RIMS-1892

A p-adic Analytic Approach to the Absolute Grothendieck Conjecture

By

Takahiro MUROTANI

August 2018

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

A p-ADIC ANALYTIC APPROACH TO THE ABSOLUTE GROTHENDIECK CONJECTURE

TAKAHIRO MUROTANI

ABSTRACT. Let K be a field, G_K the absolute Galois group of K, X a hyperbolic curve over K, and $\pi_1(X)$ the étale fundamental group of X. The absolute Grothendieck conjecture in anabelian geometry asks: Is it possible to recover X group-theoretically, solely from $\pi_1(X)$ (not $\pi_1(X) \twoheadrightarrow G_K$)?

When K is a p-adic field (i.e. a finite extension of $\mathbb{Q}_p$), this conjecture (called the p-adic absolute Grothendieck conjecture) is unsolved. To approach this problem, we introduce a certain p-adic analytic invariant defined by Serre (which we call i-invariant). Then, the absolute p-adic Grothendieck conjecture can be reduced to the following problems: (A) determining whether a proper hyperbolic curve admits a rational point from the data of i-invariants of the sets of rational points of the curve and its coverings; (B) recovering the i-invariant of the set of rational points of a proper hyperbolic curve group-theoretically. The main results of the present paper give a complete affirmative answer to (A) and a partial affirmative answer to (B).

1. INTRODUCTION

Grothendieck proposed the following conjecture in *Esquisse d'un Programme* and *Brief an G. Faltings* (cf. [14]) :

Conjecture 1.0.1
Let K be a field finitely generated over the prime field. The geometry of an "anabelian" variety V over K is completely determined by the arithmetic fundamental group $\pi_1(V,\, \xi)$ and the surjection $\pi_1(V,\, \xi) \twoheadrightarrow \pi_1(\operatorname{Spec} K,\, \xi)(\simeq \operatorname{Gal}(K^{\mathrm{sep}}/K))$ (where ξ is a geometric point of V and K^{sep} is a separable closure of K).

Although Grothendieck did not give the definition of "anabelian" varieties, he made the following conjecture:

> In the case where V is a connected and nonsingular scheme of dimension 1, V is "anabelian" if and only if its Euler-Poincaré characteristic χ is negative.

More precisely, let Y be the smooth compactification of V, g the genus of Y and n the number of geometric points of $Y \setminus V$. Then we have $\chi = 2 - 2g - n$. So, the above conjecture states that V is "anabelian" if and only if $2g + n - 2 > 0$ (we call such curves *hyperbolic curves*). In the case where K is of characteristic 0, this condition is equivalent to the condition that the geometric fundamental group of V (i.e. the étale fundamental group of $V \times_{\operatorname{Spec} K} \operatorname{Spec} \overline{K}$, where $\overline{K}$ is an algebraic closure of K) is not commutative.

2010 *Mathematics Subject Classification.* Primary 14H30; Secondary 11S20, 14G05, 14G20.

Key words and phrases. anabelian geometry, Grothendieck conjecture, p-adic analytic manifold, rational point.

Conjecture 1.0.1 for hyperbolic curves over K of characteristic 0 was partially resolved affirmatively by Nakamura [10],[11] (for K finitely generated over $\mathbb{Q}$ and $g = 0$) and Tamagawa [18] (for K finitely generated over $\mathbb{Q}$ and $n \neq 0$), and then, Mochizuki [3] gave the following final solution (which is stronger than Grothendieck's original conjecture):

Theorem 1.0.2 (cf. [3, Theorem A], [6, Theorem 1.3.4])
Let p be a prime number, K a sub-p-adic field (i.e. a field which is isomorphic to a subfield of a finitely generated extension of $\mathbb{Q}_p$) and G_K the absolute Galois group of K. Let X and Y be hyperbolic curves over K. Denote by $\pi_1(X)$ (resp. $\pi_1(Y)$) the arithmetic fundamental group of X (resp. Y); by Δ_X (resp. Δ_Y) the geometric fundamental group of X (resp. Y); by $\mathrm{Isom}_K(X, Y)$ the set of K-isomorphisms $X \xrightarrow{\sim} Y$; by $\mathrm{Isom}^{\mathrm{Out}}_{G_K}(\pi_1(X), \pi_1(Y))$ the set of Δ_Y-conjugacy classes of isomorphisms $\pi_1(X) \xrightarrow{\sim} \pi_1(Y)$ which are compatible with the surjections to G_K. Then the natural map

$$\mathrm{Isom}_K(X, Y) \to \mathrm{Isom}^{\mathrm{Out}}_{G_K}(\pi_1(X), \pi_1(Y))$$

is bijective.

In the above problems, we fix a field K and consider group isomorphisms over the absolute Galois group G_K. So, these results may be thought as "relative" results. On the other hand, in [6], Mochizuki proposed "absolute" analogues of these results (i.e. considering similar problems without fixing K and G_K) and proved the following "absolute" Grothendieck conjecture in the case where base fields are algebraic number fields:

Theorem 1.0.3 (cf. [6, Corollary 1.3.5])
Let X (resp. Y) be a hyperbolic curve over an algebraic number field K (resp. L). Denote by $\pi_1(X)$ (resp. $\pi_1(Y)$) the arithmetic fundamental group of X (resp. Y); by $\mathrm{Isom}(X, Y)$ the set of isomorphisms of schemes $X \xrightarrow{\sim} Y$; by $\mathrm{Isom}^{\mathrm{Out}}(\pi_1(X), \pi_1(Y))$ the set of $\pi_1(Y)$-conjugacy classes of isomorphisms of profinite groups $\pi_1(X) \xrightarrow{\sim} \pi_1(Y)$. Then the natural map

$$\mathrm{Isom}(X, Y) \to \mathrm{Isom}^{\mathrm{Out}}(\pi_1(X), \pi_1(Y))$$

is bijective.

In the proof of this theorem, the theorem of Neukirch-Uchida ([12, Theorem 12.2.1]) plays an important role. On the other hand, the analogue of the theorem of Neukirch-Uchida for p-adic fields (i.e. finite extensions of $\mathbb{Q}_p$) fails to hold (there is a counterexample (cf. [12, Chapter VII, §5])). So, the same method is not available. Although some affirmative results were proved (in the cases where the hyperbolic curves are "canonical lifting" (cf. [5]) or "of Belyi type" (cf. [7]), etc.), it is unknown whether or not the "absolute p-adic Grothendieck conjecture" holds in general.

On the other hand, the following theorem reduces the "absolute p-adic Grothendieck conjecture" to the group-theoretic characterization of decomposition groups:

Theorem 1.0.4 (cf. [8, Corollary 2.9], Theorem 4.2.2)
For $i = 1, 2$, let p_i be a prime number, K_i a finite extension of $\mathbb{Q}_{p_i}$, U_i a smooth and geometrically connected hyperbolic curve over K_i, X_i the smooth compactification of U_i, $\widetilde{U}_i$ the universal covering of U_i, $\widetilde{X}_i$ the integral closure of X_i in $\widetilde{U}_i$ and $\widetilde{X}_i^{\mathrm{cl}}$ the set of

closed points of $\widetilde{X_i}$. Suppose that an isomorphism of profinite groups $\alpha : \pi_1(U_1) \xrightarrow{\sim} \pi_1(U_2)$ satisfies the following condition: A closed subgroup of $\pi_1(U_1)$ is the decomposition group of a point of $\widetilde{X_1}^{\mathrm{cl}}$ if and only if the image of the subgroup by α is the decomposition group of a point of $\widetilde{X_2}^{\mathrm{cl}}$. Then $p_1 = p_2$, and α is geometric, i.e. arises from a unique isomorphism of schemes $U_1 \xrightarrow{\sim} U_2$ (more precisely, $\widetilde{U_1} \xrightarrow{\sim} \widetilde{U_2}$).

Moreover, the following theorem reduces the group-theoretic characterization of decomposition groups to the group-theoretic determination of whether or not the sets of rational points of hyperbolic curves are empty (for notations and terms, see Section 4.1):

Theorem 1.0.5 (cf. [18, Corollary 2.10], Theorem 4.2.4)
We follow the notations in Theorem 1.0.4. Let G_{K_i} be the absolute Galois group of K_i. The map $\widetilde{x}_i \mapsto D_{\widetilde{x}_i}$ from $\widetilde{X_i}^{\mathrm{cl}}$ to the set of closed subgroups of $\pi_1(U_i)$ is injective, where $D_{\widetilde{x}_i}$ is the decomposition group of $\widetilde{x}_i$. For each open subgroup $G_i \subset G_{K_i}$, the set of geometric sections $\mathcal{S}(G_i)^{\mathrm{geom}} \subset \mathcal{S}(G_i)$ is characterized by:

$$s_i \in \mathcal{S}(G_i)^{\mathrm{geom}} \Longleftrightarrow (X_i)_{\mathcal{H}_i}(L_i) \neq \emptyset \text{ for all open subgroups } \mathcal{H}_i \subset \pi_1(U_i) \text{ such that } s_i(G_i) \subset \mathcal{H}_i.$$

Here, $L_i = \overline{K_i}^{G_i}$.

Moreover, suppose that the commutative diagram

$$\begin{tikzcd} \pi_1(U_1) \arrow[r, "\sim", "\alpha"'] \arrow[d, "\mathrm{pr}_1"'] & \pi_1(U_2) \arrow[d, "\mathrm{pr}_2"] \\ G_{K_1} \arrow[r, "\sim", "\alpha_K"'] & G_{K_2} \end{tikzcd}$$

satisfies the following condition: For all open subgroups $G_1 \subset G_{K_1}$ and all $s_1 \in \mathcal{S}(G_1)$, we have:

$$s_1 \in \mathcal{S}(G_1)^{\mathrm{geom}} \Longleftrightarrow \alpha \circ s_1 \circ \alpha_K^{-1} \in \mathcal{S}(\alpha_K(G_1))^{\mathrm{geom}}.$$

Then a closed subgroup of $\pi_1(U_1)$ is the decomposition group of a point of $\widetilde{X_1}^{\mathrm{cl}}$ if and only if the image of the closed subgroup by α is the decomposition group of a point of $\widetilde{X_2}^{\mathrm{cl}}$.

The above theorems reduce the absolute p-adic Grothendieck conjecture to the group-theoretic determination of whether or not the sets of rational points of hyperbolic curves and their coverings are empty. Here, we note that for a finite extension K of $\mathbb{Q}_p$ and a proper, smooth and geometrically connected hyperbolic curve X over K, $X(K)$ has a natural structure of compact analytic manifold over K. We shall introduce the "i-invariant" of compact analytic manifold over K (cf. Section 2.1) which was defined by Serre. Roughly speaking, the fact that any compact analytic manifold over K is the disjoint union of a finite number of (closed) balls and the number of balls is well determined modulo $(q-1)$ (where q is the cardinality of the residue field of K) allows us to define the i-invariant of the manifold (over K) as the "number of balls modulo $(q-1)$". Clearly, if the i-invariant of $X(K)$ is not 0, $X(K)$ is not empty. However, the converse is not true in general. So, in some sense, the i-invariant is "weaker" data than the data of whether or not the set of rational points is empty. In other words, we may expect that the group-theoretic "recovery" of the i-invariant is easier than that of the latter data.

In terms of the i-invariants, the absolute p-adic Grothendieck conjecture is reduced to the following two problems:

(A) May the decomposition groups be recovered from the data of i-invariants of the sets of rational points of hyperbolic curves and their coverings?

(B) May the i-invariants of the sets of rational points of hyperbolic curves be recovered group-theoretically from the arithmetic fundamental groups of the curves?

The present paper gives a complete affirmative answer to (A) and a partial affirmative answer to (B).

In the following, for $i = 1, 2$, let p_i be a prime number, K_i a finite extension of $\mathbb{Q}_{p_i}$, q_i the cardinality of the residue field of K_i, G_{K_i} the absolute Galois group of K_i, U_i a smooth and geometrically connected hyperbolic curve over K_i and X_i the smooth compactification of U_i. Denote the arithmetic fundamental group of U_i by $\pi_1(U_i)$ and assume that we are given an isomorphism of profinite groups $\alpha : \pi_1(U_1) \xrightarrow{\sim} \pi_1(U_2)$. Then we have $p_1 = p_2$ and $q_1 = q_2$ (cf. Proposition 4.2.1). Thus, we shall write $p := p_1 = p_2$ and $q := q_1 = q_2$. For each open subgroup $\mathcal{H} \subset \pi_1(U_i)$, let $(U_i)_{\mathcal{H}}$ be the covering of U_i corresponding to $\mathcal{H}$, $(X_i)_{\mathcal{H}}$ the smooth compactification of $(U_i)_{\mathcal{H}}$, $(K_i)_{\mathcal{H}}$ the integral closure of K_i in $(U_i)_{\mathcal{H}}$ and $q_{\mathcal{H}}$ the cardinality of the residue field of $(K_i)_{\mathcal{H}}$. Then $(K_i)_{\mathcal{H}}$ is a finite extension of K_i. The set $(X_i)_{\mathcal{H}}((K_i)_{\mathcal{H}})$ of $(K_i)_{\mathcal{H}}$-rational points of $(X_i)_{\mathcal{H}}$ has a natural structure of compact analytic manifold over $(K_i)_{\mathcal{H}}$. Denote the i-invariant of this manifold over $(K_i)_{\mathcal{H}}$ by $i_{(K_i)_{\mathcal{H}}}((X_i)_{\mathcal{H}}((K_i)_{\mathcal{H}}))$.

The following is the first main theorem of the present paper, which shows together with Theorem 1.0.5 that the data of whether or not the sets of rational points of hyperbolic curves are empty may be recovered from the data of i-invariants of the sets of rational points of the hyperbolic curves and their coverings:

Theorem 1.0.6 (cf. Theorem 4.2.8)
Suppose that there exist an open subgroup $\mathcal{H}_0 \subset \pi_1(U_1)$ and a divisor $m > 1$ of $q_{\mathcal{H}_0} - 1$ such that:

$$i_{(K_1)_{\mathcal{H}}}((X_1)_{\mathcal{H}}((K_1)_{\mathcal{H}})) \equiv i_{(K_2)_{\alpha(\mathcal{H})}}((X_2)_{\alpha(\mathcal{H})}((K_2)_{\alpha(\mathcal{H})})) \mod m,$$

for all open subgroups $\mathcal{H}$ of $\pi_1(U_1)$ satisfying $\mathcal{H} \subset \mathcal{H}_0$. Then, for all open subgroups $G_1 \subset G_{K_1}$ and all $s_1 \in \mathcal{S}(G_1)$, we have

$$s_1 \in \mathcal{S}(G_1)^{\mathrm{geom}} \Longleftrightarrow \alpha \circ s_1 \circ \alpha_K^{-1} \in \mathcal{S}(\alpha_K(G_1))^{\mathrm{geom}}.$$

The following is the second main theorem of the present paper, which shows that the i-invariants (mod 2) of the sets of rational points of hyperbolic curves are group-theoretic in a certain situation:

Theorem 1.0.7 (cf. Theorem 4.3.3)
Suppose that p is odd. Moreover, for $i = 1, 2$, assume that X_i is of genus $g_i \geq 2$ and that X_i has log smooth reduction. Then we have

$$i_{K_1}(X_1(K_1)) \equiv i_{K_2}(X_2(K_2)) \mod 2.$$

For the definition of log smooth reduction, see Section 3.1.

Remark 1.0.8
If we prove Theorem 1.0.7 without assuming that X_i has log smooth reduction, we get the affirmative answer to (B) for p odd. Then, together with Theorem 1.0.6 (which affirms (A)), we can prove the absolute p-adic Grothendieck conjecture for p odd.

We shall review the contents of the present paper. In Chapter 2, we treat problem (A). First, we review the definition of analytic manifolds and i-invariants. Then, embedding a proper, smooth and geometrically connected hyperbolic curve X over a finite extension K of $\mathbb{Q}_p$ into the Jacobian J, we make some p-adic analytic and algebro-geometric observations. These observations imply that $X(K)$ is not empty if and only if there exists a finite étale covering X' of X such that the i-invariant of set of K-rational points of X' over K is not 0. In Chapter 3, we treat problem (B). First, we review the definitions of models and reductions of curves. There exists a finite Galois extension L/K such that $X \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L$ has a unique stable model $\mathfrak{X}$ by the Deligne-Mumford theorem (Theorem 3.1.11). $X(K)$ is characterized as the Galois-invariant subset of $X(L)$. From this point of view, we investigate the i-invariant of $X(K)$. We describe explicitly the Galois action on the inverse image by the reduction map of a rational point of the special fiber of $\mathfrak{X}$, and then, calculate the i-invariant of the Galois-invariant subset of the inverse image of each rational point of the special fiber. In Chapter 4, applying the arguments in Chapter 2 and Chapter 3, we prove the main theorems. In Appendix A, we treat an analogue over $\mathbb{R}$ of the i-invariant and the criterion for existence of rational points of hyperbolic curves given in Chapter 2.

Acknowledgement

I would like to express my deepest gratitude to Professor Akio Tamagawa for his helpful advices and warm encouragement.

2. i-invariants and rational points

Let p be a prime number, K a finite extension of $\mathbb{Q}_p$, X a proper, smooth and geometrically connected hyperbolic curve over K. Then, $X(K)$ has a natural structure of compact analytic manifold over K, where $X(K)$ denotes the set of K-rational points of X. In this chapter, we prove that one may recover whether $X(K)$ is empty or not from the i-invariants of the sets of K-rational points of X and its coverings.

2.1. The definition and properties of i-invariants.

In this section, we will review the definition of analytic manifolds and i-invariants according to [16]. Let K be a field complete with respect to a non-trivial absolute value, X a topological space. In the following sections, we consider the case in which K is a finite extension of $\mathbb{Q}_p$ and X is the set $X(K)$ of K-rational points of a proper, smooth and geometrically connected hyperbolic curve X.

Definition 2.1.1
Let $x = (x_1, \cdots, x_n) \in K^n$ and $r = (r_1, \cdots, r_n) \in \mathbb{R}^n$ $(r_i > 0,\ 1 \leq i \leq n)$. We set

$$P(r)(x) := \{y = (y_1, \cdots, y_n) \in K^n \mid |y_i - x_i| \leq r_i \ (1 \leq i \leq n)\},$$

and $P(r) := P(r)(0)$.

Definition 2.1.2 (cf. [16, Part II, Chapter II])
Let $f = \sum_i a_i X_1^{m_{i,1}} \cdots X_n^{m_{i,n}} \in K[[X_1, \cdots, X_n]]$ be a formal power series and $r = (r_1, \cdots, r_n) \in \mathbb{R}^n$ $(r_i > 0,\ 1 \leq i \leq n)$. The series f is said to be *convergent on* $P(r)$ if

$$\sum_i |a_i| r_1^{m_{i,1}} \cdots r_n^{m_{i,n}} < \infty.$$

The series f is said to be *convergent* if it is convergent on $P(r)$ for some $r = (r_1, \cdots, r_n) \in \mathbb{R}^n$ $(r_i > 0,\ 1 \leq i \leq n)$.

Definition 2.1.3 (cf. [16, Part II, Chapter II])
Let $U \subset K^n$ be an open subset and $\phi : U \to K$ a function. Then ϕ is said to be *analytic* in U if for each $x \in U$ there is a formal power series f and a radius $r = (r_1, \cdots, r_n) \in \mathbb{R}^n$ $(r_i > 0,\ 1 \leq i \leq n)$ such that:

(1) $P(r)(x) \subset U$.
(2) f converges in $P(r)$ and, for $h \in P(r)$, $\phi(x + h) = f(h)$.

Definition 2.1.4 (cf. [16, Part II, Chapter II])
Let $U \subset K^n$ be an open subset and $\phi = (\phi_1, \cdots, \phi_m) : U \to K^m$ a function. Then ϕ is said to be *analytic* if ϕ_i is analytic for $1 \leq i \leq m$.

Definition 2.1.5 (cf. [16, Part II, Chapter III, 1])
A *chart* c on X is a triple $c = (U, \phi, n)$ such that:

(1) $U \subset X$ is an open subset.
(2) $n \in \mathbb{Z}_{\geq 0}$.
(3) $\phi : U \to K^n$ is an open map and induces a homeomorphism $U \overset{\sim}{\to} \phi(U)$.

We call $O(c) := U$ the open set of c, ϕ the map of c, and n the dimension of c.

Definition 2.1.6 (cf. [16, Part II, Chapter III, 1])
Let $c = (U, \phi, n)$ and $c' = (U', \phi', n')$ be charts on X. Then c and c' are said to be *compatible* if, setting $V = U \cap U'$, the maps $\phi' \circ \phi^{-1}|_{\phi(V)}$ and $\phi \circ \phi'^{-1}|_{\phi'(V)}$ are analytic.

Definition 2.1.7 (cf. [16, Part II, Chapter III, 1])
A family $\{c_i\}_{i \in I}$ of charts on X is said to *cover* X if $\bigcup_{i \in I} O(c_i) = X$.

Definition 2.1.8 (cf. [16, Part II, Chapter III, 1])
An *atlas* A on X is a family of charts on X which covers X and such that the charts in the family are mutually compatible.

Definition 2.1.9 (cf. [16, Part II, Chapter III, 1])
Two atlases A and A' are said to be *compatible* if one of the following equivalent conditions holds:

(1) $A \cup A'$ is an atlas on X.
(2) If $c \in A$ and $c' \in A'$, then c and c' are compatible.

Remark 2.1.10 (cf. [16, Part II, Chapter III, 1])
Compatibility of atlases is an equivalence relation.

Definition 2.1.11 (cf. [16, Part II, Chapter III, 2])
An atlas A on X is *full* if whenever c is a chart on X such that c is compatible with all charts $c' \in A$ then $c \in A$. Then it is clear that each equivalence class of atlases on X contains exactly one full atlas.

Definition 2.1.12 (cf. [16, Part II, Chapter III, 2])
An *analytic manifold (over K)* is a topological space equipped with a full atlas on it.

Definition 2.1.13 (cf. [16, Part II, Chapter III, 2])
Let X be an analytic manifold. For $x \in X$, $\dim_x X$ is defined as the dimension of any chart c on X such that $x \in O(c)$; it is called the *dimension of X at x*. The function $x \mapsto \dim_x X$ is locally constant on X; if it is constant, and equal to n, one says that X is everywhere of dimension n.

Definition 2.1.14 (cf. [16, Part II, Chapter III, 3])
Let $n \in \mathbb{Z}_{\geq 0}$, $x = (x_1, \cdots, x_n) \in K^n$ and $r \in \mathbb{R}_{>0}$. Then, the *(closed) ball $B(r)(x)$ of radius r centered at x* is defined as follows:

$$B(r)(x) := \{y = (y_1, \cdots, y_n) \in K^n \mid |y_i - x_i| \leq r, \ (1 \leq i \leq n)\}.$$

Remark 2.1.15
It is clear that $B(r)(x) = P(r, \cdots, r)(x)$ by definition.

Remark 2.1.16 (cf. [16, Part II, Chapter III, Appendix 2, Remark])
If K is ultrametric, all points of a ball B in K^n is the center of B. Moreover, if B_i are balls of radius r_i for $i = 1, 2$ and $r_1 \leq r_2$, then either $B_1 \cap B_2 = \emptyset$ or $B_1 \subset B_2$.

Definition 2.1.17 (cf. [16, Part II, Chapter III, 3])
Let X be an analytic manifold and B a subset of X. Then B is said to be a *ball* if there is a chart $c = (U, \phi, n)$ such that $B \subset U$ and $\phi(B)$ is a ball in K^n.

Definition 2.1.18 (cf. [16, Part II, Chapter III, 11])
Let X be an analytic manifold over K and Y a topological subspace of X (with the induced topology). Let $\iota : Y \to X$ be the inclusion map. Then Y is said to be an *analytic submanifold of X* if for all $y \in Y$, there exist an open neighborhood V of y in Y, a chart $c = (U, \phi, n)$ on X, and a linear subspace E of K^n such that $\iota(V) \subset U$ and $\phi(\iota(V)) = E \cap \phi(U)$. In this case, an analytic manifold structure is naturally induced on Y.

Until the end of this section, we assume moreover that K is locally compact and ultrametric, and let X be an analytic manifold everywhere of dimension $n (\in \mathbb{Z}_{\geq 0})$. We assume that X is non-empty and Hausdorff as a topological space.

Remark 2.1.19
For a topological field K, the following are equivalent:

(1) K satisfies the above conditions.
(2) K is a complete discrete valuation field and the residue field is finite.
(3) K is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$.

Until the end of this section, we denote the cardinality of the residue field of K by q.

Theorem 2.1.20 (cf. [16, Part II, Chapter III, Appendix 2, Theorem 2])
Suppose that X is non-empty and compact. Then:

(1) *X is the disjoint union of a finite number of balls.*
(2) *The number of balls in a decomposition of X into a disjoint union of a finite number of balls is well determined* $\mod (q-1)$.

Definition 2.1.21
Let X be a non-empty and compact analytic manifold over K. We call the number of balls $i_K(X) \in \mathbb{Z}/(q-1)\mathbb{Z}$ in Theorem 2.1.20 the *i-invariant of X over K*. Moreover, we set $i_K(\emptyset) \equiv 0 \mod (q-1)$.

Remark 2.1.22 (cf. [16, Part II, Chapter III, Appendix 2, Theorem 2])
If X is a non-empty compact analytic manifold over K, the isomorphism class of X is determined by $i_K(X) \in \mathbb{Z}/(q-1)\mathbb{Z}$.

Remark 2.1.23
Let L be an extension of K of finite degree $d\,(\in \mathbb{Z}_{>0})$ and q_L the cardinality of the residue field of L. Then, a ball of dimension n over L is isomorphic to a ball of dimension nd over K as an analytic manifold over K. Let Y be a compact analytic manifold over L, $i_L(Y) \in \mathbb{Z}/(q_L-1)\mathbb{Z}$ the i-invariant of Y over L and $i_K(Y) \in \mathbb{Z}/(q-1)\mathbb{Z}$ the i-invariant of Y over K as an analytic manifold over K. Then, from the above observation, it is clear that

$$i_L(Y) \equiv i_K(Y) \mod (q-1).$$

We will give some examples of computations of i-invariants. Until the end of this section, let $\mathcal{O}_K$ be the ring of integers of K, $\mathfrak{M}_K$ the maximal ideal of $\mathcal{O}_K$, π a uniformizer of $\mathcal{O}_K$ and $k = \mathcal{O}_K/\mathfrak{M}_K$ the residue field of $\mathcal{O}_K$. (Thus, q is the cardinality of k.) Let v be the valuation of K such that $v(K^\times) = \mathbb{Z}$.

Example 2.1.24
We consider $\mathfrak{M}_K^m = \pi^m \mathcal{O}_K\,(m \in \mathbb{Z}_{\geq 0})$ as a metric space with respect to the distance given by v. Then, by taking the inclusion map $\mathfrak{M}_K^m \hookrightarrow K$ as a chart, we may consider $\mathfrak{M}_K^m$ as a compact analytic manifold over K, and $i_K(\mathfrak{M}_K^m) \equiv 1 \mod (q-1)$.

Similarly, we may consider $\mathfrak{M}_K^m \setminus \mathfrak{M}_K^{m+1}$ as a compact analytic manifold over K, and $i_K(\mathfrak{M}_K^m \setminus \mathfrak{M}_K^{m+1}) \equiv q-1 \equiv 0 \mod (q-1)$.

Example 2.1.25
Let $\mathbb{P}_K^n$ be a projective space of dimension $n\,(\geq 0)$ over K and $\mathbb{P}_K^n(K)$ the set of K-rational points of $\mathbb{P}_K^n$. We may consider $\mathbb{P}_K^n(K)$ as a compact analytic manifold (everywhere) of dimension n over K. Let $[a_0, a_1, \cdots, a_n]$ be the coordinates of $P \in \mathbb{P}_K^n(K)$, where $a_0, \cdots, a_n$ are elements of K and not all zero. By multiplying a constant if necessary, we may assume that $a_i \in \mathcal{O}_K$ $(0 \leq i \leq n)$ and $\min_{0 \leq i \leq n} v(a_i) = 0$. Such representation is unique up to multiplication by units of $\mathcal{O}_K$.

Let $\mathbb{P}_k^n$ be a projective space of dimension n over k and $\mathbb{P}_k^n(k)$ the set of k-rational points of $\mathbb{P}_k^n$. We denote the image of $a \in \mathcal{O}_K$ in k by $\overline{a}$. Then,

$$[\overline{a_0}, \overline{a_1}, \cdots, \overline{a_n}] \in \mathbb{P}_k^n(k).$$

This defines a map $\mathbb{P}^n_K(K) \to \mathbb{P}^n_k(k)$ and the inverse image of each point of $\mathbb{P}^n_k(k)$ is a ball of dimension n over K.

The cardinality of $\mathbb{P}^n_k(k)$ is $\dfrac{q^{n+1}-1}{q-1}$, and

$$\frac{q^{n+1}-1}{q-1} = \sum_{j=0}^{n} q^j \equiv n+1 \mod (q-1).$$

Therefore, $i_K(\mathbb{P}^n_K(K)) \equiv n+1 \mod (q-1)$.

Here is a key proposition which will be used in the following sections:

Proposition 2.1.26 (cf. [15, §3, Théorème 9, Proposition 11]) *Let $Y \subset \mathcal{O}_K^N$ be a closed analytic submanifold everywhere of dimension d over K.*

(i) *For all $y = (y_1, \cdots, y_N) \in \mathcal{O}_K^N$, $Y \cap (y + (\pi^m \mathcal{O}_K)^N)$ is either empty or a subset of $\mathcal{O}_K^N$ written in the following form for sufficiently large m:*

$$y + \pi^m Y'_y = \{(y_1 + \pi^m y'_1, \cdots, y_N + \pi^m y'_N) \in \mathcal{O}_K^N \mid (y'_1, \cdots, y'_N) \in Y'_y\},$$

where Y'_y is a set written in the following form for some permutation $\sigma \in \mathfrak{S}_N$:

$$\{(x_{\sigma(1)}, \cdots, x_{\sigma(N)}) \in \mathcal{O}_K^N \mid x_1, \cdots, x_d \in \mathcal{O}_K,\, x_j = \varphi_j(x_1, \cdots, x_d)\ (d+1 \le j \le N)\}.$$

(Here, $\varphi_{d+1}(x_1, \cdots, x_d), \cdots, \varphi_N(x_1, \cdots, x_d) \in \mathcal{O}_K[[x_1, \cdots, x_d]]$ are power series which converge on $\mathcal{O}_K^d$.) In particular, for sufficiently large m, $Y \cap (y + (\pi^m \mathcal{O}_K)^N)$ is either empty or isomorphic to a ball of dimension d over K. Moreover, given $n_0 \in \mathbb{Z}_{\ge 0}$, by taking larger m if necessary, one may take the above $\varphi_{d+1}, \cdots, \varphi_N$ so that the coefficients of terms of degree greater than 1 of φ_j $(d+1 \le j \le N)$ belong to $\pi^{n_0}\mathcal{O}_K$.

(ii) *For $y \in \mathcal{O}_K^N$ and $m \in \mathbb{Z}$, we assume that $Y \cap (y + (\pi^m \mathcal{O}_K)^N)$ is not empty and written as $y + \pi^m Y'_y$ as in (i). For all $m' \ge m$, let*

$$(\pi^m \mathcal{O}_K)^N = \coprod_{j=1}^{M} (\pi^m z^{(j)} + (\pi^{m'} \mathcal{O}_K)^N)$$

be the coset decomposition ($M\,(= q^{(m'-m)N}) \in \mathbb{Z}_{>0}$, $z^{(j)} \in \mathcal{O}_K^N$, $1 \le j \le M$). Then, for each $1 \le j \le M$, $Y \cap (y + \pi^m z^{(j)} + (\pi^{m'}\mathcal{O}_K)^N)$ is either empty or written as $y + \pi^m z^{(j)} + \pi^{m'} Y'_{z^{(j)}}$ ($Y'_{z^{(j)}}$ is a set written in a form similar to Y'_y in (i)).

(iii) *There exists $m_0 \in \mathbb{Z}$ such that for all $m \ge m_0$, Y is written as a finite disjoint union of subsets each of which is written as $y + \pi^m Y'_y$. Moreover, the number of such subsets is well determined* $\mod (q-1)$.

Proof.

Step 1.

If $y \notin Y$, it is clear that $Y \cap (y + (\pi^m \mathcal{O}_K)^N) = \emptyset$ for sufficiently large m, so we may assume that $y \in Y$. Moreover, by translating if necessary, we may assume that $y = (0, \cdots, 0)$ without loss of generality.

Let $V = T_y \mathcal{O}_K^N = K^N$ (resp. $W = T_y Y \subset V$) be the tangent space of $\mathcal{O}_K^N$ (resp. Y) at y. V is a vector space of dimension N over K and W is a d-dimensional subspace. Take a canonical basis $\{e_1, \cdots, e_N\}$ of $V = K^N$ and let $\overline{e_i}\,(1 \leq i \leq N)$ be the images of e_i in V/W. By permuting e_i's if necessary, we may assume that $\{\overline{e_{d+1}}, \cdots, \cdots, \overline{e_N}\}$ is a basis of V/W. Then, there exist $a_{i,j} \in K\,(1 \leq i \leq d,\ d+1 \leq j \leq N)$ such that

$$\overline{e_i} = \sum_{j=d+1}^{N} a_{i,j}\overline{e_j}, \tag{2.1}$$

for each $1 \leq i \leq d$. We will show that one may take a permutation of e_i's so that the coefficients $a_{i,j}$ $(1 \leq i \leq d,\ d+1 \leq j \leq N)$ belong to $\mathcal{O}_K$.

Let us call the formula in (2.1) associated to each $1 \leq i \leq d$, *the i-th formula*. First, we claim that one may permute e_i's so that the coefficients in the first formula belong to $\mathcal{O}_K$. If $a_{1,j} \in \mathcal{O}_K$ $(d+1 \leq j \leq N)$, the claim is trivial. Otherwise, by permuting $e_{d+1}, \cdots, e_N$ suitably, we may assume that $\min_{d+1 \leq j \leq N} v(a_{1,j}) = v(a_{1,d+1}) < 0$. Then,

$$\overline{e_{d+1}} = -a_{1,d+1}^{-1}\overline{e_1} + \sum_{j=d+2}^{N} a_{1,d+1}^{-1}a_{1,j}\overline{e_j},$$

and the coefficients in the right-hand side belong to $\mathcal{O}_K$. By substituting this into the i-th formula for $2 \leq i \leq d$ and switching $\overline{e_1}$ and $\overline{e_{d+1}}$, we obtain formulae similar to (2.1) where the coefficients in the first formula belong to $\mathcal{O}_K$.

Next, for $1 \leq i_0 < d$, we assume that all the coefficients in the i-th formula for $1 \leq i \leq i_0$ belong to $\mathcal{O}_K$. We claim that one may permute e_i's so that all the coefficients in the i-th formula for $1 \leq i \leq i_0+1$ belong to $\mathcal{O}_K$. If $a_{i_0+1,j} \in \mathcal{O}_K$ $(d+1 \leq j \leq N)$, the claim is trivial. Otherwise, by permuting $e_{d+1}, \cdots, e_N$ suitably, we may assume that $\min_{d+1 \leq j \leq N} v(a_{i_0+1,j}) = v(a_{i_0+1,d+1}) < 0$. Then,

$$\overline{e_{d+1}} = -a_{i_0+1,d+1}^{-1}\overline{e_{i_0+1}} + \sum_{j=d+2}^{N} a_{i_0+1,d+1}^{-1}a_{i_0+1,j}\overline{e_j}$$

and the coefficients in the right-hand side belong to $\mathcal{O}_K$. Substitute this into the i-th formula for $i \neq i_0+1$ and switch $\overline{e_{i_0+1}}$ and $\overline{e_{d+1}}$. Since all the coefficients in the i-th formula for $1 \leq i \leq i_0$ belong to $\mathcal{O}_K$ by assumption, they remain to belong to $\mathcal{O}_K$ after the substitution. So, we obtain formulae similar to (2.1) where all the coefficients in the i-th formula for $1 \leq i \leq i_0+1$ belong to $\mathcal{O}_K$.

By induction, we may assume that each $a_{i,j}$ in (2.1) belongs to $\mathcal{O}_K$ after permuting e_i's suitably.

For each $1 \leq i \leq d$, set:

$$e'_i = e_i - \sum_{j=d+1}^{N} a_{i,j}e_j.$$

Then, $e'_i \in W$. Clearly, these are linearly independent over K, so $\{e'_1, \cdots, e'_d\}$ is a basis of W. Each element in W can be written in the following form for some $x'_i \in K\,(1 \leq i \leq d)$:

$$\sum_{i=1}^{d} x'_i e'_i = \sum_{i=1}^{d} x'_i e_i - \sum_{j=d+1}^{N}\sum_{i=1}^{d} a_{i,j}x'_i e_j.$$

Therefore, for $x_i \in K\,(1 \leq i \leq N)$,

$$\sum_{i=1}^{N} x_i e_i \in W \Longleftrightarrow x_j = -\sum_{i=1}^{d} a_{i,j} x_i \ (d+1 \leq j \leq N).$$

Thus, the tangent space of Y at $y = (0, \cdots, 0)$ is determined by:

$$x_j = -\sum_{i=1}^{d} a_{i,j} x_i \ (d+1 \leq j \leq N).$$

Step 2.

By the observation in Step 1, we may permute the order of coordinates so that the tangent space of Y at $y = (0, \cdots, 0)$ is written in the following form for some $a_{i,j} \in \mathcal{O}_K\,(1 \leq i \leq d,\ d+1 \leq j \leq N)$:

$$x_j = \sum_{i=1}^{d} a_{i,j} x_i \ (d+1 \leq j \leq N).$$

(Replace $-a_{i,j}$ in Step 1 by $a_{i,j}$.) Therefore, there exist power series $\psi_j(x_1, \cdots, x_d) \in K[[x_1, \cdots, x_d]]$ $(d+1 \leq j \leq N)$ which consist of terms of degree greater than 1 and converge on some neighborhood (which does not necessarily contain $\mathcal{O}_K^d$) such that Y is determined by the following family of equations in some neighborhood of $y = (0, \cdots, 0)$:

$$x_j = \sum_{i=1}^{d} a_{i,j} x_i + \psi_j(x_1, \cdots, x_d) \ (d+1 \leq j \leq N).$$

We may take sufficiently large $m \in \mathbb{Z}$ so that by putting $x_i = \pi^m z_i\ (1 \leq i \leq N)$, $\pi^{-m}\psi_j(\pi^m z_1, \cdots, \pi^m z_d) \in K[[z_1, \cdots, z_d]]$ converges on $\mathcal{O}_K^d$ and belongs to $\mathcal{O}_K[[z_1, \cdots, z_d]]$ for all $d+1 \leq j \leq N$. Denote these power series by $\psi_{j,m}(z_1, \cdots, z_d)$. For each $d+1 \leq j \leq N$, set $\varphi_j(z_1, \cdots, z_d) = \sum_{i=1}^{d} a_{i,j} z_i + \psi_{j,m}(z_1, \cdots, z_d)$. Then,

$$Y \cap (\pi^m \mathcal{O}_K)^N = \{(\pi^m z_1, \cdots, \pi^m z_N) \in \mathcal{O}_K^N \,|\, z_i \in \mathcal{O}_K\,(1 \leq i \leq d),\ z_j = \varphi_j(z_1, \cdots, z_d)\ (d+1 \leq j \leq N)\}.$$

Thus, the first assertion of (i) follows. The second assertion of (i) follows immediately from the first. The third assertion of (i) is immediate from the definition of $\varphi_j(x_1, \cdots, x_d)$. This completes the proof of (i).

Step 3.

Assume that for $y \in \mathcal{O}_K^N$ and $m \in \mathbb{Z}$, $Y \cap (y + (\pi^m \mathcal{O}_K)^N)$ is written as $y + \pi^m Y_y'$. We may assume without loss of generality that Y_y' is written in the following form for some power series $\varphi_{d+1}(x_1, \cdots, x_d), \cdots, \varphi_N(x_1, \cdots, x_d) \in \mathcal{O}_K[[x_1, \cdots, x_d]]$ which converge on $\mathcal{O}_K^d$:

$$Y_y' = \{(x_1, \cdots, x_d, \varphi_{d+1}(x_1, \cdots, x_d), \cdots, \varphi_N(x_1, \cdots, x_d)) \in \mathcal{O}_K^N \,|\, x_1, \cdots, x_d \in \mathcal{O}_K\}.$$

Given $m' \geq m$, let

$$(\pi^m \mathcal{O}_K)^N = \coprod_{j=1}^{M} (\pi^m z^{(j)} + (\pi^{m'} \mathcal{O}_K)^N)\ (M \in \mathbb{Z}_{>0},\ z^{(j)} \in \mathcal{O}_K^N,\ 1 \leq j \leq M)$$

be the coset decomposition. Then,

$$\begin{aligned} Y \cap (y + (\pi^m \mathcal{O}_K)^N) &= \coprod_{j=1}^{M} (Y \cap (y + \pi^m z^{(j)} + (\pi^{m'} \mathcal{O}_K)^N)) \\ &= \coprod_{j=1}^{M} ((y + \pi^m Y'_y) \cap (y + \pi^m z^{(j)} + (\pi^{m'} \mathcal{O}_K)^N)) \\ &= \coprod_{j=1}^{M} (y + \pi^m (Y'_y \cap (z^{(j)} + (\pi^{m'-m} \mathcal{O}_K)^N))). \end{aligned}$$

In light of Remark 2.1.16, we may assume that $z^{(j)} \in Y'_y$ if $Y'_y \cap (z^{(j)} + (\pi^{m'-m}\mathcal{O}_K)^N) \neq \emptyset$.

Set $m' - m = n$ and consider $z^{(j)}\,(1 \leq j \leq M)$ such that $Y'_y \cap (z^{(j)} + (\pi^n \mathcal{O}_K)^N) \neq \emptyset$. For simplicity, denote $z^{(j)}$ by $z = (z_1, \cdots, z_N)$. Then,

$$z_k = \varphi_k(z_1, \cdots, z_d) \ (d+1 \leq k \leq N). \tag{2.2}$$

For $w = (w_1, \cdots, w_N) \in \mathcal{O}_K^N$, $z + \pi^n w \in Y'_y$ if and only if

$$z_k + \pi^n w_k = \varphi_k(z_1 + \pi^n w_1, \cdots, z_d + \pi^n w_d) \ (d+1 \leq k \leq N). \tag{2.3}$$

By (2.2) and (2.3),

$$\pi^n w_k = \varphi_k(z_1 + \pi^n w_1, \cdots, z_d + \pi^n w_d) - \varphi_k(z_1, \cdots, z_d) \ (d+1 \leq k \leq N).$$

The right-hand side is the product of π^n and some power series $\varphi'_k(w_1, \cdots, w_d) \in \mathcal{O}_K[[w_1, \cdots, w_d]]$ which converges on $\mathcal{O}_K^d$. Therefore,

$$z + \pi^n w \in Y'_y \iff w_k = \varphi'_k(w_1, \cdots, w_d) \ (d+1 \leq k \leq N).$$

Thus, there exists some Y'_z such that

$$Y'_y \cap (z + (\pi^{m'-m}\mathcal{O}_K)^N) = z + \pi^{m'-m} Y'_z.$$

This shows that for $z^{(j)}$ such that $Y'_y \cap (z^{(j)} + (\pi^{m'-m}\mathcal{O}_K)^N) \neq \emptyset$,

$$Y \cap (y + \pi^m z^{(j)} + (\pi^{m'}\mathcal{O}_K)^N) = y + \pi^m z^{(j)} + \pi^{m'} Y'_{z^{(j)}}.$$

This completes the proof of (ii).

Step 4.

It follows from (i) that for each $y \in Y$, there exist $m_y \in \mathbb{Z}$ and a set Y'_y in a certain form such that $Y \cap (y + (\pi^{m_y}\mathcal{O}_K)^N) = y + \pi^{m_y} Y'_y$. Since Y is compact, we can take a finite number of points $y^{(1)}, \cdots, y^{(n)} \in Y$ such that

$$Y = \bigcup_{i=1}^{n} (Y \cap (y^{(i)} + (\pi^{m_i}\mathcal{O}_K)^N)) = \bigcup_{i=1}^{n} (y^{(i)} + \pi^{m_i} Y'_{y^{(i)}}).$$

Set $m_0 = \max_{1 \leq i \leq n} m_i$ and fix any $m \geq m_0$. Then there exist finite subsets J_i of $\mathbb{Z}_{>0}$, $z^{(i,j)} \in \mathcal{O}_K^N\,(j \in J_i)$ and $Y'_{z^{(i,j)}}$ (written in a form similar to Y'_y in the statement of (i)) such that

$$y^{(i)} + \pi^{m_i} Y'_{y^{(i)}} = \coprod_{j \in J_i} (y^{(i)} + \pi^{m_i} z^{(i,j)} + \pi^m Y'_{z^{(i,j)}}).$$

Therefore, Y can be written in the following form:

$$Y = \bigcup_{i=1}^{n}(y^{(i)} + \pi^{m_i}Y'_{y^{(i)}}) = \bigcup_{i=1}^{n}\coprod_{j\in J_i}(y^{(i)} + \pi^{m_i}z^{(i,j)} + \pi^{m}Y'_{z^{(i,j)}}). \tag{2.4}$$

Assume that

$$(y^{(i_1)} + \pi^{m_{i_1}}z^{(i_1,j_1)} + \pi^{m}Y'_{z^{(i_1,j_1)}}) \cap (y^{(i_2)} + \pi^{m_{i_2}}z^{(i_2,j_2)} + \pi^{m}Y'_{z^{(i_2,j_2)}}) \neq \emptyset,$$

for some $1 \leq i_1 < i_2 \leq n$ and $j_1 \in J_{i_1}$, $j_2 \in J_{i_2}$. Then,

$$(y^{(i_1)} + \pi^{m_{i_1}}z^{(i_1,j_1)} + (\pi^{m}\mathcal{O}_K)^N) \cap (y^{(i_2)} + \pi^{m_{i_2}}z^{(i_2,j_2)} + (\pi^{m}\mathcal{O}_K)^N) \neq \emptyset.$$

So, by Remark 2.1.16,

$$y^{(i_1)} + \pi^{m_{i_1}}z^{(i_1,j_1)} + (\pi^{m}\mathcal{O}_K)^N = y^{(i_2)} + \pi^{m_{i_2}}z^{(i_2,j_2)} + (\pi^{m}\mathcal{O}_K)^N,$$

i.e.,

$$y^{(i_1)} + \pi^{m_{i_1}}z^{(i_1,j_1)} + \pi^{m}Y'_{z^{(i_1,j_1)}} = y^{(i_2)} + \pi^{m_{i_2}}z^{(i_2,j_2)} + \pi^{m}Y'_{z^{(i_2,j_2)}}.$$

Therefore, by removing redundant factors from the union in (2.4), Y can be written as in the statement of (iii). Note that each factor of this disjoint union is isomorphic to a ball of dimension d over K. By Theorem 2.1.20, the number of the factors of such decomposition of Y is well determined $\mod (q-1)$. This completes the proof of (iii), hence the proof of Proposition 2.1.26.

□

Remark 2.1.27
Théorème 9 and Proposition 11 in [15] treat only the case that $K = \mathbb{Q}_p$.

2.2. Some p-adic analytic observations.

Let p be a prime number, K a finite extension of $\mathbb{Q}_p$, $\mathcal{O}_K$ the ring of integers of K, $\mathfrak{M}_K$ the maximal ideal of $\mathcal{O}_K$, π a uniformizer of $\mathcal{O}_K$, $k = \mathcal{O}_K/\mathfrak{M}_K$ the residue field of $\mathcal{O}_K$ and q the cardinality of k. Let v be the valuation of K such that $v(K^\times) = \mathbb{Z}$. We denote the ramification index of $K/\mathbb{Q}_p$ by e. Let X be a proper, smooth and geometrically connected hyperbolic curve of genus $g\,(\geq 2)$ over K. Then, $X(K)$ has a natural structure of compact analytic manifold everywhere of dimension 1 over K, where $X(K)$ denotes the set of K-rational points of X.

In this section and the next one, we make some p-adic analytic and algebro-geometric observations on $X(K)$ to prove the main theorem of this chapter (Theorem 2.4.1).

Let J be the Jacobian of X. If $X(K) \neq \emptyset$, we fix $P_0 \in X(K)$. Then, $P \mapsto [\mathscr{L}(P - P_0)]$ determines a closed immersion $j : X \to J$. For $m \in \mathbb{Z}_{>0}$, $m_J : J \to J$ denotes multiplication by m on J. We define $X_m = X \times_J J$ by the following diagram:

$$\begin{tikzcd}
X_m := X \times_J J \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & J \arrow[d, "m_J"] \\
X \arrow[r, "j"] & J
\end{tikzcd}$$

X_m is an étale covering of X.

Let $J(K)$ be the set of K-rational points of J. $J(K)$ has a structure of abelian group and compact analytic manifold everywhere of dimension g over K. We have the following exact sequence [16, Part II, Chapter V, 7, Corollary 4]:

$$0 \to \mathcal{O}_K^{\oplus g} \to \ J(K) \to G \to 0,$$

for some finite abelian group G. There exist finite abelian groups G_p whose order is a power of p and $G_{p'}$ whose order is prime to p such that $G \simeq G_p \times G_{p'}$. Then we obtain the following exact sequences

$$0 \to \mathcal{O}_K^{\oplus g} \to J(K)^p \to G_p \to 0, \tag{2.5}$$

$$0 \to 0 \to J(K)^{p'} \to G_{p'} \to 0,$$

by taking the p-part and the prime-to-p part of the above exact sequence. Therefore $J(K) \simeq J(K)^p \times J(K)^{p'} \simeq J(K)^p \times G_{p'}$.

Remark 2.2.1
There is a one-to-one correspondence between $X_m(K)$ and $J(K) \cap m_J^{-1}(X(K))$, and we have a surjection $X_m(K) \twoheadrightarrow X(K) \cap m(J(K))$. If m is prime to p and $|G_{p'}|$, m_J induces a bijection $J(K) \to J(K)$.

Proposition 2.2.2
We regard $X(K) \subset J(K) \simeq J(K)^p \times G_{p'}$ as analytic manifolds over K as above. Then, there exists $n' \in \mathbb{Z}$ such that for all $n \geq n'$ and $a \in G_{p'}$, $X(K) \cap (p^n(J(K)^p) \times \{a\})$ is empty or isomorphic to a disjoint union of some copies of a ball of dimension 1 over K and the number of copies is a power of p.

Proof.
First we claim that $X(K) \cap (p^n(J(K)^p) \times \{0\})$ is empty or isomorphic to a disjoint union of some copies of a ball of dimension 1 over K and the number of copies is a power of p for sufficiently large n. In the following, we omit the $G_{p'}$-component of $J(K) \simeq J(K)^p \times G_{p'}$.

Let us take any n_0 such that $p^{n_0} \geq |G_p|$. Then, by (2.5), $(p^{n_0}\mathcal{O}_K)^{\oplus g} \subset p^{n_0}(J(K)^p) \subset \mathcal{O}_K^{\oplus g} \subset J(K)^p$. Therefore, $(p^{n_0+n_1}\mathcal{O}_K)^{\oplus g} \subset p^{n_0+n_1}(J(K)^p) \subset (p^{n_1}\mathcal{O}_K)^{\oplus g}$ for all $n_1 \in \mathbb{Z}_{\geq 0}$. On the other hand, we have $X(K) \cap (p^{n_1}\mathcal{O}_K)^{\oplus g} \subset X(K) \cap \mathcal{O}_K^{\oplus g}$. In the case $0 \notin X(K) \cap \mathcal{O}_K^{\oplus g}$, we may suppose $X(K) \cap (p^{n_1}\mathcal{O}_K)^{\oplus g} = \emptyset$ by taking sufficiently large n_1. Otherwise, by Proposition 2.1.26(i), we may suppose that there exist convergent power series $\varphi_2(x_1), \cdots, \varphi_g(x_1)$ which converge on $\mathcal{O}_K$, whose coefficients of terms of degree greater than 1 belong to $p^{n_0}\mathcal{O}_K$ and which satisfy

$$X(K) \cap (p^{n_1}\mathcal{O}_K)^{\oplus g} = \{(p^{n_1}x_1, p^{n_1}\varphi_2(x_1), \cdots, p^{n_1}\varphi_g(x_1)) \in \mathcal{O}_K^{\oplus g} \,|\, x_1 \in \mathcal{O}_K\}.$$

If $X(K) \cap (p^{n_1}\mathcal{O}_K)^{\oplus g} = \emptyset$, the claim is immediate. So, we may suppose $0 \in X(K) \cap \mathcal{O}_K^{\oplus g}$ and that $X(K) \cap (p^{n_1}\mathcal{O}_K)^{\oplus g}$ can be written as above. Then, for each $j = 2, \cdots, g$, $\varphi_j(0) = 0$.

$(p^{n_1}\mathcal{O}_K)^{\oplus g}/(p^{n_0+n_1}\mathcal{O}_K)^{\oplus g}$ is a finite abelian group whose order is power of p and $p^{n_0+n_1}(J(K)^p)/(p^{n_0+n_1}\mathcal{O}_K)^{\oplus g}$ is a subgroup. Since the coefficients of terms of degree greater than 1 of $\varphi_j(x_1)\,(2 \leq j \leq g)$ belong to $p^{n_0}\mathcal{O}_K$ and $\varphi_j(0) = 0$, the image of $X(K) \cap (p^{n_1}\mathcal{O}_K)^{\oplus g}$ in $(p^{n_1}\mathcal{O}_K)^{\oplus g}/(p^{n_0+n_1}\mathcal{O}_K)^{\oplus g}$ is also a subgroup. Therefore, the image of $X(K) \cap p^{n_0+n_1}(J(K)^p)$ in $(p^{n_1}\mathcal{O}_K)^{\oplus g}/(p^{n_0+n_1}\mathcal{O}_K)^{\oplus g}$ is a subgroup and its order is a power of p.

This shows that the number of cosets of $(p^{n_0+n_1}\mathcal{O}_K)^{\oplus g}$ in $p^{n_0+n_1}(J(K)^p)$ which intersect nontrivially with $X(K)$ is a power of p. Moreover, by Proposition 2.1.26(ii), the intersection of each such coset and $X(K)$ is isomorphic to a ball of dimension 1 over K.

Therefore, by taking $n \geq n_0 + n_1$, $X(K) \cap (p^n(J(K)^p) \times \{0\})$ is empty or isomorphic to a disjoint union of some copies of a ball of dimension 1 over K and the number of copies is a power of p.

For general $a \in G_{p'}$, by translating if necessary, there exists n_a such that $X(K) \cap (p^n(J(K)^p) \times \{a\})$ is empty or isomorphic to a disjoint union of some copies of a ball of dimension 1 over K and the number of copies is a power of p for all $n \geq n_a$. Since $G_{p'}$ is a finite group, $X(K) \cap (p^n(J(K)^p) \times \{a\})$ is empty or isomorphic to a disjoint union of some copies of a ball of dimension 1 over K and the number of copies is a power of p for all $n \geq \max\limits_{a \in G_{p'}} n_a$ and all $a \in G_{p'}$.

□

Proposition 2.2.3
For $m \in \mathbb{Z}_{>0}$,

$$i_K(X_m(K)) \equiv i_K(X(K) \cap m(J(K))) \times \sharp J(K)[m] \mod (q-1).$$

Proof.

If $X(K) = \emptyset$, the statement is clear. So, we may assume $X(K) \neq \emptyset$.

By (2.5), we have $m\mathcal{O}_K^{\oplus g} \subset m(J(K)^p)$. Set $(m(J(K)^p) : m\mathcal{O}_K^{\oplus g}) = r$. Then, there exist $b_1, \cdots, b_r \in m(J(K)^p)$ such that we have the following coset decomposition:

$$m(J(K)^p) = \coprod_{i=1}^{r} (b_i + m\mathcal{O}_K^{\oplus g})$$

Let us denote the element of $J(K)$ which corresponds to $(0, a) \in J(K)^p \times G_{p'}$ simply by a. Then, we have

$$m(J(K)) \simeq m(J(K)^p) \times mG_{p'} \simeq \coprod_{\substack{a \in mG_{p'} \\ 1 \leq i \leq r}} (a + b_i + m\mathcal{O}_K^{\oplus g}),$$

and

$$X(K) \cap m(J(K)) \simeq \coprod_{\substack{a \in mG_{p'} \\ 1 \leq i \leq r}} (X(K) \cap (a + b_i + m\mathcal{O}_K^{\oplus g})).$$

Since each $X(K) \cap (a + b_i + m\mathcal{O}_K^{\oplus g})$ is empty or a disjoint union of analytic manifolds each of which is isomorphic to a ball of dimension 1 over K, $X(K) \cap m(J(K))$ can be written in the following form:

$$X(K) \cap m(J(K)) \simeq \coprod_{j} (a_j + mY_j),$$

where $a_j \in m(J(K))$ and $Y_j \subset \mathcal{O}_K^{\oplus g}$ is an analytic manifold which is isomorphic to a ball of dimension 1 over K (therefore, $mY_j \subset m\mathcal{O}_K^{\oplus g}$).

By taking $a'_j \in J(K)$ such that $ma'_j = a_j$, we have

$$J(K) \cap m_J^{-1}(X(K)) = J(K) \cap m_J^{-1}(X(K) \cap m(J(K))) \simeq \coprod_{\substack{j \\ c \in J(K)[m]}} (a'_j + c + Y_j).$$

Now the proposition is immediate from Remark 2.2.1.

□

2.3. **An algebro-geometric observation.**

We follow the notations of the previous section.

Proposition 2.3.1
Assume that $X(K) \neq \emptyset$. *Set* $J(K) = B, X(K) = S$, *and* $M = \{0\} \times G_{p'} \subset J(K)^p \times G_{p'} \simeq J(K)$. *Then, there exists some* $P \in X(K)$ *such that*

$$(S - P) \cap M = \{(0,\, 0)\},$$

where $S - P := \{Q - P \in B \,|\, Q \in S\}$.

Proof.
Set $S_- := \{Q - P \in B \,|\, P\,,\, Q \in S\}$. Denote the point of $B = J(K)$ corresponding to the identity element of a group structure of B by O. Define $B \times B \to B$ by $(P, Q) \mapsto Q - P$, then a surjection $S \times S \twoheadrightarrow S_-$ is induced:

$$\begin{tikzcd}
S \times S \arrow[r, hook] \arrow[d, twoheadrightarrow] & B \times B \arrow[d] \\
S_- \arrow[r, hook] & B
\end{tikzcd}$$

The inverse image of $O \in S_- \subset B$ by this surjection is the diagonal set $\Delta_S \subset S \times S$. So, we obtain the following commutative diagram:

$$\begin{tikzcd}
(S \times S) \setminus \Delta_S \arrow[r, hook] \arrow[d] & S \times S \arrow[r, hook] \arrow[d, twoheadrightarrow] & B \times B \arrow[d] \\
S_- \setminus \{O\} \arrow[r, hook] & S_- \arrow[r, hook] & B
\end{tikzcd}$$

Then $(S_- \setminus \{O\}) \cap M$ is a (possibly empty) finite set. Let T be the inverse image of this set in $(S \times S) \setminus \Delta_S$.

$$\begin{tikzcd}
T \arrow[r, hook] \arrow[d] & (S \times S) \setminus \Delta_S \arrow[r, hook] \arrow[d] & S \times S \arrow[r, hook] \arrow[d, twoheadrightarrow] & B \times B \arrow[d] \\
(S_- \setminus \{O\}) \cap M \arrow[r, hook] & S_- \setminus \{O\} \arrow[r, hook] & S_- \arrow[r, hook] & B
\end{tikzcd}$$

Denote the composite of the first projection $S \times S \to S$ with the above injection $T \hookrightarrow S \times S$ by $\mathrm{pr}_1 : T \to S$. The condition that pr_1 is not surjective is equivalent to our assertion.

Define a morphism of schemes $f : X \times X \to J$ by $(P, Q) \mapsto Q - P$. Fix any $(P_0, Q_0) \in X \times X \setminus \Delta_X$ (where Δ_X is the diagonal set). Then, $f(P, Q) = f(P_0, Q_0)$ if and only if

$Q - P \sim Q_0 - P_0$. If there exists such $(P, Q) \in X \times X$, there exists an element F of the function field of X such that $(F) = P + Q_0 - P_0 - Q$. When $(P, Q) \neq (P_0, Q_0)$, $(F) \neq 0$. Indeed, since $P_0 \neq Q_0$ by the choice of (P_0, Q_0), one has $P = P_0$ and $Q = Q_0$ if $(F) = 0$. Then, F defines a morphism $X \to \mathbb{P}^1$ of degree at most 2. So X is a hyperelliptic curve since $g \geq 2$.

Therefore, when X is not a hyperelliptic curve, the morphism $(X \times X) \setminus \Delta_X \to J$ induced by f is injective. In particular, $T \to (S_- \setminus \{O\}) \cap M$ in the above diagram is injective. Since $(S_- \setminus \{O\}) \cap M$ is a finite set, T is also finite.

When X is a hyperelliptic curve, the fiber of $(X \times X) \setminus \Delta_X \to J$ over each point of $J(K)$ consists of at most 2 points. Since $(S_- \setminus \{O\}) \cap M$ is finite, T is again finite in this case.

So, there is no surjection from T to S, which is infinite. □

2.4. A criterion for existence of rational points in terms of i-invariants.

We follow the notations of Section 2.2. The following is the main theorem of this chapter:

Theorem 2.4.1
Assume that $q \neq 2$ and let $m > 1$ be a divisor of $q-1$. Then, the following five conditions are equivalent:

(i) $X(K) \neq \emptyset$.
(ii) *There exists a finite étale covering X' of X such that $X'(K) \neq \emptyset$.*
(iii) *There exists a finite étale covering X' of X such that $i_K(X'(K)) \not\equiv 0 \mod (q-1)$.*
(iv) *There exists a finite étale covering X' of X such that $i_K(X'(K)) \not\equiv 0 \mod m$.*
(v) *There exists a finite étale covering X' of X such that $i_K(X'(K)) \equiv (a\ power\ of\ p) \mod (q-1)$.*

Proof.
The implications (v)$\Longrightarrow$(iv)$\Longrightarrow$(iii)$\Longrightarrow$(ii)$\Longrightarrow$(i) are trivial. We will show the implication (i)$\Longrightarrow$(v).

By Proposition 2.3.1, there exists some $P_0 \in X(K)$ such that $X(K) \subset J(K) \simeq J(K)^p \times G_{p'}$ and

$$X(K) \cap (\{0\} \times G_{p'}) = \{O\},$$

with respect to the closed immersion $j : X \to J$ defined by $P \mapsto [\mathscr{L}(P - P_0)]$.

This implies that by taking sufficiently large n, we have $X(K) \cap p^n(J(K)) = X(K) \cap (p^n(J(K)^p) \times \{0\})$. Further, this intersection is isomorphic to a disjoint union of some copies of a ball of dimension 1 over K and the number of copies is a power of p by Proposition 2.2.2. In other words, $i_K(X(K) \cap p^n(J(K))) \equiv (\text{a power of} p) \mod (q-1)$. On the other hand, by Proposition 2.2.3,

$$i_K(X_{p^n}(K)) \equiv i_K(X(K) \cap p^n(J(K))) \times \sharp J(K)[p^n] \mod (q-1).$$

Since $\sharp J(K)[p^n]$ is a power of p, this completes the proof.

□

3. Galois action on the set of rational points and i-invariants

Let K be a finite extension of $\mathbb{Q}_p$, X a proper, smooth and geometrically connected hyperbolic curve over K and $X(K)$ the set of K-rational points of X. By the Deligne-Mumford theorem (Theorem 3.1.11), there exists a finite extension L/K such that $X_L := X \times_{\operatorname{Spec} K} \operatorname{Spec} L$ has a unique stable model. In this chapter, we show that $i_K(X(K))$ mod 2 can be recovered from the special fiber of the stable model of X_L, under the assumption that p is odd and that L/K is a tame extension. (We obtain partial results in the case where $p = 2$.)

We review various definitions in Section 3.1. In Section 3.2, we consider the case where X has a stable model over K, which is the origin of our arguments. In Section 3.3, we describe explicitly the Galois action on the inverse image of a rational point of the special fiber by the reduction map without assuming that L/K is tame. Then, assuming that L/K is tame, we calculate the i-invariant of the set of K-rational points of X over a smooth point (which is treated in Section 3.4) and a node (which is treated in Section 3.5) of the special fiber of the stable model. Here, the set of K-rational points is characterized as the Galois-invariant subset of the inverse image of a smooth point or a node by the reduction map.

3.1. **Review of definitions.**

We review definitions of models and reductions of curves according to [2]. In this section, we denote a Dedekind scheme (i.e., an integral, normal and Noetherian scheme of dimension 0 or 1) of dimension 1 by S, the function field of S by $K(S)$, and the generic point of S by η, unless otherwise noted.

Definition 3.1.1
Let k be a field. A separated scheme of finite type over k whose irreducible components are all of dimension 1 is called a *curve over* k.

Definition 3.1.2 (cf. [2, §8, Definition 3.1, §10, Definition 1.1])
Let C be a normal, geometrically connected and projective curve over $K(S)$. We call a flat, projective S-scheme $\mathcal{C} \to S$ with $\mathcal{C}$ integral, normal and of dimension 2 together with an isomorphism $f : \mathcal{C}_\eta \simeq C$ over $K(S)$ a *model of* C *over* S.

We will say that a model $(\mathcal{C}, f)$ verifies a property (P) if $\mathcal{C} \to S$ verifies (P).

Definition 3.1.3 (cf. [2, §10, Definition 1.18])
Let C be a normal, geometrically connected and projective curve over $K(S)$. Let us fix a closed point $s \in S$. We call the fiber $\mathcal{C}_s$ of a model $\mathcal{C}$ of C a *reduction of* C *at* s.

Definition 3.1.4 (cf. [2, §10, Definition 1.19])
Let C be as in Definition 3.1.3. We will say that C has *good reduction at* $s \in S$ if it admits a smooth model over $\operatorname{Spec} \mathcal{O}_{S,\,s}$. If C does not have good reduction at s, we will say that C has *bad reduction at* s.

Definition 3.1.5 (cf. [2, §7, Definition 5.13])
Let X be a reduced curve over an algebraically closed field k. Let $\pi : X' \to X$ be the normalization morphism. For a closed point $x \in X$, set $\delta_x = \operatorname{length}_{\mathcal{O}_{X,\,x}}(\pi_*\mathcal{O}_{X'}/\mathcal{O}_X)_x$, $m_x = |\pi^{-1}(x)|$. We say that x is an *ordinary multiple point* or a *node* if $m_x = 2$ and $\delta_x = 1$.

Definition 3.1.6 (cf. [2, §10, Definition 3.1])
Let C be a curve over an algebraically closed field k. We say that C is *semi-stable* if it is reduced, and if its singular points are ordinary double points. We say that C is *stable* if, moreover, the following conditions are verified:

(1) C is connected, projective and of arithmetic genus $p_a(C) \geq 2$.
(2) Let Γ be an irreducible component of C that is isomorphic to $\mathbb{P}^1_k$. Then it intersects the other irreducible components at at least three points.

Definition 3.1.7 (cf. [2, §10, Definition 3.2])
We say that a curve C over a field k is *semi-stable* (resp. *stable*) if its extension $C_{\overline{k}}$ to the algebraic closure $\overline{k}$ of k is a semi-stable (resp. stable) curve over $\overline{k}$.

Definition 3.1.8 (cf. [2, §10, Definition 3.8])
Let C be a semi-stable curve over a field k, let $\pi : C' \to C$ be the normalization morphism, and $x \in C$ a singular point. We will say that x is *split* if the points of $\pi^{-1}(x)$ are all rational over k.

Definition 3.1.9 (cf. [2, §10, Definition 3.14])
Let $f : X \to S$ be a morphism of finite type to S. We say that f is *semi-stable* (or a *semi-stable curve*), or that X is a *semi-stable curve over* S, if f is flat and if for any $s \in S$, the fiber X_s is a semi-stable curve over $k(s)$. We say that f is *stable* (or a *stable curve*) of genus $g \geq 2$, or that X is a *stable curve over* S of genus $g \geq 2$, if f is proper, flat, and if for any $s \in S$, the fiber X_s is a stable curve over $k(s)$ of arithmetic genus g.

Definition 3.1.10 (cf. [2, §10, Definition 3.27])
Let C be a smooth, geometrically connected and projective curve over $K(S)$. We say that C has *semi-stable reduction* (resp. *stable reduction*) at $s \in S$ if there exists a model $\mathcal{C}$ of C over $\operatorname{Spec} \mathcal{O}_{S,s}$ that is semi-stable (resp. stable) over $\operatorname{Spec} \mathcal{O}_{S,s}$. The special fiber $\mathcal{C}_s$ of a stable model over $\operatorname{Spec} \mathcal{O}_{S,s}$ is called the *stable reduction of* C *at* s.

Theorem 3.1.11 (Deligne-Mumford, (cf. [2, §10, Theorem 4.3]))
Let C be a smooth, projective, geometrically connected curve of genus $g \geq 2$ over $K(S)$. Then there exists a Dedekind scheme S' (with a function field $K(S')$) that is finite and flat over S such that $C_{K(S')} := C \times_{\operatorname{Spec} K(S)} \operatorname{Spec} K(S')$ has a stable model over S' which is unique up to isomorphism over S'. Moreover, we can take $K(S')$ separable over $K(S)$.

Here, we give a definition of log smooth reduction. The following definition is different from the usual one. However, these definitions are equivalent by [13, Theorem 4.2].

Definition 3.1.12
Let p be a prime number and K a finite extension of $\mathbb{Q}_p$. Let X be a proper, smooth and geometrically connected hyperbolic curve (hence, of genus $g \geq 2$) over K. By Theorem 3.1.11, there exists a finite extension L of K such that $X_L := X \times_{\operatorname{Spec} K} \operatorname{Spec} L$ has a stable model over $\mathcal{O}_L$. We say that X has *log smooth reduction* if we can take L tame over K.

3.2. The case where X has stable reduction.

Let p be a prime number, K a finite extension of $\mathbb{Q}_p$, $\mathcal{O}_K$ the ring of integers of K, $\mathfrak{M}_K$ the maximal ideal of $\mathcal{O}_K$, π a uniformizer of $\mathcal{O}_K$, $k = \mathcal{O}_K/\mathfrak{M}_K$ the residue field of

$\mathcal{O}_K$ and q the cardinality of k. Let v be the valuation of K such that $v(K^\times) = \mathbb{Z}$. Let X be a proper, smooth and geometrically connected hyperbolic curve over K with stable reduction over $\mathcal{O}_K$. We denote the stable model by $\mathfrak{X}$.

Let $X(K)$ (resp. $\mathfrak{X}(\mathcal{O}_K)$) be the set of K-rational (resp. $\mathcal{O}_K$-rational) points of X (resp. $\mathfrak{X}$). Set $\mathfrak{X}_k = \mathfrak{X} \times_{\operatorname{Spec}\mathcal{O}_K} \operatorname{Spec} k$ and denote the set of k-rational points of $\mathfrak{X}_k$ by $\mathfrak{X}_k(k)$.

We have natural maps $\mathfrak{X}(\mathcal{O}_K) \to X(K)$, $\rho : \mathfrak{X}(\mathcal{O}_K) \to \mathfrak{X}_k(k)$. Since $\mathfrak{X}$ is proper over $\mathcal{O}_K$, the former is bijective by the valuative criterion of properness.

$$\begin{tikzcd} X(K) & \mathfrak{X}(\mathcal{O}_K) \arrow[l, "\sim"'] \arrow[r, "\rho"] & \mathfrak{X}_k(k) \end{tikzcd} .$$

Proposition 3.2.1
Let $P \in \mathfrak{X}_k(k)$ be a smooth point over k. Then, $i_K(\rho^{-1}(P)) \equiv 1 \mod (q-1)$.

Proof.

Since $\mathfrak{X}_k \to \mathfrak{X}$ is a closed immersion, we may consider $P \in \mathfrak{X}_k(k)$ as a closed point of $\mathfrak{X}$. If P is a smooth point over k, $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_K[[T]]$ and

$$\begin{aligned}\rho^{-1}(P) &\simeq \operatorname{Hom}_{\operatorname{Spec}\mathcal{O}_K}(\operatorname{Spec}\mathcal{O}_K, \operatorname{Spec}\mathcal{O}_{\mathfrak{X},P})\\ &\simeq \operatorname{Hom}_{\mathcal{O}_K}(\mathcal{O}_{\mathfrak{X},P}, \mathcal{O}_K)\\ &\simeq \operatorname{Hom}_{\mathcal{O}_K}(\hat{\mathcal{O}}_{\mathfrak{X},P}, \mathcal{O}_K)\\ &\simeq \mathfrak{M}_K.\end{aligned}$$

The last bijection associates $x \in \mathfrak{M}_K$ with $f_x : \hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_K[[T]] \to \mathcal{O}_K$ such that $f_x(T) = x$. Since $i_K(\mathfrak{M}_K) \equiv 1 \mod (q-1)$ by Example 2.1.24, this completes the proof.

□

Proposition 3.2.2
Let $P \in \mathfrak{X}_k(k)$ be a node and assume that P is split. Then, $i_K(\rho^{-1}(P)) \equiv 0 \mod (q-1)$.

Proof.

If P is a node and split, there exists $r \in \mathbb{Z}_{>0}$ such that $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_K[[S, T]]/(ST - \pi^r)$, and we have:

$$\begin{aligned}\rho^{-1}(P) &\simeq \operatorname{Hom}_{\operatorname{Spec}\mathcal{O}_K}(\operatorname{Spec}\mathcal{O}_K, \operatorname{Spec}\mathcal{O}_{\mathfrak{X},P})\\ &\simeq \operatorname{Hom}_{\mathcal{O}_K}(\mathcal{O}_{\mathfrak{X},P}, \mathcal{O}_K)\\ &\simeq \operatorname{Hom}_{\mathcal{O}_K}(\hat{\mathcal{O}}_{\mathfrak{X},P}, \mathcal{O}_K)\\ &\simeq \{(x, y) \in \mathfrak{M}_K \times \mathfrak{M}_K \mid xy = \pi^r\} =: A_r.\end{aligned}$$

The last bijection associates $(x, y) \in A_r$ with $f_{(x,y)} : \hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_K[[S, T]]/(ST - \pi^r) \to \mathcal{O}_K$ such that $f_{(x,y)}(S) = x$, $f_{(x,y)}(T) = y$. Here, we denote the images of $S, T \in \mathcal{O}_K[[S, T]]$ in $\mathcal{O}_K[[S, T]]/(ST - \pi^r)$ simply by S, T.

On the other hand,

$$\begin{aligned} A_r &\simeq \{x \in \mathfrak{M}_K \mid 0 < v(x) < r\} \\ &\simeq \coprod_{0<i<r} (\mathfrak{M}_K^i \setminus \mathfrak{M}_K^{i+1}). \end{aligned}$$

By Example 2.1.24, $i_K(\mathfrak{M}_K^i \setminus \mathfrak{M}_K^{i+1}) \equiv 0 \mod (q-1)$ for each $0 < i < r$. Therefore, $i_K(\rho^{-1}(P)) \equiv 0 \mod (q-1)$.

□

Corollary 3.2.3
Let $\mathfrak{X}_k^{\mathrm{sm}} \subset \mathfrak{X}_k$ be the (open) set which consists of all points of $\mathfrak{X}_k$ which are smooth over k. If all nodes in $\mathfrak{X}_k(k)$ are split, $i_K(X(K)) \equiv \sharp\mathfrak{X}_k^{\mathrm{sm}}(k) \mod (q-1)$.

Proof.

Since $X(K) \simeq \mathfrak{X}(\mathcal{O}_K) = \coprod_{P \in \mathfrak{X}_k(k)} \rho^{-1}(P)$, the corollary is immediate from Proposition 3.2.1 and Proposition 3.2.2.

□

Remark 3.2.4
Let Y be a proper, smooth and geometrically connected hyperbolic curve over K which has a regular model $\mathfrak{Y}$ over $\mathcal{O}_K$ (Y does not necessarily have stable reduction). Then, by an argument similar to Proposition 3.2.1 and Corollary 3.2.3, $i(Y(K)) \equiv \sharp\mathfrak{Y}_k^{\mathrm{sm}}(k) \mod (q-1)$.

Remark 3.2.5
We will consider nodes which are not necessarily split in the following sections. However, Proposition 3.2.2 is independent of the arguments there (i.e., they do not imply Proposition 3.2.2).

3.3. Galois action on the set of rational points.

Let p be a prime number, K a finite extension of $\mathbb{Q}_p$ and X a proper, smooth and geometrically connected hyperbolic curve over K. By Theorem 3.1.11, there exists a finite Galois extension L of K such that $X_L := X \times_{\operatorname{Spec} K} \operatorname{Spec} L$ has a stable model $\mathfrak{X}$. Let $\mathcal{O}_K$ (resp. $\mathcal{O}_L$) be the ring of integers of K (resp. L), $\mathfrak{M}_K$ (resp. $\mathfrak{M}_L$) the maximal ideal of $\mathcal{O}_K$ (resp. $\mathcal{O}_L$), $k = \mathcal{O}_K/\mathfrak{M}_K$ (resp. $k_L = \mathcal{O}_L/\mathfrak{M}_L$) the residue field and q the cardinality of k. By taking an unramified extension of L if necessary, we may assume that all singular points of $\mathfrak{X}_{k_L}(k_L)$ are split, where $\mathfrak{X}_{k_L} = \mathfrak{X} \times_{\operatorname{Spec} \mathcal{O}_L} \operatorname{Spec} k_L$ and $\mathfrak{X}_{k_L}(k_L)$ is the set of k_L-rational points of $\mathfrak{X}_{k_L}$. Let π be a uniformizer of $\mathcal{O}_L$ and v the valuation of L such that $v(L^\times) = \mathbb{Z}$. We denote the Galois group of L/K by $G = \mathrm{Gal}(L/K)$ and the inertia group of L/K by $I \subset G$.

Let $X(K)$ (resp. $X(L)$) be the set of K-rational (resp. L-rational) points of X and $\mathfrak{X}(\mathcal{O}_L)$ the set of $\mathcal{O}_L$-rational points of $\mathfrak{X}$. We denote the subset of $\mathfrak{X}_{k_L}(k_L)$ which consists of smooth (resp. non-smooth) points over k_L by $\mathfrak{X}_{k_L}^{\mathrm{sm}}(k_L)$ (resp. $\mathfrak{X}_{k_L}^{\mathrm{node}}(k_L)$). In particular, $\mathfrak{X}_{k_L}(k_L) = \mathfrak{X}_{k_L}^{\mathrm{sm}}(k_L) \cup \mathfrak{X}_{k_L}^{\mathrm{node}}(k_L)$.

By the uniqueness of stable model (Theorem 3.1.11), G acts on these sets. We denote the G-invariant subsets of these sets by $X(L)^G$ and so on. There exist natural maps

$\mathfrak{X}(\mathcal{O}_L) \to X(L)$ and $\rho : \mathfrak{X}(\mathcal{O}_L) \to \mathfrak{X}_{k_L}(k_L)$. Since $\mathfrak{X}$ is proper over $\mathcal{O}_L$, the former is bijective by the valuative criterion of properness. Moreover, as P is split by assumption, these maps are G-equivariant. Since $X(K) = X(L)^G$, we obtain the following commutative diagram:

$$\begin{tikzcd}
X(L) & \mathfrak{X}(\mathcal{O}_L) \arrow[l, "\sim"'] \arrow[r, "\rho"] & \mathfrak{X}_{k_L}(k_L) \\
X(K) \arrow[u, hook] & \mathfrak{X}(\mathcal{O}_L)^G \arrow[l, "\sim"'] \arrow[r, "\rho'"] \arrow[u, hook] & \mathfrak{X}_{k_L}(k_L)^G \arrow[u, hook]
\end{tikzcd}$$

Remark 3.3.1
Since $\mathfrak{X}_{k_L} \to \mathfrak{X}$ is a closed immersion, we may consider $P \in \mathfrak{X}_{k_L}^{\mathrm{node}}(k_L)$ as a closed point of $\mathfrak{X}$. Moreover, there exists a positive integer r such that $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[S,T]]/(ST - \pi^r)$. Set:

$$\mathfrak{X}'^{\mathrm{node}}_{k_L}(k_L) = \{P \in \mathfrak{X}_{k_L}^{\mathrm{node}}(k_L) \,|\, \hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[S,T]]/(ST - \pi^r),\, r > 1\}.$$

Then the image of $\mathfrak{X}(\mathcal{O}_L)$ by ρ coincides with $\mathfrak{X}_{k_L}^{\mathrm{sm}}(k_L) \cup \mathfrak{X}'^{\mathrm{node}}_{k_L}(k_L)$.

For each $P \in \mathfrak{X}_{k_L}(k_L)^G$, we describe the G-action on $\rho^{-1}(P)$ explicitly.

Let $\mathrm{pr} : X_L := X \times_{\operatorname{Spec} K} \operatorname{Spec} L \to X$ be the projection.

$$\begin{tikzcd}
X_L \arrow[r, "\mathrm{pr}"] \arrow[d] \arrow[dr, phantom, "\square"] & X \arrow[d] \\
\operatorname{Spec} L \arrow[r] & \operatorname{Spec} K
\end{tikzcd}$$

The map $\mathrm{Hom}_{\operatorname{Spec} L}(\operatorname{Spec} L,\, X_L) \to \mathrm{Hom}_{\operatorname{Spec} K}(\operatorname{Spec} L,\, X)$, $\phi_L \mapsto \mathrm{pr} \circ \phi_L = \phi$ is a bijection. For each $\gamma \in G$, let $\widetilde{\gamma}$ be the automorphism of $\operatorname{Spec} L$ over $\operatorname{Spec} K$ induced by γ. We define a G-action on $\mathrm{Hom}_{\operatorname{Spec} K}(\operatorname{Spec} L,\, X)$ by:

$$\gamma \cdot \phi = \phi \circ \widetilde{\gamma},$$

for all $\gamma \in G$ and $\phi \in \mathrm{Hom}_{\operatorname{Spec} K}(\operatorname{Spec} L,\, X)$. We let G act on $\mathrm{Hom}_{\operatorname{Spec} L}(\operatorname{Spec} L,\, X_L)$ so that the bijection $\mathrm{Hom}_{\operatorname{Spec} L}(\operatorname{Spec} L,\, X_L) \to \mathrm{Hom}_{\operatorname{Spec} K}(\operatorname{Spec} L,\, X)$ is G-equivariant. Since $\gamma \cdot \phi_L = (\gamma \cdot \phi)_L$, the map $\gamma \cdot \phi_L$ makes the following diagram commutative:

$$\begin{tikzcd}
\operatorname{Spec} L \arrow[r, "\gamma\cdot\phi_L"] \arrow[rr, bend left, "\gamma\cdot\phi"] \arrow[dr, "\mathrm{id}"'] & X_L \arrow[r, "\mathrm{pr"] \arrow[d] \arrow[dr, phantom, "\square"] & X \arrow[d] \\
& \operatorname{Spec} L \arrow[r] & \operatorname{Spec} K
\end{tikzcd}$$

i.e.,

$$\gamma \cdot \phi_L = (\mathrm{id}_X \times \widetilde{\gamma}^{-1}) \circ \phi_L \circ \widetilde{\gamma}.$$

Denote the residue field at P by $k(P)(\simeq k_L)$. Then we have the following commutative diagram:

$$\begin{tikzcd}
 & \operatorname{Spec}(\hat{\mathcal{O}}_{\mathfrak{X},P}\otimes_{\mathcal{O}_L} L) \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & \operatorname{Spec}\hat{\mathcal{O}}_{\mathfrak{X},P} \arrow[d] \arrow[dr, phantom, "\square"] & \operatorname{Spec} k(P) \arrow[l] \arrow[d] \\
X \arrow[d] \arrow[dr, phantom, "\square"] & X_L \arrow[l] \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & \mathfrak{X} \arrow[d] \arrow[dr, phantom, "\square"] & \mathfrak{X}_{k_L} \arrow[l] \arrow[d] \\
\operatorname{Spec} K & \operatorname{Spec} L \arrow[l] \arrow[r] & \operatorname{Spec}\mathcal{O}_L & \operatorname{Spec} k_L \arrow[l]
\end{tikzcd}$$

Case 1. The case where $P \in \mathfrak{X}^{\mathrm{sm}}_{k_L}(k_L)^G$.

In this case, $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[T]]$, and

$$\begin{aligned}
\rho^{-1}(P) &\simeq \operatorname{Hom}_{\operatorname{Spec}\mathcal{O}_L}(\operatorname{Spec}\mathcal{O}_L,\, \operatorname{Spec}\mathcal{O}_{\mathfrak{X},P}) \\
&\simeq \operatorname{Hom}_{\mathcal{O}_L}(\mathcal{O}_{\mathfrak{X},P},\, \mathcal{O}_L) \\
&\simeq \operatorname{Hom}_{\mathcal{O}_L}(\hat{\mathcal{O}}_{\mathfrak{X},P}, \mathcal{O}_L) \\
&\simeq \mathfrak{M}_L.
\end{aligned}$$

The last bijection associates $x \in \mathfrak{M}_L$ with $f : \hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[T]] \to \mathcal{O}_L$ such that $f(T) = x$.

Denote the element of $\operatorname{Hom}_{\mathcal{O}_L}(\hat{\mathcal{O}}_{\mathfrak{X},P}, \mathcal{O}_L)$ which corresponds to $x \in \mathfrak{M}_L \simeq \rho^{-1}(P)$ by f_x. Let ϕ_x be the element of $\operatorname{Hom}_{\operatorname{Spec} L}(\operatorname{Spec} L,\, X_L)$ obtained from f_x. Since $\gamma \cdot \phi_x = (\mathrm{id}_X \times \widetilde{\gamma}^{-1}) \circ \phi_x \circ \widetilde{\gamma}$ for each $\gamma \in G$,

$$(\gamma \cdot f_x)(T) = \gamma(f_x(\gamma^{-1} \cdot T)).$$

On the other hand, G acts on $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[T]]$ so that the following diagram is commutative:

$$\begin{tikzcd}
G \arrow[r, phantom, "\curvearrowright"] \arrow[d, equal] \arrow[dr, phantom, "\circlearrowleft"] & \hat{\mathcal{O}}_{\mathfrak{X},P} \\
G \arrow[r, phantom, "\curvearrowright"] & \mathcal{O}_L \arrow[u, hook]
\end{tikzcd}$$

In other words, for each $\gamma' \in G$ and $a \in \mathcal{O}_L \subset \hat{\mathcal{O}}_{\mathfrak{X},P}$, we have $\gamma' \cdot a = \gamma'(a)$ (the usual Galois-action). As to $T \in \mathcal{O}_L[[T]] \simeq \hat{\mathcal{O}}_{\mathfrak{X},P}$, for each $\gamma' \in G$, $\gamma' \cdot T$ can be written in the following form for some $a_i = a_{\gamma',i} \in \mathcal{O}_L$ depending on γ':

$$\gamma' \cdot T = \sum_{i=0}^{\infty} a_i T^i.$$

In the following, we will denote $\gamma' \cdot T$ simply by $\gamma'(T)$.

Lemma 3.3.2
In the above notation, $a_0 \in \mathfrak{M}_L$ and $a_1 \in \mathcal{O}_L^{\times}$.

Proof.

$\gamma' \in G$ defines an automorphism $\gamma' : \mathcal{O}_L[[T]] \to \mathcal{O}_L[[T]]$. Let $\overline{\gamma'} : k_L[[T]] \to k_L[[T]]$ be the automorphism of $k_L[[T]]$ such that the following diagram is commutative. (Since γ' preserves $\mathfrak{M}_L$, such $\overline{\gamma'}$ exists.)

$$\begin{tikzcd}
\mathcal{O}_L[[T]] \arrow[r, "\gamma'"] \arrow[d] \arrow[dr, phantom, "\circlearrowleft"] & \mathcal{O}_L[[T]] \arrow[d] \\
k_L[[T]] \arrow[r, "\overline{\gamma'}"] & k_L[[T]]
\end{tikzcd}$$

Here, vertical arrows are natural surjections.

Denote the image of $a \in \mathcal{O}_L$ in k_L by $\overline{a}$. Since $k_L[[T]]$ is a DVR and T is a uniformizer, $\overline{\gamma'}(T)$ is also a uniformzer of $k_L[[T]]$. So, $\overline{a_0} = 0$ and $\overline{a_1} \neq 0$ in k_L, as desired.

□

By replacing γ' in the above argument by γ^{-1}, we obtain:

$$(\gamma \cdot f_x)(T) = \gamma(f_x(\gamma^{-1}(T))) = \sum_{i=0}^{\infty} \gamma(a_i x^i),$$

where $a_i = a_{\gamma^{-1},\,i} \in \mathcal{O}_L$. Therefore, if we identify $\rho^{-1}(P)$ with $\mathfrak{M}_L$, the image $[\gamma](x)$ of $x \in \mathfrak{M}_L$ by the action of $\gamma \in G$ can be written in the following form:

$$[\gamma](x) = \sum_{i=0}^{\infty} \gamma(a_i x^i).$$

<u>Case 2.</u> The case where $P \in \mathfrak{X}_{k_L}^{\mathrm{node}}(k_L)^G$.

In this case, $\hat{\mathcal{O}}_{\mathfrak{X},\,P} \simeq \mathcal{O}_L[[S,\,T]]/(ST - \pi^r)$. In the following, we will denote the images of $S,\,T \in \mathcal{O}_L[[S,\,T]]$ in $\mathcal{O}_L[[S,\,T]]/(ST - \pi^r)$ simply by $S,\,T$.

Remark 3.3.3
For each element of $\mathcal{O}_L[[S,\,T]]/(ST - \pi^r)$, the "constant term" and the " coefficient of S^i (resp. T^i)" $(i \geq 1)$ are not well-defined. However, they are well-defined modulo $\mathfrak{M}_L^r$. Since we have $ST = \pi^r$ in $\mathcal{O}_L[[S,\,T]]/(ST - \pi^r)$, any $F \in \mathcal{O}_L[[S,\,T]]/(ST - \pi^r)$ can be uniquely written in the following form:

$$F = a_0 + \sum_{i=1}^{\infty} (a_{i,\,1} S^i + a_{i,\,2} T^i) \ (a_0,\, a_{i,\,j} \in \mathcal{O}_L,\, i \geq 1,\, j = 1,\, 2).$$

As in Case 1, we have the following bijections:

$$\begin{aligned}
\rho^{-1}(P) &\simeq \mathrm{Hom}_{\mathrm{Spec}\,\mathcal{O}_L}(\mathrm{Spec}\,\mathcal{O}_L,\, \mathrm{Spec}\,\mathcal{O}_{\mathfrak{X},\,P}) \\
&\simeq \mathrm{Hom}_{\mathcal{O}_L}(\mathcal{O}_{\mathfrak{X},\,P},\, \mathcal{O}_L) \\
&\simeq \mathrm{Hom}_{\mathcal{O}_L}(\hat{\mathcal{O}}_{\mathfrak{X},\,P}, \mathcal{O}_L) \\
&\simeq \{(x, y) \in \mathfrak{M}_L \times \mathfrak{M}_L \,|\, xy = \pi^r\} =: A_r.
\end{aligned}$$

The last bijection associates $(x,\,y) \in A_r$ with $f : \hat{\mathcal{O}}_{\mathfrak{X},\,P} \simeq \mathcal{O}_L[[S,\,T]]/(ST - \pi^r) \to \mathcal{O}_L$ such that $f(S) = x,\ f(T) = y$.

Denote the element of $\mathrm{Hom}_{\mathcal{O}_L}(\hat{\mathcal{O}}_{\mathfrak{X},P},\, \mathcal{O}_L)$ which corresponds to $(x,\, y) \in A_r \simeq \rho^{-1}(P)$ by $f_{(x,\,y)}$. Let $\phi_{(x,\,y)}$ be the element of $\mathrm{Hom}_{\mathrm{Spec}\,L}(\mathrm{Spec}\,L,\, X_L)$ obtained from $f_{(x,\,y)}$. As in Case 1, for each $\gamma \in G$,

$$\begin{cases} (\gamma \cdot f_{(x,\,y)})(S) & = \gamma(f_{(x,\,y)}(\gamma^{-1} \cdot S)), \\ (\gamma \cdot f_{(x,\,y)})(T) & = \gamma(f_{(x,\,y)}(\gamma^{-1} \cdot T)). \end{cases}$$

On the other hand, as in Case 1, for each $\gamma' \in G$ and $a \in \mathcal{O}_L \subset \hat{\mathcal{O}}_{\mathfrak{X},P}$, we have $\gamma' \cdot a = \gamma'(a)$ (the usual Galois-action). As to $S,\, T \in \mathcal{O}_L[[S,\, T]]/(ST - \pi^r) \simeq \hat{\mathcal{O}}_{\mathfrak{X},P}$, for each $\gamma' \in G$, $\gamma' \cdot S$ and $\gamma' \cdot T$ can be uniquely written in the following form:

$$\gamma' \cdot \begin{pmatrix} S \\ T \end{pmatrix} = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} + \sum_{i=1}^{\infty} \begin{pmatrix} a_{i,\,1} & a_{i,\,2} \\ b_{i,\,1} & b_{i,\,2} \end{pmatrix} \begin{pmatrix} S^i \\ T^i \end{pmatrix}.$$

Here, $a_0 = a_{\gamma',\,0}$, $b_0 = b_{\gamma',\,0}$, $a_{i,\,j} = a_{\gamma',\,i,\,j}$, $b_{i,\,j} = b_{\gamma',\,i,\,j} \in \mathcal{O}_L$ $(i \geq 1,\ j = 1,\, 2)$. In the following, we will denote $\gamma' \cdot S$, $\gamma' \cdot T$ simply by $\gamma'(S)$, $\gamma'(T)$.

Lemma 3.3.4
In the above notation, $a_0,\, b_0 \in \mathfrak{M}_L^r$ and one (and only one) of the following conditions holds:

(i) $a_{1,\,1},\, b_{1,\,2} \in \mathcal{O}_L^\times$ *and* $a_{i,\,2},\, b_{i,\,1} \in \mathfrak{M}_L^r$ $(i \geq 1)$.
(ii) $a_{1,\,2},\, b_{1,\,1} \in \mathcal{O}_L^\times$ *and* $a_{i,\,1},\, b_{i,\,2} \in \mathfrak{M}_L^r$ $(i \geq 1)$.

Proof.
$\gamma' \in G$ defines an automorphism $\gamma' : \mathcal{O}_L[[S,\, T]]/(ST - \pi^r) \to \mathcal{O}_L[[S,\, T]]/(ST - \pi^r)$. Let $\overline{\gamma'} : k_L[[S,\, T]]/(ST) \to k_L[[S,\, T]]/(ST)$ be the automorphism of $k_L[[S,\, T]]/(ST)$ such that the following diagram is commutative. (Since γ' preserves $\mathfrak{M}_L$, such $\overline{\gamma'}$ exists.)

$$\begin{tikzcd} \mathcal{O}_L[[S,\, T]]/(ST - \pi^r) \arrow[r, "\gamma'"] \arrow[d] \arrow[dr, phantom, "\circlearrowleft"] & \mathcal{O}_L[[S,\, T]]/(ST - \pi^r) \arrow[d] \\ k_L[[S,\, T]]/(ST) \arrow[r, "\overline{\gamma'}"] & k_L[[S,\, T]]/(ST) \end{tikzcd}$$

Here, vertical arrows are natural surjections.

Now, we have:

$$\gamma' \begin{pmatrix} S \\ T \end{pmatrix} = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} + \sum_{i=1}^{\infty} \begin{pmatrix} a_{i,\,1} & a_{i,\,2} \\ b_{i,\,1} & b_{i,\,2} \end{pmatrix} \begin{pmatrix} S^i \\ T^i \end{pmatrix}.$$

If $a_0 \in \mathcal{O}_L^\times$, it is obvious that $\overline{\gamma'}(S) \in (k_L[[S,\, T]]/(ST))^\times$. On the other hand, the condition $\overline{\gamma'}(S) \cdot \overline{\gamma'}(T) = 0$ implies that $\overline{\gamma'}(T) = 0$, which is a contradiction. Therefore, $a_0 \in \mathfrak{M}_L$ and similarly, $b_0 \in \mathfrak{M}_L$. Since $\overline{\gamma'}$ is an automorphism of $k_L[[S,\, T]]/(ST)$, we have

$$\begin{pmatrix} \overline{a_{1,\,1}} & \overline{a_{1,\,2}} \\ \overline{b_{1,\,1}} & \overline{b_{1,\,2}} \end{pmatrix} \in \mathrm{GL}_2(k_L).$$

Thus,

$$\begin{pmatrix} a_{1,\,1} & a_{1,\,2} \\ b_{1,\,1} & b_{1,\,2} \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_L).$$

The product of $\gamma'(S)$ and $\gamma'(T)$ can be uniquely written in the following form:

$$\gamma'(S)\cdot\gamma'(T) = c_0 + \sum_{i=1}^{\infty}(c_{i,1}S^i + c_{i,2}T^i).$$

Here, $c_0,\ c_{i,j} \in \mathcal{O}_L\,(i \geq 1,\ j = 1,\ 2)$.

Easy calculation shows that:

$$\begin{aligned}
c_0 &= a_0 b_0 + \sum_{i=1}^{\infty}(a_{i,1}b_{i,2} + a_{i,2}b_{i,1})\pi^{ri},\\
c_{1,1} &= a_0 b_{1,1} + b_0 a_{1,1} + \sum_{i=1}^{\infty}(a_{i+1,1}b_{i,2} + a_{i+1,2}b_{i,1})\pi^{ri},\\
c_{k,1} &= a_0 b_{k,1} + b_0 a_{k,1} + \sum_{i=1}^{\infty}(a_{i+k,1}b_{i,2} + a_{i+k,2}b_{i,1})\pi^{ri} + \sum_{\substack{i+j=k\\ i,j\geq 1}} a_{i,1}b_{j,1}\ (k \geq 2),\\
c_{1,2} &= a_0 b_{1,2} + b_0 a_{1,2} + \sum_{i=1}^{\infty}(a_{i,1}b_{i+1,2} + a_{i,2}b_{i+1,1})\pi^{ri},\\
c_{k,2} &= a_0 b_{k,2} + b_0 a_{k,2} + \sum_{i=1}^{\infty}(a_{i,1}b_{i+k,2} + a_{i,2}b_{i+k,1})\pi^{ri} + \sum_{\substack{i+j=k\\ i,j\geq 1}} a_{i,2}b_{j,2}\ (k \geq 2).
\end{aligned}$$

(Note that $ST = \pi^r$.)

On the other hand, the condition $\gamma'(S)\cdot\gamma'(T) = \gamma'(\pi^r)$ implies that $c_0 = \gamma'(\pi^r)$, $c_{i,j} = 0\,(i \geq 1,\ j = 1,\ 2)$. Therefore,

$$\begin{pmatrix} c_{1,1} \\ c_{1,2} \end{pmatrix} \equiv \begin{pmatrix} b_{1,1} & a_{1,1} \\ b_{1,2} & a_{1,2} \end{pmatrix}\begin{pmatrix} a_0 \\ b_0 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \bmod\ \mathfrak{M}_L^r.$$

Since $\begin{pmatrix} a_{1,1} & a_{1,2} \\ b_{1,1} & b_{1,2} \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_L)$, we have $\begin{pmatrix} b_{1,1} & a_{1,1} \\ b_{1,2} & a_{1,2} \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_L)$ and

$$\begin{pmatrix} a_0 \\ b_0 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \bmod\ \mathfrak{M}_L^r.$$

This shows that:

$$\begin{pmatrix} c_{2,1} \\ c_{2,2} \end{pmatrix} \equiv \begin{pmatrix} a_{1,1}b_{1,1} \\ a_{1,2}b_{1,2} \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \bmod\ \mathfrak{M}_L^r.$$

On the other hand, since $\begin{pmatrix} a_{1,1} & a_{1,2} \\ b_{1,1} & b_{1,2} \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_L)$, one (and only one) of $a_{1,1}$, $b_{1,1}$ belongs to $\mathcal{O}_L^\times$ and one (and only one) of the following conditions holds:

(i) $a_{1,1} \in \mathcal{O}_L^\times$ and $b_{1,1} \in \mathfrak{M}_L^r$.

(ii) $a_{1,1} \in \mathfrak{M}_L^r$ and $b_{1,1} \in \mathcal{O}_L^\times$.

Similarly, one (and only one) of the following condition holds:

(i)′ $a_{1,2} \in \mathcal{O}_L^\times$ and $b_{1,2} \in \mathfrak{M}_L^r$.

(ii)′ $a_{1,2} \in \mathfrak{M}_L^r$ and $b_{1,2} \in \mathcal{O}_L^\times$.

The case where (i) holds.

Since $\begin{pmatrix} a_{1,1} & a_{1,2} \\ b_{1,1} & b_{1,2} \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_L)$, (ii)$'$ holds in this case.

We show that $a_{i,2} \in \mathfrak{M}_L^r$ $(i \geq 1)$ by induction on i. The case where $i = 1$ is already proved. Assuming that $a_{1,2}, \cdots, a_{i,2} \in \mathfrak{M}_L^r$, we show that $a_{i+1,2} \in \mathfrak{M}_L^r$. By assumption,

$$c_{i+2,2} \equiv a_{i+1,2} b_{1,2} \equiv 0 \mod \mathfrak{M}_L^r.$$

Since $b_{1,2} \in \mathcal{O}_L^\times$, we have $a_{i+1,2} \in \mathfrak{M}_L^r$.

Similar arguments show that $b_{i,1} \in \mathfrak{M}_L^r$ $(i \geq 1)$.

The case where (ii) holds.

Since $\begin{pmatrix} a_{1,1} & a_{1,2} \\ b_{1,1} & b_{1,2} \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_L)$, (i)$'$ holds in this case.

Similarly to the case where (i) holds, we obtain $a_{i,1}, b_{i,2} \in \mathfrak{M}_L^r$ $(i \geq 1)$ by induction. □

Definition 3.3.5
For $P \in \mathfrak{X}_{k_L}^{\mathrm{node}}(k_L)^G$, fix an isomorphism $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[S, T]]/(ST - \pi^r)$. For $\gamma' \in G$, $\gamma' \cdot S$ and $\gamma' \cdot T$ can be uniquely written in the following form:

$$\gamma' \begin{pmatrix} S \\ T \end{pmatrix} = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} + \sum_{i=1}^{\infty} \begin{pmatrix} a_{i,1} & a_{i,2} \\ b_{i,1} & b_{i,2} \end{pmatrix} \begin{pmatrix} S^i \\ T^i \end{pmatrix}.$$

We say that γ' is *of type (I)* (resp. *of type (II)*) *at* P (with respect to the isomorphism $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[S, T]]/(ST - \pi^r)$) if $a_0, b_0, a_{i,j}, b_{i,j} \in \mathcal{O}_L$ $(i \geq 1, j = 1, 2)$ satisfy the condition (i) (resp. (ii)) in Lemma 3.3.4.

Remark 3.3.6
For $P \in \mathfrak{X}_{k_L}^{\mathrm{node}}(k_L)^G$, the type of $\gamma' \in G$ at P with respect to an isomorphism $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[S, T]]/(ST - \pi^r)$ defined in Definition 3.3.5 is independent of the choice of the isomorphism. Indeed, a 2-element set which consists of irreducible components of $\mathrm{Spec}\,(\hat{\mathcal{O}}_{\mathfrak{X},P}/\mathfrak{M}_L\hat{\mathcal{O}}_{\mathfrak{X},P})$ is independent of the choice of the coordinates S, T. G acts on this 2-element set and the action of $\gamma' \in G$ on this set is trivial (resp. non-trivial) if and only if γ' is of type (I) (resp. of type (II)).

Remark 3.3.7
Assume that $\gamma' \in G$ is of type (II) at some $P \in \mathfrak{X}_{k_L}^{\mathrm{node}}(k_L)^G$ and denote the order of $\gamma' \in G$ by $\mathrm{ord}\,\gamma'$. Then, since $(\gamma')^{\mathrm{ord}\,\gamma'}(S) = S$, we have $\mathrm{ord}\,\gamma'$ is even. Moreover, the product of two elements of the same type is of type (I) and the product of two elements of different types is of type (II).

By replacing γ' in the above argument by γ^{-1}, we obtain:

$$\begin{pmatrix} (\gamma \cdot f_{(x,y)})(S) \\ (\gamma \cdot f_{(x,y)})(T) \end{pmatrix} = \begin{pmatrix} \gamma(f_{(x,y)}(\gamma^{-1}(S))) \\ \gamma(f_{(x,y)}(\gamma^{-1}(T))) \end{pmatrix} = \begin{pmatrix} \gamma(a_0) \\ \gamma(b_0) \end{pmatrix} + \sum_{i=1}^{\infty} \begin{pmatrix} \gamma(a_{i,1}) & \gamma(a_{i,2}) \\ \gamma(b_{i,1}) & \gamma(b_{i,2}) \end{pmatrix} \begin{pmatrix} \gamma(x^i) \\ \gamma(y^i) \end{pmatrix},$$

where $a_0 = a_{\gamma^{-1},0}$, $b_0 = b_{\gamma^{-1},0}$, $a_{i,j} = a_{\gamma^{-1},i,j}$, $b_{i,j} = b_{\gamma^{-1},i,j} \in \mathcal{O}_L$ $(i \geq 1, j = 1, 2)$. Therefore, if we identify $\rho^{-1}(P)$ with $A_r = \{(x, y) \in \mathfrak{M}_L \times \mathfrak{M}_L \mid xy = \pi^r\}$, the image

$[\gamma]\begin{pmatrix} x \\ y \end{pmatrix}$ of $(x,\, y) \in A_r$ by the action of $\gamma \in G$ can be written in the following form:

$$[\gamma]\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \gamma(a_0) \\ \gamma(b_0) \end{pmatrix} + \sum_{i=1}^{\infty} \begin{pmatrix} \gamma(a_{i,1}) & \gamma(a_{i,2}) \\ \gamma(b_{i,1}) & \gamma(b_{i,2}) \end{pmatrix} \begin{pmatrix} \gamma(x^i) \\ \gamma(y^i) \end{pmatrix}.$$

3.4. **Fixed points over $\mathfrak{X}^{\mathbf{sm}}_{k_L}(k_L)^G$.**

We follow the notations of the previous section. Moreover, we assume that X has log smooth reduction. That is to say, there exists a finite, Galois and tame extension L/K such that $X_L := X \times_{\operatorname{Spec} K} \operatorname{Spec} L$ has a stable model $\mathfrak{X}$. We may assume that all singular points of $\mathfrak{X}_{k_L}(k_L)$ are split.

Let K^{ur} be the maximal unramified extension of K in L and $\mathcal{O}_{K^{\mathrm{ur}}}$ the ring of integers of K^{ur}. Set $[L : K^{\mathrm{ur}}] = e$, $[K^{\mathrm{ur}} : K] = f$ (by assumption, e and p are coprime). Then, K^{ur} contains a primitive e-th root of unity. Furthermore, there exists a uniformizer π of $\mathcal{O}_L$ such that $L = K^{\mathrm{ur}}(\pi)$ and π^e is a uniformizer of $\mathcal{O}_{K^{\mathrm{ur}}}$.

In this case, $I = \mathrm{Gal}(L/K^{\mathrm{ur}})$ is a finite cyclic group and we fix a generator σ of I. There exists some $\tau \in G = \mathrm{Gal}(L/K)$ such that the image of the subgroup $\langle\tau\rangle \subset G$ by the natural surjection $G \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ur}}/K) \simeq \mathrm{Gal}(k_L/k)$ coincides with $\mathrm{Gal}(k_L/k)$. f divides the order of τ and we denote the order by $e_0 f$ (here, $e_0 \mid e$, in particular, $p \not| e_0$).

Until the end of this section, P will be an element of $\mathfrak{X}^{\mathrm{sm}}_{k_L}(k_L)^G$.

Lemma 3.4.1

For $\gamma \in G$ and $T \in \mathcal{O}_L[[T]] \simeq \hat{\mathcal{O}}_{\mathfrak{X},P}$, set:

$$\gamma^{-1}(T) = \sum_{i=0}^{\infty} a_i T^i,$$

where $a_i = a_{\gamma^{-1},i} \in \mathcal{O}_L$, $a_0 \in \mathfrak{M}_L$, $a_1 \in \mathcal{O}_L^{\times}$ (cf. Lemma 3.3.2). Then, for any $\nu \in \mathbb{Z}_{>0}$,

$$(\textit{the coefficient of } T \textit{ in } \gamma^{-\nu}(T)) \equiv \prod_{j=1}^{\nu} \gamma^{-(j-1)}(a_1) \mod \mathfrak{M}_L^{v(a_0)},$$

and

$$(\gamma^{-\nu}(T))|_{T=0} \equiv 0 \mod \mathfrak{M}_L^{v(a_0)}.$$

In particular,

$$(\textit{the coefficient of } T \textit{ in } \gamma^{-\nu}(T)) \equiv \prod_{j=1}^{\nu} \gamma^{-(j-1)}(a_1) \mod \mathfrak{M}_L.$$

Proof.

Use induction on ν. The assertion is obvious for $\nu = 1$.

For $\nu \geq 2$, assume that

$$(\text{the coefficient of } T \text{ in } \gamma^{-(\nu-1)}(T)) \equiv \prod_{j=1}^{\nu-1} \gamma^{-(j-1)}(a_1) \mod \mathfrak{M}_L^{v(a_0)}, \tag{3.1}$$

and that

$$(\gamma^{-(\nu-1)}(T))|_{T=0} \equiv 0 \mod \mathfrak{M}_L^{v(a_0)}. \tag{3.2}$$

Since

$$\begin{aligned}\gamma^{-\nu}(T) &= \gamma^{-(\nu-1)}\cdot\left(\sum_{i=0}^{\infty}a_iT^i\right)\\ &= \sum_{i=0}^{\infty}\gamma^{-(\nu-1)}(a_i)\cdot(\gamma^{-(\nu-1)}(T))^i,\end{aligned}$$

we have

$$\frac{d}{dT}\gamma^{-\nu}(T) = \sum_{i=0}^{\infty}\gamma^{-(\nu-1)}(a_i)\cdot i(\gamma^{-(\nu-1)}(T))^{i-1}\cdot\frac{d}{dT}\gamma^{-(\nu-1)}(T).$$

The coefficients of T in $\gamma^{-\nu}(T)$ is given by $\left.\left(\frac{d}{dT}\gamma^{-\nu}(T)\right)\right|_{T=0}$. By (3.1),

$$\left.\left(\frac{d}{dT}\gamma^{-(\nu-1)}(T)\right)\right|_{T=0} \equiv \prod_{j=1}^{\nu-1}\gamma^{-(j-1)}(a_1) \mod \mathfrak{M}_L^{v(a_0)}.$$

This and (3.2) show that

$$\begin{aligned}\left.\left(\frac{d}{dT}\gamma^{-\nu}(T)\right)\right|_{T=0} &= \sum_{i=0}^{\infty}\gamma^{-(\nu-1)}(a_i)\cdot i\left((\gamma^{-(\nu-1)}(T))|_{T=0}\right)^{i-1}\cdot\left.\left(\frac{d}{dT}\gamma^{-(\nu-1)}(T)\right)\right|_{T=0}\\ &\equiv \gamma^{-(\nu-1)}(a_1)\cdot\prod_{j=1}^{\nu-1}\gamma^{-(j-1)}(a_1) \mod \mathfrak{M}_L^{v(a_0)}.\end{aligned}$$

Therefore,

$$(\text{the coefficient of } T \text{ in } \gamma^{-\nu}(T)) \equiv \prod_{j=1}^{\nu}\gamma^{-(j-1)}(a_1) \mod \mathfrak{M}_L^{v(a_0)}.$$

Moreover,

$$(\gamma^{-\nu}(T))|_{T=0} \equiv \left.\left(\sum_{i=0}^{\infty}\gamma^{-(\nu-1)}(a_i)\cdot(\gamma^{-(\nu-1)}(T))^i\right)\right|_{T=0} \equiv 0 \mod \mathfrak{M}_L^{v(a_0)}.$$

□

Theorem 3.4.2
There exists some $T \in \hat{\mathcal{O}}_{\mathfrak{X},P}$ such that $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[T]]$ and

$$\begin{cases}\sigma^{-1}(T) &= \omega T,\\ \tau^{-1}(T) &= \dfrac{1}{u}T.\end{cases}$$

Here, $\omega \in \mathcal{O}_L^{\times}$ is an e-th root of unity (not necessarily primitive) and $u \in \mathcal{O}_L^{\times}$.

Proof.

Fix any $P \in \mathfrak{X}_{k_L}^{\mathrm{sm}}(k_L)^G$ and any isomorphism $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[T]]$. If we take a formal power series $T' \in \mathcal{O}_L[[T]]$ in T such that the constant term belongs to $\mathfrak{M}_L$ and the coefficient of T belongs to $\mathcal{O}_L^{\times}$, the homomorphism $\mathcal{O}_L[[T]] \to \mathcal{O}_L[[T]]$, $T \mapsto T'$ over $\mathcal{O}_L$

defines an automorphism of $\mathcal{O}_L[[T]]$. Then we have $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[T']]$ and may replace T' by T. This process allows us to change variable T so that the image of T by the action of G is less complicated.

Step 1.

Set $\sigma^{-1}(T) = \sum_{i=0}^{\infty} a_i T^i$ ($a_i = a_{\sigma^{-1},i} \in \mathcal{O}_L$). By Lemma 3.3.2, we have $a_0 \in \mathfrak{M}_L$, $a_1 \in \mathcal{O}_L^{\times}$. Since $\sigma^{-e}(T) = T$,

$$\prod_{j=1}^{e} \sigma^{-(j-1)}(a_1) \equiv 1 \mod \mathfrak{M}_L,$$

by lemma 3.4.1. As σ belongs to the inertia group, this shows that $a_1^e \equiv 1 \mod \mathfrak{M}_L$. Therefore, there exists an e-th root of unity $\omega \in K^{\mathrm{ur}}$ (not necessarily primitive) such that $a_1 \equiv \omega \mod \mathfrak{M}_L$.

Set:

$$T' = \omega^{e-1}T + \omega^{e-2}\sigma^{-1}(T) + \cdots + \omega\sigma^{-(e-2)}(T) + \sigma^{-(e-1)}(T) = \sum_{j=1}^{e} \omega^{e-j}\sigma^{-(j-1)}(T).$$

We regard T' as a formal power series in T. By the fact that $a_0 \in \mathfrak{M}_L$ and Lemma 3.4.1, it is clear that the constant term of T' belongs to $\mathfrak{M}_L$. As to the coefficient of T in T', by Lemma 3.4.1,

$$\begin{aligned}\text{(the coefficient of } T \text{ in } T') &\equiv \omega^{e-1}\cdot 1 + \omega^{e-2}\cdot a_1 + \cdots + \omega\cdot a_1^{e-2} + a_1^{e-1} \\ &\equiv \omega^{e-1}\cdot 1 + \omega^{e-2}\cdot \omega + \cdots + \omega\cdot\omega^{e-2} + \omega^{e-1} \\ &\equiv e\omega^{e-1} \mod \mathfrak{M}_L.\end{aligned}$$

(Note that $\sigma \in I$.) Since e and p are coprime, $e\omega^{e-1} \not\equiv 0 \mod \mathfrak{M}_L$. Thus, the coefficient of T in T' belongs to $\mathcal{O}_L^{\times}$.

As σ acts trivially on $\omega \in K^{\mathrm{ur}}$,

$$\sigma^{-1}(T') = \omega^{e-1}\sigma^{-1}(T) + \omega^{e-2}\sigma^{-2}(T) + \cdots + \omega\sigma^{-(e-1)}(T) + T = \omega T'.$$

Therefore, by changing variable T, the problem is reduced to the case where the action of σ^{-1} on $T \in \mathcal{O}_L[[T]] \simeq \hat{\mathcal{O}}_{\mathfrak{X},P}$ is given by $\sigma^{-1}(T) = \omega T$.

Step 2.

Consider the case where $\sigma^{-1}(T) = \omega T$. Since $I = \langle\sigma\rangle$ is a normal subgroup of G, there exists an integer $m \in \{0, 1, \cdots, e-1\}$ such that m and e are coprime and $\sigma^{-1}\tau^{-1} = \tau^{-1}\sigma^{-m}$. On the other hand, as $\tau^{-f} \in \mathrm{Ker}(G \to \mathrm{Gal}(K^{\mathrm{ur}}/K)) = \langle\sigma\rangle$, there exists an integer $n \in \{0, 1, \cdots, e-1\}$ such that $\tau^{-f} = \sigma^{-n}$.

Recall that a uniformizer π of $\mathcal{O}_L$ is an e-th root of a uniformizer of $\mathcal{O}_{K^{\mathrm{ur}}}$. So, there exists a primitive e-th root of unity $\zeta \in K^{\mathrm{ur}}$ such that $\sigma^{-1}(\pi) = \zeta\pi$. Since ω^{-1} is also an e-th root of unity, there exists an integer $\mu \in \{0, 1, \cdots, e-1\}$ such that $\zeta^{\mu} = \omega^{-1}$. Put $c = \pi^{\mu}$. Then, $\sigma^{-1}(c) = \omega^{-1}c$. Define $u \in \mathcal{O}_L^{\times}$ by $\tau^{-1}(c) = uc$.

Set $\tau^{-1}(T) = \sum_{i=0}^{\infty} a'_i T^i (a'_i = a'_{\tau^{-1},i} \in \mathcal{O}_L)$. By Lemma 3.3.2, we have $a'_0 \in \mathfrak{M}_L$, $a'_1 \in \mathcal{O}_L^{\times}$. Compare the coefficient of T in $\tau^{-f}(T) = \sigma^{-n}(T)$ by using Lemma 3.4.1. Then we have

$$\tau^{-(f-1)}(a'_1)\cdot\tau^{-(f-2)}(a'_1)\cdots\tau^{-1}(a'_1)\cdot a'_1\equiv\omega^n \mod \mathfrak{M}_L. \tag{3.3}$$

On the other hand,

$$\tau^{-f}(c)=\tau^{-(f-1)}(uc)=\cdots=\tau^{-(f-1)}(u)\cdot\tau^{-(f-2)}(u)\cdots\tau^{-1}(u)\cdot uc. \tag{3.4}$$

Since this is equal to $\sigma^{-n}(c)=\omega^{-n}c$,

$$\tau^{-(f-1)}(u)\cdot\tau^{-(f-2)}(u)\cdots\tau^{-1}(u)\cdot u=\omega^{-n}. \tag{3.5}$$

Set:

$$\begin{aligned}T' &= \frac{c}{c}dT+\frac{\tau^{-1}(c)}{c}\tau^{-1}(dT)+\cdots+\frac{\tau^{-(f-1)}(c)}{c}\tau^{-(f-1)}(dT)\\ &\quad+\frac{\tau^{-f}(c)}{c}\tau^{-f}(dT)+\cdots+\frac{\tau^{-(2f-1)}(c)}{c}\tau^{-(2f-1)}(dT)\\ &\quad+\cdots\\ &\quad+\frac{\tau^{-(e_0-1)f}(c)}{c}\tau^{-(e_0-1)f}(dT)+\cdots+\frac{\tau^{-(e_0f-1)}(c)}{c}\tau^{-(e_0f-1)}(dT)\\ &=\sum_{j=0}^{e_0f-1}\frac{\tau^{-j}(c)}{c}\tau^{-j}(dT),\end{aligned}$$

for some $d\in\mathcal{O}_{K^{\mathrm{ur}}}^{\times}$. We regard T' as a formal power series in T. We will show that by taking d appropriately, the constant term of T' belongs to $\mathfrak{M}_L$ and the coefficient of T in T' belongs to $\mathcal{O}_L^{\times}$. The former is obvious (for any d) from the fact that $a'_0\in\mathfrak{M}_L$ and Lemma 3.4.1. As to the latter, by Lemma 3.4.1 and (3.4),

$$\begin{aligned}&\left(\text{the coefficient of } T \text{ in } \frac{\tau^{-j}(c)}{c}\tau^{-j}(dT)\right)\\ &\equiv\tau^{-(j-1)}(u)\cdots\tau^{-1}(u)\cdot u\cdot\tau^{-j}(d)\cdot\tau^{-(j-1)}(a'_1)\cdots\tau^{-1}(a'_1)\cdot a'_1\\ &\equiv\tau^{-j}(d)\prod_{i=0}^{j-1}\tau^{-i}(ua'_1) \mod \mathfrak{M}_L,\end{aligned} \tag{3.6}$$

for each $0\le j\le e_0f-1$. Here, we set $\prod_{i=0}^{j-1}\tau^{-i}(ua'_1)=1$ for $j=0$. Note that (3.4) is still correct if we replace f by any positive integer.

By (3.6),

$$\begin{aligned}(\text{the coefficient of } T \text{ in } T')&\equiv\sum_{j=0}^{e_0f-1}\tau^{-j}(d)\cdot\prod_{i=0}^{j-1}\tau^{-i}(ua'_1)\\ &\equiv\sum_{k=0}^{e_0-1}\sum_{l=0}^{f-1}\tau^{-(kf+l)}(d)\cdot\prod_{i=0}^{kf+l-1}\tau^{-i}(ua'_1)\\ &\equiv\sum_{k=0}^{e_0-1}\sum_{l=0}^{f-1}\tau^{-(kf+l)}(d)\cdot\prod_{i=kf}^{kf+l-1}\tau^{-i}(ua'_1)\cdot\prod_{i=0}^{kf-1}\tau^{-i}(ua'_1) \mod \mathfrak{M}_L.\end{aligned}$$

This, together with (3.3) and (3.5), shows that

$$\begin{aligned}(\text{the coefficient of } T \text{ in } T') &\equiv \sum_{k=0}^{e_0-1}\sum_{l=0}^{f-1}\tau^{-l}(d)\cdot\prod_{i=0}^{l-1}\tau^{-i}(ua_1')\\ &\equiv \sum_{l=0}^{f-1}\left(e_0\prod_{i=0}^{l-1}\tau^{-i}(ua_1')\right)\tau^{-l}(d) \quad \mod \mathfrak{M}_L.\end{aligned}$$

(Note that $\tau^{-f}=\sigma^{-n}\in I$.)

Since e_0 and p are coprime, $e_0\prod_{i=0}^{l-1}\tau^{-i}(ua_1')\not\equiv 0 \mod \mathfrak{M}_L$ for each $0\le l\le f-1$. Denote the image of $\tau\in G$ in $\mathrm{Gal}(K^{\mathrm{ur}}/K)\simeq\mathrm{Gal}(k_L/k)$ by $\overline{\tau}$ and that of $a\in\mathcal{O}_L$ in k_L by $\overline{a}$. Then $\overline{\tau^{-0}}=\overline{\mathrm{id}}$, $\overline{\tau^{-1}}$, $\cdots$, $\overline{\tau^{-(f-1)}}$ are different elements of $\mathrm{Gal}(k_L/k)$. By the linear independence of automorphisms of a field [9, Lemma 2.9.9], there exists $\delta\in k_L^\times$ such that in k_L,

$$\sum_{l=0}^{f-1}\left(\overline{e_0}\prod_{i=0}^{l-1}\overline{\tau^{-i}}\left(\overline{ua_1'}\right)\right)\overline{\tau^{-l}}(\delta)\neq 0.$$

If we take $d\in\mathcal{O}_{K^{\mathrm{ur}}}^\times$ so that $\overline{d}=\delta$, the coefficient of T in T' belongs to $\mathcal{O}_L^\times$.

Consider the action of σ^{-1}, τ^{-1} on T'. For each $0\le j\le e_0f-1$,

$$\begin{aligned}\sigma^{-1}\left(\frac{\tau^{-j}(c)}{c}\tau^{-j}(dT)\right) &= \frac{\tau^{-j}\left(\sigma^{-m^j}(c)\right)}{\sigma^{-1}(c)}\tau^{-j}\left(\sigma^{-m^j}(dT)\right)\\ &= \frac{\tau^{-j}\left(\omega^{-m^j}c\right)}{\sigma^{-1}(c)}\tau^{-j}(\omega^{m^j}dT)\\ &= \frac{c}{\sigma^{-1}(c)}\cdot\frac{\tau^{-j}(c)}{c}\tau^{-j}(dT)\\ &= \omega\cdot\frac{\tau^{-j}(c)}{c}\tau^{-j}(dT).\end{aligned}$$

(Note that $\sigma^{-1}\tau^{-1}=\tau^{-1}\sigma^{-m}$). So, we have $\sigma^{-1}(T')=\omega T'$.

On the other hand, for each $0\le j\le e_0f-1$,

$$\begin{aligned}\tau^{-1}\left(\frac{\tau^{-j}(c)}{c}\tau^{-j}(dT)\right) &= \frac{\tau^{-(j+1)}(c)}{\tau^{-1}(c)}\tau^{-(j+1)}(dT)\\ &= \frac{c}{\tau^{-1}(c)}\cdot\frac{\tau^{-(j+1)}(c)}{c}\tau^{-(j+1)}(dT)\\ &= \frac{1}{u}\cdot\frac{\tau^{-(j+1)}(c)}{c}\tau^{-(j+1)}(dT).\end{aligned}$$

Thus, we have $\tau^{-1}(T')=\dfrac{1}{u}T'$.

Therefore, by changing variable T, the action of G on $\hat{\mathcal{O}}_{\mathfrak{X},P}\simeq\mathcal{O}_L[[T]]$ is given by $\sigma^{-1}(T)=\omega T$, $\tau^{-1}(T)=\dfrac{1}{u}T$.

□

Corollary 3.4.3
For $\rho' : \mathfrak{X}(\mathcal{O}_L)^G \to \mathfrak{X}_{k_L}(k_L)^G$, we have $\mathfrak{X}^{\mathrm{sm}}_{k_L}(k_L)^G \subset \rho'(\mathfrak{X}(\mathcal{O}_L)^G)$. Moreover, for each $P \in \mathfrak{X}^{\mathrm{sm}}_{k_L}(k_L)^G$, $\rho'^{-1}(P)$ is isomorphic to a ball of dimension 1 over K. In particular, $i_K(\rho'^{-1}(P)) \equiv 1 \mod (q-1)$.

Proof.

Fix any $P \in \mathfrak{X}^{\mathrm{sm}}_{k_L}(k_L)^G$. By Theorem 3.4.2, we may take an isomorphism $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[T]]$ such that $\sigma^{-1}(T) = \omega T$ and $\tau^{-1}(T) = \dfrac{1}{u}T$. We will construct an element of $\rho^{-1}(P) \simeq \mathfrak{M}_L$ fixed under the action of G. The action of σ, τ on $x \in \mathfrak{M}_L \simeq \rho^{-1}(P)$ is given by the following formulae:

$$[\sigma](x) = \sigma(\omega)\sigma(x) = \omega\sigma(x),$$
$$[\tau](x) = \frac{\tau(x)}{\tau(u)}.$$

Take a uniformizer π_K of K and set $x_0 = \dfrac{\pi_K}{c}$. Here, $c \in \mathcal{O}_L$ is defined as in Step 2 of the proof of Theorem 3.4.2. As c satisfies $0 \le v(c) \le e-1$, we have $x_0 \in \mathfrak{M}_L$ and $1 \le v(x_0) \le e$. x_0 satisfies the following formulae:

$$[\sigma](x_0) = \omega \cdot \frac{\pi_K}{\sigma(c)} = \omega \cdot \frac{\pi_K}{\omega c} = x_0,$$
$$[\tau](x_0) = \frac{1}{\tau(u)} \cdot \frac{\pi_K}{\tau(c)} = \frac{1}{\tau(u)} \cdot \pi_K \cdot \frac{\tau(u)}{c} = x_0.$$

Since G is generated by σ and τ, x_0 is fixed under the action of G and therefore, $\rho'^{-1}(P) \neq \emptyset$. This shows that $\mathfrak{X}^{\mathrm{sm}}_{k_L}(k_L)^G \subset \rho'(\mathfrak{X}(\mathcal{O}_L)^G)$.

Assume that two elements x_1, x_2 of $\mathfrak{M}_L$ fixed under G are given and that at least one of them is not equal to 0. Without loss of generality, we may assume that $v(x_1) \le v(x_2)$ (in particular, $x_1 \neq 0$). For each $i = 1, 2$, we have $\omega\sigma(x_i) = x_i$, $\dfrac{\tau(x_i)}{\tau(u)} = x_i$. So, $\sigma\left(\dfrac{x_2}{x_1}\right) = \dfrac{x_2}{x_1}$, $\tau\left(\dfrac{x_2}{x_1}\right) = \dfrac{x_2}{x_1}$. Thus, $x_2 \in \mathcal{O}_K x_1$. On the other hand, by the choice of x_0, we have $v(x_0) \le v(x)$ for all $x \in \mathfrak{M}_L$ fixed by the action of G. Indeed, suppose that $v(x_0) > v(x)$. Then, we have $x_0 \in \mathcal{O}_K x$ and $v(x_0) \ge v(x) + e \ge e + 1$, which contradicts the fact that $1 \le v(x_0) \le e$. Therefore, we obtain

$$\rho'^{-1}(P) = \rho^{-1}(P)^G \simeq \mathcal{O}_K x_0.$$

Clearly, this is isomorphic to a ball of dimension 1 over K.

□

3.5. Fixed points over $\mathfrak{X}^{\mathbf{node}}_{k_L}(k_L)^G$.

As in the previous section, assume that X has log smooth reduction.

Until the end of this section, P will be an element of $\mathfrak{X}^{\mathrm{node}}_{k_L}(k_L)^G$.

Lemma 3.5.1
Fix any $P \in \mathfrak{X}_{k_L}^{\mathrm{node}}(k_L)^G$ and any isomorphism $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[S,T]]/(ST-\pi^r)$. With respect to P and this isomorphism:

(i) *If $\gamma \in G$ is of type (I), there exists $U \in (\mathcal{O}_L[[S,T]]/(ST-\pi^r))^\times$ such that $\gamma(S) = US$, $\gamma(T) = \dfrac{\gamma(\pi^r)}{\pi^r}U^{-1}T$.*

(ii) *If $\gamma \in G$ is of type (II), there exists $U \in (\mathcal{O}_L[[S,T]]/(ST-\pi^r))^\times$ such that $\gamma(S) = UT$, $\gamma(T) = \dfrac{\gamma(\pi^r)}{\pi^r}U^{-1}S$.*

Proof.
Set:

$$\gamma(S) = a_0 + \sum_{i=1}^{\infty}(a_{i,1}S^i + a_{i,2}T^i),$$

where $a_0 = a_{\gamma,0}$, $a_{i,j} = a_{\gamma,i,j} \in \mathcal{O}_L$.

If $\gamma \in G$ is of type (I), a_0, $a_{i,2} \in \mathfrak{M}_L^r$ $(i \geq 1)$, $a_{1,1} \in \mathcal{O}_L^\times$ by Lemma 3.3.4. Therefore,

$$\gamma(S) = S\left(\sum_{i=1}^{\infty} a_{i,1}S^{i-1} + \frac{a_0}{\pi^r}T + \sum_{i=1}^{\infty}\frac{a_{i,2}}{\pi^r}T^{i+1}\right).$$

(Note that $ST = \pi^r$.) The fact that $a_{1,1} \in \mathcal{O}_L^\times$ implies that $U := \sum_{i=1}^{\infty} a_{i,1}S^{i-1} + \frac{a_0}{\pi^r}T + \sum_{i=1}^{\infty}\frac{a_{i,2}}{\pi^r}T^{i+1}$ belongs to $(\mathcal{O}_L[[S,T]]/(ST-\pi^r))^\times$. As $\gamma(S)\cdot\gamma(T) = \gamma(\pi^r)$, it is clear that $\gamma(T) = \dfrac{\gamma(\pi^r)}{\pi^r}U^{-1}T$.

If $\gamma \in G$ is of type (II), a_0, $a_{i,1} \in \mathfrak{M}_L^r$ $(i \geq 1)$, $a_{1,2} \in \mathcal{O}_L^\times$ by Lemma 3.3.4. Similarly to the case where γ is of type (I), we have:

$$\gamma(S) = T\left(\sum_{i=1}^{\infty} a_{i,2}T^{i-1} + \frac{a_0}{\pi^r}S + \sum_{i=1}^{\infty}\frac{a_{i,1}}{\pi^r}S^{i+1}\right).$$

The fact that $a_{1,2} \in \mathcal{O}_L^\times$ implies that $U := \sum_{i=1}^{\infty} a_{i,2}T^{i-1} + \frac{a_0}{\pi^r}S + \sum_{i=1}^{\infty}\frac{a_{i,1}}{\pi^r}S^{i+1}$ belongs to $(\mathcal{O}_L[[S,T]]/(ST-\pi^r))^\times$. As $\gamma(S)\cdot\gamma(T) = \gamma(\pi^r)$, it is clear that $\gamma(T) = \dfrac{\gamma(\pi^r)}{\pi^r}U^{-1}S$. □

Theorem 3.5.2
Fix any $P \in \mathfrak{X}_{k_L}^{\mathrm{node}}(k_L)^G$.

(i) *If σ^{-1} and τ^{-1} are of type (I) at P, there exist some $S, T \in \hat{\mathcal{O}}_{\mathfrak{X},P}$ and $u_1, u_2 \in \mathcal{O}_L^\times$ such that $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[S,T]]/(ST-\pi^r)$ and that*

$$\begin{cases}\sigma^{-1}(S) &= u_1 S,\\ \sigma^{-1}(T) &= \dfrac{\sigma^{-1}(\pi^r)}{\pi^r}u_1^{-1}T,\end{cases}\quad \begin{cases}\tau^{-1}(S) &= u_2 S,\\ \tau^{-1}(T) &= \dfrac{\tau^{-1}(\pi^r)}{\pi^r}u_2^{-1}T.\end{cases}$$

(ii) *Assume that p is odd. If σ^{-1} is of type (I) at P and if τ^{-1} is of type (II) at P, there exist some $S, T \in \hat{\mathcal{O}}_{\mathfrak{X}, P}$ and $u_3, u_4 \in \mathcal{O}_L^{\times}$ such that $\hat{\mathcal{O}}_{\mathfrak{X}, P} \simeq \mathcal{O}_L[[S, T]]/(ST - \pi^r)$ and that*

$$\begin{cases} \sigma^{-1}(S) & = u_3 S, \\ \sigma^{-1}(T) & = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r} u_3^{-1} T, \end{cases} \begin{cases} \tau^{-1}(S) & = u_4 T, \\ \tau^{-1}(T) & = \dfrac{\tau^{-1}(\pi^r)}{\pi^r} u_4^{-1} S. \end{cases}$$

(iii) *If σ^{-1} is of type (II) at P, then p is automatically odd and there exist $S, T \in \hat{\mathcal{O}}_{\mathfrak{X}, P}$ and $u_5, u_6 \in \mathcal{O}_L^{\times}$ such that $\hat{\mathcal{O}}_{\mathfrak{X}, P} \simeq \mathcal{O}_L[[S, T]]/(ST - \pi^r)$ and that*

$$\begin{cases} \sigma^{-1}(S) & = u_5 T, \\ \sigma^{-1}(T) & = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r} u_5^{-1} S, \end{cases} \begin{cases} \tau'^{-1}(S) & = u_6 S, \\ \tau'^{-1}(T) & = \dfrac{\tau'^{-1}(\pi^r)}{\pi^r} u_6^{-1} T. \end{cases}$$

Here,

$$\tau' = \begin{cases} \tau \ (\tau : \textit{of type (I) at } P), \\ \tau\sigma \ (\tau : \textit{of type (II) at } P). \end{cases}$$

Proof.

Fix any $P \in \mathfrak{X}_{k_L}^{\mathrm{node}}(k_L)^G$ and any isomorphism $\hat{\mathcal{O}}_{\mathfrak{X}, P} \simeq \mathcal{O}_L[[S, T]]/(ST - \pi^r)$. If we take an invertible element $U \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))^{\times}$, the homomorphism $\mathcal{O}_L[[S, T]]/(ST - \pi^r) \to \mathcal{O}_L[[S, T]]/(ST - \pi^r)$, $S \mapsto US =: S'$, $T \mapsto U^{-1}T =: T'$ over $\mathcal{O}_L$ defines an automorphism of $\mathcal{O}_L[[S, T]]/(ST - \pi^r)$. Then we have $\hat{\mathcal{O}}_{\mathfrak{X}, P} \simeq \mathcal{O}_L[[S', T']]/(S'T' - \pi^r)$ and may replace S', T' by S, T. This process allows us to change variables S, T so that the images of S, T by the action of G are less complicated.

As in Step 2 of the proof of Theorem 3.4.2, there exist integers $m \in \{0, 1, \cdots, e-1\}$ and $n \in \{0, 1, \cdots, e-1\}$ such that m and e are coprime, that $\sigma^{-1}\tau^{-1} = \tau^{-1}\sigma^{-m}$ and that $\tau^{-f} = \sigma^{-n}$.

First, we treat the case where σ^{-1} is of type (I) in Case 1. Under this assumption, we treat the case where τ^{-1} is of type (I) (resp. (II)) in Case 1.1 (resp. Case 1.2). Similarly, we treat the case where σ^{-1} is of type (II) in Case 2. Under this assumption, we treat the case where τ^{-1} is of type (I) (resp. (II)) in Case 2.1 (resp. Case 2.2). Case 2.1 is divided into Step 2.1.1 and Step 2.1.2.

Case 1. The case where σ^{-1} is of type (I).

Set:

$$\sigma^{-1}(S) = a_0 + \sum_{i=1}^{\infty} (a_{i,1} S^i + a_{i,2} T^i),$$

where $a_0 = a_{\sigma^{-1}, 0}$, $a_{i,j} = a_{\sigma^{-1}, i, j} \in \mathcal{O}_L$. By Lemma 3.3.4, we have $a_0, a_{i,2} \in \mathfrak{M}_L^r$ $(i \geq 1)$, $a_{1,1} \in \mathcal{O}_L^{\times}$. In particular,

$$\sigma^{-1}(S) \equiv \sum_{i=1}^{\infty} a_{i,1} S^i \mod \mathfrak{M}_L^r.$$

Since $\sigma^{-e}(S) = S$,

$$a_{1,1}^e \equiv 1 \mod \mathfrak{M}_L,$$

as in the proof of Lemma 3.4.1. Therefore, there exists an e-th root of unity $\omega \in K^{\mathrm{ur}}$ (not necessarily primitive) such that $a_{1,1} \equiv \omega \mod \mathfrak{M}_L$. As noted in Remark 3.3.3, the coefficient of S in $\sigma^{-1}(S)$ modulo $\mathfrak{M}_L^r$ is well-defined. So, as in Lemma 3.4.1, for any $\nu \in \mathbb{Z}_{>0}$,

$$(\text{the coefficient of } S \text{ in } \sigma^{-\nu}(S)) \equiv \prod_{j=1}^{\nu} \sigma^{-(j-1)}(a_{1,1}) \mod \mathfrak{M}_L^r. \tag{3.7}$$

Set:

$$S' = \omega^{e-1}S + \omega^{e-2}\sigma^{-1}(S) + \cdots + \omega\sigma^{-(e-2)}(S) + \sigma^{-(e-1)}(S) = \sum_{j=1}^{e} \omega^{e-j}\sigma^{-(j-1)}(S).$$

It is clear that $\sigma^{-1}(S') = \omega S'$.

By Lemma 3.5.1, $\sigma^{-1}(S) = US$ for some $U \in (\mathcal{O}_L[[S,\, T]]/(ST-\pi^r))^\times$, which allows us to set:

$$S' = S(\omega^{e-1} + \omega^{e-2}U + \omega^{e-3}U\sigma^{-1}(U) + \cdots + U\sigma^{-1}(U)\cdots\sigma^{-(e-2)}(U)) =: SU'.$$

We will show that U' is an invertible element of $\mathcal{O}_L[[S,\, T]]/(ST-\pi^r)$. It suffices to show that the coefficient of S in S' modulo $\mathfrak{M}_L$ (which is well-defined by Remark 3.3.3 and the fact that $r \geq 1$) is not 0. By (3.7) and the fact that $a_{1,1} \equiv \omega \mod \mathfrak{M}_L$,

$$(\text{the coefficient of } S \text{ in } S') \equiv \sum_{j=1}^{e} \omega^{e-j}\cdot\omega^{j-1} \equiv e\omega^{e-1} (\not\equiv 0) \mod \mathfrak{M}_L.$$

Thus, we have $U' \in (\mathcal{O}_L[[S,\, T]]/(ST-\pi^r))^\times$. Setting $S' = SU'$, $T' = TU'^{-1}$, we get $\sigma^{-1}(S') = \omega S'$, $\sigma^{-1}(T') = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r}\omega^{-1}T'$.

Therefore, by changing variables S, T, the problem is reduced to the case where the action of σ^{-1} on $S,\, T \in \mathcal{O}_L[[S,\, T]]/(ST-\pi^r) \simeq \hat{\mathcal{O}}_{\mathfrak{X},\, P}$ is given by $\sigma^{-1}(S) = \omega S$, $\sigma^{-1}(T) = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r}\omega^{-1}T$.

Case 1.1. The case where both σ^{-1} and τ^{-1} are of type (I).

By the argument in Case 1, we may assume that $\sigma^{-1}(S) = \omega S$, $\sigma^{-1}(T) = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r}\omega^{-1}T$.

As in Step 2 of the proof of Theorem 3.4.2, there exists an integer $\mu \in \{0,\, 1,\, \cdots,\, e-1\}$ such that $\sigma^{-1}(c) = \omega^{-1}c$, where $c = \pi^\mu$. Set $\tau^{-1}(c) = uc\,(u \in \mathcal{O}_L^\times)$.

Set:

$$\tau^{-1}(S) = a'_0 + \sum_{i=1}^{\infty}(a'_{i,1}S^i + a'_{i,2}T^i),$$

where $a'_0 = a'_{\tau^{-1},0}$, $a'_{i,j} = a'_{\tau^{-1},i,j} \in \mathcal{O}_L$. By Lemma 3.3.4, we have $a'_0,\, a'_{i,2} \in \mathfrak{M}_L^r$ $(i \geq 1)$, $a'_{1,1} \in \mathcal{O}_L^\times$.

Similarly to (3.7),

$$(\text{the coefficient of } S \text{ in } \tau^{-f}(S)) \equiv \prod_{j=1}^{f} \tau^{-(j-1)}(a'_{1,1}) \mod \mathfrak{M}_L^r.$$

Moreover, we have $\tau^{-f}(S) = \sigma^{-n}(S)$ and $\sigma^{-1}(S) = \omega S$. Therefore,

$$\prod_{j=1}^{f} \tau^{-(j-1)}(a'_{1,1}) \equiv \omega^n \mod \mathfrak{M}_L^r. \tag{3.8}$$

On the other hand,

$$\tau^{-f}(c) = \tau^{-(f-1)}(u) \cdots \tau^{-1}(u)uc.$$

Since we have $\sigma^{-1}(c) = \omega^{-1}c$ and $\tau^{-f}(c) = \sigma^{-n}(c)$,

$$\prod_{j=1}^{f} \tau^{-(j-1)}(u) = \omega^{-n}. \tag{3.9}$$

Set:

$$S' = \sum_{j=0}^{e_0 f-1} \frac{\tau^{-j}(c)}{c} \tau^{-j}(dS),$$

for some $d \in \mathcal{O}_{K^{\mathrm{ur}}}^{\times}$. We will show that by taking d appropriately, S' is a product of S and an invertible element (of $\mathcal{O}_L[[S, T]]/(ST - \pi^r)$). Indeed, by Lemma 3.5.1, $\tau^{-1}(S)$ is a product of S and an invertible element. So, it is clear that $S' \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))S$. Therefore, it suffices to show that the coefficient of S in S' modulo $\mathfrak{M}_L$ (which is well-defined by Remark 3.3.3 and the fact that $r \geq 1$) is not 0. By a similar argument to Step 2 of the proof of Theorem 3.4.2, we can easily check this (using (3.8) and (3.9)). Thus, there exists some $U' \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))^{\times}$ such that $S' = SU'$.

Again as in Step 2 of the proof of Theorem 3.4.2, we obtain $\sigma^{-1}(S') = \omega S'$, $\tau^{-1}(S') = \frac{1}{u}S'$.

Putting $T' = TU'^{-1}$, we get $\sigma^{-1}(T') = \frac{\sigma^{-1}(\pi^r)}{\pi^r}\omega^{-1}T'$, $\tau^{-1}(T') = \frac{\tau^{-1}(\pi^r)}{\pi^r}uT'$.

Therefore, by putting $u_1 = \omega$, $u_2 = \frac{1}{u}$ and changing variables S, T, the assertion (i) holds.

Case 1.2. The case where σ^{-1} is of type (I) and τ^{-1} is of type (II).

If f is odd, some power of τ^{-2}, which is of type (I), coincides with τ^{-1}, which contradicts Remark 3.3.7. So, f is even. Applying an argument similar to Case 1.1 to σ and τ^2, we may reduce the problem to the case where there exist some e-th root of unity ω and $u' \in \mathcal{O}_L^{\times}$ such that

$$\begin{cases} \sigma^{-1}(S) &= \omega S, \\ \sigma^{-1}(T) &= \dfrac{\sigma^{-1}(\pi^r)}{\pi^r}\omega^{-1}T, \end{cases} \begin{cases} \tau^{-2}(S) &= \dfrac{1}{u'}S, \\ \tau^{-2}(T) &= \dfrac{\tau^{-1}(\pi^r)}{\pi^r}u'T. \end{cases}$$

Furthermore, by Lemma 3.5.1, we can write $\tau^{-1}(S) = U'T$, $\tau^{-1}(T) = \frac{\tau^{-1}(\pi^r)}{\pi^r}U'^{-1}S$ for some $U' \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))^{\times}$.

Set:

$$\tau^{-1}(S) = a'_0 + \sum_{i=1}^{\infty}(a'_{i,1}S^i + a'_{i,2}T^i),$$

where $a'_0 = a'_{\tau^{-1},0}$, $a'_{i,j} = a'_{\tau^{-1},i,j} \in \mathcal{O}_L$. By Lemma 3.3.4, we have a'_0, $a'_{i,1} \in \mathfrak{M}_L^r$ $(i \geq 1)$, $a'_{1,2} \in \mathcal{O}_L^\times$. Then, by Lemma 3.5.1 and its proof, we can write U' in the following form:

$$U' = a'_{1,2} \times (1 + (\text{terms of degree at least 1 in } S,\, T)).$$

Each coefficient of Maclaurin series of $(1+x)^{1/2}$ is a rational number whose denominator is a power of 2, which belongs to $\mathcal{O}_L$ in the case where p is odd. Therefore, there exists $W' \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))^\times$ such that $U' = a'_{1,2}W'^2$.

Now, we have

$$\sigma^{-1}\tau^{-1}(S) = \sigma^{-1}(U'T) = \sigma^{-1}(U') \cdot \frac{\sigma^{-1}(\pi^r)}{\pi^r}\omega^{-1}T,$$

and

$$\tau^{-1}\sigma^{-m}(S) = \tau^{-1}(\omega^m S) = \tau^{-1}(\omega^m)U'T.$$

Since $\sigma^{-1}\tau^{-1} = \tau^{-1}\sigma^{-m}$, these show that

$$\frac{\sigma^{-1}(U')}{U'} = \tau^{-1}(\omega^m)\omega \cdot \frac{\pi^r}{\sigma^{-1}(\pi^r)}.$$

Thus,

$$\frac{\sigma^{-1}(W'^2)}{W'^2} = \tau^{-1}(\omega^m)\omega \cdot \frac{\pi^r a'_{1,2}}{\sigma^{-1}(\pi^r a'_{1,2})} \in \mathcal{O}_L^\times.$$

Set $w'_1 = \dfrac{\sigma^{-1}(W')}{W'} \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))^\times$. Then, as ${w'_1}^2 \in \mathcal{O}_L^\times$, we obtain $w'_1 \in \mathcal{O}_L^\times$.

On the other hand, since $\tau^{-1}(S) = U'T$, we have

$$\tau^{-2}(S) = \frac{\tau^{-1}(\pi^r U')}{\pi^r U'}S = \frac{\tau^{-1}(\pi^r a'_{1,2}W'^2)}{\pi^r a'_{1,2}W'^2}S.$$

Moreover, as $\tau^{-2}(S) = \dfrac{1}{u'}S$,

$$\frac{\tau^{-1}(W'^2)}{W'^2} = \frac{\pi^r a'_{1,2}}{\tau^{-1}(\pi^r a'_{1,2})} \cdot \frac{1}{u'} \in \mathcal{O}_L^\times.$$

As above, we obtain $w'_2 := \dfrac{\tau^{-1}(W')}{W'} \in \mathcal{O}_L^\times$.

Set $S' = \dfrac{S}{W'}$, $T' = W'T$. Then we have

$$\sigma^{-1}(S') = \frac{\sigma^{-1}(S)}{\sigma^{-1}(W')} = \frac{\omega S}{\sigma^{-1}(W')} = \omega \cdot \frac{W'}{\sigma^{-1}(W')} \cdot \frac{S}{W'} = \frac{\omega}{w'_1}S'.$$

Similarly, we get $\sigma^{-1}(T') = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r} \cdot \dfrac{w'_1}{\omega}T'$. On the other hand, we have

$$\tau^{-1}(S') = \frac{\tau^{-1}(S)}{\tau^{-1}(W')} = \frac{U'T}{\tau^{-1}(W')} = a'_{1,2} \cdot \frac{W'}{\tau^{-1}(W')} \cdot W'T = \frac{a'_{1,2}}{w'_2}T'.$$

Similarly, we get $\tau^{-1}(T') = \dfrac{\tau^{-1}(\pi^r)}{\pi^r} \cdot \dfrac{w'_2}{a'_{1,2}}S'$.

Therefore, by setting $u_3 = \dfrac{\omega}{w'_1}$, $u_4 = \dfrac{a'_{1,2}}{w'_2}$ and changing variables S, T, the assertion (ii) holds.

Case 2. The case where σ^{-1} is of type (II).

In this case, by Remark 3.3.7, e is even and we set $e = 2e'$. Since L/K is tame, σ^{-1} cannot be of type (II) if $p = 2$. So, we may assume that $p \neq 2$.

As σ^{-2} is of type (I), applying an argument similar to Case 1, we may assume that there exists an e'-th root of unity $\omega' \in \mathcal{O}_L^\times$ such that $\sigma^{-2}(S) = \omega' S$, $\sigma^{-2}(T) = \dfrac{\sigma^{-2}(\pi^r)}{\pi^r}\omega'^{-1}T$.

Set:

$$\sigma^{-1}(S) = a_0 + \sum_{i=1}^{\infty}(a_{i,1}S^i + a_{i,2}T^i),$$

where $a_0 = a_{\sigma^{-1},0}$, $a_{i,j} = a_{\sigma^{-1},i,j} \in \mathcal{O}_L$. By Lemma 3.3.4, we have a_0, $a_{i,1} \in \mathfrak{M}_L^r$ $(i \geq 1)$, $a_{1,2} \in \mathcal{O}_L^\times$. Then, by Lemma 3.5.1 and its proof, there exists some $U \in (\mathcal{O}_L[[S, T]]/(ST-\pi^r))^\times$ such that $\sigma^{-1}(S) = UT$, $\sigma^{-1}(T) = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r}U^{-1}S$ and we can write U in the following form:

$$U = a_{1,2} \times (1 + (\text{terms of degree at least 1 in } S,\, T)).$$

Since $p \neq 2$, there exists $W \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))^\times$ such that $U = a_{1,2}W^2$ as in Case 1.2.

As $\sigma^{-1}(S) = UT$, we have

$$\sigma^{-2}(S) = \frac{\sigma^{-1}(\pi^r U)}{\pi^r U}S = \frac{\sigma^{-1}(\pi^r a_{1,2}W^2)}{\pi^r a_{1,2}W^2}S.$$

On the other hand, since $\sigma^{-2}(S) = \omega' S$, we get

$$\frac{\sigma^{-1}(W^2)}{W^2} = \frac{\pi^r a_{1,2}}{\sigma^{-1}(\pi^r a_{1,2})}\omega' \in \mathcal{O}_L^\times.$$

Set $w = \dfrac{\sigma^{-1}(W)}{W} \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))^\times$. Then, as $w^2 \in \mathcal{O}_L^\times$, we obtain $w \in \mathcal{O}_L^\times$.

Set $S' = \dfrac{S}{W}$, $T' = WT$. Then we have

$$\sigma^{-1}(S') = \frac{\sigma^{-1}(S)}{\sigma^{-1}(W)} = \frac{UT}{\sigma^{-1}(W)} = a_{1,2} \cdot \frac{W}{\sigma^{-1}(W)} \cdot WT = \frac{a_{1,2}}{w}T'.$$

Similarly, we get $\sigma^{-1}(T') = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r} \cdot \dfrac{w}{a_{1,2}}S'$.

Therefore, by changing variables S, T, the problem is reduced to the case where the action of σ^{-1} on S, $T \in \mathcal{O}_L[[S, T]]/(ST-\pi^r) \simeq \hat{\mathcal{O}}_{\mathfrak{X},P}$ is given by $\sigma^{-1}(S) = \dfrac{a_{1,2}}{w}T$, $\sigma^{-1}(T) = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r} \cdot \dfrac{w}{a_{1,2}}S$.

Case 2.1. The case where σ^{-1} is of type (II) and τ^{-1} is of type (I).

Step 2.1.1.

By the above argument, we may assume that $\sigma^{-1}(S) = \dfrac{a_{1,2}}{w}T$, $\sigma^{-1}(T) = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r} \cdot \dfrac{w}{a_{1,2}}S$. Here, $a_{1,2}$, $w \in \mathcal{O}_L^\times$ and

$$w^2 = \frac{\pi^r a_{1,2}}{\sigma^{-1}(\pi^r a_{1,2})}\omega'. \tag{3.10}$$

By the definition of w, it is clear that $\prod_{i=0}^{e-1}\sigma^{-i}(w) = 1$. Thus, by Hilbert's Theorem 90, there exists $a \in \mathcal{O}_L$ such that $w = \dfrac{\sigma^{-1}(a)}{a}$. Let $\omega \in \mathcal{O}_L^\times$ be an e-th root of unity such that $\omega' = \omega^2$. As in Step 2 of the proof of Theorem 3.4.2, there exists an integer $\mu \in \{0, 1, \cdots, e-1\}$ such that $\sigma^{-1}(c) = \omega^{-1}c$, where $c = \pi^\mu$. Set $\tau^{-1}(c) = uc\,(u \in \mathcal{O}_L^\times)$.

Set:

$$\tau^{-1}(S) = a'_0 + \sum_{i=1}^{\infty}(a'_{i,1}S^i + a'_{i,2}T^i),$$

where $a'_0 = a'_{\tau^{-1},0}$, $a'_{i,j} = a'_{\tau^{-1},i,j} \in \mathcal{O}_L$. By Lemma 3.3.4, we have a'_0, $a'_{i,2} \in \mathfrak{M}_L^r$ $(i \geq 1)$, $a'_{1,1} \in \mathcal{O}_L^\times$.

Now, we have

$$\tau^{-f}(c) = \tau^{-(f-1)}(u)\cdots\tau^{-1}(u)uc.$$

Since $\sigma^{-1}(c) = \omega^{-1}c$ and $\tau^{-f}(c) = \sigma^{-n}(c)$,

$$\prod_{j=0}^{f-1}\tau^{-j}(u) = \omega^{-n}. \tag{3.11}$$

Set $\tau^{-1}(a) = ba\,(b \in \mathcal{O}_L^\times)$. As $\tau^{-f}(a) = \sigma^{-n}(a)$,

$$\prod_{j=0}^{f-1}\tau^{-j}(b) = \prod_{j=0}^{n-1}\sigma^{-j}(w). \tag{3.12}$$

On the other hand,

$$\sigma^{-2}(S) = \sigma^{-1}\left(\frac{a_{1,2}}{w}T\right) = \frac{w}{\sigma^{-1}(w)} \cdot \frac{\sigma^{-1}(\pi^r a_{1,2})}{\pi^r a_{1,2}}S.$$

This and (3.10) show that

$$\sigma^{-2}(S) = \frac{\omega'}{\sigma^{-1}(w)w}S. \tag{3.13}$$

Note that σ^{-1} is of type (II) and τ^{-1} is of type (I) in the equality $\sigma^{-n} = \tau^{-f}$. Thus, Remark 3.3.7 shows that n is even and we set $n = 2n'$. As $\sigma \in I$, the coefficient of S in $\sigma^{-2n'}(S) = \tau^{-f}(S)$ modulo $\mathfrak{M}_L$ is written in the following form by (3.13):

$$\frac{\omega'^{n'}}{w^{2n'}} \equiv \prod_{i=0}^{f-1}\tau^{-i}(a'_{1,1}) \mod \mathfrak{M}_L.$$

Therefore, this, together with (3.11) and (3.12), shows that

$$\prod_{i=0}^{f-1} \tau^{-i}(a'_{1,1}ub) \equiv \frac{\omega'^{n'}}{w^{2n'}} \cdot \omega^{-n} \cdot w^{n} \equiv 1 \quad \bmod \mathfrak{M}_L. \tag{3.14}$$

(Note that $\omega' = \omega^2$.)

Set:

$$S' = \sum_{j=0}^{e_0 f-1} \frac{\tau^{-j}(ac)}{ac} \tau^{-j}(dS),$$

for some $d \in \mathcal{O}_{K^{\mathrm{ur}}}^{\times}$. We will show that by taking d appropriately, S' is a product of S and an invertible element (of $\mathcal{O}_L[[S, T]]/(ST - \pi^r)$). Indeed, by Lemma 3.5.1, $\tau^{-1}(S)$ is a product of S and an invertible element. So, it is clear that $S' \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))S$. Therefore, it suffices to show that the coefficient of S in S' modulo $\mathfrak{M}_L$ (which is well-defined by Remark 3.3.3 and the fact that $r \geq 1$) is not 0.

Similarly to Lemma 3.4.1, the coefficient of S in $\dfrac{\tau^{-1}(ac)}{ac}\tau^{-j}(dS)$ $(0 \leq j \leq e_0 f - 1)$ satisfies the following formula:

$$\left(\text{the coefficient of } S \text{ in } \frac{\tau^{-j}(ac)}{ac}\tau^{-j}(dS)\right) \equiv \tau^{-j}(d) \prod_{i=0}^{j-1} \tau^{-i}(a'_{1,1}ub) \quad \bmod \mathfrak{M}_L. \tag{3.15}$$

Here, we set $\prod_{i=0}^{j-1} \tau^{-i}(a'_{1,1}ub) = 1$ for $j = 0$.

By (3.15),

$$\begin{aligned}
&(\text{the coefficient of } S \text{ in } S') \\
&\equiv \sum_{j=0}^{e_0 f-1} \tau^{-j}(d) \cdot \prod_{i=0}^{j-1} \tau^{-i}(a'_{1,1}ub) \\
&\equiv \sum_{k=0}^{e_0-1} \sum_{l=0}^{f-1} \tau^{-(kf+l)}(d) \cdot \prod_{i=0}^{kf+l-1} \tau^{-i}(a'_{1,1}ub) \\
&\equiv \sum_{k=0}^{e_0-1} \sum_{l=0}^{f-1} \tau^{-(kf+l)}(d) \cdot \prod_{i=kf}^{kf+l-1} \tau^{-i}(a'_{1,1}ub) \cdot \prod_{i=0}^{kf-1} \tau^{-i}(a'_{1,1}ub) \quad \bmod \mathfrak{M}_L.
\end{aligned}$$

This, together with (3.14) and the fact that $\tau^{-f} = \sigma^{-n} \in I$, shows that

$$\begin{aligned}
(\text{the coefficient of } S \text{ in } S') &\equiv \sum_{k=0}^{e_0-1} \sum_{l=0}^{f-1} \tau^{-l}(d) \cdot \prod_{i=0}^{l-1} \tau^{-i}(a'_{1,1}ub) \\
&\equiv \sum_{l=0}^{f-1} \left(e_0 \prod_{i=0}^{l-1} \tau^{-i}(a'_{1,1}ub) \right) \tau^{-l}(d) \quad \bmod \mathfrak{M}_L.
\end{aligned}$$

Since e_0 and p are coprime, $e_0 \prod_{i=0}^{l-1} \tau^{-i}(a'_{1,1}ub) \not\equiv 0 \mod \mathfrak{M}_L$ for each $0 \leq l \leq f-1$. Thus, similarly to Step 2 of the proof of Theorem 3.4.2, there exists some $\delta \in k_L^\times$ such that in k_L,

$$\sum_{l=0}^{f-1} \left(\overline{e_0} \prod_{i=0}^{l-1} \overline{\tau^{-i}} \left(\overline{a'_{1,1}ub} \right) \right) \overline{\tau^{-l}}(\delta) \neq 0.$$

If we take $d \in \mathcal{O}_{K^{\mathrm{ur}}}^\times$ so that $\overline{d} = \delta$, the coefficient of S in S' is not 0 modulo $\mathfrak{M}_L$.

Therefore, there exists $U' \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))^\times$ such that $S' = SU'$. Setting $T' = U'^{-1}T$, we consider the action of σ^{-2}, τ^{-1} on S', T'. By (3.13) and the fact that $\sigma^{-1}\tau^{-1} = \tau^{-1}\sigma^{-m}$, for each $0 \leq j \leq e_0 f - 1$,

$$\begin{aligned}
&\sigma^{-2}\left(\frac{\tau^{-j}(ac)}{ac} \tau^{-j}(dS) \right) \\
&= \frac{\tau^{-j}(\sigma^{-2m^j}(ac))}{\sigma^{-2}(ac)} \tau^{-j}(\sigma^{-2m^j}(dS)) \\
&= \frac{\tau^{-j}(\sigma^{-(2m^j-1)}(w) \cdots \sigma^{-1}(w)wa \cdot \omega^{-2m^j}c)}{\sigma^{-2}(ac)} \cdot \tau^{-j}(d) \cdot \tau^{-j} \left(\frac{\omega'^{m^j}}{\sigma^{-(2m^j-1)}(w) \cdots \sigma^{-1}(w)w} S \right) \\
&= \frac{\tau^{-j}(ac)}{\sigma^{-2}(ac)} \tau^{-j}(dS) \\
&= \frac{ac}{\sigma^{-2}(ac)} \cdot \frac{\tau^{-j}(ac)}{ac} \tau^{-j}(dS) \\
&= \frac{\omega^2}{\sigma^{-1}(w)w} \cdot \frac{\tau^{-j}(ac)}{ac} \tau^{-j}(dS) \\
&= \frac{\omega'}{\sigma^{-1}(w)w} \cdot \frac{\tau^{-j}(ac)}{ac} \tau^{-j}(dS).
\end{aligned}$$

So, we obtain $\sigma^{-2}(S') = \dfrac{\omega'}{\sigma^{-1}(w)w} S'$. Similarly, we get $\sigma^{-2}(T') = \dfrac{\sigma^{-2}(\pi^r)}{\pi^r} \cdot \dfrac{\sigma^{-1}(w)w}{\omega'} T'$.

On the other hand, for each $0 \leq j \leq e_0 f - 1$,

$$\begin{aligned}
\tau^{-1}\left(\frac{\tau^{-j}(ac)}{ac} \tau^{-j}(dS) \right) &= \frac{\tau^{-(j+1)}(ac)}{\tau^{-1}(ac)} \tau^{-(j+1)}(dS) \\
&= \frac{ac}{\tau^{-1}(ac)} \cdot \frac{\tau^{-(j+1)}(ac)}{ac} \tau^{-(j+1)}(dS) \\
&= \frac{1}{ub} \cdot \frac{\tau^{-(j+1)}(ac)}{ac} \tau^{-(j+1)}(dS).
\end{aligned}$$

So, we obtain $\tau^{-1}(S') = \dfrac{1}{ub} S'$. Similarly, we get $\tau^{-1}(T') = \dfrac{\tau^{-1}(\pi^r)}{\pi^r} ubT'$.

Therefore, by changing variables S, T, the problem is reduced to the case where the action of σ^{-2}, τ^{-1} on S, $T \in \mathcal{O}_L[[S, T]]/(ST - \pi^r) \simeq \hat{\mathcal{O}}_{\mathfrak{X}, P}$ is given by:

$$\begin{cases} \sigma^{-2}(S) & = \dfrac{\omega'}{\sigma^{-1}(w)w}S, \\ \sigma^{-2}(T) & = \dfrac{\sigma^{-2}(\pi^r)}{\pi^r} \cdot \dfrac{\sigma^{-1}(w)w}{\omega'}T, \end{cases} \begin{cases} \tau^{-1}(S) & = \dfrac{1}{ub}S, \\ \tau^{-1}(T) & = \dfrac{\tau^{-1}(\pi^r)}{\pi^r}ubT. \end{cases}$$

Step 2.1.2.

By the above argument, we may assume that $\sigma^{-2}(S) = \dfrac{\omega'}{\sigma^{-1}(w)w}S$, $\sigma^{-2}(T) = \dfrac{\sigma^{-2}(\pi^r)}{\pi^r} \cdot \dfrac{\sigma^{-1}(w)w}{\omega'}T$ and $\tau^{-1}(S) = \dfrac{1}{ub}S$, $\tau^{-1}(T) = \dfrac{\tau^{-1}(\pi^r)}{\pi^r}ubT$.

Set:

$$\sigma^{-1}(S) = a_0 + \sum_{i=1}^{\infty}(a''_{i,1}S^i + a''_{i,2}T^i)$$

where $a''_0 = a''_{\sigma^{-1},0}$, $a''_{i,j} = a''_{\sigma^{-1},i,j} \in \mathcal{O}_L$. By Lemma 3.3.4, we have a''_0, $a''_{i,1} \in \mathfrak{M}_L^r$ $(i \geq 1)$, $a''_{1,2} \in \mathcal{O}_L^\times$. Then, by Lemma 3.5.1 and its proof, we can write $\sigma^{-1}(S) = U''T$, $\sigma^{-1}(T) = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r}U''^{-1}S$ for some $U'' \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))^\times$ and

$$U'' = a''_{1,2} \times (1 + (\text{terms of degree at least 1 in } S, T)).$$

Since $p \neq 2$, there exists $W'' \in (\mathcal{O}_L[[S, T]]/(ST - \pi^r))^\times$ such that $U'' = a''_{1,2}W''^2$ as in Case 1.2.

As $\sigma^{-1}(S) = U''T$, we have

$$\sigma^{-2}(S) = \frac{\sigma^{-1}(\pi^r U'')}{\pi^r U''}S = \frac{\sigma^{-1}(\pi^r a''_{1,2}W''^2)}{\pi^r a''_{1,2}W''^2}S.$$

On the other hand, since $\sigma^{-2}(S) = \dfrac{\omega'}{\sigma^{-1}(w)w}S$, we get

$$\frac{\sigma^{-1}(W''^2)}{W''^2} = \frac{\pi^r a''_{1,2}}{\sigma^{-1}(\pi^r a''_{1,2})} \cdot \frac{\omega'}{\sigma^{-1}(w)w} \in \mathcal{O}_L^\times.$$

Similarly to the argument in Case 1.2, we obtain $w''_1 := \dfrac{\sigma^{-1}(W'')}{W''} \in \mathcal{O}_L^\times$.

Now, we have $\sigma^{-1}\tau^{-1} = \tau^{-1}\sigma^{-m}$. Furthermore, m and $e = 2e'$ are coprime. So, m is odd and we set $m = 2m' + 1$. Comparing

$$\sigma^{-1}\tau^{-1}(S) = \sigma^{-1}\left(\frac{1}{ub}S\right) = \frac{U''T}{\sigma^{-1}(ub)} = \frac{a''_{1,2}W''^2}{\sigma^{-1}(ub)}T$$

and

$$\begin{aligned}\tau^{-1}\sigma^{-m}(S) &= \tau^{-1}(\sigma^{-m}(S))\\ &= \tau^{-1}\sigma^{-1}(\sigma^{-2m'}(S))\\ &= \tau^{-1}\sigma^{-1}\left(\frac{\omega'^{m'}}{\sigma^{-(2m'-1)}(w)\cdots\sigma^{-1}(w)w}S\right)\\ &= \tau^{-1}\left(\frac{\omega'^{m'}}{\sigma^{-2m'}(w)\cdots\sigma^{-1}(w)}U''T\right)\\ &= \tau^{-1}\left(\frac{\omega'^{m'}}{\sigma^{-2m'}(w)\cdots\sigma^{-1}(w)}\right)\cdot\tau^{-1}(a''_{1,2}W''^2)\cdot\frac{\tau^{-1}(\pi^r)}{\pi^r}ubT,\end{aligned}$$

we get

$$\frac{\tau^{-1}(W''^2)}{W''^2} = \tau^{-1}\left(\frac{\sigma^{-2m'}(w)\cdots\sigma^{-1}(w)}{\omega'^{m'}}\right)\cdot\frac{\pi^r a''_{1,2}}{\tau^{-1}(\pi^r a''_{1,2})}\cdot\frac{1}{\sigma^{-1}(ub)ub}\in\mathcal{O}_L^\times.$$

As above, we obtain $w''_2 := \dfrac{\tau^{-1}(W'')}{W''}\in\mathcal{O}_L^\times$.

Set $S' = \dfrac{S}{W''}$, $T' = W''T$. Then we have

$$\sigma^{-1}(S') = \frac{\sigma^{-1}(S)}{\sigma^{-1}(W'')} = \frac{U''T}{\sigma^{-1}(W'')} = a''_{1,2}\cdot\frac{W''}{\sigma^{-1}(W'')}\cdot W''T = \frac{a''_{1,2}}{w''_1}T'.$$

Similarly, we get $\sigma^{-1}(T') = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r}\cdot\dfrac{w''_1}{a''_{1,2}}S'$. Moreover, we obtain

$$\tau^{-1}(S') = \frac{\tau^{-1}(S)}{\tau^{-1}(W'')} = \frac{1}{\tau^{-1}(W'')}\cdot\frac{1}{ub}S = \frac{W''}{\tau^{-1}(W'')}\cdot\frac{1}{ub}\cdot\frac{S}{W''} = \frac{1}{w''_2 ub}S'.$$

Similarly, we get $\tau^{-1}(T') = \dfrac{\tau^{-1}(\pi^r)}{\pi^r}\cdot w''_2 ubT'$.

Therefore, by setting $u_5 = \dfrac{a''_{1,2}}{w''_1}$, $u_6 = \dfrac{1}{w''_2 ub}$ and changing variables S, T, the assertion (iii) holds in the case where τ^{-1} is of type (I).

Case 2.2. The case where both σ^{-1} and τ^{-1} are of type (II).

In this case, by Remark 3.3.7, $\sigma^{-1}\tau^{-1}$ is of type (I). Moreover, $\langle\sigma^{-1}\tau^{-1}\rangle$ surjects to $\mathrm{Gal}(k_L/k)$. Therefore, by replacing τ^{-1} by $\sigma^{-1}\tau^{-1}$, we can reduce this case to Case 2.1. □

Remark 3.5.3

We use the condition that $p \neq 2$ to prove Theorem 3.5.2(ii). The author at the time of writing does not know whether a similar assertion holds in the case where $p = 2$.

Corollary 3.5.4

If p is odd, for any $P\in\mathfrak{X}^{\mathrm{node}}_{k_L}(k_L)^G$, $i_K(\rho'^{-1}(P))\equiv 0$ or $2 \mod (q-1)$. In particular, $i_K(\rho'^{-1}(P))\equiv 0 \mod 2$ (since p is odd, we have $2\,|\,(q-1)$).

Proof.

Fix any $P \in \mathfrak{X}_{k_L}^{\mathrm{node}}(k_L)^G$ and take an isomorphism $\hat{\mathcal{O}}_{\mathfrak{X},P} \simeq \mathcal{O}_L[[S, T]]/(ST - \pi^r)$.

Case 1. The case where both σ^{-1} and τ^{-1} are of type (I).

By Theorem 3.5.2, we may assume that there exist $u_1, u_2 \in \mathcal{O}_L^\times$ such that $\sigma^{-1}(S) = u_1 S$, $\sigma^{-1}(T) = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r} u_1^{-1} T$ and $\tau^{-1}(S) = u_2 S$, $\tau^{-1}(T) = \dfrac{\tau^{-1}(\pi^r)}{\pi^r} u_2^{-1} T$. We will show that $i_K(\rho'^{-1}(P)) \equiv 0 \mod (q-1)$. (Here, $\rho'^{-1}(P) = \rho^{-1}(P)^G$ is the G-invariant subset of $\rho^{-1}(P) \simeq \{(x, y) \in \mathfrak{M}_L \times \mathfrak{M}_L \mid xy = \pi^r\} =: A_r$.) The action of σ, τ on $(x, y) \in A_r \simeq \rho^{-1}(P)$ is given by the following formulae:

$$[\sigma]\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \sigma(u_1 x) \\ \dfrac{\pi^r}{\sigma(\pi^r)}\sigma(u_1^{-1} y) \end{pmatrix},$$
$$[\tau]\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \tau(u_2 x) \\ \dfrac{\pi^r}{\tau(\pi^r)}\tau(u_2^{-1} y) \end{pmatrix}.$$

If $\rho'^{-1}(P) = \rho^{-1}(P)^G = \emptyset$, it is clear that $i_K(\rho'^{-1}(P)) \equiv 0 \mod (q-1)$. So, we may assume that $\rho'^{-1}(P) \neq \emptyset$.

Consider two elements (x_1, y_2), (x_2, y_2) of A_r with $v(x_1) \leq v(x_2)$ and assume that (x_1, y_1) is fixed under G. If (x_2, y_2) is also fixed under G, then for each $i = 1, 2$, we have $\sigma(u_1 x_i) = x_i$, $\tau(u_2 x_i) = x_i$. So, $\sigma\left(\dfrac{x_2}{x_1}\right) = \dfrac{x_2}{x_1}$, $\tau\left(\dfrac{x_2}{x_1}\right) = \dfrac{x_2}{x_1}$. Thus, $x_2 \in \mathcal{O}_K x_1$. Conversely, if $x_2 \in \mathcal{O}_K x_1$, then (x_2, y_2) is fixed under G.

We fix any $(x_0, y_0) \in A_r^G$ such that $v(x_0) = \min_{(x,y) \in A_r^G} v(x)$. Then we have

$$\begin{aligned} \rho'^{-1}(P) &= \rho^{-1}(P)^G \\ &\simeq \{x \in \mathfrak{M}_L \setminus \mathfrak{M}_L^r \mid (x, \pi^r/x) \text{ is fixed under } G\} \\ &\simeq \coprod_{\substack{i \geq 0 \\ ie + v(x_0) < r}} (\mathfrak{M}_K^i \setminus \mathfrak{M}_K^{i+1}) x_0. \end{aligned}$$

For each $i \geq 0$, we have $i_K(\mathfrak{M}_K^i \setminus \mathfrak{M}_K^{i+1}) \equiv 0 \mod (q-1)$ by Example 2.1.24. Now, it is clear that $i_K(\rho'^{-1}(P)) \equiv 0 \mod (q-1)$.

Case 2. The case where σ^{-1} is of type (I) and τ^{-1} is of type (II).

By Theorem 3.5.2, we may assume that there exist $u_3, u_4 \in \mathcal{O}_L^\times$ such that $\sigma^{-1}(S) = u_3 S$, $\sigma^{-1}(T) = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r} u_3^{-1} T$ and $\tau^{-1}(S) = u_4 T$, $\tau^{-1}(T) = \dfrac{\tau^{-1}(\pi^r)}{\pi^r} u_4^{-1} S$. We will show that $i_K(\rho'^{-1}(P)) \equiv 0$ or $2 \mod (q-1)$. (Here, $\rho'^{-1}(P) = \rho^{-1}(P)^G$ is the G-invariant subset of $\rho^{-1}(P) \simeq A_r$.) The action of σ, τ on $(x, y) \in A_r \simeq \rho^{-1}(P)$ is given by the following formulae:

$$[\sigma]\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \sigma(u_3 x) \\ \dfrac{\pi^r}{\sigma(\pi^r)}\sigma(u_3^{-1}y) \end{pmatrix},$$

$$[\tau]\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \tau\,(u_4 y) \\ \dfrac{\pi^r}{\tau(\pi^r)}\tau\,(u_4^{-1}x) \end{pmatrix}.$$

If $\rho'^{-1}(P) = \rho^{-1}(P)^G = \emptyset$, it is clear that $i_K(\rho'^{-1}(P)) \equiv 0 \mod (q-1)$. So, we may assume that $\rho^{-1}(P)^G \neq \emptyset$.

Consider two elements (x_1, y_2), (x_2, y_2) of A_r with $v(x_1) \leq v(x_2)$ and assume that (x_1, y_1) is fixed under G. If (x_2, y_2) is also fixed under G, then for each $i = 1, 2$, we have $\sigma(u_3 x_i) = x_i$, $\tau\,(u_4 y_i) = x_i$. So, $\sigma\left(\dfrac{x_2}{x_1}\right) = \dfrac{x_2}{x_1}$, $\tau\left(\dfrac{y_2}{y_1}\right) = \dfrac{x_2}{x_1}$. Since $\dfrac{y_2}{y_1} = \dfrac{x_1}{x_2}$, we have $\tau\left(\dfrac{x_1}{x_2}\right) = \dfrac{x_2}{x_1}$. Thus, r is even and $v(x_1) = v(x_2)$. We set $z = \dfrac{x_2}{x_1} \in \mathcal{O}_L$. Then we have $\sigma(z) = z$ and $\tau(z) = z^{-1}$. Conversely, if $z := \dfrac{x_2}{x_1} \in \mathcal{O}_L$ satisfies $\sigma(z) = z$ and $\tau(z) = z^{-1}$, then (x_2, y_2) is fixed under G.

Consider an element $z \in \mathcal{O}_L$ satisfying $\sigma(z) = z$ and $\tau(z) = z^{-1}$. The former implies that $z \in \mathcal{O}_{K^{\mathrm{ur}}}$ and the latter implies that $z \in \mathcal{O}_L^\times$ and $\tau^2(z) = z$. Denote the intermediate field which corresponds to $\langle \sigma, \tau^2 \rangle \subset G$ by M. M/K is an unramified Galois extension of degree 2. Let $\mathcal{O}_M$ be the ring of integers of M, $\mathfrak{M}_M$ the maximal ideal of $\mathcal{O}_M$ and $k_M = \mathcal{O}_M/\mathfrak{M}_M$ the residue field. By Kummer theory, there exists some $\xi \in \mathcal{O}_K^\times$ such that $M = K(\sqrt{\xi})$ and that $\mathcal{O}_M = \mathcal{O}_K \oplus \sqrt{\xi}\mathcal{O}_K$

We have isomorphisms $\mathcal{O}_M^\times \simeq (1 + \mathfrak{M}_M) \times k_M^\times$ and $\mathcal{O}_K^\times \simeq (1 + \mathfrak{M}_K) \times k^\times$. The restriction of the norm $N_{M/K}|_{\mathcal{O}_M^\times} : \mathcal{O}_M^\times \to \mathcal{O}_K^\times$ sends $(a, b) \in (1 + \mathfrak{M}_M) \times k_M^\times$ to $(N_{M/K}(a), N_{k_M/k}(b)) = (\tau(a)a, b^{q+1}) \in (1 + \mathfrak{M}_K) \times k^\times$. We will consider the kernel of $N_{M/K}|_{\mathcal{O}_M^\times}$.

Set $a = \alpha + \sqrt{\xi}\beta \in 1 + \mathfrak{M}_M$ $(\alpha, \beta \in \mathcal{O}_K)$. Then we have $\alpha \in 1 + \mathfrak{M}_K$ and $\beta \in \mathfrak{M}_K$. If $N_{M/K}(a) = 1$, we obtain

$$\alpha^2 - \xi\beta^2 = 1 \Longleftrightarrow \alpha^2 = 1 + \xi\beta^2.$$

Since $p \neq 2$, $1 + \xi\beta^2 \in \mathcal{O}_K$ has square roots in $\mathcal{O}_K$ and one and only one of them belongs to $1 + \mathfrak{M}_K$. This implies that each $\beta \in \mathfrak{M}_K$ uniquely determines $\alpha \in 1 + \mathfrak{M}_K$ such that $\alpha^2 - \xi\beta^2 = 1$. Thus, there exists a bijection between the kernel of the restriction to $1 + \mathfrak{M}_M$ of $N_{M/K}$ and $\mathfrak{M}_K$. On the other hand, we have $|\mathrm{Ker}\, N_{k_M/k}| = q + 1$ since $N_{k_M/k}$ is surjective. Therefore, there exists a bijection between $\mathrm{Ker}\, N_{M/K}|_{\mathcal{O}_M^\times}$ and the disjoint union of $q + 1$ copies of $\mathfrak{M}_K$.

The above argument shows that if there exists $(x_0, y_0) \in A_r$ fixed under G, the G-invariant subset of A_r is given by:

$$\{(zx_0, z^{-1}y_0) \,|\, z \in \mathcal{O}_M^\times, N_{M/K}(z) = 1\}.$$

Thus, there exists a bijection between this set and $\operatorname{Ker} N_{M/K}|_{\mathcal{O}_M^\times}$. Now, it is clear that $i_K(\rho'^{-1}(P)) \equiv q+1 \equiv 2 \mod (q-1)$.

Case 3. The case where σ^{-1} is of type (II).

By Theorem 3.5.2, by replacing τ by $\tau\sigma$ if necessary, we may assume that there exist u_5, $u_6 \in \mathcal{O}_L^\times$ such that $\sigma^{-1}(S) = u_5 T$, $\sigma^{-1}(T) = \dfrac{\sigma^{-1}(\pi^r)}{\pi^r} u_5^{-1} S$ and $\tau^{-1}(S) = u_6 S$, $\tau^{-1}(T) = \dfrac{\tau^{-1}(\pi^r)}{\pi^r} u_6^{-1} T$. We will show that $i_K(\rho'^{-1}(P)) \equiv 0$ or $2 \mod (q-1)$. (Here, $\rho'^{-1}(P) = \rho^{-1}(P)^G$ is the G-invariant subset of $\rho^{-1}(P) \simeq A_r$.) The action of σ, τ on $(x,\, y) \in A_r \simeq \rho^{-1}(P)$ is given by the following formulae:

$$[\sigma]\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \sigma(u_5 y) \\ \dfrac{\pi^r}{\sigma(\pi^r)}\sigma\left(u_5^{-1} x\right) \end{pmatrix},$$

$$[\tau]\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \tau(u_6 x) \\ \dfrac{\pi^r}{\tau(\pi^r)}\tau(u_6^{-1} y) \end{pmatrix}.$$

If $\rho'^{-1}(P) = \rho^{-1}(P)^G = \emptyset$, it is clear that $i_K(\rho'^{-1}(P)) \equiv 0 \mod (q-1)$. So, we may assume that $\rho^{-1}(P)^G \neq \emptyset$.

Consider two elements $(x_1,\, y_2)$, $(x_2,\, y_2)$ of A_r with $v(x_1) \leq v(x_2)$ and assume that $(x_1,\, y_1)$ is fixed under G. If $(x_2,\, y_2)$ is also fixed under G, then for each $i = 1, 2$, we have $\sigma(u_5 y_i) = x_i$, $\tau(u_6 x_i) = x_i$. So, $\sigma\left(\dfrac{y_2}{y_1}\right) = \dfrac{x_2}{x_1}$, $\tau\left(\dfrac{x_2}{x_1}\right) = \dfrac{x_2}{x_1}$. Since $\dfrac{y_2}{y_1} = \dfrac{x_1}{x_2}$, we have $\sigma\left(\dfrac{x_1}{x_2}\right) = \dfrac{x_2}{x_1}$. Thus, r is even and $v(x_1) = v(x_2)$. We set $z = \dfrac{x_2}{x_1} \in \mathcal{O}_L$. Then we have $\sigma(z) = z^{-1}$ and $\tau(z) = z$. Conversely, if $z := \dfrac{x_2}{x_1} \in \mathcal{O}_L$ satisfies $\sigma(z) = z^{-1}$ and $\tau(z) = z$, then $(x_2,\, y_2)$ is fixed under G.

Consider an element $z \in \mathcal{O}_L$ satisfying $\sigma(z) = z^{-1}$ and $\tau(z) = z$. The former implies that $z \in \mathcal{O}_L^\times$ and $\sigma^2(z) = z$. Denote the intermediate field which corresponds to $\langle \sigma^2,\, \tau \rangle \subset G$ by M. Let $\mathcal{O}_M$ be the ring of integers of M and $\mathfrak{M}_M$ the maximal ideal of $\mathcal{O}_M$. The residue field of M is $\mathcal{O}_M/\mathfrak{M}_M \simeq k$. In this case, there exists a uniformizer π_K of $\mathcal{O}_K$ such that $M = K(\sqrt{\pi_K})$ and that $\mathcal{O}_M = \mathcal{O}_K \oplus \sqrt{\pi_K}\mathcal{O}_K$.

We have isomorphisms $\mathcal{O}_M^\times \simeq (1+\mathfrak{M}_M) \times k^\times$ and $\mathcal{O}_K \simeq (1+\mathfrak{M}_K) \times k^\times$. The restriction to $\mathcal{O}_M^\times$ of the norm $N_{M/K}|_{\mathcal{O}_M^\times} : \mathcal{O}_M^\times \to \mathcal{O}_K^\times$ sends $(a,\, b) \in (1+\mathfrak{M}_M) \times k^\times$ to $(N_{M/K}(a),\, b^2) = (\sigma(a)a,\, b^2) \in (1+\mathfrak{M}_K) \times k^\times$. We will consider the kernel of $N_{M/K}|_{\mathcal{O}_M^\times}$.

Set $a = \alpha + \sqrt{\pi_K}\beta \in 1+\mathfrak{M}_M$ $(\alpha,\, \beta \in \mathcal{O}_K)$. Then we have $\alpha \in 1+\mathfrak{M}_K$. If $N_{M/K}(a) = 1$, we obtain

$$\alpha^2 - \pi_K\beta^2 = 1 \Longleftrightarrow \alpha^2 = 1 + \pi_K\beta^2.$$

Since $p \neq 2$, $1+\pi_K\beta^2 \in \mathcal{O}_K$ has square roots in $\mathcal{O}_K$ and one and only one of them belongs to $1+\mathfrak{M}_K$. This implies that each $\beta \in \mathcal{O}_K$ uniquely determines $\alpha \in 1+\mathfrak{M}_K$ such that $\alpha^2 - \pi_K\beta^2 = 1$. Thus, there exists a bijection between the kernel of the restriction to $1+\mathfrak{M}_M$ of $N_{M/K}$ and $\mathcal{O}_K$. On the other hand, the kernel of $k \ni b \mapsto b^2$ is

$\{\pm 1\}$. Therefore, there exists a bijection between $\mathrm{Ker} N_{M/K}|_{\mathcal{O}_M^\times}$ and the disjoint union of 2 copies of $\mathcal{O}_K$.

The above argument shows that if there exists $(x_0, y_0) \in A_r$ fixed under G, the G-invariant subset of A_r is given by:

$$\{(zx_0,\, z^{-1}y_0) \,|\, z \in \mathcal{O}_M^\times,\, N_{M/K}(z) = 1\}.$$

Thus, there exists a bijection between this set and $\mathrm{Ker} N_{M/K}|_{\mathcal{O}_M^\times}$. Now, it is clear that $i_K(\rho'^{-1}(P)) \equiv 2 \mod (q-1)$.

□

Corollary 3.5.5
If p is odd,

$$i_K(X(K)) \equiv \sharp \mathfrak{X}_{k_L}^{\mathrm{sm}}(k_L)^G \mod 2.$$

Proof.
Immediate from Corollary 3.4.3 and Corollary 3.5.4.

□

Remark 3.5.6
Corollary 3.5.5 holds without assuming that all singular points of $\mathfrak{X}_{k_L}(k_L)$ are split. Indeed, let L/K be a finite extension such that singular points of $\mathfrak{X}_{k_L}(k_L)$ are not necessarily split (where $\mathfrak{X}$ is the stable model of X_L). Then, there exists a finite unramified extension L'/L such that $\mathfrak{X}' := \mathfrak{X} \times_{\mathrm{Spec}\,\mathcal{O}_L} \mathrm{Spec}\,\mathcal{O}_{L'}$ is the stable model of $X_{L'} := X_L \times_{\mathrm{Spec}\,L} \mathrm{Spec}\,L'$ and that all singular points of $\mathfrak{X}'_{k_{L'}}(k_{L'})$ are split. (Here, $\mathcal{O}_{L'}$ is the ring of integers of L' and $k_{L'}$ is the residue field.) We may assume that L' is Galois over K.

Set $G' := \mathrm{Gal}(L'/K)$ and $N := \mathrm{Gal}(L'/L)$. We have

$$\mathfrak{X}'_{k_{L'}} = (\mathfrak{X} \times_{\mathrm{Spec}\,\mathcal{O}_L} \mathrm{Spec}\,\mathcal{O}_{L'}) \times_{\mathrm{Spec}\,\mathcal{O}_{L'}} \mathrm{Spec}\,k_{L'} = \mathfrak{X}_{k_L} \times_{\mathrm{Spec}\,k_L} \mathrm{Spec}\,k_{L'}.$$

Since N acts trivially on $\mathfrak{X}_{k_L}$, the fact that $\mathfrak{X}_{k_L}^{\mathrm{sm}}(k_{L'}) = \mathfrak{X}'^{\mathrm{sm}}_{k_{L'}}(k_{L'})$ shows that

$$(\mathfrak{X}'^{\mathrm{sm}}_{k_{L'}}(k_{L'}))^N = (\mathfrak{X}_{k_L}^{\mathrm{sm}}(k_{L'}))^N = \mathfrak{X}_{k_L}^{\mathrm{sm}}(k_{L'}^N) = \mathfrak{X}_{k_L}^{\mathrm{sm}}(k_L).$$

Therefore, we have

$$(\mathfrak{X}'^{\mathrm{sm}}_{k_{L'}}(k_{L'}))^{G'} = ((\mathfrak{X}'^{\mathrm{sm}}_{k_{L'}}(k_{L'}))^N)^G = (\mathfrak{X}_{k_L}^{\mathrm{sm}}(k_L))^G.$$

This shows that we can reduce to the case where all singular points of $\mathfrak{X}_{k_L}(k_L)$ are split.

4. An application to anabelian geometry

In this chapter, we apply the arguments in Chapter 2 and Chapter 3 to anabelian geometry. We review some general facts on arithmetic fundamental groups in Section 4.1. In Section 4.2, assuming that we are given an isomorphism between arithmetic fundamental groups of hyperbolic curves over finite extensions of $\mathbb{Q}_p$, we show that the isomorphism arises from a unique isomorphism of schemes if the i-invariants of the sets of rational points of hyperbolic curves and their coverings "coincide" in some sense. In Section 4.3, assuming that p is odd and that we are given an isomorphism of arithmetic fundamental groups of hyperbolic curves which have log smooth reduction, the i-invariants of the sets of rational points of these curves coincide modulo 2.

4.1. Some general facts on arithmetic fundamental groups.

Let κ be a field, κ^{sep} a separable closure of κ and S a geometrically connected scheme of finite type over κ. Take any geometric point $\overline{s}$ of $S_{\kappa^{\mathrm{sep}}} := S \times_{\operatorname{Spec}\kappa} \operatorname{Spec}\kappa^{\mathrm{sep}}$. The image of $\overline{s}$ in S will be also denoted by $\overline{s}$. Let $\pi_1(S, \overline{s})$ (resp. $\pi_1(S_{\kappa^{\mathrm{sep}}}, \overline{s})$) be the étale fundamental group of S (resp. $S_{\kappa^{\mathrm{sep}}}$) with base point $\overline{s}$ and $G_\kappa = \mathrm{Gal}(\kappa^{\mathrm{sep}}/\kappa)$ the absolute Galois group of κ. Then, we have the following natural exact sequence of profinite groups:

$$1 \to \pi_1(S_{\kappa^{\mathrm{sep}}}, \overline{s}) \to \pi_1(S, \overline{s}) \to G_\kappa \to 1. \tag{4.1}$$

We sometimes call $\pi_1(S, \overline{s})$ (resp. $\pi_1(S_{\kappa^{\mathrm{sep}}}, \overline{s})$) the arithmetic fundamental group (resp. the geometric fundamental group) of S.

Remark 4.1.1
The isomorphism classes (as topological groups) of the étale fundamental groups $\pi_1(S, \overline{s})$ and $\pi_1(S_{\kappa^{\mathrm{sep}}}, \overline{s})$ are independent of the choice of the geometric point $\overline{s}$. In the following, unless otherwise noted, we fix any base point and omit it (e.g. $\pi_1(S)$, $\pi_1(S_{\kappa^{\mathrm{sep}}})$, etc.).

Let p be a prime number, K a finite extension of $\mathbb{Q}_p$, $\overline{K}$ an algebraic closure of K, $\mathcal{O}_K$ the ring of integers of K, $\mathfrak{M}_K$ the maximal ideal of $\mathcal{O}_K$, $k = \mathcal{O}_K/\mathfrak{M}_K$ the residue field of $\mathcal{O}_K$ and q the cardinality of k. Let U be a smooth and geometrically connected hyperbolic curve over K, X the smooth compactification of U and g the genus of X. Set $S := X \setminus U$ and $n := \sharp S(\overline{K})$. Then we have $2g + n - 2 > 0$. We denote the function field of U by K_U.

Set $U_{\overline{K}} := U \times_{\operatorname{Spec} K} \operatorname{Spec}\overline{K}$. The following is the exact sequence (4.1) with respect to U (and its geometric point $\operatorname{Spec}\overline{K_U} \to U$):

$$1 \to \pi_1(U_{\overline{K}}) \to \pi_1(U) \overset{\mathrm{pr}}{\to} G_K \to 1. \tag{4.2}$$

Let $\widetilde{K_U}$ be the maximal algebraic extension of K_U unramified on U. Then we may naturally identify (4.2) with the following exact sequence:

$$1 \to \mathrm{Gal}(\widetilde{K_U}/K_U \cdot \overline{K}) \to \mathrm{Gal}(\widetilde{K_U}/K_U) \to \mathrm{Gal}(K_U \cdot \overline{K}/K_U)\,(\simeq G_K) \to 1. \tag{4.3}$$

We denote the integral closure of U (resp. X) in $\widetilde{K_U}$ by $\widetilde{U}$ (resp. $\widetilde{X}$). Let $\widetilde{X}^{\mathrm{cl}}$ be the set of closed points of $\widetilde{X}$.

Definition 4.1.2 (cf. [18, §2])
For each $\widetilde{x} \in \widetilde{X}^{\mathrm{cl}}$, we denote the residue field at $\widetilde{x}$ by $k(\widetilde{x})$. We define the *decomposition group* $D_{\widetilde{x}}$ of $\widetilde{x}$ and the *inertia group* $I_{\widetilde{x}}$ of $\widetilde{x}$ by:

$$\begin{aligned} D_{\widetilde{x}} &= \{\gamma \in \pi_1(U) \mid \gamma(\widetilde{x}) = \widetilde{x}\}, \\ I_{\widetilde{x}} &= \{\gamma \in D_{\widetilde{x}} \mid \gamma \text{ acts trivially on } k(\widetilde{x})\}. \end{aligned}$$

For each open subgroup $\mathcal{H} \subset \pi_1(U)$, let $U_{\mathcal{H}}$ be the covering of U corresponding to $\mathcal{H}$ and $K_{\mathcal{H}}$ the integral closure of K in $U_{\mathcal{H}}$. Then $U_{\mathcal{H}}$ is a smooth and geometrically connected hyperbolic curve over $K_{\mathcal{H}}$. We denote the residue field of $K_{\mathcal{H}}$ by $k_{\mathcal{H}}$ and set $q_{\mathcal{H}} := \sharp k_{\mathcal{H}}$. Let $X_{\mathcal{H}}$ be the smooth compactification of $U_{\mathcal{H}}$ and $g_{\mathcal{H}}$ the genus of $X_{\mathcal{H}}$. Set $S_{\mathcal{H}} := X_{\mathcal{H}} \setminus U_{\mathcal{H}}$ and $n_{\mathcal{H}} := \sharp S_{\mathcal{H}}(\overline{K})$.

Definition 4.1.3 (cf. [18, Definition 2.3])
Let $G \subset G_K$ be an open subgroup, $\iota : G \to G_K$ the natural inclusion and $\mathrm{pr} : \pi_1(U) \twoheadrightarrow G_K$ the natural surjection. Let $\mathcal{H} \subset \pi_1(U)$ be an open subgroup.

(i) We define

$$\mathcal{S}(G) := \{s \in \mathrm{Hom}_{\mathrm{cont}}(G, \pi_1(U)) \,|\, \mathrm{pr} \circ s = \iota\},$$
$$\mathcal{S}_{\mathcal{H}}(G) := \{s \in \mathcal{S}(G) \,|\, s(G) \subset \mathcal{H}\}.$$

We refer to an element of $\mathcal{S}(G)$ as *section.*

(ii) We say that a section $s \in \mathcal{S}_{\mathcal{H}}(G)$ is *geometric* if its image $s(G)$ is contained in $D_{\widetilde{x}}$ for some $\widetilde{x} \in \widetilde{X}^{\mathrm{cl}}$. We denote the set of geometric sections in $\mathcal{S}_{\mathcal{H}}(G)$ by $\mathcal{S}_{\mathcal{H}}(G)^{\mathrm{geom}}$, and $\mathcal{S}_{\pi_1(U)}(G)^{\mathrm{geom}}$ simply by $\mathcal{S}(G)^{\mathrm{geom}}$.

Remark 4.1.4
In the situation of Definition 4.1.3(ii), let x be the image of $\widetilde{x}$ in X and $k(x)$ the residue field at x. Then, if $x \in U$ and $G = G_{k(x)}$, we have $D_{\widetilde{x}} = s(G)$.

4.2. **Reconstruction of decomposition groups from i-invariants.**

For $i = 1, 2$, let p_i be a prime number, K_i a finite extension of $\mathbb{Q}_{p_i}$, $\overline{K_i}$ an algebraic closure of K_i, $\mathcal{O}_{K_i}$ the ring of integers of K_i, $\mathfrak{M}_{K_i}$ the maximal ideal of $\mathcal{O}_{K_i}$, $k_i = \mathcal{O}_{K_i}/\mathfrak{M}_{K_i}$ the residue field of $\mathcal{O}_{K_i}$ and q_i the cardinality of k_i. Let U_i be a smooth and geometrically connected hyperbolic curve over K_i, X_i the smooth compactification of U_i and g_i the genus of X_i. Set $S_i := X_i \setminus U_i$ and $n_i := \sharp S_i(\overline{K_i})$.

In the following, assume that we are given an isomorphism of profinite groups $\alpha : \pi_1(U_1) \xrightarrow{\sim} \pi_1(U_2)$. By [6, Lemma 1.3.8], there exists an isomorphism of profinite groups $\alpha_K : G_{K_1} \xrightarrow{\sim} G_{K_2}$ such that the following diagram is commutative:

$$\begin{tikzcd}
\pi_1(U_1) \arrow[r, "\sim", "\alpha"'] \arrow[d, "\mathrm{pr}_1"'] & \pi_1(U_2) \arrow[d, "\mathrm{pr}_2"] \\
G_{K_1} \arrow[r, "\sim", "\alpha_K"'] & G_{K_2}
\end{tikzcd}$$

Here, $\mathrm{pr}_1 : \pi_1(U_1) \to G_{K_1}$ and $\mathrm{pr}_2 : \pi_1(U_2) \to G_{K_2}$ are natural surjections.

Proposition 4.2.1 (cf. [6, Proposition 1.2.1])
Suppose that we are given an isomorphism of profinite groups:

$$\alpha_K : G_{K_1} \xrightarrow{\sim} G_{K_2}.$$

Then:

(i) *We have $p_1 = p_2$. Thus, we shall write $p = p_1 = p_2$.*

(ii) *α_K induces an isomorphism $I_{K_1} \xrightarrow{\sim} I_{K_2}$ between the respective inertia subgroups of G_{K_1}, G_{K_2}.*

(iii) *We have $[K_1 : \mathbb{Q}_p] = [K_2 : \mathbb{Q}_p]$ and $[k_1 : \mathbb{F}_p] = [k_2 : \mathbb{F}_p]$. In particular, the ramification indices of K_1, K_2 over $\mathbb{Q}_p$ coincide.*

This proposition shows that $p_1 = p_2$ and $q_1 = q_2$. Thus, we shall write $p = p_1 = p_2$ and $q = q_1 = q_2$.

The following theorem reduces the absolute p-adic Grothendieck conjecture to the group-theoretic characterization of decomposition groups:

Theorem 4.2.2 (cf. [8, Corollary 2.9])
Suppose that an isomorphism of profinite groups $\alpha : \pi_1(U_1) \overset{\sim}{\to} \pi_1(U_2)$ satisfies the following condition: A closed subgroup of $\pi_1(U_1)$ is the decomposition group of a point of $\widetilde{X_1}^{\mathrm{cl}}$ if and only if the image of the subgroup by α is the decomposition group of a point of $\widetilde{X_2}^{\mathrm{cl}}$. Then α is geometric, i.e., arises from a unique isomorphism of schemes $U_1 \overset{\sim}{\to} U_2$ (more precisely, $\widetilde{U_1} \overset{\sim}{\to} \widetilde{U_2}$).

Remark 4.2.3
The original statement of Corollary 2.9 of [8] is stronger than that of Theorem 4.2.2. More precisely, the following result is proved there: Let Σ_i be a set of primes such that $\sharp\Sigma_i \geq 2$ and that $p_i \in \Sigma_i$, Δ_i the maximal pro-Σ_i quotient of $\pi_1(U_i \times_{\mathrm{Spec}\,K_i} \mathrm{Spec}\,\overline{K_i})$ and Π_i the quotient of $\pi_1(U_i)$ by the kernel of the natural surjection $\pi_1(U_i \times_{\mathrm{Spec}\,K_i} \mathrm{Spec}\,\overline{K_i}) \twoheadrightarrow \Delta_i$. If an isomorphism of profinite groups $\Pi_1 \overset{\sim}{\to} \Pi_2$ preserves decomposition groups in the sense as in the statement of Theorem 4.2.2, then this isomorphism is geometric.

On the other hand, the following theorem reduces the group-theoretic characterization of decomposition groups to the group-theoretic determination of whether or not the sets of rational points of hyperbolic curves are empty:

Theorem 4.2.4 (cf. [18, Corollary 2.10])
The map $\widetilde{x}_i \mapsto D_{\widetilde{x}_i}$ from $\widetilde{X_i}^{\mathrm{cl}}$ to the set of closed subgroups of $\pi_1(U_i)$ is injective. For each open subgroup $G_i \subset G_{K_i}$, $\mathcal{S}(G_i)^{\mathrm{geom}} \subset \mathcal{S}(G_i)$ is characterized by:

$s_i \in \mathcal{S}(G_i)^{\mathrm{geom}} \iff (X_i)_{\mathcal{H}_i}(L_i) \neq \emptyset$ *for all open subgroups* $\mathcal{H}_i \subset \pi_1(U_i)$ *such that* $s_i(G_i) \subset \mathcal{H}_i$.

Here, $L_i = \overline{K_i}^{G_i}$.

Moreover, suppose that the commutative diagram

$$\begin{tikzcd}
\pi_1(U_1) \arrow[r, "\sim", "\alpha"'] \arrow[d, ->>, "\mathrm{pr}_1"'] & \pi_1(U_2) \arrow[d, ->>, "\mathrm{pr}_2"] \\
G_{K_1} \arrow[r, "\sim", "\alpha_K"'] & G_{K_2}
\end{tikzcd}$$

satisfies the following condition: For all open subgroups $G_1 \subset G_{K_1}$ and all $s_1 \in \mathcal{S}(G_1)$, we have:

$$s_1 \in \mathcal{S}(G_1)^{\mathrm{geom}} \iff \alpha \circ s_1 \circ \alpha_K^{-1} \in \mathcal{S}(\alpha_K(G_1))^{\mathrm{geom}}.$$

Then a closed subgroup of $\pi_1(U_1)$ is the decomposition group of a point of $\widetilde{X_1}^{\mathrm{cl}}$ if and only if the image of the closed subgroup by α is the decomposition group of a point of $\widetilde{X_2}^{\mathrm{cl}}$.

Remark 4.2.5
In the original statement of Corollary 2.10 of [18], an explicit characterization of decomposition groups by using the data on whether or not the hyperbolic curve and its coverings admit rational points is given.

The following two lemmas are used to prove the main theorem (Theorem 4.2.8):

Lemma 4.2.6 (cf. [18, Theorem 2.8, Remark 2.11])
Let $G'_i \subset G_i$ be open subgroups of G_{K_i}. Then, for $s_i \in \mathcal{S}(G_i)$,

$$s_i|_{G'_i} \in \mathcal{S}(G'_i)^{\mathrm{geom}} \Longleftrightarrow s_i \in \mathcal{S}(G_i)^{\mathrm{geom}}.$$

Lemma 4.2.7
There exists an open subgroup $\mathcal{H}_i \subset \pi_1(U_i)$ such that $g_{\mathcal{H}_i} \geq 2$.

Proof.
We show this lemma by an argument similar to that of the proof of [18, Proposition 2.8].

By [18, Lemma 1.10], there exists an open normal subgroup H of $\pi_1(U_i \times_{\mathrm{Spec}\, K_i} \mathrm{Spec}\, \overline{K_i})$ such that the corresponding covering $(X_i)_H$ is of genus at least 2. It suffices to show that there exists an open subgroup $\mathcal{H} \subset \pi_1(U_i)$ such that $\mathcal{H} \cap \pi_1(U_i \times_{\mathrm{Spec}\, K_i} \mathrm{Spec}\, \overline{K_i}) \subset H$. Suppose that there are no such subgroups of $\pi_1(U_i)$. Then the family $\{(\mathcal{H} \cap \pi_1(U_i \times_{\mathrm{Spec}\, K_i} \mathrm{Spec}\, \overline{K_i})) \setminus H\}_{\mathcal{H} \subset \pi_1(U_i):\mathrm{open}}$ of closed subsets of $\pi_1(U_i \times_{\mathrm{Spec}\, K_i} \mathrm{Spec}\, \overline{K_i})$ has the finite intersection property. Indeed, assuming that

$$\bigcap_{j=1}^{N} ((\mathcal{H}_j \cap \pi_1(U_i \times_{\mathrm{Spec}\, K_i} \mathrm{Spec}\, \overline{K_i})) \setminus H) = \emptyset,$$

for some open subgroups $\mathcal{H}_j \subset \pi_1(U)\,(1 \leq j \leq N,\, N \in \mathbb{Z}_{>0})$, we have $\left(\bigcap_{j=1}^{N} \mathcal{H}_j\right) \cap \pi_1(U_i \times_{\mathrm{Spec}\, K_i} \mathrm{Spec}\, \overline{K_i}) \subset H$, which contradicts our assumption. Thus, by the compactness of $\pi_1(U_i \times_{\mathrm{Spec}\, K_i} \mathrm{Spec}\, \overline{K_i})$, we obtain

$$\bigcap_{\mathcal{H} \subset \pi_1(U_i):\mathrm{open}} ((\mathcal{H} \cap \pi_1(U_i \times_{\mathrm{Spec}\, K_i} \mathrm{Spec}\, \overline{K_i})) \setminus H) \neq \emptyset.$$

However, we have

$$\bigcap_{\mathcal{H} \subset \pi_1(U_i):\mathrm{open}} (\mathcal{H} \cap \pi_1(U_i \times_{\mathrm{Spec}\, K_i} \mathrm{Spec}\, \overline{K_i})) = \{1\} \subset H.$$

This is a contradiction.

□

Theorem 4.2.8
Suppose that there exist an open subgroup $\mathcal{H}_0 \subset \pi_1(U_1)$ and a divisor $m > 1$ of $q_{\mathcal{H}_0} - 1$ such that:

$$i_{(K_1)_{\mathcal{H}}}((X_1)_{\mathcal{H}}((K_1)_{\mathcal{H}})) \equiv i_{(K_2)_{\alpha(\mathcal{H})}}((X_2)_{\alpha(\mathcal{H})}((K_2)_{\alpha(\mathcal{H})})) \mod m,$$

for all open subgroups $\mathcal{H}$ of $\pi_1(U_1)$ satisfying $\mathcal{H} \subset \mathcal{H}_0$. Then, for all open subgroups $G_1 \subset G_{K_1}$ and all $s_1 \in \mathcal{S}(G_1)$, we have

$$s_1 \in \mathcal{S}(G_1)^{\mathrm{geom}} \Longleftrightarrow \alpha \circ s_1 \circ \alpha_K^{-1} \in \mathcal{S}(\alpha_K(G_1))^{\mathrm{geom}}.$$

Proof.

Take any open subgroup $G_1 \subset G_{K_1}$ and any $s_1 \in \mathcal{S}(G_1)$. By Lemma 4.2.7, there exists an open subgroup $\mathcal{H}_0'$ of $\pi_1(U_1)$ such that $\mathcal{H}_0' \subset \mathcal{H}_0$ and that $g_{\mathcal{H}_0'} \geq 2$. Then, by [6, Lemma 1.3.9], we obtain $g_{\alpha(\mathcal{H}_0')} = g_{\mathcal{H}_0'} \geq 2$. $G_1' := \mathrm{pr}_1(s_1(G_1) \cap \mathcal{H}_0')$ is an open subgroup of G_{K_1} such that $s_1(G_1') \subset \mathcal{H}_0'$. Set $L_1 := \overline{K_1}^{G_1'}$ and $L_2 := \overline{K_2}^{\alpha_K(G_1')}$. By assumption, for all open subgroups $\mathcal{H}$ of $\pi_1(U_1)$ satisfying $\mathcal{H} \subset \mathcal{H}_0'$, we have

$$i_{(K_1)_{\mathcal{H}}}((X_1)_{\mathcal{H}}((K_1)_{\mathcal{H}})) \equiv i_{(K_2)_{\alpha(\mathcal{H})}}((X_2)_{\alpha(\mathcal{H})}((K_2)_{\alpha(\mathcal{H})})) \mod m.$$

So, by Theorem 2.4.1, for all open subgroup $\mathcal{H}$ of $\pi_1(U_1)$ satisfying $s_1(G_1') \subset \mathcal{H} \subset \mathcal{H}_0'$, we have

$$(X_1)_{\mathcal{H}}(L_1) \neq \emptyset \Longleftrightarrow (X_2)_{\alpha(\mathcal{H})}(L_2) \neq \emptyset.$$

Thus, by Theorem 4.2.4,

$$s_1|_{G_1'} \in \mathcal{S}(G_1')^{\mathrm{geom}} \Longleftrightarrow s_2|_{\alpha_K(G_1')} \in \mathcal{S}(\alpha_K(G_1'))^{\mathrm{geom}},$$

where $s_2 := \alpha \circ s_1 \circ \alpha_K^{-1} \in \mathcal{S}(\alpha_K(G_1))$. Therefore, by Lemma 4.2.6, we obtain

$$s_1 \in \mathcal{S}(G_1)^{\mathrm{geom}} \Longleftrightarrow s_2 \in \mathcal{S}(\alpha_K(G_1))^{\mathrm{geom}}.$$

□

Corollary 4.2.9

Suppose that there exist an open subgroup $\mathcal{H}_0 \subset \pi_1(U_1)$ and a divisor $m > 1$ of $q_{\mathcal{H}_0} - 1$ such that:

$$i_{(K_1)_{\mathcal{H}}}((X_1)_{\mathcal{H}}((K_1)_{\mathcal{H}})) \equiv i_{(K_2)_{\alpha(\mathcal{H})}}((X_2)_{\alpha(\mathcal{H})}((K_2)_{\alpha(\mathcal{H})})) \mod m,$$

for all open subgroups $\mathcal{H}$ of $\pi_1(U_1)$ satisfying $\mathcal{H} \subset \mathcal{H}_0$. Then α arises from a unique isomorphism of schemes $U_1 \xrightarrow{\sim} U_2$ (more precisely, $\widetilde{U_1} \xrightarrow{\sim} \widetilde{U_2}$).

Proof.

Immediate from Theorems 4.2.2, 4.2.4 and 4.2.8.

□

4.3. **Group-theoreticity of i-invariants.**

We follow the notations of the previous section. Suppose that we are given an isomorphism of profinite groups $\alpha : \pi_1(U_1) \xrightarrow{\sim} \pi_1(U_2)$.

Theorem 4.3.1 (cf. [6, Theorem 2.7])

For $i = 1, 2$, suppose that X_i is of genus $g_i \geq 2$ and that X_i has a stable model $\mathfrak{X}_i$ over $\mathcal{O}_{K_i}$. Set $(\mathfrak{X}_i)_{k_i} := \mathfrak{X}_i \times_{\mathrm{Spec}\,\mathcal{O}_{K_i}} \mathrm{Spec}\,k_i$. Then an isomorphism of profinite groups $\pi_1(X_1) \xrightarrow{\sim} \pi_1(X_2)$ induces the following commutative diagram:

$$\begin{tikzcd}
\pi_1(X_1) \arrow[r, "\sim"] \arrow[d] & \pi_1(X_2) \arrow[d] \\
G_{K_1} \arrow[r, "\sim"] & G_{K_2}
\end{tikzcd}$$

Moreover, the isomorphism induces the following commutative diagram of schemes:

$$\begin{tikzcd}
(\mathfrak{X}_1)_{k_1} \arrow[r, "\sim"] \arrow[d] & (\mathfrak{X}_2)_{k_2} \arrow[d] \\
\operatorname{Spec} k_1 \arrow[r, "\sim"] & \operatorname{Spec} k_2
\end{tikzcd}$$

This correspondence is functorial in the following sense: Define X_i, K_i, etc. for $i = 3$ in the same manner as for $i = 1, 2$ and suppose that X_3 has a stable model $\mathfrak{X}_3$ over $\mathcal{O}_{K_3}$. Moreover, we assume that we are given isomorphisms of profinite groups $\alpha_{ij} : \pi_1(X_i) \overset{\sim}{\to} \pi_1(X_j)$ for $1 \leq i < j \leq 3$. Let $f_{ij} : (\mathfrak{X}_i)_{k_i} \overset{\sim}{\to} (\mathfrak{X}_j)_{k_j}$ be the isomorphism of schemes induced by α_{ij}. Then $\alpha_{13} = \alpha_{23} \circ \alpha_{12}$ implies $f_{13} = f_{23} \circ f_{12}$.

Remark 4.3.2

Theorem 2.7 of [6] shows a stronger result including the data of log structures of schemes without assuming the properness of hyperbolic curves. However, we do not use this result in the present paper.

The following theorem shows that the i-invariants (mod 2) of the sets of rational points of hyperbolic curves are group-theoretic in a certain situation:

Theorem 4.3.3

Suppose that p is odd. Moreover, for $i = 1, 2$, assume that X_i is of genus $g_i \geq 2$ and that X_i has log smooth reduction. Then we have

$$i_{K_1}(X_1(K_1)) \equiv i_{K_2}(X_2(K_2)) \quad \bmod 2.$$

Proof.

Note that we obtain the following commutative diagram from the isomorphism $\alpha : \pi_1(U_1) \overset{\sim}{\to} \pi_1(U_2)$ by [6, Lemma 1.3.9]:

$$\begin{tikzcd}
\pi_1(U_1) \arrow[r, "\sim"] \arrow[d] & \pi_1(U_2) \arrow[d] \\
\pi_1(X_1) \arrow[r, "\sim"] \arrow[d] & \pi_1(X_2) \arrow[d] \\
G_{K_1} \arrow[r, "\sim"] & G_{K_2}
\end{tikzcd}$$

There exists a finite tamely ramified extension L_1/K_1 such that $(X_1)_{L_1} := X_1 \times_{\operatorname{Spec} K_1} \operatorname{Spec} L_1$ has a stable model $\mathfrak{X}_1$ over $\mathcal{O}_{L_1}$. Then, $L_2 := \overline{K_2}^{\alpha_K(G_{L_1})}$ is a finite tamely ramified extension of K_2 by Proposition 4.2.1(iii). Moreover, $(X_2)_{L_2} := X_2 \times_{\operatorname{Spec} K_2} \operatorname{Spec} L_2$ has a stable model $\mathfrak{X}_2$ over $\mathcal{O}_{L_2}$ (cf. Remark 4.3.4) . Let k_{L_1} (resp. k_{L_2}) be the residue field of L_1 (resp. L_2).

By Theorem 4.3.1, the isomorphism of profinite groups $\pi_1(X_1) \overset{\sim}{\to} \pi_1(X_2)$ induces the following commutative diagram:

$$\begin{tikzcd}
\pi_1((X_1)_{L_1}) \arrow[r, "\sim"] \arrow[d] & \pi_1((X_2)_{L_2}) \arrow[d] \\
\pi_1(X_1) \arrow[r, "\sim"] \arrow[d] & \pi_1(X_2) \arrow[d] \\
G_{K_1} \arrow[r, "\sim"] \arrow[d] & G_{K_2} \arrow[d] \\
\mathrm{Gal}(L_1/K_1) \arrow[r, "\sim"] & \mathrm{Gal}(L_2/K_2)
\end{tikzcd}$$

Again by Theorem 4.3.1, the induced isomorphism of special fibers and the Galois actions on the fibers make the following commutative diagram:

$$\begin{tikzcd}
(\mathfrak{X}_1)_{k_{L_1}} \arrow[r, "\sim"] & (\mathfrak{X}_2)_{k_{L_2}} \\
\mathrm{Gal}\,(L_1/K_1) \arrow[r, "\sim"] \arrow[u, phantom, "\circlearrowleft"] & \mathrm{Gal}(L_2/K_2) \arrow[u, phantom, "\circlearrowleft"]
\end{tikzcd}$$

Now the theorem is immediate from Corollary 3.5.5 and Remark 3.5.6.

□

Remark 4.3.4
Suppose that we are given an isomorphism of profinite groups $\alpha : \pi_1(X_1) \overset{\sim}{\to} \pi_1(X_2)$. Then, by [6, Lemma 2.1], X_1 has stable reduction if and only if X_2 has stable reduction. On the other hand, by Proposition 4.2.1(ii) and [13], X_1 has log smooth reduction if and only of X_2 has log smooth reduction. Moreover, if L_1 is a finite tamely ramified extension of K_1 such that $(X_1)_{L_1} := X_1 \times_{\mathrm{Spec}\,K_1} \mathrm{Spec}\,L_1$ has a stable model over $\mathcal{O}_{L_1}$, $(X_2)_{L_2} := X_2 \times_{\mathrm{Spec}\,K_2} \mathrm{Spec}\,L_2$ has a stable model over $\mathcal{O}_{L_2}$ where $L_2 := \overline{K_2}^{\alpha_K(G_{L_1})}$ is a finite tamely ramified extension of K_2 by Proposition 4.2.1(iii).

Remark 4.3.5
If we prove Theorem 4.3.3 without assuming that X_i has log smooth reduction, we can prove, by using Corollary 4.2.9, the absolute p-adic Grothendieck conjecture for p odd.

In the case where X_i has stable reduction over $\mathcal{O}_{K_i}$, the following theorem holds without assuming $p \neq 2$:

Theorem 4.3.6
For $i = 1, 2$, suppose that X_i is of genus $g_i \geq 2$ and that X_i has a stable model $\mathfrak{X}_i$ over $\mathcal{O}_{K_i}$. Moreover, assume that all nodes of $(\mathfrak{X}_i)_{k_i}(k_i)$ are split. Then we have

$$i_{K_1}(X_1(K_1)) \equiv i_{K_2}(X_2(K_2)) \mod (q-1).$$

Proof.
Immediate from Corollary 3.2.3 and Theorem 4.3.1.

□

Remark 4.3.7
By Theorem 4.3.1 and [6, Lemma 2.1], X_1 has a stable model $\mathfrak{X}_1$ over $\mathcal{O}_{K_1}$ and all nodes of $(\mathfrak{X}_1)_{k_1}$ are split if and only if X_2 satisfies the similar conditions.

Appendix A. A real analogue

In Chapter 2, we gave a criterion for existence of rational points of proper, smooth and geometrically connected hyperbolic curves over K in terms of i-invariants, where K is a finite extension of $\mathbb{Q}_p$. On the other hand, for a proper, smooth and geometrically connected hyperbolic curve X over $\mathbb{R}$, the number of connected components $|\pi_0(X(\mathbb{R}))|$ of the set $X(\mathbb{R})$ of $\mathbb{R}$-rational points of X may be considered as an analogue of the i-invariants. In this appendix, we show that $|\pi_0(X(\mathbb{R}))|$ may be recovered from the arithmetic fundamental group of X.

In the following, let X be a proper, smooth and geometrically connected hyperbolic curve over $\mathbb{R}$, $X(\mathbb{R})$ the set of $\mathbb{R}$-rational points of X, $g\,(\geq 2)$ the genus of X and $\pi_1^{\mathrm{alg}}(X)$ the arithmetic fundamental group of X. Set $n(X) := |\pi_0(X(\mathbb{R}))|$. For a real manifold Y, we denote the usual topological fundamental group of Y by $\pi_1(Y)$.

The action of $G_{\mathbb{R}} = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \tau\}$ on the vector space $V := \pi_1^{\mathrm{alg}}(X \times_{\mathrm{Spec}\,\mathbb{R}} \mathrm{Spec}\,\mathbb{C})^{\mathrm{ab}} \otimes \mathbb{F}_2$ of dimension $2g$ over $\mathbb{F}_2$ defines a homomorphism $\rho : G_{\mathbb{R}} \to \mathrm{GL}(V)$. (Here, $\pi_1^{\mathrm{alg}}(X \times_{\mathrm{Spec}\,\mathbb{R}} \mathrm{Spec}\,\mathbb{C})$ is the arithmetic fundamental group of $X \times_{\mathrm{Spec}\,\mathbb{R}} \mathrm{Spec}\,\mathbb{C}$.) Let r_X be the rank of $\rho(\tau) - 1 \in \mathrm{End}(V)$. Clearly, r_X may be recovered group-theoretically from $\pi_1^{\mathrm{alg}}(X) \twoheadrightarrow G_{\mathbb{R}}$.

The following is a key proposition for the group-theoretic recoverability of $n(X)$:

Proposition A.0.1 (cf. [1, Proposition 4.4])

(i) *If $n(X) > 0$, then:*
$$r_X + n(X) = g + 1.$$

(ii) *If $n(X) = 0$, then:*
$$r_X = 2\left[\frac{g}{2}\right].$$

Here, $\left[\frac{g}{2}\right]$ is the largest integer less than or equal to $\frac{g}{2}$.

Remark A.0.2
In [1, Proposition 4.4], r_X is denoted by rank (H).

Except for the case where $g + 1 - n(X) = 2\left[\frac{g}{2}\right]$ holds, $n(X)$ can be recovered immediately from r_X by using Proposition A.0.1 (this recovery is clearly group-theoretic). On the other hand, we may not distinguish the following cases (where $g + 1 - n(X) = 2\left[\frac{g}{2}\right]$ holds) from the case where $n(X) = 0$ only by the data of r_X:

(i) g is even and $n(X) = 1$.

(ii) g is odd and $n(X) = 2$.

We distinguish these cases from the case where $n(X) = 0$ by using the data of coverings of X.

Let J be the Jacobian of X, $J(\mathbb{R})$ the set of $\mathbb{R}$-rational points of X and $J(\mathbb{R})^0$ the connected component of $J(\mathbb{R})$ which contains the unit element of the abelian group

$J(\mathbb{R})$. By [1, Proposition 1.1], there exists a finite abelian group G such that $G \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus N}$ $(0 \leq N \leq g)$ and that the following split exact sequence exists:

$$0 \to J(\mathbb{R})^0 \to J(\mathbb{R}) \to G \to 0.$$

Since $J(\mathbb{R})^0 \simeq (\mathbb{R}/\mathbb{Z})^{\oplus g}$, we have $J(\mathbb{R}) \simeq (\mathbb{R}/\mathbb{Z})^{\oplus g} \oplus G$.

Proposition A.0.3
If $n(X) \neq 0$, there exists a finite étale covering X' of X such that X' is geometrically connected over $\mathbb{R}$ and of odd genus, and that $n(X') > 2$.

Proof.

Since $n(X) \neq 0$, we have $X(\mathbb{R}) \neq \emptyset$. So, by taking a point of $X(\mathbb{R})$, we obtain a closed immersion $j : X \hookrightarrow J$. Let $2_J : J \to J$ stand for multiplication by 2 on J. We define $X_2 = X \times_J J$ by the following diagram:

$$\begin{tikzcd}
X_2 := X \times_J J \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & J \arrow[d, "2_J"] \\
X \arrow[r, "j"] & J
\end{tikzcd}$$

X_2 is a finite étale covering of X and geometrically connected over $\mathbb{R}$. Let ν $(= 2^{2g})$ be the degree of $X_2 \to X$ and g_2 the genus of X_2. By Hurwitz formula, we have $g_2 = \nu(g-1)+1$. Since ν is a positive power of 2, g_2 is odd.

Let $m_1(X)$ (resp. $m_2(X)$) be the number of the connected components of $X(\mathbb{R})$ which are contained (resp. not contained) in $J(\mathbb{R})^0$. Then we have $m_1(X) > 0$ and $n(X) = m_1(X) + m_2(X)$.

Set:

$$J(\mathbb{R}) = \coprod_{\sigma \in G} (\sigma + J(\mathbb{R})^0) =: \coprod_{\sigma \in G} A_\sigma.$$

For each $\sigma \in G$, A_σ surjects onto $J(\mathbb{R})^0$ by multiplication by 2. By translating by σ, we see that it is isomorphic to the covering $J(\mathbb{R})^0 \to J(\mathbb{R})^0$ defined by multiplication by 2. The latter covering corresponds to the surjection $\pi_1(J(\mathbb{R})^0)(\simeq \mathbb{Z}^{\oplus g}) \twoheadrightarrow (\mathbb{Z}/2\mathbb{Z})^{\oplus g}$.

On the other hand, since $m_1(X) > 0$, we may take a connected component C of $X(\mathbb{R})$ which is contained in $J(\mathbb{R})^0$ and fix it. As C is a compact manifold of dimension 1 over $\mathbb{R}$, C is homeomorphic to S^1 and we have $\pi_1(C) \simeq \mathbb{Z}$. Thus, the image of $\pi_1(C)$ in $(\mathbb{Z}/2\mathbb{Z})^{\oplus g}$ is trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$, in particular, the index of the image of $\pi_1(C)$ in $(\mathbb{Z}/2\mathbb{Z})^{\oplus g}$ is at least 2^{g-1}. This shows that the inverse image of C by the covering $A_\sigma \to J(\mathbb{R})^0$ induced by multiplication by 2 has at least 2^{g-1} connected components. Denote m_σ by the number of the connected components of $X_2(\mathbb{R})$ which are contained in A_σ. Then we have:

$$2^{g-1} m_1(X) \leq m_\sigma \leq 2^g m_1(X).$$

Summing over $\sigma \in G$, we obtain:

$$|G| \cdot 2^{g-1} m_1(X) \leq n(X_2) \leq |G| \cdot 2^g m_1(X).$$

(Note that $\sum_{\sigma \in G} m_\sigma = n(X_2)$.) In particular, we have $n(X_2) \geq 2^{g-1}$. So, if $g > 2$, we may take X_2 for X'.

If $g = 2$, we have $g_2 > 2$. Therefore, by applying the same argument for X_2, we obtain a curve with the desired properties.

□

Corollary A.0.4
$n(X) = |\pi_0(X(\mathbb{R}))|$ may be recovered group-theoretically from $\pi_1^{\mathrm{alg}}(X) \twoheadrightarrow G_{\mathbb{R}}$

Proof.
By Proposition A.0.3, whether $n(X) = 0$ or not is determined group-theoretically. Now the proposition is immediate from Proposition A.0.1.

□

Remark A.0.5
In [4, Corollary 3.13], a real analogue of the section conjecture is proved. Corollary A.0.4 also follows from this result.

References

[1] Benedict H. Gross, Joe Harris, Real algebraic curves, *Annales scientifiques de l'É.N.S. 4e série*, tome **14**, n° 2 (1981), pp. 157–182.
[2] Qing Liu, *Algebraic Geometry and Arithmetic Curves,* Oxford University Press Inc., 2006.
[3] Shinichi Mochizuki, The local pro-p anabelian geometry of curves, *Invent. Math.* **138** (1999), pp. 319–423.
[4] Shinichi Mochizuki, Topics surrounding the anabelian geometry of hyperbolic curves, *Galois Groups and Fundamental Groups, Mathematical Sciences Research Institute Publications* **41**, Cambridge University Press, 2003, pp. 119–165.
[5] Shinichi Mochizuki, The absolute anabelian geometry of canonical curves, *Kazuya Kato's fiftieth birthday, Doc. Math., Extra Vol.*, 2003, pp. 609–640.
[6] Shinichi Mochizuki, The absolute anabelian geometry of hyperbolic curves, *Galois Theory and Modular Forms*, Kluwer Academic Publishers, 2004, pp. 77–122.
[7] Shinichi Mochizuki, Absolute anabelian cuspidalizations of proper hyperbolic curves, *J. Math. Kyoto Univ.* **47** (2007), pp. 451–539.
[8] Shinichi Mochizuki, Topics in absolute anabelian geometry II: Decomposition groups and endomorphisms, *J. Math. Sci. Univ. Tokyo* **20** (2013), pp. 171–269.
[9] Masayoshi Nagata, *Theory of Commutative Fields*, Translations of mathematical monographs **125**, American Mathematical Society, 1993.
[10] Hiroaki Nakamura, Rigidity of the arithmetic fundamental group of a punctured projective line, *J. reine angew. Math.* **405** (1990), pp. 117–130.
[11] Hiroaki Nakamura, Galois rigidity of the étale fundamental groups of punctured projective lines, *J. reine angew. Math.* **411** (1990), pp. 205–216.
[12] Jürgen Neukirch, Alexander Schmidt, Kay Wingberg, *Cohomology of Number Fields*, Grundlehren der mathematischen Wissenschaften **323**, Springer-Verlag, 2000.
[13] Takeshi Saito, Log smooth extension of a family of curves and semi-stable reduction, *J. Algebraic Geometry* **13** (2004), pp. 287–321.
[14] Schneps Leila, Pierre Lochak, *Geometric Galois Actions; 1. Around Grothendieck's Esquisse d'un Programme*, London Mathematical Society Lecture Note Series **242**, Cambridge University Press, (1997).
[15] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publications Mathématiques de l'I.H.É.S.*, tome **54** (1981), pp. 123–201.
[16] J.-P. Serre, *Lie Algebras and Lie Groups*, Lecture Notes in Mathematics **1500**, Springer-Verlag, (1992).

[17] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate texts in mathematics **106**, Springer-Verlag New York Inc., 1986.

[18] Akio Tamagawa, The Grothendieck conjecture for affine curves, *Compositio Mathematica* **109** (1997), pp. 135–194.

(Takahiro Murotani) Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan
E-mail address: murotani@kurims.kyoto-u.ac.jp