ARITHMETIC AND GEOMETRY OF THE OPEN P-ADIC DISC

Scott Corry

A Dissertation

in

Mathematics

Presented to the Faculties of the University of Pennsylvania in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

2007

Florian Pop
Supervisor of Dissertation

Ching-Li Chai
Graduate Group Chairperson

Acknowledgments

First and foremost, I would like to thank my advisor Florian Pop for suggesting the topic of this dissertation, and for being a constant source of encouragement and good cheer. In addition, I am thankful to the University of Pennsylvania Department of Mathematics as a whole for providing such a stimulating environment in which to learn and produce mathematics; in particular I must single out David Harbater and Ted Chinburg for being regular sources of inspiration and advice through the weekly ritual of the Galois Seminar.

A very special and heartfelt thanks goes to Steve Shatz, who not only had a powerful influence on my mathematical education, but also provided many hours of much needed friendly conversation throughout my graduate career.

This project certainly would have been hopeless without the unfailing support of my wife, Madera, who had more patience with me than I deserve, and who never let me get discouraged. Finally, I dedicate this thesis to my son, Sebastian, who has made the last year truly joyful, and continues to energize my every thought.

ABSTRACT

ARITHMETIC AND GEOMETRY OF THE OPEN P-ADIC DISC

Scott Corry

Florian Pop, Advisor

Motivated by the local lifting problem for Galois covers of curves, this thesis investigates Galois branched covers of the open p-adic disc. Our main result is that the special fiber of an abelian cover is completely determined by arithmetic and geometric properties of the generic fiber and its characteristic zero specializations. This determination of the special fiber in terms of characteristic zero data is accomplished via the field of norms functor of Fontaine and Wintenberger. As a consequence of our result, we derive a characteristic zero reformulation of the abelian local lifting problem, and as an application we give a new proof of the p-cyclic case of the Oort Conjecture, which states that cyclic covers should always lift.

Contents

Chapter 1

Introduction

The main result of this thesis (Theorem 4.0.1) says that the special fiber of an abelian branched cover of the open p-adic disc is completely determined by characteristic zero fibers. The motivation for such a theorem comes from the *global lifting problem for Galois covers of curves*: if G is a finite group, k is an algebraically closed field of characteristic $p > 0$, and $f : C \to C'$ is a finite G-Galois branched cover of smooth projective k-curves, does there exist a lifting of f to a G-Galois branched cover of smooth projective R-curves, where R is a discrete valuation ring of mixed characteristic with residue field k? This problem has been much studied; see e.g. [9], [13], [8], [14], [16].

As a brief survey of the subject, we mention the following results:

- (Grothendieck, [9]) If f is at most tamely ramified, then a lifting exists over R, where R is any complete DVR with residue field k. Moreover, the lifting is unique once we fix a lifting of C' and the branch locus of f.

- Not all wildly ramified covers are liftable: there exist curves of genus $g \geq 2$ in positive characteristic whose automorphism groups are too large to be automorphism groups of genus g curves in characteristic zero, by the Hurwitz genus bounds. If C is such a curve, it is then clear that $C \to C' = C/\mathrm{Aut}(C)$ is not liftable to mixed characteristic.

- There are even examples of non-liftable p-elementary abelian covers. See [8] for an example with $G = (\mathbb{Z}/p\mathbb{Z})^2$ for $p > 2$.

- Oort, Sekiguchi, and Suwa showed in [13] that cyclic covers lift if p divides $|G|$ at most once. Their method was global in nature, involving a group scheme degeneration of Kummer Theory to Artin-Schreier Theory.

- Using local methods (see below), Green and Matignon proved in [8] that cyclic covers lift if p divides $|G|$ at most twice.

- Pagot has shown in [14] that Klein-four covers always lift.

- D_p-covers are liftable by [16], where the method of differential data is used.

The guiding conjecture in the subject was provided by F. Oort [12], who suggested the

Oort Conjecture: *Cyclic covers always lift.*

In Chapter 5 of this thesis, we derive an arithmetic reformulation of a stronger form of this conjecture, which specifies the ring R over which the lifting should occur:

Strong Oort Conjecture: *If $f : C \to C'$ is cyclic of order $p^e n$ with $(p, n) = 1$, then f lifts over $R = W(k)[\zeta_{p^e}]$, where $W(k)$ denotes the Witt vectors of k.*

A major breakthrough in the subject came when Green and Matignon discovered that the obstructions to lifting are not global in nature, but rather local. Indeed, using either rigid patching [8] or deformation theory [1], the global lifting problem reduces to a local one, due to the

Local-to-Global Principle: ([8] section III, [1] Corollaire 3.3.5) *Let $y \in C$ be a ramification point for the G-Galois cover $f : C \to C'$, and consider the G_y-Galois cover $f_y : Spec(\widehat{\mathcal{O}_{C,y}}) \to Spec(\widehat{\mathcal{O}_{C',f(y)}})$ obtained by completion, where G_y is the inertia subgroup at y. Suppose that for each such ramified $y \in C$, the map f_y can be lifted to a G_y-Galois cover of open p-adic discs, $F_y : D \to D$, where $D = Spec(R[[Z]])$. Then the local liftings, F_y, can be patched together to yield a lifting of f to a G-Galois cover of smooth projective R-curves.*

Since $\widehat{\mathcal{O}_{C,y}} \cong k[[t]]$, we are led to consider the following *local lifting problem for Galois covers of curves*: given a finite G-Galois extension of power series rings $k[[t]]|k[[z]]$, does there exists a lifting to a G-Galois extension $R[[T]]|R[[Z]]$, where R is a mixed characteristic DVR with residue field k? One could also consider the (weaker) *birational local lifting problem for Galois covers of curves*: given a finite G-Galois extension of Laurent series fields $k((t))|k((z))$, does there exists a lifting to a G-Galois extension of normal rings $\mathcal{A}|R[[Z]]$? By a lifting in this case, we mean that $\mathcal{A}_s := \mathcal{A}/\varpi\mathcal{A}$ is an integral domain (where ϖ is a uniformizer for R), and the fields $\mathrm{Frac}(\mathcal{A}_s)$ and $k((t))$ are isomorphic as G-Galois extensions of $k((z))$. In particular, in the birational version of the local problem, we do not require $\mathrm{Spec}(\mathcal{A})$ to be smooth: in terms of geometry, this corresponds to allowing the curve C to acquire singularities.

As mentioned above, the local lifting problem does not always have a positive solution. On the other hand, Garuti has shown in [6] that the birational local lifting problem *does* always have a positive solution, so the birational problem is indeed weaker than the local lifting problem. It is clearly advantageous to work with Laurent series fields rather than power series rings, however, and the following criterion for good reduction ensures that we may do so without sacrificing the smoothness of our liftings.

Local Criterion for Good Reduction: ([10] section 5, [8] 3.4) *Let $\mathcal{A}$ be a normal integral local ring, which is also a finite $R[[Z]]$-module. Assume moreover that $\mathcal{A}_s := \mathcal{A}/\varpi\mathcal{A}$ is reduced and Frac$(\mathcal{A}_s)|k((z))$ is separable. Let $\widetilde{\mathcal{A}_s}$ be the integral closure of $\mathcal{A}_s$, and define $\delta_k := \dim_k(\widetilde{\mathcal{A}_s}/\mathcal{A}_s)$. Also, setting $K = \mathrm{Frac}(R)$, denote by d_η the degree of the different of $(\mathcal{A}\otimes K)|(R[[Z]]\otimes K)$, and by d_s the degree of the different of Frac$(\mathcal{A}_s)|k((z))$. Then $d_\eta = d_s + 2\delta_k$, and if $d_\eta = d_s$, then $\mathcal{A} \cong R[[T]]$.*

Using this criterion, we obtain the

Birational Criterion for Local Lifting: *Suppose that $k[[t]]|k[[z]]$ is a G-Galois* *extension of power series rings. Then a G-Galois extension of normal integral local rings, $\mathcal{A}|R[[Z]]$, is a lifting of $k[[t]]|k[[z]]$ if and only if it is a birational lifting of $k((t))|k((z))$, and $d_s = d_\eta$.*

Hence, the local lifting problem can be reformulated as follows: given a G-Galois extension $k((t))|k((z))$, does there exist a G-Galois birational lifting $\mathcal{A}|R[[Z]]$ which preserves the different, i.e. such that $d_s = d_\eta$?

It is this last formulation of the local lifting problem that provides our motivation for studying Galois covers of the open p-adic disc. In particular, given such a G-Galois branched cover $Y = \mathrm{Spec}(\mathcal{A}) \to D$, we are interested in determining geometric and arithmetic properties of the special fiber $Y_k \to D_k$ (such as irreducibility, separability, and the degree of the different d_s) from the corresponding properties of the generic fiber $Y_K \to D_K$ and its specializations at various points $x \in D_K$. Our main result (Theorem 4.0.1) provides precisely such a characterization of the special fiber in terms of characteristic zero data. Roughly speaking, our result says that the special fiber of a Galois cover of the open p-adic disc "wants" to be the field of norms of the characteristic zero fibers, and the degree to which this fails is the phenomenon of inseparability. Our work can be regarded as a concrete investigation of the class field theory of the open p-adic disc, and our main result suggests that the local lifting problem would be answered by a Grunwald-Wang type theorem for the open disc, with control over the generic different.

In Chapter 2 of this thesis we review the basic structure of the open p-adic disc, and then in Chapter 3 we describe the theory of the field of norms due to Fontaine and Wintenberger, which plays a major role in our main result. Chapter 4 contains the proof of our main theorem characterizing the special fiber of a Galois branched cover of the open p-adic disc in terms of the characteristic zero fibers of the cover. An arithmetic reformulation of the Oort Conjecture is deduced in Chapter 5, together with a new proof of this conjecture in the p-cyclic case. Finally, Appendix A amends a result of Brylinksi to derive a formula for the different of a p^n-cyclic extension of a local field of characterstic p in terms of the classifying Witt vector.

1.1 Notation

Let K be a complete discretely valued field. We make the following notational conventions:

- R_K denotes the valuation ring of K;
- $\mathfrak{m}_K$ denotes the maximal ideal of R_K;
- k_K denotes the residue field of R_K;
- ν_K denotes the normalized discrete valuation on K, determined by the condition that $\nu_K(K^\times) = \mathbb{Z}$;
- $|\cdot|_K$ is the absolute value on K induced by ν_K, normalized so that $|\alpha|_K = p^{-\nu_K(\alpha)}$.

- if L is the completion of an algebraic extension of K, then we also denote by ν_K (resp. $|\cdot|_K$) the unique prolongation of ν_K (resp. $|\cdot|_K$) to L;

- for $N \in \mathbb{Z}$, the symbol $o(N)$ denotes an element of K such that $\nu_K(o(N)) \geq N$;

- if $L|K$ is algebraic, then K_0 denotes the maximal unramified subextension, and K_1 the maximal tamely ramified subextension.

Chapter 2

The Open p-adic Disc

Let K be a complete discretely valued p-adic field, with valuation ring $R = R_K$. Then the *open p-adic disc* (over K) is defined to be $D_K := \operatorname{Spec}(R[[Z]] \otimes_R K)$, and its smooth integral model is denoted by $D = \operatorname{Spec}(R[[Z]])$. The key result for understanding the structure of the open p-adic disc is the Weierstrass Preparation Theorem:

Proposition 2.0.1. (Weierstrass Preparation Theorem, [2] VII.3.8, Prop. 6) *Suppose that $g(Z) \in R[[Z]]$ has a nonzero* reduced series *$\overline{g}(z) \in k[[z]]$, of valuation $\nu_{k((z))}(\overline{g}(z)) = d \geq 0$. Then $g(Z)$ can be written uniquely as*

$$g(Z) = (Z^d + a_{d-1}Z^{d-1} + \cdots + a_0)U(Z),$$

where all $a_i \in \mathfrak{m}$ and $U(Z)$ is a unit in $R[[Z]]$. The degree d is called the Weierstrass degree *of $g(Z)$.*

Polynomials $Z^d + a_{d-1}Z^{d-1} + \cdots + a_0$ as in the proposition are called *distinguished polynomials*, and we see that the ring $R[[Z]]$ has the following properties: it is a 2-dimensional regular local ring with maximal ideal (ϖ, Z), where ϖ is a uniformizer for R. Moreover, if $\mathcal{P}$ is a height 1 prime of $R[[Z]]$, then either $\mathcal{P} = (\varpi)$, or $\mathcal{P} = (f(Z))$ for some irreducible distinguished polynomial in $R[Z]$. It follows that $R[[Z]] \otimes K$ is a Dedekind domain whose maximal ideals are in one-to-one correspondence with the irreducible distinguished polynomials over R. Finally, the geometric points of D_K can be described as:

$$
\begin{aligned}
D_K(\overline{K}) &= \left\{\alpha \in \overline{K} \mid f(\alpha) = 0 \;\&\; f \in R[Z] \text{ irred. distinguished}\right\} \\
&= \left\{\alpha \in \overline{K} \mid |\alpha|_K < 1\right\},
\end{aligned}
$$

which explains the name of D_K.

2.1 The Weierstrass Argument

As a consequence of the Weierstrass Preparation Theorem, we see that an arbitrary nonzero power series $g(Z) \in R[[Z]]$ can be written in the form $g(Z) = \varpi^c f(Z)U(Z)$, where $c \geq 0$ and $f(Z)$ is distinguished of degree $d \geq 0$. In the course of our investigation, we will very often have to work with the ring $R[[Z]]_{\mathfrak{m}}$, the local ring of D at the generic point of the special fiber $D_k = \mathrm{Spec}(k[[z]]) \subset D$. Now the previous remarks imply that an arbitrary nonzero element $\xi(Z) \in R[[Z]]_{\mathfrak{m}}$ has the form

$$\xi(Z) = \frac{\varpi^c f_1(Z) U(Z)}{f_2(Z)},$$

where the $f_i(Z)$ are distinguished. In particular, the denominator $f_2(Z)$ will be relatively prime to almost all height one primes of $R[[Z]]$, so if $\mathcal{P} = (h(Z))$ is one of these primes, we will have $\xi(Z) \in R[[Z]]_{\mathcal{P}}$, and it will make sense to look at the image of ξ in $R[[Z]]_{\mathcal{P}}/\mathcal{P} \cong K(\alpha)$, where α is a root of $h(Z)$ in $\overline{K}$. When we have chosen a particular root α, we will refer to the image of ξ as the *specialization* of ξ at the point $Z = \alpha$. Since in any particular argument only finitely many such elements ξ will be involved, it will generally make sense to specialize everything in sight at most points of D_K. In the rest of this thesis, we will refer to this argument (which allows us to specialize almost everywhere) as the *Weierstrass Argument*.

2.2 The Ramification Argument

Suppose that $\{x_m\}_m \subset D_K$ is a sequence of points corresponding to a sequence $\{\alpha_m\}_m \in \overline{K}$ with each α_m being a uniformizer for the discrete valuation field $K(\alpha_m)$. Moreover, suppose that $|\alpha_m|_K \to 1$ as $m \to \infty$, so that the points x_m are approaching the boundary of D_K. Equivalently, we are assuming that the ramification index $e_m := e(K(\alpha_m)|K)$ goes to ∞ with m. Given $\xi(Z) = \varpi^c \frac{f_1(Z)}{f_2(Z)} U(Z) \in R[[Z]]_{\mathfrak{m}}$, we can consider the specialization of ξ at x_m for $m >> 0$ (by the Weierstrass Argument). Denoting this specialization by $\xi_m \in K(\alpha_m)$, we see that

$$\nu_{K(\alpha_m)}(\xi_m) = c\nu_{K(\alpha_m)}(\varpi) + \nu_{K(\alpha_m)}\left(\frac{f_1(\alpha_m)}{f_2(\alpha_m)}\right).$$

Note that for any $a \in \mathfrak{m}_K$ we have $\nu_{K(\alpha_m)}(a) \geq \nu_{K(\alpha_m)}(\varpi) = e_m$. Hence, if d_i is the Weierstrass degree of $f_i(Z)$, then for $m >> 0$ we have $\nu_{K(\alpha_m)}(a) \geq d_1 + d_2$ for all $a \in \mathfrak{m}_K$. It follows that $\nu_{K(\alpha_m)}(f_i(\alpha_m)) = \nu_{K(\alpha_m)}(\alpha_m^{d_i}) = d_i$, so

$$\nu_{K(\alpha_m)}(\xi_m) = ce_m + (d_1 - d_2) \geq -d_2.$$

Thus, we see that the normalized valuations of the specializations $\xi_m \in K(\alpha_m)$ are bounded below by $-d_2 = -$(degree of the pole of $\xi(Z)$). Moreover, if $c > 0$ (i.e. if $\overline{\xi}(z) = 0$), then $\nu_{K(\alpha_m)}(\xi_m) \to \infty$ as $m \to \infty$. Finally, if $d_1 \geq d_2$, then $\xi_m \in R_{K(\alpha_m)}$ for $m >> 0$, even if $c = 0$.

Again, since in any particular argument only finitely many such elements ξ will be involved, the foregoing remarks imply that there will be a uniform lower bound on the normalized valuations of the specializations at the points x_m, independently of m. Moreover, we see that it will be easy to check whether these specializations are integral, and whether their valuations run off to infinity. We will refer to this argument as the *Ramification Argument* in the sequel.

Chapter 3

The Field of Norms

3.1 Review of ramification theory

In this section we briefly recall the definitions and important properties of the upper and lower ramification filtrations. For complete proofs and a more leisurely treatment, the classic source is [15], Chapter IV.

Let K be a complete discretely valued field, and let $L|K$ be a finite Galois extension. Then we define a function $i_L : \mathrm{Gal}(L|K) \to \mathbb{Z} \cup \{\infty\}$ by

$$i_L(\sigma) := \min_{x \in R_L} (\nu_L(\sigma(x) - x) - 1).$$

Remark 3.1.1. The function i_L just defined differs slightly from the function i_G defined by Serre in [15]: $i_L = i_G - 1$ for $G = \mathrm{Gal}(L|K)$. We prefer to use the function i_L in order to match the notations of [17].

Lemma 3.1.2. *Suppose that $L|K$ is totally ramified, and let π be any uniformizer for L. Then $i_L(\sigma) = \nu_L(\frac{\sigma(\pi)}{\pi} - 1)$ for all $\sigma \in Gal(L|K)$.*

Proof: Since $L|K$ is totally ramified, it follows that $R_L = R_K[\pi]$. On the other hand, $i_L(\sigma)$ is the greatest integer i such that σ acts trivially on the quotient $R_L/\mathfrak{m}_L^{i+1} = R_K[\pi]/(\pi^{i+1})$. But σ acts trivially on this quotient if and only if $\nu_L(\sigma(\pi) - \pi) \geq i + 1$, which implies that

$$i_L(\sigma) = \nu_L(\sigma(\pi) - \pi) - 1 = \nu_L(\frac{\sigma(\pi)}{\pi} - 1)$$

as claimed. $\square$

Definition 3.1.3. Let $L|K$ be a finite Galois extension with group G. Then for an integer $i \geq -1$,

$$G_i := \{\sigma \in G \mid i_L(\sigma) \geq i\}$$

is called the *ith ramification subgroup in the lower numbering*. We extend the indexing to the set of real numbers ≥ -1 by setting

$$G_t := G_{\lceil t \rceil} \qquad \forall t \in \mathbb{R}_{\geq -1}.$$

Note that G_i is a normal subgroup of G, being the kernel of the natural map

$$G \to \mathrm{Aut}(R_L/\mathfrak{m}_L^{i+1}).$$

Moreover, the groups G_i form a decreasing and separated filtration of G, with $G_{-1} = G$ and $G_0 =$ the inertia subgroup of G.

Definition 3.1.4. Define the *Herbrand function of* $L|K$, $\varphi_{L|K} : \mathbb{R}_{\geq -1} \to \mathbb{R}_{\geq -1}$ by

$$\varphi_{L|K}(t) := \int_0^t \frac{\#G_s}{\#G_0} ds.$$

The function $\varphi_{L|K}$ is an increasing, continuous, piecewise-linear bijection, and hence has an increasing, continuous, and piecewise-linear inverse $\psi_{L|K}$. If $K'|K$ is a Galois subextension of the finite Galois extension $L|K$, then we have the following transitivity formulas for the functions φ and ψ:

$$\begin{aligned} \psi_{L|K} &= \psi_{L|K'} \circ \psi_{K'|K} \\ \varphi_{L|K} &= \varphi_{K'|K} \circ \varphi_{L|K'}. \end{aligned}$$

Finally, if $K'|K$ is an arbitrary subextension (possibly non-Galois) of the finite Galois extension $L|K$, then we define a Herbrand function $\varphi_{K'|K}$ by

$$\varphi_{K'|K} := \varphi_{L|K} \circ \psi_{L|K'}.$$

This definition coincides with our previous definition in the case where $K'|K$ is Galois, and the transitivity formulas above ensure that $\varphi_{K'|K}$ does not depend on the containing Galois extension $L|K$.

Using the function $\psi_{L|K}$, we define a new ramification filtration on the Galois group G.

Definition 3.1.5. For a real number $s \geq -1$, define

$$G^s := G_{\psi_{L|K}(s)}.$$

The decreasing and separated filtration $\{G^s\}_s$ is called *the ramification filtration in the upper numbering.* Note that $G^{-1} = G_{-1} = G$ and $G^s = G_0$ for $-1 < s \leq 0$.

Using the upper numbering, we can give an integral expression for the inverse Herbrand function $\psi_{L|K}$:

$$\psi_{L|K}(s) = \int_0^s \frac{\#G^0}{\#G^t} dt \qquad \forall s \in \mathbb{R}_{\geq -1}. \tag{3.1.1}$$

The difference between the upper and lower ramification filtrations of G is that the latter behaves well under taking subgroups of G, while the former behaves well under forming quotient groups.

Proposition 3.1.6. *Let H be a subgroup of $G = Gal(L|K)$ with fixed field K'. Then the lower ramification filtration of $H = Gal(L|K')$ is induced by the lower ramification filtration of G:*

$$H_i = H \cap G_i \qquad \forall i \geq -1.$$

Proof: This is clear from the fact that H_i is the kernel of the composition

$$H \hookrightarrow G \to \mathrm{Aut}(R_L/\mathfrak{m}_L^{i+1}),$$

while G_i is the kernel of the second map. □

Proposition 3.1.7. ([15], Chapter IV, Prop. 14) *Let H be a normal subgroup of $G = Gal(L|K)$, with fixed field K'. Then the upper ramification filtration on $G/H = Gal(K'|K)$ is induced by the upper ramification filtration of G:*

$$(G/H)^s = G^s H/H \qquad \forall s \in \mathbb{R}_{\geq -1}.$$

Now suppose that $L|K$ is an infinite Galois extension. Then Proposition 3.1.7 allows us to define an upper ramification filtration on the profinite group $G = \mathrm{Gal}(L|K)$:

Definition 3.1.8. For a real number $s \geq -1$, define

$$G^s := \varprojlim Gal(K'|K)^s$$

where the limit is over all finite Galois subextensions $K'|K$ of $L|K$. Then the groups $\{G^s\}_s$ form a decreasing, exhaustive, and separated filtration of G by closed normal subgroups, called the *upper ramification filtration*. We say that a real number $r \geq -1$ is a *jump* for the upper ramification filtration if $G^{r+\epsilon} \neq G^r$ for all $\epsilon > 0$.

In particular, if $K^{sep}|K$ is a separable closure of K, then the absolute Galois group $G_K := \mathrm{Gal}(K^{sep}|K)$ is equipped with its upper ramification filtration $\{G_K^s\}_s$.

Lemma 3.1.9. *Suppose that $L|K$ is a (possibly infinite) Galois extension with group G, and let $K'|K$ be a finite subextension corresponding to the open subgroup H. Then for all $u \geq -1$ we have*

$$H^u = H \cap G^{\varphi_{K'|K}(u)}.$$

Proof: Let $\mathcal{G}$ be the set of all finite extensions $L'|K'$ contained in L such that L' is Galois over K. Then $\mathcal{G}$ is cofinal in the set of all finite Galois subextensions of $L|K'$, so

$$H^u = \varprojlim_{L' \in \mathcal{G}} \mathrm{Gal}(L'|K')^u.$$

But for each $L' \in \mathcal{G}$ we have

$$\begin{aligned} \mathrm{Gal}(L'|K')^u &= \mathrm{Gal}(L'|K')_{\psi_{L'|K'}(u)} \\ &= \mathrm{Gal}(L'|K') \cap \mathrm{Gal}(L'|K)_{\psi_{L'|K'}(u)} \\ &= \mathrm{Gal}(L'|K') \cap \mathrm{Gal}(L'|K)^{\varphi_{L'|K} \circ \psi_{L'|K'}(u)} \\ &= \mathrm{Gal}(L'|K') \cap \mathrm{Gal}(L'|K)^{\varphi_{K'|K} \circ \varphi_{L'|K'} \circ \psi_{L'|K'}(u)} \\ &= \mathrm{Gal}(L'|K') \cap \mathrm{Gal}(L'|K)^{\varphi_{K'|K}(u)}. \end{aligned}$$

Taking the limit now yields

$$H^u = \varprojlim_{L' \in \mathcal{G}} \mathrm{Gal}(L'|K') \cap \mathrm{Gal}(L'|K)^{\varphi_{K'|K}(u)} = H \cap G^{\varphi_{K'|K}(u)}. \square$$

3.2 Arithmetically profinite extensions

The field of norms construction applies to a certain type of field extension, which we now describe. The basic reference for this material is [17].

Definition 3.2.1. Let K be a complete discrete valuation field with perfect residue field k_K of characteristic $p > 0$, and K^{sep} a fixed separable closure. Then an extension $L|K$ contained in $K^{sep}|K$ is called *arithmetically profinite (APF)* if for all $u \geq -1$, the group $G_K^u G_L$ is open in G_K.

If we set $K^u := \mathrm{Fix}(G_K^u) \subset K^{sep}$, then this definition means simply that $K_u := K^u \cap L$ is a finite extension of K for all $u \geq -1$. Since the upper ramification filtration is separated, it follows that $K^{sep} = \cup_u K^u$, which implies that $L = \cup_u K_u$.

A concrete example of an infinite APF extension is $\mathbb{Q}_p(\zeta_{p^\infty})|\mathbb{Q}_p$, and in this case $K_m = \mathbb{Q}_p(\zeta_{p^m})$.

Note that an APF extension need not be Galois. However, many statements about APF extensions become more transparent in the Galois case, so we will take special care in the following exposition to explain the meaning of various properties and definitions in the Galois situation.

One way of thinking about APF extensions is that they are exactly those which allow for the definition of the inverse Herbrand function (which we defined in the previous section only for finite Galois extensions). Indeed, if $L|K$ is a (possibly infinite) APF extension, then we set $G_L^0 := G_K^0 \cap G_L$ and define

$$\psi_{L|K}(u) := \begin{cases} \int_0^u (G_K^0 : G_L^0 G_K^t) dt & \text{if } u \geq 0 \\ u & \text{if } -1 \leq u \leq 0. \end{cases}$$

If $L|K$ is Galois with group $G = G_K/G_L$, then $G^t = G_K^t G_L/G_L$, and

$$G^0/G^t = (G_K^0 G_L/G_L)/(G_K^t G_L/G_L) \cong G_K^0 G_L/G_K^t G_L \cong G_K^0/G_K^t G_L^0.$$

This implies that in the Galois case we have

$$\psi_{L|K}(u) = \int_0^u (G^0 : G^t) dt \qquad \text{for } u \geq 0,$$

which accords with equation (3.1.1) given previously for finite Galois extensions.

For a general APF extension $L|K$, the function $\psi_{L|K}$ just defined is increasing, continuous, and piecewise-linear, with inverse $\varphi_{L|K}$ which is also increasing, continuous, and piecewise-linear. Of course, when $L|K$ is finite, $\varphi_{L|K}$ coincides with our previous definition of the Herbrand function.

An important quantity attached to an APF extension $L|K$ is

$$i(L|K) := \sup\{u \geq -1 \mid G_K^u G_L = G_K\}.$$

In terms of the ramification subextensions $K_u|K$, the quantity $i(L|K)$ is the supremum of the indices u such that $K_u = K$. In the case where $L|K$ is Galois with group $G = G_K/G_L$, we have $G^u = G_K^u G_L/G_L$, and $i(L|K)$ is the first jump in the upper ramification filtration on G. Note that $i(L|K) \geq 0$ if and only if $L|K$ is totally ramified, and $i(L|K) > 0$ if and only if $L|K$ is totally wildly ramified. Because the inverse Herbrand function $\psi_{L|K}$ and the quantity $i(L|K)$ will be essential for our later work, we include here the

Proposition 3.2.2. ([17], Proposition 1.2.3) *Let M and N be two extensions of K contained in K^{sep} with $M \subset N$. Then*

1. *if $M|K$ is finite, then $N|K$ is APF if and only if $N|M$ is APF;*
2. *if $N|M$ is finite, then $N|K$ is APF if and only if $M|K$ is APF;*
3. *if $N|K$ is APF then $M|K$ is APF;*
4. *if $N|K$ is APF, then $i(M|K) \geq i(N|K)$, and if in addition $M|K$ is finite, then $i(N|M) \geq \psi_{M|K}(i(N|K)) \geq i(N|K)$.*

Proof: Note that the following equality always holds, and in particular, the finiteness of any two of the quantities implies the finiteness of the third:

$$(G_K : G_N G_K^u) = (G_K : G_M G_K^u)(G_M : G_N(G_M \cap G_K^u)).$$

If $M|K$ is finite, then the first term on the right hand side is finite, which means that the remaining terms are either both finite or both infinite. But by definition, $N|K$ is APF if and only if the left hand side is finite. On the other hand, $G_M \cap G_K^u = G_M^{\psi_{M|K}(u)}$ by Lemma 3.1.9, so the finiteness of the right hand side again amounts to the arithmetic profiniteness of $N|M$. This proves 1.

Part 2 follows immediately from the fact that $N|M$ finite implies that the second term on the right hand side is finite, hence the remaining two terms are either both finite or both infinite.

For 3, if $N|K$ is APF, then the left hand side is finite, and this implies the finiteness of the right hand side, and in particular the fact that $M|K$ is APF.

Finally, we prove part 4. First suppose only that $N|K$ is APF. Then by part 3, $M|K$ is APF, and by the definition of $i(-)$ we have

$$G_K = G_K^{i(N|K)} G_N \subset G_K^{i(N|K)} G_M \subset G_K.$$

Hence, all of these inclusions are equalities, which implies that $i(M|K) \geq i(N|K)$. If we also assume that $M|K$ is finite, then $N|M$ is APF by part 1, and we have

$$G_M^{\psi_{M|K}(i(N|K))} G_N = (G_M \cap G_K^{i(N|K)}) G_N = G_M \cap G_K = G_M.$$

Hence, $i(N|M) \geq \psi_{M|K}(i(N|K)) \geq i(N|K)$, the last inequality coming from the fact that the integrand in the definition of $\psi_{M|K}$ is ≥ 1. □

Parts 1 and 2 of this proposition say that the APF property is insensitive to finite extensions of the top or bottom, while part 3 says that the APF property is inherited by subextensions. Part 4 says that the quantity $i(-)$ can only increase in subextensions or under a finite extension of the base $M|K$. In the latter case, we get a lower bound on the increase of $i(-)$ in terms of the inverse Herbrand function $\psi_{M|K}$.

Given an infinite APF extension $L|K$, let $\mathcal{E}_{L|K}$ denote the set of finite subextensions of $L|K$, partially ordered by inclusion. The key technical fact about the extension $L|K$ is the following property of the quantity $i(-)$, which generalizes part 4 of the previous proposition:

Proposition 3.2.3. ([17], Lemme 2.2.3.1) *The numbers $i(L|E)$ for $E \in \mathcal{E}_{L|K}$ tend to ∞ with respect to the directed set $\mathcal{E}_{L|K}$.*

3.3 The field of norms

Having discussed some general properties of infinite APF extensions, we are now ready to describe the field of norms construction, following [17]: given an infinite APF extension $L|K$, set

$$X_K(L)^* = \varprojlim_{\mathcal{E}_{L|K}} E^*,$$

the transition maps being given by the norm $N_{E'|E} : E'^* \to E^*$ for $E \subset E'$. Then define

$$X_K(L) = X_K(L)^* \cup \{0\}.$$

Thus, a nonzero element α of $X_K(L)$ is given by a norm-compatible sequence $\alpha = (\alpha_E)_{E \in \mathcal{E}_{L|K}}$. We wish to endow this set with an additive structure in such a way that $X_K(L)$ becomes a field, called the *field of norms* of $L|K$. This is accomplished by the following

Proposition 3.3.1. ([17], Théorème 2.1.3 (i)) *If $\alpha, \beta \in X_K(L)$, then for all $E \in \mathcal{E}_{L|K}$, the elements $\{N_{E'|E}(\alpha_{E'} + \beta_{E'})\}_{E'}$ converge (with respect to the directed set $\mathcal{E}_{L|E}$) to an element $\gamma_E \in E$. Moreover, $\alpha + \beta := (\gamma_E)_{E \in \mathcal{E}_{L|K}}$ is an element of $X_K(L)$.*

With this definition of addition, the set $X_K(L)$ becomes a field, with multiplicative group $X_K(L)^*$. Moreover, there is a natural discrete valuation on $X_K(L)$. Indeed, if K_0 denotes the maximal unramified subextension of $L|K$ (which is finite over K by APF), then $\nu_{X_K(L)}(\alpha) := \nu_E(\alpha_E) \in \mathbb{Z}$ does not depend on $E \in \mathcal{E}_{L|K_0}$. In fact ([17], Théorème 2.1.3 (ii)), $X_K(L)$ is a complete discrete valuation field with residue field isomorphic to k_L (which is a finite extension of k_K). The isomorphism of residue fields $k_{X_K(L)} \cong k_L$ comes about as follows. For $x \in k_L$, let $[x] \in K_0$ denote the Teichmüller lifting. That is, $[-] : k_L \to K_0$ is the unique multiplicative section of the canonical map $R_0 \twoheadrightarrow k_{K_0} = k_L$. Note that $E|K_1$ is of p-power degree for all $E \in \mathcal{E}_{L|K_1}$, so $x^{\frac{1}{[E:K_1]}} \in k_L$ for all such E, since k_L is perfect. The element

$([x^{\frac{1}{[E:K_1]}}])_{E \in \mathcal{E}_{L|K_1}}$ is clearly a coherent system of norms, hence (by cofinality) defines an element $f_{L|K}(x) \in X_K(L)$. The map $f_{L|K} : k_L \to X_K(L)$ is a field embedding which induces the isomorphism $k_L \cong k_{X_K(L)}$ mentioned above.

The following result will be used several times in the proof of our Main Theorem 4.0.1. Before stating it, we make a

Definition 3.3.2. For any subfield $E \in \mathcal{E}_{L|K}$, define

$$r(E) := \left\lceil \frac{p-1}{p} i(L|E) \right\rceil.$$

Proposition 3.3.3. ([17], Proposition 2.3.1 & Remarque 2.3.3.1) *Let $L|K$ be an infinite APF extension and $F \in \mathcal{E}_{L|K_1}$ be any finite extension of K_1 contained in L. Then*

1. *for any $x \in R_F$, there exists $\hat{x} = (\hat{x}_E)_{E \in \mathcal{E}_{L|K}} \in X_K(L)$ such that*

$$\nu_F(\hat{x}_F - x) \geq r(F);$$

2. *for any $\alpha, \beta \in R_{X_K(L)}$, we have*

$$(\alpha + \beta)_F \equiv \alpha_F + \beta_F \mod \mathfrak{m}_F^{r(F)}.$$

The construction just described, which produces a complete discrete valuation field of characteristic $p = \mathrm{char}(k_K)$ from an infinite APF extension $L|K$ is actually functorial in L. Precisely, $X_K(-)$ can be viewed as a functor from the category of infinite APF extensions of K contained in K^{sep} (where the morphisms are K-embeddings of finite degree) to the category of complete discretely valued fields of characteristic p (where the morphisms are separable embeddings of finite degree). Moreover, this functor preserves Galois extensions and Galois groups.

Fixing an infinite APF extension $L|K$, the functorial nature of $X_K(-)$ allows us to define a field of norms for *any* separable algebraic extension $M|L$. Namely, given such an M, we may write it as the colimit of finite extensions of L, say

$$M = \varinjlim_{L'|L \text{ finite}, L' \subset M} L'.$$

Then we define

$$X_{L|K}(M) := \varinjlim_{L'} X_K(L').$$

With this definition, we can consider $X_{L|K}(-)$ as a functor from the category of separable algebraic extensions of L to the category of separable algebraic extensions of $X_K(L)$. The amazing fact about this functor is the following

Proposition 3.3.4. ([17], Théorème 3.2.2) *The field of norms functor $X_{L|K}(-)$ is an equivalence of categories.*

In particular, $X_{L|K}(K^{sep})$ is a separable closure of $X_K(L)$, and we have an isomorphism $G_{X_K(L)} \cong G_L$.

Since $X_K(L)$ is a complete discrete valuation field with residue field k_L, it follows that any choice of uniformizer $\pi = (\pi_E)_E$ for $X_K(L)$ yields an isomorphism $k_L((z)) \cong X_K(L)$, defined by sending z to π. Via this isomorphism, an element $\alpha = (\alpha_E)_E \in R_{X_K(L)}$ corresponds to a power series $g_\alpha(z) \in k_L[[z]]$. The following lemma describes the relationship between $g_\alpha(z)$ and the coherent system of norms

$\alpha = (\alpha_E)_E$ in terms of the chosen uniformizer $\pi = (\pi_E)_E$. First we need to introduce some notation. Given a power series

$$g(z) = \sum_{i=0}^{\infty} a_i z^i \in k_L[[z]],$$

define for each $E \in \mathcal{E}_{L|K_1}$ a new power series

$$g_E(z) := \sum_{i=0}^{\infty} [a_i^{\frac{1}{[E:K_1]}}] z^i = \sum_{i=0}^{\infty} (f_{L|K}(a_i))_E z^i \in R_E[[z]].$$

Lemma 3.3.5. *For all $\alpha = (\alpha_E)_E \in X_K(L)$, we have*

$$\alpha_E \equiv g_{\alpha,E}(\pi_E) \mod \mathfrak{m}_E^{r(E)}$$

for all $E \in \mathcal{E}_{L|K_1}$, where $r(E) := \lceil \frac{p-1}{p} i(L|E) \rceil$.

Proof: By definition of the isomorphism $k_L((z)) \cong X_K(L)$, if $g_\alpha(z) = \sum_{i=0}^{\infty} a_i z^i$, then

$$\alpha = \sum_{i=0}^{\infty} f_{L|K}(a_i)\pi^i = \lim_{n\to\infty} \sum_{i=0}^{n} f_{L|K}(a_i)\pi^i.$$

Now by Proposition 3.3.3, for any $E \in \mathcal{E}_{L|K_1}$ we have

$$\left(\sum_{i=0}^{n} f_{L|K}(a_i)\pi^i \right)_E \equiv \sum_{i=0}^{n} (f_{L|K}(a_i))_E \pi_E^i \mod \mathfrak{m}_E^{r(E)}.$$

Thus we see that

$$\alpha_E \equiv \lim_{n\to\infty} \sum_{i=0}^{n} (f_{L|K}(a_i))_E \pi_E^i = g_{\alpha,E}(\pi_E) \mod \mathfrak{m}_E^{r(E)}. \ \square$$

The congruence of the previous lemma can be replaced by an equality if one is willing to restrict attention to Lubin-Tate extensions of local fields. This is a theorem of Coleman ([4], Theorem A), to which we now turn.

3.4 Coleman's Theorem

A special class of infinite APF extensions are the Lubin-Tate extensions, which we now briefly recall (see [11] Chapter V for proofs). Let H be a finite extension of $\mathbb{Q}_p$, and Γ a Lubin-Tate formal group associated to a uniformizer ϖ of H. Then Γ is a formal R_H-module, and interpreting the group Γ in $\mathfrak{m}^{sep}$ makes this ideal into an R_H-module (here $\mathfrak{m}^{sep}$ is the maximal ideal of the valuation ring of H^{sep}). Let $\Gamma_m \subset \mathfrak{m}^{sep}$ be the ϖ^m-torsion of this R_H-module. Then $R_H/\varpi^m R_H \cong \Gamma_m$ for all m, and in particular Γ_m is finite. Now define $L_0 := \cup_m H(\Gamma_m)$, which is an infinite totally ramified abelian extension of H, the *Lubin-Tate extension of H associated to ϖ*. Let K be a complete unramified extension of H with Frobenius element $\phi \in \mathrm{Gal}(K|H)$, and define $L := L_0 K$. Then $L|K$ is an infinite abelian APF extension, with ramification subfields $K_m := \mathrm{Fix}(G(L|K)^m) = K(\Gamma_m)$ ([11], Corollary V.5.6). Moreover, we have $[K_m : K] = q^{m-1}(q-1)$, where $q := \#(k_H)$. We will refer to extensions of this type as Lubin-Tate extensions, despite the fact that they are really the compositum of a Lubin-Tate extension with an unramified extension.

Now fix a primitive element $(\omega_m)_m$ for the Tate module

$$T_\varpi(\Gamma) := \varprojlim \Gamma_m.$$

That is, ω_m is a generator for Γ_m as an R_H-module, and if $[\varpi]_\Gamma$ denotes the endomorphism of Γ corresponding to ϖ, then $[\varpi]_\Gamma(\omega_{m+1}) = \omega_m$ for all $m \geq 1$. Note that the Frobenius $\phi \in \mathrm{Gal}(K|H)$ acts coefficient-wise on the ring $R_K[[Z]][\frac{1}{Z}]$.

Theorem 3.4.1. ([4], Theorem A) *For all $\alpha = (\alpha_m)_m \in X_K(L)$, there exists a unique $f_\alpha(Z) \in R_K[[Z]][\frac{1}{Z}]^*$ such that for all $m \geq 1$,*

$$(\phi^{-(m-1)} f_\alpha)(\omega_m) = \alpha_m.$$

We may suppose that the endomorphism $[\varpi]_\Gamma(Z) \in R_H[[Z]]$ is actually a polynomial of degree $q = \#(k_H)$:

$$[\varpi]_\Gamma(Z) = Z^q + a_{q-1}Z^{q-1} + \cdots + \varpi Z \qquad\qquad a_i \in \mathfrak{m}_H.$$

Then if $p \neq 2$, I claim that every primitive element $(\pi_m)_m$ for $T_\varpi(\Gamma)$ is also a uniformizer for $X_K(L)$. Indeed, for all $m \geq 1$ we have $[\varpi]_\Gamma(\pi_{m+1}) = \pi_m$, so π_{m+1} satisfies the polynomial $[\varpi]_\Gamma(Z) - \pi_m \in K_m[Z]$. But this polynomial is Eisenstein, and hence is the minimal polynomial for π_{m+1} over the field K_m. This means that $N_{K_{m+1}/K_m}(\pi_{m+1}) = (-1)^q(-\pi_m) = \pi_m$, since $q = p^{[k_H:\mathbb{F}_p]}$ is odd.

We will say that we are in the *Coleman situation* when $p \neq 2$ and we have chosen a uniformizer $\pi = (\pi_m)_m \in X_K(L)$ that is also a primitive element for $T_\varpi(\Gamma)$. An example of the Coleman situation is given by $K = \mathbb{Q}_p$ and $L = K(\zeta_{p^\infty})$, the p-cyclotomic extension (for p odd). $L|K$ is then of Lubin-Tate type, corresponding to the uniformizer $\varpi = p \in \mathbb{Q}_p$ and the formal group $\Gamma = \widehat{\mathbb{G}_m}$ with endomorphism

$$[p]_\Gamma(Z) = (1+Z)^p - 1.$$

Moreover, the choice of a compatible system of roots of unity $\{\zeta_{p^m}\}_m \subset L$ yields a uniformizer $\pi := (\zeta_{p^m} - 1)_m \in X_K(L)$ which is also a primitive element for the Tate module $T_p(\widehat{\mathbb{G}_m})$.

Now suppose that we are in the Coleman situation with uniformizer π determining an isomorphism $k_L((z)) \cong X_K(L)$. Note that $L|K$ is totally ramified, so $k_L = k_K =: k \subset \overline{\mathbb{F}}_p$. It is easy to check that the subfield $\mathbb{F}_{q^l}((z)) \subset k((z))$ corresponds to $X_{H(\zeta_{q^l-1})}(L_0(\zeta_{q^l-1})) \subset X_K(L)$ under the isomorphism above. In the following lemma, we make use of the *Teichmüller lifting* $\tau : k[[z]] \to R_K[[Z]]$:

$$\tau(\sum_{i=0}^{\infty} a_i z^i) = \sum_{i=0}^{\infty} [a_i] Z^i.$$

Lemma 3.4.2. *Suppose that* $\alpha \in R_{X_K(L)}$ *corresponds to the power series* $g_\alpha(z) \in \mathbb{F}_{q^l}[[z]]$ *under the isomorphism above, where* $q = \#(k_H)$*. Then*

$$f_\alpha(Z) \equiv g_\alpha(z) \mod (\varpi)$$

where $f_\alpha(Z) \in R_K[[Z]]$ *is the Coleman power series for* α*.*

Proof: By lemma 3.3.5, the power series $g_\alpha(z)$ has the property that

$$g_{\alpha,K_m}(\pi_m) \equiv \alpha_m \mod \mathfrak{m}_m^{r_m}.$$

On the other hand, the Coleman series $f_\alpha(Z)$ satisfies

$$(\phi^{-(m-1)} f_\alpha)(\pi_m) = \alpha_m.$$

Note that the operation of raising to the q^lth power is the identity on $\mathbb{F}_{q^l}$, and ϕ^l acts as the identity on $H(\zeta_{q^l-1}) \subset K$. Hence, for all $m \equiv 1 \mod l$ we have

$g_{\alpha,K_m} = \tau(g_\alpha)$ and $\phi^{-(m-1)}(f_\alpha) = f_\alpha$. Restricting attention to these indices m, we find that

$$f_\alpha(\pi_m) = \alpha_m \equiv (\tau(g))(\pi_m) \mod \mathfrak{m}_m^{r_m}.$$

Now apply the Weierstrass Preparation Theorem to the power series $f_\alpha(Z) - \tau(g)(Z) \in R_K[[Z]]$ to conclude that

$$f_\alpha(Z) - \tau(g)(Z) = \varpi^c(Z^n + a_{n-1}Z^{n-1} + \cdots + a_0)U(Z)$$

for $c \geq 0$, $U(Z)$ a unit, and all $a_i \in \mathfrak{m}_K$. Evaluating at π_m for $m \equiv 1 \mod t$ yields

$$\varpi^c(\pi_m^n + a_{n-1}\pi_m^{n-1} \cdots + a_0)U(\pi_m) \in \mathfrak{m}_m^{r_m}.$$

Hence for $m >> 0$ we have

$$c\nu_m(\varpi) + n \geq r_m \to \infty$$

as $m \to \infty$ by proposition 3.2.3. Since n is a constant, it follows that we must have $c > 0$, so

$$f_\alpha(Z) \equiv g_\alpha(Z) \mod (\varpi). \ \Box$$

Hence, in the Coleman situation, a choice of uniformizer (that is also a primitive element) defines a lifting of the multiplicative group $(\cup_{1\leq l\leq[K:H]}\mathbb{F}_{q^l}[[z]])^*$ to $R_K[[Z]]^*$. Of course, if $K|H$ is finite then the first group above is simply $k[[z]]^*$. Note that the multiplicativity of this lifting is guaranteed by the uniqueness in Coleman's Theorem. We extend this to a lifting $C : (\cup_{1\leq t\leq[K:H]}\mathbb{F}_{q^t}[[z]]) \to R_K[[Z]]$ by setting $C(0) := 0$, and we note that this *Coleman lifting* provides an alternative to the more obvious Teichmüller lifting. In the Coleman situation, the use of C will allow for some simplification in the proof of our Main Theorem 4.0.1. However, the Main Theorem holds for $p = 2$ and also for an arbitrary choice of uniformizer π, and the proof in the general case has recourse to the usual Teichmüller lifting, τ.

3.5 Connection with the open p-adic disc

Given a totally ramified APF extension $L|K$, we have seen how any choice of a uniformizer $\pi = (\pi_m)_m \in X_K(L)$ determines an isomorphism $k((z)) \cong X_K(L)$ defined by sending z to π (here we set $k := k_K = k_L$). We would now like to explicitly describe a connection between the field of norms $X_K(L)$ and the open p-adic disc $D_K := \mathrm{Spec}(R[[Z]] \otimes K)$ that will underly the rest of our investigation (here $R := R_K$). Namely, the special fiber of the smooth integral model $D := \mathrm{Spec}(R[[Z]])$ is $D_k = \mathrm{Spec}(k[[z]])$, with generic point $D_{k,\eta} = \mathrm{Spec}(k((z)))$. Via the isomorphism above coming from the choice of uniformizer π, we can thus identify $D_{k,\eta}$ with $\mathrm{Spec}(X_K(L))$. On the other hand, each component π_m of π is a uniformizer in K_m, and in particular has absolute value $|\pi_m|_K < 1$. Hence, each π_m corresponds to a point $x_m \in D_K$ with residue field K_m. In terms of the Dedekind domain $R[[Z]] \otimes K$, the point x_m corresponds to the maximal ideal $\mathcal{P}_m$ generated by the minimal polynomial of π_m over R. Thus, the uniformizer π defines a sequence of points $\{x_m\}_m \subset D_K$ which approaches the boundary.

Chapter 4

The Main Theorem

Let $L|K$ be a Lubin-Tate extension as described in section 3.4, with residue field $k := k_K = k_L$. Hence, there exists a p-adic local field H such that $K|H$ is unramified and $L = KL_0$, where $L_0|H$ is an honest Lubin-Tate extension, associated to a formal group Γ. As usual, we let $K_m := \mathrm{Fix}(G(L|K)^m)$, and we recall that

$$[K_m : K_1] = \#(k_H)^{m-1} = q^{m-1}.$$

Choose a uniformizer $\pi = (\pi_m)_m \in X_K(L)$, which yields the identification $D_{k,\eta} = \mathrm{Spec}(X_K(L))$ as well as the sequence of points $\{x_m\}_m \subset D_K$ as described in the last section.

Consider a G-Galois regular branched cover $Y \to D$, with Y normal. We consider this cover to be a family over $\mathrm{Spec}(R_K)$, and we introduce the following notations:

- $Y_k \to D_k$ denotes the special fiber of the cover, obtained by taking the fiber product with Spec(k);

- $Y_K \to D_K$ denotes the generic fiber, obtained by taking the fiber product with Spec(K);

- for each $m \geq 0$, we denote by $Y_{K,m}$ the fiber of Y_K at $x_m \in D_K$;

- If X is an affine scheme, then $F(X)$ denotes the total ring of fractions of X, obtained from the ring of global sections, $\Gamma(X)$, by inverting all non-zero-divisors.

If the special fiber Y_k is reduced, then $F(Y_k)$ is a product of n_s copies of a field $\mathcal{K}$:

$$F(Y_k) \cong \prod_{j=1}^{n_s} \mathcal{K},$$

where $\mathcal{K}$ is a finite normal extension of $k((z)) = X_K(L)$. On the other hand, only finitely many of the points x_m are ramified in the cover $Y_K \to D_K$, so for $m >> 0$ the fiber $Y_{K,m}$ is also reduced and we have an isomorphism of $F(Y_{K,m})$ with a product of n_m copies of a field K'_m:

$$F(Y_{K,m}) \cong \prod_{j=1}^{n_m} K'_m,$$

where $K'_m|K_m$ is a finite Galois extension. Let $d_m := \nu_{K'_m}(\mathcal{D}(K'_m|K_m))$ denote the degree of the different of $K'_m|K_m$, and set $L_m := LK'_m \subset K^{sep}$.

Theorem 4.0.1. *Let $Y \to D$ be a G-Galois regular branched cover of the open p-adic disc, with Y normal and Y_k reduced. Then*

1. *If $Y_k \to D_k$ is generically separable, then there exists $l > 0$ such that for $m >> 0$ and $m \equiv 1$ modulo l, we have $n_m = n_s$ and*

$$\mathcal{K} = X_{L|K}(L_m)$$

as subfields of $X_K(L)^{sep} = X_{L|K}(K^{sep})$. Moreover, for these m we have an isomorphism

$$Gal(\mathcal{K}|X_K(L)) \cong Gal(K'_m|K_m)$$

which respects the ramification filtrations. In particular, if d_s is the degree of the different of $\mathcal{K}|X_K(L)$, then $d_s = d_m$.

2. *If G is abelian, then the number of components of Y_k is less than or equal to the number of components of $Y_{K,m}$ for $m >> 0$, independently of any separability assumption. In particular, Y_k is irreducible if $Y_{K,m}$ is irreducible for $m >> 0$.*

3. *If Y_k is irreducible, then $Y_k \to D_k$ is generically inseparable if and only if $d_m \to \infty$.*

Remark 4.0.2. If k is a finite field, say $\#(k) = q^t$, then we can take $l = t$ in part 1 of the Theorem. That is, in the case of a finite residue field, the number l is independent of the particular cover $Y \to D$.

Remark 4.0.3. The knowledgeable reader will note that much of our proof of part 1 is inspired by the proof in [17] of the essential surjectivity statement in Proposition 3.3.4. The main difficulty is to spread the construction of [17] over the open p-adic disc.

Proof: Let $Y = \text{Spec}(\mathcal{A})$, so that $\mathcal{A}|R[[Z]]$ is a G-Galois extension of normal rings (here $R = R_K$). We are assuming that $\mathcal{A}_s := \mathcal{A}/\varpi\mathcal{A}$ is reduced, where ϖ is a uniformizer of R. Moreover, we have $(\mathcal{A} \otimes K)/\mathcal{P}_m(\mathcal{A} \otimes K) = \prod_{j=1}^{n_m} K'_m$ for $m >> 0$ (here $\mathcal{P}_m$ is the maximal ideal of $R[[Z]] \otimes K$ corresponding to x_m).

1): Suppose that $Y_k \to D_k$ is generically separable, which means that the field extension $\mathcal{K}|k((z))$ is separable, hence Galois. By the Primitive Element Theorem, there exists $x \in \mathcal{K}$ such that $\mathcal{K} = k((z))[x]$. Moreover, we can choose x to be integral over $k[[z]]$, say with minimal polynomial $f(T) \in k[[z]][T]$. Further, since $k((z))$ is infinite, we can choose n_s different primitive elements $x_j \in \mathcal{K}$ such that the corresponding minimal polynomials $f_j(T) \in k[[z]][T]$ are distinct. Even more, by Krasner's Lemma, we may assume that each $f_j(T) \in k[z][T]$, so that in fact $f_j(T) \in \mathbb{F}_{q^l}[T]$ for some $l > 0$. Having fixed this l, we replace the sequence of points $\{x_m\}_m \subset D_K$ with the subsequence corresponding to indices m congruent to 1 modulo l.

Setting $f(T) := \prod_{j=1}^{n_s} f_j(T)$, the Chinese Remainder Theorem implies that we have an isomorphism

$$k((z))[T]/(f(T)) \cong \prod_{j=1}^{n_s} k((z))[x_j] = \prod_{j=1}^{n_s} \mathcal{K} \cong F(Y_k)$$

Let x be the element of $F(Y_k)$ corresponding to $\overline{T}$ under this isomorphism, and choose a lifting, ξ, of x to $\mathcal{A}_{(\varpi)}$. Denote the minimal polynomial of ξ over $R[[Z]]_{(\varpi)}$

by $F(T)$, so that $\overline{F}(T) = f(T)$. Then $F(T)$ has the form

$$F(T) = T^N + A_{N-1}(Z)T^{N-1} + \cdots + A_0(Z) \in R[[Z]]_{(\varpi)}[T].$$

Now by the Weierstrass Argument (see section 2.1), the coefficients of $F(T)$ have the form

$$A_i(Z) = \frac{g(Z)}{Z^n + a_{n-1}Z^{n-1} + \cdots + a_0},$$

where $g(Z) \in R[[Z]]$ and the denominator is a distinguished polynomial. Moreover, because $\overline{F}(T) = f(T) \in k[[z]][T]$, it follows that each $\overline{A_i}(z) \in k[[z]]$, which implies that either $\varpi | g(Z)$ in $R[[Z]]$ (in which case $\overline{A_i}(z) = 0$), or the Weierstrass degree of $g(Z)$ is greater than n (the degree of the denominator).

Again by the Weierstrass Argument, for $m >> 0$ we can specialize the polynomial $F(T)$ at the point $Z = \pi_m$, and we have the

Lemma 4.0.4. *For $m >> 0$, the specialized polynomial $F_m(T) \in R_m[T]$, where R_m is the valuation ring of K_m.*

Proof: This follows immediately from the previous remarks and the Ramification Argument (section 2.2). $\square$

Since $f(T) \in k[[z]][T] = R_{X_K(L)}[T]$ is separable, we have $\mathrm{disc}(f) = (\mathrm{disc}(f)_{K_m})_m \neq 0$ in $X_K(L)$. Setting $r_m := \lceil \frac{p-1}{p} i(L|K_m) \rceil$, we know by Proposition 3.2.3 that $\lim_{m\to\infty} r_m = \infty$, so there exists n_0 such that for $m \geq n_0$ we have

$$r_m \geq r_{n_0} > \nu_{X_K(L)}(\mathrm{disc}(f)) := \nu_{K_m}(\mathrm{disc}(f)_{K_m}).$$

Now

$$f(T) = \overline{F}(T) = T^N + \overline{A_{N-1}}(z)T^{N-1} + \cdots + \overline{A_0}(z) \in k[z][T].$$

Under our fixed identification of $k((z))$ with $X_K(L)$, each coefficient $\overline{A_i}(z)$ corresponds to a coherent system of norms $\alpha_i = (\alpha_{i,K_m})_m$. Hence, we can write

$$f(T) = T^N + \alpha_{N-1}T^{N-1} + \cdots + \alpha_0 \in R_{X_K(L)}[T].$$

Now let $f_m(T) \in R_m[T]$ be the polynomial obtained from $f(T)$ by selecting the mth component from each coefficient:

$$f_m(T) := T^N + \alpha_{N-1,K_m}T^{N-1} + \cdots + \alpha_{0,K_m} \in R_m[T].$$

Lemma 4.0.5. *For $m >> 0$ we have $\nu_{X_K(L)}(\mathrm{disc}(f)) = \nu_{K_m}(\mathrm{disc}(F_m))$.*

First suppose that we are in the Coleman situation, so that we have the Coleman lifting, C, as described in section 3.4. The proof of Lemma 4.0.5 (and also Lemma 4.0.7) is simpler in this case, so we will give it first and then make the necessary changes to prove the general case. In particular, the following proof does not apply when $p = 2$.

Proof of Lemma 4.0.5 in the Coleman situation: Let $G(T)$ be the Coleman lifting of $f(T)$ to $R[[Z]][T]$:

$$G(T) := T^N + C(\overline{A_{N-1}})(Z)T^{N-1} + \cdots + C(\overline{A_0})(Z).$$

Then $G(T) \equiv f(T) \equiv F(T) \mod \varpi$, hence

$$F(T) = G(T) + \varpi g(Z,T)$$

for some $g(Z,T) \in R[[Z]]_{(\varpi)}[T]$. Specializing at $Z = \pi_m$ yields the equation

$$F_m(T) = f_m(T) + \varpi g(\pi_m, T).$$

Indeed, by Theorem 3.4.1, if ϕ is the Frobenius of the unramified extension $K|H$ in the setup of the Coleman situation, then

$$(\phi^{-(m-1)} C(\overline{A}_i))(\pi_m) = \alpha_{i,m} \in R_m.$$

Now recall that $m \equiv 1 \mod l = [\mathbb{F}_{q^l} : k_H]$, so

$$\phi^{-(m-1)} = \phi^{lt}.$$

But $\overline{A_i} \in \mathbb{F}_{q^l}[z]$, which implies that $C(\overline{A_i}) \in R_{H(\zeta_{q^l-1})}[[Z]]$, on which ϕ^l acts as the identity. Thus we have $C(\overline{A}_i)(\pi_m) = \alpha_{i,m}$, so that $G(T)|_{Z=\pi_m} = f_m(T)$ as claimed.

Now consider

$$\nu_{K_m}(\mathrm{disc}(f)_{K_m} - \mathrm{disc}(F_m)) = \nu_{K_m}(\mathrm{disc}(f)_{K_m} - \mathrm{disc}(f_m) + \mathrm{disc}(f_m) - \mathrm{disc}(F_m)).$$

By Proposition 3.3.3, $\nu_{K_m}(\mathrm{disc}(f)_{K_m} - \mathrm{disc}(f_m)) \geq r_m$, and

$$\nu_{K_m}(\mathrm{disc}(f_m) - \mathrm{disc}(f_m + \varpi g(\pi_m, T))) \geq r_{n_0}$$

for $m >> 0$, by the Ramification Argument applied to $\varpi g(\pi_m, T)$. It follows that

$$\nu_{K_m}(\mathrm{disc}(f)_{K_m} - \mathrm{disc}(F_m)) \geq r_{n_0}$$

for $m >> 0$, which implies that

$$\nu_{X_K(L)}(\mathrm{disc}(f)) := \nu_{K_m}(\mathrm{disc}(f)_{K_m}) = \nu_{K_m}(\mathrm{disc}(F_m)),$$

since $\nu_{K_m}(\mathrm{disc}(f)_{K_m}) < r_{n_0}$. $\square$

Now let x_m be a root of $F_m(T)$ in K^{sep}, and define $\tilde{K}_m := K_m(x_m), \tilde{L}_m := L(x_m)$. Then $\tilde{L}_m|\tilde{K}_m$ is APF by Proposition 3.2.2, and we set $\tilde{r}_m := \lceil \frac{p-1}{p} i(\tilde{L}_m|\tilde{K}_m) \rceil$. Moreover, note that for $m >> 0$ we have $K'_m = \tilde{K}_m$ and thus $L_m := LK'_m = \tilde{L}_m$ (recall that $F(Y_{K,m}) \cong \prod_{j=1}^{n_m} K'_m$). This follows from the fact that there exists $g \in R[[Z]]$ such that $\xi \in (\mathcal{A} \otimes K)_g$ (for example, take g to be the product of the denominators of the coefficients $A_i(Z)$ of $F(T) \in R[[Z]]_{(\varpi)}[T]$). Then the conductor of the subring $(R[[Z]] \otimes K)_g[\xi] \subset (\mathcal{A} \otimes K)_g$ defines a closed subset of Y_K, and if x_m lies outside the image of this set in D_K, then the splitting of $F(T)$ mod $\mathcal{P}_m$ determines the fiber $Y_{K,m}$ (see [11], Prop. I.8.3). In particular, $\tilde{L}_m = L_m$ is Galois over L.

At this point we introduce the following lemma from [17], and we include the proof for completeness, as well as to demonstrate that it only depends on Lemma 4.0.5:

Lemma 4.0.6. ([17], Lemme 3.2.5.4) *For $m >> 0$, the extensions $L|K_m$ and $\tilde{K}_m|K_m$ are linearly disjoint. Moreover, we have*

$$i(\tilde{L}_m|\tilde{K}_m) = \psi_{\tilde{K}_m|K_m}(i(L|K_m)) \geq i(L|K_m).$$

Proof: Choose $m >> 0$ so that $i(L|K_m) \geq \deg(F)\nu_{X_K(L)}(\mathrm{disc}(f))$. Then I claim that $G_{K_m}^{i(L|K_m)} \subset G_{\tilde{K}_m}$. Indeed, let $\sigma \in G_{K_m}^{i(L|K_m)}$, so that $i_{\tilde{K}_m}(\sigma|_{\tilde{K}_m}) \geq \psi_{\tilde{K}_m|K_m}(i(L|K_m)) \geq i(L|K_m) \geq \deg(F)\nu_{X_K(L)}(\mathrm{disc}(f)) = \deg(F)\nu_{K_m}(\mathrm{disc}(F_m))$, the last equality holding by Lemma 4.0.5. It follows that

$$\nu_{\tilde{K}_m}(\sigma(x_m) - x_m) - 1 \geq i_{\tilde{K}_m}(\sigma) \geq \nu_{\tilde{K}_m}(\mathrm{disc}(F_m)).$$

Hence $\nu_{\tilde{K}_m}(\sigma(x_m) - x_m) > \nu_{\tilde{K}_m}(\mathrm{disc}(F_m))$, which implies that $\sigma(x_m) = x_m$ since both are zeros of F_m. But x_m generates $\tilde{K}_m$ over K_m, so we see that $\sigma \in G_{\tilde{K}_m}$, as claimed.

To show the linear disjointness, let $S = \mathrm{Fix}(G_{K_m}^{i(L|K_m)})$. Then we certainly have $K_m \subset S \cap L$. On the other hand $S \cap L$ is fixed by $G_{K_m}^{i(L|K_m)} G_L = G_{K_m}$, so in fact $K_m = S \cap L$. Since S and L are Galois over K_m, it follows that S and L are linearly disjoint over K_m. But by the first part of the proof, $\tilde{K}_m \subset S$, so a fortiori $\tilde{K}_m$ and L are linearly disjoint over K_m.

Finally, we prove that $i(\tilde{L}_m|\tilde{K}_m) = \psi_{\tilde{K}_m|K_m}(i(L|K_m))$. By Lemma 3.1.9 we have

$$G_{K_m}^u \cap G_{\tilde{K}_m} = G_{\tilde{K}_m}^{\psi_{\tilde{K}_m|K_m}(u)}.$$

But $G_{K_m}^{i(L|K_m)} \subset G_{\tilde{K}_m}$, so we see that for $u \geq i(L|K_m)$ we have

$$G_{K_m}^u = G_{\tilde{K}_m}^{\psi_{\tilde{K}_m|K_m}(u)}.$$

Now set $\Gamma = G(L|K_m)$ and $\tilde{\Gamma} = G(\tilde{L}_m|\tilde{K}_m)$, and note that $\Gamma \cong \tilde{\Gamma}$ canonically, by linear disjointness. Moreover, for $u \geq i(L|K_m)$, this canonical map takes $\Gamma^u = G_{K_m}^u G_L / G_L$ isomorphically onto $\tilde{\Gamma}^{\psi_{\tilde{K}_m|K_m}(u)} = G_{\tilde{K}_m}^{\psi_{\tilde{K}_m|K_m}(u)} G_{\tilde{L}_m} / G_{\tilde{L}_m}$. In particular, for $u \geq i(L|K_m)$ we see that $\Gamma^u = \Gamma$ if and only if $\tilde{\Gamma}^{\psi_{\tilde{K}_m|K_m}(u)} = \tilde{\Gamma}$. This immediately implies that $i(\tilde{L}_m|\tilde{K}_m) = \psi_{\tilde{K}_m|K_m}(i(L|K_m))$. □

Since $L|K_m$ is totally wildly ramified, it follows from this lemma that

$$i(\tilde{L}_m|\tilde{K}_m) \geq i(L|K_m) > 0,$$

so $\tilde{L}_m|\tilde{K}_m$ is totally wildly ramified. Hence, Proposition 3.3.3 says that there exists $\hat{x}_m = (\hat{x}_{m,E})_E \in X_K(\tilde{L}_m)$ such that

$$\nu_{\tilde{K}_m}(\hat{x}_{m,\tilde{K}_m} - x_m) \geq \tilde{r}_m.$$

Our immediate goal is to prove the following lemma about the polynomial $f(T) \in k[[z]][T] = R_{X_K(L)}[T]$ from the beginning of the proof.

Lemma 4.0.7. $\lim_{m\to\infty} f(\hat{x}_m) = 0$.

Proof of Lemma 4.0.7 in the Coleman situation: First, note that

$$\nu_{X_K(L)}(f(\hat{x}_m)) \geq \frac{1}{\deg(f)}\nu_{X_K(\tilde{L}_m)}(f(\hat{x}_m)).$$

But $\tilde{L}_m|\tilde{K}_m$ is totally ramified, hence

$$\nu_{X_K(\tilde{L}_m)}(f(\hat{x}_m)) = \nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m}).$$

Denote by $f_{\tilde{K}_m} \in \tilde{K}_m[T]$ the polynomial obtained by replacing each coefficient of $f \in X_K(L)[T] \subset X_K(\tilde{L}_m)[T]$ by its component in $\tilde{K}_m$. Then by the linear disjointness of $L|K_m$ and $\tilde{K}_m|K_m$, it follows that $f_m = f_{\tilde{K}_m}$ and we have

$$\begin{aligned}\nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - F_m(\hat{x}_{m,\tilde{K}_m})) &= \nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - f_{\tilde{K}_m}(\hat{x}_{m,\tilde{K}_m}) \\ &\quad + f_{\tilde{K}_m}(\hat{x}_{m,\tilde{K}_m}) - F_m(\hat{x}_{m,\tilde{K}_m})) \\ &= \nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - f_{\tilde{K}_m}(\hat{x}_{m,\tilde{K}_m}) \\ &\quad + f_m(\hat{x}_{m,\tilde{K}_m}) - F_m(\hat{x}_{m,\tilde{K}_m})).\end{aligned}$$

Now by Proposition 3.3.3 we have

$$\nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - f_{\tilde{K}_m}(\hat{x}_{m,\tilde{K}_m})) \geq \tilde{r}_m.$$

On the other hand, we have (by the Ramification Argument)

$$\begin{aligned}
\nu_{\tilde{K}_m}(f_m(\hat{x}_{m,\tilde{K}_m}) - F_m(\hat{x}_{m,\tilde{K}_m})) &= \nu_{\tilde{K}_m}(f_m(\hat{x}_{m,\tilde{K}_m}) - f_m(\hat{x}_{m,\tilde{K}_m}) \\
&\quad -\varpi g(\pi_m, \hat{x}_{m,\tilde{K}_m})) \\
&= \nu_{\tilde{K}_m}(\varpi g(\pi_m, \hat{x}_{m,\tilde{K}_m})) \\
&\geq \nu_{\tilde{K}_m}(\varpi) - Be(\tilde{K}_m|K_m) \\
&\geq e(\tilde{K}_m|K) - B\deg(f),
\end{aligned}$$

where B is the order of the worst pole in the coefficients of g. Thus, we see that

$$\nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - F_m(\hat{x}_{m,\tilde{K}_m})) \geq \min\{\tilde{r}_m, e(\tilde{K}_m|K) - B\deg(f)\}.$$

Together with the fact that $\nu_{\tilde{K}_m}(\hat{x}_{m,\tilde{K}_m} - x_m) \geq \tilde{r}_m$, this implies that

$$\begin{aligned}
\nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m}) &= \nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - F_m(x_m)) \\
&\geq \nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - F_m(\hat{x}_{m,\tilde{K}_m} - (\hat{x}_{m,\tilde{K}_m} - x_m))) \\
&\geq \min\{\tilde{r}_m, e(\tilde{K}_m|K) - B\deg(f)\}.
\end{aligned}$$

Thus we have shown that

$$\begin{aligned}
\nu_{X_K(L)}(f(\hat{x}_m)) &\geq \frac{1}{\deg(f)}(\nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m})) \\
&\geq \frac{1}{\deg(f)}\min\{\tilde{r}_m, e(\tilde{K}_m|K) - B\deg(f)\}.
\end{aligned}$$

But $\tilde{r}_m \to \infty$ as $m \to \infty$, and since B is a constant, we also have $e(\tilde{K}_m|K) - B\deg(f) \to \infty$. It follows that $\nu_{X_K(L)}(f(\hat{x}_m)) \to \infty$ so that

$$\lim_{m\to\infty} f(\hat{x}_m) = 0$$

as claimed. $\square$

We now turn to the proof of Lemmas 4.0.5 and 4.0.7 in the general case. We no longer have the Coleman lifting, C, and have to make use of the Teichmüller lifting, τ, instead. As a consequence, the equality $C(f)(T)|_{Z=\pi_m} = f_m(T)$ coming from Theorem 3.4.1 is replaced by a congruence coming from Lemma 3.3.5.

Proof of Lemma 4.0.5: Let $G(T) \in R[Z][T]$ be the Teichmüller lifting of $f(T)$:

$$G(T) := \tau(f)(T) = T^N + \tau(\overline{A_{N-1}})(Z)T^{N-1} + \cdots + \tau(\overline{A_0})(Z).$$

Then as before, G and F both reduce mod ϖ to f, hence

$$F(T) = G(T) + \varpi g(Z,T)$$

for some $g(Z,T) \in R[[Z]]_{(\varpi)}[T]$. Specializing at $Z = \pi_m$ now yields the equation

$$F_m(T) = f_m(T) + \pi_m^{r_m} h_m(T) + \varpi g(\pi_m, T) \tag{4.0.1}$$

for some $h_m(T) \in R_m[T]$. Indeed, by Lemma 3.3.5, we have

$$\overline{A}_{i,K_m}(\pi_m) \equiv \alpha_{i,K_m} \mod \mathfrak{m}_{K_m}^{r_m}.$$

But $[K_m : K_1] = q^{m-1} = q^{lt}$ by our choice of indices m. Note that the operation of raising to the q^lth power on the Teichmüller representatives $\tau(\mathbb{F}_{q^l}) \subset R$ is the identity. Since the coefficients of $\overline{A_i}(z)$ lie in $\mathbb{F}_{q^l}$, it follows that $\overline{A}_{i,K_m}(Z) = \tau(\overline{A_i})(Z)$, so that

$$\tau(\overline{A_i})(\pi_m) \equiv \alpha_{i,K_m} \mod \mathfrak{m}_{K_m}^{r_m},$$

from which equation (4.0.1) follows immediately.

Consider

$$\nu_{K_m}(\mathrm{disc}(f)_{K_m} - \mathrm{disc}(F_m)) = \nu_{K_m}(\mathrm{disc}(f)_{K_m} - \mathrm{disc}(f_m) + \mathrm{disc}(f_m) - \mathrm{disc}(F_m)).$$

Now by Proposition 3.3.3, $\nu_{K_m}(\mathrm{disc}(f)_{K_m} - \mathrm{disc}(f_m)) \geq r_m$, and

$$\nu_{K_m}(\mathrm{disc}(f_m) - \mathrm{disc}(f_m + \pi_m^{r_m} h_m + \varpi g(\pi_m, T))) \geq r_{n_0}$$

for $m >> 0$, by the Ramification Argument applied to $\varpi g(\pi_m, T)$ and the fact that $r_m \to \infty$. It follows that

$$\nu_{K_m}(\mathrm{disc}(f)_{K_m} - \mathrm{disc}(F_m)) \geq r_{n_0}$$

for $m >> 0$, which implies that

$$\nu_{X_K(L)}(\mathrm{disc}(f)) := \nu_{K_m}(\mathrm{disc}(f)_{K_m}) = \nu_{K_m}(\mathrm{disc}(F_m))$$

for $m >> 0$. □

Lemma 4.0.6 still holds in the general situation, since it depends only on the validity of Lemma 4.0.5. Using these lemmas, we can prove that $\lim_{m\to\infty} f(\hat{x}_m) = 0$ in the general situation.

Proof of lemma 4.0.7: We follow the outline of the proof from the strict Coleman situation, and the only new difficulty is to manage the extra term in equation (4.0.1).

So recall that

$$\nu_{X_K(L)}(f(\hat{x}_m)) \geq \frac{1}{\deg(f)}\nu_{X_K(\tilde{L}_m)}(f(\hat{x}_m)).$$

Moreover, just as before $\tilde{L}_m|\tilde{K}_m$ is totally ramified, hence

$$\nu_{X_K(\tilde{L}_m)}(f(\hat{x}_m)) = \nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m}).$$

Denote by $f_{\tilde{K}_m} \in \tilde{K}_m[T]$ the polynomial obtained by replacing each coefficient of $f \in X_K(L)[T] \subset X_K(\tilde{L}_m)[T]$ by its component in $\tilde{K}_m$. Then by the linear disjointness of $L|K_m$ and $\tilde{K}_m|K_m$, it follows that $f_m = f_{\tilde{K}_m}$ and we have

$$\begin{aligned}
\nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - F_m(\hat{x}_{m,\tilde{K}_m})) &= \nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - f_{\tilde{K}_m}(\hat{x}_{m,\tilde{K}_m}) \\
&\quad + f_{\tilde{K}_m}(\hat{x}_{m,\tilde{K}_m}) - F_m(\hat{x}_{m,\tilde{K}_m})) \\
&= \nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - f_{\tilde{K}_m}(\hat{x}_{m,\tilde{K}_m}) \\
&\quad + f_m(\hat{x}_{m,\tilde{K}_m}) - F_m(\hat{x}_{m,\tilde{K}_m})).
\end{aligned}$$

As always, we have

$$\nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - f_{\tilde{K}_m}(\hat{x}_{m,\tilde{K}_m})) \geq \tilde{r}_m.$$

On the other hand, we have by the Ramification Argument

$$\begin{aligned}
\nu_{\tilde{K}_m}(f_m(\hat{x}_{m,\tilde{K}_m}) - F_m(\hat{x}_{m,\tilde{K}_m})) &= \nu_{\tilde{K}_m}(f_m(\hat{x}_{m,\tilde{K}_m}) - f_m(\hat{x}_{m,\tilde{K}_m}) \\
&\quad - \pi_m^{r_m} h_m(\hat{x}_{m,\tilde{K}_m}) - \varpi g(\pi_m, \hat{x}_{m,\tilde{K}_m})) \\
&= \nu_{\tilde{K}_m}(\pi_m^{r_m} h_m(\hat{x}_{m,\tilde{K}_m}) + \varpi g(\pi_m, \hat{x}_{m,\tilde{K}_m})) \\
&\geq \min\{r_m, \nu_{K_m}(\varpi) - B\} \\
&= \min\{r_m, e(K_m|K) - B\},
\end{aligned}$$

where B is the order of the worst pole in the coefficients of g. Thus, we see that

$$\nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - F_m(\hat{x}_{m,\tilde{K}_m})) \geq \min\{r_m, e(K_m|K) - B\},$$

since $\tilde{r}_m \geq r_m$. Together with the fact that $\nu_{\tilde{K}_m}(\hat{x}_{m,\tilde{K}_m} - x_m) \geq \tilde{r}_m$, this implies (as before) that

$$\nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m}) = \nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m} - F_m(x_m)) \geq \min\{r_m, e(K_m|K) - B\}.$$

Thus we have shown that

$$\begin{aligned} \nu_{X_K(L)}(f(\hat{x}_m)) &\geq \frac{1}{\deg(f)}(\nu_{\tilde{K}_m}(f(\hat{x}_m)_{\tilde{K}_m})) \\ &\geq \frac{1}{\deg(f)}\min\{r_m, e(K_m|K) - B\}. \end{aligned}$$

But $r_m \to \infty$ as $m \to \infty$, and since B is a constant, we also have $e(K_m|K) - B \to \infty$. It follows that $\nu_{X_K(L)}(f(\hat{x}_m)) \to \infty$ so that

$$\lim_{m\to\infty} f(\hat{x}_m) = 0$$

as claimed. $\square$

The rest of the proof now proceeds with no special treatment for the Coleman situation.

Replacing the sequence $\{\hat{x}_m\}$ by a subsequence, we may assume that it converges to a root $\tilde{x}$ of f. But then $\tilde{x}$ is conjugate to one of the roots x_j from the beginning of this proof, and since $\mathcal{K}|k((z))$ is Galois, we have that $\mathcal{K} = k((z))(x_j) = k((z))(\tilde{x})$. Moreover, by Krasner's Lemma, $\tilde{x} \in X_K(L)(\hat{x}_m) \subset X_K(\tilde{L}_m)$ for $m >> 0$. This implies that $\mathcal{K} \subset X_K(\tilde{L}_m)$ for $m >> 0$, and I claim that this inclusion is actually an equality.

Now if $\sigma \in \mathrm{Gal}(\tilde{L}_m|L)$, then $X_{L|K}(\sigma) \in \mathrm{Gal}(X_K(\tilde{L}_m)|X_K(L))$ and we have

$$X_{L|K}(\sigma)(\hat{y}) = (\sigma(\hat{y}^{(n)}))_n \qquad \forall \hat{y} \in X_K(\tilde{L}_m),$$

where $\hat{y}^{(n)}$ is the component of $\hat{y} \in X_K(\tilde{L}_m)$ in the field $\tilde{K}_m K_n \subset \tilde{L}_m$.

Lemma 4.0.8. *Given $\sigma \in Gal(\tilde{L}_m|L)$, suppose that $y \in \tilde{K}_m$ is an element such that*

$$\nu_{\tilde{K}_m}(\sigma(y) - y) < \tilde{r}_m.$$

Using proposition 3.3.3, choose an element $\hat{y} \in X_K(\tilde{L}_m)$ such that

$$\nu_{\tilde{K}_m}(\hat{y}^{(m)} - y) \geq \tilde{r}_m.$$

Then

$$\nu_{X_K(\tilde{L}_m)}(X_{L|K}(\sigma)(\hat{y}) - \hat{y}) = \nu_{\tilde{K}_m}(\sigma(y) - y).$$

Proof: We compute (here $o(r)$ denotes an element of valuation at least r):

$$\begin{aligned}
\nu_{X_K(\tilde{L}_m)}(X_{L|K}(\sigma)(\hat{y}) - \hat{y}) &= \nu_{X_K(\tilde{L}_m)}((\sigma(\hat{y}^{(n)}))_n - (\hat{y}^{(n)})_n) \\
&:= \nu_{\tilde{K}_m}([(\sigma(\hat{y}^{(n)}))_n - (\hat{y}^{(n)})_n]_{\tilde{K}_m}) \\
&= \nu_{\tilde{K}_m}(\sigma(\hat{y}^{(m)}) - \hat{y}^{(m)} + o(\tilde{r}_m)) \\
&= \nu_{\tilde{K}_m}(\sigma(y + o(\tilde{r}_m)) - y + o(\tilde{r}_m)) \\
&= \nu_{\tilde{K}_m}(\sigma(y) - y + o(\tilde{r}_m)) \\
&= \nu_{\tilde{K}_m}(\sigma(y) - y). \ \square
\end{aligned}$$

We wish to apply this lemma with $y = x_m$ and $\hat{y} = \hat{x}_m$, so we compute

$$\begin{aligned} \nu_{\tilde{K}_m}(\sigma(x_m) - x_m) &\leq \nu_{\tilde{K}_m}(\mathrm{disc}(F_m)) \\ &\leq (\deg F)\nu_{K_m}(\mathrm{disc}(F_m)) \\ &= (\deg F)\nu_{X_K(L)}(\mathrm{disc}(f)) \end{aligned}$$

for $m >> 0$ by Lemma 4.0.5. Since $\tilde{r}_m \to \infty$, it follows that x_m satisfies the hypothesis of Lemma 4.0.8 for $m >> 0$, and we conclude that

$$\nu_{X_K(\tilde{L}_m)}(X_{L|K}(\sigma)(\hat{x}_m) - \hat{x}_m) = \nu_{\tilde{K}_m}(\sigma(x_m) - x_m)$$

for $m >> 0$. This immediately implies that $X_K(L)(\hat{x}_m) = X_K(\tilde{L}_m)$, because if the inclusion were proper, then there would exist $\sigma \neq 1$ in $\mathrm{Gal}(\tilde{L}_m|L)$ such that $X_{L|K}(\sigma)(\hat{x}_m) = \hat{x}_m$, which is a contradiction since since $\sigma(x_m) \neq x_m$.

Thus, in order to show that $\mathcal{K} = X_K(\tilde{L}_m)$, we just need to show that $X_K(L)(\hat{x}_m) \subset X_K(L)(\tilde{x})$. But the sequence $\{\hat{x}_m\}$ converges to $\tilde{x}$, and our computation above shows that the Krasner radii

$$\max\{\nu_{X_K(L)}(X_{L|K}(\sigma)(\hat{x}_m) - \hat{x}_m) \mid \sigma \in G(\tilde{L}_m|L), \sigma \neq 1\} < C$$

for some constant C independent of m. Hence for $m >> 0$ so that $\nu_{X_K(L)}(\tilde{x} - \hat{x}_m) > C$, Krasner's lemma tells us that

$$X_K(L)(\hat{x}_m) \subset X_K(L)(\tilde{x})$$

as required.

Thus, we have shown that $\mathcal{K} = X_{L|K}(\tilde{L}_m) = X_{L|K}(L_m)$. It now follows from the fundamental equality that $n_s = n_m$:

$$n_s = \frac{\deg f}{[\mathcal{K} : k((z))]} = \frac{\deg F}{[L_m : L]} = \frac{\deg F}{[K'_m : K_m]} = n_m.$$

It remains to prove the statement about the Galois groups. By the general theory of the field of norms, we have

$$\mathrm{Gal}(L_m|L) \cong \mathrm{Gal}(X_K(L_m)|X_K(L)) = \mathrm{Gal}(\mathcal{K}|X_K(L)).$$

Moreover, since $L_m = K'_m L$ and $L|K_m$ and $K'_m|K_m$ are linearly disjoint, it follows that

$$\mathrm{Gal}(L_m|L) = \mathrm{Gal}(K'_m L|L) \cong \mathrm{Gal}(K'_m|K'_m \cap L) = \mathrm{Gal}(K'_m|K_m).$$

Thus, we just need to show that the ramification filtrations are preserved under these isomorphisms.

First note that for all $m, n >> 0$, we have $L_m = L_n$, since by the preceding proof we have that $X_K(L_m) = \mathcal{K} = X_K(L_n)$ and $X_{L|K}(-)$ is an equivalence of categories. Denote this common field by L'.

Lemma 4.0.9. (compare [17], Proposition 3.3.2) *For $\sigma \in$ Gal$(L'|L)$ and $m >> 0$, we have $i_{K'_m}(\sigma) = i_{X_K(L')}(X_{L|K}(\sigma))$.*

Proof: This has essentially been proven on the previous pages: recall that

$$i_{K'_m}(\sigma) := \min_{x \in R'_m} \{\nu_{K'_m}(\sigma(x) - x) - 1\},$$

and similarly for $i_{X_K(L')}(X_{L|K}(\sigma))$. But for any $\hat{y} = (\hat{y}^{(n)})_n \in X_K(L')$, we have

$$\begin{aligned} \nu_{X_K(L')}(X_{L|K}(\sigma)(\hat{y}) - \hat{y}) &= \nu_{X_K(L')}((\sigma(\hat{y}^{(n)}))_n - (\hat{y}^{(n)})_n) \\ &:= \nu_{K'_m}([(\sigma(\hat{y}^{(n)}))_n - (\hat{y}^{(n)})_n]_{K'_m}) \\ &= \nu_{K'_m}(\sigma(\hat{y}^{(m)}) - \hat{y}^{(m)} + o(r'_m)) \\ &\geq \min\{\nu_{K'_m}(\sigma(\hat{y}^{(m)}) - \hat{y}^{(m)}), r'_m). \end{aligned}$$

Now $r'_m \to \infty$, so for $m >> 0$ and for any $\hat{y}$ not fixed by $X_K(L)(\sigma)$ we have

$$\nu_{X_K(L')}(X_{L|K}(\sigma)(\hat{y}) - \hat{y}) < r'_m,$$

which implies that

$$\nu_{X_K(L')}(X_{L|K}(\sigma)(\hat{y}) - \hat{y}) = \nu_{K'_m}(\sigma(\hat{y}^{(m)}) - \hat{y}^{(m)})$$

for $m >> 0$. It follows that $i_{X_K(L')}(X_{L|K}(\sigma)) \geq i_{K'_m}(\sigma)$. For the other inequality, choose $m >> 0$ so that $\nu_{K'_m}(\sigma(x_m) - x_m) < r'_m$ (this is possible by our previous computations). Then clearly $i_{K'_m}(\sigma) < r'_m$, and if $x \in K'_m$ is the element achieving the minimum value $i_{K'_m}(\sigma)$, lemma 4.0.8 says that

$$\nu_{X_K(L')}(X_{L|K}(\sigma)(\hat{x}) - \hat{x}) = \nu_{K'_m}(\sigma(x) - x) = i_{K'_m}(\sigma) + 1$$

for a suitably chosen $\hat{x} \in X_K(L'_m)$. It follows that

$$i_{X_K(L')}(X_{L|K}(\sigma)) \leq i_{K'_m}(\sigma),$$

so we have equality as claimed. □

Since the lower ramification filtration is determined by the function i, it follows that the isomorphism

$$\mathrm{Gal}(K'_m|K_m) \cong \mathrm{Gal}(L'|L) \cong \mathrm{Gal}(\mathcal{K}|X_K(L))$$

induced by $X_K(-)$ preserves the ramification filtrations. Since the degree of the different depends only on the ramification filtration, it follows that $d_s = d_m$ for $m >> 0$.

2): We now assume that G is abelian, but make no separability assumption on the special fiber $Y_k \to D_k$. Since G is abelian, the decomposition groups at the n_s primes of $\mathcal{A}_{(\varpi)}$ lying over $(\varpi) \in \mathrm{Spec}(R[[Z]])$ all coincide. Call this decomposition group $\mathcal{Z}$. Taking $\mathcal{Z}$-invariants, we observe that $Y^{\mathcal{Z}} \to D$ is a $G/\mathcal{Z}$-Galois regular branched cover with totally split special fiber:

$$F(Y_k^{\mathcal{Z}}) \cong \prod_{j=1}^{n_s} k((z)). \tag{4.0.2}$$

In particular, there is no more splitting in the special fiber $Y_k \to Y_k^{\mathcal{Z}}$. Moreover, the isomorphism (4.0.2) of $k((z))$-algebras is clearly defined over $\mathbb{F}_p((z))$, so we can apply part 1 with $l = 1$ to the cover $Y^{\mathcal{Z}} \to D$. We conclude that $n_m^{\mathcal{Z}} = n_s$ for $m >> 0$ (here $n_m^{\mathcal{Z}}$ is the number of components of $Y_{K,m}^{\mathcal{Z}}$). Since $Y_{K,m} \to Y_{K,m}^{\mathcal{Z}}$ is surjective, it follows that $n_m \geq n_m^{\mathcal{Z}} = n_s$ as claimed.

3): Note that by part 1, if $d_m \to \infty$, then the special fiber must be generically inseparable, without any irreducibility hypothesis or restriction on the group G.

Now suppose that Y_k is irreducible and $Y_k \to D_k$ is generically inseparable. Let V be the first ramification group at the unique prime of $\mathcal{A}$ lying over (ϖ). Taking V-invariants, we consider the tower

$$Y \to Y^V \to D.$$

Now V is a nontrivial p-group, and thus has a p-cyclic quotient. Hence $Y \to Y^V$ possesses a p-cyclic subcover, $W \to Y^V$, and we have the tower

$$Y \to W \to Y^V \to D.$$

Now consider the associated tower of special fibers

$$Y_k \to W_k \to Y_k^V \to D_k,$$

which corresponds (by considering the generic points) to a chain of field extensions

$$k((z)) \subset k((s)) \subset \mathcal{W} \subset \mathcal{K}.$$

Note that there is no extension of constants in this tower because the cover $Y \to D$ was assumed to be regular.

The extension $\mathcal{W}|k((s))$ is purely inseparable of degree p. Hence, there exists $x \in \mathcal{W}$ such that $x \notin k((s))$ but $x^p = s^a u \in k((s))$, where $a \in \mathbb{Z}$ and u is a unit in $k[[s]]$. Moreover, we may assume that u is a principle unit since k is perfect and we can always multiply this equation by a p-power. Similarly, we may assume that

$0 \leq a < p$. First take the case where $a \neq 0$. Then by Hensel's Lemma, u has an ath root in $k((s))$, call it v. Thus, $x^p = (sv)^a := \tilde{s}^a$, and $\tilde{s}$ is a uniformizer for $k((s))$. Now a generates the cyclic group $\mathbb{Z}/p\mathbb{Z}$, so there exists j with $0 < j < p$ such that $ja \equiv 1 \ (p)$. We get:

$$(x^j)^p = (x^p)^j = (\tilde{s}^a)^j = \tilde{s}^{ja} = \tilde{s}\tilde{s}^{rp}$$

for some $r \in \mathbb{Z}$. Dividing by $\tilde{s}^{rp}$ yields

$$\left(\frac{x^j}{\tilde{s}^r}\right)^p = \tilde{s}.$$

Note that $x^j \notin k((s))$ since the minimal polynomial of x over $k((s))$ has degree p. Hence, replacing x by $\frac{x^j}{\tilde{s}^r}$, we may assume that $x^p = \tilde{s} = sv$, so that x is the pth root of a uniformizer.

Now consider the case where $a = 0$ above, so that we have $x^p = u$, a principle unit in $k[[s]]$. Write $u = 1 + \sum_{i=1}^{\infty} \alpha_i s^i$ with $\alpha_i \in k$. Note that there exists i such that $(i,p) = 1$ and $\alpha_i \neq 0$. Indeed, if $u \in k[[s^p]]$, then u is a pth power in $k[[s]]$ and $(x - u^{\frac{1}{p}})^p = x^p - u = 0$, contradicting our assumption that Y_k is reduced. So let i_0 be the least i such that $(i,p) = 1$ and $\alpha_i \neq 0$. Then we have

$$u = 1 + \sum_{1 \leq j < \frac{i_0}{p}} \alpha_{jp} s^{jp} + s^{i_0} u'$$

for some unit u'. Then replacing x by $x - 1 - \sum_{1 \leq j < \frac{i_0}{p}} \alpha_{jp}^{\frac{1}{p}} s^j$ yields the equation

$$x^p = s^{i_0} u',$$

so that we are in the first case already considered.

Thus, we have shown that in any case, there exists $x \in \mathcal{W}$ such that $x \notin k((s))$ and $x^p = \tilde{s} = sv$, a uniformizer for $k((s))$. Replacing s by $\tilde{s}$, we may assume that $x^p = s$. Now let ξ be a lifting of x to the localized ring of global sections $\Gamma(W)_{(\varpi)}$. Then ξ is integral over $\mathcal{A}^V_{(\varpi)}$ and we let $F(T) \in \mathcal{A}^V_{(\varpi)}[T]$ be its minimal polynomial. By Nakayama's Lemma, the powers of ξ generate $\Gamma(W)_{(\varpi)}$ as an $\mathcal{A}^V_{(\varpi)}$-module, so $F(T)$ has degree p and we conclude that modding out by ϖ yields

$$\overline{F}(T) = (T^p - s).$$

Now let $S \in \mathcal{A}^V_{(\varpi)}$ be any lifting of $s \in k((s))$. Then we have

$$F(T) = T^p - S + \varpi H(T),$$

where $H(T) \in \mathcal{A}^V_{(\varpi)}[T]$ is of degree at most $p-1$.

The extension $k((s))|k((z))$ is totally ramified, so the minimal polynomial of s over $k((z))$ is Eisenstein:

$$g(T) = T^c + za_{d-1}(z)T^{c-1} + \cdots + za_1(z)T + zu(z) \in k[[z]][T],$$

where $u(z)$ is a unit. Again by Nakayama's Lemma, the powers of S generate $\mathcal{A}^V_{(\varpi)}$ as a $R[[Z]]_{(\varpi)}$-module, so the minimal polynomial of S, $G(T)$, is of degree c and we have

$$\overline{G}(T) = g(T).$$

Using the Teichmüller lifting $\tau : k[[z]] \to R[[Z]]$, we find that

$$\begin{aligned} G(T) &= \tau(g)(T) + \varpi P(Z,T) \\ &= T^c + Z\tau(a_{d-1})(Z)T^{c-1} + \cdots + Z\tau(u)(Z) + \varpi P(Z,T), \end{aligned}$$

for some polynomial $P(Z,T) \in R[[Z]]_{(\varpi)}[T]$ of degree at most $c-1$ in T.

Setting $Z = \pi_m$, we get the specialized polynomial

$$G_m(T) = T^c + \pi_m \tau(a_{d-1})(\pi_m)T^{c-1} + \cdots + \pi_m \tau(u)(\pi_m) + \varpi P(\pi_m, T),$$

which for $m >> 0$ is Eisenstein by the Ramification Argument applied to $\varpi P(\pi_m, T)$. Letting S_m denote the image of S in $F(Y^V_{K,m})$, it follows that $Y^V_{K,m}$ is irreducible for $m >> 0$ and S_m is a uniformizer for the field $F(Y^V_{K,m})$.

Now consider the polynomial $H(T) \in \mathcal{A}^V_{(\varpi)}[T]$, which has the form

$$H(T) = T^r + c_{r-1}T^{r-1} + \cdots + c_1 T + c_0,$$

where $r < p$. Now each coefficient $c_i \in \mathcal{A}^V_{(\varpi)}$ is integral over $R[[Z]]_{(\varpi)}$, say with minimal polynomial

$$p_i(T) = T^n + b_{n-1}(Z)T^{n-1} + \cdots b_0(Z) \in R[[Z]]_{(\varpi)}[T].$$

Setting $Z = \pi_m$ yields the specialized polynomial

$$p_{i,m}(T) = T^n + b_{n-1}(\pi_m)T^{n-1} + \cdots + b_0(\pi_m) \in K_m[T].$$

Now by the Ramification Argument, the coefficients of the polynomials $p_m(T)$ are bounded in absolute value independently of m. Hence, if $c_{i,m}$ denotes the image of the coefficient c_i in the field $F(Y^V_{K,m})$, then the absolute value of $c_{i,m}$ is bounded independently of m. Hence, for $m >> 0$, we see that

$$F_m(T) = T^p - S_m + \varpi H(T)_{Z=\pi_m}$$

is an Eisenstein polynomial over the field $F(Y_{K,m}^V)$, again by the Ramification Argument applied to $\varpi H(T)$.

We obtain the chain of field extensions

$$K_m \subset K_m(S_m) = F(Y_{K,m}^V) \subset K_m(S_m, \xi_m) = F(W_{K,m}) \subset K'_m$$

and note that ξ_m satisfies the Eisenstein polynomial $F_m(T)$ over $K_m(S_m)$.

Thus ξ_m is a uniformizer in the totally ramified extension $K_m(S_m, \xi_m)|K_m(S_m)$, so

$$\mathcal{D}(K_m(S_m, \xi_m)|K_m(S_m)) = (F'_m(\xi_m)) = (p\xi_m^{p-1} + \varpi H'(\xi_m)_{Z=\pi_m}).$$

But

$$\begin{aligned} \nu_{K_m(S_m,\xi_m)}(p\xi_m^{p-1} \quad + \quad & \varpi H'(\xi_m)_{Z=\pi_m}) \geq \\ & \min\{\nu_{K_m(S_m,\xi_m)}(p\xi_m^{p-1}), \nu_{K_m(S_m,\xi_m)}(\varpi H'(\xi_m)_{Z=\pi_m})\}, \end{aligned}$$

and the latter quantity goes to ∞ as m goes to ∞. By multiplicativity of the different in towers we conclude that

$$d_m \geq \nu_{K_m(S_m,\xi_m)}(\mathcal{D}(K_m(S_m, \xi_m)|K_m(S_m))),$$

so d_m goes to ∞ as m goes to ∞ as claimed. $\square$

Chapter 5

Arithmetic Form of the Oort Conjecture

Using Theorem 1, we deduce a new local lifting criterion for abelian extensions of $\overline{\mathbb{F}}_p((z))$. For this, consider a Lubin-Tate extension $L|K$ with $K = H\widehat{\mathbb{Q}_p^{un}}$ for some finite extension $H|\mathbb{Q}_p$. Then choose a uniformizer $\pi \in X_K(L)$, which defines an isomorphism $\overline{\mathbb{F}}_p((z)) \cong X_K(L)$ as well as a sequence of points $\{x_m\}_m \subset D_K$.

Proposition 5.0.10. *Suppose that G is a finite abelian group, and let $M|L$ be a G-Galois extension, corresponding to the G-Galois extension $X_K(M)|X_K(L)$ via the field of norms functor. Suppose that $Y \to D$ is a G-Galois regular branched cover with Y normal and Y_k reduced. Then $Y \to D$ is a smooth lifting of $X_K(M)|X_K(L)$ if and only if there exists $l > 0$ such that for $m >> 0$ and $m \equiv 1 \mod l$, we have $L_m = M$ as G-Galois extensions of L, and $d_m = d_\eta$.*

Proof: First suppose that $Y \to D$ is a smooth lifting of $X_K(M)|X_K(L)$. Then $Y_k \to D_k$ is generically separable, so by part 1 of Theorem 4.0.1 we see that $X_K(M) = X_K(L_m)$ and $d_m = d_s$ for $m >> 0$ and $m \equiv 1 \mod l$, for some $l > 0$. Since $X_K(-)$ is an equivalence of categories, we conclude that $M = L_m$ for these values of m. Moreover, by the local criterion for good reduction (see Introduction), we have $d_s = d_\eta$, which implies that $d_m = d_\eta$ for $m >> 0$ and $m \equiv 1 \mod l$, as claimed.

Now suppose that there exists $l > 0$ so that $L_m = M$ and $d_m = d_\eta$ for $m >> 0$ and $m \equiv 1 \mod l$. Then by part 2 of Theorem 4.0.1, Y_k is irreducible, and then by part 3, $Y_k \to D_k$ is generically separable. Hence we may apply part 1 to conclude that there exits $l_1 > 0$ such that $F(Y_k) = X_K(L_m)$ and $d_s = d_m$ for $m >> 0$ and $m \equiv 1 \mod l_1$. But the two arithmetic progressions $\{tl + 1\}_t$ and $\{tl_1 + 1\}_t$ have a common subsequence. It follows that $F(Y_k) = X_K(M)$ and $d_s = d_\eta$, so $Y \to D$ is a birational lifting of $X_K(M)|X_K(L)$ which preserves the different. By the local criterion for good reduction, it follows that $Y \to D$ is actually a smooth lifting. □

In particular, we obtain an "arithmetic reformulation" of the Oort Conjecture concerning the liftability of cyclic covers over an algebraically closed field k of characteristic p. For this, note that it suffices to prove the Oort Conjecture over the algebraic closure of a finite field, $k = \overline{\mathbb{F}}_p$, by standard techniques of model theory. So set $K = \widehat{\mathbb{Q}_p^{un}}$, and let $L = K(\zeta_{p^\infty})$. Then $L|K$ is Lubin-Tate for $H = \mathbb{Q}_p$ and $\Gamma = \widehat{\mathbb{G}_m}$. Finally, if C is a finite cyclic group, define $R_C := \mathcal{O}_K[\zeta_{|C|}] \subset \mathcal{O}_L$. Then we have the following "arithmetic form" of the Strong Oort Conjecture from the

Introduction:

Arithmetic Form of the Oort Conjecture: Suppose that $M|L$ is a finite cyclic extension of L, with group C. Then there exists a normal, C-Galois regular branched cover $Y \to D := \text{Spec}(R_C[[Z]])$ with Y_k reduced such that for some $l > 0$ we have:

1. $L_m = M$ for $m >> 0$ and $m \equiv 1 \mod l$;

2. $d_\eta = d_m$ for $m >> 0$ and $m \equiv 1 \mod l$.

Proposition 5.0.11. *The arithmetic form of the Oort Conjecture is equivalent to the Strong Oort Conjecture.*

Proof: This follows immediately from Proposition 5.0.10. □

Now we would like to give a direct proof of the arithmetic form of the Oort Conjecture for p-cyclic covers, and for this we need to make some preliminary observations. First note that $K_m := \text{Fix}(G(L|K)^m) = K(\zeta_{p^m})$, and therefore $[K_{m+1} : K_m] = p$ for $m \geq 1$. Moreover, by Proposition 3.2.3, the numbers $i(L|K_m) \to \infty$ as $m \to \infty$. But then by Proposition 3.2.2 we have

$$i(K_{m+1}|K_m) \geq i(L|K_m) \to \infty \quad \text{as} \quad m \to \infty.$$

Hence given any $N > 0$, there exists $m_0 >> 0$ such that for $m \geq m_0$, $K_{m+1}|K_m$ is a p-cyclic extension with $G(K_{m+1}|K_m)^N = G(K_{m+1}|K_m)$. In particular, if σ is a generator of $G(K_{m+1}|K_m)$, then

$$\nu_{m+1}(\sigma(\pi_{m+1}) - \pi_{m+1}) \geq \psi_{K_{m+1}|K_m}(N) + 1 > N$$

for any uniformizer $\pi_{m+1} \in K_{m+1}$.

Now suppose that $\pi = (\pi_m)$ is a uniformizer for $X_K(L)$, so that

$$N_{K_{m+1}|K_m}(\pi_{m+1}) = \pi_m$$

for all m. If $p_m(T)$ is the minimal polynomial of π_{m+1} over K_m, then we have

$$p_m(T) = T^p + a_1 T^{p-1} + \cdots + a_{p-1}T + (-1)^p \pi_m,$$

an Eisenstein polynomial.

Lemma 5.0.12. *For any $B > 0$, there exists $m_1 >> 0$ so that if $m \geq m_1$, the coefficients of $p_m(T) \in R_m[T]$ satisfy $\nu_m(a_i) \geq B$ for $i = 1, \ldots, p-1$.*

Proof: Given $B > 0$, set $N = pB$ and choose $m_1 >> 0$ so that $i(K_{m+1}|K_m) > N$ and $e_{m+1} > N$ for $m \geq m_1$, where e_m is the absolute ramification index of K_m. If we denote by $o(N+1)$ an element of R_{m+1} of valuation greater than or equal to $N+1$, then for any generator σ of $\mathrm{Gal}(K_{m+1}|K_m)$ we have

$$\begin{aligned} \pm a_i &= \sum_{j_1, j_2, \ldots, j_i, \text{distinct}} \sigma^{j_1}(\pi_{m+1}) \cdots \sigma^{j_i}(\pi_{m+1}) \\ &= \sum (\pi_{m+1} + o(N+1))^i \\ &= \sum (\pi_{m+1}^i + o(N+1)) \\ &= \binom{p}{i} \pi_{m+1}^i + o(N+1). \end{aligned}$$

Since $p | \binom{p}{i}$ for $i = 1, \ldots, p-1$, we find that

$$\nu_m(a_i) = \frac{1}{p}\nu_{m+1}(a_i) \geq \frac{1}{p}\min\{\nu_{m+1}(p) + i, N\} \geq \frac{1}{p}\min\{e_{m+1}, N\} = B. \ \square$$

In the course of our proof of the arithmetic form of the Oort Conjecture for p-cyclic covers, we will need a result about the stability of the ramification filtration under base change by subfields of an infinite APF extension $L|K$. Of course, the ramification filtration behaves badly in general under ramified base change, but in our situation we have the following

Proposition 5.0.13. *(*[17], 3.3.2*) Let σ be a K-automorphism of L. Then there exists a subfield $E \in \mathcal{E}_{L|K}$ such that for $E' \in \mathcal{E}_{L|E}$ we have $i_{E'}(\sigma) = i_{X_K(L)}(X_K(\sigma))$.*

To see how this gives the type of stability that we require, suppose that $M|L$ is a finite G-Galois extension, say defined over K_{m_0}. That is, there exists a G-Galois extension $K'_{m_0}|K_{m_0}$ such that $M = K'_{m_0}L$. Then $M|K$ is APF and any $\sigma \in G$ is a K-automorphism of M to which we may apply the proposition. Hence there exists $E \in \mathcal{E}_{M|K}$ such that for any finite extension $E'|E$ contained in M we have $i_{E'}(\sigma) = i_{X_K(L)}(X_K(\sigma))$. Moreover, by enlarging E we may assume that it contains K_{m_0} and works for all $\sigma \in G$. But $G(M|K'_{m_0}) \cong \mathbb{Z}_p$ is procyclic (since $L|K_{m_0}$ is), so there is a unique subextension of $M|K'_{m_0}$ of each p-power degree. But $K_{m+i}K'_{m_0}|K'_{m_0}$ is a subextension of degree p^i, so it follows that E coincides with one of them. Increasing m_0 if necessary, we may assume that $E = K'_{m_0}$. It now follows immediately from Proposition 5.0.13 that for $m \geq m_0$, the canonical isomorphism $G(K_mK'_{m_0}|K_m) \cong G(K'_{m_0}|K_{m_0})$ preserves the ramification filtrations on these groups. In particular, we see that for $m \geq m_0$, the conductor of $K_mK'_{m_0}|K_m$ is equal to the conductor of $K'_{m_0}|K_{m_0}$.

Theorem 5.0.14. *The arithmetic form of the Oort Conjecture holds for p-cyclic covers.*

Proof: Let $M|L$ be a p-cyclic extension, say defined by adjoining the pth root of a principle unit $u \in K_{m_0}$ (note that every such M is so defined if we take $m_0 >> 0$). Then $\tilde{K}_{m_0}|K_{m_0}$ is totally ramified, where $\tilde{K}_{m_0} = K_{m_0}(u^{\frac{1}{p}})$, since $k_{K_{m_0}} = k_K$ is algebraically closed. Moreover, take $m_0 >> 0$ so that the conductor of $\tilde{K}_{m_0}|K_{m_0}$ is stable under base change by $K_m|K_{m_0}$ (see remarks after Proposition 5.0.13). Then modifying u by a p-power in K_{m_0}, we have

$$u = 1 + \frac{\lambda^p}{\pi_{m_0}^c} v,$$

where v is a unit in K_{m_0}, $\lambda = \zeta_p - 1$, and $c + 1$ is the Artin conductor of $\tilde{K}_{m_0}|K_{m_0}$ (see [7] Proposition 1.6.3). Now choose $N > c$ and increase m_0 if necessary so that $\min\{r_{m_0}, \frac{e_{m_0}}{p-1}\} \geq N$.

By Proposition 3.3.3, there exists a unit $\hat{v} \in X_K(L)$ such that $\nu_{m_0}(\hat{v}_{K_{m_0}} - v) \geq r_{m_0} \geq N$. Hence we can write

$$u = 1 + \frac{\lambda^p}{\pi_{m_0}^c}(\hat{v}_{K_{m_0}} - (\hat{v}_{K_{m_0}} - v)) = 1 + \frac{\lambda^p \hat{v}_{K_{m_0}}}{\pi_{m_0}^c} w$$

where $w \in K_{m_0}$ is a unit of index at least N. Now $(c, p) = 1$, so by Hensel's Lemma $\hat{v}$ has a cth root in $X_K(L)$. Then replace the uniformizer $\pi = (\pi_m)$ by $\pi \hat{v}^{-\frac{1}{c}}$. Again calling this uniformizer π, we find that

$$u = 1 + \frac{\lambda^p}{\pi_{m_0}^c} w$$

where w is a unit of index at least N, say

$$w = 1 + b_1\pi_{m_0}^N + b_2\pi_{m_0}^{N+1} + \cdots ,$$

where the $b_i \in K$ are Teichmüller representatives. Now set $W = 1 + b_1Z^N + b_2Z^{N+1} + \cdots \in R[[Z]]^\times$ and consider the extension of normal rings $\mathcal{A} \mid R_1[[Z]]$ defined generically by the Kummer equation

$$T^p = 1 + \frac{\lambda^p}{Z^c}W.$$

Lemma 5.0.15. (compare [5], Proposition 1.4) $\mathcal{A}_s = \mathcal{A}/\lambda\mathcal{A}$ *is reduced.*

Proof: Let $S_0 = \widehat{R_1[[Z]]_{(\lambda)}}$ be the completion of the base ring at the special fiber, and suppose on the contrary that the extension of normal rings, $S|S_0$, defined generically by the equation $T^p = 1 + \frac{\lambda^p}{Z^c}W$ is totally ramified of degree p. Then $\lambda = B\omega^p$, where ω is a uniformizer for S and B is a unit in S. Now in S we have the factorization (where we set $V = \frac{W}{Z^c} \in S_0^\times$)

$$T^p - 1 = (T-1)(T-\zeta_p)\cdots(T-\zeta_p^{p-1}) = V\lambda^p.$$

But all factors in this product are (up to units) Galois-conjugate over S_0, and hence have the same valuation. It follows that

$$\nu_S(T-1) = \frac{1}{p}\nu_S(V\lambda^p) = \frac{1}{p}\nu_S(VB^p\omega^{p^2}) = p,$$

so $T = 1 + A\omega^p$ for some unit $A \in S$. Taking p-powers yields:

$$T^p = (1 + A\omega^p)^p = 1 + pA\omega^p + \cdots + A^p\omega^{p^2} = 1 + VB^p\omega^{p^2}.$$

Now $p = U\lambda^{p-1} = UB^{p-1}\omega^{p(p-1)}$, for some unit $U \in S_0$. Then considering the terms of valuation p^2 in the previous equation implies that

$$UB^{p-1}A + A^p \equiv VB^p \mod \omega.$$

Setting $X = \frac{A}{B}$, it follows that $\overline{V} = \overline{UX} + \overline{X}^p$ in $k_S = k_{S_0}$. But then $1 + V\lambda^p$ is a pth power in S_0. Indeed, lift $\overline{X}$ to a unit $X_0 \in S_0$ and compute

$$\begin{aligned}
(1 + V\lambda^p)(1 - X_0\lambda)^p &= (1 + V\lambda^p)(1 - pX_0\lambda + \cdots - X_0^p\lambda^p) \\
&= (1 + V\lambda^p)(1 - (UX_0 - X_0^p)\lambda^p + o(p+1)) \\
&= 1 + (V - UX_0 - X_0^p)\lambda^p + o(p+1) \\
&= 1 + o(p+1).
\end{aligned}$$

But any unit of index greater than $\nu_{S_0}(\lambda^p) = p$ in S_0 is a pth power, so $1 + V\lambda^p$ is a pth power in S_0 as claimed. But then $S = S_0$, contrary to our supposition. Hence $S/\lambda S$ is reduced, which implies the same for $\mathcal{A}_s$. □

Setting $\tilde{T} = TZ^c$ yields the integral equation

$$\tilde{T}^p = Z^{cp} + \lambda^p Z^{(p-1)c}W = Z^{(p-1)c}(Z^c + W\lambda^p).$$

The right hand side has zeros where $Z = 0$ and where $\left(\frac{Z^c}{W}\right) = \left(\frac{Z}{W^{\frac{1}{c}}}\right)^c = \lambda^p$, which gives $c+1$ points each having ramification index p in the cover. It follows that the degree of the generic different is $d_\eta = (c+1)(p-1)$.

On the other hand, specializing the equation at $Z = \pi_m$ yields

$$T^p = 1 + \frac{\lambda^p}{\pi_m^c}W(\pi_m),$$

and so all of the specializations $K'_m|K_m$ are field extensions having Artin conductor $c+1$, hence degree of different $d_m = (c+1)(p-1) = d_\eta$. Thus, from Theorem 1 the special fiber is separable and irreducible, and we have $d_\eta = d_s$. Hence, the lifting is smooth, and we just need to verify that $M = K'_m L$ for all $m >> 0$. But we have fixed things so that at level m_0 we have $K'_{m_0} = \tilde{K}_{m_0}$, hence $M = \tilde{K}_{m_0} L = K'_{m_0} L$. Now for $m > m_0$, the extension $K'_m|K_m$ is defined by adjoining a pth root of $1 + W(\pi_m)\frac{\lambda^p}{\pi_m^c}$, so by Kummer Theory, it suffices to show that

$$(1 + W(\pi_m)\frac{\lambda^p}{\pi_m^c})(1 + W(\pi_{m+1})\frac{\lambda^p}{\pi_{m+1}^c})^{-1}$$

is a pth power in L.

For ease of notation, set $u_m = W(\pi_m)$, a unit of index at least N in K_m. Thus, we wish to show that

$$(1 + u_m\frac{\lambda^p}{\pi_m^c})(1 + u_{m+1}\frac{\lambda^p}{\pi_{m+1}^c})^{-1}$$

is a pth power in L. In fact, I claim that

$$(1 + u_m\frac{\lambda^p}{\pi_m^c})(1 + u_{m+1}\frac{\lambda^p}{\pi_{m+1}^c})^{-1}(1 - \frac{\lambda}{\pi_{m+1}})^p$$

is a pth power in K_{m+1}.

By Lemma 5.0.12 concerning the minimal polynomial of π_{m+1} over K_m we have

$$(-1)^{(p-1)}\pi_m = \pi_{m+1}^p + \sum_{i=1}^{p-1} a_i \pi_{m+1}^{p-i} = \pi_{m+1}^p(1 + \sum_{i=1}^{p-1} \frac{a_i}{\pi_{m+1}^i}),$$

and we may assume $\nu_{m+1}(\frac{a_i}{\pi_{m+1}^i}) \geq pN$ for each i.

Note that any principal unit in K_m of index greater than $\nu_m(\lambda^p)$ is a pth power in K_m. Since our goal is to show that something is a pth power, we only need to keep track of enough terms to determine the index in our computation. So we compute (here $o(-)$ refers to the valuation $\nu_{K_{m+1}}$):

$$\begin{aligned}(1+u_m\frac{\lambda^p}{\pi_m^c}) &= 1+(-1)^{p-1}\frac{(1+o(pN))\lambda^p}{\pi_{m+1}^{cp}(1+o(pN))}\\ &= 1+(-1)^{p-1}\frac{\lambda^p}{\pi_{m+1}^{cp}}(1+o(pN)).\end{aligned}$$

Multiplying by a pth power we get

$$\begin{aligned}(1+u_m\frac{\lambda^p}{\pi_m^c})(1-\frac{\lambda}{\pi_{m+1}^c})^p &= (1+(-1)^{p-1}\frac{\lambda^p}{\pi_{m+1}^{cp}}(1+o(pN))\cdot\\ &\quad (1+(-1)^p\frac{\lambda^p}{\pi_{m+1}^{cp}}-\frac{p\lambda}{\pi_{m+1}^c}(1+o(\frac{e_{m+1}}{p-1}-c)))\\ &= 1-\frac{p\lambda}{\pi_{m+1}^c}(1+o(pN-c(p-1))).\end{aligned}$$

Finally, we compute

$$\begin{aligned}(1+u_{m+1}\frac{\lambda^p}{\pi_{m+1}^c})^{-1}(1+u_m\frac{\lambda^p}{\pi_m^c})(1-\frac{\lambda}{\pi_{m+1}^c})^p &=\\ (1-\frac{\lambda^p}{\pi_{m+1}^c}(1+o(N)))(1-\frac{p\lambda}{\pi_{m+1}^c}(1+o(pN-c(p-1))) &=\\ 1-\frac{\lambda^p+p\lambda}{\pi_{m+1}^c}+\lambda^p o(N-c),\end{aligned}$$

and this unit has index greater than $\nu_{m+1}(\lambda^p)$. Indeed, the last term has valuation greater than $\nu_{m+1}(\lambda^p)$ by our choice of N. For the second term, note that

$$0=(\lambda+1)^p-1=\lambda^p+p\lambda+p\lambda^2o(0).$$

It follows that

$$
\begin{aligned}
\nu_{m+1}(\frac{\lambda^p + p\lambda}{\pi_{m+1}^c}) &\geq \nu_{m+1}(p\lambda^2) - c \\
&= e_{m+1} + 2\frac{e_{m+1}}{p-1} - c \\
&= \nu_{m+1}(\lambda^p) + \frac{e_{m+1}}{p-1} - c \\
&\geq \nu_{m+1}(\lambda^p) + N - c > \nu_{m+1}(\lambda^p).
\end{aligned}
$$

Hence, $K'_{m+1} = K'_m K_{m+1}$, which implies that $K'_m L = K'_{m_0} L = \tilde{K}_{m_0} L = M$, as required. This completes the proof of the p-cyclic case of the arithmetic form of the Oort Conjecture. □

Appendix A

Computing the Different From Witt Vectors

In the course of this thesis, we have seen the importance of preserving the different in the lifting process. This raises the question of how to compute the different of a p^n-cyclic extension of a local field of characteristic p. The answer to this question involves the relationship between Artin-Schreier-Witt theory and local class field theory. This relationship is the subject of L. Brylinski's paper [3], which we describe here.

In this section, $K = k((t))$, where k is a finite field of characteristic $p > 0$. Then Artin-Schreier-Witt theory says that p^n-cyclic extensions of K are classified by Witt vectors of length n:

$$W_n(K)/(F-1)W_n(K) \cong \mathrm{Hom}(G_K^{ab}/p^n, \mathbb{Z}/p^n\mathbb{Z}).$$

On the other hand, the reciprocity homomorphism of local class field theory ϕ_K : $K^* \to G_K^{ab}$ induces an isomorphism

$$K^*/(K^*)^{p^n} \cong G_K^{ab}/p^n,$$

and the unit filtration $\{U_K^{(r)}\}$ on K^* corresponds under ϕ_K to the ramification filtration $\{G_K^{ab,r}\}$ of G_K^{ab} in the upper numbering. Combining these two isomorphisms yields a non-degenerate bilinear form

$$K^*/(K^*)^{p^n} \otimes W_n(K)/(F-1)W_n(K) \longrightarrow \mathbb{Z}/p^n\mathbb{Z}. \qquad (*)$$

Recall that the Artin conductor of an abelian extension $L \mid K$ is defined to be the least positive integer $f = f_{L/K}$ such that $\phi_{L/K}(U_K^{(f)}) = 0$, or equivalently such that $U_K^{(f)} \subset N_{L/K}(U_L)$. In terms of the ramification filtration on $\mathrm{Gal}(L/K)$, the Artin conductor is the least positive integer $f = f_{L/K}$ such that $\mathrm{Gal}(L/K)^f = 0$. Starting from the Hilbert formula for the degree of the different of $L \mid K$ ([15] Ch. IV, Prop. 4), a straightforward computation yields the following relation between the different and conductor:

Proposition A.0.16. *Given a p^n-cyclic totally ramified extension $L \mid K$, let $L_i \mid K$ be the subextension of degree p^i. Then*

$$d_{L/K} := \nu_L(\mathcal{D}_{L/K}) = \sum_{i=1}^{n}(f_{L_i/K} - f_{L_{i-1}/K})p^{i-1}(p^{n-i+1}-1) \qquad (f_{L_0/K} := 0).$$

Our goal is to compute $d_{L/K}$ directly from the Witt vector classifying L/K. By the above formula, this amounts to computing the Artin conductor $f_{L/K}$, which by definition is determined by the unit filtration on $K^*/(K^*)^{p^n}$. Hence, our task is to compute the dual filtration on $W_n(K)/(F-1)W_n(K)$ with respect to the bilinear form $(*)$. Brylinski accomplishes this in [3] using Kato's residue homomorphism in Milnor K-theory.

Definition A.0.17. For each $m \in \mathbb{Z}$, let

$$W_n^{(m)}(K) = \{(x_0, \ldots, x_{n-1}) \in W_n(K) \mid p^{n-i-1}\nu(x_i) \geq m,\ 0 \leq i < n\}.$$

Proposition A.0.18. ([3], Proposition 1) *$\{W_n^{(m)}(K)\}_{m\in\mathbb{Z}}$ forms a decreasing filtration of $W_n(K)$ by subgroups which is exhaustive and separated. The quotient group $W_n^{(m)}(K)/W_n^{(m+1)}(K)$ is generated by elements of the form*

$$(0, \ldots, 0, \lambda t^{p^{i-n+1}m}, 0, \ldots, 0)$$

where $0 \leq i < n$ ranges over all values such that $\frac{m}{p^{n-i-1}} \in \mathbb{Z}$, the nonzero entry is in the ith place, and $\lambda \in k$. Endowing the quotient group $W_n(K)/(F-1)W_n(K)$ with the quotient filtration $\{W_n^{(m)}(K) \mathrm{mod}(F-1)\}$, we have:

$$\begin{aligned}
W_n^{(m)}(K)\mathrm{mod}(F-1)/W_n^{(m+1)}(K)\mathrm{mod}(F-1) &= 0 \qquad \textit{for } m > 0 \\
W_n^{(0)}(K)\mathrm{mod}(F-1)/W_n^{(1)}(K)\mathrm{mod}(F-1) &\cong [k/(F-1)k]^n \\
W_n^{(m)}(K)\mathrm{mod}(F-1)/W_n^{(m+1)}(K)\mathrm{mod}(F-1) &\cong \\
\begin{cases} 0 & \textit{if } \nu_p(m) \geq n \\ k & \textit{if } \nu_p(m) = n-i-1,\ i \geq 0 \end{cases} & \qquad \textit{for } m < 0.
\end{aligned}$$

Moreover, in the case $m < 0$, when the quotient group is nonzero, the isomorphism with k is given by

$$\lambda \mapsto \overline{(0, \ldots, 0, \lambda t^{p^{i-n+1}m}, 0, \ldots, 0)}.$$

We are now ready to state Brylinski's

Theorem A.0.19. ([3], Theoreme 1) *For the bilinear form $(*)$, the right annihilator of $\overline{U_K^{(m)}}$ is $W_n^{(-m+1)}(K)\mathrm{mod}(F-1)$ for all $m > 0$.*

Unfortunately, the corollary to this result stated by Brylinski is not quite true. Since this corollary computes the Artin conductor of $L \mid K$ in terms of the classifying Witt vector, we take this opportunity to introduce the concept necessary to fix Brylinksi's statement.

Definition A.0.20. A Witt vector of length n, say $(x_0, \ldots, x_{n-1}) \in W_n(K)$, is *minimal* if and only if for $i = 0, \ldots, n-1$ the following implication holds:

$$\min\{p^i\nu(x_0), p^{i-1}\nu(x_1), \ldots, \nu(x_i)\} = m_i \Rightarrow (x_0, \ldots, x_i) \notin W_{i+1}^{(m_i+1)} mod(F-1).$$

Minimality ensures that modding out by the image of the Artin-Schreier-Witt transformation $F - 1$ doesn't change which piece of the filtration a Witt vector belongs to. The next proposition gives a nice condition guaranteeing minimality. Before stating it, however, we need another

Definition A.0.21. A Witt vector $(x_0, \ldots, x_{n-1}) \in W_n(K)$ is *essentially prime-to-p* if and only if for all i we have

$$\min\{p^i\nu(x_0), p^{i-1}\nu(x_1), \ldots, \nu(x_i)\} = p^{i-j}\nu(x_j) \Rightarrow p \not| \nu(x_j).$$

In other words, if a minimum is ever attained at a certain component, then that component has valuation prime to p.

Proposition A.0.22. *If* $x = (x_0, \ldots, x_{n-1}) \in W_n(K)$ *is essentially prime-to-p and* $\nu(x_0) < 0$*, then* x *is minimal.*

Proof: We proceed by induction on the length n. For the case $n = 1$, suppose that $\nu(x_0) = m_0 < 0$ and $(m_0, p) = 1$. The first condition implies that the image of x_0 is nonzero in $W_1^{(m_0)}(K)/W_1^{(m_0+1)}(K)$. We wish to show that $\overline{x_0}$ is still nonzero in $W_1^{(m_0)}(K)\text{mod}(F-1)/W_1^{(m_0+1)}(K)\text{mod}(F-1)$. But since $m_0 < 0$ is prime to p, both of these groups are isomorphic to k by Brylinski's proposition, hence isomorphic to each other. Thus $\overline{x_0}$ is nonzero.

Now suppose that the claim holds for length $n-1 > 0$, and consider an essentially prime-to-p Witt vector of length n: $x = (x_0, \ldots, x_{n-1})$. By the induction hypothesis, the Witt vector $(x_0, \ldots, x_{n-2}) \in W_{n-1}(K)$ is minimal. So all we need to show is that $\overline{x}$ is nonzero in

$$W_n^{(m_{n-1})}(K)\text{mod}(F-1)/W_n^{(m_{n-1}+1)}(K)\text{mod}(F-1),$$

where $m_{n-1} = \min\{p^{n-1}\nu(x_0), \ldots, \nu(x_{n-1})\}$. This is equivalent to the statement that for all $a \in W_n(K)$, setting $\alpha = x + (F-1)(a)$ yields

$$\min\{p^{n-1}\nu(\alpha_0), \ldots, \nu(\alpha_{n-1})\} \leq m_{n-1}.$$

Since $(x_0, \ldots, x_{n-2})$ is minimal, we know that

$$\begin{aligned}\min\{p^{n-1}\nu(\alpha_0), \ldots, \nu(\alpha_{n-1})\} &\leq \min\{p^{n-1}\nu(\alpha_0), \ldots, p\nu(\alpha_{n-2})\} \\ &\leq \min\{p^{n-1}\nu(x_0), \ldots, p\nu(x_{n-2})\}.\end{aligned}$$

Thus, we are done unless $\nu(x_{n-1}) < \min\{p^{n-1}\nu(x_0), \ldots, p\nu(x_{n-2})\}$. So suppose that this inequality holds. Then by essentially prime-to-p, p does not divide $m_{n-1} = \nu(x_{n-1})$. Then again by Brylinski's proposition, we have the isomorphisms

$$\begin{aligned}W_n^{(m_{n-1})}(K)\text{mod}(F-1)/W_n^{(m_{n-1}+1)}(K)\text{mod}(F-1) &\cong k \\ &\cong W_n^{(m_{n-1})}(K)/W_n^{(m_{n-1}+1)}(K).\end{aligned}$$

Since the image of x in the last group is nonzero by definition, it follows that $\overline{x}$ is nonzero in the first group as well. This shows that x is minimal as claimed. □

Now that we have the notion of minimality, we can correctly state the corollary to Brylinski's theorem:

Corollary A.0.23. *Suppose that $(x_0, \ldots, x_{n-1}) \in W_n(K)$ is minimal with $\nu(x_0) < 0$, and for $1 \leq i \leq n$ let $L_i \mid K$ be the p^i-cyclic subextension of the corresponding totally ramified p^n-cyclic extension $L \mid K$. Then for each i the Artin conductor of $L_i \mid K$ is given by*

$$f_{L_i/K} = -m_{i-1} + 1 = -\min\{p^{i-1}\nu(x_0), \ldots, \nu(x_{i-1})\} + 1.$$

Putting this together with our earlier formula for the different yields

$$d_{L/K} = \sum_{i=0}^{n-1}(m_{i-1} - m_i)p^i(p^{n-i} - 1),$$

where as always $m_i = \min\{p^i\nu(x_0), \dots, \nu(x_i)\}$ and we set $m_{-1} = 1$. Note that this formula only holds for minimal Witt vectors. This is enough to calculate the different for any p^n-cyclic extension $L \mid K$, since we can always choose a classifying Witt vector that is prime-to-p.

Bibliography

[1] Bertin, J., Mézard, A. *Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques*. Invent. math. **141**, pp.195-238 (2000).

[2] Bourbaki, N. *Commutative Algebra: Chapters 1-7*. Springer-Verlag, 1989.

[3] Brylinski, L. *Théorie du corps de classes de Kato et revêtements abéliens de surfaces*. Ann. de l'inst. Fourier **33**, 3, pp.23-38 (1983).

[4] Coleman, R.F. *Division Values in Local Fields*. Invent. math. **53**, pp.91-116 (1979).

[5] Epp, H.P. *Eliminating Wild Ramification*. Invent. math. **19**, pp. 235-249 (1973).

[6] Garuti, M. *Prolongement de revêtements Galoisiens en géometrie rigide*. Comp. math. **104**, pp.305-331 (1996).

[7] Gras, G. *Class Field Theory: From Theory to Practice*. Springer-Verlag, 2003.

[8] Green, B., Matignon, M. *Liftings of Galois covers of smooth curves*. Comp. math. **113**, pp.237-272 (1998).

[9] Grothendieck, A. *Revêtements étale et groupe fondamental*, SGA I. Lecture Notes in Math. **224**, Springer-Verlag, 1971.

[10] Kato, K. (with collaboration of T. Saito). *Vanishing cycles, ramification of valuations, and class field theory*. Duke math. **55**, 3, pp.629-659 (1987).

[11] Neukirch, J. *Algebraic Number Theory*. Springer-Verlag, 1999.

[12] Oort, F. *Some questions in algebraic geometry*. Manuscript (1995). www.math.uu.nl/people/oort/

[13] Oort F., Sekiguch, T., Suwa, N. *On the deformation of Artin-Schreier to Kummer*. Ann. scient. Éc.Norm. Sup., 4^e série, t. **22**, pp. 345-375 (1989).

[14] Pagot, G. *Relèvement en caractéristique zéro d'actions de groupes abéliens de type* $(p, \cdots, p)$. Ph.D. thesis, Université Bordeaux 1, 2002.

[15] Serre, J.P. *Corps Locaux*. Hermann, Paris, 1962.

[16] Wewers, S., Bouw, I. *The local lifting problem for dihedral groups*. arxiv.org/math.AG/0409395.

[17] Wintenberger, J.P. *Le corps des normes de certaines extensions infinies de corps locaux; applications*. Ann. scient. Éc. Norm. Sup., 4^e série, t. **16**, pp. 59-89 (1983).