Universiteit Utrecht

MASTER THESIS

Mono-Anabelian Geometry

Author:
Alexander Gietelink Oldenziel

Supervisors:
Prof. dr. C.F. Faber
dr. E. Lepage
Second Reader:
Prof. dr. G. Cornelissen

November 16, 2017

Acknowledgements

First and foremost, I would like to thank my advisor Emmanuel Lepage for his guidance and time throughout the project. He went beyond the call of duty to explain mathematics and support me in writing my thesis. Suffice to say that without his help this thesis would have been wholly impossible. I would also like to thank Carel Faber for serving as my official supervisor and Gunther Cornelissen acting as my second reader.

Thanks to Yuichiro Hoshi for his extremely detailed answers to my many questions. I would like to thank Taylor Dupuy for his crisp explanations and for inviting me to the conference on anabelian geometry at Vermont that he and his wife Christelle Vincent organized. I have also benefited hugely from a seminar that was held at the UPMC on anabelian geometry, and I'd like to thank all the participants for many mathematical discussions. I would also like to thank the mathematical department at Nottingham who kindly hosted Emmanuel Lepage and me.

There have been many people who have contributed to the final form of this thesis, some of whom I will name: Florian Pop, Olivia Caramello, Pol van Hoften, David Corwin, Lars Kuehne, Chung Pang Mok, Jacob Stix, Mathijs Henquet, Vincent Daruvar, Jackson Morrow, Wojtek Porowski, Arno Kret and many others. My gratitude goes out to all of them.

Contents

1 Introduction to Anabelian Geometry

This thesis considers the question to what degree a scheme is determined by its étale fundamental group. The study of this question is the field of Anabelian geometry. In general, abelian fundamental groups are too simple to determine all of the scheme structure. The schemes in question therefore have to possess étale fundamental groups that are not abelian; hence the epithet 'anabelian'.

1.1 Fields

The cornerstone of Anabelian Geometry is the lauded Neukirch-Uchida theorem, stating that the structure of a global field is encoded in its absolute Galois group, from now on called just its Galois group.

Let k_1, k_2 be two global fields and fix two separable closures $\overline{k}_1, \overline{k}_2$. Let $\mathrm{Isom}(k_1, k_2)$ be the set of field isomorphisms $k_1 \xrightarrow{\sim} k_2$ and let $\mathrm{Isom}(\overline{k}_1/k_1, \overline{k}_2/k_2)$ be the isomorphisms $\overline{k}_1 \xrightarrow{\sim} \overline{k}_2$ that send k_1 to k_2. We consider the Galois groups $\mathrm{G}_1 = \mathrm{Gal}(\overline{k}_1, k_1), \mathrm{G}_2 = \mathrm{Gal}(\overline{k}_2, k_2)$. The automorphism group G_1 acts on $\mathrm{Isom}(\overline{k}_1/k_1, k_2/\overline{k}_2)$ by the application $\alpha(\phi) = \phi \circ \alpha^{-1}$ and we have an isomorphism

$$\mathrm{Isom}(\overline{k_1}/k_1, \overline{k}_2, k_2)/\,\mathrm{G}_1 \xrightarrow{\sim} \mathrm{Isom}(k_1, k_2)$$

An element $\phi \in \mathrm{Isom}(\overline{k_1}/k_1, \overline{k}_2/k_2)$ induces an isomorphism $\phi^* : \mathrm{G}_2 \xrightarrow{\sim} \mathrm{G}_1$ given as

$$\phi^*(\alpha_2)(x_1) = \phi^{-1}(\alpha_2(\phi(x_1))), \quad x_1 \in \overline{k_1}, \alpha_2 \in \mathrm{G}_2\,.$$

An *inner automorphism* of a group G is an automorphism of the form $c_h : \mathrm{G} \to \mathrm{G}$

$$g \mapsto hgh^{-1}, \quad g \in \mathrm{G}$$

for a fixed $h \in \mathrm{G}$. An *outer morphism* of groups $G \to H$ is an equivalence class of group homomorphisms f where the equivalence relation is induced by $f \mapsto f \circ c_h^{-1}$.

Theorem 1.1 (Neukirch-Uchida)**.** *Let k_1, k_2 be global fields; fix algebraic closures $\overline{k_1}, \overline{k_2}$ and let $\mathrm{G}_1, \mathrm{G}_2$ denote their Galois groups. There is a natural bijection*

$$\mathrm{Isom}(\overline{k_1}/k_1, \overline{k_2}/k_2) = \mathrm{Isom}(\mathrm{G}_1, \mathrm{G}_2).$$

If we do not keep track of the basepoints we have a natural bijection

$$\mathrm{Isom}(k_1, k_2) \xrightarrow{\sim} \mathrm{Isom}^{\mathrm{Out}}(\mathrm{G}_1, \mathrm{G}_2)$$

where on the right we have outer isomorphisms.

Proof. See Theorem 12.2.1 [NSW08]. □

The above theorem was proved by Neukirch for number fields that are Galois over $\mathbb{Q}$, conditional on an earlier result of Gassmann on arithmetic equivalence. Uchida was the first to prove it for general number fields and function fields. Apparently, Iwasawa also had a proof which was not written down. In the statement of the Neukirch-Uchida theorem I kept explicit track of the basepoints. In the following I will generally suppress mention of the basepoint.

Definition 1.2. A profinite group is a topological group Π that is isomorphic to the projective limit of finite groups endowed with the discrete topology.

Suppose that a suitable class of schemes V is completely determined by their etale fundamental groups- these are often called 'anabelian' schemes. One might phrase this as stating that $\pi_1 : V \to \mathbf{ProGrp}$ fully faithfully embeds the class of schemes V into the category of profinite groups **ProGrp**.

Following Neukirch-Uchida, can we now say that the scheme $\mathrm{Spec}(k)$ is completely determined by G_k? Not exactly. Suppose I 'gave' you G_k as a profinite group, could you 'reconstruct' k with just that information? It isn't very clear how this is possible.

A fundamental distinction is made between 'fully-faithfullness' type results and 'reconstruction algorithms'. Sometimes they are called bi-anabelian, respectively mono-anabelian, results, see the introduction of [Moc15]. A fully faithfullness result states that π_1 is fully faithful for suitably chosen $V \to \mathbf{ProGrp}$.

As of the time of writing, there is not yet an elegant formulation. In the case of π_1, what is meant is that one should describe the scheme inverse to a given profinite group in mathematical formulae that only use the 'language' of profinite groups. Hence we might talk of various kinds of subgroups, torsion elements, open immersions of groups et cetera.

Definition 1.3. A *Species* $\mathfrak{C}$ is a collection of set-theoretic formulae $\{\phi_i\}_i$ such that interpreted in any model $\mathfrak{M}$ of set theory the $\{\phi_i\}_i$ determine a category $\mathcal{C}$. The objects $\{c_j\}$ in the category $\mathcal{C}$ defined by the formulae $\{\phi_i\}$ are called *specimen* and the morphisms *morphisms of specimens*. Let $\mathfrak{C}, \mathfrak{D}$ be two species defined by formulae $\{\phi_i\}, \{\psi_j\}$. A *functorial algorithm* or *mutation* is a collection of set-theoretic formulae $\{\tau_k\}$ such that interpreted in any given model $\mathfrak{M}$ of set theory the $\{\tau_k\}$ define a functor $\mathcal{A}\colon \mathcal{C} \to \mathcal{D}$.

Other words that mean the same thing are: 'mono-anabelian reconstruction; group-theoretic recipe.'

Example 1.4. The usual description of groups as 'sets G with an operation satisfying etc...' together with the description of group homomorphisms as 'functions $f : G \to H$ such that $f(a*b) = f(a)*f(b)$ etc' furnishes a Species $\mathfrak{Group}$. The specimen are descriptions of individual groups such as 'the group $\mathbb{Z}$ is the free group on a single generator etc.'.

Example 1.5. Let G be a fixed group [like $\mathbb{Z}/n\mathbb{Z}$] and consider its usual description in set theoretic formulae. This yields a Specie $\mathfrak{C}_1$ with associated category the trivial category. Of course we may also consider group homomorphisms $G \to G$ through the usual set theoretic formulae to obtain a different Specie $\mathfrak{C}_2$ whose associated category has one object and morphisms equal to $\mathrm{Aut}(G)$.

We will see examples of functorial algorithms shortly.

Remark 1.6. Given the Galois group G_k of a number field k just as 'abstract' profinite group [i.e. we are not provided with the action $\mathrm{G} \curvearrowright \overline{k}$] can we reconstruct the number field? One very trivial answer would be: 'k is the field such that G_k is its absolute Galois group'. This is clearly not the answer we wanted.

Definition 1.7. An *isomorph* of an object X is simply any object Y such that Y is isomorphic to X. To simplify notation I will use a dagger † to denote an isomorph of an object. For instance, if X is a scheme and Π_X is its étale fundamental group—notice that we suppress the dependence on basepoints—then $\Pi_X^\dagger$ is a profinite group that is isomorphic to Π_X. Alternatively, I will often use Π, G for isomorphs of a G_k, Π_X where the schemes in question should be clear from the context.

Definition 1.8. Let k be a field. Suppose G is an isomorph of G_k. Let M be a set, a monoid, group, field, ring, topological group, ind-topological group et cetera, together with an action G. Then we say that $\mathrm{G} \curvearrowright M$ is a *Galois pair*.

In the case of function fields a simple rewriting of Uchida's proof furnishes a functorial algorithm for reconstructing the field from its absolute Galois group. The number field case requires more care but was recently solved by Hoshi.

Let k be a number field and $\overline{k}$ an algebraic closure. Let $\mathcal{G}$ denote the category with objects profinite groups isomorphic to G_k and morphisms to be isomorphisms of profinite groups. Let $\mathcal{G} - \mathrm{Pair}$ denote the category of 'Galois pairs' $\mathrm{G} \curvearrowright \overline{k}$, i.e. a pair of a profinite group G acting on an algebraically closed field k, where morphisms are isomorphisms of pairs.

Theorem 1.9 (Hoshi)**.** *There is a functorial algorithm A*

$$\begin{aligned} A : \mathcal{G} &\to {\sim}\mathcal{G} - \mathrm{Pair} \\ \mathrm{G} &\longmapsto \mathrm{G} \curvearrowright \overline{k}(\mathrm{G})) \end{aligned}$$

that reconstructs the number field k together with its Galois action, functorial with respect to isomorphisms of profinite groups.

Proof. See [Hos15]. □

Remark 1.10. The functorial reconstruction of a number field immediately implies Neukirch-Uchida. Indeed, it is clear that any isomorphism of fields induces a unique morphism of Galois groups.

We have a mono-anabelian reconstruction algorithm for reconstituting a number field from its Galois group. What about other fields? The case of finite fields is easy: the Galois groups of finite fields are all isomorphic to $\widehat{\mathbb{Z}}$ so there is little to say about this case.

The Neukirch-Uchida theorem does not hold for p-adic fields (= finite extensions of $\mathbb{Q}_p$). It is possible for two p-adic fields to have the same absolute Galois groups. This was first discovered by Jarden and Ritter and independently by Yamagawa. In the following fix

k	a finite extension of $\mathbb{Q}_p$
$\overline{k}$	an algebraic closure of k
G_k	the absolute Galois group of k
$\mathcal{O}_k$	the ring of integers of k
$\mathcal{O}_k^\times$	the units of $\mathcal{O}_k$
μ_k	the roots of unity of k
m	the maximal ideal of $\mathcal{O}_k$
Π	a uniformizer of m
κ	the residue field of κ
p	the residue characteristic of κ
q	the size of the residue field κ
e	the ramification degree
d	the absolute degree $[k\colon \mathbb{Q}_p]$
I_k	the inertia group $\mathrm{Ker}(\mathrm{G}_k \to \mathrm{G}_\kappa)$
P_k	the wild inertia group
G_κ	the Galois group of the residue field κ
Fr	the Frobenius element in G_κ or sometimes a lift in G_k

Theorem 1.11 (Jarden-Ritter)**.** *Let $p \neq 2$. Let k_1, k_2 be finite extensions of $\mathbb{Q}_p$. Let ζ_p be a p-th root of unity. If $\zeta_p \in k_1$ then k_1, k_2 have isomorphic absolute Galois groups if and only if*

(i) The absolute degrees are equal: $[k_1 : \mathbb{Q}_p] = [k_2 : \mathbb{Q}_p]$

(ii) The maximal abelian subextensions $k_1^{\mathrm{ab}}, k_2^{\mathrm{ab}}$ are isomorphic over $\mathbb{Q}_p$.

Proof. See Jarden and Ritter [JR79]. □

Example 1.12 (Exotic automorphisms)**.** A related obstruction for us will be the existence of automorphisms of the Galois group G_k that do not arise from automorphisms of fields. These are called *exotic automorphisms*. It is not terribly important to understand how these automorphisms work in detail. I try to give a sense of how they arise below, but feel free to skip it.

Assume $p \neq 2$, let the order p^s of the group μ_{p^s} of all p-power roots of unity in the maximal tamely ramified extension.

We may describe the Galois group explicitly, see Theorem 7.5.10 in [NSW08], as the profinite group generated by $d+3$ generators $\sigma, \tau, x_0, \cdots, x_d$ such that the closed normal subgroup, topologically generated by $x_0, \cdots, x_d$ is a prop-p-group and we have the relation

$$\sigma\tau\sigma^{-1} = \tau^q, \qquad \sigma x_0 \sigma^{-1} = C[x_1, x_2][x_3, x_4]\cdots[x_{d-1}, x_d]$$

where C is some monstrous expression in x_0, x_1, τ, p^s and the parity of d defined in [NSW08].

We now come to exotic automorphisms, first discovered by Jannsen and Wingberg, see Theorem 7.5.10 in [NSW08] or [JW83]. Define the map

$$\psi\colon \mathrm{G}_k \to \mathrm{G}_k$$

as $\psi(x) = x$ for all generators $\sigma, \tau, x_0, \cdots x_{d-1}$ and $\psi(x_d) = x_{d-1}x_d$. Since $[x_{d-1}, x_d x_{d-1}] = x_{d-1}x_d x_{d-1} x_{d-1}^{-1}(x_d x_{d-1})$ $[x_{d-1}, x_d]$ this is an automorphism. It turns out that it cannot arise from a field automorphism, see the remark following Theorem 7.5.10 in [NSW08].

Nevertheless, we can recover a lot of data associated to a p-adic field $k/\mathbb{Q}_p$ by looking at its Galois group G_k.

Theorem 1.13. *We have the following commutative diagram*

(i) There is a morphism of short exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_k^\times & \longrightarrow & k^\times & \longrightarrow & \mathbb{Z} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{I}_k & \longrightarrow & \mathrm{G}_k^{\mathrm{ab}} & \longrightarrow & \mathrm{G}_\kappa & \longrightarrow & 1 \end{array}$$

and the vertical arrows are the inclusions of the groups into their profinite completions. Here $\widehat{\mathbb{Z}} \hookrightarrow \mathrm{G}_\kappa \cong \widehat{\mathbb{Z}}$ is the inclusion given by sending a uniformizer to the Frobenius element.

(ii) We have

$$\mathcal{O}_k^\times \cong \mathbb{F}_q^\times \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$$

where $a \geq 0$; this has to do with how many p-th roots of unity k has.

(iii) We have

$$\mathrm{G}_k^{\mathrm{ab}} \cong \widehat{\mathbb{Z}} \times (\mathbb{F}_q)^\times \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d.$$

(iv) We have a short exact sequence

$$1 \to \mathrm{I}_k / P_k \to \mathrm{G}_k / P_k \to \mathrm{G}_k / \mathrm{I}_k \to 1$$

where $\mathrm{G}_k / \mathrm{I}_k = \mathrm{Gal}(k^{un}/k) = \mathrm{G}_k^{un} \cong \mathrm{G}_\kappa, \mathrm{I}_k / P_k = \mathrm{Gal}(k^{tr}/k^{un})$ where k^{un}, k^{tr} are the maximally unramified extension, respectively maximally tamely ramified extension of k. Moreover, as a G_κ-module $\mathrm{I}_k / P_k = \mathrm{Gal}(k^{tr}/k^{un})$ is given as $\prod_{l \neq p} \mathbb{Z}_l(1)$.

Proof. The statement of (i) is Local Class Field Theory. A proof of assertion (i) can be found in [Neu99, Chapter V]. For (ii) see Propostion 5.3 and 5.7 of [Neu99, Chapter II]. To prove (iii) we make use of (ii) and (i); if we can prove that

$$1 \longrightarrow \mathrm{I}_k \longrightarrow \mathrm{G}_k^{\mathrm{ab}} \longrightarrow \mathrm{G}_\kappa \longrightarrow 1 \tag{1.1}$$

splits we can conclude that

$$\mathrm{G}_k^{ab} \cong \mathrm{G}_\kappa \times \mathrm{I}_k \cong \widehat{\mathbb{Z}} \times \widehat{\mathcal{O}_k^\times} \cong \widehat{\mathbb{Z}} \times \widehat{\mathbb{F}_q^\times} \times \widehat{\mathbb{Z}/p^a\mathbb{Z}} \times \widehat{\mathbb{Z}_p^d} \cong \widehat{\mathbb{Z}} \times \mathbb{F}_q^\times \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$$

To prove that the short exact sequence in equation 1.1 splits we note that

$$1 \longrightarrow \mathcal{O}_k^\times \longrightarrow k^\times \longrightarrow \mathbb{Z} \longrightarrow 1$$

splits [i.e. any element in a local field can be written as $b \cdot \pi_k^a$, $b \in \mathcal{O}_k^\times$ $a \in \mathbb{Z}$ for some chosen uniformizer π_k] and the short exact sequence 1.1 is obtained as the profinite completion, which preserves splittings.

Let us proceed with (iv). The short exact sequence is basic group theory, the identifications follow from the definition of I_k, P_k. To compute I_k / P_k we argue as follows. This argument is the remark preceding Proposition 7.5.1 in [NSW08, Chapter VII].

Let $\mu_{\overline{k}}^{(p')}$ the group of roots of unity prime to p in $\overline{k}$; $\mu_{\overline{k}}^{(p)}$ is a G_κ-module. Moreover, under the reduction map $\mu_{\overline{k}^{(p')}}$ corresponds to the multiplicative group $\overline{\kappa}^\times$ of the residue field of k. Let $\mathrm{Val}(-)$ denote the value group. After normalization the value group $\mathrm{Val}(k)$ of k is $\mathbb{Z}$; extending this valuation we have $\mathrm{Val}(k^{tr}) = \bigcup_{p \nmid n} \frac{1}{n}$.

Next, we have an isomorphism

$$\mathrm{I}_k / P_k \cong \mathrm{Hom}(\mathrm{Val}(k^{tr}) / \mathrm{Val}(k), \overline{\kappa}^\times) \cong \mathrm{Hom}((\mathbb{Q}/\mathbb{Z})^{(p')}, \overline{\kappa}^\times)$$

see p. 174 in [Neu99, Chapter II].

In detail the argument runs as follows: we have a morphism $I_k \to \mathrm{Hom}(\mathrm{Val}(k^{tr}) / \mathrm{Val}(k), \overline{\kappa}^\times)$ given as follows. Let $\sigma \in \mathrm{I}_k$ and send it to χ_σ acting on $d \mod \mathbb{Z} \in \mathrm{Val}(k^{tr})/\mathbb{Z}$ as: pick an element $x \in k^{tr}$ such that the valuation equals $\mathrm{val}(x) = d$ and set

$$\chi_\sigma(d \mod \mathbb{Z}) = \frac{\sigma x}{x} \mod \mathfrak{P}$$

where $\mathfrak{P}$ is the unique prime ideal of the local field $\overline{k}$. One checks that this definition is independent of the element $x \in k^{tr}$, that it is an homomorphisms of groups, see p.174 [Neu99, Chapter II] and that P_k is the kernel. We prove the last property, let $\tau \in P_k$ and consider χ_τ. Remark that τ acts as $\pi_k^{1/p^n} \mapsto \zeta_{p^n}^j \pi_k^{1/p^n}$ for some j, were ζ_{p^n} is a primitive p^n-th root of unity which is send to one in the residue field. This implies that χ_τ is trivial. Given any $\sigma \in \mathrm{I}_k$ it also acts by multiplication by roots of unity, but these are nontrivial in the residue field if $\sigma \notin P_k$ so I conclude P_k is the kernel.

The Frobenius automorphism $\mathrm{Fr} \in \mathrm{G}_k^{un} \cong \mathrm{G}_\kappa$ acts trivially on the domain and as multiplication by q [in additive notation] on the codomain of $\mathrm{Hom}(\mathrm{Val}(k^{tr}) / \mathrm{Val}(k), \overline{\kappa}^\times)$. I conclude that $\mathrm{I}_k / P_k \cong \oplus_{l \neq p} \mathbb{Z}_p(1)$. □

Theorem 1.14. *Let k be a finite extension of $\mathbb{Q}_p$ and let G_k the absolute Galois group. Let G be an isomorph of G_k. We want to extract p and as much about k as possible purely from the datum of G. Define the 'group-theoretic' functorial algorithm*

(i) Let $p(\mathrm{G})$ be the unique prime p such that

$$\log_p((\#(\mathrm{G}^{ab} / \mathrm{tor}) / (p\, \mathrm{G}^{ab} / \mathrm{tor})) \geq 2.$$

where l is a prime distinct from p.

(ii) Let the anabelian degree be

$$d(\mathrm{G}) = \log_{p(\mathrm{G})}(\#(\mathrm{G}^{ab} / \mathrm{tor}) / (p(\mathrm{G})\, \mathrm{G}^{ab} / \mathrm{tor})) - 1.$$

(iii) Let $f(\mathrm{G})$ the anabelian residue degree

$$f(\mathrm{G}) = \log_{p(\mathrm{G})}(1 + (\#(\mathrm{G}^{\mathrm{ab}})_{\mathrm{tor}})^{(p')})$$

where l is any prime coprime with $p(\mathrm{G})$, where $G^{(p')}$ denotes the prime-to-p quotient of G.

(iv) Define the anabelian ramification index $e(\mathrm{G}) := \dfrac{d(\mathrm{G})}{f(\mathrm{G})}$.

(v) Construct the inertia group $\mathrm{I}(\mathrm{G})$ as

$$\mathrm{I}(\mathrm{G}) = \bigcap_{i \in I} \{N_i \lhd \mathrm{G} \mid N_i \text{ normal open},\ e(N_i) = e(\mathrm{G})\}$$

(vi) Construct the wild inertia group $P(\mathrm{G})$ *as*

$$P(\mathrm{G}) := \bigcap \{N \lhd \mathrm{G} \mid N \textit{ normal open}, \ \frac{e(N)}{e(\mathrm{G})} \textit{ is prime to } p\}$$

(vii) Let $\mathrm{G}_k^{un}(\mathrm{G}) = \mathrm{G} / \mathrm{I}(\mathrm{G})$.

(viii) Define the anabelian Frobenius element $\mathrm{Fr}(\mathrm{G})$ *as the unique element of* $\mathrm{G} / \mathrm{I}_{\mathrm{G}}$ *whose image under the natural conjugation map*

$$\mathrm{conj}\colon \ \mathrm{G} / I(\mathrm{G}) \to \mathrm{Aut}(I(\mathrm{G})/P(\mathrm{G}))$$

is multiplication by $p(\mathrm{G})^{f(\mathrm{G})}$.

Proof. Calculate $\mathrm{G}^{ab} /\mathrm{tor} \cong \widehat{\mathbb{Z}} \times \mathbb{Z}_p^d$. Recall that $\widehat{\mathbb{Z}} \cong \prod \mathbb{Z}_l$ and $\mathbb{Z}_p/l\mathbb{Z}_p$ is equal $\mathbb{Z}/p\mathbb{Z}$ if $p = l$ and zero otherwise. If $l \neq p$ then $(\mathrm{G}^{ab} /\mathrm{tor})/(l\, \mathrm{G}^{ab} /\mathrm{tor}) \cong \mathbb{Z}/l\mathbb{Z}$; if $l = p$ then $((\mathrm{G}^{ab} /\mathrm{tor})/(l\, \mathrm{G}^{ab} /\mathrm{tor})) \cong (\mathbb{Z}/p\mathbb{Z})^{d+1}$, so (i) and (ii) follow. Since $\mathbb{Z}_p$ is torsionfree $\mathrm{G}^{ab}_{\mathrm{tor}} = \mathbb{F}_q^\times \times \mathbb{Z}/p^a\mathbb{Z}$ and (iii) follows. For (iv) remark that k is a separable extension of $\mathbb{Q}_p$ and its valuation is discrete - in that case the stated equality holds, see Chapter II, Proposition 6.8 in [Neu99]. Assertions (v), (vi), (vii) follow immediately from the definition. For (viii) we have the split short exact sequence

$$1 \to \mathrm{I}(\mathrm{G})/P(\mathrm{G}) \to \mathrm{G} /P(\mathrm{G}) \to \mathrm{G} / \mathrm{I}(\mathrm{G}) \to 1$$

which describes $\mathrm{G} /P(\mathrm{G})$ as a semi-direct product of the Galois modules $\mathrm{I}(\mathrm{G})/P(\mathrm{G})$ and $\mathrm{G} / \mathrm{I}(\mathrm{G}) = \mathrm{Gal}(k^{unr}/k) \cong \widehat{\mathbb{Z}}$. Now lifting elements of $\mathrm{G} / \mathrm{I}(\mathrm{G})$ to elements of G and letting them act on $\mathrm{I}(\mathrm{G})/P(\mathrm{G})$ by conjugation furnishes a well-defined action. In Theorem 1.13(iv) we computed the structure of $\mathrm{I}(\mathrm{G})/p(\mathrm{G})$ as $\mathrm{G}^{un} = \mathrm{G} / \mathrm{I}(\mathrm{G})$-module. The Frobenius action then acts as multiplication by $q = p^f$ on $\prod_{l \neq p} \mathbb{Z}_l(1)$ as required. □

Remark 1.15. Mochizuki proved that an isomorphism between the Galois groups of two p-adic fields that preserves the filtration by ramification groups induces an isomorphism between the fields ([Moc97]).

1.2 Curves

Let X be a connected scheme. Recall the following: the category of finite étale covers $\mathcal{X}_{fet}$ of X form a Galois category. A choice of basepoint $\overline{x} : \mathrm{Spec}(\overline{k}) \to X$ is equivalent to a fiber functor $F_{\overline{x}} : \mathcal{X}_{fet} \to$ Sets obtained as taking the scheme theoretic fiber $Y_{\overline{x}}$ over $\overline{x}$ for any finite etale cover $Y \to X$. The etale fundamental group is obtained as the group of automorphisms of the fiber functor $\pi_1(X, \overline{x}) := \mathrm{Aut}(F_{\overline{x}})$. The theory of etale fundamental groups unifies Galois theory and the theory of topological fundamental groups.

Lemma 1.16 (Homotopy sequence)**.** *Let X be a geometrically connected locally Noetherian scheme over a field k with a chosen separable closure $\overline{k}$. Let Π_X be its étale fundamental group. We have the fundamental exact sequence*

$$1 \to \Delta_X \to \Pi_X \to \mathrm{G}_k \to 1$$

where $\Delta_X \cong \pi_1(X_{\overline{k}})$. The group Δ_X is called the geometric *(etale) fundamental group, the Galois group G_k is sometimes called the arithmetic fundamental group.*

Proof. See [Sta16, Tag 0BTU]. □

Remark 1.17. The geometric connectivity is essential. If $X_{\overline{k}}$ is not connected, the étale fundamental group is not well defined - it depends on a choice of connected component.

Example 1.18. From the sequence we obtain a natural Galois-module structure on Δ_X. Let $g \in \mathrm{G}_k$ and lift g to $\widetilde{g}$ in Π_X. We have a natural action by conjugation on Δ_X.

More important than knowing the definitions may be understanding a number of examples.

Example 1.19. (i) The etale fundamental group of the spectrum of a field $\mathrm{Spec}(k)$ coincides with the absolute Galois group G_k.

(ii) The etale fundamental group $\pi_1(\mathrm{Spec}(\mathbb{Z})) = 0$ since any nontrivial finite extension of $\mathbb{Z}$ is ramified by Minkowski's theorem.

(iii) Similarly, $\mathbb{P}^1_k$ is etale simply connected, essentially because of Riemann-Hurwitz.

(iv) Suppose the characteristic of k is zero. The etale fundamental group of an elliptic curve E/k coincides with the Tate module $T(E) := \oplus_l \varprojlim_n E[l^n]$. The underlying abelian group is isomorphic to $\widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}$ with a natural Galois module structure induced by the action of G_k on the torsion points. This case will be examined in more detail later on. Remark that since we are implicitly working with pointed schemes the associated covers are those of elliptic curves, not of genus one curves.

(v) In general, for a smooth curve C/k the geometric etale fundamental group coincides with the profinite completion of the topological fundamental group, see Lemma 2.2 below.

Definition 1.20. A curve (i.e. a smooth integral geometrically connected one dimensional scheme of finite type over k) of genus g with r punctures is called hyperbolic if

$$2 - 2g - r < 0$$

Equivalently, the Euler characteristic is smaller than zero.

Most curves are hyperbolic, the fundamental exceptions being elliptic curves and the projective line minus zero, one or two points. The n punctures of the hyperbolic curve are also called the 'cusps' and are of great importance in the theory.

Let $X \to \mathrm{Spec}(k)$ be a scheme, and suppose $x \in X(k)$ is a k-rational point, i.e. a section $\mathrm{Spec}(k) \to X$. By functoriality of π_1, a rational point $x \in X(k)$ implies that the above exact sequence has a section (is a split exact sequence). The section conjecture is the converse statement.

Conjecture 1. Let X be a proper hyperbolic curve over a field k of characteristic 0. Let $s : \mathrm{G}_k \to \Pi_X$ be a splitting of the fundamental exact sequence

$$1 \to \Delta_X \to \Pi_X \to \mathrm{G}_k \to 1$$

then s arises from a rational point $x \in X(k)$.

Remark 1.21. Why is the section conjecture interesting? It suggests a way to prove Mordell's conjecture/ Faltings theorem using 'group-theoretic' methods; i.e. it would be enough to show that there are only finitely many sections of the homotopy sequence for hyperbolic curves. Despite significant progress, this dream has not come to fruition. It should be mentioned on the other hand that Minhyong Kim's proof of Siegel's theorem (see [Kim05]) is fundamentally based on thinking of rational points as sections, though the details differ somewhat.

Remark 1.22. The section conjecture is false in some settings, e.g. over $\mathbb{F}_p$ [see Theorem 224 in [Sti13]].

In general, the section conjecture has been checked only in the 'trivial' case, i.e. there are examples where one can prove that no sections exist, implying that there are also no rational points.

Definition 1.23. Let k a field. If k is a subfield of a finitely generated extension of $\mathbb{Q}_p$ for some p then we call k sub-p-adic. In particular number fields and finite extensions of $\mathbb{Q}_p$ are sub-p-adic.

One direction is already known:

Theorem 1.24. *Let X/k be a hyperbolic curve over a sub-p-adic field. Then the following map from rational points to sections of the fundamental exact sequence is injective:*

$$X(k) \longrightarrow \mathrm{Sect}(\Pi_X \to G_k)/\sim$$

where the equivalence relation is induced by conjugacy by $\Delta_X = \pi_1(X_{\overline{k}})$.

Let $\mathcal{V}$ be a given class of schemes, and for all $X \in \mathcal{V}$, let Π_X its étale fundamental group. The Anabelian Grothendieck conjecture is the assertion that Π_X determines the scheme X. There are a couple of basic distinctions in the precise way we can ask what is meant by this assertion.

The first distinction is between the Hom-version and the Isom-version of the Grothendieck conjecture. That means that we have functoriality with regard to all morphisms between schemes or just isomorphisms.

The second distinction is that between relative and absolute anabelian geometry. In relative anabelian geometry we start with the étale fundamental group $\Pi_X^{\dagger}$ together with a projection $\Pi_X^{\dagger} \to G_k$, and we ask about morphisms over the field k. In absolute anabelian geometry, on the other hand, we start with just the étale fundamental group $\Pi_X^{\dagger}$ and ask about maps of schemes. The absolute conjecture trivially implies the relative conjecture.

Historically, the first breakthrough was Tamagawa's proof of the absolute Isom-conjecture for affine curves. The base field may be either a number field or a finite field. This is very surprising since finite fields themselves are not anabelian, seeing as the absolute Galois group of $\mathbb{F}_p$ is independent of p!

Theorem 1.25 (see[Tam97])**.**

1. (Theorem 0.6 of [Tam97]) *Let X_i be smooth connected affine curves over finite fields $F_i, i = 1, 2$. Then*

$$\mathrm{Isom}(X_1, X_2) \cong \mathrm{Isom}^{out}(\Pi_1, \Pi_2)$$

2. (Theorem 0.4 of [Tam97]) *Let X_i be smooth connected affine hyperbolic curves over finitely generated fields $F_i, i = 1, 2$ of characteristic 0. Then*

$$\mathrm{Isom}(X_1, X_2) \cong \mathrm{Isom}^{out}(\Pi_1, \Pi_2)$$

Mochizuki soon proved a much stronger result using different methods:

Theorem 1.26 (Relative Anabelian Hom Conjecture, Theorem A of [Moc99])**.** *Let X, Y be hyperbolic curves over a sub-p-adic field k. Let $\Pi_X \to G_k$ respectively $\Pi_Y \to G_k$ be their étale fundamental groups together with their projection to G_k. We have a natural bijection*

$$\mathrm{Hom}_k^{dom}(X, Y) \cong \mathrm{Hom}_{\mathrm{G}_k}^{out}(\Pi_X, \Pi_Y)$$

where $\mathrm{Hom}_k^{dom}(X, Y)$ denotes dominant morphisms over k and $\mathrm{Hom}_{\mathrm{G}_k}^{out}(\Pi_X, \Pi_Y)$ denotes open outer homomorphisms over G_k.

Remark 1.27. Notwithstanding the fact that the theorem is stated in a completely bi-anabelian way, the proof of the theorem actually furnishes a mono-anabelian algorithm that reconstructs X from $\Pi_X^\dagger \to \mathrm{G}_k$, functorial with respect to open outer continous homomorphisms of profinite groups over G_k. The proof of the theorem is a technical tour de force and will not be covered here.

In our terminology, this has the advantage of applying to the Hom version but the disadvantage of being relative.

In Section 4.3 of [Moc03], Mochizuki generalized the main result of [Moc99] to the case that k is *generalized sub-p-adic*, i.e. a subfield of a finitely generated field extension of the maximal unramified extension of $\mathbb{Q}_p$.

Although this will not be of further interest to us, the following was also proven in [Moc99]:

Theorem 1.28 (Birational Relative Anabelian Hom-conjecture, Theorem B of [Moc99])**.** *Let M, L be function fields of strictly positive transcendence degree over the sub-p-adic field k. We have a natural bijection*

$$\mathrm{Hom}_k(\mathrm{Spec}(M), \mathrm{Spec}(L)) \cong \mathrm{Hom}^{out}_{\mathrm{G}_k}(\mathrm{G}_M, \mathrm{G}_L)$$

where the Hom*-sets are as above. From the proof, there is a functorial algorithm that reconstructs* $\mathrm{Spec}(M)$ *from its Galois group* G_M.

It should be noted that F. Pop had already proven a version of this theorem in which k is finitely generated over its prime field.

Remark 1.29. The above theorems were proven in the 90's, before the distinction between reconstruction and fully-faithfulness results was fully appreciated, hence are stated in a 'bi-anabelian' way in the original papers. Mochizuki claims that all known anabelian results can be stated as a mono-anabelian reconstruction algorithm, except for Neukirch-Uchida (which is now solved by Hoshi). See p.7 of [Moc15]. The paper [Moc15] is not the first to consider the importance of explicit anabelian reconstruction. The distinction was appreciated earlier, under different terminology, but as far as I know it was never applied.

By forgetting the projection to G_k, the absolute results imply relative results. Can we go the other way? The first result in this direction is the reconstruction of the geometric fundamental group.

Theorem 1.30 (Reconstruction of the geometric fundamental group, Lemma 1.1.4 of [Moc04])**.** *Let Π_X be the étale fundamental group of a hyperbolic curve X over a number field or p-adic field k. Then there is a functorial algorithm that reconstructs the geometric fundamental group as an open subgroup*

$$\Pi_X^\dagger \mapsto (\Delta_X^\dagger \subset \Pi_X^\dagger)$$

functorially with respect to open immersions.

For number fields we then have:

Theorem 1.31 (Absolute Anabelian conjecture over number fields)**.** *Let X, Y be hyperbolic curves over a number field k. Then*

$$\mathrm{Isom}^{dom}(X, Y) \cong \mathrm{Isom}^{out}(\Pi_X, \Pi_Y)$$

Proof. From $\Pi_X^\dagger$ we may reconstruct $\Delta_X^\dagger$. Subsequently reconstruct $\mathrm{G}_k^\dagger$ as $\mathrm{G}_k^\dagger := \Pi_X^\dagger/\Delta_X^\dagger$ hence the homotopy sequence

$$1 \to \Delta_X^\dagger \to \Pi_X^\dagger \to G_k^\dagger \to 1$$

by the mono-anabelian reconstruction algorithm furnished by the relative Hom-conjecture for hyperbolic curves we may reconstruct the curve $X^\dagger$. We get an isomorphism

$$\mathrm{Hom}_k^{dom}(X, Y) \cong \mathrm{Hom}_{\mathrm{G}_k}(\Pi_X, \Pi_Y)$$

as well as on the isomorphisms sets. Let $\beta \in \mathrm{Hom}(\Pi_X, \Pi_Y)$ not necessarily over G_k. We obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Delta_X^\dagger & \longrightarrow & \Pi_X^\dagger & \longrightarrow & G_k^\dagger & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle\alpha} & & \\ 0 & \longrightarrow & \Delta_Y^\dagger & \longrightarrow & \Pi_Y^\dagger & \longrightarrow & G_k^\dagger & \longrightarrow & 0 \end{array}$$

by the Neukirch-Uchida the theorem follows. □

Remark 1.32. Can we also apply the above argument in the case of p-adic fields? No! The issue is slightly subtle; suppose we have a open continuous outer morphism $f\colon \Pi_X^\dagger \to \Pi_Y^\dagger$ over a p-adic fields k. Reconstructing the geometric fundamental groups $\Delta_X^\dagger \subset \Pi_X^\dagger, \Delta_Y^\dagger \subset \Pi_Y^\dagger$ yields a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Delta_X^\dagger & \longrightarrow & \Pi_X^\dagger & \longrightarrow & G_k^\dagger & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle\alpha} & & \\ 0 & \longrightarrow & \Delta_Y^\dagger & \longrightarrow & \Pi_Y^\dagger & \longrightarrow & G_k^\dagger & \longrightarrow & 0 \end{array}$$

In spite of the fact that it looks as if we obtained the desired functoriality, there is a subtle problem: we don't know whether α arises from a geometric morphism of fields. It might be an exotic isomorphism!

Remark 1.33. In [Moc12], example 2.13, Mochizuki constructs two étale fundamental groups of hyperbolic curves X_i and a morphism $\phi\colon \Pi_{X_1}^\dagger \to \Pi_{X_2}^\dagger$ such that $\phi(\Delta_1) \not\subset \Delta_2$ where Δ_i are the corresponding geometric fundamental groups. Since every geometric morphism $f : X_1 \to X_2$ must induce a morphism f_* such that $f_*(\Delta_1) \subset \Delta_2$ we conclude that in general the absolute anabelian Hom-conjecture for hyperbolic curves is false!

Remark 1.34. In spite of the fact that the 'relative' versus 'absolute' condition seems rather technical, it is in fact of great importance in the theory. It is correspondingly difficult to obtain absolute results in the p-adic fields due to the presence of exotic automorphisms. By a novel technique called 'cuspidalization,' it has now been possible to obtain absolute results.

Recall the famous Belyi theorem

Theorem 1.35 (Belyi)**.** *A smooth projective curve X over $\mathbb{C}$ is defined over a number field, if and only if there exists a non-constant morphism $t : X \to P^1_{\mathbb{C}}$ unramified outside* $0, 1, \infty$.

Proof. See e.g. [Kö]. □

The theorem underlies the following definitions:

Definition 1.36. Let X_i be hyperbolic curves, $i = 1, 2$. Then we shall say X_1, X_2 are isogenous if there exists a hyperbolic curve X and finite etale maps $X \to X_i$ for $i = 1, 2$.

Definition 1.37. Let L/k be an extension of fields. Given a scheme X/L we say that X is defined over k if there exists a scheme Y/k such that $Y_L \cong X$.

Definition 1.38. A hyperbolic curve X is said to be of strictly Belyi type if it defined over a number field and is isogenous to a hyperbolic curve of genus zero.

We will see that for curves of strictly Belyi type the absolute anabelian Hom-conjecture holds.

Remark 1.39. How strict is this condition? One way to formalize whether a condition on curves is very strict or quite lenient is asking whether the set of points determined by this class of curves of type

(g, r) is Zariski dense in $M_{g,r}$. As suggested by the terminology, for $2g - 2 + r \geq 3$ and $g \geq 1$ the set of strictly Belyi curves is not Zariski dense in $M_{g,r}$. See Theorem B in [Moc98] and use Riemann-Hurwitz. There are also notions of 'Belyi curves' and 'quasi-Belyi curves'; a similar theory can be set up for them, but we won't need them later on. At the time of writing it is not clear whether they are Zariski dense in $M_{g,r}$. See remark 31 in [Moc07a].

The following is the main theorem of [Moc15]. In the following sections we will go through the entire proof.

Theorem 1.40 (Absolute Anabelian geometry of curves of strictly Belyi type, Theorem 1.9 of [Moc15])**.** *Let X be a hyperbolic curve of strictly Belyi type over a p-adic field or a number field k. Let $\overline{k}$ a separable algebraic closure of k. There exists a functorial 'group-theoretic' algorithm for reconstructing from $\Pi_X^\dagger$ the function field and the base field of X.*

$$\Pi_X^\dagger \mapsto \Pi_X^\dagger \twoheadrightarrow \mathrm{G}_k^\dagger \curvearrowright \overline{k}$$

and

$$\Pi_X^\dagger \mapsto \Pi_X^\dagger \curvearrowright \overline{K}(X)$$

where $K(X)$ denotes the function field of X.

Proof sketch. The algorithm is reasonably involved consisting roughly of eight steps.

1. **Geometric fundamental group** Reconstruction of the geometric fundamental groups. This is section 2.1.

2. **The decomposition and inertia groups** Reconstruct the inertia and decomposition groups I_x, D_x for $x \in \overline{X}$ the compactification of X. See [Nak90], [Nak97], and [Sti12] for the number field case. See Lemma 1.3.9 of [Moc04] for the p-adic case. See also [Moc07b] and [Moc12]. This is section 2.2.

3. **Belyi Cuspidalization** Recover the family $\Pi_U \twoheadrightarrow \Pi_X$ corresponding to open subschemes $U \subset X$, together with the collection of inertia decomposition groups of the cusps. Said differently, we can reconstruct the topology on X group-theoretically. This is section 2.4.

4. **Synchronization of Geometric Cyclotomes** Find a canonical isomorphism $I_x \to M_X \cong \widehat{\mathbb{Z}}(1)$ for all cuspidal decomposition groups I_x. This M_X is called the 'global cyclotome'. This is section 2.3

5. **Cuspidal Principal Divisors** Characterize the group of principal cuspidal divisors inside the group of divisors on the subschemes $U \subset X$ as a certain subset of the Galois cohomology group $H^1(\Pi_U, M_X)$. This step and the following two steps are covered in section 2.5.

6. **Kummer classes of rational functions** The Kummer classes of constant and nonconstant rational functions can be characterized as a certain subgroup of the cuspidal principal divisors from step 3. This is done using the important technique of '*Kummer evaluation*'.

7. **Reconstruction of the additive structure** Using an old trick due to Uchida one reconstructs the additive structure on the multiplicative group of rational functions described in Step 4. This uses the elementary theory of divisors and *Kummer evaluation*.

8. **Reconstruction of the full function field** In the earlier steps we only recovered the 'NF-part' of the function field, This will not be covered in this thesis to save space, though it is not so difficult [see Corollary 1.10 in [Moc15]].

□

Corollary 1.41 (Absolute Mono-anabelian reconstruction of strictly Belyi Curves)**.** We may reconstruct a strictly Belyi curve X over a p-adic field or number field from its étale fundamental group $\Pi_X^{\dagger}$.

Proof. By the theorem above we reconstructed the function field of X. Since X is a smooth curve we may reconstruct the smooth compactification $X \hookrightarrow \overline{X}$. By reconstruction of the cuspidal inertia groups we know the cusps of X. □

2 Absolute Anabelian geometry and Belyi Cuspidalization

2.1 Recovery of the Geometric Fundamental group

In the following we make the first step towards reducing a relative anabelian reconstruction result to an absolute anabelian result.

Definition 2.1. A group Π is topologically finitely generated if it contains an open dense subgroup that is finitely generated.

Lemma 2.2. *Let X be a curve of genus g with r punctures over a field k of characteristic zero. The geometric fundamental group Δ_X is isomorphic to the profinite completion of*

$$\langle a_i, b_i, c_j \mid \prod_{i=1}^{g}[a_i, b_i] \prod_{j=1}^{r} c_j = 1\rangle$$

Proof. The proof follows essentially from a prototypical GAGA-result: the Riemann existence theorem which states that category of finite etale covers of X is equivalent to the category of finite analytic covers of the complex analytification X^{an}. The above explicit description is of course the description of the topological group of the Riemann surface X^{an}. This is the case for k a subfield of the complex numbers; for a general field k of characteristic zero we make use of an instance of the Lefshetz principle. For an extension L/k where L, k are both algebraically closed we obtain a map $X_L \to X$ which is homeomorphism on the underlying topological spaces. It follows from Corollary 1.5.3 in [Maj] that the resulting etale fundamental groups (in particular the geometric fundamental groups) are isomorphic. For a complete proof see Exposé XII, Corollaire 5.2 in [Gro63]. □

We see from the explicit description that the geometric fundamental group of a curve is topologically finitely generated.

The reconstruction of the geometric fundamental group is true in great generality, see sections 1 and 2 of [Moc12], but we will only consider the case of curves over p-adic fields and number fields. Moreover, we will examine both cases separately.

2.1.1 The case of a number field

In the following k will be a number field.

Lemma 2.3 (Tamagawa)**.** *Let X be a variety over a number field k. Suppose Δ_X is topologically finitely generated. Then we can characterize Δ_X as the unique maximal closed normal subgroup of Π_X that is topologically finitely generated. That is*

$$\Delta_X = \bigcap_i \Delta_i$$

where $\Delta_i \subset \Pi_X$ is any closed normal and topologically finitely generated subgroup.

Proof. From the homotopy exact sequence

$$1 \to \Delta_X \to \Pi_X \xrightarrow{p} \mathrm{G}_k \to 1$$

we get $\Delta_X = \ker(p)$. The kernel $\ker(p)$ is closed and normal and it is also topologically finitely generated (since Δ_X is from the explicit description we saw earlier).

Let Δ_0 be a closed normal topologically finitely generated subgroup of Π_X. Because p is surjective and open (since we have a projection) the image under p is also normal and closed. Since p is open the image is topologically finitely generated. By the lemma below we conclude that the image is trivial, i.e. lies in $\ker(p) = \Delta_X$. Hence Δ_X is the maximal closed normal and topologically finitely generated subgroup. □

Lemma 2.4. *Every topologically finitely generated subgroup of G_k which is normal and closed is trivial.*

For the proof we will use the theory of 'Hilbertian' fields. A good reference is chapter 15 in [FJ86]. Beware that there are several editions out there, the oldest (1986) is the correct one.

Definition 2.5. A field k of characteristic is said to be Hilbertian if for every irreducible polynomial $P(T, X)$ the set of $a \in k$ such that $P(a, X)$ is irreducible is Zariski dense. A set of such 'a's is called a k-Hilbertian set.

Example 2.6.

- The rational numbers $\mathbb{Q}$ form a Hilbertian field. This is the content of Hilbert irreducibility theorem.
- A finite extension of Hilbertian fields is Hilbertian.
- Abelian extensions of Hilbertian fields are Hilbertian. This result is due to Kuyk.

The algebraic closure $\overline{k}$ of a Hilbertian field k is not Hilbertian. Indeed $X^2 - T$ is irreducible for such $\overline{k}$ but $X^2 - a = (X - \sqrt{a})(x + \sqrt{a})$ for all $a \in \overline{k}$.

Theorem 2.7 (Weissauer)**.** *Let k be a Hilbertian field and L a—possibly infinite—Galois extension of k. Suppose M is a nontrivial finite extension of L. Then M is Hilbertian.*

Proof. See Corollary 12.15 in [FJ86]. □

A group G is said to be realizable over a field k if there exists a Galois extenstion L such that $\mathrm{Gal}(L/k) \cong G$. We will see that Hilbertian fields allow for 'many' independent finite extensions hence may realize arbitrary product of finite abelian groups hence are not topologically finitely generated.

Proof of the lemma. The number field k is a Hilbertian field. Let N be a nontrivial closed normal subgroup of G_k; it corresponds to a Galois extension L of k. Suppose N is topologically finite generated; i.e. it has a open finitely generated subgroup G_M corresponding to a nontrivial finite extension M of L. From the lemma we know M is Hilbertian. We want to show G_M is not finitely generated since in this case we are done.

Remark that $X^2 - T$ is irreducible over M so there is a $\alpha_1 \in M$ such that $X^2 - \alpha_1$ is irreducible. Set $M_1 := M[X]/X^2 - \alpha_1$. But as $X^2 - T$ is still irreducible over M_1 we can apply the same trick again to obtain a $\alpha_2 \in M$ such that $X^2 - \alpha_2$ is irreducible over M_1. By taking the compositum of $M_1, \cdots, M_n$ we get an increasing sequence of Galois extensions of M with Galois group $(\mathbb{Z}/2\mathbb{Z})^n$; since these are quotients of G_M we conclude G_M cannot be finitely generated. □

2.1.2 The case of a p-adic field

Now we'll continue with the p-adic case. From now one assume $k/\mathbb{Q}_p$ be finite, $\mathrm{G} = \mathrm{G}_k$ the absolute Galois group. We have the following elementary lemma.

Lemma 2.8 (Arithmetic and Geometric factorization of Covers)**.** *Suppose X and Y are curves over k. Let $Y \to X$ be a finite étale cover. Then this cover splits into a geometric and an arithmetic part.*

$$\begin{array}{ccc} Y & & \\ \downarrow & \searrow & \\ & & X_L \\ \downarrow & \swarrow & \\ X & & \end{array}$$

where $X_L \to X$ is 'arithmetic', meaning it is simply induced by basechange of the base field $k \to L$, and $Y \to X_L$ is geometric which means that the extension of the constant field of the function field is trivial. On the group-theoretic side we have the following diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_Y & \longrightarrow & \Pi_Y & \longrightarrow & \mathrm{G}_L & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \Delta_{X_L} & \longrightarrow & \Pi_{X_L} & \longrightarrow & \mathrm{G}_L & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \Delta_X & \longrightarrow & \Pi_X & \longrightarrow & \mathrm{G}_k & \longrightarrow & 1 \end{array}$$

where we have the projection $\Pi_Y \to \mathrm{G}_L$ since $Y_L = Y$. In particular for any open subgroup $\Pi_0 \subset \Pi_X$ we have the equality of degrees $[\Pi_X : \Pi_0] = [\Delta_X : \Delta_0][\mathrm{G}_k : \mathrm{G}_0]$.

Proof. Indeed $Y \to X$ corresponds to an open subgroup $\Pi_Y \subset \Pi_X$. Set $\Delta_Y \coloneqq \Pi_Y \bigcap \Delta_X$ and $\mathrm{G}_L \coloneqq \mathrm{Im}(\Pi_Y \to \mathrm{G}_k)$. We obtain the homotopy exact sequence

$$1 \to \Delta_Y \to \Pi_Y \xrightarrow{p} \mathrm{G}_L \to 1$$

Now set $\Pi_{X_L} = p^{-1}(\mathrm{G}_L)$ and $\Delta_{X_L} = \ker(\Pi_{X_L} \to \mathrm{G}_L)$. The statement follows. $\square$

The idea of the reconstruction of the geometric fundamental group of a hyperbolic curve over a p-adic field will be as follows. We want to consider only 'geometric' covers. That means covers corresponding to an open subgroup $\Pi_0 \subset \Pi_X$ such that $[\Pi_0 : \Pi_X] = [\mathrm{G}_0 : \mathrm{G}_k]$ where $\mathrm{G}_0 \coloneqq \mathrm{Im}(\Pi_0) \subset \mathrm{G}_k$. The geometric fundamental group Δ_X will then be the intersection of the open subgroups Π_0. Of course on first glance the $[\mathrm{G}_0 : \mathrm{G}]$ is dependent on the Galois group G which is the object we are trying to reconstruct; we will see it is possible to characterize the above degree without reference to G.

Our first step will be to recover the residue characteristic from $\Pi = \Pi_X$ (as opposed to G, where we saw that it is possible earlier).

Definition 2.9. Let H be a profinite group. Define

$$\dim_{\mathbb{Q}_l}(H) \coloneqq \dim_{\mathbb{Q}_l}(H^{\mathrm{ab}} \widehat{\otimes}_{\widehat{\mathbb{Z}}} \mathbb{Q}_l)$$

Lemma 2.10. *Let l be a prime.*

$$\dim_{\mathbb{Q}_l}(\mathrm{G}^{\mathrm{ab}}\,\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Q}_l) = \begin{cases} [k\colon \mathbb{Q}_l]+1 & l=p \\ 1 & l\neq p \end{cases}$$

where $\widehat{\otimes}_{\widehat{\mathbb{Z}}}$ denotes the completed tensor product which is simply the completion of the usual tensor product. If we are working with modules over $\mathbb{Q}_l$ we even have the tensor norm.

Proof. Let $d := [k : \mathbb{Q}_p]$.

First I claim that

$$\mathbb{Z}_p\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Q}_l = \begin{cases} \mathbb{Q}_l & l=p \\ 0 & l\neq p \end{cases}$$

note that $a\widehat{\otimes}_{\widehat{\mathbb{Z}}}b = p^n a\widehat{\otimes}_{\widehat{\mathbb{Z}}}p^{-n}b$; hence every element is arbitrarily small in the tensor norm induced by the p-adic, respectively l-adic norms on $\mathbb{Z}_p, \mathbb{Q}_l$. We conclude the resulting group equals the zero group.

We compute

$$\begin{aligned}
\dim_{\mathbb{Q}_l}(\mathrm{G}^{\mathrm{ab}}\,\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Q}_l) &= \dim_{\mathbb{Q}_l}(\widehat{k}^{\times}\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Q}_l) \\
&= \dim_{\mathbb{Q}_l}(\widehat{\mathcal{O}_k^{\times}\times\pi\mathbb{Z}}\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Q}_l) \\
&= \dim_{\mathbb{Q}_l}(\widehat{\mu_k}(\widehat{1+\pi\mathcal{O}_k})\times\widehat{\pi\mathbb{Z}}\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Q}_l) \\
&= \dim_{\mathbb{Q}_l}((\widehat{\mathbb{Z}}\times\mathbb{Z}_p^d)\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Q}_l) \\
&= \dim_{\mathbb{Q}_l}(\widehat{\mathbb{Z}}\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Q}_l) + \dim_{\mathbb{Q}_l}(\mathbb{Z}_p^d\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Q}_l) \\
&= \begin{cases} [k\colon \mathbb{Q}_l]+1 & l=p \\ 1 & l\neq p \end{cases}
\end{aligned}$$

□

Remark 2.11. The profinite tensor product $\widehat{\otimes}_{\widehat{\mathbb{Z}}}$, the topological tensor product over $\widehat{\mathbb{Z}}$, is essential. The regular tensor product over $\mathbb{Z}$ given as $\mathbb{Z}_p\otimes_{\mathbb{Z}}\mathbb{Z}_q$ is $\neq 0$.

Definition 2.12. A *central extension* of a group G is a short exact sequence of groups

$$1\to A\to E\to \mathrm{G}\to 1$$

such that A is in $Z(E)$ the center of the group E. It is a well-known fact that the set of isomorphism classes of central extensions of G by A is in bijection with the cohomology group $\mathrm{H}^2(\mathrm{G}, A)$.

Lemma 2.13 (Recovery of residue characteristic from Π_X, as opposed to G_k.)**.** *Let $\Pi_X \twoheadrightarrow \mathrm{G}_k$ be the étale fundamental group of a curve X/k together with the natural map to the Galois group of the base field. Let Π be an isomorph of Π_X,* G *an isomorph of G_k. Let $\Pi_0\subset\Pi$. Then for prime numbers $l\neq l'$*

$$\left|\dim_{\mathbb{Q}_{l'}}(\Pi_0)-\dim_{\mathbb{Q}_l}(\Pi_0)\right| = \begin{cases} [k\colon \mathbb{Q}_p] & l=p \\ 0 & l,l'\neq p \end{cases}$$

The residue characteristic $p(k)$ can be characterized as the unique prime p such that the above expression is nonzero for $l=p$ and all primes $l'\neq l$. Similarly, the absolute degree $d=[k:\mathbb{Q}_p]$ may be characterized using the above equation.

Proof. We only consider Π, the proof goes through just the same for Π_0. Consider the short exact sequence induced by the abelianisation of Π

$$0 \to \mathrm{Im}(\Delta) \to \Pi^{\mathrm{ab}} \to \mathrm{G}^{\mathrm{ab}} \to 0$$

in general it is *not* true that $\mathrm{Im}(\Delta) = \Delta^{\mathrm{ab}}$. We do have a map $\Delta^{\mathrm{ab}} \twoheadrightarrow \mathrm{Im}(\Delta)$, as $\mathrm{Im}(\Delta) \subset \Pi^{\mathrm{ab}}$ so we obtain a morphism by the universal property of abelianisation. Let $\Delta^{\mathrm{ab}} \twoheadrightarrow Q$ be the maximal torsion-free quotient on which G acts trivially. We have a natural surjection $Q \twoheadrightarrow \mathrm{Im}(\Delta)/\mathrm{tor}$. This is because G acts on $\mathrm{Im}(\Delta)$ through G^{ab} by conjugation so the action is trivial and $\mathrm{Im}(\Delta)/\mathrm{tor}$ is torsion free and Q is the maximal such quotient of Δ^{ab}. We have the following diagram

$$\begin{array}{ccccc}
\Delta^{\mathrm{ab}} & \longrightarrow & \Pi^{\mathrm{ab}} & \twoheadrightarrow & \Pi^{\mathrm{ab}}/\mathrm{tor} \\
\downarrow & \searrow\!\!\!\!\searrow & \nearrow & & \nearrow \\
 & & \mathrm{Im}(\Delta) & & \\
\downarrow\!\!\!\!\downarrow & & \searrow\!\!\!\!\searrow & & \\
Q & \twoheadrightarrow & \mathrm{Im}(\Delta)/\mathrm{tor} & &
\end{array}$$

We want to prove that $Q \cong \mathrm{Im}(\Delta)/\mathrm{tor}$. Below follows a proof that Q injects in $\Pi^{\mathrm{ab}}/\mathrm{tor}$ through $Q \to \mathrm{Im}(\Delta)/\mathrm{tor}$ hence $Q \to \mathrm{Im}(\Delta)/\mathrm{tor}$ is injective. We conclude $Q \cong \mathrm{Im}(\Delta)/\mathrm{tor}$.

The group $K = \ker(\Delta \to Q)$ is normal in Π; consider the quotient P. We have a short exact sequence

$$0 \to Q \to P \to \mathrm{G} \to 0$$

We have the following map of short exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Q & \overset{h_1}{\twoheadrightarrow} & P & \longrightarrow & G & \longrightarrow & 0 \\
 & & \downarrow & \overset{h}{\searrow} & \downarrow h_2 & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Im}(\Delta)/\mathrm{tor} & \longrightarrow & \Pi^{\mathrm{ab}}/\mathrm{tor} & \longrightarrow & G/\mathrm{tor} & \longrightarrow & 0
\end{array}$$

Since the action of G on Q is trivial [it acts through G^{ab} by conjugation] the extension is central, and consequently defines a class c in $\mathrm{H}^2(\mathrm{G}, Q)$. Since X has a rational point over some finite extension, there exists an open subgroup G_0 of G such that $P_0 \to \mathrm{G}_0$ admits a section s, so that the restriction of c in $\mathrm{H}^2(\mathrm{G}_0, Q)$ is 0. But the composite $\mathbf{Cor} \circ \mathbf{Res} : \mathrm{H}^2(\mathrm{G}, Q) \to \mathrm{H}^2(\mathrm{G}, Q)$ of restriction followed by corestriction is multiplication by $n = [G : G_0]$. Therefore we have $nc = 0$. We have the pushout along multiplication by $n\colon Q \to Q$

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Q & \longrightarrow & P & \longrightarrow & \mathrm{G} & \longrightarrow & 0 \\
 & & \downarrow \cdot n & & \downarrow & & \| & & \\
0 & \longrightarrow & Q & \longrightarrow & P_1 & \longrightarrow & \mathrm{G} & \longrightarrow & 0
\end{array}$$

whose class is $nc = 0$ so that this sequence splits $P_1 = Q \times G$. Therefore there is some retraction $P_1 \to Q$, whose composition with the composite $P \to P_1$ gives a morphism $f\colon P \to Q$ such that fh_1 is multiplication by n (which is injective since Q is torsionfree). We have the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Q & \longrightarrow & P & \longrightarrow & \mathrm{G} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cdot n} & & \downarrow & & \| & & \\
0 & \longrightarrow & Q & \longrightarrow & P_1 & \longrightarrow & \mathrm{G} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Im}(\Delta)/\mathrm{tor} & \longrightarrow & \Pi^{\mathrm{ab}}/\mathrm{tor} & \longrightarrow & G/\mathrm{tor} & \longrightarrow & 0
\end{array}$$

Since Q is abelian and torsion-free f factors through $\Pi^{\mathrm{ab}}/\mathrm{tor}$. That is $f = f_1 h_2$. Then $f_1 h = f h_1$ is injective and therefore h is injective.

To proceed we will make use of the following (difficult) fact.

$$Q \text{ is a finitely generated} free \widehat{\mathbb{Z}}\text{-module.} \tag{2.1}$$

The proof will come later, see Lemma 2.29. Assuming the above we compute

$$\begin{aligned}
\dim_p(\Pi) - \dim_l(\Pi) &= \dim_p(\mathrm{Im}(\Delta)) + \dim_p(\mathrm{G}) - \dim_l(\mathrm{Im}(\Delta)) - \dim_l(\mathrm{G}) \\
&= \dim_p(\mathrm{Im}(\Delta)/\mathrm{tor}) + \dim_p(\mathrm{G}) - \dim_l(\mathrm{Im}(\Delta)/\mathrm{tor}) - \dim_l(\mathrm{G}) \\
&= \dim_p(Q) + \dim_p(\mathrm{G}) - \dim_l(Q) - \dim_l(\mathrm{G}) \\
&= \dim_p(\mathrm{G}) - \dim_l(\mathrm{G}) \\
&= [k : \mathbb{Q}_p]
\end{aligned}$$

where the last equality follows from Lemma 2.10. Remark that the finiteness of $\dim_l(\mathrm{G})$ stems from the fact that we describe local Galois groups explicitly. □

Remark 2.14. Recall that we recovered the residue characteristic and the absolute degree of k already from the Galois group G_k. The above theorem shows that we can reconstruct them from Π as well.

We can reconstruct the residue characteristic $p = p(\Pi)$ and the degree $[k : \mathbb{Q}_p] = d(\Pi)$.

Lemma 2.15 (Reconstruction of the geometric fundamental group)**.** *Let X be a curve over a p-adic field $k/\mathbb{Q}_p$. The geometric fundamental group may be reconstructed in a mono-anabelian fashion from $\Pi = \Pi_X^{\dagger}$ as*

$$\Delta = \{\Pi_0 \subset \Pi \mid \Pi_0 \textit{ open, such that } \frac{\dim_p(\Pi_0) - \dim_l(\Pi_0)}{[\Pi : \Pi_0]} = [k : \mathbb{Q}_p] = d(\Pi)\}$$

Proof. First remark that

$$\frac{\dim_p(\Pi_0) - \dim_l(\Pi_0)}{[\Pi : \Pi_0]} = [k : \mathbb{Q}_p] \iff \Pi_0 = p^{-1}(G_0) \text{ with } G_0 \subset G \text{ open}$$

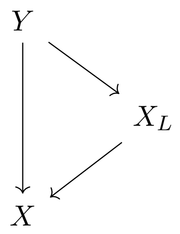
Suppose $\Pi_0 = p^{-1}(G_0)$. Let L be the fixed field of G_0; it is a finite extension of k. Then $\Pi_0 \cong \Pi_{X_L}$ by the Arithmetic and Geometric factorization of covers. In detail we have $[\Pi : \Pi_0] = [\mathrm{G} : \mathrm{G}_0]$ so

$$\frac{\dim_p(\Pi_0) - \dim_l(\Pi_0)}{[\Pi : \Pi_0]} = \frac{[L : \mathbb{Q}_p]}{[G : G_0]} = \frac{[L : k][k : \mathbb{Q}_p]}{[L : k]} = [k : \mathbb{Q}_p]$$

Conversely, suppose $\Pi_0 \subset \Pi$ open with

$$\frac{\dim_p(\Pi_0) - \dim_l(\Pi_0)}{[\Pi : \Pi_0]} = [k : \mathbb{Q}_p]$$

The subgroup Π_0 corresponds to some cover $Y \to X$. We have a factorization of covers



for a finite extension $L/\mathbb{Q}_p$. Use $[\Pi : \Pi_0] = [\Delta : \Delta_0][G : G_0]$. Now compute

$$\begin{aligned}[k : \mathbb{Q}_p] &= \frac{\dim_p(\Pi_0) - \dim_l(\Pi_0)}{[\Pi : \Pi_0])} \\ &= [L : \mathbb{Q}_p[\mathrm{G} : \mathrm{G}_0][\Delta : \Delta_0] \\ &= \frac{[L : \mathbb{Q}_p]}{[L : k][\Delta : \Delta_0]}\end{aligned}$$

hence $[\Delta : \Delta_0] = 1$ and $\Pi_0 = p^{-1}(G_0)$. □

Proposition 2.16. *Let A be an abelian variety over a field F. For simplicity assume the characteristic of F is zero. Let F^{sep} be a separable closure of F. Then the etale fundamental group Π_A of A coincides with the Tate module $T(A) = \prod_l T_l(A)$ where $T_l(A) = \varprojlim_n A[l^n]$.*

Proof sketch. For the whole argument see Corollary 10.37 and the surrounding theory in [GvdG]. The etale fundamental group Π_A is a profinite group. That means $\Pi_A \cong \varprojlim_H \Pi_A/H$ where H is a normal subgroup. Such a normal subgroup corresponds to an etale covering $f\colon B \to A$ together with a geometric point in the fibre over 0_A. By the Serre-Lang theorem we even know B is an abelian variety. This implies that $f\colon B \to A$ is a separable isogeny, in particular a Galois covering with Galois group isomorphic to $\mathrm{Ker}(f)$. The collection of isogenies $[n]\colon B/\ker[n] \to B$ is cofinal. Call this collection T. In conclusion

$$\Pi_A = \varprojlim_{f \in T} \mathrm{Ker}(f)(k) = \varprojlim_n A[n](k)$$

□

Remark 2.17. For any finite abelian group G

$$\mathrm{Hom}_{\text{conts}}(\Pi_X, G)$$

the set of continuous homomorphisms equals the set of isomorphisms classes of Galois coverings with Galois group G, see Example 11.3 of [Milb].

Proposition 2.18. *Let X be a complete smooth curve over a field k, which for simplicity we assume to be of characteristic zero. Then the abelianization of Δ_X coincides with the geometric fundamental group of the Jacobian J.*

$$\Delta_X^{\text{ab}} \cong \Delta_J$$

compatible with the outer Galois action $\mathrm{G}_k \curvearrowright \Delta_X^{\text{ab}}$. It is the Tate module of the Jacobian!

Proof sketch. For the whole argument see Proposition 9.1, Chapter III Jacobian Varieties and the surrounding theory in [Mila]. We have the Jacobian map

$$X \to J(X)$$

Let $A \to J(X)$ be a finite étale map. We know that A must be an abelian variety by the Serge-Lang theorem and that the covering is abelian. Consider the base change $Y := A \times_{J(X)} X$ along the Jacobian map. Write $J = J(X)$. This is a finite etale cover of X, by stability of finite etale maps under base change, which is abelian. Abelian coverings are classified by

$$\mathrm{Hom}(\Pi_X, \mathrm{G})$$

where we can assume for simplicity that $G = \mathbb{Z}/n\mathbb{Z}$. To conclude we need to show

$$\mathrm{Hom}(\Pi_X, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(\Pi_J, \mathbb{Z}/n\mathbb{Z})$$

but the left hand side, respectively the right hand side, is isomorphic to $\mathrm{Pic}(X)_n$, respectively $\mathrm{Pic}(J)_n$ (Corollary 9.2 Chapter III in [Mila]). These are isomorphic since the Jacobian of the Jacobian is the Jacobian (Corollary 9.3, Remark 6.10 Chapter III in [Mila]). □

Definition 2.19. A *semi-abelian variety* A over a field F is a commutative group variety A which fits in a short exact sequence

$$1 \to T \to A \to B \to 1$$

of linear algebraic groups, where B is an abelian variety and T is a torus.

Definition 2.20 (Good reduction of Abelian Varieties)**.** An *Abelian scheme* $\mathcal{A}$ over an integral base scheme S is a proper smooth group scheme over S all fibres of which are geometrically connected; this implies the fibers are abelian varieties. Let k be a finite extension of $\mathbb{Q}_p$. We say an abelian variety A/k has good reduction if there exists an abelian scheme $\mathcal{A}$ over $\mathcal{O}_k$ such that $\mathcal{A}_k \xrightarrow{\sim} A$. A semi-abelian variety J is said to be of good reduction if it is the extension of an abelian variety A of good reduction along a torus T.

Definition 2.21 (Néron Models)**.** Suppose that R is a Dedekind domain with field of fractions k, and suppose that A_k is a smooth separated scheme over k (such as an abelian variety). Then a Néron model of A_k is defined to be a smooth separated scheme A_R over R with fiber A_k that is universal in the following sense.

If X is a smooth separated scheme over R then any k-morphism from X_k to A_k can be extended to a unique R-morphism from X to A_R (Néron mapping property).

In particular, the canonical map $A_R(R) \to A_k(k)$ is an isomorphism. If a Néron model exists then it is unique up to unique isomorphism.

Theorem 2.22 (Stable reduction of abelian varieties)**.** *Let B be an abelian variety over k, let Y be the Néron model. After a finite extension of the base field, the Néron model Y of the abelian variety B over k has the following property: The identity component Y_k^o of the special fiber Y_κ, is an extension of an abelian variety by a split algebraic torus over κ.*

Proof. See Theorem 6.7.6 in [FvdP04] □

After base change of the base field we can apply the following theorem

Theorem 2.23 (Rigid uniformization of abelian varieties)**.** *Suppose an abelian variety B over a p-adic field k has a Néron model Y such that the connected component of the identity of the special fiber Y_κ^o is an extension of an abelian variety C over k by a split algebraic torus over k. Then the following holds*

- *There is an abelian scheme $\mathcal{A}$ over $\mathcal{O}_k$ and an extension $\widetilde{B}$ of $A = \mathcal{A}_k$ by a split torus S over k.*
- *a $\mathbb{Z}$-lattice $\Lambda \subset \widetilde{B}(k)$*
- *The rigid space $\widetilde{B}^{an}/\Lambda$ is isomorphic to B. The abelian variety C is canonically isomorphic to A_κ. In addition, $\widetilde{B}, \Lambda$ are uniquely determined by B.*

Proof. See Theorem 6.7.8 in [FvdP04] □

Remark 2.24. Roughly speaking, these two theorems tell us that after a change of basis *any* abelian variety is uniformized by a semi-abelian variety $\widetilde{B}$ of good reduction.

Remark 2.25. Before we continue, it is perhaps helpful to recall what we were doing and why all the preceding theory is needed. In the following, we will work with the Galois representation of the Tate module of a semi-abelian variety J. The above two theorems will be used to reduce to the case of good reduction. Recall that this semi-abelian variety J was obtained as the Jacobian $J(X)$ of our original hyperbolic curve X. The Tate module coincides with the etale fundamental group Π_J of this Jacobian $J = J(X)$ as well as the abelianization Π_X^{ab}. Finally, this will be used to prove equation (2.1) which was the final ingredient for recovering the geometric fundamental group Δ_X over the p-adic field k.

The Tate module $T(A_k)$ naturally decomposes into l-adic modules and a $p-$adic module: $T(A_k) = \prod_{l \neq p} T_l(A_k) \times T_p(A_k)$. Let us examine the case $l \neq p$ first.

Definition 2.26. A Galois representation $\mathrm{G} \curvearrowright M$ is said to be *unramified* if the induced representation is trivial on the inertia group $I(\mathrm{G})$.

Lemma 2.27 (Néron-Ogg-Shavarevich criterion)**.** *Let A be an abelian variety over a local field k with residue characteristic p. Suppose l is a prime not equal to p. Then A has good reduction over k if and only if the l-adic Tate module $T_l(A)$ of A is unramified.*

Proof. See [ST68]. □

Suppose for simplicity that B is an abelian variety of good reduction. From the Néron–Ogg–Shafarevich criterion we know that the associated l-adic Galois representation $\mathrm{G}_k \curvearrowright T_p(B) \otimes \mathbb{Q}_l$ is unramified. Since the action is unramified it is completely determined by the Galois group of the maximal unramified extension G_k^{un} which is isomorphic to the Galois group G_κ where κ is the residue field of k. The action of G_κ is determined by the Frobenius element $\mathrm{Fr} \in \mathrm{G}_\kappa$. We have a handle on how Fr acts:

Theorem 2.28 (Riemann hypothesis for Abelian varieties over finite fields)**.** *Let B be an abelian variety over a finite field $\mathbb{F}_q$. The characteristic polynomial of (a n-th iteration of) the Frobenius on $V_l(B) = T_l(B) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ is given by a polynomial $P_n(T)$*

$$P_n(T) = \prod_{i=1}^{2g} (T - \omega_i)$$

with $|\omega_i| = q^{1/2}$ for any Archimedean valuation.

Proof. See p.206 in [Mum08]. □

We are now ready for the proof of equation (2.1), which will finish the proof of Lemma 2.13, hence of Lemma 2.15.

Lemma 2.29. *Let $T(J)$ be the Tate module of J, where we suppose J is any semi-abelian variety [such as the generalized Jacobian of a smooth but possibly nonproper curve]. Then the maximal torsion-free quotient of the Tate module $T(J) \twoheadrightarrow Q$ on which G_k acts trivially is a finitely generated free $\widehat{\mathbb{Z}}$-module.*

Proof. We will need to work with $V_l(J) = T_l(J) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ the associated l-adic representations of the l-adic Tate modules. It too has a torsionfree Galois-trivial quotient which identifies as $V(J) = \prod_l V_l(J) \twoheadrightarrow Q \otimes \mathbb{Q}_l$.

Remark that we may always reduce to the case of an abelian variety. Indeed, J is the extension of a torus S and an abelian variety B

$$0 \to S \to J \to B \to 0$$

Next, consider the Tate module $T(S)$. It splits after some finite extension of the base field (which corresponds to restricting to an open subgroup of the Galois group G_k) into a sum of Tate twists $\oplus \widehat{\mathbb{Z}}(1)$ none of which have submodules that have nontrivial G_k-action [the action is by the cyclotomic character] hence the issue is reduced to a careful study of the Tate module of B.

After applying Theorem 2.23 and possibly restricting to an open subgroup of G_k -to apply semi-stable reduction- we are reduced to considering the short exact sequence

$$0 \to T(\widetilde{B}) \to T(B) \to \Lambda \otimes \widehat{\mathbb{Z}} \to 0$$

where recall $\widetilde{B}$ is 'a semi-abelian variety of good reduction'.

We will show that the surjection $T(B) \to Q$ factors through $T(\Lambda) \cong \Lambda \otimes \widehat{\mathbb{Z}}$. I claim $\widehat{\mathbb{Z}}$ is $\mathbb{Z}$-faithfully flat. Indeed, $\widehat{\mathbb{Z}}$ is $\mathbb{Z}$-flat since it is the direct product of $\mathbb{Z}_p$ which are completions along the prime p which implies flatness. It also faithfully flat by the criterion that a module M over a ring R is flat over R if for all maximal ideals $m \subset R$ we have $mM \neq M$ (see Proposition 9.3 in [Mat]). Since $\mathbb{Q}$ is torsion free we have the factorization. So we have to prove that $T(\widetilde{B}) \to Q$ is the zero map.

As stated above, $\widetilde{B}$ is of 'good reduction' meaning [cf Theorem 2.23]

$$0 \to T(S) \to T(\widetilde{B}) \to T(A_k) \to 0$$

where A has good reduction over k and S is a torus. As we did earlier we can immediately reduce to A_k, as above.

For $l \neq p$ the Neron-Ogg-Shavarevich criterion tells us that $T_l(A_k)$ is unramified; in other words, it is completely determined by the Galois module $T_l(A_\kappa)$. We have the associated l-adic representation $V_l(A_\kappa)$. By the Riemann Hypothesis for Abelian varieties over finite fields [Theorem 2.28] we see that every nonzero submodule of $V_l(A_\kappa)$ is nontrivial. Hence, $V_l(A_\kappa) \to Q \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l$ is zero; by faithfull flatness this means that $T_l(A_\kappa \to Q$ is zero.

Next, we consider the case $l = p$. Consider the exact sequence

$$0 \to T_p^o(A_k) \to T_p(A_k) \to T_p(A_\kappa) \to 0$$

obtained by $T_p(A_k) \to T_p(A_\kappa)$; the group $T_p^o(A_k)$ is simply the kernel. Consider the p-divisible groups $A_k[p^\infty], A_\kappa[p^\infty], A[p^\infty]$. We have the Galois action of G_k on $A_k[p^\infty]$; the main theorem of [Tat67][Theorem 4.1] now states that this action lifts uniquely to $A[p^\infty]$. From the p-divisible groups $A_k[p^\infty], A_\kappa[p^\infty], A[p^\infty]$ we may obtain the p-adic Tate modules compatible with the Galois action. Hence we have a corresponding map of p-divisible groups

$$0 \to K \to A_k[p^\infty] \to A_\kappa[p^\infty] \to 0$$

where K is the kernel [corresponding to $T_p(A_k)^o$]. Given a map $T_p(A_k) \to Q$ we have a corresponding map on p-divisible group: consider the kernel $\ker(T_p(A_k) \to Q)$ and mod out by p^n; this yields a submodule of the p^n-torsion of $T_p(A_k)[p^n]$ and form an inductive system, hence it is a p-divisible group.

For any $n \in \mathbb{N}$ the etale part of the n-torsion $A[n]^{et}$ is a locally constant sheaf on $A \to \mathcal{O}_k$. The only possible p-torsion is a group scheme $H[n]$ obtained as a successive group extension of $\mathbb{Z}/p\mathbb{Z}$'s [since μ_p is not etale in characteristic p, hence not etale over $\mathcal{O}_k$]. This means that $H[n]$ is a constant group scheme hence $H[n](k) \cong H[n](\kappa)$. After modding out by $H[n]$ we may assume that $A[n]^{et}$ is a locally constant sheaf with torsion at any stalk prime to p. Since $A \to \mathcal{O}_k$ is smooth and proper we may apply the proper smooth basechange theorem in etale cohomology [Milb][Theorem 20.4] to conclude that

$$A[n]^{et}(k) \cong \mathrm{H}^0_{et}(A_{\overline{k}}, A[n]^{et}) \xrightarrow{\sim} \mathrm{H}^0_{et}(A_{\overline{\kappa}}, A[n]^{et}) \cong A[n]^{et}(\kappa)$$

is an isomorphism. I conclude that on the etale part $A_k^{et}[p^\infty] \to A_\kappa^{et}[p^\infty]$ is an isomorphism. This means that K is connected.

The abelian variety A_k is of good reduction hence the Galois representation given by the p-adic Tate module $T_p(A_k)$ is crystalline [this is the Neron-Ogg-Shavarevich criterion is characteristic p, see [CI99]]. Quotient of crystalline representation are crystalline hence Q is crystalline and we can talk about its Dieudonne module.

Apply the Dieudonne functor to the short exact sequence of p-divisible groups to obtain the short exact sequence

$$0 \to D(K) \to D(A_k[p^\infty]) \to D(A_\kappa[p^\infty]) \to 0$$

It follows from Theorem 4 of [Wei] that since K is a connected p-divisible group its Dieudonne module $D(K)$ has the property that the Frobenius is topologically nilpotent; meaning that $\mathrm{Fr}^n(x) \to 0$. Therefore under $p : D(T_p(A_k)) \to D(Q)$ we have $p(x) = \mathrm{Fr}^n\, p(x) = p(\mathrm{Fr}^n\, x) = p(0) = 0$. By the equivalence of categories between p-divisible groups and Dieudonne modules this implies that the corresponding map for p-divisible groups, hence also on the p-adic Tate module $T_p(A_k)^o \to Q$ is zero.

The argument above now implies that the map $T_p(A_k) \to Q$ factors through $T_p(A_\kappa)$. Next, suppose by contradiction that $V_p(A_\kappa) \to Q \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ is nontrivial; then it has an eigenvalue 1. So the characteristic polynomial of the Frobenius has a root equal to 1, but by the Honda-Tate theorem the only eigenvalues that can occur have absolute value $\sqrt{p^f}$ where $q = p^f$, see [Tat71].

□

2.2 Reconstruction of the Cuspidal Inertia groups

In this section and all other sections X is a hyperbolic curve over a p-adic field or number field k unless stated otherwise.

Definition 2.30. Let k be an arbitrary field, l an invertible prime. Let X/k be a smooth projective variety. The l-adic etale cohomology

$$\mathrm{H}^n(X_{\overline{k}}, \mathbb{Q}_l)$$

is a finite dimensional $\mathbb{Q}_l$-vector space with a continuous action of G_k. This follows from the functoriality of etale cohomology; let $\sigma \in \mathrm{G}_k$ act on $X_{\overline{k}} = X \times_k \overline{k}$ as $id \times \sigma$; by the functoriality we have a morphism $(id \times \sigma)^* \colon \mathrm{H}^n(X_{\overline{k}}, \mathbb{Q}_l) \to \mathrm{H}^n(X_{\overline{k}}, \mathbb{Q}_l)$.

Next consider the case that $k = \mathbb{F}_q$.

Definition 2.31. Let U be a variety over $\mathbb{F}_q$. Consider the absolute Frobenius map $\mathrm{Fr}_U : U \to U$. For each closed point $x \in U$ we can consider the Frobenius morphism Fr_x by looking at the action of Fr_U on the residue field $k(x)$. A finite dimensional $\mathbb{Q}$-vector space V with a continuous action of Π_U is said to have weight n [which may be a fraction] if for all closed points $x \in U$ each eigenvalue of

$$\mathrm{Fr}_x : V \to V$$

is an algebraic number all of whose conjugates have absolute value $q^{n \deg(x)}$.

Example 2.32. The Galois module $\mathbb{Q}_l(1)$ has weight 1. The Galois module $\mathbb{Q}_l(n) = \otimes^n \mathbb{Q}_l(1), n \in \mathbb{Z}$ has weight n.

Caution 2.33. Be warned that there is a different convention for weights where $\mathbb{Q}_l(1)$ has weight -2, which is more natural from a certain perspective.

To aid computation of the etale fundamental group we will make use of the following lemma.

Lemma 2.34. *Let X be a connected and locally noetherian scheme, let x be a geometric point of X. Consider the projective system $\{X_i\}_i$ where we have morphisms $X_j \to X_i, i < j$ where X_i are the Galois covers of X [i.e. finite etale covers $X_i \to X$ such that $\# \mathrm{Aut}_X(X_i) = \deg(X_i/X)$]. Then we may compute the etale fundamental group as the projective limit*

$$\pi_1(X, x) = \varprojlim \mathrm{Aut}_X(X_i)$$

Proof. This is discussed in section 4, p. 99 of [Gro63, Éxpose V] and relies on proposition 3.1 on the prorepresentability of functors proved in [Gro95]. Said proposition requires the functor F to preserve finite products, finite fiber products [both easy] and finally to satisfy condition A below. every pair $(F(X), \zeta), \zeta \in F(X)$ is dominated by a minimal pair. A pair $(F(X), \zeta), \zeta \in F(X)$ is minimal if for all strict monomorphisms $u : X' \to X$ and $\zeta' \in F(X')$ such hat $\zeta = F(u)(\zeta')$ it follows that u is an isomorphism. Condition A then requires that every pair $(F(X), \zeta), \zeta \in F(X)$ is dominated by a minimal pair. Strict monomorphism for (affine) schemes are closed immersions, it follows from the definition of the fiber functor F_x that every pair is minimal hence we have prorepresentability. □

Definition 2.35. A projective system $\{X_i\}_i$ [such as the projective system of Galois covers] that is cofinal in the category of finite etale covers $Y \to X$ is also said to be a choice of *etale universal cover*, unique up to choice of basepoint.

In this section we will want to reconstruct the cusps and the closed points of a hyperbolic curve X. Let $\widetilde{X}$ be the étale universal cover of X, given by Galois covers $Y \to X$. Let x be a cusp of X in the compactification $\overline{X}$. Lift x to $\widetilde{x} \in \widetilde{X}$. Once again we have the fundamental exact sequence

$$1 \to \Delta_X \to \Pi_X \to \mathrm{G}_k \to 1$$

The fundamental group Π_X naturally acts on $\widetilde{X}$, through its action as the Galois groups of the Galois covers $Y \to X$.

Definition 2.36. The *decomposition group D_x* is defined to be the stabilizer of $\widetilde{x}$ in Π_X. The *inertia group* is defined as

$$I_x = D_x \cap \Delta_X$$

Remark 2.37. As suggested by the notation the definition is independent of the lift $\widetilde{x}$ of x up to conjugacy. Indeed, suppose we have another lift $\widetilde{x}'$. Then for every Galois cover $Y \to X$ we have lifts y, y' of x. The group $\mathrm{Aut}(Y/X)$ also works on $Y \to X$. The Galois group $\mathrm{Aut}(Y/X)$ works on the fiber Y_x of x transitively by Galois theory. Hence there is a $\gamma \in \mathrm{Aut}(Y/X)$ such that $\gamma(y) = y'$. Taking the projective limit over these γ I obtain $\widetilde{\gamma} \in \Pi_X$, noting that the limit over nonempty finie sets is nonempty. It follows that $\widetilde{\gamma} I_{\widetilde{x}/x} \widetilde{\gamma} = I_{\widetilde{\gamma}(\widetilde{x})/x} = I_{\widetilde{x}/x}$ as required.

Example 2.38. Suppose $x \in \overline{X}$ is a cusp in an hyperbolic curve X. I claim $I_x \cong \widehat{\mathbb{Z}}(1)$. The inertia group can be computed as follows. Let $Y_i \to X$ be a cofinal system of finite etale covers, such that $\Pi_X = \varprojlim_i \mathrm{Aut}(Y_i/X)$. Then the decomposition group is obtained as the projective limit over this system of the stabilizer $\mathrm{Stab}_{Y_i}(x_i)$ of $x_i \in \widetilde{x}$. Since we are computing the stabilizer it suffices to compute it on a cofinal system of finite etale cover $Y_i \to X$ as above. In fact this also gives a cofinal system of etale neighborhoods of x in $\overline{X}$; in other words we are computing the etale fundamental group of the etale stalk. We know that this equals $\pi_1(\mathrm{Spec}(\mathcal{O}^{et}_{X,x})) = \pi_1(\mathrm{Spec}(\mathcal{O}^{sh}_{X,x}))$, the strict henselization of the Zariski stalk.

It is known that if x is a nonsingular point of X, there is a map $\phi : U \to \mathbb{A}^d$ where $d = \dim(X) = 1, U$ an etale neighborhood of x such that ϕ is etale at x, see prop 4.9 in [Milb]. Moreover, given an etale morphism $\phi : Y \to X$, there is an isomorphism on etale stalks: $\mathcal{O}^{et}_{X,\phi(y)} \cong \mathcal{O}^{et}_{Y,y}$, see prop 4.8. [Milb], which equals the strict Henselization of the Zariski stalks. Furthermore, we can pass to the completion, by [Sta16, Tag 039M]. Compute $\pi_1(\mathcal{O}^{sh}_{X,x}) = \pi_1(\mathcal{O}^{sh}_{\mathbb{A}^1,x}) = \pi_1(\mathcal{O}^{\wedge}_{\mathbb{A}^1,x})$. To compute the inertia group we need only compute the geometric part, hence we may assume that $k = \overline{k}$. By the Cohen structure theorem [Sta16, Tag 0323] or direct computation

$$\pi_1(\mathcal{O}^{\wedge}_{\mathbb{A}^1,x}) = \mathrm{G}_{k((T))} = \widehat{\mathbb{Z}}(1)$$

where G_k acts through the G_κ which in turns acts through the cyclotomic character as $T^{1/n} \mapsto \zeta_n T^{1/n}$ where ζ_n is a primitive n-th root of unity. The wedge denotes the completion.

Definition 2.39. Let l a prime. A profinite group G is said to be a pro-l group if for any open normal subgroup $N \subset \mathrm{G}$ the quotient G/N is a l-group [i.e. each element has order a power of l]. Given a profinite group G we may consider its maximal pro-l quotient G^l defined as the maximal $\mathrm{G} \twoheadrightarrow \mathrm{G}^l$ quotient such that G^l is a pro-l group.

Example 2.40. The prototypical example of a profinite group is $\widehat{\mathbb{Z}}$. Its pro-l quotient is

$$\widehat{\mathbb{Z}} \twoheadrightarrow \mathbb{Z}_l$$

Given a group G and a subgroup $H \subset \mathrm{G}$ we might hope that H is a normal subgroup of G, but in general this is too much to hope for. In fact, inertia subgroups are *not* normal in the geometric fundamental group but they are ' close to being normal'.

Definition 2.41. Let the commensurator be defined as

$$C_{\mathrm{G}}(H) := \{g \in \mathrm{G} \,|[H : gHg^{-1} \bigcap H] < \infty\}$$

we say $H \subset G$ is *commensurably terminal* if $H = C_G(H)$.

To proceed we need one other ingredient, a classical technique for describing branched covers of Riemann surfaces. It is as follows. Let X be a projective curve, of genus g. Let $S \subset X$ be a finite collection of points of cardinality r. We want to produce finite etale covers of $U := X - S$ that are branched at S. Moreover, we want and will be able to control the ramification behaviour of these coverings. Recall Lemma 2.2 to the effect that the geometric fundamental group Δ_U is isomorphic to the profinite completion of

$$< a_i, b_i, c_j \mid \prod_{i=1}^{g} [a_i, b_i] \prod_{j=1}^{r} c_j = 1 >$$

The c_j should be thought of as 'loops around the cusps'. Let us be given a map

$$\phi\colon \Delta_U = \pi_1(U_{\overline{k}}) \to S_n$$

where S_n is the symmetric group on n generators. Let G denote the image of ϕ, with g_j the images of c_j. Then by passing to the kernel we obtain a cover $Y \to X$ which is finite etale on U and moreover has branch type g_j at the cusp corresponding to c_j.

Example 2.42 (See also [Vis])**.** Let $U \subset X$ a curve of genus $g > 1$ and cusps q_1, q_2, q_3. Let

$$\phi : \pi_1(U_{\overline{k}}) \to S_n$$

be the map given by sending $c_1 \mapsto (1 \cdot 2 \cdots n-1 \cdot n)$ [the n-cycle in the symmetric group] and $c_2 \mapsto (1 \cdot 2 \cdots n-1 \cdot n)^{-1}$ and $a_i, b_i,\ i = 1, \cdots, g$ to the identity. This forces the last ' cuspidal loop element' c_3 to be equal to

$$c_3 = (\prod_{i=1}^{g} [a_i, b_i] c_1 c_2)^{-1} = 1$$

In short we have found a cover that is totally ramified at q_1, q_2 and unramified everywhere else, including q_3. Moreover since $g > 1$ we know the resulting curve is hyperbolic.

Lemma 2.43. *Let $\overline{X}$ be a compactification of X. Consider the corresponding short exact sequence*

$$1 \to K \to \Delta_X \to \Delta_{\overline{X}} \to 1.$$

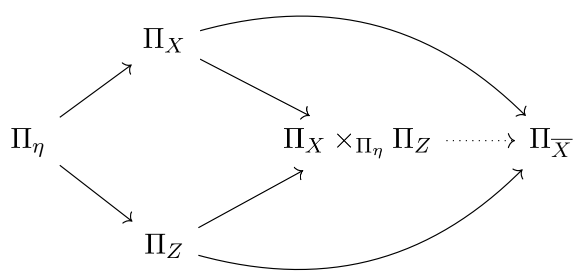
where K is defined to be the kernel. Then, the subgroup K is generated by conjugacy classes of the cuspidal inertia groups $I_x \subset \Delta_X$.

Proof. Since we are only interested in the geometric part of the etale fundamental groups we reduce to the case of algebraically closed fields: $X_{\overline{k}}/\overline{k}$. For ease of exposition, assume X has just one cusp, $\overline{X} = X \cup x$. Consider the covering

$$X \sqcup \operatorname{Spec}(\mathcal{O}^{sh}_{\overline{X},x}) \to \overline{X}$$

I claim it is a fpqc-covering. That it is quasi-compact is clear. $X \hookrightarrow \overline{X}$ is an open immersion hence flat, as is the inclusion of the spectrum of the stalk $\operatorname{Spec}(\mathcal{O}^{sh}_{\overline{X},x}) \to \overline{X}$, [Sta16, Tag 0250]. As the covering is flat and surjective it is faithfully flat hence fpqc.

Let $Z = \operatorname{Spec}(\mathcal{O}^{sh}_{\overline{X},x})$ and let $\eta \hookrightarrow \operatorname{Spec}(\mathcal{O}^{sh}_{\overline{X},x})$ be the spectrum of the generic point. We have the etale Seifert-Van Kampen theorem from flat descent, see Theoreme 5.1 [Gro63][Chap IX, Theorem 5.1] and also Corollaire 5.4. For a lucid exposition on descent see Chapter 6, section 1 of [BLR90]. We have a pushout diagram



where the dashed arrow is an isomorphism. So the conjugacy class of the image of Δ_η is exactly the kernel of $\Delta_X \times \Delta_Z \to \Delta_{\overline{X}}$. We saw earlier that $\Delta_\eta \cong I_x$. Finally, remark that $\Pi_Z \cong \Pi_{k(x)} = \mathrm{G}_{\overline{k}} = \{0\}$. Actually, this is really the same as the above quoted Corollaire 5.4 in [Gro63][Chap IX]. ☐

Lemma 2.44. *The cuspidal inertia group $I_x \subset \Delta_X$, as well as its pro-l counterpart $I_x^{(l)} \subset \Delta_X^{(l)}$ is commensurably terminal.*

Proof. We prove the case for $I_x \subset \Delta_X$; the pro-l case is similar. Let us suppose the proposition is false. Let $\sigma \in C_{\Delta_X}(I_{\widetilde{x}/x})$ such that

$$[I_{\widetilde{x}/x} : I_{\widetilde{x}/x} \cap \sigma I_{\widetilde{x}/x} \sigma^{-1}] = n < \infty$$

but $\sigma \notin I_{\widetilde{x}/x}$. This implies that we have a finite etale covering

$$Y \to X_{\overline{k}}$$

unramified over x with a cusp y of Y mapping to x such that $\sigma(y) \neq y$. By taking a smaller open subgroup we may suppose there is another cusp y' such that $y, \sigma(y), y'$ are all distinct.

Next, take an open subgroup $\Delta_Z \subset \Delta_Y$ such that $\Delta_Z \cap I_{\widetilde{y}/y} = \Delta_Z \cap \sigma I_{\widetilde{y}/y} \sigma^{-1}$. We obtain finite etale coverings

$$Z \to Y \to X_{\overline{k}}$$

together with cusps $z, \sigma(z), z'$ lying over $y, \sigma(y), y'$. By passing to the normalization we may assume the cover is Galois. We have $\sigma I_{\widetilde{z}/z} \sigma^{-1} = I_{\sigma(z)}$

In Δ_Z we have the inertia groups $I_{\widetilde{z}/} := I_{\widetilde{x}/x} \cap \Delta_Z$ and the cusp z associated with $I_{\widetilde{z}/z}$ maps to x. Next, $I_{\sigma(\widetilde{z}/z)} = \sigma I_{\widetilde{z}/z} \sigma^{-1} = I_z$ in Δ_Z. The associated cusps, $z, \sigma(z)$ have conjugate inertia subgroups, but are not equal.

The following step is to construct an abelian or pro-l cover that is totally ramified at z', z but *not* at $\sigma(z)$. This was done in Example 2.42. This contradicts the fact that $z, \sigma(z)$ have conjugate inertia groups. This is because of the following fact: open subgroups of Δ_Z that intersect with proper subgroups of I_z corresponds etale cover of Z ramified at z; but if two inertia groups are conjugate these proper subgroups have to correspond as well. $\square$

Theorem 2.45 (Nakamura). *Let X, Π_X be as above over field k assumed to be a finite extension of $\mathbb{Q}_p$ or a number field. Then for every cusp x of X the cuspidal decomposition group I_x may be reconstructed from Π_X.*

Proof. In the case that k is a number field we may reduce to the p-adic case as follows. From the reconstruction of the geometric fundamental group we have the fundamental exact sequence

$$1 \to \Delta_X \to \Pi_X \to \mathrm{G}_k \to 1$$

hence we may reconstruct G_k. Using the fact that the decomposition groups can be group-theoretically characterized, see section 1 of [NSW08, Chapter 12], pick a decomposition group D_p of a nonarchimedean prime; we have $D_p \cong \mathrm{G}_{k_p}$. Finally, pullback the above sequence along the induced map $\mathrm{G}_{k_p} \hookrightarrow \mathrm{G}_k$ to obtain

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta_X & \longrightarrow & \Pi_{X_{k_p}} & \longrightarrow & \mathrm{G}_{k_p} & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \Delta_X & \longrightarrow & \Pi_X & \longrightarrow & \mathrm{G}_k & \longrightarrow & 1 \end{array}$$

We follow a proof due to Mochizuki, see Lemma 1.3.9 of [Moc04]. The curve X is a hyperbolic curve; i.e. a projective curve of genus g punctured at r points. We may recover whether $r = 0$ or not by looking at the geometric fundamental group - which we may recover as we have seen earlier- and seeing whether it is a free group or not.

The natural representation $G_k \curvearrowright \Delta_X$ obtained from the homotopy sequence is rather complicated so let us restrict to understanding how the Frobenius element works, i.e. the lift $\widetilde{\mathrm{Fr}} \in G_k$ of $g = \mathrm{Fr} \in G_\kappa$.

We may moreover take the abelianization of $\Delta_X, \Delta_{\overline{X}}$; after that tensor with $\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Q}_l$ to get $\Delta_X^{ab} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l, \Delta_{\overline{X}}^{ab} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l$. This Galois representation is much better understood. In fact, it is equal to the l-adic Tate module of the Jacobian of X [as we used earlier in our discussion of the recovery of the geometric fundamental group].

We have strong control over how the Frobenius element acts. We know that these weights are restricted to lie in $\{0, \frac{1}{2}, 1\}$. This follows from an argument that is similar to what we saw earlier. In the Galois representation $T_l(J(X))$ we can reduce to the case where $J(X)$ has good reduction. To wit, by rigid uniformization of abelian varieties [Theorem 2.23] we may write the Jacobian $J = J(X)$ as $J = \widetilde{J}/L$ such that $\widetilde{J}$ is a semi-abelian variety fitting into a short exact sequence

$$0 \to S \to \widetilde{J} \to A \to 0 \tag{2.2}$$

where A has good reduction, and S is a torus. The Tate module $T_l(J)$ fits into

$$0 \to T_l(\widetilde{J}) \to T_l(J) \to L\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Z}_l \to 0$$

where $L\widehat{\otimes}_{\widehat{\mathbb{Z}}}\mathbb{Z}_l$ is pure of weight zero and the above equation 2.2 implies that $T_l(\widetilde{J})$ is the sum of modules of weight 1 [the Tate module of the torus $T_l(S)$]and $1/2$ [the Tate module of an abelian variety of good reduction, by the Neron-Ogg-Shavarevich criterion and the Riemann hypothesis for abelian varieties over finite fields, Theorem 2.28].

It follows from the Grothendieck monodromy theorem, Theorem 17 of [vB], that this type of Galois representation is *quasi-unipotent* which means that after possibly restricting to an open subgroup of G_k the action of the inertia group of G_k is unipotent. This implies in turn that the eigenvalues of the Frobenius $\widetilde{\mathrm{Fr}}$ is independent of the lift. Indeed let $\widetilde{\mathrm{Fr}}'$ be another lift and consider their difference which is unipotent hence has eigenvalue 1, since $\widetilde{\mathrm{Fr}}, \widetilde{\mathrm{Fr}}'$ commute their eigenvalues must be equal.

Remark that the Frobenius may be group-theoretically reconstructed hence we may talk of weights.

Set $I = \mathrm{Ker}(\Delta_X^{ab} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l \to \Delta_{\overline{X}}^{ab} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l)$. Compute

$$\begin{aligned} r - 1 &= \dim_{\mathbb{Q}_l}(I) \\ &= \dim_{\mathbb{Q}_l}(I^{wt1}) \\ &= \dim_{\mathbb{Q}_l}(\Delta_X^{ab,1}) - \dim_{\mathbb{Q}_l}(\Delta_{\overline{X}}^{ab,1}) \\ &= \dim_{\mathbb{Q}_l}(\Delta_X^{ab,1}) - \dim_{\mathbb{Q}_l}(\Delta_{\overline{X}}^{ab,0}) \\ &= \dim_{\mathbb{Q}_l}(\Delta_X^{ab,1}) - \dim_{\mathbb{Q}_l}(\Delta_X^{ab,0}) \end{aligned}$$

The left hand side of the equation is a priori not 'group-theoretic' but the right hand side is. The first equality follows from the explicit forms of the abelianized geometric fundamental groups. The second and fifth equalities follow from that fact that the Frobenius acts on I with eigenvalue q, i.e. weight 1. The third equality follows by definition. For the fourth equality we need

Theorem 2.46 (Tate duality). *Let k be a local field, M a finitely generated l-adic representation of G_k. The cup product furnishes a perfect pairing*

$$\mathrm{H}^r(G_k, M) \times \mathrm{H}^{2-r}(G_k, M^*(1))^* \to \mathrm{H}^2(G_k, \mathbb{Q}_l(1)) \cong \mathbb{Q}_l$$

where the star denotes the dual, $M^* := \mathrm{Hom}(M, \mathbb{Q}_l)$*.*

Proof. See theorem 1.4.1 of [Rub00] or corollary I2.3 of [Mil06]. □

Remark that $(\Delta^{ab,1}_{\overline{X}})^* = \mathrm{Hom}(\Delta^{ab,1}_{\overline{X}}, \mathbb{Q}_l(1)) = \Delta^{ab,0}_{\overline{X}}$ so the fourth equality follows from Tate duality for $r = 1, M = \Delta^{ab,1}_{\overline{X}}$.

So the above computation is also group-theoretic. Since

$$\dim_{\mathbb{Q}_l}(\Delta^{ab}_X) = 2g - 1 + r$$

we can reconstruct both the genus g and the number of punctures r group-theoretically.

The surjection $p : \Delta_X \twoheadrightarrow \Delta_{\overline{X}}$ is group-theoretically characterized as follows: open subgroups $H \subset \Delta_X$ are in the kernel of p if and only if $r(X_H) = [\Delta - X : H]r(X)$ where X_H is the corresponding etale cover. All this can be similarly done for the pro-l group quotient $\Delta^{(l)}$ for any $l \neq p$.

Next, characterize the inertia subgroups of $\Delta^{(l)}$ as follows: a closed subgroup $A \subset \Delta^{(l)}$ isomorphic to $\mathbb{Z}_l$ is contained in an inertia subgroup if for any open subgroup $\Delta^{(l)}_Y$ the composite

$$A \cap \Delta^{(l)}_Y \subset \Delta^{(l)}_Y \twoheadrightarrow \Delta^{(l)}_{\overline{Y}} \twoheadrightarrow (\Delta^{(l)}_{\overline{Y}})^{ab}$$

is zero. Let me prove that this works. The 'only if' claim is immediate since inertia subgroups are killed in $\Delta_{\overline{Y}}$. For the 'if' claim we argue as follows. Given any finite etale cover $Y \to X$ we want to split of the part that is totally ramified of degree l at a cusp. Set $\Delta^{(l)}_Z := A\Delta^{(l)}_Y \subset \Delta^{(l)}_Y$. The surjection

$$\Delta^{(l)}_Z \twoheadrightarrow \Delta^{(l)}_Z / \Delta^{(l)}_Y \cong A / A \cap \Delta^{(l)}_Y$$

factors through

$$\Delta^{(l)}_Z \twoheadrightarrow (\Delta^{(l)}_Z / \Delta^{(l)}_Y)^{ab} \cong A / A \cap \Delta^{(l)}_Y$$

since $A / A \cap \Delta^{(l)}_Y$ is isomorphic to $\mathbb{Z}/l^n\mathbb{Z}$ for some $n \in \mathbb{N}$. Since $A \cap \Delta^{(l)}_Z \twoheadrightarrow \Delta^{(l)}_Z / \Delta^{(l)}_Y \cong A/A \cap \Delta^{(l)}_Y \to (\Delta^{(l)}_{\overline{Y}})^{ab}$ vanishes the $\mathrm{Im}(A \cap \Delta^{(l)}_Y \to (\Delta^{(l)}_Y)^{ab})$ is contained in the subgroup generated by the inertia subgroups in $\Delta^{(l)}_Y$. Consequently, the image $\mathrm{Im}(A \cap \Delta^{(l)}_Y \to (\Delta^{(l)}_Y)^{ab} \to (\Delta^{(l)}_Z)^{ab} \twoheadrightarrow A/(A \cap \Delta^{(l)}_Y) \cong \mathbb{Z}/l^n\mathbb{Z})$ is contained in the image in $A/(A \cap \Delta^{(l)}_Y)$ generated by the inertia subgroups in $\Delta^{(l)}_Y$.

The composite $A \subset \Delta^{(l)}_Z \twoheadrightarrow \Delta^{(l)}_Z / \Delta^{(l)}_Y \cong A/(A \cap \Delta^{(l)}_Y) \cong \mathbb{Z}/l^n\mathbb{Z}$ is surjective and maps to a cyclic group; this implies that there exists an inertia subgroups I_z such that $I_z \hookrightarrow \Delta^{(l)}_Z \to (\Delta^{(l)}_Z)^{ab} \twoheadrightarrow A/(A \cap \Delta^{(l)}_Y)$ is surjective. This finally implies that the corresponding subcovering $Y \to Z$ is totally ramified at z and we are done.

Using the above construction we may recover the set of cusps of X as the set of $\Delta^{(l)}_X$-orbits of the inertia subgroups in $\Delta^{(l)}_X$, this gives the right answer because of commensurable terminality of inertia subgroups. We may apply this procedure to any cover $Y \to X$ and thereby construct the cusps of the universal pro-cover $\widetilde{X} \to X$. The inertia subgroups $I_x \subset \Delta_X$ are the reconstructed as those subgroups that fix some cusp $\widetilde{x}$ of $\widetilde{X}$.

□

We can also recover the decomposition groups.

Lemma 2.47. *Let x be a cusp of X. Then $D_x \subset \Pi_X$, the decomposition group of x, is the normalizer*

$$D_x = N_{\Pi_X}(I_x)$$

in Π_X.

Proof. Since Δ_X is normal in Π_X, we have that I_x is normal in D_x. This is a basic fact from group theory and can be seen from the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Delta_X & \longrightarrow & \Pi_X & \longrightarrow & \mathrm{G}_k & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & I_x & \longrightarrow & D_x & \longrightarrow & \mathrm{G}_{k(x)} & \longrightarrow & 0 \end{array}$$

where $\mathrm{G}_{k(x)} \coloneqq \mathrm{Im}(D_x \to \mathrm{G}_k)$ so automatically the kernel equals $I_x = D_x \cap \Delta_X$.

Consequently, $D_x \subset N(I_x)$. It suffices to show that for the projection map

$$p : \Pi_X \to \mathrm{G}_k$$

the images of D_x and $N(I_x)$ coincide. Suppose by contradiction that $g \in p(N(I_x)), g \notin p(D_x)$. Then g is nontrivial on the residue field $k(x)$, which implies that $gx \neq x$.

Next, let x be a closed point of $\overline{X}_{\overline{k}} \setminus X_{\overline{k}}$, define S_x as the set of lifts over x. Let

$$T_x = \bigcup_{y \in S_x} I_y.$$

For $x' \neq x$ we have $T_x \cap T_{x'} = \{0\}$. We have

$$T_x \cap gT_xg^{-1} = T_x \cap T_{gx} = \{0\}$$

which contradicts the fact that, after possibly restricting to an open subgroup, there exists a lift $\widetilde{g}$ of g such that $\widetilde{g}I_y\widetilde{g}^{-1} = I_y$ [this is Commensurably Terminality of cuspidal inertia groups, Theorem 2.44.] □

2.3 Synchronization of Geometric Cyclotomes

Let X be a proper curve over a field k of characteristic zero. If $U \subset X$ is a nonempty open subscheme, then we have the natural exact sequence of profinite groups

$$1 \to \Delta_U \to \Pi_U \to \mathrm{G}_k \to 1$$

Remark that all the cuspidal inertial groups I_x are naturally isomorphic to $\widehat{\mathbb{Z}}(1)$. But this identification is 'scheme theoretic'. What we want is a canonical identification of a 'local' cyclotome I_x with a some global cyclotome which we will denote by M_X.

Proposition 2.48. *There is a group-theoretic algorithm that outputs a natural isomorphism*

$$I_x \to M_X$$

from the datum Π.

Remark 2.49. The cuspidal inertia group I_x is not normal in Δ_{U_x} as we would like. This can be remedied, for let $\Delta_{U_x}^{c-cn}$ denote the *maximal cuspidally central quotient* of $\Delta_{U_x} \twoheadrightarrow Q$ which is defined to be the maximal *intermediate* quotient Q such that $\ker(Q \to \Delta_X)$ lies in the center of Q. So we have a sequence of surjections

$$\Delta_{U_x} \to \Delta_{U_x}^{c-cn} \to \Delta_X$$

Proof. We have a short exact sequence

$$1 \to I_x \to \Delta_{U_x}^{c-cn} \to \Delta_X \to 1$$

Indeed this follows from the fact for any intermediate quotient $\Delta_{U_x} \twoheadrightarrow Q \twoheadrightarrow \Delta_X$ such that $\mathrm{Ker}(Q \twoheadrightarrow \Delta_X)$ lies in the center of Q, the kernel $\mathrm{Ker}(Q \to \Delta_{U_x})$ is generated by I_x [we got rid of the conjugation ambiguity].

From the short exact sequence, we have a natural action of Δ_X by conjugation on I_x. Recall the inflation restriction sequence

$$0 \to \mathrm{H}^1(G/N, A^N) \to \mathrm{H}^1(G, A) \to \mathrm{H}^1(N, A)^{G/N} \to \mathrm{H}^2(G/N, A^N) \to \mathrm{H}^2(G, A) \to \cdots$$

and take $N = I_x, A = I_x, G = \Delta_{U_x}^{c-cn}$ so $G/N = \Delta_X$. We obtain a map

$$\mathrm{H}^1(I_x, I_x)^{\Delta_X} \to \mathrm{H}^2(\Delta_X, I_x^{I_x})$$

On the one hand,

$$\begin{aligned} \mathrm{H}^1(I_x, I_x)^{\Delta_X} &\cong \mathrm{H}^1(I_x, I_x) \\ &= \mathrm{Hom}(I_x, I_x) \end{aligned}$$

on the other hand,

$$\begin{aligned} \mathrm{H}^2(\Delta_X, I_x^{I_x}) &= \mathrm{H}^2(\Delta_X, I_x) \\ &\cong \mathrm{H}^2(\Delta_X, \hat{\mathbb{Z}}) \otimes_{\hat{\mathbb{Z}}} I_x \\ &\cong \mathrm{Hom}(\mathrm{Hom}(\mathrm{H}^2(\Delta_X, \hat{\mathbb{Z}}), \hat{\mathbb{Z}}), I_x) \end{aligned}$$

where we used that $I_x^{I_x}$ is canonically isomorphic to I_x since $I_x \cong \widehat{\mathbb{Z}}(1)$. So $1 \in \hat{\mathbb{Z}} \cong \mathrm{Hom}(I_x, I_x)$ yields an element of $\mathrm{Hom}(M_X, I_x)$ where we write

$$M_X = \mathrm{Hom}(\mathrm{H}^2(\Delta_X, \hat{\mathbb{Z}}), \hat{\mathbb{Z}})$$

Which yields a 'group theoretic' isomorphism $M_X \cong I_x$. □

2.4 Cuspidalization

Let X be a curve and $U \subset X$ a nonempty open subscheme. Let Π_X, Π_U denote their etale fundamental groups. Counter to naive intuition, Π_U is in some sense bigger than Π_X, that is $U \to X$ induces a surjection

$$\Pi_U \twoheadrightarrow \Pi_X$$

We reconstruct surjections $\Pi_U \twoheadrightarrow \Pi_X$ for every open subscheme U. In effect one reconstructs the topology on X group-theoretically. Since all subschemes U are isomorphic to X minus a finite number of cusps, one might also phrase this as characterizing the cusps, hence the name cuspidalization.

Remark 2.50. As one might guess cuspidalization is not easy. It's not clear at all how given a profinite group Π that is 'secretely isomorphic to Π_X' we can find a group extension $\Pi' \to \Pi$ such that $\Pi' \cong \Pi_U$. But for a certain class of curves, the so called elliptically admissable hyperbolic curves and the hyperbolic curves of strictly Belyi type, it is possible. This will utilize the structure of isogenies of elliptic curves and Belyi theorem, respectively. In this thesis we will only consider curves of strictly Belyi type.

Remark 2.51. Two curves can be related by one being an open subset of the other. Another natural way for two curves to be related is by one to be a cover of the other. A sequences of curves related by these operations have corresponding operations on the level of étale fundamental groups; both sequences of operations will be called *Type Chains*. The final group-theoretic functorial algorithm will characterize the surjection $\Pi_U \to \Pi_X$ as the final map of type chain which starts and end at Π_X. Let us formalize this idea.

Definition 2.52. Let X be a hyperbolic curve over a field k and let $\widetilde{X}$ be its pro-étale cover.

A X-*chain* is a sequence of hyperbolic curves $X = X_0 \leftrightsquigarrow X_j \leftrightsquigarrow X_n$ over $\operatorname{Spec} k_j$ where $k \subset k_j$ is a finite extension of k. Moreover each X_j is equipped with 'rigidifying' morphism $\rho_j : \widetilde{X} \to X_j$ compatible with the structure maps. Each $X_j \leftrightsquigarrow X_{j+1}$ corresponds to one of the following 'operations'

- $\curlywedge$ A finite étale covering $X_{j+1} \to X_j$ (open immersion $\Pi_{j+1} \hookrightarrow \Pi_j$)
- $\curlyvee$ A finite étale quotient $X_j \to X_{j+1}$ (open immersion $\Pi_{j+1} \hookleftarrow \Pi_j$)
- $\bullet$ (de-Cuspidalization): An open immersion $X_j \hookrightarrow X_{j+1}$ of hyperbolic curves, the complement of whose image is a finite collection of k_{j+1}-points of X_{j+1}. (surjection $\Pi_{j+1} \twoheadleftarrow \Pi_j$).

Definition 2.53. Type chains form a category. Let $\mathrm{Chain}(Y/X)$ have as objects chains $X = X_0 \rightsquigarrow X_j \rightsquigarrow X_n$. A morphism between $X_0 \rightsquigarrow X_j \rightsquigarrow X_n$ and $X = X_0 \rightsquigarrow X_j \rightsquigarrow X_k$ is simply a morphism $X_n \to X_k$.

Completely analogously we define Π-chains and their corresponding categories.

Definition 2.54. An Π-chain is a sequence of profinite groups $\Pi = \Pi_0 \rightsquigarrow \Pi_j \rightsquigarrow \Pi_n$ with each Π_j equipped with a morphism $\widetilde{\Pi} \to \Pi_j$ such that each satisfying the following properties:

- $\curlywedge$ Open immersion $\Pi_{j+1} \hookrightarrow \Pi_j$ (Finite étale covering $X_{j+1} \to X_j$)
- $\curlyvee$ Open immersion $\Pi_{j+1} \hookleftarrow \Pi_j$ (Finite étale quotient $X_j \to X_{j+1}$)
- $\bullet$ (de-Cuspidalization): Surjection $\Pi_{j+1} \twoheadleftarrow \Pi_j$. (An open immersion $X_j \hookrightarrow X_{j+1}$ of hyperbolic curves, the complement of whose image is a finite collection of k_{j+1}-points of X_{j+1}.)

Definition 2.55. Type chains form a category. Let $\mathrm{Chain}(\widetilde{X}/X)$ have as objects chains $X = X_0 \rightsquigarrow$

$X_j \rightsquigarrow X_n$. A morphism between $X_0 \rightsquigarrow X_j \rightsquigarrow X_n$ and $X = X_0 \rightsquigarrow X_j \rightsquigarrow X_k$ is simply a morphism $X_n \to X_k$.

Definition 2.56. A profinite group Π is *slim* if every open subgroup is centerfree.

Lemma 2.57. *The étale fundamental groups of hyperbolic curves are slim.*

Proof. See proposition 2.3 in [Moc12] □

Remark 2.58. Why is it interesting to be centerfree? Given a profinite group Π we have an exact sequence

$$\Pi \to \mathrm{Aut}(\Pi) \to \mathrm{Out}(\Pi) \to 1$$

If Π is centerfree than $\Pi \hookrightarrow \mathrm{Aut}(\Pi)$ is injective, hence we have a complete short exact sequence:

$$1 \to \Pi \to \mathrm{Aut}(\Pi) \to \mathrm{Out}(\Pi) \to 1$$

If we have a map $H \to \mathrm{Out}(\Pi)$ then we can pull back the above short exact sequence to obtain

$$1 \to \Pi \to \Pi \times_{\mathrm{Out}(\Pi)} H \to H \to 1$$

For instance if we have an action of a finite group H on X we have a map H to Out(Π). The fibre product is naturally isomorphic to $\pi_1(X//H)$ "the stack theoretic quotient" of X by H. As mentioned before, this thesis does not cover the theory of stacks, but just to give a bit of intuition: if one has a finite Galois cover $Y \to X$, and we take the stack-theoretic quotient of Y by the natural action of $\mathrm{Gal}(Y/X)$ we get, unsurprisingly, the scheme X.

We have an etale covering $X \to X//H$, even a Galois cover with Galois group H. In fact we have the short exact sequence

$$1 \to \pi_1(X) \to \pi_1(X//H) \to H \to 1$$

So we have an action of a finite group H on X over a field k, for instance we have an etale quotient $X \to Y$. This corresponds to a map $H \to \mathrm{Out}(\Pi)$ over Π/Δ which means that given a commutative diagram

$$\Pi \to \Pi$$

$$\Pi/\Delta \to \Pi/\Delta$$

then the maps on Π/Δ must be inner. So we cannot have exotic automorphism.

Suppose we have an open immersion $X \hookrightarrow Y$. Can we give a group-theoretic description of $\Pi_X \to \Pi_Y$ given Π_X? Yes, the kernel is exactly the group generated by conjugacy classes of cuspidal decomposition groups, and we can recover the cuspidal decomposition groups.

2.4.1 Belyi Cuspidalization

Definition 2.59. Let L/k be an extension of fields. Given a scheme X/L we say that X is defined over k if there exists a scheme Y/k such that $Y_L \cong X$.

Definition 2.60. We say an hyperbolic curve X is of stricly Belyi type when X is defined over a number field and is isogenous to a hyperbolic curve of genus 0.

We assume now X is a hyperbolic curve of strictly Belyi type over a sub-p-adic field k. We have the following diagram

$$\begin{array}{ccccc} & & V & & \\ & \swarrow & & \searrow & \\ X & & & & Q \hookrightarrow \mathbb{P}^1 \setminus \{0,1,\infty\} \end{array}$$

where Q is a hyperbolic curve of genus zero and V is a hyperbolic curve defined over a number field; the cusps of V defined over a finite extension L/k. By considering the normal closure we may assume that $V \to X$ is Galois. Assume now that we have an open subscheme $U_X \hookrightarrow X$ defined over a number field. Set $U := U_X \times_X V$. Now U is also defined over a number field. By Belyi's theorem we obtain an open subset $W \subset U$ and a map $W \to \mathbb{P}^1 \setminus \{0,1,\infty\}$. Remark that we need to restrict to an open $W \subset U$ because although U is defined over a number field the corresponding map to $\mathbb{P}^1 \setminus \{0,1,\infty\}$ might not be finite etale. We therefor have the following diagram

$$\begin{array}{ccccccc} W & & & & & \searrow & \\ \downarrow & & & & & & \\ U & \hookrightarrow & V & \longrightarrow & Q & \hookrightarrow & \mathbb{P}^1 \setminus \{0,1,\infty\} \\ \downarrow & & \downarrow & & & & \\ U_X & \hookrightarrow & X & & & & \end{array}$$

We have the type chain

$$X \overset{\curlywedge}{\rightsquigarrow} V \overset{\curlyvee}{\rightsquigarrow} Q \overset{\bullet}{\rightsquigarrow} \mathbb{P}^1 \setminus \{0,1,\infty\} \overset{\curlywedge}{\rightsquigarrow} W \overset{\bullet}{\rightsquigarrow} U \overset{\bullet}{\rightsquigarrow} V \overset{\curlyvee}{\rightsquigarrow} X$$

Definition 2.61. Let X be a hyperbolic curve of strictly Belyi type, Π_X its étale fundamental group.

Theorem 2.62 (Belyi Cuspidalization)**.** *Let X be an hyperbolic curve of strictly Belyi type over a sub-p-adic field k, and fix the data as above. Let $\mathcal{O}^{NF}(\Pi_X)$ denote the set of surjections $\Pi_{U_X} \twoheadrightarrow \Pi_X$ where U_X is an open subscheme defined over a number field. Then there are functorial algorithms*

(i) To reconstruct the set of surjections $\mathcal{O}^{NF}(\Pi_X)$

$$\Pi_X \longmapsto \mathcal{O}^{NF}(\Pi_X).$$

(ii) To reconstruct the cuspidal inertia and decompositions groups $I_z \subset \Delta_{U_X}$.

Proof. (i) **Step 1:** From Π_X we may reconstruct the fundamental exact sequence

$$1 \to \Delta_X \to \Pi_X \to \mathrm{G}_k \to 1$$

This implies that any point we may restrict to an open subgroup $\mathrm{G}_L \subset \mathrm{G}_k$ and corresponding open subgroup $\Pi_{X_L} \subset \Pi_X$ so that in the following the cusps and points are always defined over the base field. **Step 2:** The category $\mathrm{Chain}(\Pi)$ may be reconstructed in a purely group-theoretic matter. This follows from the group-theoretic characterizations we have given of finite etale covers, finite etale quotients and decuspidalization together with the Relative-Anabelian Hom-conjecture[which ensures the morphisms match up].

For every nonempty open subscheme $U_X \subset X$ defined over a number field, the natural surjection $\Pi_U \twoheadrightarrow \Pi$ may be constructed via 'group-theoretic' operations as follows: For some normal open subgroup $\Pi_V \subset \Pi$, corresponding to a finite covering $V \to X$ of hyperbolic curves, there exists a [not necessarily unique] Π-chain

$$\curlywedge, \curlyvee, \bullet, \curlywedge, \bullet, \bullet, \curlyvee$$

that admits a terminal isomorphism with the trivial Π-chain of length 0, such that moreover in the second step we obtain a curve of genus zero, and in the third step a hyperbolic curve with exactly three cusps. These last conditions can be read off from the geometric fundamental group using the characterization of g, r. Call the map obtained in the second to last step $p : \Pi_U^\dagger \twoheadrightarrow \Pi_V^\dagger$. As stated, this Π-chain is not unique; be warned that the map above corresponds to $i_* : \Pi_U \to \Pi_V$ by the relative GC-conjecture for hyperbolic curve, but that there is an ambiguity in reconstruction $i : U \to V$ since we do not have access to the absolute conjecture.

Step 3 Next choose the Π-chain

$$\curlywedge, \curlyvee, \bullet, \curlywedge, \bullet, \bullet, \curlyvee$$

such that the natural morphism $\Pi_X/\Pi_V^\dagger \to \mathrm{Out}(\Pi_V^\dagger)$ has a *unique* lift $\Pi_X/\Pi_V^\dagger \to \mathrm{Out}(\Pi_U^\dagger)$ [This corresponds to $U \subset V$ invariant under $\mathrm{Gal}(V/X)$]. We obtain the surjection $\Pi_{U_X}^\dagger \to \Pi_X$ using the group-theoretic charaterization of finite étale quotients with respect to the unique lifting $\Pi_X/\Pi_V^\dagger \to \mathrm{Out}(\Pi_U^\dagger)$.

(ii) The cuspidal decomposition groups of the cusps of $U_X \subset X$ are obtained as the images of $\Pi_{U_X} \twoheadrightarrow \Pi$ of the cuspidal decomposition groups of Π_{U_X}. □

2.5 Kummer theory

In this section, let X be a **proper** hyperbolic curve, $U \subset X$ a nonempty open subscheme. Our next step in the reconstruction of the base field will be to encode rational functions in certain cohomology groups of Π_U. This will be done via the Kummer map to which we now turn. Consider the Kummer sequence

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{(\cdot)^n} \mathbb{G}_m \to 1$$

where $(\cdot)^n : \mathbb{G}_m \to \mathbb{G}_m$ is exponentiation to the n-th power. Apply to the scheme U and look at the long exact sequence

$$1 \to \Gamma(U, \mu_n(\mathcal{O}_U^\times)) \to \Gamma(U, \mathcal{O}_U^\times) \to \Gamma(U, \mathcal{O}_U^\times) \to \mathrm{H}^1(U, \mu_n(\mathcal{O}_U^\times)) \to \cdots$$

Take the limit over all $n \in \mathbb{N}$. We obtain a map

$$\kappa_U : \Gamma(U, \mathcal{O}_U^\times) \to \mathrm{H}^1(U, \varprojlim_n \mu_n(\mathcal{O}_U^\times))$$

the epynomous Kummer map. We will need a more hands-on approach to the Kummer map. .

Suppose k contains n distinct n-th roots of unity. There is an isomorphism

$$k^\times/(k^\times)^n \cong \mathrm{Hom}(\mathrm{Gal}(L/k), \mu_n)$$

given by

$$a \mapsto \left(\sigma \mapsto \frac{\sigma(a^{1/n})}{a^{1/n}}\right)$$

where α is any n-th root of a in L.

Definition 2.63. Let k be a field of characteristic zero, $\overline{k}$ an algebraic closure of k. Then k is said to be *Kummer-faithful* if, for every finite extension $k \subset k^H \subset \overline{k}$, where $H \subset \mathrm{G}_k$ a normal subgroup, and every semi-abelian variety J/k^H we have

$$\cap_{N\geq 1} N \cdot J(k^H) = \{0\}, \qquad \forall N \in \mathbb{N}$$

where $N \cdot (-)$ denotes multiplication by $N \in \mathbb{N}$.

Lemma 2.64. *A finite extension $k/\mathbb{Q}_p$ is Kummer-faithful, and so is a number field.*

Proof. Given a number field k consider the inclusion $k \hookrightarrow k_p$ into the completion of k at a nonarchimedean place p. The statement follows immediately from the corresponding statement for k_p. Assume from now on that k is a p-adic field. Because k is a p-adic field so is k^H. For a semi-abelian variety J we have a short exact sequence

$$0 \to T \to J \to A \to 0$$

where T is a torus, A is an abelian variety. Evaluating at k^H, i.e. applying the Galois cohomology of H on the Galois modules $T(\overline{k}), J(\overline{k}), A(\overline{k})$ furnishes

$$0 \to \mathrm{H}^0(H, T(\overline{k})) \to \mathrm{H}^0(H, J(\overline{k})) \to \mathrm{H}^0(H, A(\overline{k})) \to \mathrm{H}^1(H, T(\overline{k})) \to \cdots$$

Next, use $T(\overline{k}) \cong \oplus\mathbb{G}_m(\overline{k})$, so $\mathrm{H}^0(H, T(\overline{k})) = \oplus(\overline{k}^\times)^H = \oplus(k^H)^\times$ and Hilbert 90 to the effect that $\mathrm{H}^1(H, (\overline{k}^\times)) = \{0\}$, we obtain

$$0 \to \oplus(k^H)^\times \to J(k^H) \to A(k^H) \to 0$$

So to check the condition for Kummer-faithfullness reduces to show that the torsion group of $A(k^H)$ is finite. This follows from the lemma below. $\square$

Lemma 2.65. *The torsion subgroup of $A(k^H)$ is finite.*

Proof. The semi-abelian variety A is a proper group scheme over a p-adic field k^H. There is a notion of p-adic analytification which furnishes the structure of a p-adic Lie group on $A^{an}(k^H)$. Similar to the situation for real and complex Lie groups, p-adic Lie groups have tangent spaces which are free $\mathbb{Z}_p$-modules of free rank and so have finite torsions subgroups. The p-adic Lie group $A^{an}(k^H)$ also has an exponential map, see Chapter V section 7 of [Ser06].

The exponential map for the p-adic Lie group determines an isomorphism of an open neighborhood of the identity of $A_X^{an}(k^H)$ with a free $\mathbb{Z}_p$ module of finite rank. Since A is proper, $A(k^H)$ is compact hence may be covered with a finite set of suitably small neighborhoods; the finiteness of $A(k^H)$ follows from this fact and the fact that these opens can be taken to be suitable translates of opens around 0. $\square$

Lemma 2.66. *Let X be a curve not isomorphic to $\mathbb{P}^1$. Let $\overline{x} \in X$ be a geometric point. For a locally constant sheaf L we have a* canonical *isomorphism*

$$\mathrm{H}^i(X, L) \cong \mathrm{H}^i(\pi_1(X, \overline{x}), L_{\overline{x}})$$

Proof. See [Ach]. $\square$

In particular since $\mu_{n,\overline{x}} \cong \mathbb{Z}/n\mathbb{Z}$ [μ_n is locally constant in the etale topology] we know

$$\mathrm{H}^1(U, \varprojlim_n \mu_n) \cong \mathrm{H}^1(\Pi_U, \widehat{\mathbb{Z}}(1)) \cong \mathrm{H}^1(\Pi_U, M_X).$$

Remark 2.67. One of the most important techniques of Anabelian Geometry is Kummer Evaluation. It is the process of evaluating Kummer classes of functions at points; it thus furnishes a method of evaluating functions in a group-theoretic manner.

Let $x = \operatorname{Spec} k \hookrightarrow X$ be a point. Then from the functoriality of the Kummer map we obtain the commutative diagram

$$\begin{array}{ccc} \mathcal{O}_X^\times & \longrightarrow & \mathrm{H}^1(\Pi_X, \widehat{\mathbb{Z}}(1)) \\ \downarrow & & \downarrow \\ \mathcal{O}_{\operatorname{Spec} k}^\times & \longrightarrow & \mathrm{H}^1(\Pi_{\operatorname{Spec} k}, \widehat{\mathbb{Z}}(1)) \end{array}$$

moreover, we have $k \cong \mathcal{O}_{\operatorname{Spec} k}^\times$ and $\mathrm{H}^1(\Pi_{\operatorname{Spec} k}, \widehat{\mathbb{Z}}(1)) \cong \mathrm{H}^1(\mathrm{G}_k, \widehat{\mathbb{Z}}(1)) \cong \widehat{k^\times}$. The induced map $\mathrm{H}^1(\Pi_X, \widehat{\mathbb{Z}}(1)) \to \mathrm{H}^1(\mathrm{G}_k, \widehat{\mathbb{Z}}(1))$ corresponds with evaluation of the Kummer class at the point x, we call this *Kummer evaluation*.

We can therefor 'read off' the value of a function (in its instance as a Kummer class) from the etale fundamental group. In fact we can do more. Given an open subscheme $U \hookrightarrow X$ and a cusp $x \in X - U$ we can ask what the valuation of an entire function on U is at x. It turns out that indeed we can *recover the valuation* by *restricting the relevant Kummer class to the Inertia group of the cusp*.

Indeed, consider the object $Z_x := \operatorname{Spec} \mathcal{O}_{X,x}^{sh} - \{x\}$, the etale zoomed-in neighborhood of the cusp x. Here the $\mathcal{O}_{X,x}^{sh}$ denotes the strict henselisation. We saw earlier that $\pi_1(Z_x) = I_x$. Again we consider restriction to obtain the commutative diagram

$$\begin{array}{ccc} \mathcal{O}_X^\times & \longrightarrow & \mathrm{H}^1(\Pi_X, \widehat{\mathbb{Z}}(1)) \\ \downarrow & & \downarrow \\ \mathcal{O}_{Z_x}^\times & \longrightarrow & \mathrm{H}^1(I_x, \widehat{\mathbb{Z}}(1)) \end{array}$$

Moreover, we have

Lemma 2.68. *In the diagram restriction to I_x sends the Kummer class κ_f to the valuation of f at the cusp x.*

Proof. We note that $Z_x = \operatorname{Spec} \overline{k}((T))^{sh}$ and an element of the etale fundamental group $(\zeta_n)_n \in I_x = \widehat{\mathbb{Z}}(1)$ act as $T^{1/n} \to \zeta_n T^{1/n}$. Suppose we have a function $f = T^r \cdot g$ where g is invertible at the cusp, so r is the valuation. Compute

$$\kappa_f \colon \zeta_n \to \frac{\zeta f^{1/n}}{f^{1/n}} = \frac{\zeta_n T^{r/n} g^{1/n}}{T^{r/n}} = (\kappa_f)^r = r \in \widehat{\mathbb{Z}}(1)$$

□

Lemma 2.69. *The Kummer map $\kappa_U : \Gamma(U, \mathcal{O}_U^\times) \to \mathrm{H}^1(\Pi_U, M_X)$ is injective.*

Proof. Suppose $\kappa_U(f) = 0$. For every closed point $x \in X$ we have a map $\mathrm{H}^1(\Pi_U, M_X) \to \mathrm{H}^1(\mathrm{G}_k, M_X) \cong (k^\times)^\wedge$ whose image is the evaluation of the function f at the point x. By assumption is the image zero. This implies that for some $N \in \mathbb{N}$ then for all $n \geq N$ we have $v_x(f) \in (k^\times)^n$. The field k Kummer faithful, which implies

$$\bigcap_{n \in \mathbb{N}} (k^\times)^n = \{0\}$$

We have $\forall x \in X$

$$ev_x(f) = 0$$

Since all valuations of f are zero this implies f is nilpotent. But all the our scheme is smooth hence reduced so $f = 0$ and the Kummer map is injective. □

Lemma 2.70. *The Galois cohomology group* $\mathrm{H}^0(\mathrm{G}_k, \Delta_X^{ab})$ *vanishes.*

Proof. We have

$$\mathrm{H}^0(\mathrm{G}_k, \Delta_X^{ab}) = \mathrm{H}^0(\mathrm{G}_k, T(J_X))$$

Elements $x \in T(J_X)^{\mathrm{G}_k}$ are compatible systems of torsion points $x = \{x_n\}_{n\in\mathbb{N}}$ with $x_n \in J_X[n](\overline{k})$ invariant under G_k, that is $x_n \in J_X[n](k)$.

It suffices to show the torsion subgroup of $J_X(k)$ is finite. This follows from Lemma 2.65. □

Theorem 2.71 (Grothendieck Spectral Sequence)**.** *Let $\mathcal{A}, \mathcal{B}$ be abelian categories and suppose $\mathcal{B}$ has enough injectives. Let $F : \mathcal{A} \to \mathcal{B}, G : \mathcal{B} \to \mathcal{C}$ be additive and left exact functors such that F takes F-acyclic objects to G-acyclic objects. For each object $A \in \mathcal{A}$ there is a spectral sequence that admits an F-acyclic resolution*

$$E_2^{pq} = (R^pG \circ R^qF)(A) \Longrightarrow R^{p+q}(G \circ F)(A).$$

Proof. See Theorem 5.8.3. in [Wei94]. □

Remark 2.72. As is well-known the Grothendieck spectral sequence should be thought of as the chain rule for derived functors. When applied to the case of pushforward of a morphism between topological space on the abelian category of abelian sheaves we obtain the Leray Spectral sequence. We will want to apply it in the case of group cohomology.

Recall that the group cohomology of a G-module M is defined as

$$\mathrm{H}^n(G, M) := \mathrm{Ext}^n_{\mathbb{Z}(G)}(\mathbb{Z}, M)$$

the right derived functor of $\mathrm{Hom}_{\mathbb{Z}(G)}(\mathbb{Z}, M) = M^G$, the invariants of M under the action of G.

Proposition 2.73. *We have an isomorphism*

$$\mathrm{H}^1(\Pi_X, M_X) \cong \mathrm{H}^1(\mathrm{G}_k, M_X)$$

Proof. We want to apply the Grothendieck Spectral Sequence. Let $\mathcal{A} = \Pi_X$-*Mod*, $\mathcal{B} = \mathrm{G}_k$-*Mod* the abelian categories of G_k and Π_X-modules. The surjection $\Pi_X \twoheadrightarrow \mathrm{G}_k$ induces a functor $F : \Pi_X$-*Mod* $\to$ G_k-*Mod* given as

$$F : (\Pi_X \curvearrowright M) \mapsto (\mathrm{G}_k \curvearrowright M^{\Delta_X})$$

where $\mathrm{G}_k \curvearrowright M^{\Delta_X}$ is defined by $g(m) = \widetilde{g}m, m \in M^{\Delta_X}$ where $\widetilde{g} \in \Pi_X$ is a lift of $g \in \mathrm{G}_k$. We check that if $\widetilde{g}' = \widetilde{g}h, h \in \Delta_X = \ker(\Pi_X \to \mathrm{G}_k)$ is another lift, then $\widetilde{g}'(m) = (\widetilde{g}h)(m) = \widetilde{g}(m)h(m) = \widetilde{g}(m)$ since $m \in M^{\Delta_X}$, so the action is well-defined.

Let $\mathcal{C} = \mathbf{Ab}$ the abelian category of abelian groups and consider $\mathrm{H}^0(\mathrm{G}_k, \cdot) : \mathrm{G}_k$-*Mod* $\to \mathbf{Ab}$, $\mathrm{H}^0(\Pi_X, \cdot) : \Pi_X$-*Mod* $\to \mathbf{Ab}$. It follows from Tensor-Hom adjunction that $\mathrm{H}^0(\mathrm{G}_k, \cdot)$ is left exact. In the same vein, the functor $F : \Pi_X$-*Mod* $\to \mathrm{G}_k$-*Mod* is left exact since it is right adjoint to $E : \mathrm{G}_k$-*Mod* $\to \Pi_X$-*Mod* given by $(\Pi_X \curvearrowright M) \mapsto (\Pi_X \twoheadrightarrow \mathrm{G}_k \curvearrowright M)$. It is well-known that $\mathcal{B} = \mathrm{G}_k$-*Mod* has enough injectives. Next, F sends $\mathrm{H}^0(\Pi_X, \cdot)$-acyclic objects to $\mathrm{H}^0(\mathrm{G}_k, \cdot)$-acyclic objects. Since Π_X acts on M_X through the surjection $\Pi_X \to \mathrm{G}_k$ we have a factorization

$$\mathrm{Hom}_{\mathbb{Z}(\Pi_X)}(\mathbb{Z}, M_X) = F \circ \mathrm{Hom}_{\mathbb{Z}(\mathrm{G}_k)}(\mathbb{Z}, M_X)$$

hence we may apply Theorem 2.71. The spectral sequence immediately implies that it remains to prove $\mathrm{H}^0(\mathrm{G}_k, \mathrm{H}^1(\Delta_X, M_X)) = 0$. Compute

$$\mathrm{H}^0(\mathrm{G}_k, \mathrm{H}^1(\Delta_X, M_X)) \cong \mathrm{H}^0(\mathrm{G}_k, \mathrm{H}^1(\Delta_{J(X)}, M_X)) \cong \mathrm{H}^0(\mathrm{G}_k, \Delta_X^{ab})$$

which vanishes by Lemma 2.70. □

We want to encode the rational functions as Kummer classes, meaning we want to group theoretically characterize the image of the Kummer map.

Remark 2.74. Let J_d denote the Picard scheme parametrizing degree d line bundles. We have a natural morphism $X \to J_1$ that sends a point of X to the line bundle of degree 1 associated to the this point. This morphism induces a surjection

$$\Pi_X \to \Pi_{J_1}$$

on the etale fundamental groups.

We have seen earlier that the etale fundamental group of the associated Picard (or Jacobian variety) scheme of a scheme X is the abelianization of Δ_X. Hence the kernel of the above map is the commutator subgroup of Δ_X. In some sense passing to the Jacobian variety 'abelianizes' everything. I should make a small technical note here, the theorems that we proved before strictly speaking only apply to proper smooth curves whose Jacobian is then an Abelian variety. In our case the curves are not necessarily proper hence we the Jacobian will in general be semi-abelian varieties; yet this is no matter. Let $X \hookrightarrow \overline{X}$ be the compactification. To reduce clutter write $J(k) = J_0(k)$. We have

$$0 \to \mathrm{Ker}(p) \to \pi_1(X) \xrightarrow{p} \pi_1(\overline{X}) \to 0.$$

Abelianization is right exact so we obtain a short exact sequence

$$(\mathrm{Ker}(p))^{ab}) \to \pi_1^{ab}(X) \xrightarrow{p} \pi_1^{ab}(\overline{X}) \to 0.$$

The map $X \to J(X)$ [really $X \to \mathrm{Pic}^0(X)$] induces a map

$$\begin{array}{ccccccc} (\mathrm{Ker}(p))^{ab}) & \longrightarrow & \pi_1^{ab}(X) & \xrightarrow{\quad p \quad} & \pi_1^{ab}(\overline{X}) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ \mathrm{Ker}(q) & \longrightarrow & \pi_1^{ab}(J(X)) & \xrightarrow{\quad q \quad} & \pi_1^{ab}(J(\overline{X})) & \longrightarrow & 0 \end{array}$$

We know $J(X)$ is a semi-abelian variety, $\mathrm{Ker}(q)$ coincides with the Tate module of the toric part, which is exactly a sum of Tate twists $\widehat{\mathbb{Z}}(1)$ (one for each cusp), and so coincides with $\mathrm{Ker}(p)^{ab} = \mathrm{Ker}(p) \cong \oplus_{cusp}\widehat{\mathbb{Z}}(1)$. I conclude $\pi_1(X)^{ab} \cong \pi_1^{ab}(J(X)) \cong T(J(X))$.
For each $x \in X(k)$ we have a section $s_x : \mathrm{G}_k \to \Pi_X$ well defined up to conjugation by Δ_X. Compose this with the surjection $\Pi_X \to \Pi_{J_1}$ to obtain maps $t_x : \mathrm{G}_k \to \Pi_{J_1}$. For any divisor D we similarly have a map $t_D : \mathrm{G}_k \to \Pi_{J_d}$, where $d = \deg(D)$.

The origin O of $J(X)$ furnishes a section $t_O : \mathrm{G}_k \to \Pi_{J_0}$. If D is of degree 0, then the difference of sections $t_D - t_O\colon\ \mathrm{G}_k \to \Pi_{J_0}$ [in additive notation] defines a 1-cocycle $\mathrm{G}_k \to \Delta_J$ hence a cohomology class $\eta_D \in \mathrm{H}^1(\mathrm{G}_k, \Delta_X^{ab})$.

Proposition 2.75. *1. A principal divisor will coincide with the section associated to the identity element of $J(k)$.*

2. *By restricting the cohomology classes of Π_U in $\mathrm{H}^1(\Pi_U, M_X)$ to the I_x for x a cusp, yields a natural exact sequence*

$$1 \to (k^\times)^\wedge \cong \mathrm{H}^1(\Pi_X, M_X) \to \mathrm{H}^1(\Pi_U, M_X) \to \oplus_{x \in \textit{cusps}} \widehat{\widehat{\mathbb{Z}}} \tag{2.3}$$

where we use synchronization of geometric cyclotomes to identify $\mathrm{Hom}_{\mathbb{Z}}(I_x, M_X)$ with $\hat{\mathbb{Z}}$; $(k^\times)^\wedge$ denotes the profinite completion of $k^\times$. Moreover, the image of $\Gamma(U, \mathcal{O}_U^\times)$ under κ_U in $\mathrm{H}^1(\Pi_U, M_X)/(k^\times)^\wedge$ is equal to the inverse image in $\mathrm{H}^1(\Pi_U, M_X)/(k^\times)^\wedge$ of the submodule of $\oplus_{x \in \textit{cusps}} \hat{\mathbb{Z}}$ determined by the principal divisors with support in the cusps.

Proof. There is a natural isomorphism

$$\mathrm{H}^1(\mathrm{G}_k, \Delta_X^{ab}) \to J(k)^\wedge$$

sending η_D to the element of $J(k)$ corresponding to D. Statement 1. then boils down to the fact that the identity element of $J(k)$ [principal divisors] correspond to the identity section $\mathrm{G}_k \to J(k)$. Let us prove the above isomorphism. Consider the short exact sequence

$$1 \to J(\overline{k})[n] \to J(\overline{k}) \to J(\overline{k}) \to 1$$

given by multiplication by n and apply the functor $\mathrm{H}^*(G_k, -)$ to this short exact sequence to obtain the long exact sequence

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathrm{H}^0(\mathrm{G}_k, J(\overline{k})[n]) & \longrightarrow & \mathrm{H}^0(\mathrm{G}_k, J(\overline{k})) \\ \hookrightarrow \mathrm{H}^0(G_k, J(\overline{k})) & \longrightarrow & \mathrm{H}^1(\mathrm{G}_k, J(\overline{k})[n]) & \longrightarrow & \mathrm{H}^1(\mathrm{G}_k, J(\overline{k})) \\ \hookrightarrow \mathrm{H}^1(\mathrm{G}_k, J(\overline{k})) & \longrightarrow & \mathrm{H}^2(\mathrm{G}_k, J(\overline{k})[n]) & \longrightarrow & \cdots \end{array}$$

take the limit over all $n \in \mathbb{N}$ to get

$$\begin{array}{ccccc} 0 & \longrightarrow & \varprojlim_n J(k)[n] & \longrightarrow & J(k) \\ \hookrightarrow J(k) & \longrightarrow & \mathrm{H}^1(\mathrm{G}_k, \Delta_X^{ab}) & \longrightarrow & \mathrm{Hom}(\mathrm{G}_k, J(\overline{k})) \\ \hookrightarrow \mathrm{Hom}(\mathrm{G}_k, J(\overline{k})) & \longrightarrow & \mathrm{H}^2(\mathrm{G}_k, \Delta_X^{ab}) & \longrightarrow & \cdots \end{array}$$

I claim $\mathrm{Hom}(\mathrm{G}_k, J(\overline{k})) \to \mathrm{Hom}(\mathrm{G}_k, J(\overline{k}))$ is an isomorphism. If this is true then $\mathrm{H}^1(G_k, \Delta_X^{ab}) \cong \varprojlim J(k)/nJ(k) = J(k)^\wedge$ as required.

The injectivity of $\mathrm{Hom}(\mathrm{G}_k, J(\overline{k})) \to \mathrm{Hom}(\mathrm{G}_k, J(\overline{k}))$ follows from the injectivity of $J(\overline{k}) \to J(\overline{k})$ which in turn, notice that we are talking about a projective limit of n-th power maps, corresponds to the 'Kummer-faithfullness' of the field k:

$$\bigcap_n J(k)[n] = \{0\}$$

We know that $\mathrm{H}^*(\mathrm{G}_k, J(\overline{k})[n]) \cong \mathrm{H}^*(\mathrm{G}_k, \Delta_X^{ab})$. The surjectivity would follow from the vanishing of $\mathrm{H}^2(\mathrm{G}_k, \Delta_X^{ab})$. From Tate duality again we obtain $\mathrm{H}^2(\mathrm{G}_k, \Delta_X^{ab}) \cong \mathrm{H}^0(\mathrm{G}_k, \Delta_X^{ab}(1)^\wedge = 0$ by Lemma 2.70

above. Hence we have an isomorphism for the limit over all $n \in \mathbb{N}$ of the cokernel of $J(\overline{k}) \to J(\overline{k})$, which is exactly $J(k)^\wedge$, with $\mathrm{H}^1(\mathrm{G}_k, \Delta_X^{ab})$.

Let us now continue with the proof of (2). This follows from the inflation restriction sequence. We just need to prove that $\mathrm{H}^1(\Pi_X, M_X) \cong \mathrm{H}^1(\mathrm{G}_k, M_X)$, which is exactly the content of Proposition 2.73.

Finally the rest of the statement is a restatement of Kummer evaluation: a function $f \in \mathcal{O}_U^\times$ is encoded by its divisor of zeroes and poles at the cusps. □

Definition 2.76. Let k be a sub-p-adic field. Let the 'number field closure' $\overline{k}_{NF} \subset \overline{k}$ be the algebraic closure of $\mathbb{Q}$ in $\overline{k}$. A curve X/k is a *NF curve* if $X_{\overline{k}} := X \times_k \overline{k}$ is defined over $\overline{k}^{NF}$. We shall call $\overline{k}$-points and rational functions on $X_{\overline{k}}$ that descend [take values in] to $\overline{k}_{NF}$ *NF-points* and *NF-rational functions*.

We may reconstruct the Galois cohomology group $\mathrm{H}^1(\Pi_U, M_X)$; to recover the function field we want to recover the image of the kummer map (using that it is injective). Consider the diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & k^\times & \longrightarrow & O_U^\times & \longrightarrow & \oplus_S \mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow & & \| \\ 1 & \longrightarrow & \widehat{k^\times} & \longrightarrow & P_U & \longrightarrow & \oplus_S \mathbb{Z} \\ \| & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \widehat{k^\times} & \longrightarrow & \mathrm{H}^1(\Pi_U, M_X) & \longrightarrow & \oplus_S \widehat{\mathbb{Z}} \end{array} \tag{2.4}$$

where the bottom line is the sequence from the proposition above, P_U the pullback. The function field $k^\times$ is obtained from pulling back from the second sequence. The validity of this construction follows from Proposition 2.75. As P_U is simply the pullback from $\mathrm{H}^1(\Pi_U, M_X)$ and $\oplus_S \widehat{\mathbb{Z}}$ it can be group-theoretically reconstructed. As seen from the graph above elements of P_U are principal divisors times the profinite completion of elements in $k^\times$. We will need to distinguish the cohomology classes $\eta \in P_U$ that come from 'genuine rational functions' from those that represent 'fake profinite rational functions'.

Proposition 2.77. *Suppose X is a NF-curve. Let $\eta \in P_U \subset \mathrm{H}^1(\Pi_U, M_X)$. We may group-theoretically characterise those Kummer cohomology classes κ_f arising from* NF rational functions $f \in k_U^\times$.

(i) A cohomology class $\eta \in P_U$ is a nonconstant *NF rational function if there exists a positive multiple $\eta^\dagger$ of η, finite extensions k_{x_i}/k and NF-points $x_i \in U(k_{x_i})$ for $i = 1, 2$ such that*

$$\eta(x_1) := s_{x_i}^*(\eta) = 1$$

and

$$\eta(x_1) := s_{x_i}^*(\eta) \neq 1$$

where $s_{x_i}^*$ denote the maps

$$s_{x_i}^* : \mathrm{H}^1(\Pi_U, M_X) \to \mathrm{H}^1(\mathrm{G}_{k_{x_i}}, M_X)$$

induced from the sections $s_{x_i} \colon \mathrm{G}_{k_{x_i}} \to \Pi_U$ associated with the points.

(ii) A cohomology class $\eta \in P_U \bigcap \mathrm{H}^1(\mathrm{G}_k, M_X) \cong \widehat{k^\times}$ [see the above short exact sequence 2.3] is a constant *NF rational function if there exists a nonconstant rational function $f \in P_U$ and a point $x \in U(k_x)$, such that*

$$s_x^* f = f(x) = \eta(x)$$

Proof. A general element $\eta \in P_U$ is a product of a rational function f in the linear system associated to the divisor that is the image of η under $P_U \to \oplus_S \widehat{\mathbb{Z}}$ and an element $\lambda \in \widehat{k^\times}$: $\eta = \lambda \cdot f$. This follows from the diagram 2.4 above. To distinguish the 'genuine rational functions' from the ' fake profinite rational functions' we need to find those $\eta = \lambda \cdot f$ such that $\lambda \in k^\times$; the idea is to evaluate at a point and force its value to lie in $k^\times$. It is difficult to pick out, that is to characterize, individual elements of $k^\times$. The only exception is $1 \in k^\times$.

Proof of (i) Given X or U we may consider the basechange $X_{\overline{k}}$ along the algebraic closure $\overline{k}$ of k; under our assumption that X [or U] is a NF curve this descends to $X_{\overline{k}_{NF}}$. A rational function $f \in \overline{k}_{NF}^\times(X)$ gives a morphism $X_{\overline{k}_{NF}} \to \mathbb{P}^1_{\overline{k}_{NF}}$; if the rational function is nonconstant the induced map $X_{\overline{k}_{NF}}(\overline{k}_{NF}) \to \mathbb{P}^1_{\overline{k}_{NF}}(\overline{k}_{NF})$ is surjective. This follows from the Zariski topology since the map is finite hence closed and the image is infinite.

This means that the fiber of $1 \in \mathbb{P}^1_{\overline{k}_{NF}}(\overline{k}_{NF})$ in $X_{\overline{k}_{NF}}(\overline{k}_{NF})$ is nonempty; it may happen however, that while the fiber of 1 is nonempty it does not have any elements in U. The solution is to consider positive powers of η; if one of these have value 1 at an NF-point $x \in U(k_x$ this means that η has value $\zeta_n = s_x^*(\eta)$. This means exactly

$$\zeta_n = s_x^*(\eta) = \lambda \cdot s_x^*(f) = \lambda f(x)$$

or

$$\lambda = \zeta_n f(x)^{-1}$$

hence $\lambda \in k^\times$.

To distinguish the nonconstant functions we simply pick those rational functions that have two different values at two different points. **Proof of (ii)** Forcing the twin conditions $\eta \in P_U \bigcap \mathrm{H}^1(\mathrm{G}_k, M_X) \cong \widehat{k^\times}$ and $\eta_x \in k^\times$ implies $\eta \in k^\times$ as required. □

Finally we come to reconstructing the function field of X. From the previous steps we obtained the multiplicative group $k^\times$. I claim we can reconstruct the additive structure. Let me also remark that we have access to the valuation of the function $f \in k^\times$ by the discussion in Remark 2.67.

The reconstruction of the additive structure will follow by an old argument due to Uchida using the linear systems associated with divisors. Because we have reconstructed the decomposition groups of closed points, cf Belyi Cuspidalisation, it makes sense to talk about divisors.

Definition 2.78. Suppose X is proper and k is algebraically closed. Set $\mathrm{Div}(f)$ to be the divisor of $f \in k_X$, If D is a divisor on X write

$$L(D) := \{f \in k_X \mid Div(f) + D \geq 0\}$$

Proposition 2.79. *Let X be proper [so that the divisor of a rational function is of degree zero] over a field k that is algebraically closed. Given*

(i) The abstract group $K_X^\times$

(ii) the set of surjective homomorphisms

$$V_X = \{ord_x \colon k_X^\times \twoheadrightarrow \mathbb{Z}\}_{x \in X(k)}$$

(iii) for each homomorphisms $v_x = ord_x \in V_X$, the subgroup $U_v \subset k_X^\times$ given by the $f \in k_X^\times$ such that $f(x) = 1$.

Proof. We will reconstruct the additive structures in several steps.
Our first observation is that $k^\times$ can be characterized inside $K^\times$ as

$$k^\times = \bigcap_{v \in V_X} \mathrm{Ker}(v)$$

Remark that if we can recover the additive structure on k we automatically obtain the additive structure on $K^\times$. We have group-theoretic access to the points and valuations so it makes sense to talk about divisors. To add two elements a, b in k we will find a divisor D, points x, y_1, y_2 and functions $f_1, f_2 \in L(D)$ such that $f_1(x) + f_2(x) = a + b$.

Start with any divisor D such that $l(D) \geq 2$. By subtracting a well chosen effective divisor we can reduce to the case that $l(D) = 2$. Take $x \in X(k) - \mathrm{Supp}(D)$ to be a point such that $L(D)$ has a section that doesn't vanish at x, i.e. $l(D - x) = 1$. Then take y_1 similarly, i.e. such that $l(D - x - y_1) = 0$. Finally pick $y_2 \in X(k) - \mathrm{Supp}(D) \bigcup \{x, y_1\}$ such that $l(D - x - y_2) = l(D - y_1 - y_2) = 0$.

With this setup it follows that there exists $f_1, f_2 \in L(D), a, b \in k^\times$ such that $f_1(y_1) \neq 0, f_1(y_2) = 0, f_1(x) = a$ and $f_2(y_2) \neq 0, f_2(y_1) = 0, f_2(x) = b$.

Now we can add a and b as follows. Suppose $\frac{a}{b} \neq -1$ [otherwise $a + b = 0$, -1 is the unique element of order 2] and let $f_1 + f_2$ be the unique element in $L(D)$ such that $(f_1 + f_2)(y_1) = f_1(y_1)$ and $(f_1 + f_2)(y_2) = f_2(y_2)$. Then $a + b := (f_1 + f_2)(x)$.

□

We can now prove Theorem 1.40 and hence Corollary 1.41.

Theorem 2.80. *Let X be a hyperbolic curve of strictly Belyi type over a p-adic field or a number field k. Let $\overline{k}$ a separable algebraic closure of k. There exists a functorial 'group-theoretic' algorithm for reconstructing from $\Pi_X^\dagger$ the function field and the base field of X.*

$$\Pi_X^\dagger \mapsto \Pi_X^\dagger \twoheadrightarrow \mathrm{G}_k^\dagger \curvearrowright \overline{k}$$

and

$$\Pi_X^\dagger \mapsto \Pi_X^\dagger \curvearrowright \overline{K}(X)$$

where $K(X)$ denotes the function field of X.

Proof. We apply all the results we have seen before, in the following steps

Step 1: Recover the geometric fundamental group [Lemma 2.15, Lemma 2.3] and the homotopy sequence

$$1 \to \Delta_X \to \Pi_X \to \mathrm{G}_k \to 1$$

Step 2: Recover the [conjugacy classes of] inertia subgroups $I_y = I_{\tilde{y}/y} \subset \Delta_X$ as in Theorem 2.45.

Step 3: Using Step 2 apply Belyi Cuspidalization [Theorem 2.62] to obtain the surjections

$$\Pi_U \twoheadrightarrow \Pi_Y \subset \Pi_X$$

where $Y \to X$ is any hyperbolic NF-curve that arises as a finite etale cover of X, and $U \subset Y$ is an open obtained from Y by removing a finite collection of NF-points. Additionally, using Step 2 and the fact that the normalizers $N_{\Pi_U}(I_x)$ of cuspidal inertia groups are the cuspidal decomposition groups D_y [where the cusps are NF-points!], reconstruct the decomposition groups of closed NF points of X as the images of the cuspidal decomposition groups $D_y \subset \Pi_U \twoheadrightarrow \Pi_X$. Remark that we can characterize hyperbolic NF-curves $Y \to X$ [that is, the corresponding open subgroups of Π_X]: hyperbolicity is easy and is a simple genus and punctures count while the NF-ness of a curve can be checked by applying Belyi's theorem.

Step 4: Apply synchronization of cyclotomes to obtain natural isomorphisms

$$I_z \xrightarrow{\sim} \mu_{\overline{k}}^{\widehat{\mathbb{Z}}}(\Pi_U) = M_{\overline{Y}}$$

where $U \subset Y \to X$ is as in Step 3, Y is of genus ≥ 2 [this can be easily detected as in the proof of Theorem 2.45], and $Y \hookrightarrow \overline{Y}$ is the canonical compactification of Y.

Step 5: For $U \subset Y \subset \overline{Y}$ as in Step 4, construct the subgroup

$$\mathcal{P}_U \subset \mathrm{H}^1(\Pi_U, \mu_{\overline{k}}^{\widehat{\mathbb{Z}}}(\Pi_U))$$

of cuspidal principal divisors [Proposition 2.75].

Step 6 Next, construct

$$\overline{k_{NF}^{\times}} \subset K_{\overline{Y},NF}^{\times} \hookrightarrow \varinjlim_{V} \mathrm{H}^1(\Pi_V, \mu_{\overline{k}}^{\widehat{\mathbb{Z}}}(\Pi_U))$$

using the characterization of NF-functions [Proposition 2.77]. Here V ranges over the open subschemes obtained by removing a finite number of NF-points from $\overline{Y} \times k'$, where k' is a finite extension of k. This can obviously be detected using the recovery of decompostion groups.

Step 7: Reconstruct the additive structure on $\overline{k}_{NF}^{\times} \cup \{0\}$ and $K_{\overline{Y},NF}^{\times}$ using Proposition 2.79, Step 2,3,5 and the fact that Kummer evaluation yields a group-theoretic way to recover the order of a function at a cusp. Be aware that Proposition 2.79 requires an algebraically closed field, so may only be applied to the algebraically closed $\overline{k}_{NF}^{\times}$. But if we know the addition on the constant field $\overline{k}_{NF}^{\times}$ we immediately recover the addition on the function field $K_{\overline{Y},NF}^{\times}$.

Step 8: From Step 6 one easily reduces to the [NF-part of the] function field $K_{NF,X}$ of X. One finally applies the result of Corollary 1.10 of [Moc15], which has not been covered in this thesis because of space constraints.

□

Bibliography

[Ach] Piotr Achinger. Group cohomology of fundamental group of a curve. MathOverflow. URL:https://mathoverflow.net/questions/239195/group-cohomology-of-fundamental-group-of-a-curve (visited on 12-07-2017).

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[CI99] Robert Coleman and Adrian Iovita. The Frobenius and monodromy operators for curves and abelian varieties. *Duke Math. J.*, 97(1):171–215, 1999.

[FJ86] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1986.

[FvdP04] Jean Fresnel and Marius van der Put. *Rigid analytic geometry and its applications*, volume 218 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 2004.

[Gro63] Alexander Grothendieck. *Revêtements étales et groupe fondamental. Fasc. I: Exposés 1 à 5*, volume 1960/61 of *Séminaire de Géométrie Algébrique*. Institut des Hautes Études Scientifiques, Paris, 1963.

[Gro95] Alexander Grothendieck. Technique de descente et théorèmes d'existence en géométrie algébrique. II. Le théorème d'existence en théorie formelle des modules. In *Séminaire Bourbaki, Vol. 5*, pages Exp. No. 195, 369–390. Soc. Math. France, Paris, 1995.

[GvdG] Ben Moonen Gerard van der Geer. *Abelian Varieties, preliminary version*.

[Hos15] Yuichiro Hoshi. Mono-anabelian reconstruction for number fields. *RIMS preprint*, 2015.

[JR79] Moshe Jarden and Jürgen Ritter. On the characterization of local fields by their absolute Galois groups. *J. Number Theory*, 11(1):1–13, 1979.

[JW83] Uwe Jannsen and Kay Wingberg. Die Struktur der absoluten Galoisgruppe P-adischer Zahlkörper. *Invent. Math.*, 70(1):71–98, 1982/83.

[Kim05] Minhyong Kim. The motivic fundamental group of $\mathbf{P}^1 - \{\mathbf{0}, \mathbf{1}, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[Kö] Bernard Köck. Belyi's theorem revisited.

[Maj] Hadian Majid. Lectures on etale fundamental groups. *preprint*.

[Mat] Akhil Mathew. Flatness revisited.

[Mila] J.S. Milne. *Jacobian varieties*.

[Milb] J.S. Milne. *Lectures on Etale Cohomology*.

[Mil06] J. S. Milne. *Arithmetic duality theorems*. BookSurge, LLC, Charleston, SC, second edition, 2006.

[Moc97] Shinichi Mochizuki. A version of the Grothendieck conjecture for p-adic local fields. *Internat. J. Math.*, 8(4):499–506, 1997.

[Moc98] Shinichi Mochizuki. Correspondences on hyperbolic curves. *Journal of Pure and Applied Algebra*, pages 227–244, 1998.

[Moc99] Shinichi Mochizuki. The local pro-p anabelian geometry of curves. *Invent. Math.*, 138(2):319–423, 1999.

[Moc03] Shinichi Mochizuki. Topics surrounding the anabelian geometry of hyperbolic curves. In *Galois groups and fundamental groups*, volume 41 of *Math. Sci. Res. Inst. Publ.*, pages 119–165. Cambridge Univ. Press, Cambridge, 2003.

[Moc04] Shinichi Mochizuki. The absolute anabelian geometry of hyperbolic curves. In *Galois theory and modular forms*, volume 11 of *Dev. Math.*, pages 77–122. Kluwer Acad. Publ., Boston, MA, 2004.

[Moc07a] Shinichi Mochizuki. Absolute anabelian cuspidalizations of proper hyperbolic curves. *Journal of Mathematics, Kyoto University*, pages 451–539, 2007.

[Moc07b] Shinichi Mochizuki. A combinatorial version of the Grothendieck conjecture. *Tohoku Math. J. (2)*, 59(3):455–479, 2007.

[Moc12] Shinichi Mochizuki. Topics in absolute anabelian geometry I: generalities. *J. Math. Sci. Univ. Tokyo*, 19(2):139–242, 2012.

[Moc15] Shinichi Mochizuki. Topics in absolute anabelian geometry III: global reconstruction algorithms. *J. Math. Sci. Univ. Tokyo*, 22(4):939–1156, 2015.

[Mum08] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[Nak90] Hiroaki Nakamura. Galois rigidity of the étale fundamental groups of punctured projective lines. *J. Reine Angew. Math.*, 411:205–216, 1990.

[Nak97] Hiroaki Nakamura. Galois rigidity of profinite fundamental groups [translation of Sūgaku **47** (1995), no. 1, 1–17; MR1362515 (98d:14027)]. *Sugaku Expositions*, 10(2):195–215, 1997. Sugaku Expositions.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Rub00] Karl Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.

[Ser06] Jean-Pierre Serre. *Lie algebras and Lie groups*, volume 1500 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2006. 1964 lectures given at Harvard University, Corrected fifth printing of the second (1992) edition.

[ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[Sta16] The Stacks Project Authors. *stacks project, 2016.*

[Sti12] Jakob Stix. On cuspidal sections of algebraic fundamental groups. In Galois-Teichmüller theory and arithmetic geometry*, volume 63 of* Adv. Stud. Pure Math.*, pages 519–563. Math. Soc. Japan, Tokyo, 2012.*

[Sti13] Jakob Stix. Rational points and arithmetic of fundamental groups*, volume 2054 of* Lecture Notes in Mathematics*. Springer, Heidelberg, 2013. Evidence for the section conjecture.*

[Tam97] Akio Tamagawa. The grothendieck conjecture for affine curves. Compositio Math 109*, pages 135–194, 1997.*

[Tat67] J. T. Tate. p-divisible groups. In Proc. Conf. Local Fields (Driebergen, 1966)*, pages 158–183. Springer, Berlin, 1967.*

[Tat71] John Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda). In Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363*, volume 175 of* Lecture Notes in Math.*, pages Exp. No. 352, 95–110. Springer, Berlin, 1971.*

[vB] R. van Bommel. The grothendieck monodromy theorem.

[Vis] Angelo Vistoli. Branched covers of compact riemann surfaces. MathOverflow. URL:`https://mathoverflow.net/questions/69904/branched-covers-of-compact-riemann-surfaces`*, URL = https://mathoverflow.net/questions/69904/branched-covers-of-compact-riemann-surfaces, URLDATE = 12-07-2017,.*

[Wei] Jared Weinstein. The geometry of lubin-tate spaces.

[Wei94] Charles A. Weibel. An introduction to homological algebra*, volume 38 of* Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.*