CLASSIFYING EXTENSIONS OF THE FIELD OF FORMAL LAURENT SERIES OVER $\mathbb{F}_p$

ALFEEN HASMANI, LINDSEY HILTNER, ANGELA KRAFT, AND DANIEL SCOFIELD

Abstract. In previous works, Jones and Roberts have studied finite extensions of the p-adic numbers $\mathbb{Q}_p$. In this paper, we extend the results of Jones and Roberts regarding finite extensions of $\mathbb{Q}_p$ to the setting of local fields with characteristic p. In particular we are able to produce analogous results to Jones and Roberts in the case that the characteristic does not divide the degree of the field extension. Also in this case, following from the work of Pauli and Roblot, we prove the defining polynomials of these extensions can be written in a certain form. Furthermore, if p divides the degree of the extension, we show there are infinitely many extensions of this degree and thus cannot be classified in the same manner.

1. Introduction

Classifying extensions of $\mathbb{Q}_p$ has been of interest for many years. Pauli and Roblot [14] describe a method for computing defining polynomials for all extensions of $\mathbb{Q}_p$ of a given degree. Jones and Roberts [9] constructed an online database that identifies degree n extensions of $\mathbb{Q}_p$ for small values of p and n. They describe how to compute various invariants for each extension, including the Galois group.

In a similar fashion, we extend these results to characteristic p local fields, focusing on the unramified, totally tamely ramified, and totally wildly ramified cases. We begin by introducing the reader to essential background topics such as Galois theory, local field theory, the p-adic numbers, the field of formal Laurent series, and ramification groups.

We follow the work of Jones and Roberts [9] in the unramified case. In particular, we rely on Hensel's Lemma to show the existence and uniqueness of degree f unramified extensions with a brief word about the Galois groups of these extensions. We then explore totally tamely ramified extensions. Here we focus on the class of defining polynomials for these extensions, namely a specific type of Eisenstein polynomial. This type of polynomial arises from the work of Pauli and Roblot [14] and is shown to apply to extensions of characteristic p local fields. In the totally wildly ramified case, our results for degree p extensions are not analogous to the case of characteristic 0 local fields, as there are infinitely many degree p extensions. Finally, we conclude with an example, classifying an extension of $\mathbb{F}_p((T))$ to put our results in context.

Date: August 25, 2012.

The authors would like to thank their faculty advisor Dr. Jim Brown and graduate student advisor Kirsti Wash for all of their help, support, and patience on this project. We would also like to thank Dr. Mohammed Tesemma, Dr. Kevin James, and Dr. Neil Calkin as well as graduate students Rodney Keaton, Dania Zantout and Janine Janoski for their assistance throughout the Clemson University REU. This research was supported by NSF grant number 1156761.

2. Background

2.1. Basic Galois Theory Definitions.

Definition 2.1. Let L/K be a finite field extension. An automorphism of L/K is defined to be an automorphism of L that fixes the elements of K. That is, an automorphism of L/K is an isomorphism σ from L to L such that $\sigma(x) = x$, for all $x \in K$.

The set of automorphisms form a group under function composition, which is denoted $\mathrm{Aut}(L/K)$.

Definition 2.2. The **mass** of L/K is defined as $m(L) = \frac{[L:K]}{|\mathrm{Aut}(L/K)|}$. If $m(L) = 1$, then L is called a **Galois extension** and $\mathrm{Aut}(L/K)$ is called the **Galois group** of L, denoted $\mathrm{Gal}(L/K)$.

The following statements are equivalent:

- L/K is a Galois extension;
- L/K is a normal and separable extension;
- L is the splitting field of a separable polynomial with coefficients in K;
- $[L : K] = |\mathrm{Aut}(L/K)|$.

For more information on Galois theory and field theory, see [6].

2.2. Local Fields.

In order to define a local field, we first introduce the following concepts.

Definition 2.3. Given a field F, a function $|\cdot| : F \to \mathbb{R}_{\geq 0}$ is called an **absolute value** if for all $x, y \in F$ we have:

(1) $|x| \geq 0$ where equality holds if and only if $x = 0$,
(2) $|xy| = |x||y|$,
(3) $|x + y| \leq |x| + |y|$.

Example 2.4. The usual absolute value on the real numbers has the above properties.

Example 2.5. The Euclidean distance for $\mathbf{x} = (x_1, x_2, ..., x_n) \in \mathbb{R}^n$, which is defined as $|\mathbf{x}| = \sqrt{x_1^2 + x_2^2 + ... + x_n^2}$, is an absolute value on $\mathbb{R}^n$.

Example 2.6. We can define additional absolute values on the rational numbers $\mathbb{Q}$. Given a prime number p and a rational number $x = p^m \frac{r}{s}$ where $m, r, s \in \mathbb{Z}$ and r, s are coprime to p, we define a function on the rational numbers to be $|x|_p = p^{-m}$ where $|0|_p = 0$. This function is called the p-adic absolute value. To check if this function is indeed an absolute value, we must check that properties (1)-(3) hold. Clearly, $|x| \geq 0$ regardless of the value of m. Thus (1) is satisfied. To see (2), let $x = p^{m_1} \frac{r_1}{s_1}$ and let $y = p^{m_2} \frac{r_2}{s_2}$ be elements of $\mathbb{Q}$. Then

$$\begin{aligned} |xy|_p &= \left| p^{m_1} \frac{r_1}{s_1} p^{m_2} \frac{r_2}{s_2} \right|_p = \left| p^{m_1+m_2} \frac{r_1 r_2}{s_1 s_2} \right|_p \\ &= p^{-m_1-m_2} = p^{-m_1} p^{-m_2} = \left| p^{m_1} \frac{r_1}{s_1} \right|_p \left| p^{m_2} \frac{r_2}{s_2} \right|_p \\ &= |x|_p |y|_p. \end{aligned}$$

To check that (3) holds, let x, y be defined as above. Assume without loss of generality that $|x|_p \geq |y|_p$. This implies that $m_1 \leq m_2$. Then

$$\begin{aligned} |x+y|_p = \left| p^{m_1}\frac{r_1}{s_1} + p^{m_2}\frac{r_2}{s_2} \right|_p &= \left| \frac{p^{m_1} r_1 s_2 + p^{m_2} r_2 s_1}{s_1 s_2} \right|_p \\ &= \left| p^{m1} \frac{r_1 s_2 + p^{m_2 - m_1} r_2 s_1}{s_1 s_2} \right|_p \\ &\leq p^{-m_1} = \left| p^{m_1}\frac{r_1}{s_1} \right|_p = |x|_p \end{aligned}$$

which we assumed was equal to the maximum of $\{|x|_p, |y|_p\}$ and thus $|x+y|_p \leq |x|_p \leq |x|_p + |y|_p$ and property (3) holds. Therefore, the function $|\cdot|_p$ is an absolute value.

Note that for property (3), a stronger condition holds. The absolute value is said to be **non-Archimedean** if it satisfies this stronger condition that $|x+y| \leq \max\{|x|, |y|\}$ for all x, y in a field F. The usual absolute value and the Euclidean distance do not satisfy this additional property, but clearly the p-adic absolute value does, so we call it a non-Archimedean absolute value.

Definition 2.7. A **valuation** on a field F is a function $\nu : F \to \mathbb{R} \cup \{\infty\}$ such that

(1) $\nu(x) = \infty$ if and only if $x = 0$,
(2) $\nu(xy) = \nu(x) + \nu(y)$,
(3) $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$.

We say ν is a **discrete valuation** if $\nu : F \to \mathbb{Z} \cup \{\infty\}$. This function behaves on a non-Archimedean absolute value as a logarithm behaves on an exponential function. In terms of the p-adic absolute value and a rational number $x = p^m \frac{r}{s}, p \nmid rs$, we have

$$\nu_p(x) = m \qquad \text{and} \qquad |x|_p = p^{-\nu_p(x)}.$$

In this sense, the p-adic valuation provides a measure of how divisible the element is by the prime p. Although the focus of this project is on local fields equipped with a slightly different absolute value, a basic understanding of the p-adic absolue value is essential in what follows. For more information on the p-adic numbers, see [8].

Definition 2.8. Suppose R is a commutative ring and m is its maximal ideal. The **residue field** of R is the quotient ring R/m.

Let K be a field with valuation ν_K. Then we define the ring of integers

$$\mathcal{O}_K = \{x \in K | \nu_K(x) \geq 0\}.$$

Note that K is the field of fractions of $\mathcal{O}_K$. Within $\mathcal{O}_K$, we have

$$\mathcal{U}_K = \{x \in K | \nu_k(x) = 0\},$$

and

$$\mathcal{M}_K = \{x \in K | \nu_k(x) > 0\}.$$

Theorem 2.9. $\mathcal{M}_K$ is the unique maximal ideal of $\mathcal{O}_K$, and $\mathcal{U}_K$ is the group of units.

Proof. Let ν represent ν_K. First, we show that $\mathcal{M}_K$ is an ideal. Let $x, y \in \mathcal{M}_K$. Then, $\nu(x+y) \geq \min\{\nu(x), \nu(y)\} > 0$, hence $x+y \in \mathcal{M}_K$. If $x \in \mathcal{O}_K$ and $y \in \mathcal{M}_K$, then $\nu(xy) = \nu(x) + \nu(y) > 0$ and $xy \in \mathcal{M}_K$. Thus it follows that $\mathcal{M}_K$ is an ideal.
We next show that $\mathcal{U}_K = \mathcal{O}_K - \mathcal{M}_K$ consists of all the units of $\mathcal{O}_K$, thereby proving that $\mathcal{M}_K$ is the unique maximal ideal of $\mathcal{O}_K$ since for $\mathcal{M}_K$ to be larger, it would include a unit which would automatically make it equal to $\mathcal{O}_K$. For this, let $x \in \mathcal{U}_K$. Then the identity element $1_K \in \mathcal{U}_K$ since $\nu(1_K) = 0$ so all that remains to be shown is the existence of inverses. Since $x \in \mathcal{U}_K$, the there exists $x^{-1} \in K$ such that $\nu(x^{-1}) + \nu(x) = \nu(1) = 0$. Thus $\nu(x^{-1}) = 0$ and we have $x^{-1} \in \mathcal{U}_K$. Thus $\mathcal{U}_K$ is a group under multiplication. Since each $x \in \mathcal{U}_K$ has a multiplicative inverse, each $x \in \mathcal{U}_K$ is a unit. We call $\mathcal{U}_K$ the group of units and $\mathcal{M}_K$ the unique maximal ideal. □

Definition 2.10. A **local field** is a field which is complete with respect to a discrete, non-Archimedean valuation and whose residue field is finite.

Note that the quotient $k = \mathcal{O}_K/\mathcal{M}_K$ is the residue field of K.

Definition 2.11. A **principal ideal domain** is an integral domain in which every ideal is generated by a single element. In other words, every ideal is principal.

Theorem 2.12. If ν_K is discrete then $\mathcal{O}_K$ is a principal ideal domain.

Proof. Let $\nu : \mathcal{O}_K \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ be the discrete valuation restricted to $\mathcal{O}_K$. Let I be a non-zero ideal of $\mathcal{O}_K$. Then since $\mathbb{Z}_{\geq 0}$ is well ordered, we can choose $a \in I$ such that $\nu(a)$ is minimum. We claim that $I = (a)$. Let $x \in I$ and write $\nu(x) = \nu(a)q + r$ where $q \in \mathbb{N}$ and $0 \leq r < \nu(a)$. Now consider $xa^{-1} \in K$,

$$\begin{aligned} \nu(xa^{-1}) &= \nu(x) + \nu(a^{-1}) \\ &= \nu(x) - \nu(a) \\ &\geq \nu(x) - q\nu(a) \\ &= r \geq 0 \end{aligned}$$

Thus $xa^{-1} \in \mathcal{O}_K$ and we can fix $y = xa^{-1} \in \mathcal{O}_K$. Then $x = ay$ and therefore $I = (a)$ and $\mathcal{O}_K$ is a principal ideal domain. □

Since $\mathcal{M}_K \subset \mathcal{O}_K$, $\mathcal{M}_K$ is also principal.

Definition 2.13. A **discrete valuation ring** is a principal ideal domain with exactly one non-zero maximal ideal.

Theorem 2.14. $\mathcal{O}_K$ is a discrete valuation ring.

Proof. This is clear from 2.9 and 2.12. □

Definition 2.15. Any element $\pi_K \in K$ which generates $\mathcal{M}_K$ is called a **uniformizer** of K. Note $\nu_K(\pi_K) = 1$.

Note that all the ideals in K have the form (π_K^j) for some j. To see this, first recall $\mathcal{O}_K$ is a principal ideal domain. Also, recall every non-unit element of $\mathcal{O}_K$ is an element of $\mathcal{M}_K$. Thus, every ideal is a subset of $\mathcal{M}_K$. This requires those ideals to be generated by a power of π_K, the generator of $\mathcal{M}_K$.

Given a field K with an absolute value $|\cdot|_K$ and a finite extension L/K of degree n, one can extend the absolute value of K to a absolute value on L in the following way: for any $x \in L$,

$$|x|_L = |\,\mathrm{N}_{L/K}(x)|^{\frac{1}{n}}$$

where $\mathrm{N}_{L/K}(x)$ is a norm from L to K, that is, it maps the elements in L to K in such a way that the absolute value on K is preserved. There are three ways to compute the norm from L to K as described in [8, p.145]:

(1) For an element $\alpha \in L$, take L as a finite-dimensional K vector space and consider the K-linear map from L to L given by multiplication by α. Since multiplication by α is linear, it corresponds to a matrix. Define $\mathrm{N}_{L/K}(\alpha)$ to be the determinant of this matrix.
(2) For an element $\alpha \in L$, consider the subextension $K(\alpha)$. Let $r = [L : K(\alpha)]$ and let $f(X) = X^n + a_{n-1} + ... + a_1X + a_0 \in K[X]$ be the minimal polynomial of α over K. Define $\mathrm{N}_{L/K}(\alpha) = (-1)^{nr}a_0^r$.
(3) If the extension L/K is normal, then define $\mathrm{N}_{L/K}$ to be the product of all the $\sigma(\alpha)$, for $\sigma \in \mathrm{Aut}(L/K)$. Note that if L/K is Galois, then it is necessarily normal and thus $\mathrm{N}_{L/K}(\alpha)$ is the product of all the $\sigma(\alpha)$, for $\sigma \in \mathrm{Gal}(L/K)$.

Definition 2.16. Let L/K be a Galois extension with $\alpha \in L$. The **trace** of α is defined by

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Definition 2.17. Let L/K be a finite extension of the local field K of degree n. Let $\mathcal{M}_K = (\pi_K)$ and $\mathcal{M}_L = (\pi_L)$. One has $\pi_K = {\pi_L}^e$ for some $e \geq 1$. The degree e is called the **ramification index**. The integer

$$[k_L : k_K] = f$$

is called the **inertial degree** of the extension L/K. An extension of a field K with characteristic of the residue field equal to a prime $p \geq 0$ is called **unramified** if $e = 1$. Thus, in unramified extensions the prime remains a prime. The extension is **totally ramified** if $e = n$, **tamely ramified** if $p \nmid e$, and **wildly ramified** if $p \mid e$. Thus, in ramified extensions, the prime factors.

It is a fact that $n = ef$. Also, if π_L is a uniformizer in L, then $\nu_K(\pi_L) = 1/e$.
The extension may consist of unramified and ramified subextensions. We use **ramification groups**, which form a chain of normal subgroups of the Galois group, to find structural information for the Galois group of the entire extension L/K. The ramification groups have certain properties that will be described in section 3. These properties can be used to determine which transitive subgroups of S_n might be isomorphic to the Galois group of L/K.

2.3. **The Field of Formal Laurent Series.** As discussed in the introduction, finite extensions of $\mathbb{Q}_p$ have been studied by several authors [2–5, 9, 14]. Our focus in this paper is to study finite extensions of the field of formal Laurent series $\mathbb{F}_p((T))$.

Definition 2.18. A formal Laurent series $f(T)$ is an infinite series of the form

$$\sum_{i=-m}^{\infty} a_i T^i$$

with $m, i \in \mathbb{Z}$, $a_i \in \mathbb{F}_p$ for all i.

The elements of $\mathbb{F}_p((T))$ are formal Laurent series in T. We construct this field by considering the polynomial ring $\mathbb{F}_p[T]$. The field of fractions of $\mathbb{F}_p[T]$ is denoted $\mathbb{F}_p(T)$.

Definition 2.19. Given $x \in \mathbb{F}_p(T)$, write x as $T^r \frac{g}{h}$ with $g, h \in \mathbb{F}_p[T],\ T \nmid gh$. We define a valuation ν_T by:

$$\nu_T\left(T^r \frac{g}{h}\right) = r$$

with $\nu_T(0) = \infty$.

An equivalent expression for the valuation defined above is

$$\nu_T(x) = \nu_T\left(\sum_{i=-m}^{\infty} a_i T^i\right) = -m.$$

We also define an absolute value $|\cdot|_T$ such that $\left|T^r \frac{g}{h}\right|_T = p^{-r}$. Note that we could give this absolute value an equivalent definition in terms of something other than p. The above definition of $|\cdot|_T$ will remain in use for the rest of the paper.

Theorem 2.20. $\mathbb{F}_p((T))$ is the completion of the field $\mathbb{F}_p(T)$ with respect to $|\cdot|_T$.

Proof. Consider the set S of distinct limits of Cauchy sequences in $\mathbb{F}_p(T)$. Each element in S can be represented by a unique Cauchy series of the form

$$a_{-n}\pi^{-n} + \ldots + a_0 + a_1\pi + \ldots + a_n\pi^n + \ldots$$

where all a_i are in the residue field k, and π is the largest-valued element of $\mathbb{F}_p(T)$ such that $|\pi|_T < 1$ [12, p.113-115]. In this case, $k = \mathbb{F}_p$ and $\pi = T$. This means that all the elements in the completion of $\mathbb{F}_p(T)$ have the form

$$a_{-n}T^{-n} + \ldots + a_0 + a_1 T + \ldots + a_n T^n + \ldots = \sum_{i=-m}^{\infty} a_i T^i$$

with $m, i \in \mathbb{Z}, a_i \in \mathbb{F}_p$ for all i. Thus the completion of $\mathbb{F}_p(T)$ is the field of formal Laurent series, $\mathbb{F}_p((T))$. □

Note that $\mathbb{F}_p((T))$ is a non-Archimedean local field with characteristic p. As we will only discuss the valuation on $\mathbb{F}_p((T))$, we will be using the notation $\nu(x)$ rather than $\nu_T(x)$ to denote this specific valuation for the remainder of the paper unless otherwise specified.

As a local field, $K = \mathbb{F}_p((T))$ has the following structure:

- The ring of integers $\mathcal{O}_\mathcal{K} = \{x \in \mathbb{F}_p((T)) : \nu(x) \geq 0\}$ is the ring of formal power series

$$\mathbb{F}_p[[T]] = \left\{\sum_{n\geq 0} a_n T^n : a_n \in \mathbb{F}_p\right\}.$$

- The group of units $\mathcal{U}_\mathcal{K} = \{x \in \mathbb{F}_p((T)) : \nu(x) = 0\}$ is a subgroup of the formal power series which contains only those elements with a non-zero constant term.
- The maximal ideal $\mathcal{M}_\mathcal{K} = \{x \in \mathbb{F}_p((T)) : \nu(x) > 0\}$ is (T), the ring of formal power series whose constant term is zero. Any uniformizer of $\mathbb{F}_p((T))$ will generate the maximal ideal. It follows that T is the uniformizer of $\mathbb{F}_p((T))$.
- The residue field $k = \mathcal{O}_\mathcal{K}/\mathcal{M}_\mathcal{K}$ is $\mathbb{F}_p$.

3. Ramification Groups

We define ramification groups in terms of elements from the Galois group G of L/K in the following way:

$$G_i = \{\sigma \in G : \nu_L(\sigma(x) - x) \geq i + 1 \text{ for all } x \in \mathcal{O}_L\}$$

where $i \geq -1$. The ramification groups, as mentioned in section 2, make up a chain of subgroups of the Galois group which are eventually trivial. These G_i may not be distinct for all i.

Definition 3.1. In the subgroup chain of ramification groups, a **ramification break** is defined to occur at $i \geq 0$ such that $G_i \neq G_{i+1}$. Depending on the Galois group and ramification groups themselves, this break may be unique.

Note that the chain of ramification groups is an invariant of the field, so distinct chains give distinct fields. Also if G is cyclic and of prime order p then there will be a single ramification break since G_i will be isomorphic to either $\mathbb{Z}/p\mathbb{Z}$ or $\{1\}$.

As previously mentioned, the ramification groups give information about the Galois group G of an extension. In particular, G_{-1} is equal to G. G_0 is called the **inertia group** and is equal to the subgroup of G with automorphisms fixing K^{ur} where K^{ur} is the maximal unramified extension, which will be discussed later. For $i > 0$, G_i is equal to the subgroup of G with automorphisms fixing an intermediate subextension of L. In addition, G/G_0 is isomorphic to the Galois group of K^{ur}/K, and for $i \geq 0$, G_i/G_{i+1} is isomorphic to the subgroup of G with automorphisms that fix the base field of G_i in an extension from the base field of G_i to the base field of G_{i+1}. Intuitively, the quotient can be thought of as the extension resulting from "subtracting" the extension corresponding to G_{i+1} from the extension corresponding to G_i. See Figure 1 below for an illustration of this idea.

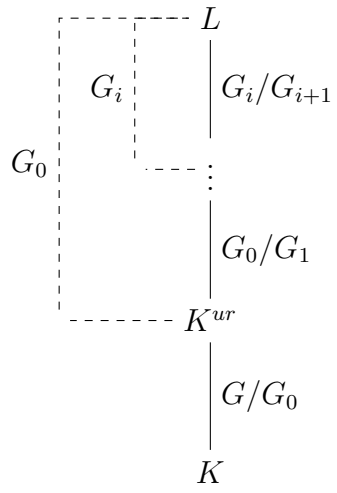
The following lemma concerning properties of the ramifications groups of an extension appears in Serre [15, p.67] and is referenced in many of Awtrey's works [2–5].

Lemma 3.2. Let K be a field of characteristic p. Let L/K be a Galois extension with Galois group G and let $\mathcal{M}_L$ denote the maximal ideal of the integers in L. For $i \geq -1$, let G_i be the i-th ramification group. Let U_0 be the units in L and for $i \geq 1$, let $U_i = 1 + (\pi_L^i)$, where π_L is the generator of $\mathcal{M}_L$.

(a) For $i \geq 0$, G_i/G_{i+1} is isomorphic to a subgroup of U_i/U_{i+1}.
(b) The group G_0/G_1 is cyclic and isomorphic to a subgroup of the group of roots of unity in the residue field of L. Its order is prime to p.
(c) The quotients G_i/G_{i+1} for $i \geq 1$ are abelian groups and are direct products of cyclic groups of order p. The group G_1 is a p-group.
(d) The group G_0 is the semi-direct product of a cyclic group of order prime to p with a normal subgroup whose order is a power of p.

(e) The groups G_0 and G are both solvable.

FIGURE 1. Field Diagram with Ramification Groups



Proof. Our first step is to define a map $\Phi : G_i \to U_i/U_{i+1}$. Let $\sigma \in G_i$. Since $\pi_L \in \mathcal{O}_L$ and $\sigma \in G_i$, we have

$$i + 1 \leq v_L(\sigma(\pi_L) - \pi_L).$$

Thus, we have

$$\begin{aligned} i + 1 &\leq v_L\left(\pi_L\left(\frac{\sigma(\pi_L)}{\pi_L} - 1\right)\right) \\ &= v_L(\pi_L) + v_L\left(\frac{\sigma(\pi_L)}{\pi_L} - 1\right) \\ &= 1 + v_L\left(\frac{\sigma(\pi_L)}{\pi_L} - 1\right), \end{aligned}$$

i.e.,

$$v_L\left(\frac{\sigma(\pi_L)}{\pi_L} - 1\right) \geq i.$$

This shows we have a well-defined map

$$\begin{aligned} f : G_i &\to U_i/U_{i+1} \\ \sigma &\mapsto \frac{\sigma(\pi_L)}{\pi_L}. \end{aligned}$$

Our next step is to show that f is a homomorphism. We have

$$\begin{aligned} f(\sigma\tau) &= \frac{\sigma\tau(\pi_L)}{\pi_L} \\ &= \frac{\sigma\left(\frac{\tau(\pi_L)}{\pi_L}\right)}{\frac{\pi_L}{\sigma(\pi_L)}} \\ &= \frac{\sigma(\pi_L)\tau(\pi_L)}{\pi_L^2}\frac{\sigma\left(\frac{\tau(\pi_L)}{\pi_L}\right)}{\frac{\tau(\pi_L)}{\pi_L}} \\ &= f(\sigma)f(\tau)\frac{\sigma\left(\frac{\tau(\pi_L)}{\pi_L}\right)}{\frac{\tau(\pi_L)}{\pi_L}}. \end{aligned}$$

Thus, to show that f is a homomorphism it only remains to show that

$$\frac{\sigma\left(\frac{\tau(\pi_L)}{\pi_L}\right)}{\frac{\tau(\pi_L)}{\pi_L}} \in U_{i+1}.$$

Note that since $\frac{\tau(\pi_L)}{\pi_L}$ is a unit for any $\tau \in G_i$, we have $\sigma\left(\frac{\tau(\pi_L)}{\pi_L}\right)$ is easily seen to be a unit as well. Let $u = \frac{\tau(\pi_L)}{\pi_L}$ We now show that

$$\frac{\sigma(u)}{u} \in U_{i+1}$$

if $\sigma \in G_i$. To see this, observe that we have

$$\begin{aligned} v_L\left(\frac{\sigma(u)}{u} - 1\right) &= v_L(u)^{-1} + v_L(\sigma(u) - u) \\ &= -v_L(\sigma(u)) + v_L(\sigma(u) - u) \\ &= v_L(\sigma(u) - u) \\ &\geq i + 1. \end{aligned}$$

Thus, we have that f is a group homomorphism as claimed.

It only remains to show that the kernel of f is G_{i+1}. Let $\sigma \in G_i$ with $f(\sigma) = 1$. Then we have $\frac{\sigma(\pi_L)}{\pi_L} \in U_{i+1}$, i.e., $v_L\left(\frac{\sigma(\pi_L)}{\pi_L} - 1\right) \geq i + 1$. However, this simplifies to the condition that

$$v_L(\sigma(\pi_L) - \pi_L) \geq i + 2,$$

i.e., $\sigma \in G_{i+1}$. (Note we strictly need to show that inequality for all elements of $\mathcal{O}_L$, but it is not hard to show it is enough to show it for the uniformizer.) Thus, $\ker(f) \subset G_{i+1}$. Essentially the same argument shows that $G_{i+1} \subset \ker(f)$, which finishes the proof of part (a).

For (b) note that U_0/U_1 is isomorphic to the multiplicative group of the residue field of L. Thus it follows that G_0/G_1 is cyclic and a subgroup of the roots of unity in the residue field of L.

For (c), note that for $i \geq 1$, U_i/U_{i+1} is isomorphic to the additive group of the residue field. It then follows that G_i/G_{i+1} is cyclic and by the fundamental theorem of finite abelian groups every finite abelian group can be expressed as a direct sum, or in other words a direct product of abelian groups. That G_1 is a p-group follows from $|G_1| = \prod_{i=1}^{\infty} |G_i/G_{i+1}|$. Note that this is actually a finite product since the G_i eventually become trivial.

For (d), since G_0 and G_1 have relatively prime order, there is a subgroup of G_0 that projects isomorphically onto G_0/G_1. From (b) we know that this quotient group is cyclic with order prime to p. Then (d) follows based on knowledge of semi-direct products.

For (e), consider the fact that G/G_0 is isomorphic to the Galois group of the residue field and is cyclic. Recall also that the ramification groups define a sequence of decreasing normal subgroups. From (b) and (c) we know that the quotient groups are abelian and thus G_0 and G_1 are solvable. □

Suppose L/K is a degree n extension of a characteristic p field K. We can use Lemma 3.2 to determine possible Galois groups for L/K. Following [2, Ch. 4], we consider the transitive subgroups of the symmetric group S_n. Possible Galois groups are those which meet the following criteria:

(1) G contains a solvable normal subgroup G_0 such that G/G_0 is cyclic of order dividing n.
(2) G_0 contains a normal subgroup G_1 that is a p-group, which is possibly trivial.
(3) G_0/G_1 is cyclic of order dividing $p^{[G:G_0]-1}$.

Through direct computation, we can reduce our list of transitive subgroups to those which meet the conditions above. To precisely identify the Galois group of L/K, we would need to find a defining polynomial $f(x)$ for L/K. We would then use invariants such as centralizer order and parity to match $f(x)$ with one of the remaining subgroups of S_n.

4. Unramified Extensions

In order to classify the extensions of $\mathbb{F}_p((T))$, we must first examine unramified extensions. This will require several results carried over from the study of p-adic fields. Some of the proofs in this section follow methods used in [8, Ch. 5]. In particular, Hensel's Lemma is true for all local fields including $\mathbb{F}_p((T))$.

Theorem 4.1 (Hensel's Lemma)**.** Let K be a field, $f(x)$ be a polynomial in $\mathcal{O}_K[x]$, and $\alpha_0 \in \mathcal{O}_K$ such that $f(\alpha_0) \equiv 0 \pmod{\mathcal{M}_K}$ and $f'(\alpha_0) \not\equiv 0 \pmod{\mathcal{M}_K}$. Then there exists $\alpha \in \mathcal{O}_K$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{\mathcal{M}_K}$.

Corollary 4.2. Let $K/\mathbb{F}_p((T))$ be a finite extension and let $f = f(K/\mathbb{F}_p((T)))$. Then $\mathcal{O}_K^{\times}$ contains the cyclic group of the $(p^f - 1)$st roots of unity.

Proof. Observe that $\mathcal{O}_K/\mathcal{M}_K$ is a finite field of degree p^f. Because every subgroup of a finite field is cyclic, $(\mathcal{O}_K/\mathcal{M}_K)^{\times}$ is a cyclic group of order $p^f - 1$. So for each m that divides $p^f - 1, F_m(x) = x^m - 1$ has exactly m roots in $(\mathcal{O}_K/\mathcal{M}_K)^{\times}$. Any lift of these roots to $\mathcal{O}_K$ gives us m non-congruent approximate roots. The derivative $F_m'(x) = mx^{m-1}$ will be non-zero in $\mathcal{O}_K$ (because the approximate roots are units). Thus since $p \nmid m$, Hensel's Lemma

gives us m different mth roots of unity in $\mathcal{O}_K^\times$. This is true for any m that divides $p^f - 1$, so $\mathcal{O}_K^\times$ contains the cyclic group of $(p^f - 1)$st roots of unity. □

Definition 4.3. Let K and L be two extensions of the field F. The **compositum** of K and L, denoted KL, is defined to be the intersection of all fields containing both K and L.

In other words, the compositum is the smallest field containing both K and L. It can be formed by adjoining generators of K to L or alternatively, adjoining generators of L to K.

In the discussion that follows, we let $K = \mathbb{F}_p((T))$ and K^u be an unramified extension of K. For every positive integer f, we can show there exists a unique degree f unramified extension of K, and that we obtain this extension by adjoining a primitive $(p^f - 1)$st root of unity.

Theorem 4.4. For every integer $f \geq 1$, K has a unique unramified extension of degree f.

Proof. It can be shown that the compositum of unramified extensions is unramified [10, p.48]. Keeping that in mind, consider two unramified degree f extensions of K, say L_f and K_f. Then $K_f L_f / K$ is unramified and has the same residue field as K_f, since a finite field has a unique extension for a given degree. Thus,

$$[K_f L_f : K] = [K_f L_f : K_f][K_f : K]$$

with $[K_f L_f : K] = [K_f : K] = f$, which shows $K_f \subset L_f$ and $L_f \subset K_f$. Therefore, $K_f = L_f$ and an unramified extension of a given degree is unique. □

Theorem 4.5. The unique degree f unramified extension of K, K^u/K is obtained by adjoining a primitive $(p^f - 1)$st root of unity to K. Consequently every unramified extension is a Galois extension.

Proof. By 4.2, K^u contains the $(p^f - 1)$st roots of unity. Let β be a primitive $(p^f - 1)$st root of unity in K^u. Then we have a tower of extensions

$$K \subset K(\beta) \subset K^u.$$

The powers of β are the $(p^f - 1)$st roots of unity, which are distinct by 4.2. Thus $\bar{\beta}$ is a $(p^f - 1)$st root of unity, so that the residue field of the extension $K(\beta)/K$ contains $\mathbb{F}_{p^f} \cong k$. The degree of the residue field extension must be less than or equal to the degree of the extension of K. Thus the degree of $K(\beta)/K$ is at least f. Since K^u/K is of degree f, it follows that $K^u = K(\beta)$. □

Definition 4.6. The **maximal unramified extension**, denoted K^{ur}, is the compositum of all the unramified extensions of K.

Unramified extensions are already well understood. So, when we build up our tower of fields, we focus on building ramified extensions over our maximal unramified extension.

5. Totally Ramified Extensions

Let L/K be a finite extension of K and let K^{ur}, a subfield of L, be the maximal unramified extension of K. Then L/K^{ur} is totally ramified. This means that we can construct all finite extensions of K by looking at unramified and totally ramified extensions. In this section, we focus on totally tamely ramified extensions. Unless otherwise specified, we will assume that $p \nmid n$ and $e = n$ which implies $f = 1$.

Definition 5.1. Let $f(x) \in \mathcal{O}_K[x]$ be a monic polynomial:

$$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0.$$

If $\nu(a_i) \geq 1$ for each $i = 0, ..., n-1$, and $\nu(a_0) = 1$, then $f(x)$ is said to be **Eisenstein**.

The definition for Eisenstein can also be described in terms of the maximal ideal. That is, let (π_k) be the maximal ideal of K. Then a polynomial $f(x)$ is Eisenstein if $a_i \in (\pi_K)$ for each $i = 0, ..., n-1$ but $a_0 \notin (\pi_k^2)$. Note that if a polynomial is Eisenstein then it is irreducible. The following well-known theorem can also be found in [7, p.54].

Lemma 5.2. If $x_0, \cdots, x_{n-1} \in K$ where $|x_i|_K \neq |x_j|_K$ for $i \neq j$, then

$$\left|\sum_{i=0}^{n-1} x_i\right|_K = \max_{0 \leq i \leq n-1}\{|x_i|_K\}.$$

Proof. Let $|\cdot|_K = |\cdot|$. We show without loss of generality that if $|x_0| > |x_1| > \cdots > |x_{n-1}|$, then $|x_0 + x_1| \leq \max\{|x_0|, |x_1|\} = |x_0|$. On the other hand we have $|x_0| = |x_0 + x_1 - x_1| \leq \max\{|x_0 + x_1|, |x_1|\} = |x_0 + x_1|$ since $|x_0| > |x_1|$. Thus, $|x_0 + x_1| = |x_0|$. Now assume for some j we have $|x_0 + x_1 + \cdots + x_{j-1}| = |x_0|$. Then

$$\begin{aligned}\left|\sum_{i=0}^{j-1} x_i + x_j\right| &\leq \max\left\{\left|\sum_{i=0}^{j-1} x_i\right|, |x_j|\right\} \\ &= \max\{|x_0|, |x_j|\} \\ &= |x_0|.\end{aligned}$$

On the other hand we have

$$\begin{aligned}|x_0| = \left|\sum_{i=0}^{j-1} x_i\right| = \left|\sum_{i=0}^{j} x_i - x_j\right| &\leq \max\left\{\left|\sum_{i=0}^{j} x_i\right|, |x_j|\right\} \\ &= \left|\sum_{i=0}^{j} x_i\right|\end{aligned}$$

since $|x_0| > |x_j|$. Therefore,

$$\left|\sum_{i=0}^{n-1} x_i\right| = \max_{0 \leq i \leq n-1}\{|x_i|\}.$$

□

Theorem 5.3. For $p \nmid n$, a finite extension L/K of a non-Archimedean local field is totally ramified if and only if $L = K[\alpha]$, with α a root of an Eisenstein polynomial.

Proof. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be an Eisenstein polynomial of degree n and L/K be an extension with defining polynomial f. Suppose α is a root of f. Then

$$-a_n\alpha^n = a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha^1 + a_0.$$

So taking the valuation of both sides we get

$$\nu_L(-a_n\alpha^n) = \nu_L(a_n\alpha^n) = \nu_L\left(\sum_{i=0}^{n-1} a_i\alpha^i\right) \geq \min_{0\leq i\leq n-1}\{\nu_L(a_i\alpha^i)\},$$

$$= \min_{0\leq i\leq n-1}\{\nu_L(a_i) + \nu_L(\alpha^i)\}.$$

For this valuation, we can see that for an element $s \in K$, $\nu_L(s^t) = t\nu_L(s)$. Using this fact and the fact that $\nu_L(s) = e\nu_K(s)$, the following is the above steps reduced:

$$n\nu_L(\alpha) \geq \min_{0\leq i\leq n-1}\{e\nu_K(a_i) + i\nu_L(\alpha)\}.$$

It follows that $\nu_L(\alpha) > 0$ because by definition of Eisenstein, for all $i > 0$, $\nu(a_i) \geq 1$ and $\nu(a_0) = 1$. Also, $e\nu_K(a_0) < e\nu_K(a_i) + i\nu_L(\alpha)$ for all $i > 0$, so $n\nu_L(\alpha) = e\nu_K(a_0) = e$. Thus, $\nu_L(\alpha) = 1$ and $n = e$. Therefore, this polynomial defines a totally ramified extension of degree n. See [7, p.54].

For the converse, let L/K be a totally and tamely ramified extension of degree n and let π_L be a uniformizer of L. For the minimal polynomial $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ of π_L over K, then

$$\begin{aligned} n = n\nu_L(\pi_l) &= \nu_L(\sum_{0}^{n-1} a_i\pi_L^i) \\ &= \min_{0\leq i\leq n-1}\{\nu_L(a_i) + \nu_L(\pi_L^i)\} \\ &= \min_{0\leq i\leq n-1}\{n\nu_K(a_i) + \frac{i}{n}\}. \end{aligned}$$

Since from the second method for calculating the norm $a_0 = N_{L/K}(\pi_L) = 1$, then $|a|_0 = |\pi_L|^n$ which implies $\nu_K(a_0) = \nu_L(\pi_L) = 1$. Now for $1 \leq i \leq n-1$ we have:

$$\begin{aligned} n &\leq n\nu_K(a_i) + \frac{i}{n} \\ 0 < n - \frac{i}{n} &\leq n\nu_K(a_i) \end{aligned}$$

Since $0 < \nu_K(a_i)$, this necessarily implies that $1 \leq \nu_K(a_i)$. It follows that $f(x)$ is Eisenstein. □

Note that since K^{ur} is the maximal unramified sub-extension of L then L/K^{ur} is also a totally ramified extension and Theorem 5.3 applies.

5.1. **Totally Tamely Ramified Extensions.** Using the work of Pauli and Roblot [14], we can show exactly what the totally tamely ramified extensions look like, but first we need some theorems adapted from Pauli [13]. This section only deals with extensions over $\mathbb{F}_p((T))$ and so we define $K/\mathbb{F}_p((T))$ to be the maximal unramified extension and L/K to be the totally tamely ramified extension. Also we will denote $|\pi_K|_K = |\mathcal{M}_K|_K$.

Definition 5.4. Let L/K be an algebraic extension of degree n. Then a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$ is an **integral basis** of L/K. Let $(\delta_0, \cdots, \delta_{n-1})$ be an integral basis of L/K. Then

$$\mathrm{disc}(L/K) = \det((\delta_k^{(l)})_{0\le k\le n-1, 1\le l\le n})^2$$

is the **discriminant** of L/K.

The discriminant of the field generated by an Eisenstein polynomial is exactly the discriminant of the polynomial.

Lemma 5.5. Let $L = K(\alpha)/K$ be a finite Galois extension of degree n and f be the minimal polynomial over K with roots $\alpha_1, \ldots, \alpha_n$ where $\alpha = \alpha_1$. then $\mathrm{disc}(L/K) = \mathrm{disc}(f)$ and $\mathrm{disc}(f) = n\nu(f'(\alpha))$.

Proof. Let $\sigma_i \in \mathrm{Gal}(L/K)$ and consider $\sigma_i(\alpha) = \alpha_i$ for $i \in \{1, \ldots, n\}$. Then $\sigma_i(x^j) = x_i^j$ where $o \le j \le n-1$. Note $\mathrm{disc}(L/K)$ is the square of the determinant of the matrix

$$\nu = \begin{bmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \ldots & x_n^{n-1} \end{bmatrix}.$$

Since ν is a Vandermonde matrix, $\det \nu = \pi_{i<j}(\alpha_i - \alpha_j)$ and it follows that $\mathrm{disc}(L/K) = \mathrm{disc}(f)$. Next we have

$$f'(x_i) = \sum_k \pi(x_i - x_j).$$

However, only the $k = i$ term is non-zero, hence

$$f'(x_i) = \prod_{j\ne i}(x_i - x_j)$$

then it follows that

$$\mathrm{disc}(f) = \prod_{i=1}^{n} f'(x_i)$$

therefore,

$$\nu_K(\mathrm{disc}(f)) = \nu_K(\prod_{i=1}^{n} f'(x_i)) = n\nu_K(f'(x_i)).$$

□

Theorem 5.6. (Ore's Conditions) Let K be a finite extension of $\mathbb{F}_p((T))$ with the maximal ideal $\mathcal{M}_K$ and note that the valuation $\nu_K(x) = e \cdot \nu_T(x)$. Then there exist totally ramified extensions L/K of degree n and discriminant $\mathcal{M}_K^{n-1}$.

Proof. By theorem 5.3, every totally ramified extension L of K can be generated by adjoining a root α of an Eisenstein polynomial $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$. Then we have $\mathrm{disc}(F/K) = \mathrm{disc}(f(x))$ since $f(x)$ is Eisenstein and we can write $\nu_K(\mathrm{disc}(f(x)))/n = \nu_K(f'(\alpha))$ because $f(x)$ is irreducible. Since α is a uniformizer in F, $\nu_K(\alpha) = 1/e = 1/n$.

Then the valuations of $ia_i\alpha^{i-1}$ for $1 \leq i < n$ and $n\alpha^{n-1}$ are all different and so by lemma 5.2 we get:

$$\begin{aligned}\nu_K(f'(\alpha)) &= \nu_K(n\alpha^{n-1} + (n-1)a_{n-1}\alpha^{n-1} + ... + a_1) \\ &= \min_{1\leq i\leq n-1}\left\{\nu_K(n) + \frac{n-1}{n}, \nu_K(i) + \nu_K(a_i) + \frac{i-1}{n}\right\}\end{aligned}$$

Note that $\nu_K(x) = 0$ for all $x \in \mathbb{Z}$ and $\nu_K(a_i) \geq 1$ for all $1 \leq i \leq n-1$, so

$$\begin{aligned}&= \min_{1\leq i\leq n-1}\left\{\frac{n-1}{n}, \nu_K(a_i) + \frac{i-1}{n}\right\} \\ &= \frac{n-1}{n}\end{aligned}$$

Thus since $f(x)$ is irreducible and $\nu_K(\text{disc}(f(x))) = n\nu_K(f'(\alpha)) = n-1$ it is clear that we can construct an Eisenstein polynomial $f(x)$ such that $\text{disc}(f(x)) = \mathcal{M}_K^{n-1}$. □

Let $\mathbf{L}_n$ denote the set of all totally ramified extension L/K of degree n and discriminant $\mathcal{M}_K^{n-1}$. Also let $\mathbf{E}_n$ denote the set of all Eisenstein polynomials over K of degree n and discriminant $\mathcal{M}_K^{n-1}$. It is known from Theorem 5.6 that roots of the polynomial in $\mathbf{E}_n$ generate all the extensions $L \in \mathbf{L}_n$.

Definition 5.7. An **ultrametric distance** is a metric which satisfies the stronger condition of the triangle inequality:

$$d(f,h) \leq \max\{d(f,g), d(g,h)\}$$

for all f, g, h and at least two of $d(f,h), d(f,g)$, and $d(g,h)$ are equal.

Theorem 5.8. Let $f, g \in \mathbf{E}_n$ of degree n. Then $d(f,g) := |f(\beta)|_K = |g(\alpha)|_K$ where α (resp. β) is any root of f (resp. g) defines an ultrametric distance over $\mathbf{E}_n$. Furthermore, for fixed root α of f we can choose the root β of g such that $|\beta - \alpha|$ is minimal with respect to all roots α_i of f which gives

$$d(f,g) = \prod_{i=1}^{n} \max\{|\beta - \alpha|, |\alpha_i - \alpha|\}.$$

Proof. Since f and g are Eisenstein of degree n where $p \nmid n$, these polynomials generate a totally and tamely ramified extension of degree n. Let $L_f, L_g \in \mathbf{L}_n$ be the extensions generated by f and g, respectively. Since we are only considering Galois extension, L_f and L_g are Galois. Let $G = \text{Gal}(L_g/K)$ and define $d(f,g) := |f(\beta)|$ for any root β of g. The fact that $d(f,g) \geq 0$ follows from the nonnegativity of $|\cdot|$. Next, suppose $d(f,g) = 0$. Since $|\cdot|$ is Galois invariant, then for $\sigma \in G$ and root $\beta' = \sigma(\beta)$ we have

$$|f(\beta)| = |\sigma(f(\beta))| = |f(\sigma(\beta))| = |f(\beta')|.$$

Thus

$$\begin{aligned}d(f,g) = |f(\beta)| = 0 &\Leftrightarrow |f(\sigma_i(\beta))| = 0 \qquad \text{for all } \sigma_i \in G \\ &\Leftrightarrow f(\sigma_i(\beta)) = 0 \\ &\Leftrightarrow \sigma_i(\beta) \text{ is a root of } f \text{ for all } i \\ &\Leftrightarrow f = g.\end{aligned}$$

The above also shows that $d(f,g)$ does not depend on the choice of β. Moreover, if $\gamma_1, \ldots, \gamma_n$ represent the roots of f and $\beta_1, \cdots, \beta_n$ represent the roots of g then for any $\gamma \in \{\gamma_1, \ldots, \gamma_n\}$.

$$\begin{aligned} |f(\beta)|^n = \prod_{i=1}^{n} |f(\beta_i)| &= \prod_{i=1}^{n}\prod_{j=1}^{n} |\beta_i - \gamma_j| \\ &= \prod_{j=1}^{n}\prod_{i=1}^{n} |\gamma_j - \beta_i| \\ &= \prod_{j=1}^{n} |g(\gamma_j)| \\ &= |g(\gamma)|^n. \end{aligned}$$

Consequently, $d(f,g) = d(g,f)$ since $|f(\beta)|, |g(\gamma)| \in \mathbb{R}_{\geq 0}$. Now fix a root γ of f and choose a root β of g such that the distance $|\beta - \gamma|$ is minimal. Notice that this distance does not depend on the choice of γ since $|g(\gamma)| = \prod_{i,j} |\gamma_i - \beta_j| = |g(\gamma')|$ for all roots γ' of f. We can write

$$d(f,g) = |f(\beta)| = \prod_{i=1}^{n} |\beta - \gamma_i|.$$

Next suppose that there exists a root γ_i such that $|\beta - \gamma_i| \neq |\beta - \gamma|$. Then $|\beta - \gamma_i| > |\beta - \gamma|$ and by Lemma 5.2

$$|\gamma - \gamma_i| = |\gamma - \beta + \beta - \gamma_i| = |\beta - \gamma_i|.$$

So

$$d(f,g) = \prod_{i=1}^{n} \max\{|\beta - \gamma|, |\gamma - \gamma_i|\}.$$

Finally, to show d satisfies the ultrametric inequality, let $h \in E_n$ with roots λ and λ' and choose γ and β such that $|\beta - \lambda|$ is minimal with respect to all roots of g and $|\gamma - \lambda'|$ is minimal with respect to all roots of f. Then

$$\begin{aligned} d(f,h) &= \prod_{i=1}^{n} \max\{|\gamma - \lambda'|, |\gamma - \gamma_i|\} \\ &\leq \prod_{i=1}^{n} \max\{|\gamma - \lambda|, |\gamma - \gamma_i|\} \\ &\leq \prod_{i=1}^{n} \max\{\max\{|\gamma - \beta|, |\beta - \lambda|\}, |\gamma - \gamma_i|\} \\ &\leq \max\left\{\prod_{i=1}^{n} \max\{|\gamma - \beta|, |\gamma - \gamma_i|\}, \prod_{i=1}^{n} \max\{|\beta - \lambda|, |\gamma - \gamma_i|\}\right\} \\ &\leq \max\{d(f,g), d(g,h)\}. \end{aligned}$$

Therefore d is an ultrametric. □

The distance $d(f,g)$ is calculated using the following lemma.

Lemma 5.9. Let $f, g \in \mathbf{E}_n$. Write $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_0$ and $g(x) = x^n + g_{n-1}x^{n-1} + \cdots + g_0$ and set

$$w = \min_{0 \le i \le n-1} \left\{ \nu_K(g_i - f_i) + \frac{i}{n} \right\}$$

Then $d(f, g) = |\mathcal{M}_K|^w$.

Proof. Let θ be a root of the defining polynomial of the unramified extension $\mathbb{F}_p((T))/K$ and γ be a root of $f(x)$. Then we can write

$$g(x) = \sum_{i=0}^{n} g_i(\theta)x^i$$

where $g_i(\beta) \in K[\beta]$. From this we observe the following:

$$g(\gamma) = g(\gamma) - f(\gamma) = \sum_{i=0}^{n-1} (g_i(\theta) - f_i(\theta))\gamma^i$$

. We have $\nu_K(\gamma) = \frac{1}{n}$ since γ is a prime element. Therefore, all the terms in the sum, $\sum_{i=0}^{n-1}(g_i(\theta) - f_i(\theta))\gamma^i$, have different valuations. It follows from Lemma 5.2 that the valuation of $g(\gamma)$ is the minimum of all the terms. Thus, $d(f, g) = |g(\gamma)| = |\mathcal{M}_K|^w$. □

5.2. **Construction of Generating Polynomials.** We adapt the work of [14] to construct a finite set of polynomials that will generate all the extension in $\mathbf{L}_n$. We define $K/\mathbb{F}_p((T))$ to be the maximal unramified extension and L/K to be the totally tamely ramified extension. Let Γ be the Galois group of the abelian extension $\mathbb{F}_p((T))/K$ and let $\mathcal{R}_{1,2}$ be a fixed Γ-stable system of representatives of the quotient $\mathcal{M}_K^1/\mathcal{M}_K^2$. We denote $\mathcal{R}_{1,2}^*$ to be the subset of $\mathcal{R}_{1,2}$ whose ν_K -valuation is 1.
Let Ω be the set of n-tuples $(\omega_0, \cdots, \omega_{n-1}) \in (K)^n$ which satisfy the following conditions:

$$\omega_i \in \begin{cases} \mathcal{R}_{1,2}^* \text{ if } i = 0 & (1) \\ \mathcal{R}_{1,2} \text{ if } 1 \le i \le n-1 & (2) \end{cases}$$

Each element of $\omega = (\omega_0, \ldots, \omega_{n-1}) \in \Omega$ is associated with the polynomial $A_\omega(x) \in \mathcal{O}_K[x]$ given by

$$A_\omega(x) = x^n + \omega_{n-1}x^{n-1} + \cdots + \omega_1 x + \omega_0$$

Lemma 5.10. The polynomials A_ω are Eisenstein polynomials of discriminant $\mathcal{M}_K^{n-1}$.

Proof. By construction $\nu_K(\omega_i) \ge 1$ for all i and (1) gives $\nu_K(\omega_0) = 1$. So A_ω is an Eisenstein polynomial.

Let α be a root of A_ω. Since the discriminant of A_ω is the norm from $K(\alpha)/K$ of $A'_w(\alpha)$, then

$$\nu_K(A'_w(\alpha)) = \frac{n-1}{n}$$

as seen in Theorem 5.6. So it follows that $\nu_K(\mathrm{disc}(A_\omega)) = n - 1$ and $\mathrm{disc}(A_\omega) = \mathcal{M}_K^{n-1}$. □

Definition 5.11. For any $f \in \mathbf{E}_n$ we define the **closed disc** with a radius r to be $D_{\mathbf{E}_n} = \{g \in \mathbf{E}_n | d(f, g) \le r$.

Theorem 5.12. (Krasner) The set $\mathbf{E}_n$ is the disjoint union of the closed discs $D_{\mathbf{E}_n}(A_\omega, |\mathcal{M}_K^2|)$ with center A_ω and radius $|\mathcal{M}_K^2|$ as ω runs through Ω.

Proof. Lemma 5.10 shows that the polynomials A_ω are elements of $\mathbf{E}_n$. Let ω, ω' be two distinct elements of Ω and let i be such that $\omega_i \neq \omega_i'$. Then

$$r = \nu_K(\omega_i - \omega_i') + \frac{i}{n} \leq 1 + \frac{i}{n} < 2$$

since $\omega, \omega' \in \mathcal{M}_K$. Therefore, $d(A_\omega, A_\omega') = |\mathcal{M}_K|^r > |\mathcal{M}_K^2|$ and by the ultrametric property of d the discs D_ω and D_ω' are disjoint.

Now let $f \in \mathbf{E}_n$ and write $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_0$. Since f is an Eisenstein polynomial, $\nu_K(f_0) = 1$ and there exists $\omega_0 \in \mathcal{R}_{1,2}^*$ such that

$$f_0 = \omega_0(\text{ mod } \mathcal{M}_K^2).$$

Furthermore, $\nu_K(f_i) \geq 1$ for all $i > 1$ then there exists $\omega_i \in \mathcal{R}_{1,2}$ such that $\nu_K(f_i) \equiv$ (mod $\mathcal{M}_K^2$). Let $\omega = (\omega_0, \ldots, \omega_{n-1})$. We claim that $f \in D_\omega$. We have $\nu_K(f_i - \omega_i) \geq 2$ since $f_i - \omega_i \in \mathcal{M}_K^2$. Thus for all i we have

$$\nu_K(f_i - \omega_i) + \frac{i}{n} \geq 2.$$

Therefore, $d(A_\omega, f) < |\mathcal{M}_K^2|$ and so $f \in D_\omega$

□

Corollary 5.13. Let ω be an element of Ω and let α be a root of $A_\omega(x)$. The extension $K(\alpha)/K$ is a totally ramified extension of degree n and discriminant $\mathcal{M}_K^{n-1}$. Conversely, if L/K is totally ramified extension of degree n and discriminant $\mathcal{M}_K^{n-1}$ then there exists $\omega \in \Omega$ and a root α of $A_\omega(x)$ such that $L = K(\alpha)$.

Proof. The first claim is true because we know that the polynomials $A_\omega \in \mathbf{E}_n$. To prove the second claim, let $\gamma = \gamma_1, \ldots, \gamma_n$ denote the roots of f and let Δf be the minimal distance between γ and any other root of f. Then

$$|f'(\gamma)| = \prod_{i=2}^{n} |\gamma - \gamma_i| \leq \Delta f \cdot |\mathcal{M}_K^{(n-2)/(n)},$$

since the γ_i are prime elements. But,

$$|f'(\gamma)| = |\mathcal{M}_K^{(n-1)/n}|$$

and thus

$$\Delta f \geq |\mathcal{M}_K^{1/n}|.$$

Now let $\omega \in \Omega$ be such that $d(f, A_\omega) \leq r = |\mathcal{M}_K^2|$ and let α denote a root of A_ω such that $|\alpha - \gamma|$ is minimal. Then we claim that $|\alpha - \gamma| < \Delta f$, for otherwise

$$\begin{aligned} d(f, A_\omega) &= \prod_{i=1}^{n} \max\{|\gamma - \alpha|, |\gamma - \gamma_i|\} \\ &\geq \prod_{i=1}^{n} \max\{\Delta f, |\gamma - \gamma_i|\} \\ &\geq \prod_{i=2}^{n} |\gamma - \gamma_i| = \Delta f |f'(\gamma)| \\ &\geq |\mathcal{M}_K|. \end{aligned}$$

This contradicts that $|\mathcal{M}_K| > r$. Hence $|\alpha - \gamma| < \Delta f$ and it follows from Krasner's lemma that $L = K(\alpha)$. □

Lemma 5.14. The number of polynomials A_ω, or equivalently by Theorem 5.12 the number of disjoint closed discs of radius $r = |\mathcal{M}_K^2|$ in $\mathbf{E}_n$, where $\omega \in \Omega$, is given by

$$\#D_{\mathbf{E}_n}(r) = (q-1)q^{n-1}.$$

Proof. Since $\mathcal{R}_{1,2}$ is a fixed Γ-stable system of representatives and Γ is the Galois group of the unramified extension of the residue field of $\mathbb{F}_p((T))$, then the number of elements in $\mathcal{R}_{1,2}^*$ is $(q-1)$ and the number of elements in $\mathcal{R}_{1,2}$ is q. For each A_ω, $\omega_0 \in \mathcal{R}_{1,2}^*$ and for $1 \leq i \leq n$, $\omega_i \in \mathcal{R}_{1,2}$. Thus we have:

$$\#D_{\mathbf{E}_n}(r) = (q-1)q^{n-1}$$

and the formula holds. □

Lemma 5.15. Let $t > 1$ be an integer and let $s = |\mathcal{M}_K^{(n-1+t)/n}|$. Let $\#D_{\mathbf{E}_n}(s)$ denote the number of disjoint closed discs of radius s in $\mathbf{E}_n$. Then the number of elements in $\mathbf{L}_n$ is

$$\#\mathbf{L}_n = \#D_{\mathbf{E}_n}(s) \frac{n}{(q-1)q^{t-2}} \ .$$

Proof. Let Π_n denote the set of all prime elements of members of $\mathbf{L}_n$. Alternatively, since Π_n is essentially the set of constant terms of Eisenstein polynomials, Π_n can be defined as the union of the sets $\mathfrak{P}\backslash\mathfrak{P}^2$, where $\mathfrak{P}$ is the prime ideal of some member $L \in \mathbf{L}_n$. Let χ be the map from Π_n to $\mathbf{E}_n$ that sends a prime element to its minimal polynomial over K.

Let $u = |\mathcal{M}_K^t|^{1/n}$, and let α and β be two elements of Π_n such that $|\alpha - \beta| \leq u$. Then α and β generate the same field $L \in \mathbf{L}_n$ by Krasner's lemma. Observe we have $d(\chi(\alpha), \chi(\beta)) \leq u|\mathcal{M}_K^{n-1}|^{1/n} = s$ by the same reasoning as in Corollary 5.13. We define a closed disc $D_\pi(\alpha, r) = \{\beta \in \pi || \alpha \cdot \beta \leq r\}$. Hence, $\chi(D_\Pi(\alpha, u)) \subset D_{\mathbf{E}_n}(\chi(\alpha), s)$, where $D_\Pi(\alpha, u)$ is the closed disc of center α and radius u in Π_n . Conversely, let $f(x) \in \mathbf{E}_n$ and let α denote any root of $f(x)$, so $f(x) = \chi(\alpha)$. Then it is straightforward to prove, using the same methods, that $D_{\mathbf{E}_n}(\chi(\alpha), s) \subset \chi(D_\Pi(\alpha, u))$. Thus, for all $\alpha \in \Pi_n$

$$D_{\mathbf{E}_n}(\chi(\alpha), s) = \chi(D_\Pi(\alpha, u)).$$

Now, the map χ is clearly surjective and n-to-one. Furthermore, the inverse image of $\chi(\alpha)$ is the set of conjugates of α over K, and since $t > 1$, the closed discs of radius u centered at the conjugates of α are all disjoint. It follows that the inverse image of any closed disc

of radius s in $\mathbf{E}_n$ is the disjoint union of n closed discs of radius u in Π_n. But, again by the remark above, any such disc is in fact contained in $\mathfrak{P}\backslash\mathfrak{P}^2$ for some $L \in \mathbf{L}_n$. Thus, the number of disjoint closed discs of radius u in Π_n is equal to

$$\#\mathbf{L}_n q^{t-2}(q-1) = n\#D_E(s),$$

and the result is proven. □

Theorem 5.16. Let K be a finite extension of $\mathbb{F}_p((T))$ with maximal ideal $\mathcal{M}_K$ and ramification index e. Let $q = p^f$ equal the order of the residue field of K. Then the number of totally ramified extensions of K of degree n and discriminant $\mathcal{M}_K^{n-1}$ is

$$\#\mathbf{L}_n = n$$

Proof. Choose $t = n+1$. By Theorem 5.15,

$$\#\mathbf{L}_n = \#D_{\mathbf{E}_n}(|\mathcal{M}_K^{(n-1+n+1)/n}|)\frac{n}{(q-1)q^{n-1}} = \#D_{\mathbf{E}_n}(|\mathcal{M}_K^2|)\frac{n}{(q-1)q^{n-1}}.$$

Then by applying Theorem 5.14

$$\#D_{\mathbf{E}_{n,j}}(|\mathcal{M}_K^2|)\frac{n}{(q-1)q^{n-1}} = (q-1)q^{n-1}\cdot\frac{n}{(q-1)q^{n-1}} = n$$

Thus for a given degree there are exactly n distinct, but not necessarily non-isomorphic, totally tamely ramified extensions. □

Pauli and Roblot have calculated convenient polynomials that generate totally tamely ramified extensions of $\mathbb{Q}_p$. We adapt their methods to prove the following result:

Theorem 5.17. Let ζ be a (p^f-1)st root of unity in K^{ur} and let $g = \gcd(p^f-1, n)$. Then for $0 \le r \le g-1$, all totally tamely ramified extensions over K^{ur} are generated by roots of the polynomial

$$x^n - \zeta^r\pi_K.$$

Proof. Consider the set of generating polynomials $\mathcal{R}_{1,2}^* = \{\zeta^i\pi_K \text{ with } 0 \le i \le p^f\}$ and $\mathcal{R}_{1,2} = \mathcal{R}_{1,2}^* \cup \{0\}$ Then the roots of the polynomials $x^n + \omega_{n-1}x^{n-1} + ... + \omega_0$, where $\omega_i \in \mathcal{R}_{1,2}$ for $1 \le i \le n-1$ and $\omega_0 \in \mathcal{R}_{1,2}^*$, generate all totally tamely ramified extensions of discriminant $\mathcal{M}_K^{n-1}$ by Theorem 5.13.

Consider extensions of K generated by roots of the polynomials $x^n - \zeta^i\pi$ so that $\omega_i = 0$ for $1 \le i \le n-1$. Suppose that α is such a root and $g = \gcd(n, p^f-1)$. Then since $\alpha \in L$ if and only if $\zeta^h\alpha \in L$ because $\zeta \in K$, $\zeta^h\alpha$ generates this same extension. If we choose h so that $nh + i \equiv r(\mod p^f-1)$ with $0 \le r < g$, then the minimal polynomial of $\zeta^h\alpha$ is $x^n + \zeta^{nh+i}\pi$ since:

$$\begin{aligned}(\zeta^h\alpha)^n + \zeta^{nh+i}\pi &= \zeta^{nh}\alpha^n + \zeta^{nh+i}\pi \\ &= \zeta^{nh}(\alpha^n + \zeta^i\pi).\end{aligned}$$

Hence we only need to consider the polynomials $x^n - \zeta^r\pi$ for $0 \le r \le g-1$. This polynomial is Eisenstein and by Theorem 5.3, it will define a totally tamely ramified extension.

Let $x^n - \zeta^r\pi$ and $x^n - \zeta^{r'}\pi$ be two of these polynomials which generate a totally tamely ramified extension where $0 \le r, r' \le g-1$ and $r \ne r'$. Let α and α' be roots of $x^n - \zeta^r\pi$ and $x^n - \zeta^{r'}\pi$ respectively. Suppose that α and α' generate the same field. Then this field would

contain an n-th root of $\zeta^{r-r'}$. To see this, consider the following: If we assume $\alpha \in L$ if and only if $\alpha' \in L$ then

$$\begin{aligned} \alpha^n + \zeta^r\pi = \quad 0 \quad &= (\alpha')^n + \zeta^{r'}\pi \\ \alpha^n - (\alpha')^n \quad &= \quad \zeta^{r'}\pi - \zeta^r\pi \\ &= \quad \pi(\zeta^{r'} - \zeta^r) \\ &= \quad \zeta^{r'}\pi(1 - \zeta^{r-r'}) \end{aligned}$$

Thus this field contains an n-th root of $\zeta^{r-r'}$ which contradicts our assumption that the field only contains the (p^f-1)-th roots of unity since $r-r'$ is never a multiple of n modulo p^f-1. Therefore α and α' must generate two distinct extensions of K. Let ρ be a primitive n-th root of unity in the algebraic closure of $\mathbb{F}_p((T))$ denoted $\overline{\mathbb{F}_p((T))}$ such that for $m = n/g$, $\rho^m = \zeta^{(p^f-1)/g}$. Then the conjugates of α over K are $\alpha, \rho\alpha, ..., \rho^{n-1}\alpha$. So $\alpha, \rho^m\alpha, ..., \rho^{(g-1)m}\alpha$ all generate the same field, but $\alpha, \rho\alpha, ...\rho^{m-1}\alpha$ all generate distinct isomorphic extensions. More specifically, the roots of the polynomial $x^n + \zeta^r\pi$ generate g classes of m distinct isomorphic extensions. Thus there are n total extensions generated by the roots of these polynomials. By Theorem 5.16 there are exactly n totally ramified extensions of degree n of K, which proves that all totally tamely ramified extensions of degree n of K are generated by the roots of the polynomials $x^n - \zeta^i\pi$. □

5.3. **Totally Wildly Ramified Extensions of Degree p.** Before discussing extensions of degree p, recall how the ramification groups were defined previously. In correspondence with these ramification groups are the groups of units. The group $\mathcal{U}_i = 1 + (\pi_L^i)$, which will also be written as $\mathcal{U}_i = 1 + \mathcal{M}_L^i$ corresponds to the group G_i. Recall that values i for which $G_i \neq G_{i+1}$ are called ramification breaks. From Artin-Schreier theory, which deals with extensions of degree equal to the characteristic, the Galois group G will be cyclic, namely $\mathbb{Z}/p\mathbb{Z}$. Because of that fact, the ramification groups will either be G or $\{1\}$ causing there to be a single, unique ramification break.

Definition 5.18. For K a field of characteristic p, an **Artin-Schreier polynomial** is a polynomial of the form $x^p - x - \alpha$ for $\alpha \in K^\times$ with $\alpha \neq 0$.

The following is a well-known result that leads to our next theorem.

Lemma 5.19 (Hilbert's Theorem 90, Additive Form)**.** Let L/K be a cyclic Galois extension with degree n and Galois group G. Let σ be a generator of G and let $\beta \in L$. Then $\mathrm{Tr}_{L/K}(\beta)$ is equal to 0 if and only if there exists $\alpha \in K$ such that $\beta = \alpha - \sigma(\alpha)$.

Proof. See [11, p.290]. □

Theorem 5.20. Any Galois extension of K of degree p is the splitting field of an Artin-Schreier polynomial.

Proof. Let L/K be a Galois extension of degree p. As stated above, the Galois group G will be cyclic of order p. Then $\mathrm{Tr}_{L/K}(-1) = p(-1) = 0$, since K has characteristic p. Let σ be a generator of G. By Lemma 5.19, there exists $\alpha \in L$ such that $\sigma(\alpha) - \alpha = 1$. Thus $\sigma(\alpha) = \alpha + 1$ and $\sigma^i(\alpha) = \alpha + i$ for $i = 1, \ldots, p$. Since α has p distinct conjugates, $[K(\alpha) : K] \geq p$. It follows that $L = K(\alpha)$. Note that

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha.$$

Since $\alpha^p - \alpha$ is fixed by σ, the generator of G, it is fixed by every element of G. Hence $\alpha^p - \alpha \in K$. Let $a = \alpha^p - \alpha$. Then α satisfies the equation $x^p - x - a = 0$ and L/K is the splitting field of an Artin-Schreier polynomial. $\square$

Theorem 5.21. There are infinitely many totally ramified extensions of a characteristic p field K of degree p.

Proof. Let $f(x) = x^p - x - \pi_K^{-m} \in K[x]$ with $m \in \mathbb{Z}$ be a generating polynomial such that $L = K[x]/f(x)$. Suppose L/K is a totally ramified extension with ν_L a discrete valuation on L and $G = \mathbb{Z}/p\mathbb{Z}$ the Galois group. Let $\pi_L \in L$ be a uniformizer. It suffices to show that there are an infinite number of values at which the unique ramification break can occur.

Consider $\nu_L(\sigma(\pi_L) - \pi_L) = \nu_L\left(\pi_L\left(\frac{\sigma(\pi_L)}{\pi_L} - 1\right)\right) = 1 + \nu_L\left(\frac{\sigma(\pi_L)}{\pi_L} - 1\right)$. With this equality, in G_i we can look at $\nu_L\left(\frac{\sigma(x)}{x} - 1\right) \geq i$ rather than $\nu_L(\sigma(x) - x) \geq i + 1$. It can be found in the proof of Lemma 3.2 that $\frac{\sigma(\pi_L)}{\pi_L} \in \mathcal{U}_L$. Thus, $\frac{\sigma(\pi_L)}{\pi_L} = u$ for some unit $u \in L$. Let $u = u_K w$ for $u_K \in \mathcal{U}_K$ and $w \in 1 + \mathcal{M}_L$. It is easily shown that we can define u in this way:

$$\begin{aligned} u &= a_0 + a_1\pi_L + \cdots \text{ (for some } a_i \in \mathcal{U}_K, i \geq 0) \\ &= a_0(1 + \frac{a_1}{a_0}\pi_L + \cdots) \text{ with } 1 + \frac{a_1}{a_0}\pi_L + \cdots \in 1 + \mathcal{M}_L. \end{aligned}$$

Write

$$\frac{\sigma(\pi_L)}{\pi_L} = u_K w.$$

Then we have

$$\sigma\left(\frac{\sigma(\pi_L)}{\pi_L}\right) \cdot \frac{\sigma(\pi_L)}{\pi_L} = \sigma(u_K w) \cdot u_K w.$$

Thus

$$\begin{aligned} \frac{\sigma^2(\pi_L)}{\pi_L} &= \sigma(u_K w) \cdot u_K w \\ &= u_K^2 w \cdot \sigma(w). \end{aligned}$$

The above comes from the fact that all σ in the Galois group fix elements of K by definition and $u_K \in \mathcal{U}_K$. Continue this process of multiplying by $\frac{\sigma(\pi_L)}{\pi_L} = \sigma(u_K w)$ on each side until, on the left hand side, the term is equal to $\frac{\sigma^p(\pi_L)}{\pi_L}$. Because this is a degree p extension with cyclic Galois group,

$$1 = \frac{\sigma^p(\pi_L)}{\pi_L} = u_K^p w\sigma(w) \cdots \sigma^{p-1}(w) \text{ where } w\sigma(w) \cdots \sigma^{p-1}(w) \in 1 + \mathcal{M}_L.$$

Thus, $u_K^p \in 1 + \mathcal{M}_L$ because, from above, $w\sigma(w) \cdots \sigma^{p-1}(w)$ and u_K^p must be units. Divide by $w\sigma(w) \cdots \sigma^{p-1}(w)$ to see $u_K^p \in 1 + \mathcal{M}_L$. This implies $u_K \in 1 + \mathcal{M}_L$ and, since the residue field of L will be the same as that of K in a totally ramified extension, $u_K \in 1 + \mathcal{M}_K$. Then, $\frac{\sigma(\pi_L)}{\pi_L} \in 1 + \mathcal{M}_L$.

This gives $\frac{\sigma(\pi_L)}{\pi_L} = 1 + u_L\pi_L^s$ for some $u_L \in \mathcal{U}_L$ and $s \geq 1$, where s does not depend of choice of uniformizer. From the proof of 3.2 part (a) we saw $\frac{\sigma(u)}{u} \equiv 1 (\text{mod } \pi_L^{s+1})$ for $u \in \mathcal{U}_L$. We can conclude for any $\lambda \in L^\times$, $\frac{\sigma(\lambda)}{\lambda} \in 1 + \pi_L^s\mathcal{U}_L$. To see this let $\lambda = u_L\pi_L^a$ with $p \nmid a$.

Then

$$\begin{aligned}\frac{\sigma(\lambda)}{\lambda} &= \frac{\sigma(u_L\pi_L^a)}{u_L\pi_L^a} \\ &= \frac{\sigma(u_L)}{u_L}\left(\frac{\sigma(\pi_L)}{\pi_L}\right)^a \in 1 + \pi_L^s\mathcal{U}_L.\end{aligned}$$

Thus, $\nu_L\left(\frac{\sigma(\lambda)}{\lambda} - 1\right) = s$. This implies that $G = G_s$ and $G_{s+1} = \{1\}$. This shows that the unique ramification break occurs at $i = s$.

Now suppose λ is a root of $f(x) = x^p - x - \alpha$, where $\alpha = \pi_K^{-m}$. Then,

$$\alpha = \lambda(\lambda + 1)\cdots(\lambda + (p - 1))$$

because if λ is a root, then $\lambda + n$ for $n \in \mathbb{Z}/p\mathbb{Z}$ is a root. In the above product, π_L^s divides λ but π_L^s does not divide $n = 1, \ldots, p - 1$. Thus, $(\lambda + 1), \cdots, (\lambda + (p - 1))$ are units. So, $\nu_K(\alpha) = \nu_L(\lambda)$, since $\alpha \in K$ and $\lambda \in L^\times$.

Therefore, $\nu_K(\alpha) = s$. For $\alpha = \pi_K^{-m}$, $-m = s$; because there are infinitely many choices for m, there are infinitely many ramification breaks, thus extensions of degree p. □

Example 5.22. Let $p = 5$ and $f(x) = x^5 - x - T^{-3}$.

- This will generate a degree 5 extension of $\mathbb{F}_5((T))$.
- Then the ramification groups $G_{-1} = G_0 = \cdots = G_3 = \mathbb{Z}/5\mathbb{Z}$ are cyclic.
- For $i \geq 4$, we have the groups $G_i = \{1\}$.

Note that when given two Artin-Schreier polynomials $f(x) = x^p - x - a$ and $g(x) = x^p - x - b$ for $a,\ b \in K$, $\nu(a) = \nu(b)$ does not imply the extensions generated by f and g are isomorphic. If the constant terms a and b differ by a function of the form $c^p - c$, then f and g will generate isomorphic extensions.

6. Example and Future Direction

To illustrate our results, we will look at counting all finite field extensions L/K where $K = \mathbb{F}_3((T))$ of degree $n = 10$ for $p = 3$ and discuss general properties of the defining polynomials and Galois group. We will also look at calculating the Galois group of a particular extension. For $n = 10$ and $p = 3$, $L/\mathbb{F}_3((T))$ is one of the following:

(1) a degree 10 unramified extension,
(2) a degree 2 totally tamely ramified extension of a degree 5 unramified extension,
(3) a degree 5 totally tamely ramified extension of a degree 2 unramified extension,
(4) or a degree 10 totally tamely ramified extension.

For the first case, there is one unique unramified extension by Theorem 4.4. This unique unramified extension is defined by the cyclotomic polynomial $x^{p^f} - 1$. For the degree 10 unramified extension, $f = 10$ and thus $x^{3^{10}} - 1$ is a defining polynomial. It is important to

note that this is not the only possible defining polynomial. In fact, Dummit and Foote [6, p.587] outline an algorithm for finding irreducible polynomials in the ring $\mathbb{F}_p[x]$, which can easily be applied to the polynomial ring over $\mathbb{F}_p((T))$ as well. The Galois group for this unramified extension is cyclic and isomorphic to $\mathbb{Z}/f\mathbb{Z}$, or $\mathbb{Z}/10\mathbb{Z}$ in this case.

For the second and third cases, there are unique unramified extensions of degree 2 and 5 respectively. These are each defined by the cyclotomic polynomial $x^{p^f} - 1$, where f is the residue degree of the unramified extension. This gives defining polynomials $x^{3^2} - 1$ and $x^{3^5} - 1$. The Galois group of each unramified portion of the extension is isomorphic to $\mathbb{Z}/f\mathbb{Z}$.

For the totally tamely ramified portion of the extensions in cases $2 - 4$, it is necessary to use a formula to count the non-isomorphic extensions. Since $3 \nmid 10$ we can use theorems in subsection 5.1 to count all distinct extensions. Theorem 5.16 states that there are n distinct degree n totally tamely ramified extensions. Theorem 5.17 tells us that for $g = \gcd(n, p^f - 1)$ there are g non-isomorphic extensions of degree n. Thus we know that there is 1 extension for case 1, $\gcd(3^2 - 1, 10) = 2$ non-isomorphic extensions for case 2, $\gcd(3^5 - 1, 10) = 2$ non-isomorphic extensions for case 3, and $\gcd(3^1 - 1, 10) = 2$ non-isomorphic extensions for case 4 for a total of 5 non-isomorphic extensions of degree 10 for $p = 3$. Theorem 5.17 also states that for the totally tamely ramified portion of the extension, the defining polynomials are in the form $x^n - \zeta^r \pi$.

Now let us look at calculating the Galois group of a specific extension of case 2. Suppose $L/\mathbb{F}_3((T))$ is a finite field extension and L is a degree 2 totally tamely ramified extension of a degree 5 maximal unramified extension of $\mathbb{F}_3((T))$, K^{ur}. Using methods described in [6, p.587], we find that $x^5 - x + 1$ is a defining polynomial for L/K^{ur}. Consider the polynomial $x^2 + Tx + T$ where T generates the maximal ideal in K^{ur}. Then this polynomial is Eisenstein and by Theorem 5.3, it generates a totally tamely ramified extension of degree 2. We can then use the properties of the ramification groups outlined in Theorem 3.2 to find the Galois group for the extension $L/\mathbb{F}_3((T))$. We will discuss two different methods of finding the Galois group for $L/\mathbb{F}_3((T))$ using the information from this theorem. The first method is to use the online L-functions and Modular Forms Database (LMFDB). The second technique is to use the GAP package in Sage to design a program for narrowing down possibilities for the Galois group.

For the first method, we use LMFDB [1], which has a Galois group database that gives such information as name, order, parity, solvability, and possible subfields for transitive subgroups of S_n. All possible Galois groups are given labels of the form $n\mathrm{T}k$. Here n signifies that the Galois group is a subgroup of S_n and k serves as an index of transitive subgroups of S_n. In our example, we know that the Galois group of L/K is a solvable subgroup of S_10. Using LMFDB we find that there are 24 such groups which satisfy this criterion. We also know that our Galois group will have two subfields since we need a group G_0/G_1 to correspond to the group of automorphisms of L/K^{ur}. According to LMFDB, there are only five groups with subfields. These possible Galois groups are:

Label	Name	Order	Parity	Solvable	Subfields
10T1	C_{10}	10	-1	Yes	2T1, 5T1
10T2	D_5	10	-1	Yes	2T1, 5T2
10T3	D_{10}	20	-1	Yes	2T1, 5T2
10T4	F_5	20	-1	Yes	2T1, 5T3
10T5	$F_5 \times C_2$	40	-1	Yes	2T1, 5T3

Finally, we consider the fact that the unramified portion of the extension is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Looking at the subfields, we find that 5T1 is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ and the only possible Galois group with 5T1 as a subfield is 10T1, which is isomorphic to $\mathbb{Z}/10\mathbb{Z}$. Note that there is additional data available from the LMFDB tables. In other cases, information such as order and parity is necessary for determining the Galois group and is also necessary for using the Galois groups to count the number of non-isomorphic extensions of a given degree.

A second method for determining the Galois group of an extension is to design a program in Sage using the GAP database. Again we use Theorem 3.2 to give us information on the possible Galois group for L/K. The main difference between this method and the first one is that Sage provides different information than LMFDB. For example, while Sage will not directly show the subfields, Sage can check the order of elements to see if a group is a p-group. The first step, as in the first method, is to find solvable transitive subgroups of S_{10}. Again, we find that there are 24 of these. We also know that our Galois group will contain a solvable subgroup, G_0 such that G/G_0 is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. We find that there are three such groups that fit this criteria: 10T1, 10T8, and 10T14. One final step is to check if there is a G_1 such that G_0/G_1 is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. This narrows it down to only one possible Galois group for L/K, 10T1, which is isomorphic to $\mathbb{Z}/10\mathbb{Z}$. This produced the same result as the first method.

Below is the program we used to find the Galois group of L/K:

```
Set G to be the set of transitive subgroups of S_10
Set a to be an empty list
for n in the range (1, cardinality of G plus 1) do
    if G[n] is a solvable group then
        Append n to the list a
    end if
end for
Set L to be an empty list
for n in the list a do
    Set G_0 to be the set of normal subgroups of G[n]
    for i in the range (1, cardinality of G_0) do
        if G_0[i] is solvable and n is not in our list L then
            Set G/G_0 equal to the quotient group G[n]/G_0[i]
            if G/G_0 is cyclic and has cardinality equal to 5 and n is not in the list L then
                if G_0[i] is cyclic and has cardinality equal to 2 then
                    Append n to the list L
                end if
            end if
        end if
    end for
end for
Print L
```

Both methods have their advantages and disadvantages. Each works only for classifying low degree extensions. While LMFDB gives detailed information about Galois groups, the possibilities must be examined by hand. Although programming in Sage is more efficient in some cases, our program becomes significantly slower as the degree of the extension increases.

In addition, the program may not be able to narrow the possibility down to a single Galois group and may need case-by-case alterations.

Further research could focus on generalizing the results to count the number of non-isomorphic tamely ramified extensions for a given degree regardless of the prime or for a given prime regardless of the degree much in the same way as Jones and Roberts did for extensions of $\mathbb{Q}_p$. In addition, it remains to extend our results for extensions of degree equal to the characteristic of the field to extensions of degree equal to a power of the characteristic of the field using Witt vectors.

7. Notation

Here is an appendix of notation used throughout this paper.

$\mathrm{Aut}(E/F)$	Automorphism group of the field E which fixes F
$\mathrm{Gal}(E/F)$	Galois group of the Galois extension E/F
$[E:F]$	Degree of the field extension E/F
$\lvert G\rvert, \lvert x\rvert$	Order of the group G or the element x respectively
$\lvert\cdot\rvert_T$	The absolute value, or norm, for $\mathbb{F}_p((T))$
$\nu(\cdot)$	The valuation in general and later, specifically for $\mathbb{F}_p((T))$
$\nu_p(\cdot)$, $\nu_T(\cdot)$	The valuation for the p-adic numbers, and for $\mathbb{F}_p((T))$, respectively
$\mathrm{Tr}_{L/K}(\cdot)$	The trace associated with the Galois extension L/K
$\mathcal{O}_K$	Ring of integers of K
$\mathcal{M}_K$	Maximal ideal of K
$\mathcal{U}_K$	Group of units of K
$k = \mathcal{O}/\mathcal{M}$	Residue field of K
e	Ramification index
f	Degree of the residue field
n	Degree of the extension
$\mathbb{F}_p[T]$	Polynomial ring over $\mathbb{F}_p$
$\mathbb{F}_p[[T]]$	Ring of formal power series over $\mathbb{F}_p$
$\mathbb{F}_p((T))$	Field of formal Laurent series over $\mathbb{F}_p$
G_i	The ith ramification group in G (Sec. 3)
K^{ur}	Maximal unramified extension of K (Sec. 4)

References

[1] LMFDB. Online database, 2012.

[2] Chad Awtrey. *Dodecic Local Fields*. PhD thesis, Arizona State University, 2010.

[3] Chad Awtrey. On galois groups of totally and tamely ramified sextic extensions of local fields. *International Journal of Pure and Applied Mathematics*, 70:855–863, 2011.

[4] Chad Awtrey. Dodecic 3-adic fields. *International Journal of Number Theory*, 8:933–944, 2012.

[5] Chad Awtrey and Trevor Edwards. Dihedral p-adic fields of prime degree. *International Journal of Pure and Applied Mathematics*, 75:185–194, 2012.

[6] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley and Sons, Inc., 3rd edition, 2004.

[7] I.B. Fesenko and S.V. Vostokov. *Local Fields and Their Extensions*. American Mathematical Society, 2nd edition, 2001.

[8] Fernando Q. Gouvêa. *p-adic Numbers*. Springer, 2nd edition, 1997.

[9] John W. Jones and David P. Roberts. A database of local fields. *Journal of Symbolic Computation*, 41:80–97, 2006.

[10] Kiran S. Kedlaya. *p-adic Differential Equations*. Cambridge University Press, 2010.

[11] Serge Lang. *Algebra*. Springer, 3nd edition, 2002.

[12] James S. Milne. Algebraic number theory (v3.04), 2012. Available at www.jmilne.org/math/.

[13] Sebastian Pauli. *Efficient Enumeration of Extensions of Local Fields with Bounded Discriminant*. PhD thesis, Concordia University, 2001.

[14] Sebastian Pauli and Xavier-François Roblot. On the computation of all extensions of a p-adic field of a given degree. *Mathematics of Computation*, 70(236):1641–1659, 2001.

[15] Jean-Pierre Serre. *Local Fields*. Springer, 1979.