Publ. RIMS Kyoto Univ. **59** (2023), 843–882
DOI 10.4171/PRIMS/59-4-6

Pro-p Criterion of Good Reduction of Punctured Elliptic Curves

by

Wojciech Porowski

Abstract

In this paper we consider an affine hyperbolic curve X over a p-adic local field K obtained from an elliptic curve E by removing a K-rational point given by the origin O. We introduce the maximal geometrically pro-p quotient Π_X of the étale fundamental group $\pi_1^{\text{ét}}(X)$ of the hyperbolic curve X and analyse the problem of determining the reduction type of the elliptic curve E from the topological group Π_X. As our main result we give a group-theoretic construction of the reduction type of E from the group Π_X under the assumption that $p \geq 5$ and that E has a nontrivial K-rational p-torsion point.

2020 Mathematics Subject Classification: 14H30.
Keywords: Anabelian geometry, étale fundamental group.

§1. Introduction

Let E be an elliptic curve over a p-adic local field K and consider a hyperbolic curve X obtained from E by removing a K-rational point given by the origin O of E. Let Π_X be the maximal geometrically pro-p étale fundamental group of the hyperbolic curve X. Fix an algebraic closure K^{alg} of K. Then we have a short exact sequence of topological groups

$$1 \to \Delta_X \to \Pi_X \to \mathrm{Gal}(K^{\mathrm{alg}}/K) \to 1,$$

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

In this paper we consider the following problem: Given the topological group Π_X, is it possible to determine the reduction type of the elliptic curve E over K? The result we prove here is the following theorem.

Communicated by S. Mochizuki. Received May 11, 2021. Revised December 3, 2021; January 21, 2022.

W. Porowski: School of Mathematics, University of Nottingham, Nottingham NG7 2RD, UK;
e-mail: wo.porowski@gmail.com

Theorem 1.1. *Assume that $p \geq 5$ and that E has a nontrivial K-rational p-torsion point. Then the reduction type of E over K can be determined group theoretically from the topological group Π_X.*

We will see that even when the above assumptions are not satisfied we may recover the reduction type in some special cases. In fact, we will prove a slightly stronger theorem, where the assumption on the existence of a p-torsion point is replaced by assuming that Π_X is equipped with certain additional data.

Theorem 1.2. *Assume that $p \geq 5$. Then the reduction type of E over K can be determined group theoretically from the topological group Π_X equipped with one discrete section.*

We briefly explain the notion of a "discrete section" used in the above statement. First, it is well known that the subgroup $\Delta_X \subset \Pi_X$ can be characterized group theoretically; therefore we may also construct the quotient

$$\Pi_X \twoheadrightarrow \Pi_X/\Delta_X.$$

Clearly, the quotient Π_X/Δ_X is isomorphic to the Galois group $\mathrm{Gal}(K^{\mathrm{alg}}/K)$. Then the set of discrete sections is a certain subset of the set of all sections of the above surjection coming from cotangent vectors at the cusp of X; for a more precise definition, see Section 7.

The problem considered in this paper is motivated by the results of [H], where it is proved that for a proper hyperbolic curve X one can determine, from data of the fundamental group Π_X, whether the curve X has good ordinary reduction, i.e., the curve X has good reduction and the reduction of the Jacobian $J(X)$ of X is an ordinary abelian variety. Thus, the main result of this paper strengthens [H] in the case of punctured elliptic curves.

Before continuing, let us explain the reason why recovering the reduction type in the absolute setting (i.e., from the group Π_X) is more difficult than in the relative case (i.e., from the surjection $\Pi_X \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{alg}}/K)$). It is easy to see that in the relative case one can recover the representation

$$\iota\colon \mathrm{Gal}(K^{\mathrm{alg}}/K) \to \mathrm{GL}(T_p(E))$$

on the p-adic Tate module $T_p(E)$ of E. Thus the elliptic curve E has good reduction if and only if the representation ι is crystalline. On the other hand, even though in the absolute case one can still construct a representation

$$\iota_0\colon \Pi_X/\Delta_X \to \mathrm{GL}(T_p(E)),$$

it is not clear how to choose group theoretically an isomorphism between Π_X/Δ_X and the absolute Galois group of K. Any two choices of such an isomorphism would differ by an automorphism of the group $\mathrm{Gal}(K^{\mathrm{alg}}/K)$; however, this automorphism may not preserve the category of crystalline representations. Indeed, it is known that there exists an automorphism α of the group $\mathrm{Gal}(K^{\mathrm{alg}}/K)$ and a Hodge–Tate representation

$$j\colon\ \mathrm{Gal}(K^{\mathrm{alg}}/K) \to \mathrm{GL}(V)$$

such that $j \circ \alpha$ is not a Hodge–Tate representation. Therefore, the method of considering the p-adic representation $\mathrm{GL}(T_p(E))$ that may be used in the relative case is not applicable in the absolute case. 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 the absolute Galois group of K and are purely group theoretic.

Let us briefly summarize the content of this paper. In Sections 3 and 4 we recall some classical results from p-adic Hodge theory concerning p-adic Tate modules which are then applied in Section 5 to reduce the proof of Theorem 1.2 to the case of an elliptic curve with good supersingular reduction. The rest of the paper uses methods of (mono)-anabelian geometry. In Section 6 we briefly discuss Kummer classes of functions and their group-theoretic evaluation at points. This construction is applied in Section 8, where we consider cohomology classes of certain rational functions on the elliptic curve E. In Section 7 we introduce the notions of discrete and integral sections, then in Section 10 we discuss their anabelian constructions. The crucial method we use there is based on a group-theoretic version of the operation

$$\mathcal{O}(X)^* \ni f \mapsto v(f(P)) \in \mathbb{Q},$$

namely evaluating a rational function at a point P and applying the p-adic valuation. This will be applied to compute local heights of torsion points, following a pro-p variant of a method described in [P]. The most important step of this construction consists of determining a certain isomorphism of Galois modules which we call the *rigidity* isomorphism; this task is achieved in Section 9. Finally, after these preparations, in Section 11 we give the proof of the main theorem.

§2. Notation

For a field K we write K^{alg} for a fixed algebraic closure of K. When K is a complete discrete valuation field of characteristic zero we write $G_K = \mathrm{Gal}(K^{\mathrm{alg}}/K)$ for the absolute Galois group of K and $I_K \subset G_K$ for the inertia subgroup.

In this paper by a *local* field we always mean a p-adic local field i.e., a finite extension of $\mathbb{Q}_p$. For a local field K we have a discrete valuation $v_K\colon K^* \to \mathbb{Z}$

normalized by $v_K(\pi_K) = 1$, where π_K is a uniformizer of K. We denote by k the residue field of K. On the algebraic closure K^{alg} we also have a valuation $v\colon (K^{\mathrm{alg}})^* \to \mathbb{Q}$ normalized by requiring $v(p) = 1$. Thus $v_K(x) = ev(x)$ for every $x \in K^*$, where e is the absolute ramification degree of K. We also write $U_K \subset \mathcal{O}_K^* \subset \mathcal{O}_K$ for the group of principal units, the group of units and the valuation ring, respectively.

For a local field K we denote by $\widehat{K^*}$ the inverse limit

$$\widehat{K^*} = \varprojlim_{n\in\mathbb{N}} K^*/(K^*)^{p^n}.$$

Note that in this limit we consider only powers of p. By Kummer theory we have

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

here $\mu_{p^n} \subset K^{\mathrm{alg}}$ is the group of p^nth roots of unity. Therefore, by taking the inverse limit over all natural numbers n, we obtain an isomorphism

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

The kernel of the natural homomorphism of groups $K^* \to \widehat{K^*}$ is equal to the subgroup of roots of unity of order prime to p contained in K, which we denote by $\mu_K^{\neq p}$. For every local field L we define the quotient

$$L^{\times\mu} = L^\times/\mu_L^{\neq p}.$$

We have a natural isomorphism $U_L \cong \mathcal{O}_L^*/\mu_L^{\neq p}$, as well as injections

$$U_L \hookrightarrow L^{\times\mu} \hookrightarrow \widehat{L^*}$$

When X is a scheme over K and L/K is a field extension, we write X_L for the scheme over L obtained as a base change of X. For a curve X over K we write Δ_X for the maximal pro-p quotient of the geometric fundamental group $\pi_1(X_{K^{\mathrm{alg}}})$. Then the maximal geometrically pro-p fundamental group Π_X of X is defined as the quotient of the fundamental group $\pi_1(X)$ by the kernel of the surjection $\pi_1(X_{K^{\mathrm{alg}}}) \twoheadrightarrow \Delta_X$. Thus, we have a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(X_{K^{\mathrm{alg}}}) \arrow[r] \arrow[d, two heads] & \pi_1(X) \arrow[r] \arrow[d, two heads] & G_K \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \Delta_X \arrow[r] & \Pi_X \arrow[r] & G_K \arrow[r] & 1.
\end{tikzcd}$$

Throughout the paper, an elliptic curve will be denoted by E and its origin by O.

§3. Application of p-adic Hodge theory

In this section we recall a few facts from the theory of p-adic representations that we will use later. Let V be a finite-dimensional vector space over $\mathbb{Q}_p$ equipped with a linear continuous G_K-action. We will simply say that V is a representation of G_K. Let $\mathbb{Q}_p(1)$ be the one-dimensional representation given by the cyclotomic character. For every integer $n \in \mathbb{Z}$ we will denote by $V(n)$ the nth Tate twist of the representation V. We write $\mathbf{B}_{\mathrm{cris}}$, $\mathbf{B}_{\mathrm{st}}$ and $\mathbf{B}_{\mathrm{dR}}$ for the crystalline, semistable and de Rham period rings. For a G_K-representation V, we denote

$$D_{\mathrm{dR}}(V) = (V \otimes_{\mathbb{Q}_p} \mathbf{B}_{\mathrm{dR}})^{G_K}.$$

The ring $\mathbf{B}_{\mathrm{dR}}$ is equipped with a decreasing filtration $\mathbf{B}^i_{\mathrm{dR}}$ for $i \in \mathbb{Z}$, which induces a decreasing filtration $D_{\mathrm{dR}}(V)^i$ on the vector space $D_{\mathrm{dR}}(V)$. Moreover, if the representation V is de Rham then the dimension of the i-graded subquotient

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

is equal to the multiplicity of the weight i in the Hodge–Tate decomposition of V.

For an elliptic curve E over a p-adic local field K, we write $T_p(E)$ for the (p-adic) Tate module and $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ for the induced G_K-representation. The fundamental result which we are going to use is the following theorem connecting the reduction of E/K and the p-adic representation $V_p(E)$ (see [CI] for the good reduction case and [B] for the semistable case).

Theorem 3.1. *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 semiabelian reduction over K if and only if the p-adic representation $V_p(E)$ is semistable.*

We also recall, following [BK], 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 consider the kernel of the natural map

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

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

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

be the extension of representations corresponding to α, via the identification

$$H^1(G_K, V) = \mathrm{Ext}^1_{\mathbb{Q}_p[G_K]}(\mathbb{Q}_p, V).$$

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 3.2. *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 [BK] (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 3.1). 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 3.3. *Let V be a two-dimensional p-adic representation of G_K 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. Moreover, if V' and V'' are not isomorphic then the representation V is in fact crystalline.

Proof. By tensoring with the dual of the character V'' we may assume that $V'' = \mathbb{Q}_p$. Moreover, by Lemma 3.2 we may assume that the unramified character V' is nontrivial. Therefore, it is enough to prove that in this case the representation V is crystalline.

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 [NSW, Thm. 7.3.1 and Cor. 2.7.6]) 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, if 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 the local Tate duality (see [NSW, Thm. 7.2.6]) that

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

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 [BK, Cor. 3.8.4], we know that for every de Rham representation W we have the equality

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

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. □

Remark 3.4. Clearly, one can also give a proof of Lemma 3.3 using the machinery of (ϕ, N)-modules and a straightforward linear algebra computation.

§4. Structure of the 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 local field. A similar discussion would be valid in the more general case of abelian varieties. All the results are well known; e.g., see [T].

Let E be an elliptic curve over a p-adic local field K. We assume that E has split semiabelian reduction over K, i.e., the Néron model $\mathcal{E}$ of E, which is a smooth scheme over $\mathrm{Spec}(\mathcal{O}_K)$, has the special fiber $\mathcal{E}_k$ isomorphic to either an elliptic curve or to a split torus. Equivalently, the special fiber 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 semiabelian reduction we know that E is a Tate curve. Thus, there exists a unique element $q \in K^*$ with $|q| < 1$ and an isomorphism $E \cong E_q$; here E_q is the Tate elliptic curve associated to q. Hence we also have a G_K-equivariant isomorphism $E(K^{\mathrm{alg}}) \cong (K^{\mathrm{alg}})^*/q^{\mathbb{Z}}$. In particular, the group of n-torsion points is isomorphic to the subgroup of $(K^{\mathrm{alg}})^*/q^{\mathbb{Z}}$ generated by the elements

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

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 by n 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

$$1 \to \varprojlim_{k \geq 1} \mu_{p^k} \to T_p(E) \to \varprojlim_{k \geq 1} \mathbb{Z}/p^k\mathbb{Z} \to 1.$$

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 the group G_K,

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

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 $\mathrm{Spec}(\mathcal{O}_K)$. Since $\mathcal{O}_K$ is complete (hence also henselian), its connected component of identity $\mathcal{E}[p^i]^\circ$ naturally has an induced structure of a group 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 $\operatorname{Spec}(\mathcal{O}_K)$. 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

$$\mathcal{E}[p^i]^{\text{ét}}(K^{\text{alg}}) = \mathcal{E}_k[p^i](k^{\text{alg}}),$$

where k^{alg} is an algebraic closure of the residue field k of K. 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 fiber $\mathcal{E}_k$ 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 the 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

$$T_p(E)^\circ = \varprojlim_{i \geq 1} \mathcal{E}[p^i]^\circ(K^{\text{alg}})$$

and 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

$$1 \to V_p(E)^\circ \to V_p(E) \to V_p(E)^{\text{ét}} \to 1. \tag{2}$$

Because the p-divisible group $\mathcal{E}[p^i]^{\text{ét}}$ is étale over $\operatorname{Spec}(\mathcal{O}_K)$, 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 from Cartier duality together with the self-duality of elliptic curves that there exists a G_K-equivariant isomorphism

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

Therefore, we obtain that in the ordinary case the short exact sequence (2) 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, 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 [M1, Lem. 8.1]).

Lemma 4.1. *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 a connected-to-étale exact sequence is functorial with respect to unramified extensions of henselian local rings, after replacing K by the completion of its maximal unramified extension we may assume that $I_K = G_K$. Let $V_p(E) \to \mathbb{Q}_p$ be any G_K-equivariant homomorphism, coming from a G_K-equivariant 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

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

of p-divisible groups over the field K. Now, by a theorem of Tate (see [T, Thm. 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 $E[p^\infty]_K \to (\mathbb{Q}_p/\mathbb{Z}_p)_K$ of p-divisible groups over the generic fiber $\mathrm{Spec}(K)$ is trivial as well. Then it follows that the map $T_p(E) \to \mathbb{Z}_p$ is also trivial. □

§5. 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, where $X = E \setminus O$ is a hyperbolic curve introduced in Section 1. 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 mentioned in the introduction.

Proposition 5.1. *The 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 characterization. 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 $H_1 H_2$ 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 a 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 [NSW, Thm. 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 [NSW, Prop. 7.5.1]); hence it has no nontrivial closed normal subgroups which are topologically finitely generated. Thus, the group M is trivial, hence $H = \Delta_X$. □

Therefore, from the topological group Π_X we may recover the short exact sequence

$$1 \to \Delta_X \to \Pi_X \to \Pi_X/\Delta_X \to 1,$$

as well as the representation

$$\Pi_X/\Delta_X \curvearrowright \Delta_X^{\mathrm{ab}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

which is isomorphic to the representation $G_K \curvearrowright V_p(E)$. In the rest of the paper we will abuse the notation and simply write $G_K = \Pi_X/\Delta_X$. This will not lead to confusion as long as we use only those properties of the group G_K that are group theoretic, hence preserved by its group of automorphisms (see the discussion in Section 1). Similarly, we will identify the vector space $\Delta_X^{\mathrm{ab}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ with $V_p(E)$.

Proposition 5.2. *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. Recall that there exists a constant $C > 0$ such that for every elliptic curve E over K there exists a finite field extension L/K over which E acquires split semiabelian reduction and, moreover, the degree $[L : K]$ is bounded by C (which does not depend on the elliptic curve E). Indeed, if E has essentially bad reduction then E becomes isomorphic to a Tate curve over a quadratic extension of K (see [Si2, Chap. V, Thm. 5.3]). On the other hand, if E has potentially good reduction then it follows from [SeTa, §2, Cor. 2] that E has good reduction over the field $K(E[m])$, where $m \geq 3$ and m is not divisible by p. This proves the existence of a constant C.

For a natural number $d \geq 1$, it is known that every local field K has only finitely many field extensions L/K inside K^{alg} such that $[L : K] \leq d$. Define F to be the compositum field of all finite field extensions L/K contained in K^{alg} such that $[L : K] \leq C$, where C is the constant introduced in the previous paragraph. Then F/K is a finite extension, hence F is also a local field. By construction, every elliptic curve over K has split semiabelian reduction over F. Moreover, the corresponding open subgroup $G_F \subset G_K$ is clearly group theoretic. Therefore, by restricting to the subgroup G_F we may and do assume that the elliptic curve E has split semiabelian reduction over K.

We claim 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 sequence (2) provides us with such a homomorphism. On the other hand, suppose that E has good reduction and let ϕ be a G_K-equivariant homomorphism $\phi\colon V_p(E) \to \mathbb{Q}_p$. We are going to prove that every such homomorphism is trivial. If the reduction is supersingular then we saw in Lemma 4.1 that the homomorphism ϕ must be trivial. Suppose now that the reduction is ordinary. Then, as we saw in Section 4, 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 nontrivial, 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 5.3. *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 in the proof of Proposition 5.2, 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 one-dimensional representation must be trivial. □

Proposition 5.4. *Assume that 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 a short exact sequence of G_K-modules

$$1 \to W^*(1) \to V_p(E) \to W \to 1, \tag{3}$$

where W is a one-dimensional unramified representation such that $W^{\otimes 2}$ is non-trivial. First, let us observe that this condition is necessary. As we saw in Section 4, if E has good ordinary reduction over K then there exists a short exact sequence of G_K-modules

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

where χ is an unramified character. Moreover, the character χ does not have a finite order, as follows from the argument that we used at the end of the proof of Proposition 5.2. Thus the condition is necessary. We now prove that it is also sufficient. Suppose that we have a sequence of representations as in (3). Since by assumption W and W^* are not isomorphic, we may use Lemma 3.3 to obtain that the p-adic representation $V_p(E)$ is crystalline. Therefore, by Theorem 3.1, this implies that the elliptic curve E has good reduction over K. □

Remark 5.5. The proof of Proposition 5.4 was suggested by the referee; it replaced a less elementary argument which had been given by the author.

Summarizing, by looking at the Tate module of E, we were able to determine group theoretically the potential reduction type of E. Moreover, in the case when the curve E does have potentially good ordinary reduction, we were able to detect whether E has good reduction over K. Therefore, we are reduced to recovering the reduction type of E under the assumption that E has potentially good supersingular reduction. This is in fact the main case of Theorem 1.2 and resolving it will occupy the rest of the paper.

§6. Kummer classes of functions

In this section we briefly recall a construction of anabelian Kummer classes of certain regular functions on a hyperbolic curve. For more details, see [M3, §2].

Let X be a hyperbolic curve over a p-adic local field K with the smooth compactification $\overline{X}$ of positive genus. We write $\mathcal{O}$ for the sheaf of regular functions on X. We assume that all cusps of X, i.e., points on the boundary $\overline{X} \setminus X$, are K-rational. Define

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

which is a $\mathbb{Z}_p$-module of rank one, equipped with a natural isomorphism

$$\alpha_1 \colon M_X \cong \mathbb{Z}_p(1)$$

coming from the Poincaré duality. Then there exists a group-theoretic construction of an exact sequence

$$1 \to H^1(G_K, M_X) \to H^1(\Pi_X, M_X) \to \bigoplus_{x \in \text{cusps}} \mathbb{Z}_p. \tag{4}$$

We briefly recall how this construction proceeds. First, we need to construct group theoretically a certain isomorphism $\varrho \colon M_X \cong I_x$, where I_x is an inertia group of a cusp x. Assuming we have constructed ϱ, consider the inflation exact sequence with coefficients in M_X:

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

Write $I \subset \Delta_X^{\mathrm{ab}}$ for the subgroup generated by inertia groups I_x of cusps; thus we have a surjection $\bigoplus_{x\in\text{cusps}} I_x \twoheadrightarrow I$. Then one computes that

$$H^1(\Delta_X, M_X)^{G_K} = \mathrm{Hom}_{G_K}(\Delta_X^{\mathrm{ab}}, M_X) \hookrightarrow \mathrm{Hom}(I, M_X).$$

Thus, using the surjection $\bigoplus_{x\in\text{cusps}} I_x \twoheadrightarrow I$ together with the isomorphism ϱ we obtain

$$\mathrm{Hom}(I, M_X) \hookrightarrow \mathrm{Hom}\left(\bigoplus_{x\in\text{cusps}} I_x, M_X\right) \cong \bigoplus_{x\in\text{cusps}} \mathbb{Z}_p,$$

hence also the sequence (4). We now recall the construction of the isomorphism ϱ. Let x be a fixed cusp; without loss of generality we may assume that x is K-rational. Let $U = \overline{X} \setminus \{x\}$ be an open subscheme of $\overline{X}$ obtained by removing the point x from $\overline{X}$; thus we have a surjection $\Delta_U \twoheadrightarrow \Delta_{\overline{X}}$. Consider now the maximal centrally cuspidal subquotient

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

i.e., the maximal subquotient Q of $\Delta_U \twoheadrightarrow \Delta_{\overline{X}}$ in which inertia groups I_x are central. Hence we have a central extension

$$1 \to I_x \to Q \to \Delta_{\overline{X}} \to 1.$$

Consider the coboundary map from the inflation exact sequence in group cohomology associated to the above short exact sequence with coefficients in I_x:

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

By definition of M_X, we have canonical isomorphisms

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

Therefore, by composition we obtain a natural and group-theoretic homomorphism

$$\mathrm{Hom}(I_x, I_x) \to \mathrm{Hom}(M_X, I_x).$$

Finally, the desired isomorphism $\varrho\colon M_X \cong I_x$ is constructed as the image of the identity map on I_x.

The exact sequence (4) is closely related to the usual divisor map. More precisely, we have a Kummer map

$$\mathcal{O}(X)^* \to H^1(\Pi_X, M_X),$$

and a commutative diagram

$$\begin{tikzcd}
K^* \arrow[r] \arrow[d] & \mathcal{O}(X)^* \arrow[r, "\mathrm{div}"] \arrow[d] & \bigoplus_{x\in\text{cusps}} \mathbb{Z} \arrow[d, hook] \\
H^1(G_K, M_X) \arrow[r] & H^1(\Pi_X, M_X) \arrow[r] & \bigoplus_{x\in\text{cusps}} \mathbb{Z}_p,
\end{tikzcd}$$

where the map div is the divisor map. Moreover, the kernel of the left vertical map is equal to the subgroup of roots of unity in K^* of order prime to p.

From the topological group G_K one can functorially construct a G_K-module, denoted by $\mathbb{Z}_p(G_K)$, as follows. First, let $(G_K^{\mathrm{ab}})_{\mathrm{tor}}$ be the torsion subgroup of the abelianization G_K^{ab} and consider the colimit

$$\mu(G_K) = \varinjlim_{L/K} (G_L^{\mathrm{ab}})_{\mathrm{tor}},$$

indexed by all finite extensions L/K with transition maps given by the transfer. Finally, write $\mu_n(G_K)$ for the n-torsion subgroup of $\mu(G_K)$ and define

$$\mathbb{Z}_p(G_K) = \varprojlim_{i \in \mathbb{N}} \mu_{p^i}(G_K).$$

From the construction we obtain a natural isomorphism $\alpha_2 \colon \mathbb{Z}_p(1) \cong \mathbb{Z}_p(G_K)$ of G_K-modules induced by the reciprocity map from local class field theory. It is easy to see that the inclusion of any open subgroup $G_L \hookrightarrow G_K$ induces an isomorphism $\mathbb{Z}_p(G_L) \cong \mathbb{Z}_p(G_K)$. Moreover, from the data of the topological group G_K, there exists a group-theoretic construction of a canonical map

$$H^1(G_K, \mathbb{Z}_p(G_K)) \twoheadrightarrow \mathbb{Z}_p \tag{5}$$

which makes the following diagram commutative:

$$\begin{tikzcd}
H^1(G_K, \mathbb{Z}_p(1)) \arrow[d, "\wr"] & \widehat{K^*} \arrow[l, "\simeq"'] \arrow[d, two heads] & K^* \arrow[l] \arrow[d, two heads] \\
H^1(G_K, \mathbb{Z}_p(G_K)) \arrow[r, two heads] & \mathbb{Z}_p & \mathbb{Z}. \arrow[l, hook']
\end{tikzcd}$$

We also note here that the subset $\mathbb{Z} \subset \mathbb{Z}_p$, as well as the element $1 \in \mathbb{Z}_p$ of the quotient (5), have a purely group-theoretic characterization.

Definition 6.1. The isomorphism $\Xi : M_X \cong \mathbb{Z}_p(G_K)$ obtained as a composition $\alpha_2 \circ \alpha_1$ will be called the *rigidity* isomorphism.

The isomorphism Ξ will play an important role in what follows. Observe that it is not clear from the construction if Ξ can be constructed group theoretically since its definition uses the module $\mathbb{Z}_p(1)$, which is not group theoretic. We will see in Section 9 that such a construction exists when the compactification $\overline{X}$ of X is an elliptic curve with potentially good supersingular reduction. Note that the set $\mathrm{Isom}(M_X, \mathbb{Z}_p(G_K))$ of isomorphisms of G_K-modules is naturally a $\mathbb{Z}_p^*$-torsor; hence any isomorphism β in this set is equal to $\lambda\Xi$ for some $\lambda \in \mathbb{Z}_p^*$ (using additive notation).

We define the valuation map

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

where the first map is induced by Ξ and the second map is the canonical surjection (5). Here we use the same notation as for the valuation map $v_K \colon K^* \twoheadrightarrow \mathbb{Z}$; we will see shortly that it does not lead to confusion. We also have the normalized version

$$v \colon H^1(G_K, M_X) \xrightarrow{v_K} \mathbb{Z}_p \xrightarrow{1 \mapsto e(K)^{-1}} \mathbb{Q}_p \tag{6}$$

obtained as a composition of v_K and a map of $\mathbb{Z}_p$-modules $\mathbb{Z}_p \to \mathbb{Q}_p$ sending 1 to the inverse of the absolute ramification degree $e(K)$ of K. The map v does not depend on K, in the sense that it is compatible with restriction to open subgroups $G_L \hookrightarrow G_K$.

Next we come to evaluating functions at points. Let $s\colon G_K \to \Pi_X$ be a section of the surjection $\Pi_X \twoheadrightarrow G_K$ coming from a K-rational point P of the curve X. We define the map

$$\mathrm{val}_{P,K}\colon H^1(\Pi_X, M_X) \xrightarrow{s^*} H^1(G_K, M_X) \xrightarrow{v_K} \mathbb{Z}_p,$$

as well as its normalized version

$$\mathrm{val}_P\colon H^1(\Pi_X, M_X) \xrightarrow{s^*} H^1(G_K, M_X) \xrightarrow{v} \mathbb{Q}_p.$$

Here the map s^* is a restriction morphism determined by the section s. Then we have $v_K(f(P)) = \mathrm{val}_{P,K}(f)$ and $v(f(P)) = \mathrm{val}_P(f)$; in other words the following diagram is commutative:

$$\begin{tikzcd}
\mathcal{O}(X)^* \arrow[r, "f\mapsto v_K(f(P))"] \arrow[d] & \mathbb{Z} \arrow[d] \\
H^1(\Pi_X, M_X) \arrow[r, "\mathrm{val}_{P,K}"] & \mathbb{Z}_p,
\end{tikzcd}$$

which justifies the abuse of notation for v_K and v.

It will be convenient to introduce slightly more general evaluation maps. Let $\beta\colon M_X \cong \mathbb{Z}_p(G_K)$ be an isomorphism of G_K-modules, say $\beta = \lambda\Xi$ for some $\lambda \in \mathbb{Z}_p^*$. We define a map

$$v_{K,\beta}\colon H^1(G_K, M_X) \cong H^1(G_K, \mathbb{Z}_p(G_K)) \twoheadrightarrow \mathbb{Z}_p,$$

where the first isomorphism is induced by β and the second map is again the homomorphism (5). Thus we have an equality $v_{K,\beta} = \lambda v_K$. Similarly, for a section $s\colon G_K \to \Pi_X$ coming from a rational point P we denote

$$\mathrm{val}_{P,\beta}\colon H^1(\Pi_X, M_X) \xrightarrow{s^*} H^1(G_K, M_X) \xrightarrow{v_{K,\beta}} \mathbb{Z}_p,$$

thus we also have $\mathrm{val}_{P,\beta} = \lambda\, \mathrm{val}_{P,K}$. Clearly, the collection of all maps $v_{K,\beta}$ and $\mathrm{val}_{P,\beta}$, where β goes through all G_K-equivariant isomorphisms $M_X \cong \mathbb{Z}_p(G_K)$, is group theoretic.

As we have observed, the construction of the map val_P is not a priori group theoretic since it uses the rigidity isomorphism Ξ, which in turn relies on the scheme-theoretic module $\mathbb{Z}_p(1)$. Moreover, it follows from the above discussion that determining the trivialization Ξ of the torsor $\mathrm{Isom}_{G_K}(M_X, \mathbb{Z}_p(G_K))$ would allow group-theoretic construction of the values $v_K(f(P))$.

§7. Cuspidal sections

In this section we introduce the definition of a discrete section associated to a cusp of a hyperbolic curve and its relation to the integral model of the curve. This notion has already been considered in [M2].

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

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

The group Π acts by conjugation on A and determines a left action $\Pi \to \mathrm{Aut}(A)$ descending to an action $G \to \mathrm{Aut}(A)$. Therefore, the abelian group A is naturally a left G-module. Denote by $\mathrm{Sec}(\Pi, G)$ the set of all sections of the surjection $\Pi \twoheadrightarrow G$. This set has a natural left action of the group A given by conjugation. Let $\mathscr{S}(\Pi, G)$ 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. The following lemma is well known.

Lemma 7.1. *There is a natural bijection of sets $C \simeq \mathscr{S}(\Pi, G)$ given explicitly 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 $s(g) = (a_\pi)^{-1}\pi$, 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 the 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 p and s are homomorphisms 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 $a_\pi = \pi$ for all $\pi \in A$; thus the restriction to A is the identity map. 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 $\alpha^\pi\alpha^{-1} = b_\pi a_\pi^{-1}$, and hence the equality of classes $[a_\pi] = [b_\pi]$.

Now let $[a_\pi]$ be a cohomology class in $H^1(\Pi, A)$ defined by a cocycle $\pi \mapsto a_\pi$ such that its restriction to A is the identity map. 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 we have

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

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

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

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

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

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

Let x be a K-rational cusp of the hyperbolic curve X. We fix a decomposition group $D \subset \Pi_X$ of x and denote 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 canonically isomorphic to $\mathbb{Z}_p(1)$ as a G_K-module. We recall the definition of a cuspidal section.

Definition 7.2. We say that a section s of the surjection $\Pi_X \twoheadrightarrow G_K$ is *cuspidal* at 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 conjugacy classes of cuspidal sections at the cusp x is a torsor over the group $H^1(G_K, I) \cong \widehat{K^*}$. Moreover, by Lemma 7.1, we may identify this torsor with a set of cohomology classes in $H^1(D, I)$ whose restriction to $H^1(I, I)$ is the identity.

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

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

The field K_x is noncanonically isomorphic to the field $K(\!(T)\!)$ of Laurent series with coefficients in K. Let G_x be the absolute Galois group of the field K_x (defined with respect to some algebraic closure K_x^{alg} which we may assume to satisfy $K^{\mathrm{alg}} \subset K_x^{\mathrm{alg}}$). Then we have the induced 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 noncanonically isomorphic as a G_K-module to the group $\widehat{\mathbb{Z}}(1)$. The decomposition 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

$$\begin{tikzcd}
1 \arrow[r] & \Delta_x \arrow[r] \arrow[d, two heads] & G_x \arrow[r] \arrow[d, two heads] & G_K \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & I \arrow[r] & D \arrow[r] & G_K \arrow[r] & 1.
\end{tikzcd}$$

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 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 checks that the field M_t satisfies $\mathrm{Gal}(L_x/M_t) \cong G_K$; hence it defines a cuspidal 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 see that the group U_x is divisible. Thus, for any two uniformizers satisfying $t \equiv t' \bmod \widehat{\mathfrak{m}}_x^2$, we have $M_t = M_{t'}$ for some choice of compatible systems of roots. This implies that 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 $\bar{t} \in \widehat{\mathfrak{m}}_x/\widehat{\mathfrak{m}}_x^2$. We denote by

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

the cotangent space at the point x. For a nonzero vector ω belonging to the (one-dimensional) K-vector space $T_K^\vee$, we define the conjugacy class of cuspidal sections s_ω as a 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

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

Definition 7.3. We say that a cuspidal 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 all sections of the surjection $D \twoheadrightarrow G_K$ is a torsor over the group

$$H^1(G_K, I) \cong H^1(G_K, \mathbb{Z}_p(1)) \cong \widehat{K^*}.$$

Moreover, the set of nonzero differentials $\omega \in T_K^\vee$ is clearly a K^*-torsor. One easily observes that these torsor structures are compatible with the natural map $K^* \to \widehat{K^*}$; in other words, for every $a \in K^*$ and $\omega \in T_K^\vee$ we have $as_\omega = s_{a\omega}$. Indeed, the description of the torsor structure of cuspidal sections is given as follows. Let a be an element of $\widehat{K^*}$ which defines a sequence of elements $a_i \in K^*/(K^*)^{p^i}$ satisfying $a_j = a_i \mod (K^*)^{p^i}$ 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 as_t; hence the compatibility follows. In particular, the set of discrete sections is naturally a $K^{*\mu}$-torsor.

Suppose now that the hyperbolic curve X has stable reduction over K (see [K] for a definition of a stable curve), and denote by $\mathcal{X}$ the stable model of X over $\mathcal{O}_K$. Then the cotangent space $T_K^\vee$, which is of dimension one over K, has a canonical $\mathcal{O}_K$-submodule $T_{\mathcal{O}_K}^\vee$ of rank one determined by the stable model $\mathcal{X}$. Thus, the set of generators of this $\mathcal{O}_K$-submodule is an $\mathcal{O}_K^*$-torsor.

Definition 7.4. Assume that the curve X has stable reduction over K . We say that a cuspidal 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 $\mathcal{O}_K^*$-torsor of generators of the $\mathcal{O}_K$-module $T^\vee_{\mathcal{O}_K}$. Similarly, we say that a uniformizer or a differential is *integral* if the corresponding section is integral.

The set of integral sections is a U_K-torsor whose extension along the group homomorphism $U_K \hookrightarrow K^{*\mu}$ may be identified with the $K^{*\mu}$-torsor of discrete sections.

For a cuspidal section s we may consider its restriction to an open subgroup $G_L \subset G_K$ which determines a cuspidal section s_L at the unique lift of the cusp x to the curve X_L. It is easy to see that if the section s is discrete then its restriction s_L is discrete as well. However, it may happen that a nondiscrete section s becomes discrete after some field extension. On the other hand, we observe that the notion of an integral section is invariant under base change.

Lemma 7.5. *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 an integral section 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 $a \in \widehat{K^*}$, 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 $U_L \cap \widehat{K^*} = U_K$; therefore a belongs to U_K. It implies that s is an integral section. □

In the following we will need to compare the cohomology class associated to a cuspidal section with a certain Kummer class. First, fix a cotangent vector ω in $T^\vee_K$ and let s_ω be a discrete cuspidal section associated to ω. Using the bijection from Lemma 7.1 we obtain a cohomology class α in $H^1(D, I)$ determined by the section s_ω. 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 $\eta_f \in H^1(\Pi_U, \mathbb{Z}_p(1))$ of the function f. Consider now the composition

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

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

Lemma 7.6. *Using notation from the above discussion, the cohomology classes α and β are equal.*

Proof. This follows immediately from the construction. 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 $H^1(D, \mathbb{Z}_p(1))$ is equal to the cohomology class associated to the projective limit of cocycles

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

On the other hand, let s be a cuspidal 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 $\pi = a_\pi s(p(\pi))$. Here, p denotes the projection $p\colon D \twoheadrightarrow G$. Recall that the section s was constructed using a certain quotient of the absolute Galois group of the field $M_t = \bigcup_{i\geq 1} K_x(t^{1/p^i})$ 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

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

Moreover, by the construction of the natural isomorphism $I \cong \mathbb{Z}_p(1)$ 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/p^nI. Therefore, by taking the 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. □

§8. Cohomology classes of standard 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 a p-adic local field K with $p > 2$ and X be the hyperbolic curve $E \setminus \{O\}$. Choose a minimal Weierstrass equation of E over K,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6; \tag{7}$$

thus coefficients a_i belong to the valuation ring $\mathcal{O}_K$. We fix the minimal Weierstrass equation (7) and when we refer to the function x it is always understood to be the chosen coordinate function. It will be useful to introduce the following definition.

Definition 8.1. Let P be a nonzero K-rational point on E. We say that a rational function f on E is a *standard* function associated to P if it has a double pole at the origin O and is regular on X with a zero at P; equivalently f is of the form $f = \lambda(x - x(P))$ for some $\lambda \in K^*$. Moreover, we say that the function f is an *integral* standard function if λ is a p-adic unit.

For a fixed point P the set of standard functions at P is a K^*-torsor; similarly the set of integral standard functions is an $\mathcal{O}_K^*$-torsor. For a finite field extension L/K we may also consider the L^*-torsor of standard functions at P on the curve E_L, and it is clear that a standard function on E remains standard on E_L. Thus we may speak unambiguously of a standard function at P, without mentioning the base field. However, this is not true for integral standard functions since the base change of a minimal Weierstrass model may no longer be minimal over a larger field. On the other hand, if we assume that E has good reduction over K, then we see that integral standard functions remain integral after finite field extension.

For a natural number n we denote by X_n the open subscheme of E obtained by removing all p^n-torsion points and by $K_n = K(E[p^n])$ the field extension obtained by adding coordinates of all p^n-torsion points. We recall that by applying the elliptic cuspidalization (see [M2]), one can reconstruct group theoretically from the topological group Π_X the Δ_X-outer surjection $\Pi_{X_n} \twoheadrightarrow \Pi_X$ corresponding to the open immersion $X_n \hookrightarrow X$ (up to a choice of K-rational cusp of X_n corresponding to the origin of E). Furthermore, by considering automorphisms of the group Π_{X_n} over Π_X, one can also reconstruct a group structure on the set of cusps of X_n corresponding to the group structure of the set of p^n-torsion points of E.

Next, for every finite field extension L/K, we write $\Pi_{X_n,L}$ for the preimage of G_L under the surjection $\Pi_{X_n} \twoheadrightarrow G_K$, i.e., the corresponding fundamental group of the base changed curve $(X_n)_L$. Then, for every finite field extension L/K containing K_n, we may apply Kummer theory to construct group theoretically the exact sequence

$$1 \to H^1(G_L, M_X) \to H^1(\Pi_{X_n,L}, M_X) \to \bigoplus_{x \in \text{cusps}} \mathbb{Z}_p. \tag{8}$$

Here, the set of cusps is equal to the group of p^n-torsion points; we denote the rightmost map by $\alpha \mapsto (\mathrm{ord}(\alpha)_x)_x$. The morphism $\mathrm{ord}(\cdot)_x \colon H^1(\Pi_{X_n}, M_X) \to \mathbb{Z}_p$ at a cusp x is a profinite analogue of the usual notion of the order of zero (or pole) of a rational function. In particular, if α is a cohomology class of a nonzero rational function f on X, then $\mathrm{ord}(f)_x$ is an integer equal to the order of f at x. Moreover, the map $\mathrm{ord}(\cdot)_x$ is compatible with base field extensions. Suppose now that α is a cohomology class in $H^1(\Pi_{X_n,L}, M_X)$ such that $\mathrm{ord}(\alpha)_x$ lies in the submodule $\mathbb{Z} \subset \mathbb{Z}_p$. Then we say that α is regular at x (has pole at x) if $\mathrm{ord}(\alpha)_x$ is nonnegative (negative) with corresponding order equal to the absolute value of $\mathrm{ord}(\alpha)_x$.

For a fixed nonzero p^n-torsion point P, we consider a subset of the group $H^1(\Pi_{X_n,L}, M_X)$ consisting of all classes which have a double pole at the cusp O and single zeros at points P and $-P$. This set is a torsor over the group $H^1(G_L, M_X) \cong \widehat{L^*}$ and contains Kummer classes of standard functions at P. Elements in this set may be written as functions of the form $\lambda(x - x(P))$, where $\lambda \in \widehat{L^*}$. Cohomology classes contained in this $\widehat{L^*}$-torsor will be called *profinite* standard functions (at P). Classes corresponding to the images of standard functions under the Kummer map will also be called *standard* classes; they form an $L^{*\mu}$-torsor. Similarly, when E has stable reduction over L, then classes corresponding to the images of integral standard functions will be called *integral*; they form a U_L-torsor.

Observe that the notion of a profinite standard function is group theoretic. Indeed, since the group structure on the set of cusps (i.e., p^n-torsion points of E) can be reconstructed, for a cusp P it is possible to define the cusp $-P$ group theoretically. Then the torsor of profinite standard functions is obtained from the sequence (8) as the preimage of an appropriate divisor. On the other hand, observe that it is not clear a priori whether the subset of standard classes is group theoretic.

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

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

which is injective. Also, for a finite field extension L/K, the restriction map

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

is injective. With respect to these injections, we introduce the colimit

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

over all natural numbers n and finite extensions L/K. It follows from the construction that the group $S(X)$ contains all Kummer classes of rational functions on $E_{K^{\mathrm{alg}}}$ which are standard at a nonzero p-power torsion point.

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 $a, b \in (K^{\mathrm{alg}})^*$, be two standard functions associated to points P and Q, respectively. We say that f and g are *equivalent* if the element $ab^{-1} \in (K^{\mathrm{alg}})^*$ 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. Moreover, observe that for $P \neq \pm Q$, the functions f and g are equivalent if and only if $f(Q)g(P)^{-1}$ is a torsion element in the group $(K^{\mathrm{alg}})^*$.

We can make a similar construction at the level of cohomology classes. Let L/K be a finite field extension and let $f = a(x - x(P))$ and $g = b(x - x(Q))$, for some $a, b \in \widehat{L^*}$, be two profinite standard functions associated to P and Q. We say that the classes f and g are *equivalent* if the element $ab^{-1} \in \widehat{L^*}$ is torsion. Observe that two standard functions are equivalent if and only if their Kummer classes are equivalent. Indeed, it follows from the fact that for every local field L the kernel of the map $L^* \to \widehat{L^*}$ is contained in the group of roots of unity. The next lemma shows this notion of equivalence is group theoretic.

Lemma 8.2. *From the topological group Π_X we may construct, group theoretically, equivalence classes of profinite standard functions, considered as cohomology classes inside the colimit $S(X)$.*

Proof. Pick any two torsion points P and Q as above and two profinite standard functions $f, g \in S(X)$ associated to these two points. We need to determine whether they are equivalent. We may assume that $P \neq \pm Q$. Fix some finite field extension L such that P and Q become L-rational and a natural number m such that they are both p^m-torsion. By further extending L we may also assume that f and g belong to $H^1(\Pi_{X_m,L}, M_X)$; thus $f = a(x - x(P))$ and $g = b(x - x(Q))$ for some $a, b \in \widehat{L^*}$. Fix two sections s_P, s_Q of the map $\Pi_{X_m,L} \twoheadrightarrow G_L$ corresponding to points P and Q, respectively.

Consider now the evaluation maps

$$H^1(\Pi_{X_m,L}, M_X) \xrightarrow{s_P^*} H^1(G_L, M_X)$$

and

$$H^1(\Pi_{X_m,L}, M_X) \xrightarrow{s_Q^*} H^1(G_L, M_X),$$

obtained by pulling back along sections s_P and s_Q. By evaluating the classes f and g at points Q and P we obtain two elements $s_P^*(g)$ and $s_Q^*(f)$ of the group $H^1(G_L, M_X) \cong \widehat{L^*}$. Then it is enough to observe that f is equivalent to g if and only if the element $s_P^*(g)s_Q^*(f)^{-1}$ is torsion in the group $H^1(G_L, M_X)$. □

§9. Determination of the rigidity isomorphism

In this section (apart from Corollary 9.7) we assume that the elliptic curve E has good supersingular reduction over K. We are going to use the theory developed in Sections 6 and 8 to give a group-theoretic construction of two closely related objects: (1) the rigidity isomorphism Ξ defined in Section 6; (2) various torsors of Kummer classes of integral standard functions at p-power torsion points.

Let $P \in E(K^{\mathrm{alg}})$ be a torsion point of p-power order. Since the p-divisible group associated to the elliptic curve $\mathcal{E}_k$ is connected, it has no nontrivial field-valued points; hence the image of P under the reduction map

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

is trivial. In other words, using equation (7), 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 $v(y(P)) < 0$. Moreover, by comparing absolute values in equation (7), we also obtain $v(x(P)) < 0$; in fact $v(x(P)) = -2h(P)$ and $v(y(P)) = -3h(P)$, where h is the local Néron–Tate height function. Therefore, it follows from the transformation formula for the Weierstrass equation that the value $v(x(P))$ is in fact independent of the choice of a minimal Weierstrass equation.

We are going to use a result from [Si] (originally due to Cassels), which bounds the value $v(x(P))$ from below. The formulation we will need is the following lemma.

Lemma 9.1. *Let $P = (x(P), y(P))$ be a torsion point on the elliptic curve (7) 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 [Si, Chap. VII, Thm. 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 by [Si, Chap. VII, Thm. 3.4] 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.

Corollary 9.2. *Let E be an elliptic curve with good supersingular reduction and let x be a rational function from the minimal Weierstrass equation* (7)*. For each natural number n, let P_n be a torsion point on the elliptic curve E of exact order p^n. Then $v(x(P_n)) < 0$ for all n, and moreover we have*

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

Let us show how Corollary 9.2 may be applied to the problem of constructing the rigidity isomorphism Ξ. Recall that the set of G_K-equivariant isomorphisms $M_X \cong \mathbb{Z}_p(G_K)$ is a $\mathbb{Z}_p^*$-torsor with a canonical trivialization Ξ. Define $\mathbb{Q}_{(p)}^*$ to be the intersection $\mathbb{Q}^* \cap \mathbb{Z}_p^*$, i.e., a subgroup of $\mathbb{Q}^*$ consisting of all rational numbers a/b, where a, b are nonzero, relatively prime and such that ab is not divisible by p. As a first approximation to a group-theoretic construction of Ξ, we construct a reduction of this $\mathbb{Z}_p^*$-torsor to a $\mathbb{Q}_{(p)}^*$-torsor.

Lemma 9.3. *The $\mathbb{Q}_{(p)}^*$-orbit of the rigidity isomorphism Ξ may be reconstructed group theoretically from the topological group Π_X.*

Proof. Let n be a sufficiently large natural number, which we will specify later. Pick a torsion point P_n of exact order p^n and denote by $K_n = K(E[p^n])$ the field extension obtained by adjoining coordinates of all p^n-torsion points. We also choose another nontrivial p^n-torsion point Q such that $Q \neq \pm P_n$ and let $s_Q\colon G_{K_n} \to \Pi_{X_n}$ be a cuspidal section at Q. Finally, choose any G_K-equivariant isomorphism $\beta\colon M_X \cong \mathbb{Z}_p(G_K)$; it induces the valuation map $\mathrm{val}_{Q,\beta}\colon H^1(\Pi_{X_n}, M_X) \to \mathbb{Q}_p$, as constructed in Section 6.

Consider now the set S_n of profinite standard functions f associated to the point P_n which satisfy the equality $\mathrm{val}_{Q,\beta}(f) = 0$ after restriction to G_{K_n}. Recall that the kernel of the valuation map $v_\beta\colon H^1(G_{K_n}, M_X) \to \mathbb{Q}_p$ does not depend on the choice of isomorphism β; thus the set S_n is also independent of the choice of isomorphism β. Moreover, every profinite function f in S_n is in fact standard; more precisely, $f = u(x - x(P_n))$ with some element $u \in L^{*\mu}$ satisfying $v(u) = -v(x(Q) - x(P_n))$. We choose one function from S_n and call it f_n.

We introduce the subset $A_n \subset \mathbb{Q}_p$ consisting of all valuations $\mathrm{val}_{R,\beta}(f_n)$, where R runs through the set of all nontrivial p^n-torsion points different from $\pm P_n$.

Because the function f_n is standard, the set A_n is contained in a one-dimensional $\mathbb{Q}$-vector subspace $\mathbb{Q}\lambda \subset \mathbb{Q}_p$, where $\lambda \in \mathbb{Z}_p^*$ is such that $\beta = \lambda\Xi$. Moreover, it follows from Corollary 9.2 that for n large enough the set A_n is not a singleton; therefore, it generates $\mathbb{Q}\lambda$ as a $\mathbb{Q}$-vector space. Finally we observe that an isomorphism β belongs to the $\mathbb{Q}^*_{(p)}$-orbit of the rigidity isomorphism Ξ if and only if the subspace $\mathbb{Q}\lambda$ is equal to the natural $\mathbb{Q}$-vector subspace $\mathbb{Q} \subset \mathbb{Q}_p$ generated by $1 \in \mathbb{Q}_p$ (which is group theoretic, as we mentioned in Section 6). □

Recall that in Section 8 we also defined (in the case of stable reduction) the torsor of integral standard functions at a nonzero torsion point. Since the elliptic curve E has good reduction, the construction of this torsor is compatible with finite field extensions. The next proposition says this torsor can also be constructed group theoretically. Here the proof relies crucially on Corollary 9.2.

Proposition 9.4. *Assume that the elliptic curve E has good supersingular reduction and fix a nonzero torsion point P of p-power order. Then, for a sufficiently large finite field extension L/K the U_L-torsor of integral standard functions at P can be reconstructed group theoretically from the topological group Π_X and a decomposition group $D_P \subset \Pi_X$ of P, as a subset of the group $S(X)$.*

Proof. Let $\beta\colon M_X \cong \mathbb{Z}_p(G_K)$ be an isomorphism of G_K-modules belonging to a $\mathbb{Q}^*_{(p)}$-orbit of Ξ; by Lemma 9.3 this condition is group theoretic. Thus we have $\beta = \lambda\Xi$ for some $\lambda \in \mathbb{Q}^*_{(p)}$ and the valuation map v_β determined by β satisfies $v_\beta = \lambda v$.

For every nontrivial p-power torsion point R we choose a profinite standard function $f_R \in S(X)$ associated to the point R. Using Lemma 8.2, we may assume that all functions f_R lie in the same equivalence class. Moreover, we may also assume that for every R as above and for every nontrivial p-power torsion point Q satisfying $Q \neq \pm R$, we have that $\mathrm{val}_Q(f_R) \in \mathbb{Q} \subset \mathbb{Q}_p$. Observe that the last condition is group theoretic since it is equivalent to $\mathrm{val}_{Q,\beta}(f_R) \in \mathbb{Q}$ by the choice of β.

Now pick a sequence of p-power torsion points P_i, for $i \geq 1$, such that the point P_i is of exact order p^i; in particular, the exact orders of these points go to infinity as $i \to \infty$. To ease the notation, we write $f_j = f_{P_j}$. Finally, for every pair of distinct natural numbers i, j we consider the absolute value

$$v_{i,j} = \mathrm{val}_{P_i}(f_j) \in \mathbb{Q}.$$

Then, by Lemma 9.3, the double sequence $(v_{i,j})_{i,j}$ of rational numbers can be reconstructed group theoretically up to multiplication by a rational number, since $v_\beta = \lambda v$ for $\lambda \in \mathbb{Q}^*_{(p)}$.

Observe that for a fixed i the sequence $(v_{i,j})_j$ becomes constant for sufficiently large j. Indeed, if we denote $f_j = u_j(x - x(P_j))$, then the valuation $v(u_j)$ does not depend on j since, by construction, the functions f_j are in the same equivalence class. Denote this constant value by $a = v(u_j)$. Thus, from Corollary 9.2 we see that for sufficiently large index j we have

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

Therefore, for a fixed i, the sequence $(v_{i,j})_j$ is eventually constant; we write $v_i = v_{i,j}$ for all $j \gg 0$.

We claim that the sequence v_i of rational numbers converges to zero if and only if every function f_j is an integral standard function associated to the point P_j. Indeed, we have seen that $v_i = a+v(x(P_i))$; thus, again using Corollary 9.2, we obtain that the sequence v_i converges to a. Since $a = v(u_j)$ for every j, the result is clear. Finally, observe that this statement provides a desired group-theoretic characterization since the convergence property $v_i \to 0$ is invariant by multiplication by a nonzero rational number λ. □

Remark 9.5. Observe that in the proof of Proposition 9.4 we also determined the set of absolute values $v(x(P))$ of all nontrivial p-power torsion points up to multiplication by some rational number λ. Indeed, using notation from the proof, when functions f_j are in fact all integral standard functions then we have $v_i = v(x(P_i))$. Therefore, for every two nontrivial p-power torsion points P, Q, the quotient $h(P)/h(Q) = v(x(P))/v(x(Q)) \in \mathbb{Q}$ can be determined group theoretically. Here $h(P)$ is the Néron–Tate local height function of the point P.

We are now going to eliminate the $\mathbb{Q}^*_{(p)}$-indeterminacy in Lemma 9.3, i.e., to give a group-theoretic construction of the rigidity isomorphism Ξ. For this, we first need to recall a few facts concerning the height of p-torsion points of an elliptic curve with a good supersingular reduction. Here we follow [Se, Sects 1.10 and 1.11].

Let E be an elliptic curve over K and assume that it has good supersingular reduction over K. Thus, the p-divisible group $\mathcal{E}[p^\infty]$ determined by E is connected and one-dimensional, and thus determines a formal group law $F(X,Y) \in \mathcal{O}_K[\![X,Y]\!]$, which is a power series of the form

$$F(X,Y) = X + Y + \sum_{i,j\geq 2} c_{i,j}X^iY^j.$$

Let $[p](X)$ be a power series in $\mathcal{O}_K[\![X]\!]$ corresponding to multiplication by p; more precisely, we define recursively $[1](X) = X$ and $[n+1](X) = F([n]X, X)$ for $n \geq 1$.

Then we have

$$[p](X) = \sum_{i \geq 1} a_i X^i$$

for some $a_i \in \mathcal{O}_K$ with $a_1 = p$. Moreover, since we assume that E has supersingular reduction (i.e., the formal group $F(X, Y)$ is of height 2), we have $a_i \in \mathfrak{m}_K$ for all $i < p^2$ and a_{p^2} is a p-adic unit. With the standard coordinates on the xy-plane, we consider the set of points $(i, v_K(a_i))$ for all $1 \leq i \leq p^2$, which determines the (truncated) Newton polygon of the series $[p](X)$. By [Se], it has the shape displayed in Figure 1.

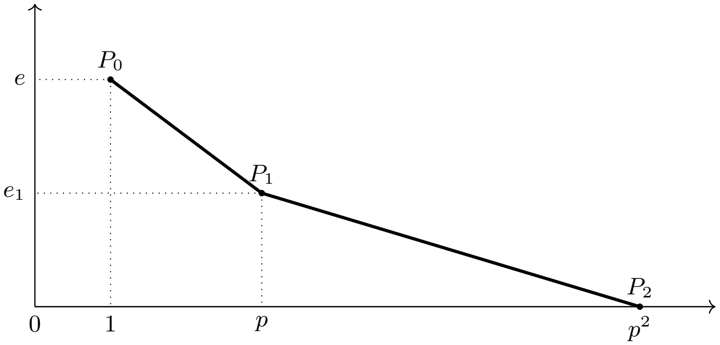

Figure 1.

Here, e is equal to the absolute ramification degree of K. When the point P_1 lies on the line P_0P_2, the Newton polygon consists of only one segment $|P_0P_2|$ with slope $\delta_0 = e/(p^2 - 1)$. Otherwise, it consists of two segments $|P_0P_1|$ and $|P_1P_2|$ with corresponding slopes

$$\delta_1 = \frac{e - e_1}{p - 1} \quad \text{and} \quad \delta_2 = \frac{e_1}{p^2 - p}. \tag{9}$$

It is known that the slopes of the Newton polygon are equal to p-adic valuations of roots of the power series $[p](X)$. Moreover (see [Se, Sect. 1.11, Case (2)]), these valuations are equal to the heights of the corresponding p-torsion points of E.

Corollary 9.6. *The heights of p-torsion points of the elliptic curve E can be determined group theoretically from the topological group Π_X.*

Proof. We saw in Remark 9.5 that the set of quotients $h(P)/h(Q)$, for nontrivial p-torsion points P and Q, can be determined group theoretically. Then we have two cases:

Case 1: For all nontrivial p-torsion points P and Q we have $h(P)/h(Q) = 1$.

This implies that the Newton polygon consists of only one segment. Therefore, its unique slope, as well as the height of every p-torsion point, is equal to $\delta_0 = e/(p^2 - 1)$.

Case 2: There exist two p-torsion points P and Q such that $h(P)/h(Q) \neq 1$.

In this case the Newton polygon consists of two segments and their slopes are given by (9). Thus, the heights of torsion points in $E[p] \setminus \{O\}$ attain exactly two values δ_1 and δ_2. For $i = 1, 2$ we write $A_i \subset E[p] \setminus \{O\}$ for the subset of points with height equal to δ_i. Since the number of roots of the power series $[p](T)$ with valuation δ_i is equal to the length of the projection of an appropriate segment to the OX-axis, we have $\#A_1 = p - 1$ and $\#A_2 = p^2 - p$. Observe that both sets A_1 and A_2 can be defined group theoretically. Indeed, the set A_2 is the unique subset A of the set of nontrivial p-torsion points that are of cardinality $p^2 - p$ and are such that $h(P)/h(Q) = 1$ for all P, Q belonging to A (also observe that $p^2 - p > p - 1$).

Now choose two points Q_1 and Q_2 such that Q_i belongs to A_i for $i = 1, 2$. Then we have

$$h(Q_1)/h(Q_2) = \delta_1/\delta_2 = \frac{p(e - e_1)}{e_1};$$

thus, knowing the quotient $h(Q_1)/h(Q_2)$ we may determine the value of e_1, which in turn determines both values δ_1 and δ_2. □

Then we immediately obtain the following corollary, which applies to the more general case of elliptic curves with potentially good supersingular reduction.

Corollary 9.7. *Assume that the elliptic curve E has potentially good supersingular reduction. Then the rigidity isomorphism Ξ can be constructed group theoretically from the topological group Π_X.*

Proof. Since the rigidity isomorphism is invariant under finite field extensions, we may and do assume that E has good supersingular reduction over K. This can be done group theoretically, as we saw at the beginning of the proof of Proposition 5.2. Next, choose an isomorphism $\beta\colon M_X \cong \mathbb{Z}_p(G_K)$ of G_K-modules belonging to $\mathbb{Q}^*_{(p)}$-orbit of Ξ; this can also be done group theoretically by Lemma 9.3. Thus we have $\beta = \lambda\Xi$ for some $\lambda \in \mathbb{Q}^*_{(p)}$, hence also $v_\beta = \lambda v$. Therefore, we need to find a group-theoretic characterization of the equality $\lambda = 1$.

Using the proof of Proposition 9.4 (see also Remark 9.5), we may construct the set of values $v_\beta(x(P)) = \lambda v(x(P))$ for all p-torsion points P. On the other hand, from Corollary 9.6 we may determine the set of values $v(x(P))$ for all p-torsion points. Clearly, by using Corollary 9.2, these two sets are equal if and only if $\lambda = 1$, which finishes the proof. □

§10. Construction of sections

In this section we assume that the elliptic curve E has potentially good supersingular reduction. We will use Corollary 9.7 to obtain various results concerning construction of torsors of discrete and integral sections.

Lemma 10.1. *Suppose that we are given one discrete section of the surjection $\Pi_X \twoheadrightarrow G_K$. Then the $K^{*\mu}$-torsor of all discrete sections of the surjection $\Pi_X \twoheadrightarrow G_K$ can be constructed group theoretically.*

Proof. Let $s_0 \colon G_K \to \Pi_X$ be the given discrete section. It defines a splitting of the short exact sequence

$$1 \to I \to D \to G_K \to 1. \tag{10}$$

The set of splittings of (10) is a torsor over the group $H^1(G_K, I)$. Recall that we have a natural isomorphism $I \cong M_X$, as well as the rigidity isomorphism $M_X \cong \mathbb{Z}_p(G_K)$. Thus, by applying their composition to cohomology groups, we obtain a map

$$H^1(G_K, I) \cong H^1(G_K, \mathbb{Z}_p(G_K)) \twoheadrightarrow \mathbb{Z}_p \tag{11}$$

which, thanks to Corollary 9.7, can be constructed group theoretically. Therefore, we may define a subgroup $K(G_K, I)^{*\mu}$ of $H^1(G_K, I)$ as a preimage of $\mathbb{Z} \subset \mathbb{Z}_p$ under the map (11). Note that this subgroup corresponds exactly to the subgroup $K^{*\mu}$ of $H^1(G_K, \mathbb{Z}_p(1))$ embedded via the Kummer map through the natural isomorphism $I \cong \mathbb{Z}_p(1)$. Then the orbit of s_0 under the action of the group $K(G_K, I)^{*\mu}$ is equal to the set of all discrete sections. □

In other words, it is enough to construct one discrete section to obtain all of them. We are going to show a group-theoretic construction of a discrete section under the assumption that there exists a nontrivial p-torsion point on E which is K-rational.

Lemma 10.2. *Suppose that there exists a K-rational nontrivial p-torsion point P of E. Fix such a point P. Then the $K^{*\mu}$-torsor of standard functions at the point P can be constructed group theoretically from the topological group Π_X and a decomposition group $D_P \subset \Pi_X$ of P.*

Proof. We already know that the torsor of profinite standard functions, i.e., functions f of the form $f = \lambda(x - x(P))$ for $\lambda \in \widehat{K^*}$, can be constructed group theoretically. Thus we need to find a condition to characterize those functions for which λ belongs to $K^{*\mu}$.

Let Q be a nontrivial p^n-torsion point for n sufficiently large. Since $v(x(P))$ is negative and $v(x(Q)) \to 0$ as $n \to \infty$, we have $v(x(Q) - x(P)) = v(x(P))$. Recall from Section 6 that there are maps $v\colon H^1(G_K, M_X) \twoheadrightarrow \mathbb{Q}_p$ as well as $\mathrm{val}_Q\colon H^1(\Pi_X, M_X) \twoheadrightarrow \mathbb{Q}_p$ which, thanks to Corollary 9.7, are group theoretic. Observe that the map val_Q may also be considered as a map defined on the cohomology group $H^1(\Pi_{X_1}, M_X)$. Thus, by applying it to the function f we obtain

$$\mathrm{val}_Q(f) = v(\lambda) + v(x(Q) - x(P)) = v(\lambda) + v(x(P)).$$

Since $v(x(P))$ belongs to $v(K^*) \subset \mathbb{Q}_p$, we see that $v(\lambda)$ belongs to $v(K^*)$ if and only if $\mathrm{val}_Q(f)$ belongs to $v(K^*)$. As the last condition is group theoretic, it means that we can determine functions f for which $v(\lambda) \in v(K^*)$, which is equivalent to $\lambda \in K^{*\mu}$. □

Proposition 10.3. *Suppose that there exists a K-rational nontrivial p-torsion point P of E. Then the $K^{*\mu}$-torsor of discrete sections at the cusp O may be constructed group theoretically from the topological group Π_X.*

Proof. Recall that we have a surjection $\Pi_{X_1} \twoheadrightarrow \Pi_X$ corresponding to the open immersion $X_1 \hookrightarrow X$, which can be constructed group theoretically. Moreover, choosing an appropriate decomposition group of the cusp O, it is enough to construct the torsor of discrete sections of the surjection $\Pi_{X_1} \twoheadrightarrow G_K$.

Let f be a standard function at the point P, considered as a cohomology class inside the group $H^1(\Pi_{X_1}, M_X)$. Let D_P and I_P be decomposition and inertia groups of P; thus we have a short exact sequence

$$1 \to I_P \to D_P \to G_K \to 1.$$

By applying the restriction map and the natural isomorphism $I_P \cong M_X$, we obtain a map

$$c\colon H^1(\Pi_{X_1}, M_X) \to H^1(D_P, I_P).$$

Consider now the element $c(f) \in H^1(D_P, I_P)$. In the exact sequence

$$1 \to H^1(G_K, I_P) \to H^1(D_P, I_P) \to \mathrm{Hom}(I_P, I_P)$$

the restriction of $c(f)$ to the group $\mathrm{Hom}(I_P, I_P)$ is the identity map; this follows from the fact that f has a simple zero at P. Therefore, by Lemma 7.1 we obtain a section s_P of the surjection $D_P \twoheadrightarrow G_K$. Moreover, by construction the section s_P is in fact a discrete section (at the cusp P).

To obtain a discrete section at the cusp O, we may simply apply the same reasoning as above, switching the roles of points O and P (they are both K-rational). Alternatively, we may choose a geometric automorphism $\rho\colon \Pi_{X_1} \cong \Pi_{X_1}$ which maps a decomposition group of the cusp P onto a decomposition group of O. We briefly describe how to construct such an automorphism ρ. Consider the Galois étale cover $Y \to X$ obtained as a pullback along the immersion $X \hookrightarrow E$ of the multiplication by p map $[p]\colon E \to E$ on the elliptic curve E. Then Π_Y is a normal open subgroup of Π_X and the conjugation action of Π_X on Π_Y determines the Galois group of the cover $Y \to X$. Finally, using the elliptic cuspidalization we transport these geometric automorphisms of Π_Y to geometric automorphisms of Π_{X_1}. Clearly, they act transitively on the set of cusps of X_1; thus we may choose one of them as ρ. Then, since the automorphism ρ comes from a geometric automorphism of X_1, it preserves sets of discrete sections. Therefore, by composing s_P with ρ we obtain a discrete section at the cusp O. □

Lemma 10.4. *Suppose that we are given the set of all discrete sections of the surjection $\Pi_X \twoheadrightarrow G_K$. Then, for every open subgroup $G_L \subset G_K$, corresponding to a finite field extension L/K, we may reconstruct the set of all discrete sections of the surjection $\Pi_{X_L} \twoheadrightarrow G_L$.*

Proof. By Lemma 10.1 it is enough to construct one discrete section of the surjection $\Pi_{X_L} \twoheadrightarrow G_L$. This is easy since the restriction of a discrete section of the surjection $\Pi_X \twoheadrightarrow G_K$ to an open subgroup is also discrete. □

Recall from Section 7 that, when the elliptic curve E has good reduction over K, we have defined a U_K-torsor of integral sections which is compatible with finite field extensions. Moreover, by extending this torsor along the homomorphism $U_K \to K^{*\mu}$ we obtain the $K^{*\mu}$-torsor of discrete sections.

Proposition 10.5. *Assume that E has good supersingular reduction. Suppose that we are given the set of all discrete sections of the surjection $\Pi_X \twoheadrightarrow G_K$. Then we may reconstruct group theoretically the U_K-torsor of integral sections.*

Proof. Observe that by using Lemma 7.5 together with Lemma 10.4 we may pass to a finite field extension and assume that p-torsion points of E are K-rational. Let P be a nontrivial p-torsion point. From Proposition 9.4 we obtain a construction of the U_K-torsor of an integral standard function at P, as a subset of the cohomology group $H^1(\Pi_{X_1}, M_X)$.

Let $\omega \in T^{\vee}_{O,K}$ be an integral cotangent vector at the cusp O. We write $K_O = \mathrm{Frac}(\mathcal{O}_{\overline{X},O})$ for the fraction field of the local ring of $\overline{X}$ at O and F for the completion of the field K_O. Thus $F \cong K((T))$ noncanonically and we have the valuation map $v_F \colon F^* \twoheadrightarrow \mathbb{Z}$; denote by R_O and $\mathfrak{m}_O$ the corresponding discrete valuation ring and its maximal ideal.

Observe that there exists a lift t of ω to the field F such that for every integral standard function f associated to P we have $f^{-1} = rt^2$ (equality in the field F) for some $r \in \mathcal{O}^*_K$. Indeed, recall that integral functions f are of the form $f = u(x - x(P))$, where u belongs to $\mathcal{O}^*_K$. Since our fixed Weierstrass equation is minimal, we know that the function $z = x/y$ determines an integral uniformizer at the cusp O. Moreover, in the field F 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 $s \in 1 + \mathfrak{m}_O$. Hence we may take $t = zs$.

Fix a decomposition group D of the cusp O; hence we have a short exact sequence

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

Consider inverses f^{-1} of the Kummer classes of integral standard functions f associated to the point P. We restrict these classes to the decomposition group D. Denote this set of classes by B; it is a U_K-torsor contained in the cohomology group $H^1(D, M_X)$. Applying the canonical isomorphism $M_X \cong I$ we may treat B as a U_K-torsor contained in the cohomology group $H^1(D, I)$. Thus the torsor B is determined by (local) Kummer classes of functions ut^2, where $u \in \mathcal{O}^*_K$ and t is an integral uniformizer. By assumption, we are given the set of discrete sections of the surjection $\Pi_X \twoheadrightarrow G_K$; thus by applying Lemma 7.1 we obtain a $K^{*\mu}$-torsor of cohomology classes in $H^1(D, I)$ corresponding to discrete sections; let us call these classes discrete as well.

Let A be a subset of $H^1(D, I)$ consisting of all discrete 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 deduce that A is determined by Kummer classes of functions ut for all $u \in U_K$. Here we use the fact that if $x \in \widehat{K^*}$ satisfies $x^2 \in U_K$ then also $x \in U_K$.

By construction, for every $\alpha \in A$, its restriction to $H^1(I, I) = \mathrm{Hom}(I, I)$ is the identity. Therefore, using Lemma 7.1 together with Lemma 7.6, the U_K-torsor A determines the torsor of integral sections. □

§11. Criterion in the supersingular case

In this section we are going to give the proof of Theorem 1.2. Recall that E is an elliptic curve over K and $X = E \setminus \{O\}$.

Proposition 11.1. *Assume that E has potentially good supersingular reduction. Then, from the topological group Π_X equipped with one discrete section, 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 L; we have seen that such an L may be chosen group theoretically. 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 Proposition 10.5, applied to the fundamental group Π_{X_L}, we may reconstruct the U_L-torsor of integral sections s_L of the surjection $D_L \to G_L$. Consider now the diagram

$$\begin{tikzcd} D_L \arrow[r] \arrow[d, hook] & G_L \arrow[l, bend right, "s_L"'] \arrow[d, hook] \\ D_K \arrow[r] & G_K. \arrow[l, bend left, dotted, "s_K"] \end{tikzcd} \tag{12}$$

We are going to prove that the value $v_K(\Delta)$ is divisible by 12 if and only if there exists an integral section s_L which extends to a discrete section $s_K \colon G_K \to D_K$ of the surjection $D_K \twoheadrightarrow G_K$ as in diagram (12). 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 $\mathcal{O}_L^*$-torsor of integral differentials. We have the diagram

$$\begin{tikzcd} S \arrow[r, hook] & T_L^\vee \\ S \cap T_K^\vee \arrow[u, hook] \arrow[r, hook] & T_K^\vee . \arrow[u, hook] \end{tikzcd} \tag{13}$$

We claim that there exists an integral section s_L which extends to a discrete section over G_K as in diagram (12) if and only if the intersection $S \cap T_K^\vee$ is nonempty. Indeed, choose any integral section s_L of the surjection $D_L \twoheadrightarrow G_L$ corresponding to a cotangent vector $\omega_L \in T_L^\vee$. Moreover, choose any discrete 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 $a \in K^{*\mu}$ 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 $a \in K^*$ and $b \in \mathcal{O}_L^*$. This finishes the proof of the claim.

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

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

for some $u \in L^*$ 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 $u^{-1}\omega_L = \omega_K$, 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 $a \in K^*$ and $b \in \mathcal{O}_L^*$. Thus, we obtain $a\omega_K = bu\omega_K$, which implies that $a = bu$; hence, comparing valuations we have $v(a) = v(u)$. Therefore we finally compute that $v(\Delta) = 12v(a)$ 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 $b \in \mathcal{O}_L^*$ 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 paper.

Proof of Theorems 1.1 *and* 1.2. In view of Proposition 10.3 we see that it is enough to prove Theorem 1.2. As we saw in Section 5, 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 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 11.1 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 known that, for an elliptic curve over K with potentially good reduction, we have the 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. □

Acknowledgements

I thank Prof. Shinichi Mochizuki for various conversations concerning the content of this paper and Prof. Akio Tamagawa for his comment on the cyclotomic rigidity isomorphism. I am grateful to Kyoto University for supporting my stay in Kyoto, where I had a chance to interact with various mathematicians at RIMS. The content of this paper is based on Chapter 2 of my PhD thesis; I thank my supervisor Prof. Ivan Fesenko for his help and encouragement.

Moreover, I would like to express my gratitude to the referee for their careful and insightful review of the first version of this paper.

This work was partially supported by the EPSRC Programme Grant "Symmetries and Correspondence" EP/M024830/1.

References

[BK] S. Bloch and K. Kato, L-functions and Tamagawa numbers of motives, in *The Grothendieck Festschrift, Vol. I*, Progress in Mathematics 86, Birkhäuser Boston, Boston, MA, 1990, 333–400. Zbl 0768.14001 MR 1086888

[B] C. Breuil, Groupes p-divisibles, groupes finis et modules filtrés, Ann. of Math. (2) **152** (2000), 489–549. Zbl 1042.14018 MR 1804530

[CI] R. Coleman and A. Iovita, The Frobenius and monodromy operators for curves and abelian varieties, Duke Math. J. **97** (1999), 171–215. Zbl 0962.14030 MR 1682268

[H] Y. Hoshi, On the pro-p absolute anabelian geometry of proper hyperbolic curves, J. Math. Sci. Univ. Tokyo **25** (2018), 1–34. Zbl 1412.14021 MR 3790875

[K] F. F. Knudsen, The projectivity of the moduli space of stable curves. II. The stacks $M_{g,n}$, Math. Scand. **52** (1983), 161–199. Zbl 0544.14020 MR 702953

[M1] S. Mochizuki, The profinite Grothendieck conjecture for closed hyperbolic curves over number fields, J. Math. Sci. Univ. Tokyo **3** (1996), 571–627. Zbl 0889.11020 MR 1432110

[M2] S. Mochizuki, Galois sections in absolute anabelian geometry, Nagoya Math. J. **179** (2005), 17–45. Zbl 1129.14042 MR 2164400

[M3] S. Mochizuki, Absolute anabelian cuspidalizations of proper hyperbolic curves, J. Math. Kyoto Univ. **47** (2007), 451–539. Zbl 1143.14305 MR 2402513

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften 323, Springer, Berlin, 2008. Zbl 1136.11001 MR 2392026

[P] W. Porowski, Anabelian reconstruction of the Néron–Tate local height function, Eur. J. Math. **8** (2022), 1172–1195. Zbl 1497.14051 MR 4498832

[Se] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), 259–331. Zbl 0235.14012 MR 387283

[SeTa] J.-P. Serre and J. Tate, Good reduction of abelian varieties, Ann. of Math. (2) **88** (1968), 492–517. Zbl 0172.46101 MR 236190

[Si2] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151, Springer, New York, 1994. Zbl 0911.14015 MR 1312368

[Si] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics 106, Springer, Dordrecht, 2009. Zbl 1194.11005 MR 2514094

[T] J. T. Tate, p-divisible groups, in *Proc. Conf. Local Fields (Driebergen, 1966)*, Springer, Berlin-New York, 1967, 158–183. Zbl 0157.27601 MR 231827