut}_G(\mathcal{O}_L^\triangleright)$.

Corollary 4.4.18. *Let L/K be a Galois extension with Galois group G. Then, the group $\mathrm{Aut}_G(\mathcal{O}_L^\triangleright)$ is trivial if and only if the following three conditions are satisfied:*

1. *The group V_L is $p(q-1)$-divisible,*
2. *We have the equality of supernatural numbers $r_L^{(p')} = e'(L/K)$,*
3. *The injection $\mathbb{Z}_p^\times \hookrightarrow \mathrm{Aut}_G(U_L)$ is an isomorphism.*

Proof. As we have seen, the group V_L is $p(q-1)$-divisible if and only if the group $\mathrm{Hom}(V_L, \mathcal{O}_K^\times)$ is trivial. We look at the diagram

$$\begin{array}{ccccccccc} & & & & & & \widehat{\mathbb{Z}}^\times & & \\ & & & & & & \downarrow{\scriptstyle \alpha} \quad \searrow^{\beta} & & \\ 1 & \longrightarrow & \mathrm{Hom}(V_L, \mathcal{O}_K^\times) & \longrightarrow & \mathrm{Aut}_G(\mathcal{O}_L^\triangleright) & \longrightarrow & \mathrm{Aut}_G(\mathcal{O}_L^\times) & \longrightarrow & V(L/K)^\times \longrightarrow 1. \end{array}$$

Therefore, we may assume that the group $\mathrm{Hom}(V_L, \mathcal{O}_K^\times)$ is trivial. Observe now that the equality $r_L^{(p')} = e'(L/K)$ is equivalent to the equality $\ker(\alpha) = \ker(\beta)$, moreover the third condition is equivalent to the surjectivity of the map α. Hence the result follows. □

We will concentrate on the third condition from the above corollary. It will be convenient to introduce the following definition.

Definition 4.4.19. Let L/K be a Galois extension with the Galois group G and let φ be a G-equivariant automorphism of the group U_L. We say that φ is a *standard* automorphism if it induced by the image of some element $\mathbb{Z}_p^\times$

through the map $\mathbb{Z}_p^\times \hookrightarrow \mathrm{Aut}_G(U_L)$. Moreover, we say that φ is a *nonstandard* automorphism if it is not a standard automorphism.

Thus, by Corollary 4.4.18, the existence of nonstandard automorphisms of the group U_L implies that the group $\mathrm{Aut}_G(\mathcal{O}_L^\flat)$ is nontrivial. We are going to describe certain class of field extensions L/K for which there exists a nonstandard automorphism. First, we introduce another definition.

Definition 4.4.20. Let L/K be a Galois field extension with the Galois group G and let φ_0 be a G-equivariant endomorphism of the group U_L. We say that φ_0 is *small* if for every element $x \in U_L$ the sequence $\varphi_0^{(n)}(x)$ converges to 1 (where by $\varphi_0^{(n)}$ we mean the composition $\underbrace{\varphi_0 \circ \ldots \circ \varphi_0}_{n}$).

For example, it is easy to see that the endomorphism of U_L determined by $N \in \mathbb{Z}_p$ is small if and only if N is divisible by p.

Lemma 4.4.21. *Let φ_0 be a G-equivariant continuous endomorphism of U_L. Assume that φ_0 is a small endomorphism. Then, the G-equivariant endomorphism φ of the group U_L defined as $\varphi(x) = \varphi_0(x)x$, for all $x \in U_L$, is a G-equivariant automorphism.*

Proof. First we prove surjectivity of the endomorphism φ. Let x be an element of U_L, thus x lies in some finite field extension M/K. Define the following infinite product

$$y = \frac{x}{\varphi_0(x)} \frac{\varphi_0^{(2)}(x)}{\varphi_0^{(3)}(x)} \frac{\varphi_0^{(4)}(x)}{\varphi_0^{(5)}(x)} \ldots,$$

which converges due to the assumption that φ_0 is small and completeness of the group U_M. Because the map φ_0 is continuous, we also obtain

$$\varphi_0(y) = \frac{\varphi_0(x)}{\varphi_0^{(2)}(x)} \frac{\varphi_0^{(3)}(x)}{\varphi_0^{(4)}(x)} \ldots,$$

hence we have $\varphi(y) = \varphi_0(y)y = x$, which proves the surjectivity of φ.

Thus, for every finite extension M/K we have a surjective homomorphism $\varphi\colon U_M \twoheadrightarrow U_M$ of $\mathbb{Z}_p$-modules. Since the extension M/K is finite, the group U_M is a finitely generated $\mathbb{Z}_p$-module. Therefore, the restriction of φ to U_M must be injective as well. Indeed, every surjective endomorphism of a finitely generated module over a ring is automatically injective. Hence the injectivity holds for every finite extension M/K, so φ is injective on U_L as well. □

Proposition 4.4.22. *Let $L'/L/K$ be a tower of Galois extensions with $L' \neq L$ and with Galois groups $G' = \mathrm{Gal}(L'/K)$ and $G = \mathrm{Gal}(L/K)$. Assume that the degree $[L' : L]$ is not divisible by p^∞ (as a supernatural number). Then, there exists a nonstandard G'-equivariant automorphism of the group $U_{L'}$.*

Proof. We easily reduce the proof to the following two cases: (1) when L'/L is finite of degree $[L' : L]$ which is a power of p, (2) when the degree $[L' : L]$ is not divisible by p. In each case we are going to construct a nontrivial small G'-equivariant endomorphism φ_0 of the group $U_{L'}$ which factorizes through the group U_L

$$\varphi_0 \colon U_{L'} \to U_L \hookrightarrow U_{L'}.$$

In the case (1), we consider the norm map $N = N_L^{L'} \colon U_{L'} \to U_L$ and simply define $\varphi_0(x) = N(x)$ for every $x \in U_{L'}$. Since the subgroup $\mathrm{Gal}(L'/L) \subset G'$ is normal, the homomorphism φ_0 is G'-equivariant. Moreover, it is small since we have $\varphi_0^{(n)}(x) = (N(x))^{p^{n-1}}$, which converges to 1 as $n \to \infty$.

In the case (2), we define first a normalized norm $N \colon U_{L'} \to U_L$ as follows. Let $x \in U_{L'}$ be any element, choose a finite extension M/L such that x belongs to M and define $N(x)$ to be $N_L^M(x)^{1/d}$, where $d = [M : K]$. This is well defined since by assumption d is prime to p, hence raising to the power d is an isomorphism of the group U_L. Moreover, the definition does not depend on the choice of the intermediate field M due to the normalizing factor $1/d$. Finally, we define the endomorphism φ_0 as $\varphi_0(x) = N(x)^p$ for $x \in L'$, which again has required properties.

We may now define a G'-equivariant endomorphism φ of the group U_L by the formula $\varphi(x) = \varphi_0(x)x$. By Lemma 4.4.21, it is in fact an automorphism of the group U_L. We claim that it is a nonstandard automorphism. Indeed, if we had $\varphi(x) = x^n$ for some $n \in \mathbb{Z}_p^\times$, then $\varphi_0(x) = x^{n-1}$ for every $x \in U_{L'}$. Since $\varphi_0(x) \in L$ and $L' \neq L$, it is only possible when $n = 1$, but then $\varphi_0(x) = 1$ which is a contradiction as the image a norm map is open. □

In particular, when the field extension L/K is finite there always exist nonstandard automorphisms.

Remark 4.4.23. Using the previous proposition one can give many examples of Galois field extensions L/K such that the group $\mathrm{Aut}_G(\mathcal{O}_L^\flat)$ is nontrivial. For instance, let M/K be any Galois extension with $V_M \cong \mathbb{Q}$ and let F/K a Galois extension not contained in M and of degree not divisible by p^∞. Then the field $L = MF$ contains all p'-roots of unity, hence it trivially satisfies conditions (1) and (2) from Corollary 4.4.18. On the other hand, it does not satisfy the condition (3). Indeed, from Proposition 4.4.22 applied to the extension L/M we see that there exist nonstandard automorphisms of the group U_L. Therefore, the group $\mathrm{Aut}_G(\mathcal{O}_L^\flat)$ must be nontrivial.

4.5 Complements

In this section we gather a few results complementing the previous discussion.

Definition 4.5.1. Let L/K be a finite extension of local fields and let φ be an automorphism of the group U_L. We write φ_0 for an endomorphism of U_L defined by the formula $\varphi(x) = \varphi_0(x)x$, for all $x \in U_L$. For any two automorphisms ψ and φ of the group U_L, we say that they are *p-equivalent* if there exist two natural numbers i, j such that $\varphi_0(x)^{p^i} = \psi_0(x)^{p^j}$, for all $x \in U_L$. This induces an equivalence relation on the group of all automorphisms of the group U_L.

Similarly if ψ and φ are two endomorphisms of the additive group $(L, +)$, we say that they are *p-equivalent* if there exists an integer k such that $\varphi(x) = p^k\psi(x)$, for all $x \in L$. Again, this induces an equivalence relation on the group of all endomorphisms of the group $(L, +)$.

Proposition 4.5.2. *Let L/K be a finitely ramified extension (i.e. the extension LK^{ur}/K^{ur} is finite). Then, there exists a natural bijection between the set of p-equivalence classes of automorphisms of the group U_L and the set of p-equivalence classes of endomorphisms of the group $(L, +)$. Moreover, if L/K is a Galois extension with the Galois group G, then this bijection preserves the equivalence classes of G-equivariant morphisms.*

Proof. Consider the p-adic logarithm map $\log\colon U_L \to L$. It induces an isomorphism of groups $U_L/\mu_L^p \cong \log(L) \subset L$ which is G-equivariant when L/K is a Galois extension,. Moreover, the group $\log(L)$ is open and compact due to the finite ramification assumption.

Let now φ be an automorphism of the group U_L and consider the endomorphism φ_0 of U_L. Using the logarithm map it defines an endomorphism $\log(\varphi_0)$ of the (additive) group $\log(L)$ hence also an endomorphism of the (additive) group $\log(L) \otimes \mathbb{Q}_p \cong L$. Moreover, if we replace φ by some p-equivalent automorphism then φ_0 changes to $\varphi_0^{p^i}$ thus $\log(\varphi_0)$ changes to a p-equivalent endomorphism $p^i \log(\varphi_0)$.

On the other hand, suppose that α is an endomorphism of the additive group L. Because the submodule $\log(L)$ is compact and open in L, there exists a natural number n such that $p^n\alpha(\log(L)) \subset \log(L)$. Thus, replacing α by a p-equivalent endomorphism we may assume that $\alpha(\log(L)) \subset \log(L)$. Therefore, by using the inverse of the logarithm map, we obtain an endomorphism $\exp(\alpha)$ of the group U_L/μ_L^p. Because U_L contains only finitely many roots of unity we may assume, after enlarging n, that $\exp(\alpha)$ defines a morphism $U_L/\mu_L^p \to U_L$. Denote by φ_0 the endomorphism of U_L given by the composition

$U_L \twoheadrightarrow U_L/\mu_L^p \to U_L$. Enlarging n if necessary, we may assume that for every $x \in U_L$ the sequence $\varphi_0^{(i)}(x)$ converges to 1, as i goes to infinity. Thus, using Lemma 4.4.21, we define an automorphism φ of the group U_L by the formula $\varphi(x) = x\varphi_0(x)$. It is easy to see that these two constructions define bijection from the statement.

Moreover, it is obvious that when the field extension L/K is Galois both these constructions preserve the property of being G-equivariant. Indeed, it follows immediately from the G-equivariance of the p-adic logarithm map. □

Let L/K be a Galois extension with the Galois group G. Fix an automorphism φ of the monoid $\mathcal{O}_L^{\triangleright}$, thus φ induces an automorphism of the subgroup μ_L of roots of unity. Suppose that L contains a primitive root of unity of order n. Then, the induced action of φ on nth roots of unity is given by $\zeta \mapsto \zeta^{r_n}$ for some unique element $r_n \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Lemma 4.5.3. *Let $a \in \mathcal{O}_K^{\triangleright}$. Suppose that there exists $x \in \mathcal{O}_L^{\triangleright}$ such that $x^n = a$ for some natural number n. Then, n divides $(r_n - 1)v_K(a)$. Therefore, when n is prime to $v_K(a)$ we obtain $r_n = 1$, in other words φ is the identity homomorphism on the set of nth roots of unity.*

Proof. Take any $\sigma \in G$. As $\sigma(x)/x$ is a root of unity, we obtain

$$\frac{\sigma(\varphi(x))}{\varphi(x)} = \varphi\left(\frac{\sigma(x)}{x}\right) = \left(\frac{\sigma(x)}{x}\right)^{r_n} = \frac{\sigma(x^{r_n})}{x^{r_n}}$$

Therefore $\varphi(x)/x^{r_n}$ is stabilized by every element σ in G, hence it belongs to K. It follows that $\varphi(x) = tx^{r_n}$ for some $t \in K$ and raising to nth power gives $\varphi(a) = t^n a^{r_n}$. Applying now v_K we obtain $v_K(a) = nv_K(t) + r_n v(a)$, hence $(r_n - 1)v_K(a) = -nv_K(t)$. When n is prime to $v_K(a)$ we have that n divides $r_n - 1$ which together with $0 \leq r_n - 1 \leq n - 2$ implies $r_n = 1$. □

Lemma 4.5.4. *Suppose that φ restricts to the identity on the set of nth roots of unity. Let $a \in \mathcal{O}_K^{\triangleright}$ and assume that there exists $x \in \mathcal{O}_L^{\triangleright}$ such that $x^n = a$. Then, $\varphi(a)/a$ lies in $(\mathcal{O}_K^\times)^n$.*

Proof. Using the same computation as in the previous lemma (with $r_n = 1$) we obtain $\varphi(x) = tx$ for some $t \in \mathcal{O}_K^\times$ and again raising to the nth power gives us $\varphi(a) = at^n$. □

Corollary 4.5.5. *Suppose that φ restricts to the identity on the group of roots of unity of p-power order. Let $a \in \mathcal{O}_K^{\triangleright}$ and assume that for every natural number n there exists $x \in \mathcal{O}_L^{\triangleright}$ such that $x^{p^n} = a$. Then $\varphi(a) = \zeta a$, where ζ is a root of unity of order prime to p.*

Proof. Indeed, applying Lemma 4.5.4 we see that $\varphi(a)/a$ belongs to the intersection $\bigcap_{n\geq 1}(\mathcal{O}_K^{\times})^{p^n}$, which is equal to the subgroup of roots of unity of K of order prime to p. □

Corollary 4.5.6. *Assume that K contains pth roots of unity and let L/K be the maximal pro-p-extension. Then, every G-equivariant automorphism of the monoid $\mathcal{O}_L^{\triangleright}$ is of the form $a \mapsto \zeta_a a$ where ζ_a is p'-root of unity. In other words, we have the equality*

$$\mathrm{Aut}_G(\mathcal{O}_L^{\triangleright}) = \mathrm{Aut}_G^{p'}(\mathcal{O}_L^{\triangleright}).$$

Proof. Fix an G-equivariant automorphism φ of the monoid $\mathcal{O}_L^{\triangleright}$ and let π_K be a uniformizer of K. By assumption, the field L contains all p^nth roots of π_K, thus applying Lemma 4.5.3 we obtain that φ acts trivially on all roots of unity of p-power order. Now, fix any $a \in L$ and observe that all roots of a of p-power order also belong to L. Therefore, applying Corollary 4.5.5 we conclude that $\varphi(a) = \zeta a$ for some $\zeta \in \mu^p$. □

Remark 4.5.7. Let L/K be as in the Corollary 4.5.6. Using the sequence (4.6) (or repeating the proof of the previous corollary) we easily see that every G-equivariant automorphism of the group U_L is standard, hence L/K satisfies condition (3) from Corollary 4.4.18. On the other hand, conditions (1) and (2) are not satisfied.

Corollary 4.5.8. *Let L/K be the maximal tamely ramified extension of K. Then, every G-equivariant automorphism of the monoid $\mathcal{O}_L^{\triangleright}$ is of the form $a \mapsto \varphi_0(a)a$, where $\varphi_0(a)$ is a principal unit. In other words, we have the equality*

$$\mathrm{Aut}_G(\mathcal{O}_L^{\triangleright}) = \mathrm{Aut}_G^0(\mathcal{O}_L^{\triangleright})$$

Proof. The proof is analogous to the proof of the previous corollary. Let φ be a G-equivariant automorphism of the monoid $\mathcal{O}_L^{\triangleright}$. For every prime number $l \neq p$ all the lth roots of a uniformizer π_K of K belong to L, hence by Lemma 4.5.3 we see that φ acts trivially on prime to p roots of unity. Take any $x \in \mathcal{O}_L^{\triangleright}$, hence $x \in \mathcal{O}_M^{\triangleright}$ for some finite extension M/K. Then, using Lemma 4.5.4, we have $\varphi_0(x) \in \bigcap_{l\neq p}(\mathcal{O}_M^{\times})^l = U_M$. □

Remark 4.5.9. Let L/K be as in Corollary 4.5.8. Observe that the conditions (1) and (2) from Corollary 4.4.18 are trivially satisfied. On the other hand, we easily see using Proposition 4.4.22 that the condition (3) is not satisfied, i.e., there exist nonstandard automorphisms of U_L.

Remark 4.5.10. We have provided a few examples of Galois field extension L/K such that the group $\mathrm{Aut}_G(\mathcal{O}_L^{\triangleright})$ is nontrivial. On the other hand, we

gave only one example for which the group $\mathrm{Aut}_G(\mathcal{O}_L^{\triangleright})$ is trivial, namely when $L = K^{\mathrm{alg}}$. Therefore, one may pose the following question: Does there exist a Galois field extension L/K which is not algebraically closed such that the group $\mathrm{Aut}_G(\mathcal{O}_L^{\triangleright})$ is trivial? The author's attempts to answer this question provided another motivation for developing the results contained in this chapter.

4.6 Surjectivity of the restriction

In this section we briefly discuss certain results concerning the image of the restriction map

$$\mathrm{Aut}(G \curvearrowright \mathcal{O}_L^{\triangleright}) \to \mathrm{Aut}(G). \tag{4.7}$$

As we have already mentioned, it is the existence of outer automorphisms of G that makes this problem nontrivial.

We start again with the local field K, a finite extension of $\mathbb{Q}_p$. We are going to define a tower of field extensions K_n of K, for every natural number $n \in \mathbb{N}$. First, let $K_0 = K$ and then for every $n \geq 1$ we take $K_n = K_{n-1}^{\mathrm{ab}}$ to be the maximal abelian extension of K_{n-1}. Then, K_n/K is also a Galois field extension, denote its Galois group by G_n. We have surjective maps $G_{n+1} \twoheadrightarrow G_n$ and the kernel of this map is a characteristic subgroup of G_{n+1}. In particular, we have a natural homomorphism $\mathrm{Aut}(G_{n+1}) \to \mathrm{Aut}(G_n)$.

We now consider the sequence of Galois monoids $G_n \curvearrowright \mathcal{O}_{K_n}^{\triangleright}$ as well as their "shifted" versions $G_{n+1} \curvearrowright \mathcal{O}_{K_n}^{\triangleright}$. Again, using the fact that the quotient $G_{n+1} \twoheadrightarrow G_n$ is characteristic, we obtain natural maps

$$\mathrm{Aut}(G_{n+1} \curvearrowright \mathcal{O}_{K_{n+1}}^{\triangleright}) \to \mathrm{Aut}(G_{n+1} \curvearrowright \mathcal{O}_{K_n}^{\triangleright}) \to \mathrm{Aut}(G_n \curvearrowright \mathcal{O}_{K_n}^{\triangleright}).$$

Together with the restriction map (4.7) we obtain the following commutative diagram

$$\begin{array}{ccc}
\mathrm{Aut}(G_{n+1} \curvearrowright \mathcal{O}_{K_{n+1}}^{\triangleright}) & \xrightarrow{\alpha_{n+1}} & \mathrm{Aut}(G_{n+1}) \\
\downarrow{\scriptstyle \gamma_{n+1}} & & \| \\
\mathrm{Aut}(G_{n+1} \curvearrowright \mathcal{O}_{K_n}^{\triangleright}) & \xrightarrow{\beta_{n+1}} & \mathrm{Aut}(G_{n+1}) \\
\downarrow & & \downarrow \\
\mathrm{Aut}(G_n \curvearrowright \mathcal{O}_{K_n}^{\triangleright}) & \xrightarrow{\alpha_n} & \mathrm{Aut}(G_n)
\end{array}$$

for every $n \geq 1$, where various restriction maps are denoted by α_n, β_n and γ_n.

Proposition 4.6.1. *The map β_n is surjective for every $n \geq 1$. Moreover, for $n \geq 2$, we have the equality*

$$\ker(\alpha_n) = \ker(\gamma_n).$$

Proof. Observe first that starting from the topological group G_n, for some $n \geq 1$, we may reconstruct group theoretically the sequence of quotients

$$G_n \twoheadrightarrow G_{n-1} \twoheadrightarrow \ldots \twoheadrightarrow G_0.$$

Indeed, denote $H_s = \ker(G_n \twoheadrightarrow G_s)$ for $0 \leq s \leq n-1$, thus have a filtration

$$H_{n-1} \subset H_{n-2} \subset \ldots \subset H_0.$$

Then, it is easy to see that $H_1 = \ker(G_n \twoheadrightarrow G_n^{\mathrm{ab}})$. Moreover, we have $H_{i+1} = \ker(H_i \twoheadrightarrow H_i^{\mathrm{ab}})$, which determines all quotients $G_n \twoheadrightarrow G_i$ for $i \leq n$.

We are going to use similar arguments as in the proof of Proposition 1.3.1. Let H be an open subgroup of G_n containing H_{n-1} and consider its preimage H_K under the surjection $G_K \twoheadrightarrow G_n$

$$\begin{array}{ccc} H_K & \hookrightarrow & G_K \\ \downarrow & & \downarrow \\ H & \hookrightarrow & G_n \end{array}$$

It follows immediately from definitions that the surjection $H_K \twoheadrightarrow H$ induces an isomorphism $H_K^{\mathrm{ab}} \cong H^{\mathrm{ab}}$. Denote by L_H/K the field extension corresponding to the open subgroup H of G_K. Then, by applying the argument used in the proof of Proposition 1.3.1, we may reconstruct the ramification index $e(L_H/K)$ of this field extension. Therefore, by taking intersection over all open subgroups H corresponding to unramified field extensions, together with the fact that $K^{\mathrm{ur}} \subset K^{\mathrm{ab}}$, we may determine the inertia subgroup I_n of the group G_n. Moreover, by considering p'-torsion of H^{ab} for all open subgroups H as above we may determine the p'-cyclotomic character $G_n \to \widehat{\mathbb{Z}}^{p'}$, which consequently determines uniquely the Frobenius element in the quotient G_n/I_n. Thus, we reconstruct the natural surjection $G_m \twoheadrightarrow \widehat{\mathbb{Z}}$.

We may apply the same construction to any open subgroup $H \subset G_m$ which contains the closed subgroup H_{n-1}, hence we reconstruct surjections $H \twoheadrightarrow H^{\mathrm{ab}} \twoheadrightarrow \widehat{\mathbb{Z}}$. Then, by taking preimage of the Frobenius element $1 \in \widehat{\mathbb{Z}}$ under the map $H^{\mathrm{ab}} \twoheadrightarrow \widehat{\mathbb{Z}}$ we reconstruct the monoid $\mathcal{O}^{\triangleright}_{L_H}$ equipped with its natural G_n-action. Finally, we consider the colimit of modules $\mathcal{O}^{\triangleright}_H$ under the transfer map for all open subgroup H containng the closed subgroup H_{n-1}. This produces a G_n monoid $\mathcal{O}^{\triangleright}_{K_{n-1}}(G_n)$, which is isomorphic to the G_n-monoid $\mathcal{O}^{\triangleright}_{K_{n-1}}$. Since this construction is functorial, any automorphism of G_n induces an automorphism of $\mathcal{O}^{\triangleright}_{K_{n-1}}(G_n)$ compatible with the G_n-action. This proves the surjectivity of the map β_n.

Now we are going to prove the equality of kernels of α_n and γ_n, for $n \geq 2$. Only the inclusion $\ker(\alpha_n) \subset \ker(\gamma_n)$ is nontrivial. Let $\varphi \in \ker(\alpha_n)$, in other

words φ is a G_n-equivariant automorphism of the monoid $\mathcal{O}^{\triangleright}_{K_n}$. We need to show that the restriction of φ to the monoid $\mathcal{O}^{\triangleright}_{K_{n-1}}$ is the identity homomorphism. From the assumption we have $K_1 \subset K_{n-1}$, hence the K_{n-1} contains all roots of unity. Therefore, for any $x \in K_{n-1}$, the field K_n contains all roots of x. Thus, we may apply Lemma 4.5.3 to obtain that φ is the identity on the set of roots of unity. Finally, using Lemma 4.5.4 we see that φ is trivial on the monoid $\mathcal{O}^{\triangleright}_{K_{n-1}}$. Indeed, if $x \in M$ for some finite extension M/K, then $\varphi_0(x) \in \bigcap_{n\in\mathbb{N}}(\mathcal{O}^{\times}_M)^n = \{1\}$. □

Corollary 4.6.2. *Let φ_n be an automorphism of G_n. Suppose that φ_n lifts to an automorphism of G_{n+1}. Then φ_n lifts to an automorphism of the pair $G_n \curvearrowright \mathcal{O}^{\triangleright}_{K_n}$.*

Proof. It follows from the surjectivity of the map β_{n+1}. □

Bibliography

[1] *Revêtements étales et groupe fondamental (SGA 1)*, volume 3 of *Documents Mathématiques (Paris) [Mathematical Documents (Paris)]*. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)].

[2] Yves André. On a geometric description of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ and a p-adic avatar of $\widehat{GT}$. *Duke Math. J.*, 119(1):1–39, 2003.

[3] Yves André. *Period mappings and differential equations. From* $\mathbb{C}$ *to* $\mathbb{C}_p$, volume 12 of *MSJ Memoirs*. Mathematical Society of Japan, Tokyo, 2003. Tôhoku-Hokkaidô lectures in arithmetic geometry, With appendices by F. Kato and N. Tsuzuki.

[4] Fabrizio Andreatta, Adrian Iovita, and Minhyong Kim. A p-adic nonabelian criterion for good reduction of curves. *Duke Math. J.*, 164(13):2597–2642, 2015.

[5] Tom M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York-Heidelberg, 1976. Undergraduate Texts in Mathematics.

[6] Vladimir G. Berkovich. Smooth p-adic analytic spaces are locally contractible. *Invent. Math.*, 137(1):1–84, 1999.

[7] Spencer Bloch and Kazuya Kato. L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.

[8] Siegfried Bosch. *Lectures on formal and rigid geometry*, volume 2105 of *Lecture Notes in Mathematics*. Springer, Cham, 2014.

[9] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[10] Christophe Breuil. Groupes p-divisibles, groupes finis et modules filtrés. *Ann. of Math. (2)*, 152(2):489–549, 2000.

[11] Robert Coleman and Adrian Iovita. The Frobenius and monodromy operators for curves and abelian varieties. *Duke Math. J.*, 97(1):171–215, 1999.

[12] Gary Cornell, Joseph H Silverman, and Michael Artin. *Arithmetic geometry*. Springer, 1986.

[13] I. B. Fesenko and S. V. Vostokov. *Local fields and their extensions*, volume 121 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, second edition, 2002. With a foreword by I. R. Shafarevich.

[14] Jean-Marc Fontaine. Le corps des périodes p-adiques. Number 223, pages 59–111. 1994. With an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988).

[15] Jean Fresnel and Marius van der Put. *Rigid analytic geometry and its applications*, volume 218 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 2004.

[16] Yuichiro Hoshi. On the pro-p absolute anabelian geometry of proper hyperbolic curves. *J. Math. Sci. Univ. Tokyo*, 25(1):1–34, 2018.

[17] Yuichiro Hoshi. Mono-anabelian reconstruction of number fields. *RIMS Preprint*, 2019.

[18] Finn F. Knudsen. The projectivity of the moduli space of stable curves. II. The stacks $M_{g,n}$. *Math. Scand.*, 52(2):161–199, 1983.

[19] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[20] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[21] Shinichi Mochizuki. The profinite Grothendieck conjecture for closed hyperbolic curves over number fields. *J. Math. Sci. Univ. Tokyo*, 3(3):571–627, 1996.

[22] Shinichi Mochizuki. The local pro-p anabelian geometry of curves. *Invent. Math.*, 138(2):319–423, 1999.

[23] Shinichi Mochizuki. The absolute anabelian geometry of hyperbolic curves. In *Galois theory and modular forms*, volume 11 of *Dev. Math.*, pages 77–122. Kluwer Acad. Publ., Boston, MA, 2004.

[24] Shinichi Mochizuki. Galois sections in absolute anabelian geometry. *Nagoya Math. J.*, 179:17–45, 2005.

[25] Shinichi Mochizuki. Semi-graphs of anabelioids. *Publ. Res. Inst. Math. Sci.*, 42(1):221–322, 2006.

[26] Shinichi Mochizuki. Absolute anabelian cuspidalizations of proper hyperbolic curves. *J. Math. Kyoto Univ.*, 47(3):451–539, 2007.

[27] Shinichi Mochizuki. A combinatorial version of the Grothendieck conjecture. *Tohoku Math. J. (2)*, 59(3):455–479, 2007.

[28] Shinichi Mochizuki. *Topics in Absolute Anabelian Geometry: Generalities. I.* Kyoto University, Research Institute for Mathematical Sciences, 2008.

[29] Shinichi Mochizuki. The étale theta function and its Frobenioid-theoretic manifestations. *Publ. Res. Inst. Math. Sci.*, 45(1):227–349, 2009.

[30] Shinichi Mochizuki. Topics in absolute anabelian geometry III: global reconstruction algorithms. *J. Math. Sci. Univ. Tokyo*, 22(4):939–1156, 2015.

[31] Shinichi Mochizuki. Inter-universal Teichmüller Theory I: Construction of Hodge Theaters. *to appear in PRIMS*, 2020.

[32] David Mumford. An analytic construction of degenerating abelian varieties over complete rings. *Compositio Math.*, 24:239–272, 1972.

[33] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[34] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[35] Alain Robert. *Elliptic curves*. Lecture Notes in Mathematics, Vol. 326. Springer-Verlag, Berlin-New York, 1973. Notes from postgraduate lectures given in Lausanne 1971/72.

[36] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[37] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[38] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[39] J. T. Tate. p-divisible groups. In *Proc. Conf. Local Fields (Driebergen, 1966)*, pages 158–183. Springer, Berlin, 1967.