Local-to-Global Extensions for Wildly Ramified Covers of Curves

by

Renee Hyunjeong Bell

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Mathematics

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2018

Signature redacted

Author . . . .
Department of Mathematics
April 27, 2018

Certified by . . . . Signature redacted . . . .
Bjorn Poonen
Professor of Mathematics
Thesis Supervisor

Signature redacted

Accepted by . . . .
William Minicozzi
Chairman, Department Committee on Graduate Theses

Local-to-Global Extensions for Wildly Ramified Covers of Curves

by

Renee Hyunjeong Bell

Submitted to the Department of Mathematics
on April 27, 2018, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Mathematics

Abstract

Given a Galois cover of curves $X \to Y$ with Galois group G which is totally ramified at a point x and unramified elsewhere, restriction to the punctured formal neighborhood of x induces a Galois extension of Laurent series rings $k((u))/k((t))$. If we fix a base curve Y, we can ask when a Galois extension of Laurent series fields comes from a global cover of Y in this way. Harbater proved that over a separably closed field, every Laurent series extension comes from a global cover for any base curve if G is a p-group, and he gave a condition for the uniqueness of such an extension. Using a generalization of Artin–Schreier theory to non-abelian p-groups, we characterize the curves Y for which this extension property holds and for which it is unique up to isomorphism, but over a more general ground field.

Thesis Supervisor: Bjorn Poonen
Title: Professor of Mathematics

Acknowledgments

This thesis is dedicated to my mother, Kimberly; without her love, wisdom, and countless sacrifices there is no question that I would not have made it to where I am today. I would like to thank her for empowering and liberating me with her unconditional support, for reminding me to look after my physical and mental health first, and for regularly sending me the most moving text messages known to humankind.

I would also like to thank my advisor, Bjorn Poonen, for giving me this problem, for teaching me new things every time we meet, for his unparalleled generosity with his time, and for his unwavering support and advocacy in all of my endeavors, mathematical and otherwise.

Much of my mathematical growth has come from helpful conversations, especially with Andrew Obus, David Harbater, Piotr Achinger, Drew Sutherland, Davesh Maulik, François Charles, and Rachel Pries. I have benefited greatly from their guidance, insights, and experience.

My dear friends in the MIT math department have blessed me with joy and mathematical inspiration, especially Padma Srinivasan, Ruthi Hortsch, Eva Belmont, Isabel Vogt, Nicholas Triantafillou, and the late and incomparable Amelia Perry (may she rest in power). I would also like to thank Barbara Peskin and Michele Gallarelli for just being fun and delightful people and for their genuine care for and investment in me and the other graduate students; I truly felt that they were rooting for me and that helped me persevere.

I would like to thank my family, who have been there for me outside of math, before math, and in the aftermath: my grandparents, who have believed in me and encouraged me from my infancy, and my grandma who has brightened my mood every day with all the nice grandma things she has told me over the phone; my aunts and uncles, who were constantly encouraging me and made me feel like I was really making them proud; and my cousins Esther, John, and Lawrence, for providing so much happiness and light during vacations, visits, and group KaTalk chats. I would also like to thank my Big Brothers Big Sisters of Massachusetts Bay family, Alyssa and Miguelina Santiago. I would like to thank Alyssa for all the fun, creativity, and energy she has brought into my life, for inspiring me to be a better person, and for giving me hope for the future. I would like to thank Miguelina for being an inspiration by being such a dedicated mom, and for being like family to me, which made me feel much more at home in Cambridge.

Finally, I would like to thank Yehonatan Sella for making my life better every single day with his kindness, support, and ability to see the best of every situation and every person.

Contents

Chapter 1

Introduction

This thesis concerns Galois covers of curves in characteristic p. We give conditions under which one can extend very local data about a formal neighborhood of a point to a global cover of curves with specified ramification, extending work of Harbater in [Har80] to arbitrary fields, which might not be algebraically closed. We do this by working explicitly with equations for covers of curves, which we do by introducing a cohomological interpretation and refinement of Inaba's nonabelian Artin–Schreier theory.

In general, arithmetic geometers are interested in the geometry of spaces defined over more number-theoretic fields, not only $\mathbb{C}$; our primary focus is curves over fields of characteristic p. Many of the tools used in complex geometry do not translate directly to geometry over other fields. For example, the fundamental group $\pi_1(X)$ of a topological space X is an invariant which is used to classify unramified covers of X. However, over fields of characteristic p, literal paths do not make sense and we cannot rely on them for geometric information. The theory of the étale site and the étale fundamental group π_1^{et}, as introduced by Artin and Grothendieck, provided beautiful analogues of these topological objects.

For a smooth affine curve X over $\mathbb{C}$, $\pi_1^{et}(X)$ turns out to be the profinite completion of $\pi_1(X)$, which admits a simple description in terms of its genus g and the number r of points of $\bar{X} - X$, where $\bar{X}$ is a smooth compactification of X. Grothendieck proved that the same description of $\pi_1^{et}(X)$ in terms of g and r applies over any algebraically closed field k of characteristic 0; in particular, in characteristic 0, $\pi_1^{et}(X)$ does not depend on the field. Grothendieck also showed that the prime-to-p quotient of $\pi_1^{et}(X)$ is the same in characteristic p as the prime-to-p quotient of π_1^{et} of a curve over $\mathbb{C}$ having the same g and r.

However, when k has characteristic p, looking at Galois covers with Galois group a p-group reveals some dramatic differences from the characteristic 0 case. For example, we know $\pi_1^{et}(\mathbb{A}^1_{\mathbb{C}}) = \{1\}$, so $\mathbb{A}^1_{\mathbb{C}}$ has no nontrivial unramified $\mathbb{Z}/p\mathbb{Z}$ covers, whereas for k of characteristic p, $\mathbb{A}^1_k$ has many $\mathbb{Z}/p\mathbb{Z}$-covers. Indeed, they are parameterized by $k[t]/\wp(k[t])$ via the map sending f to the affine cover $k[t,y]/(y^p - y - f)$, where $\wp$ is the Artin–Schreier map $f \mapsto f^p - f$. From this, we can already see that the fundamental group is more complicated, and even depends on the base field. Using covers such as these, one sees that the pro-p fundamental group $\pi_1^p(X)$ of any affine curve is infinitely generated. The rich study of p-group covers of curves has motivated this thesis.

Now fix an arbitrary field k of characteristic p and a finite p-group G.

Let Y be a smooth proper curve over k and $y \in Y(k)$. We define a "y-ramified G-cover of Y" to be a Galois cover of curves $q \colon X \to Y$ with Galois group G, totally ramified over y and unramified above the complement $Y' := Y - \{y\}$. Now let x be the k-point of X lying above y; then q induces a map Spec $\hat{\mathcal{O}}_{X,x} \to$ Spec $\hat{\mathcal{O}}_{Y,y}$. Let t be a uniformizer at y, so by the Cohen structure theorem, $\hat{\mathcal{O}}_{Y,y} \cong k[[t]]$. We can also choose a uniformizer u such that $\hat{\mathcal{O}}_{X,x} \cong E[[u]]$ for E a finite extension of k, but in fact we must have $\hat{\mathcal{O}}_{X,x} \cong k[[u]]$ since the extension E/k would be unramified, and would have to be degree 1 since q is totally ramified at x. Taking fraction fields gives rise to an extension of Laurent series fields $k((u))/k((t))$ which is Galois with Galois group G.

We say that the extension $k((u))/k((t))$ *arises from* the G-action on X.

Thus, for each curve Y and point $y \in Y$, we obtain a functor

$$\varphi_{Y,y}\colon \left\{\begin{matrix} y\text{-ramified} \\ p\text{-group covers} \\ \text{of } Y \end{matrix}\right\} \to \left\{\begin{matrix} \text{Galois field extensions} \\ k((u)) \text{ over } k((t)) \text{ with Galois} \\ \text{group a } p\text{-group} \end{matrix}\right\}^{op} l$$

The functor $\varphi_{Y,y}$ can be extended to the entire category of Galois covers (as defined in Definition 2.1.4) X of Y with Galois group a p-group which are unramified over Y', including covers where X is not integral. We define $\psi_{Y,y}$ by mapping the cover $q : X \to Y$ to $\mathcal{O}(X \times_Y \operatorname{Spec} k((t)))$ and obtain a functor

$$\psi_{Y,y}\colon \left\{\begin{matrix} \text{Galois covers } X \\ \text{of } Y \text{ with Galois group} \\ \text{a } p\text{-group that are} \\ \text{unramified over } Y' \end{matrix}\right\} \to \left\{\begin{matrix} \text{Galois étale algebras} \\ \text{over } k((t)) \text{ with Galois} \\ \text{group a } p\text{-group} \end{matrix}\right\}^{op}$$

From now on, we denote the source category by $\mathcal{C}$ and the target category by $\mathcal{D}$.

Understanding the functors $\psi_{Y,y}$ and $\varphi_{Y,y}$ allows one to use the geometry of Galois covers of curves to classify automorphisms of $k[[t]]$ as in [BCPS17]. In the other direction, it allows us to use extensions of $k((t))$ in order to classify possibilities for the ramification filtration for a Galois covers of curves with Galois group a p-group, as noted in the survey [HOPS].

Questions about $\psi_{Y,y}$ and $\varphi_{Y,y}$ can be approached by turning to étale cohomology. Throughout this thesis, for a scheme S and a (not necessarily abelian) group G, we denote by $\underline{G}$ the constant sheaf of groups associated to G with respect to the étale site on X, and we denote by $H^1(S, G)$ the Čech cohomology set $\check{H}^1_{et}(S, \underline{G})$;

this cohomology set parameterizes principal G-bundles on X, as noted on p. 75 of [Mil08]. Let $\mathcal{O}(Y')$ be the ring of regular functions on Y'. The inclusion $\mathcal{O}(Y') \hookrightarrow k((t))$ induces a map Spec $k((t)) \to Y'$ which we can think of as inclusion of the formal deleted neighborhood around y into Y'. Hence, we obtain a map $\Psi_{Y,y,G} : H^1(Y', G) \to H^1(k((t)), G)$.

We denote by $\mathcal{C}_G$ be the category of pairs consisting of an object $X \to Y$ of $\mathcal{C}$ and an injective homomorphism $G \to \mathrm{Aut}(X/Y)$; a morphism in $\mathcal{C}_G$ is a morphism in $\mathcal{C}$ that respects the G-actions. Define $\mathcal{D}_G$ similarly using objects of $\mathcal{D}$. We denote by $\psi_{Y,y,G}$ the functor $\mathcal{C}_G \to \mathcal{D}_G$ which is the restriction of $\psi_{Y,y}$.

Elements of $H^1(Y', G)$ correspond to isomorphism classes of G-Galois étale covers of Y'. From a G-Galois étale cover X' of Y', we can get a G-Galois cover X of Y by taking the normalization of Y in X'. Conversely, a G-Galois cover X of Y which is unramified over Y' restricts to a G-Galois étale cover of Y', and this restriction gives us a bijective map from the isomorphism classes of $\mathcal{C}$ to $H^1(Y', G)$; similarly we have a bijective map from isomorphism classes of $\mathcal{D}$ to $H^1(k((t)), G)$, and we see that $\Psi_{Y,y,G}$ comes from $\psi_{Y,y,G}$ applied to isomorphism classes.

By the above discussion, $\psi_{Y,y}$ is essentially surjective if and only if $\Psi_{Y,y,G}$ is surjective for every p-group G. And $\psi_{Y,y}$ is an equivalence of categories if and only if $\Psi_{Y,y,G}$ is an isomorphism for every p-group G. Also, $\psi_{Y,y}$ is injective on isomorphism classes of $\mathcal{C}$ if and only if $\Psi_{Y,y,G}$ is injective for every p-group G.

We pose some basic questions about $\Psi_{Y,y,G}$.

Question 1.0.1. *When is $\Psi_{Y,y,G}$ surjective?*

A positive answer would imply that every G-Galois extension of $k((t))$ extends to a global Galois cover of Y, and so $\psi_{Y,y}$ is essentially surjective, by the above remarks. In [Har80], Harbater showed that if the ground field k is algebraically closed, then $\psi_{Y,y,G}$ is surjective for any p-group G. In this thesis, we provide an answer to Question 1.0.1 over a more general field k, not necessarily algebraically or even separably closed, in Theorem 1.0.2.

Notation: for any ring R of characteristic p, let $\wp\colon R \to R$ denote the Artin–Schreier map $f \mapsto f^p - f$.

Theorem 1.0.2. *Let G be a nontrivial finite p-group. Then the following are equivalent:*

(a) The equality $k((t)) = \wp(k((t))) + \mathcal{O}(Y')$ holds.

(b) The map $\Psi_{Y,y,G}$ is surjective.

We note that (a) is *independent of* G, so for any nontrivial p-groups G and G', the map $\Psi_{Y,y,G}$ is surjective if and only if $\Psi_{Y,y,G'}$ is surjective.

We can also ask whether two global Galois covers of Y in $\mathcal{C}$ which are not isomorphic over Y can induce isomorphic extensions of $k((t))$.

Question 1.0.3. *When is $\Psi_{Y,y,G}$ injective?*

An answer to this over algebraically closed fields k was given as well by Harbater in [Har80]. In fact, he calculates that each fiber of $\Psi_{Y,y,G}$ has size p^r, where r is the p-rank of Y. We extend the answer to Question 1.0.3 to a more general field k, which might not be separably closed.

Theorem 1.0.4. *Let G be a nontrivial finite p-group. Then the following are equivalent:*

(a) The equality $\wp(k((t))) \cap \mathcal{O}(Y') = \wp(\mathcal{O}(Y'))$ holds.

(b) The map $\Psi_{Y,y,G}$ is injective.

We note that (a) of this theorem also is independent of G, so for any nontrivial p-groups G and G', the map $\Psi_{Y,y,G}$ is injective if and only if $\Psi_{Y,y,G'}$ is injective.

Combining our answers to Questions 1.0.1 and 1.0.3, without assuming that the base field is algebraically or even separably closed, gives a criterion for $\Psi_{Y,y,G}$ to be a bijection, or equivalently for $\psi_{Y,y}$ to be an equivalence of categories. This generalizes the result of Katz in [Kat86], which states that over any field of characteristic p, the functor $\psi_{\mathbb{P}^1,\infty}$ is an equivalence of categories. Curves satisfying the criteria of Theorems 1.0.2 and 1.0.4 are particularly useful for relating the geometry of the curve and its covers to properties of $k((t))$ and its extensions. In Chapter 4 of this thesis, we give examples of such curves beyond $\mathbb{P}^1$.

Our proofs of these theorems use new and more explicit methods. Proofs in previous work, as in [Kat86], have reduced the problem to the case in which G is abelian. In this case, one can use the vanishing of certain H^2 groups or a characterization of abelian p-group field extensions using Witt vector theory, as noted in [HOPS]. However, in this thesis, we prove our results using a different method: describing and working with an explicit characterization of G-Galois étale algebras for G not necessarily abelian, given in Theorem 3.2. This characterization, which we will call the Inaba classification, is a generalization of a theorem of Inaba in [Ina61], which extends Artin–Schreier–Witt theory to nonabelian Galois étale algebras.

Chapter 2

Background and Definitions

2.1 Galois Covers and Étale Cohomology

In topology, a lot of information about a space can be gleaned from its covers and the automorphism groups of those covers (also called *deck transformations*). In particular, a useful algebraic invariant of a path-connected, locally path-connected topological space X (with base point x) is the fundamental group $\pi_1(X, x)$, which can be defined as either homotopy classes of loops at x, or automorphisms of a universal cover over X.

By a variety over k, where k is a field, we mean a separated geometrically reduced scheme of finite type over k. Varieties over the complex numbers have analytic spaces associated to them, and one can compute the topological fundamental group of these. But for varieties V over other fields, like finite fields, there is not a sensible theory of continuous maps from the interval $[0, 1]$ to V, and we also need a more algebro-geometric sense of "cover" that does not rely on the analytic notion of "local diffeomorphism" or purely topological notions. To this end, Alexander Grothendieck defined étale maps for schemes. We now recall this theory, following Milne's lectures on étale cohomology [Mil08].

Definition 2.1.1. *We say a morphism of varieties $f : X \to Y$ is étale if it is smooth and unramified.*

In topology, a cover $f : X \to Y$ is *regular* if the action of $G := \mathrm{Aut}(X/Y)$ is transitive on each fiber, which is equivalent to X being a principal G-bundle over Y, or, for finite covers, equivalent to the size of each fiber being equal to $|G|$. Principal G-bundles are in one-to-one correspondence with homomorphisms $\pi_1(Y) \to G$. *Finite* étale maps serve as analogues to covering maps; the analogue to regular covering maps is as follows:

Definition 2.1.2. [PS11, p. 4] *For a finite group G, a G-Galois étale cover is a finite étale map $f : X \to Y$ together with an inclusion $\rho : G \hookrightarrow \mathrm{Aut}(X/Y)$ such that $f^{-1}(\mathcal{O}_Y)$ is equal to the sheaf of G-invariants of $\mathcal{O}_X$.*

Definition 2.1.3. [Mil08, p. 29] *For a connected normal variety Y and a geometric point $\bar{y}$ of Y lying over the generic point of Y, and Ω the corresponding algebraic closure of the function field $k(Y)$, we let L be the union of all the finite separable field extensions K of $k(Y)$ in Ω such that the normalization of Y in K is étale over Y; then the étale fundamental group $\pi_1^{et}(Y, \bar{y})$ is*

$$\pi_1(Y, \bar{y}) = \mathrm{Gal}(L/k(Y)).$$

When Y is a smooth variety, it is also of interest of us to consider maps to Y which are almost étale but have some ramification. For this purpose, we introduce the following definition.

Definition 2.1.4. *A G-Galois cover is a finite, generically étale map $f : X \to Y$ of regular schemes together with an inclusion $\rho : G \hookrightarrow \mathrm{Aut}(X/Y)$ such that $f^{-1}(\mathcal{O}_Y)$ is equal to the sheaf of G-invariants of $\mathcal{O}_X$.*

If Y is a curve, a G-Galois cover of Y is ramified above finitely many points of Y.

Another type of useful invariant of a topological space is its singular cohomology; Galois cohomology provides a similar invariant for fields which classifies finite separable extensions of the base. Since étale maps include both covering maps of complex varieties and separable extensions of fields, we use them as the basis for another cohomology theory. Open immersions are also étale, so this motivates us to first extend the notion of a collection of open maps covering a space to étale maps.

Definition 2.1.5. *A collection of étale maps $\{f_i : U_i \to Y\}$ is an étale covering if $\bigcup_i f_i(U_i) = Y$.*

Definition 2.1.6. *The étale site on Y is the category of all étale maps $X \to Y$, together with the Grothendieck topology in which coverings are étale coverings.*

Definition 2.1.7. *An étale sheaf on Y is a contravariant functor from the category of étale maps to Y to the category of abelian groups that satisfies the sheaf conditions with respect to the étale site.*

Definition 2.1.8. *The ith étale cohomology group $H^i_{et}(Y, -)$ is the ith right derived functor of the functor of global sections of étale sheaves on Y.*

Étale cohomology coincides with Galois cohomology when $Y = \mathrm{Spec}\ k$, as noted in [Mil08] p. 7. And for Λ finite and Y a variety over $\mathbb{C}$, we also have $H^r(Y_{et}, \Lambda) \cong H^r_{sing}(Y(\mathbb{C}), \Lambda)$.

We note, however, that étale cohomology is usually defined for sheaves of *abelian* groups, and we want to consider covers of spaces with a nonabelian Galois group G. This can be done by considering the Čech cohomology set $\check{H}^1(U, G)$; for sheaves of abelian groups, the Čech cohomology groups agree with étale cohomology groups by Proposition 10.6 of [Mil08]. And most importantly, the first cohomology set still classifies principal homogeneous spaces, per Proposition 11.1 of [Mil08]:

Theorem 2.1.9. *For a scheme U and finite group G, there is a natural bijection from the set of isomorphism classes of principal homogeneous spaces for G over U to $\check{H}^1(U, G)$.*

2.2 Prime-to-p-covers

In this section, we discuss Galois covers of curves whose Galois groups are prime to p, the characteristic of the field.

We first recall the classification of Galois covers of complex curves.

Theorem 2.2.1. *Let X be a smooth projective curve over $\mathbb{C}$ of genus g, and let S be a nonempty, finite subset of points of X with $|S| = r$. Then a finite group G is the Galois group of a cover of X unramified outside S if and only if G can be generated by $2g + r - 1$ elements.*

One can see this by noting X is isomorphic to a quotient of a polygon and using Van Kampen's theorem to compute the topological fundamental group. And from the theory of base change for proper normal curves (Corollary 4.6.11 of [Sza]), this result actually holds over any algebraically closed field of characteristic 0.

Over characteristic p fields, there is a philosophy that the theory of Galois covers with Galois groups of order prime to p is the same as in characteristic 0. This is made precise by the following theorem of Grothendieck, as presented in Theorem 4.6.11 of [Sza], for which we denote by $\pi_1(U)^{(p')}$ the inverse limit of quotients of $\pi_1(G)$ having order prime to p.

Theorem 2.2.2. *Let k be an algebraically closed field of characteristic $p \geq 0$ and let Y be an integral proper normal curve of genus g over k. Let $U \subset Y$ be an open sub curve, and $r \geq 0$ the number of closed points in $Y \backslash U$. Then $\pi_1(U)^{(p')}$ is isomorphic to the profinite p'-completion of the group*

$$\Pi_{g,r} := \langle a_1, b_1, ..., a_g, b_g, \gamma_1, ..., \gamma_r | [a_1, b_1] \cdots [a_g, b_g]\gamma_1 \cdots \gamma_n = 1\rangle$$

This suggests that the richest behavior unique to characteristic p comes from p-group covers of curves, which we investigate in this thesis.

2.3 Artin–Schreier–Witt theory

We first focus on the simplest nontrivial p-group, $G = \mathbb{Z}/p\mathbb{Z}$; this is the topic of Artin–Schreier theory. Classically, Artin–Schreier theory has been used to describe $\mathbb{Z}/p\mathbb{Z}$-extensions of *fields* explicitly in terms of equations defining the extension over the ground field; we give this characterization in the following proposition:

Proposition 2.3.1. *Let k be a field of characteristic p.*

(i) Let L be a $\mathbb{Z}/p\mathbb{Z}$-Galois étale algebra over k. Then L is isomorphic to an algebra of the form $k[y]/(y^p - y - f)$ for some $f \in k$, and the Galois action of $i \in \mathbb{Z}/p\mathbb{Z}$ sends $y \mapsto y + i$.

(ii) Given $f \in k$, the algebra $L_f := k[y]/(y^p - y - f)$ is a $\mathbb{Z}/p\mathbb{Z}$-Galois étale algebra

over k, and two such algebras L_f and $L_{\tilde{f}}$ are isomorphic (as $\mathbb{Z}/p\mathbb{Z}$-Galois k-algebras) if and only if $f - \tilde{f} = g^p - g$ for some $g \in k$.

Proof. We denote by G_k the absolute Galois group of k, and consider the sequence of G_k modules

$$0 \to \mathbb{Z}/p\mathbb{Z} \to k^{\mathrm{sep}} \xrightarrow{\wp} k^{\mathrm{sep}} \to 0,$$

where the action of G_k on $\mathbb{Z}/p\mathbb{Z}$ is trivial, and $\wp$ is the Artin–Schreier map sending $h \mapsto h^p - h$. We see that $\wp$ is surjective onto k^{sep} since the polynomial $H(x) = x^p - x - 1$ has $H' = -1$, so H is separable and has a root in k^{sep}. And the kernel of $\wp$ is exactly $\mathbb{Z}/p\mathbb{Z}$, the p roots of $x^p - x = 0$, so in fact the sequence is exact. This gives rise to a long exact sequence in Galois cohomology:

$$\begin{aligned} 0 \to H^0(G_k, \mathbb{Z}/p\mathbb{Z}) \to H^0(G_k, k^{\mathrm{sep}}) \to H^0(G_k, k^{\mathrm{sep}}) \\ \xrightarrow{\delta} H^1(G_k, \mathbb{Z}/p\mathbb{Z}) \to H^1(G_k, k^{\mathrm{sep}}) \to \cdots \end{aligned}$$

but by the additive version of Hilbert's Theorem 90, $H^1(G_k, k^{\mathrm{sep}}) = 0$, so we can rewrite the above exact sequence as

$$0 \to \mathbb{Z}/p\mathbb{Z} \to k \xrightarrow{\wp} k \xrightarrow{\delta} H^1(G_k, \mathbb{Z}/p\mathbb{Z}) \to 0,$$

and the map δ sending $f \in k$ to the isomorphism class of the algebra $k[x]/(x^p - x - f)$ with Galois action in which $i \in \mathbb{Z}/p\mathbb{Z}$ acts as $x \mapsto x + i$. Since δ is surjective, statement (i) holds. And since the kernel of δ is elements of k of the form $g^p - g$ for $g \in k$, statement (ii) holds. □

Another commonly used characterization of extensions of characteristic p-fields comes from Artin–Schreier–Witt theory, which classifies extensions by *abelian p-*

groups. We give a proof of it as outlined in Exercises 49–51 of Chapter VI of [Lan].

Let $W_n(K)$ denote the ring of truncated Witt vectors over a field K of characteristic p, and $F : W_n(K) \to W_n(K)$ to be the map sending $(x_0, ..., x_{n-1}) \mapsto (x_0^p, ..., x_{n-1}^p)$.

Proposition 2.3.2. *Let k be a field of characteristic p and n an integer greater than 0. Let L be a $\mathbb{Z}/p^n\mathbb{Z}$-Galois étale algebra over k. Then $L_\xi \cong K[x_0, ..., x_{n-1}]/(\wp(x) = \xi)$ where the x_i are indeterminates, $\xi = (\xi_0, ..., \xi_{n-1})$ is a Witt vector in $W_n(k)$, and $(\wp(x) = \xi)$ represents the ideal coming from the entrywise equalities of the Witt vector equation*

$$(x_0^p, ..., x_{n-1}^p) - (x_0, ..., x_{n-1}) = (\xi_0, ..., \xi_{n-1}).$$

Conversely, every $\mathbb{Z}/p^n\mathbb{Z}$-Galois étale algebra over k is isomorphic to L_ξ for some $\xi \in W_n(k)$, and two such algebras L_ξ and $L_{\tilde{\xi}}$ are isomorphic as $\mathbb{Z}/p^n\mathbb{Z}$-Galois k-algebras if and only if $\xi - \tilde{\xi} = Fw - w$ for some Witt vector $w \in W_n(k)$.

Proof. We now denote by $\wp$ the map $W_n(K) \to W_n(K)$ sending $(x_0, ..., x_{n-1}) \mapsto (x_0^p, ..., x_{n-1}^p) - (x_0, ..., x_{n-1})$, where the minus is understood to be subtraction in the ring of Witt vectors.

We first prove by induction on n that the sequence

$$0 \to W_n(\mathbb{F}_p) \to W_n(k^{\text{sep}}) \xrightarrow{\wp} W_n(k^{\text{sep}}) \to 0$$

is exact.

The base case $n = 1$ is the Artin–Schreier case, proved in Theorem 2.3.1.

Now we assume the sequence is exact for $n - 1$.

We denote by π the map $W_n(K) \to W_{n-1}(K)$ which is projection onto the first $n-1$ coordinates. We denote by ι the map $K \to W_n(K)$ which sends $a \mapsto (0, 0, ..., 0, a)$.

These maps give us an exact sequence

$$0 \to K \xrightarrow{\iota} W_n(K) \xrightarrow{\pi} W_{n-1}(K) \to 0.$$

We now consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{\iota} & W_n(K) & \xrightarrow{\pi} & W_{n-1}(K) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \wp} & & \downarrow{\scriptstyle \wp} & & \downarrow{\scriptstyle \wp} & & \\ 0 & \longrightarrow & K & \xrightarrow{\iota} & W_n(K) & \xrightarrow{\pi} & W_{n-1}(K) & \longrightarrow & 0 \end{array}$$

which has exact rows. By the inductive hypothesis, the left and right vertical $\wp$ maps are surjective, with kernel $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^{n-1}\mathbb{Z}$ respectively. By the Five Lemma, the middle map $\wp : W_n(K) \to W_n(K)$ is surjective. To calculate the kernel, we note that from the Snake Lemma the sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \ker(\wp : W_n(K) \to W_n(K)) \to \mathbb{Z}/p^{n-1}/\mathbb{Z} \to 0$$

so $\ker(\wp : W_n(K) \to W_n(K))$ has order p^n. But also, the Frobenius F acts as the identity on $W_n(\mathbb{F}_p) \subset W_n(K)$, so $W_n(\mathbb{F}_p)$ is a subgroup of the kernel, but bedause $W_n(\mathbb{F}_p)$ also has order p^n, we must have $W_n(\mathbb{F}_p) = \ker(\wp : W_n(K) \to W_n(K))$.

Now since the sequence

$$0 \to W_n(\mathbb{F}_p) \to W_n(k^{\text{sep}}) \xrightarrow{\wp} W_n(k^{\text{sep}}) \to 0$$

is exact, we have a long exact sequence in Galois cohomology

$$0 \to H^0(G_k, W_n(\mathbb{F}_p)) \to H^0(G_k, W_n(k^{\text{sep}})) \to H^0(G_k, W_n(k^{\text{sep}}))$$
$$\xrightarrow{\delta} H^1(G_k, W_n(\mathbb{F}_p)) \to H^1(G_k, W_n(k^{\text{sep}})) \cdots$$

We also have that $H^1(G_k, W_n(k^{\text{sep}})) = 0$, by devissage, so in fact

$$W_n(k)/\wp(W_n(k)) \xrightarrow{\delta} H^1(G_k, W_n(\mathbb{F}_p))$$

is an isomorphism.

□

2.4 Theorem of Inaba

Given a characteristic p field k and a finite (possibly non-abelian) p-group G, Inaba (in [Ina61]) gave an explicit characterization of Galois field extensions of k with Galois group G.

The proof is similar to concrete proofs of Hilbert's Theorem 90 and the classification of Artin–Schreier extensions, as presented on p. 302 of [Lan].

We first establish some notation. For each integer $n > 1$, we define the algebraic group U_n from the functor of points perspective. For an $\mathbb{F}_p$-algebra R, we define $U_n(R)$ to be the group of upper triangular $n \times n$ matrices with coefficients in R, such that all the diagonal entries are 1, and the group action is matrix multiplication. We also denote by X the upper triangular matrix of indeterminates, where the (i,j) entry is the indeterminate x_{ij} for $j-i > 0$ and the (i,i) entry is 1. For a characteristic p ring R and a matrix $C \in U_n(R)$, we denote by $C^{(p)}$ the matrix obtained by raising each entry of C to the pth power (different from matrix multiplication of C with itself p times). We denote by L_M the R-algebra $R[X]/(X^{(p)} - MX)$, by which we mean the R-algebra generated by the indeterminate entries of X, modulo the relations coming from the matrix equation $X^{(p)} = MX$. This has a $U_n(\mathbb{F}_p)$-action given by $X \mapsto X \cdot g$ for $g \in U_n(\mathbb{F}_p)$ (with indeterminates mapping to the corresponding entry of the matrix $X \cdot g$). We say that L_M is the $U_n(\mathbb{F}_p)$-Galois étale algebra arising from the matrix M. Lastly, we say that two matrices $M, M' \in U_n(R)$ are p-equivalent over R if there exists $C \in U_n(R)$ such that $M = C^{(p)} M' C^{-1}$.

We now reproduce Inaba's argument here.

Proposition 2.4.1. *Let k be a field of characteristic p. Then, to every Galois field extension L/k whose Galois group G has order a power of p, and embedding $\Lambda \colon G \hookrightarrow U_n(\mathbb{F}_p)$ there corresponds a unipotent matrix $M \in U_n(k)$, unique up to p-equivalence, such that L is generated as a k-algebra by the entries of a matrix $A \in U_n(k^{\text{sep}})$ satisfying the matrix equation*

$$A^{(p)} = MA.$$

Conversely, for every unipotent matrix $M \in U_n(k)$, there exists a unique Galois extension L/k and embedding Λ of the Galois group of L/k in $U_n(\mathbb{F}_p)$ such that L is generated as a k-algebra by the entries of one solution $A \in U_n(k^{\text{sep}})$ to the matrix equation

$$A^{(p)} = AX,$$

and the embedding $\Lambda : \mathrm{Gal}(L/K) \hookrightarrow U_n(\mathbb{F}_p)$ is determined uniquely by the p-equivalence class of M.

Proof. First, suppose we have a Galois field extension L/k and an embedding Λ :

$G \hookrightarrow U_n(\mathbb{F}_p)$ of the Galois group. Let γ be an element of L such that $\mathrm{Tr}_{L/k}(\gamma) \neq 0$, and let

$$A := \frac{1}{\mathrm{Tr}_{L/k}(\gamma)} \sum_{\sigma \in G} \lambda(\sigma^{-1}) \cdot \sigma(\gamma)$$

Then for all $\tau \in G$,

$$\tau A = A\Lambda(\tau)$$

This implies that if L' is the extension of k given by adjoining the entries of A, and σ is any automorphism of L over L', then in fact $\sigma(A) = A$ so σ acts trivially on L' and $L = L'$.

We also have that

$$\begin{aligned}
\sigma(A^{(p)}A^{-1}) &= \sigma(A^{(p)})(\sigma(A))^{-1} \\
&= A^{(p)}\Lambda(\sigma)^{(p)}(A\Lambda(\sigma))^{-1} \\
&= A^{(p)}\Lambda(\sigma)(\Lambda(\sigma))^{-1}A^{-1} \\
&= A^{(p)}A^{-1}
\end{aligned}$$

so $M := A^{(p)}A^{-1} \in U_n(k)$ and A satisfies the matrix equation

$$X^{(p)} = MX.$$

Conversely, for some $M \in U_n(k)$ consider the matrix equation

$$X^{(p)} = MX.$$

We first note that this has at least one solution $A \in U_n(k^{\mathrm{sep}})$; this can be obtained by iteratively adjoining roots of Artin–Schreier polynomials. So let A be such a matrix and let L be the extension of k generated by adjunction of all entries a_{ij} of A to k. We want to show that L is a Galois extension of k and that its Galois group G is isomorphic to a subgroup of $U_n(\mathbb{F}_p)$. Firstly, since Artin–Schreier polynomials are separable, L/k is a separable extension. Next, we note that for $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$,

$$\sigma(A) = \sigma(M^{-1}A^{(p)}) = M^{-1}(\sigma A)^{(p)}$$

so $\sigma(A)$ also satisfies the equation $X^{(p)} = MX$. But if $\tilde{A}$ is any matrix in $U_n(k^{\mathrm{sep}})$, then $(\tilde{A}A^{-1})^{(p)} = Id$, so $\tilde{A}A^{-1} \in U_n(\mathbb{F}_p)$. But then the entries of $\sigma(A)$ are also in L, so L/k is Galois, and from this we also see that the Galois group of L/k is a subgroup of $U_n(\mathbb{F}_p)$. □

Chapter 3

Main Results

3.1 Preliminary Lemmas

We begin with a useful lemma that allows us to work with p-groups by viewing them as subgroups of a nice matrix group.

Lemma 3.1.1. *If G is a finite p-group, then there exists an $n \in \mathbb{Z}_{>0}$ and an injective homomorphism $\Lambda : G \hookrightarrow U_n(\mathbb{F}_p)$.*

Proof. Let $\varphi : G \to GL_n(\mathbb{F}_p)$ be the regular representation, so $n = |G|$. If we consider an eigenvalue λ of the matrix $\varphi(g)$ for some $g \in G$, we see that since $g^{|G|} = 1$, we must have $\lambda^{|G|} = 1$. But since $|G|$ is a power of p, we have $\lambda = 1$, so $\varphi(g)$ is unipotent. Then by Proposition 2.4.12 of [Spr], after a change of basis, G embeds into $U_n(\mathbb{F}_p)$. $\square$

Next, we prove a lemma that allows us to work with unipotent matrices inductively, one diagonal at a time.

Lemma 3.1.2. *Let R be a ring of characteristic p. Suppose that $M = (m_{ij}), M' = (m'_{ij}) \in U_n(R)$ are p-equivalent, so $M = B^{(p)}M'B^{-1}$ for some $B = (b_{ij}) \in U_n(R)$. Then for each pair i, j, there exists an element C of the $\mathbb{Z}$-subalgebra of R generated by $\{m_{\tilde{i}\tilde{j}}, b_{\tilde{i}\tilde{j}}, m'_{\tilde{i}\tilde{j}} | \tilde{j}-\tilde{i} < j-i\}$ such that $m_{ij} = \wp(b_{ij})+m'_{ij}+C$. That is, $m_{ij} = \wp(b_{ij})+m'_{ij}$ modulo the elements on the lower diagonals.*

Proof. Consider two matrices $W = (w_{ij}), Z = (z_{ij}) \in U_n(R)$. The (i, j) entry of WZ, which we call a_{ij}, is $\sum_k w_{ik}z_{kj}$, but since these matrices are in U_n we have

$$a_{ij} = 1 \cdot z_{ij} + w_{ij} \cdot 1 + \sum_{i<k<j} w_{ik}z_{kj},$$

and in this range, $i - k < i - j$ and $k - j < i - j$. Applying this to both sides of the equation $MB = B^{(p)}M'$ yields the result. □

3.2 Non-abelian p-group Covers of Affine Schemes

Theorem 3.2.1. *Let G be a finite p-group, and fix an injective homomorphism $\Lambda : G \to U_n(\mathbb{F}_p)$ for some suitable n. Let R be a ring of characteristic p such that Spec R is connected, and let L/R be a Galois étale algebra with Galois group G.*

(i) The R-algebra L is generated by elements $a_{ij} \in L$ for $1 \leq i < j \leq n$ such that the unipotent matrix $A := (a_{ij})$ satisfies $A^{(p)} = MA$ for some $M \in U_n(R)$. Also, for $\sigma \in G$, ${}^{\sigma}A = A\Lambda(\sigma)$, where σ acts entrywise on A.

(ii) Given two G-Galois étale algebras L and L', if we choose (A, M) for L and (A', M') for L', then L and L' are isomorphic as R-algebras equipped with an action of G if and only if $M = C^{(p)}M'C^{-1}$ for some $C \in U_n(R)$.

We now provide generalizations of Artin–Schreier theory to non-abelian groups. We begin with a lemma about $U_n(\mathbb{F}_p)$-extensions.

Lemma 3.2.2. *Let R be a ring of characteristic p such that Spec R is connected. Then the finite Galois étale algebras over Spec R with Galois group $U_n(\mathbb{F}_p)$ are the algebras $L_M := R[X]/(X^{(p)} = MX)$ where M ranges over all matrices in $U_n(R)$, and the Galois action is given by matrix multiplication $X \mapsto X \cdot g$. Two such Galois algebras defined by matrices M and M' are isomorphic as R-algebras with $U_n(\mathbb{F}_p)$-action if and only if $M = C^{(p)}M'C^{-1}$ for some $C \in U_n(R)$.*

Proof. We identify the abstract group $U_n(\mathbb{F}_p)$ with the associated constant group scheme over the ground field $\mathbb{F}_p$. We have a sequence

$$U_n(\mathbb{F}_p) \to U_n \xrightarrow{\mathcal{L}} U_n$$

where $\mathcal{L}$ is the morphism $B \mapsto B^{(p)}B^{-1}$ (which is not a group homomorphism). By Lang's theorem [Lan56], $\mathcal{L}$ is surjective and identifies $U_n/U_n(\mathbb{F}_p)$ with U_n. Since Spec R is connected, $H^0(\text{Spec } R, U_n(\mathbb{F}_p)) = U_n(\mathbb{F}_p)$, so by Proposition 36 of [Ser], we have an exact sequence of pointed sets

$$1 \to U_n(\mathbb{F}_p) \to U_n(R) \xrightarrow{\mathcal{L}} U_n(R) \xrightarrow{\delta} H^1(\text{Spec } R, U_n(\mathbb{F}_p)) \to H^1(\text{Spec } R, U_n)$$

where δ sends a matrix $M \in U_n(R)$ to the class of the étale algebra L_M. The action of $U_n(R)$ on $U_n(R)$ via $\mathcal{L}$ is given as follows. Since $\mathcal{L}$ is surjective, there is some étale R-algebra S and some $N \in U_n(S)$ such that $M = N^{(p)}N^{-1}$. The action of $C \in U_n(R)$ sends M to $\mathcal{L}(CN) = C^{(p)}N^{(p)}N^{-1}C^{-1} = C^{(p)}MC^{-1}$.

Next, since $H^1(X, \mathcal{O}_X) = 0$ for affine schemes and U_n has a composition series whose factors are $\mathbb{G}_a$, we see by induction that $H^1(\text{Spec } R, U_n) = 1$. So the map $U_n(R) \to H^1(\text{Spec } R, U_n(\mathbb{F}_p))$ is surjective and expresses $H^1(\text{Spec } R, U_n(\mathbb{F}_p))$ as quotient of $U_n(R)$ by the left action of $U_n(R)$ via the map $\mathcal{L}$. So every $U_n(\mathbb{F}_p)$ étale algebra is isomorphic to some L_M with the condition for equivalence as stated in the lemma. □

Now we look at a general p-group and fix an embedding $\Lambda : G \to U_n(\mathbb{F}_p)$.

Proof of Theorem 3.2.1. First, the inclusion $\Lambda : G \to U_n(\mathbb{F}_p)$ induces a map

$$H^1(\text{Spec } R, G) \to H^1(\text{Spec } R, U_n(\mathbb{F}_p))$$

sending the class of L to the class of the R-algebra

$$\tilde{L} := \prod_{G\backslash U_n(\mathbb{F}_p)} L$$

with the following left $U_n(\mathbb{F}_p)$-action. Let $u_1, ..., u_r$ be coset representatives for $G\backslash U_n(\mathbb{F}_p)$, with $u_1 = e$ being the identity element. Then we can write any element of $\prod_{G\backslash U_n(\mathbb{F}_p)} L$ as $(\ell_i)_{i=1}^r$ with $\ell_i \in L$. For each $u \in U_n(\mathbb{F}_p)$, there exist $g_i \in G$ such that $u_i u = g_i u_{j(i)}$, where $j(i)$ is the index of the coset of $u_i u$. Then $u \cdot (\ell_i)_i = ({}^{g_{j^{-1}(i)}}\ell_{j^{-1}(i)})_i$.

Let $\pi : \tilde{L} \to L$ be projection onto the first component. For an element $h \in G$, we see that $\pi\left({}^h(\ell_i)_{i=1}^r\right) = {}^h\ell_1$, so π respects the action of G. But by Lemma 3.2.2, $\tilde{L} \cong R[X]/(X^{(p)} = MX)$ as G-Galois étale R-algebras, so the surjection π expresses L as $R[A]$, where A is the matrix with ij-coordinate equal to $\pi(x_{ij})$. And since π is compatible with the action of G, the original G-action on L agrees with the action coming from matrix multiplication by $\Lambda(G)$.

Lastly, the map $H^0(\text{Spec } R, U_n(\mathbb{F}_p)) \to H^0(\text{Spec } R, U_n(\mathbb{F}_p)/G)$ is surjective, since it is the map $U_n(\mathbb{F}_p) \to U_n(\mathbb{F}_p)/G$, so by the exact sequence in Proposition 36 of [Ser], the map $U_n(\mathbb{F}_p)/G \to H^1(\text{Spec } R, G)$ is zero, which implies that the map $H^1(\text{Spec } R, G) \to H^1(\text{Spec } R, U_n(\mathbb{F}_p))$ is injective. This tells us that the condition for equivalence of G-Galois étale algebras is the same as in Lemma 3.3.2.

3.3 Existence of Local-to-Global Extensions

Throughout the rest of this chapter, let Y be a smooth proper curve over k, let $y \in Y(k)$, let $Y' := Y - \{y\}$, and let t be a uniformizer at y.

Theorem 3.3.1. *Let G be a nontrivial finite p-group. Then the following are equivalent:*

(i) The equality $k((t)) = \wp(k((t))) + \mathcal{O}(Y')$ holds.

(ii) The map $\Psi_{Y,y,U_n(\mathbb{F}_p)}$ is surjective for all $n > 1$.

(iii) The map $\Psi_{Y,y,G}$ is surjective.

Proof. We first show that (i) implies (ii). Suppose $k((t)) = \mathcal{O}(Y') + \wp(k((t)))$. Let L be a $U_n(\mathbb{F}_p)$-Galois étale $k((t))$-algebra, so by Lemma 3.2.2, $L \cong L_M$ for some $M \in U_n(k((t)))$. We want to find a matrix $M' \in U_n(\mathcal{O}(Y'))$ which is p-equivalent over $k((t))$ to M. Suppose that not all entries of M are in $\mathcal{O}(Y')$. Let m_{ij} be such an entry on the lowest diagonal not having all entries in $\mathcal{O}(Y')$. By the assumption in (i), there exists $b \in k((t))$ such that $m_{ij} + \wp(b) \in \mathcal{O}(Y')$. Let B be the matrix in $U_n(k((t)))$ which has b in the (i, j) entry and is equal to the identity matrix elsewhere. Then the (i, j) entry of $B^{(p)}MB^{-1}$ is $m_{ij} + \wp(b) + C$ with $C \in \mathcal{O}(Y')$. And by Lemma 3.1.2, the (i, j) entry and entries of all lower diagonals of $B^{(p)}MB^{-1}$ are in $\mathcal{O}(Y')$, so we can iterate this process until we have a matrix M' in $U_n(\mathcal{O}(Y'))$.

Next, we show that (ii) implies (iii), so suppose $\Psi_{Y,y,U_n(\mathbb{F}_p)}$ is surjective. Since $U_2(\mathbb{F}_p) \cong \mathbb{Z}/p\mathbb{Z}$, we can also assume that $\Psi_{Y,y,\mathbb{Z}/p\mathbb{Z}}$ We proceed by induction on the order of G. Since G is a p-group, G has a central subgroup H which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. The morphism Spec $k((t)) \to Y'$ induces the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(Y', \mathbb{Z}/p\mathbb{Z}) & \xrightarrow{\iota_Y} & H^1(Y', G) & \xrightarrow{\varphi_Y} & H^1(Y', G/H) & \longrightarrow & 0 \\ & & \downarrow \Psi_{Y,y,\mathbb{Z}/p\mathbb{Z}} & & \downarrow \Psi_{Y,y,G} & & \downarrow \Psi_{Y,y,G/H} & & \\ 0 & \longrightarrow & H^1(k((t)), \mathbb{Z}/p\mathbb{Z}) & \xrightarrow{\iota_{k((t))}} & H^1(k((t)), G) & \xrightarrow{\varphi_{k((t))}} & H^1(k((t)), G/H) & \longrightarrow & 0 \end{array}$$

By Proposition 42 of [Ser] and Lemma 1.4.3 of [Kat86] (which states that both $H^2(k((t)), \mathbb{Z}/p\mathbb{Z})$ and $H^2(Y', \mathbb{Z}/p\mathbb{Z})$ are zero), this diagram has exact rows, and two elements of $H^1(Y', G)$ have the same image in $H^1(Y', G/H)$ if and only if they are in the same $H^1(Y', \mathbb{Z}/p\mathbb{Z})$-orbit (and similarly for $H^1(k((t)), G)$). And by the inductive hypothesis, $\Psi_{Y,y,\mathbb{Z}/p\mathbb{Z}}$ and $\Psi_{Y,y,G/H}$ are surjective. The surjectivity of $\Psi_{Y,y,G}$ is proved via the following diagram chase.

Let $\tilde{\beta}$ be an element of $H^1(k((t)), G)$, and let $\tilde{\gamma} := \varphi_{k((t))}(\tilde{\beta})$. By the inductive hypothesis, there exists an element $\gamma \in H^1(Y', G/H)$ such that $\Psi_{Y,y,G/H}(\gamma) = \tilde{\gamma}$. Let β be an element of $H^1(Y', G)$ mapping to γ. Then by Proposition 42 of [Ser], there exists an element $\tilde{\alpha} \in H^1(k((t)), \mathbb{Z}/p\mathbb{Z})$ such that $\iota_{k((t))}(\tilde{\alpha}) \cdot \Psi_{Y,y,G}(\beta)$ equals $\tilde{\beta}$. Now let α be an element of $H^1(Y', \mathbb{Z}/p\mathbb{Z})$ mapping to $\tilde{\alpha}$. We see that $i_Y(\alpha) \cdot \beta$ maps to $\tilde{\beta}$ under $\Psi_{Y,y,G}$, so $\Psi_{Y,y,G}$ is surjective.

Next, we show that (iii) implies (i), so suppose $\Psi_{Y,y,G}$ is surjective, and again let H be a nontrivial central subgroup of G isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Again consider the aforementioned diagram. Since $\varphi_{k((t))} \circ \Psi_{Y,y,G}$ is surjective, $\Psi_{Y,y,G/H}$ is surjective. Iterating this process shows that $\Psi_{Y,y,\mathbb{Z}/p\mathbb{Z}}$ is surjective. Let $f \in k((t))$, so $k((t))[x]/(x^p - x - f)$ is a $\mathbb{Z}/p\mathbb{Z}$-Galois étale algebra over $k((t))$. Since $\Psi_{Y,y,\mathbb{Z}/p\mathbb{Z}}$ is surjective, Theorem 3.2.1 tells us that f is p-equivalent to an element g of $\mathcal{O}(Y')$, so $f = \wp(b) + g$ for some $b \in k((t))$. Thus the equality in (i) holds. $\square$

3.4 Uniqueness of Local-to-Global Extensions

Theorem 3.4.1. *Let G be a nontrivial finite p-group. Then the following are equivalent:*

(i) The equality $\wp(k((t))) \cap \mathcal{O}(Y') = \wp(\mathcal{O}(Y'))$ holds.

(ii) The map $\Psi_{Y,y,G}$ is injective.

(iii) The map $\Psi_{Y,y,\mathbb{Z}/p\mathbb{Z}}$ is injective.

Proof. First, we show that (i) implies (ii), so suppose that $\wp(k((t))) \cap \mathcal{O}(Y') = \wp(\mathcal{O}(Y'))$. Let Spec L and Spec L' be two étale G-covers of Y' that become isomorphic over $k((t))$. By Theorem 3.2.1, $L = L_M$ and $L' = L_{M'}$ for some M and $M' \in U_n(\mathcal{O}(Y'))$, and since they are isomorphic over $k((t))$, we have that $M = B^{(p)}M'B^{-1}$ for some $B \in U_n(k((t)))$. Suppose for contradiction that there exists an entry b_{ij} of B not in $\mathcal{O}(Y')$, chosen such that all entries on lower diagonals are in $\mathcal{O}(Y')$. Then by Lemma 3.1.2, $\wp(b_{ij}) = m_{ij} - m'_{ij} + C$ where C is a polynomial in the entries of lower diagonals of B, M, and M'. Then $\wp(b_{ij}) \in \mathcal{O}(Y')$, and by (i), $b_{ij} \in \mathcal{O}(Y')$, a contradiction.

Next we show that (ii) implies (iii), so assume that $\psi_{Y,y,G}$ is injective. Since G is a nontrivial p-group, it has a nontrivial subgroup H which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, so by Proposition 42 of [Ser], we have a commutative square

$$\begin{array}{ccc} H^1(Y', \mathbb{Z}/p\mathbb{Z}) & \hookrightarrow & H^1(Y', G) \\ \downarrow{\scriptstyle \Psi_{Y,y,\mathbb{Z}/p\mathbb{Z}}} & & \downarrow{\scriptstyle \Psi_{Y,y,G}} \\ H^1(k((t)), \mathbb{Z}/p\mathbb{Z}) & \hookrightarrow & H^1(k((t)), G) \end{array}$$

and since the top and right arrows are injective, we know that $\Psi_{Y,y,\mathbb{Z}/p\mathbb{Z}}$ is injective.

Next we show that (iii) implies (i), so assume that $\psi_{Y,y,\mathbb{Z}/p\mathbb{Z}}$ is injective. Let b be an element of $k((t))$ such that $\wp(b) \in \mathcal{O}(Y')$. Then, by the Lemma 3.2.2 for $n = 2$, we have that $k((t))[x]/(x^p - x)$ is isomorphic to $k((t))[x]/(x^p - x - \wp(b))$ as $\mathbb{Z}/p\mathbb{Z}$-Galois $k((t))$-algebras. But since $\Psi_{Y,y,\mathbb{Z}/p\mathbb{Z}}$ is injective, $\mathcal{O}(Y')[x]/(x^p - x) \cong \mathcal{O}(Y')[x]/(x^p - x - \wp(b))$, so by Lemma 3.2.2, $0 = \wp(c) + \wp(b)$ for some $c \in \mathcal{O}(Y')$, which means that $b - c \in \mathbb{F}_p$, so $b \in \mathcal{O}(Y')$. So $\wp(k((t))) \cap \mathcal{O}(Y') \subseteq \wp(\mathcal{O}(Y'))$. The direction $\wp(k((t))) \cap \mathcal{O}(Y') \supseteq \wp(\mathcal{O}(Y'))$ is clear. $\square$

3.5 Characterization of an Equivalence of Categories

We now give a concise reformulation of the criterion for when $\Psi_{Y,y,G}$ is a bijection. We denote by F the Frobenius morphism $\mathcal{O}_Y \to \mathcal{O}_Y$ sending $f \mapsto f^p$. This induces a homomorphism $F^*\colon H^1(Y, \mathcal{O}_Y) \to H^1(Y, \mathcal{O}_Y)$; we also let $\wp^* := F^* - Id$ be the endomorphism of $H^1(Y, \mathcal{O}_Y)$ induced by Artin–Schreier. Then our reformulation is as follows.

Let G be a finite nontrivial p-group.

Theorem 3.5.1.

(i) The map $\Psi_{Y,y,G}$ is a surjection if and only if $\wp^*\colon H^1(Y, \mathcal{O}_Y) \to H^1(Y, \mathcal{O}_Y)$ is a surjection.

(ii) *The map* $\Psi_{Y,y,G}$ *is a injection if and only if* $\wp^*\colon H^1(Y,\mathcal{O}_Y)\to H^1(Y,\mathcal{O}_Y)$ *is a injection.*

(iii) *The map* $\Psi_{Y,y,G}$ *is a bijection if and only if* $\wp^*\colon H^1(Y,\mathcal{O}_Y)\to H^1(Y,\mathcal{O}_Y)$ *is a bijection.*

Proof. Let $\mathrm{skysc}_y\left(\frac{k((t))}{k[[t]]}\right)$ denote the skyscraper sheaf at y, with value group $k((t))/k[[t]]$, where the group structure is given by the additive structure on $k((t))$. The natural open immersion $i\colon Y'\hookrightarrow Y$ gives the following exact sequence of sheaves on Y:

$$0\to\mathcal{O}_Y\to i_*\mathcal{O}_{Y'}\to\mathrm{skysc}_y\left(\frac{k((t))}{k[[t]]}\right)\to 0.$$

We see that $H^1(Y,i_*\mathcal{O}_{Y'})=H^1(Y',\mathcal{O}_{Y'})=0$ since Y' is affine, so the induced long exact sequence in cohomology gives us an isomorphism

$$\frac{H^0\left(Y,\mathrm{skysc}_y\left(\frac{k((t))}{k[[t]]}\right)\right)}{\mathrm{im}(H^0(Y,i_*\mathcal{O}_{Y'}))}=\frac{k((t))}{\mathcal{O}(Y')+k[[t]]}\xrightarrow{\sim}H^1(Y,\mathcal{O}_Y).$$

We also see that the p-th power endomorphism of $\frac{k((t))}{\mathcal{O}(Y')+k[[t]]}$ sending $\bar f\mapsto\bar f^p$ for $f\in k((t))$ corresponds to the Frobenius endomorphism F^* of $H^1(Y,\mathcal{O}_Y)$.

We first prove part (i). Now we will show that if $\wp^*$ is a surjection, then $\Psi_{Y,y,G}$ is a surjection, so assume $\wp^*$ is a surjection. Since $\wp^*$ is surjective, for every $f\in k((t))$ there exist $g\in k((t)),h\in\mathcal{O}(Y'),l\in k[[t]]$ such that $f=g^p-g+h+l$. Let a_0 be the constant term of l; by setting $h':=h+a_0$ and $l':=l-a_0$ we can assume l has no constant term. So $l=\sum_{i=1}^{\infty}a_it^i$. We define a power series $\tilde l:=\sum_{i=1}^{\infty}b_it^i$ where $b_i=-a_i$ for i not divisible by p and $b_{np}=b_n^p-a_{np}$. So $f=\wp(g+\tilde l)+h$, and since $\wp(\tilde l)=l$, we see that $f\in\wp(k((t))+\mathcal{O}(Y')$. This is condition (i) of Theorem 3.3.1, so $\Psi_{Y,y,G}$ is surjective.

Conversely, suppose $\Psi_{Y,y,G}$ is a surjection. First, let $\bar{f} \in k((t))/(k[[t]] + \mathcal{O}(Y'))$, with $\bar{f}$ represented by $f \in k((t))$. Since $\Psi_{Y,y,G}$ is surjective, condition (i) of Theorem 3.3.1 tells us that $f = g^p - g + h$ for some $g \in k((t))$ and $h \in \mathcal{O}(Y')$, so $\bar{f}$ is the image of $\bar{g}$ under the endomorphism of $k((t))/(k[[t]] + \mathcal{O}(Y'))$ corresponding to $\wp^*$. Therefore, $\wp^*$ is surjective, and we have proved part (i) of the theorem.

We now prove part (ii) of the theorem. Suppose that $\wp^*$ is injective; we will show that this implies $\Psi_{Y,y,G}$ is injective. Consider $f \in k((t))$ such that $\wp(f) \in \mathcal{O}(Y')$. Since $\wp^*$ is injective, $f \in k[[t]] + \mathcal{O}(Y')$, so there exist $g \in \mathcal{O}(Y')$ and $l \in k[[t]]$ such that $f = g + l$. Again, we can assume that l has no constant term, so $l \in tk[[t]]$. But then $\wp(g) + \wp(l) \in \mathcal{O}(Y')$, which implies $\wp(l) \in \mathcal{O}(Y')$, and so $\wp(l) \in \mathcal{O}(Y') \cap tk[[t]] = \{0\}$ since nonzero elements of $\mathcal{O}(Y')$ have nonpositive valuation at y. This shows that $\wp(k((t))) \cap \mathcal{O}(Y') = \wp(\mathcal{O}(Y'))$, which is condition (i) of Theorem 3.4.1, so $\Psi_{Y,y,G}$ is injective.

Next, assume $\Psi_{Y,y,G}$ is injective. Now consider $f \in k((t))$ such that $\wp(f) = g + l$ for some $g \in \mathcal{O}(Y'), l \in tk[[t]]$. We can write $l = \wp(\tilde{l})$ for $\tilde{l}$ as above, so $\wp(f - \tilde{l}) \in \mathcal{O}(Y')$, which implies $f - \tilde{l} \in \mathcal{O}(Y')$ by Theorem 3.4.1 (ii) $\Rightarrow$ (i). Then $\bar{f} = \bar{0}$ in $k((t))/(k[[t]] + \mathcal{O}(Y'))$, so $\wp^*$ is injective, proving part (ii) of the theorem.

Lastly, part (iii) follows from parts (i) and (ii). $\square$

Chapter 4

Examples

4.1 The Affine Line

It is a theorem of Katz and Gabber ([Kat86] Proposition 1.4.2) that the functor $\psi_{\mathbb{P}^1_k,\infty}$ is an equivalence of categories for any characteristic p ground field k. We can recover this result from Corollary 3.5.1 of this thesis, since the map $\wp : H^1(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1}) \to H^1(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1})$ is an isomorphism because $H^1(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1}) = 0$.

4.2 Elliptic Curves over $\mathbb{F}_p$

In this section, we apply Theorem 3.5.1 to study $\Psi_{E,O}$ for an elliptic curve E over $\mathbb{F}_p$ with O denoting the point at infinity. The operator F^* on $H^1(E, \mathcal{O}_E)$ acts as multiplication by some $a \in \mathbb{F}_p$, and in fact $\#E(\mathbb{F}_p) \equiv 1 - a \mod p$. We say that E is **anomalous** if $a \equiv 1 \mod p$.

Theorem 4.2.1. *For an elliptic curve E over $\mathbb{F}_p$, the following are equivalent:*

(a) E is not anomalous.

(b) The map $\Psi_{E,O,G}$ is injective for all p-groups G.

(c) The map $\Psi_{E,O,G}$ is surjective for all p-groups G.

Proof. First, we note that since $H^1(E, \mathcal{O}_E)$ is finite, the endomorphism $\wp^*$ on $H^1(E, \mathcal{O}_E)$ is surjective if and only if it is injective. Since F^* acts as multiplication by a, $\wp^*$ acts as multiplication by $a-1$. Then $\wp^*$ is surjective if and only if $a \neq 1$, and $\wp^*$ injective if and only if $a \neq 1$. Applying (i) and (ii) of Theorem 3.5.1 gives the result. □

As indicated in [Sie35], the number of anomalous curves over $\mathbb{F}_p$ is on the order of $p^{1/2+o(1)}$, as opposed to the total number of elliptic curves which is on the order of p, and so Theorem 4.2.1 provides us with a broad class of curves whose p-group Galois covers correspond nicely to p-group $k((t))$ extensions.

4.3 Elliptic Curves over $\mathbb{F}_q$

Let E be an elliptic curve over $\mathbb{F}_q$, where $q = p^n$. Then $H^1(E, \mathcal{O}_E)$ is a 1-dimensional vector space over $\mathbb{F}_q$; we let b be a generator and write $H^1(E, \mathcal{O}_E) = \mathbb{F}_q \cdot b$. By Theorem 3.5.1 and the remarks in Chapter 1, we know that $\psi_{E,O}$ gives an equivalence of categories if and only if $\wp^*$ is a bijection. Since $H^1(E, \mathcal{O}_E)$ is finite, we know $\wp^* : H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)$ is bijective if and only if it is injective, which is true if and only if $F^* : H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)$ has no nonzero fixed points.

Now let $a \in \mathbb{F}_q$ be such that $F^*b = ab$. Then F^* has a nonzero fixed point if and only if there exists $\lambda \in \mathbb{F}_q$ such that $(\lambda^p a)b = \lambda b$, which holds if and only if $a \in (\mathbb{F}_q^\times)^{p-1}$. But since $(\mathbb{F}_q^\times)^{p-1}$ is cyclic of order $(q-1)/(p-1) = 1+p+\ldots+p^{n-1}$, this is equivalent to saying $N_{\mathbb{F}_q/\mathbb{F}_p}(a) = 1$. By Theorem I of [Man61], this is equivalent to a being congruent to $1 \mod p$, which is equivalent to $p \mid \#E(\mathbb{F}_q)$. So for a nontrivial p-group G, $\Psi_{E,O,G}$ is a bijection if and only if p does not divide $\#E(\mathbb{F}_q)$.

4.4 Higher Genus Curves over $\mathbb{F}_p$

Theorem 4.4.1. *Let Y be a curve over $\mathbb{F}_p$ of genus g. Let A be its Hasse–Witt matrix and let π be the characteristic polynomial of the Frobenius morphism on the Jacobian $J(Y)$. Then the following are equivalent:*

(a) $\Psi_{Y,y}$ *is an equivalence of categories.*

(b) $\wp^*$ *on* $H^1(Y, \mathcal{O}_Y)$ *is a bijection.*

(c) $\det(A - I) \neq 0$ *where I is the $g \times g$ identity matrix.*

(d) $\pi(1) \not\equiv 0 \pmod{p}$

(e) $\#J(\mathbb{F}_p) \not\equiv 0 \pmod{p}$

Proof. By Theorem I of [Man61],

$$\pi(\lambda) \equiv (-1)^g \lambda^g \det(A - \lambda I) \mod p.$$

By Theorem 3.5.1, $\psi_{Y,y}$ gives an equivalence of categories if and only if p does not divide $\#J(\mathbb{F}_p)$. But looking at the characteristic polynomial, we see that this is equivalent to $\det(A - I) = 0$. □

For many curves, like hyperelliptic curves, the Hasse–Witt matrix can be computed with fast algorithms (as demonstrated in [HS14]), so one can check in practice if $\psi_{Y,y}$ is an equivalence of categories.

Bibliography

[BCPS17] F.M. Bleher, T. Chinburg, B. Poonen, and P. Symonds, *Automorphisms of Harbater–Katz–Gabber curves*, Mathematische Annalen **368** (2017), 811–836. ↑1

[Har80] D. Harbater, *Moduli of p-covers of curves*, Communications in Algebra **8** (1980), no. 12, 1095–1122. ↑1, 1, 1

[HOPS] D. Harbater, A. Obus, R. Pries, and K. Stevenson, *Abhyankar's conjectures in Galois theory: Current status and future directions.* arXiv:1408.0859 [math.AG]. ↑1, 1

[HS14] D. Harvey and A. V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time*, LMS Journal of Computation and Mathematics **17** (2014), 257–273. ↑4.4

[Ina61] E. Inaba, *On matrix equations for Galois extensions of fields with characteristic p*, Natural Science Report, Ochanomizu University **12** (1961), no. 2, 26–36. ↑1, 2.4

[Kat86] N. Katz, *Local-to-global extensions of representations of fundamental groups*, Annales de l'institut Fourier **36** (1986), no. 4, 69–106. ↑1, 3.3, 4.1

[Lan56] S. Lang, *Algebraic groups over finite fields*, American Journal of Mathematics **78** (1956), no. 3, 555–563. ↑3.2

[Lan] ———, *Algebra*, Graduate Texts in Mathematics, Springer-Verlag New York. ↑2.3, 2.4

[Man61] Y. Manin, *The Hasse–Witt matrix of an algebraic curve*, Izv. Akad. Nauk SSSR Ser. Mat. **25** (1961). ↑4.3, 4.4

[Mil08] J. S. Milne, *Lectures on Étale cohomology (v2.21)*, 2008. ↑1, 2.1, 2.1.3, 2.1

[PS11] R. Pries and K. Stevenson, *A survey of Galois theory of curves in characteristic p*, Win—women in numbers: Research directions in number theory, 2011, pp. 169–192. ↑2.1.2

[Ser] J. P. Serre, *Cohomologie Galoisienne: Progrès et problèmes*, Lecture Notes in Mathematics, Springer-Verlag Berlin Heidelberg. ↑3.2, 3.3, 3.4

[Sie35] C. Siegel, *Uber die Klassenzahl quadratischer Zahlkörper*, Acta Arith. **1** (1935). ↑4.2

[Spr] T.A. Springer, *Linear algebraic groups*, Modern Birkhaüser Classics, Birkhaüser Basel. ↑3.1

[Sza] T. Szamuely, *Galois groups and fundamental groups*, Cambridge studies in advanced mathematics, Cambridge. ↑2.2