Lubin-Tate Formal Groups and Local Class Field Theory

Submitted by
Emily Riehl
in partial fulfillment of the requirements
for the degree of Bachelor of Arts with Honors

Department of Mathematics
Harvard University

April 3, 2006

1 Introduction

The goal of local class field theory is to classify abelian Galois extensions of a *local field* K. Several definitions of local fields are in use. In this thesis, local fields, which will be defined explicitly in Section 2, are fields that are complete with respect to a discrete valuation and have a finite residue field. A prototypical first example is $\mathbb{Q}_p$, the completion of $\mathbb{Q}$ with respect to the absolute value $|\frac{a}{b}|_p := p^{-e}$, where e is the unique integer such that $\frac{a}{b} = p^e\frac{c}{d}$ and p does not divide the product cd.

Why study the abelian extensions of local fields? Initially, this area of study was motivated by questions about number fields. When K is a number field, its fractional ideals form a free abelian group generated by the prime ideals, and thus the quotient of this group modulo its principal ideals, called the *class group* C_K, is abelian. There exists a canonical everywhere unramified extension L/K such that the primes that split in L are precisely the principal ideals in K and such that $\mathrm{Gal}(L/K) \simeq C_K$, so the study of class groups leads naturally to the study of abelian extensions of K.

In some sense, number fields can be studied by investigating their behavior near a fixed prime ideal $\mathfrak{p}$. Let K be a number field with ring of integers A. The ideal $\mathfrak{p}$ is maximal in A because the quotient $A/\mathfrak{p}$ is a finite integral domain and hence a field. The inverse limit

$$A_\mathfrak{p} = \varprojlim A/\mathfrak{p}^n$$

defines a complete local ring containing A with a unique maximal ideal given by the kernel of the map $A_\mathfrak{p} \to A/\mathfrak{p}$. The field of fractions $K_\mathfrak{p}$ of $A_\mathfrak{p}$ is a local field, which contains K as

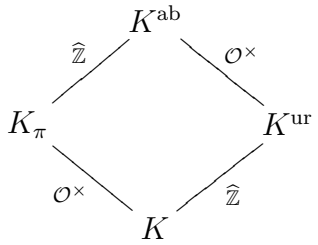
a dense subfield. If the finite field $A/\mathfrak{p}$ has characteristic p, then $K_\mathfrak{p}$ is a finite extension of $\mathbb{Q}_p$. This construction can be repeated for all global fields, which include algebraic function fields over a finite field as well as number fields, relating the study of local and global fields.

At first, results in local class field theory were derived as a consequence of the global case, but it was soon discovered that local class theory can be constructed independently and in fact provides tools that can be used to prove global theorems. Motivated by an analogy with the theory of complex multiplication on elliptic curves, Lubin and Tate showed how formal groups over local fields can be used to deduce several foundational theorems of local class field theory, beginning by explicitly describing the maximal abelian extension K^{ab} of a local field K. Their 1965 paper [4] provides a particularly elegant and approachable foundation for the subject by introducing formal power series that in some sense define a group law without a group, which will be used to provide a set of elements that are adjoined to K to produce certain abelian extensions with a natural module structure. Milne provides a concise, detailed account on the connection to multiplication on elliptic curves (see [6, pg 36-37]), though this is best read after one is familiar with the applications of the Lubin-Tate formal groups defined in Section 4.

More specifically, it is often useful to decompose extensions of local fields into what is called their *ramified* and *unramified* parts. When K is a local field and $\mathcal{O}$ its ring of integers, the ring $\mathcal{O}$ contains a unique maximal ideal $\mathfrak{m}$ that is also its only prime ideal. In an unramified extension, this ideal remains prime, so unramified extensions occur in bijection with extensions of the residue field $k = \mathcal{O}/\mathfrak{m}$. It follows that these extensions can be constructed canonically and that a maximal unramified extension $K^{\text{ur}} \subset K^{\text{ab}}$ exists. The Galois group $\text{Gal}(K^{\text{ur}}/K)$ is isomorphic to $\widehat{\mathbb{Z}}$, the inverse limit of the cyclic groups $\mathbb{Z}/n\mathbb{Z}$ for all positive n. Unramified extensions are discussed in greater detail in Section 2.2.

By contrast, a maximal *totally ramified* extension, i.e., an extension in which the prime ideal $\mathfrak{m}$ of K ramifies as much as possible, does not exist canonically because the composite of two totally ramified extensions is not always totally ramified. One of the first applications of Lubin-Tate formal groups is to construct a maximal totally ramified abelian extension $K_\pi \subset K^{\text{ab}}$ corresponding to each prime element $\pi \in K^{\text{ab}}$. In Section 6.1, we will prove that $K^{\text{ab}} = K_\pi \cdot K^{\text{ur}}$; hence, this construction provides the desired decomposition of K^{ab} into unramified and totally ramified parts.

Additionally, Lubin-Tate formal groups can be used to construct an injective homomorphism $\phi : K^\times \to \text{Gal}(K^{\text{ab}}/K)$ called the *Artin map*, named after a similar map first constructed in the global case by Emil Artin. The Artin map gives an isomorphism between the subgroup $\text{Gal}(K^{\text{ab}}/K^{\text{ur}})$ and $\mathcal{O}^\times$, the integral units of K. Combining this information, we get the following field diagram:



In particular, $\mathrm{Gal}(K^{\mathrm{ab}}/K) \simeq \widehat{\mathbb{Z}} \times \mathcal{O}^\times$. By choosing a prime element of K, we obtain an isomorphism $K^\times \simeq \mathbb{Z} \times \mathcal{O}^\times$. As $K^\times/\mathcal{O}^\times \simeq \mathbb{Z}$ is dense in $\widehat{\mathbb{Z}}$ and ϕ maps π to an element that generates this subgroup of $\mathrm{Gal}(K^{\mathrm{ur}}/K) \simeq \widehat{\mathbb{Z}}$, the image $\phi(K^\times)$ is dense in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. The Artin map satisfies further functorial properties as well. For example, this map factors through quotients of the norm groups $N(L^\times)$ of finite abelian extensions L/K to yield isomorphisms $K^\times/N(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$.

With the Langlands program, work is now being done on non-abelian class field theory, although this is beyond the scope of this thesis.

In Section 2, we will formally introduce local fields and their extensions and prove some preliminary results. In Section 3, we will discuss formal group laws in general, and in Section 4, we will define Lubin-Tate formal groups. In Section 5, we will state a theorem characterizing the Artin map and begin its proof by constructing homomorphisms to the Galois groups of large abelian extensions of K. In Section 6, we will show that the abelian extensions that we have constructed are in fact the maximal abelian extension K^{ab}, prove that the Artin map factors through quotients of finite norm groups, and conclude with a summary of these results. In Section 7, we provide an application of these results to the problem of counting abelian extensions with certain Galois groups.

The results in Sections 3, 4, and 5 have become fairly standard and were written in consultation with Milne [6], Iwasawa [3], Serre in [1], and the original Lubin Tate [4]. Milne [6] and Serre [1] both give cohomological proofs of the existence of the Artin map, and this result is assumed in Lubin Tate [4]. I will not assume that the local Artin map exists and will instead prove this in Section 6. Consequently, for this section as well as for the characterization of the norm groups of totally ramified extensions in Section 5, I will follow Iwasawa [3] instead. Section 7 represents my own work, in frequent consultation with Frank Calegari.

In my work on this project, I am indebted to many people. First and foremost, I would like to thank my thesis adviser Frank Calegari for help on all levels of this project, and particularly for suggesting many exercises that have helped improve the depth of my understanding of this material. John Tate has also been very generous with his time, allowing me to discuss these topics with him, both in person and over e-mail. Greg Valiant read a draft and provided many helpful comments. I am also indebted to Dick Gross, who first suggested that I study Lubin-Tate formal groups, read a draft of this paper, and has been a mentor to me for the past several years. Finally, I would like to thank the Harvard Math Department for challenging me and for making these past four years quite enjoyable.

2 Preliminaries

Let K be a field. A *discrete valuation* on K is a function $v : K^\times \to \mathbb{R}$ such that

(a) v is a group homomorphism, i.e., $v(xy) = v(x) + v(y)$ for all $x, y \in K$;

(b) the image of v is a discrete subgroup of $\mathbb{R}$;

(c) $v(x + y) \geq \min(v(x), v(y))$

with the convention that $v(0) = \infty$. A discrete valuation defines a topology on K with

respect to the metric $|x-y| = c^{-v(x-y)}$ for any constant $c > 1$. The choice of c is unimportant, because the resulting topologies are equivalent. The map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ is called a *multiplicative valuation* (to contrast with the *additive* discrete valuation defined above) and the restriction to $K^\times$ gives a multiplicative homomorphism $K^\times \to \mathbb{R}_+^\times$. By property (c), $|x+y| \leq \max(|x|, |y|)$ for all $x, y \in K$; such valuations $|\cdot|$ are said to be *non-archimedian*.

The *ring of integers* or *valuation ring* $\mathcal{O}$ of K is the set of elements with non-negative valuation. More generally, the valuation ring is the set $\{x \in K : |x| \leq 1\}$, a definition that applies to fields where only a multiplicative and not a discrete valuation is defined. The ring $\mathcal{O}$ has a unique maximal ideal $\mathfrak{m} = \{x \in \mathcal{O} : v(x) > 0\} = \{x \in \mathcal{O} : |x| < 1\}$ because all elements $x \in \mathcal{O}$ with valuation 0 are units, i.e., $\mathfrak{m} = \mathcal{O} - \mathcal{O}^\times$. Hence, $\mathcal{O}$ is a local ring. When v is normalized so that its image is equal to $\mathbb{Z}$, an element $\pi \in K$ such that $v(\pi) = 1$ is called an *uniformizer* or equivalently a *prime element*. For a fixed uniformizer π, every $a \in K$ can be expressed uniquely in the form $a = u\pi^n$ where $u \in \mathcal{O}^\times$ and $n = v(a) \in \mathbb{Z}$. It follows that $\mathcal{O}$ is a discrete valuation ring and its non-trivial ideals have the form $\pi^n\mathcal{O}$, $n \in \mathbb{Z}^+$. The quotient $k = \mathcal{O}/\mathfrak{m}$ is called the *residue field* of K.

A field, which is complete with respect to the topology defined by a discrete valuation v and such that its residue field k is finite, is called a *local field*. A good first example is $\mathbb{Q}_p$, the completion of $\mathbb{Q}$ with respect to the p-adic metric, a local field with ring of integers $\mathbb{Z}_p$. The ring $\mathbb{Z}_p$ can be thought of as the set of power series $\sum_{i=0}^{\infty} a_i p^i$ with coefficients $a_i \in \mathbb{Z}$ and p chosen as a natural uniformizer. Partial sums of these series form a sequence of rational integers that converge in the p-adic topology to an element of $\mathbb{Z}_p$. If the coefficients are restricted to a lift of the residue field $k \simeq \mathbb{Z}/p$, then these power series uniquely correspond to elements of $\mathbb{Z}_p$. Similarly, elements of $\mathbb{Q}_p$ uniquely correspond to Laurent series $\sum_{i=-n}^{\infty} a_i p^i$ with $a_i \in \{0, 1, \ldots, p-1\}$.

If the prime p is replaced with an indeterminate variable T, the resulting field is still local. In fact, these examples completely characterize our definition of a local field, as seen in the following Theorem (for proof, see Serre [7, pg 33-40]).

Theorem 2.1. *Let K be a local field.*

(a) If K has characteristic 0, then K is isomorphic to a finite extension of $\mathbb{Q}_p$ for some prime p.

(b) If K has characteristic p, then K is isomorphic to $k((T))$, the field of Laurent series over a finite field k of characteristic p.

Throughout this thesis, let the residue field k be a field of order q and characteristic p.

2.1 Hensel's Lemma and Teichmüller Representatives

One key tool in studying the algebra of local fields is Hensel's Lemma, which gives a criterion for when a polynomial has roots near a particular element of a local field K. There are many versions of this result. This formulation and proof are taken from Cassels Fröhlich [1].

Lemma 2.2 (Hensel's Lemma)**.** *Let K be a local field and let $f(X) \in \mathcal{O}[X]$. Let $\alpha_0 \in \mathcal{O}$ be*

such that $|f(\alpha_0)| < |f'(\alpha_0)|^2$. *Then there exists* $\alpha \in \mathcal{O}$ *such that* $f(\alpha) = 0$ *and*

$$|\alpha - \alpha_0| \leq \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|.$$

Proof. We will define a Cauchy sequence $\alpha_0, \alpha_1, \alpha_2, \ldots$ of approximate roots of $f(X)$ that converges to a root α by an iterative procedure similar to Newton's method. Define a sequence of functions $f_i(X) \in \mathcal{O}[X]$ by the algebraic identity

$$f(X + Y) = f(X) + f_1(X)Y + f_2(X)Y^2 + \cdots$$

over two independent variables. So $f_1(X) = f'(X)$. Define β_0 by the equation

$$f(\alpha_0) + \beta_0 f_1(\alpha_0) = 0.$$

Because $f_i(\alpha_0) \in \mathcal{O}$, $|f_i(\alpha_0)| \leq 1$, which means that

$$|f(\alpha_0 + \beta_0)| \leq \max_{i \geq 2} |f_i(\alpha_0)\beta_0^i| \leq \max_{i \geq 2} |\beta_0|^j \leq \frac{|f(\alpha_0)|^2}{|f_1(\alpha_0)|^2} < |f(\alpha_0)|.$$

Similarly, by expanding the polynomial $f_1(X + Y)$, $|f_1(\alpha_0 + \beta_0) - f_1(\alpha_0)| < |f_1(\alpha_0)|$. Let $\alpha_1 = \alpha_0 + \beta_0$. It follows from these equations that

$$(a)\ |f(\alpha_1)| \leq \frac{|f(\alpha_0)|^2}{|f_1(\alpha_0)|^2}, \quad (b)\ |f_1(\alpha_1)| = |f_1(\alpha_0)|, \quad (c)\ |\alpha_1 - \alpha_0| \leq \frac{|f(\alpha_0)|}{|f_1(\alpha_0)|}.$$

By hypothesis, $|f(\alpha_0)| < |f_1(\alpha_0)|^2$, so (a) implies that $|f(\alpha_1)| < |f(\alpha_0)|$, i.e., $v(f(\alpha_1)) > v(f(\alpha_0))$. By repeating this process, we can construct a sequence $\alpha_0, \alpha_1, \alpha_2, \ldots$, where each pair α_n, α_{n+1} also satisfies (a), (b), and (c). Because v is discrete, $v(f(\alpha_{n+1})) > v(f(\alpha_n))$ implies that $f(\alpha_n)$ approaches 0 as n gets large. Combining this fact with (b) and (c), we see that the sequence $\alpha_0, \alpha_1, \alpha_2, \ldots$ is Cauchy. Consequently, because K is complete, there exists $\alpha = \lim_{n \to \infty} \alpha_n$ in K, which has the desired properties. In fact, α is unique, because each iteration of this procedure essentially computes α mod $\mathfrak{m}^n$ for increasing n. □

It is worth illustrating how Hensel's Lemma may be applied. One example that highlights the analogy with Newton's method in $\mathbb{R}$ is finding a square root α of 2 in $\mathbb{Q}_7$, i.e., a root of the polynomial $f(X) = X^2 - 2$. Take $\alpha_0 = 3$ because $f(3) \equiv 0 \bmod 7$, so $v(f(\alpha_0)) = 1$ and $v(f'(\alpha_0)) = 0$. Hence, $v(f(\alpha_0)) > 2v(f'(\alpha_0))$, so $|f(\alpha_0)| < |f'(\alpha_0)|^2$ and the hypothesis of Hensel's Lemma are satisfied. The equation $f(\alpha_0) + \beta_0 f_1(\alpha_0) = 0$ gives $\beta_0 = -7/6$, which is the 7-adic integer $7 + 7^2 + 7^3 + \cdots$ (for a leisurely introduction to p-adic arithmetic, see Gouvêa [2]). So $\alpha_1 = \alpha_0 + \beta_0 = 3 + 7 + 7^2 + 7^3 + \cdots$ which indicates that $\alpha \equiv 10 \bmod 7^2$. The next iteration of this process shows that $\alpha \equiv 108 \bmod 7^3$. Continuing in this manner, this process very slowly constructs $\alpha \in \mathbb{Q}_7$ such that $\alpha^2 = 2$.

Another useful construction is the *Teichmüller representative*, which provides an inverse of sorts to the map $\mathcal{O}^\times \to k^\times$ by associating each $\alpha \in k^\times$ with a $(q-1)$-st root of unity $\overline{a}$

in $\mathcal{O}^\times$. The Teichmüller representatives are in bijection with the residue field and have the same multiplicative structure. Given any lift $a \in \mathcal{O}^\times$ of $\alpha \in k^\times$, define

$$\overline{a} := \lim_{n\to\infty} a^{q^n}.$$

Because the residue field has q elements, $a^q \equiv a \pmod{\mathfrak{m}}$ for each $a \in \mathcal{O}$ by an analogue of Fermat's Little Theorem. Furthermore, if $a \equiv b \pmod{\mathfrak{m}^n}$, then $a^q \equiv b^q \pmod{\mathfrak{m}^{n+1}}$. So the sequence, a^{q^n} is clearly Cauchy, and hence completeness of local fields implies that its limit is in $\mathcal{O}^\times$. The limit $\overline{a}$ clearly satisfies $X^q - X$, and so is in bijection with an element of $k^\times$, because a, and hence $\overline{a}$, is non-zero. Of course, additively, elements of $\mathcal{O}^\times$ behave quite differently from elements of $k^\times$, but multiplicatively the bijection between $\overline{a}$ and its image in the residue field is a homomorphism.

Alternatively, Hensel's Lemma can be used to prove the existence of Teichmüller representatives. Because the multiplicative group of the residue field k is cyclic of order $q-1$, the polynomial $f(X) = X^{q-1} - 1$ splits modulo $\mathfrak{m}$ into $q-1$ distinct linear factors. For any $a \in \mathcal{O}$ with valuation 0, $a \neq 0 \bmod \mathfrak{m}$, so $a^{q-1} - 1 \equiv 0 \bmod \mathfrak{m}$. However, the derivative $(q-1)a^{q-2} \neq 0 \bmod \mathfrak{m}$ because both terms on the left hand side are units. In particular, $v(f(a)) \geq 1 > 0 = 2v(f'(a))$, i.e., $|f(a)| < |f'(a)|^2$. By Hensel's Lemma, there exists a $(q-1)$-st root of unity α such that $\alpha - a \in \mathfrak{m}$, and because we can choose a to be in each of the $q-1$ distinct residue classes, there must $q-1$ distinct roots in K. In identifying a representative for a particular element of $\mathcal{O}^\times$, however, the construction via exponentiation is preferred to the more complicated construction given in the proof of Hensel's Lemma.

One important application of Teichmüller representatives is in the proof of the following lemma.

Lemma 2.3. *Let K be a local field with integers $\mathcal{O}$, maximal ideal $\mathfrak{m}$, and residue field k. Then $\mathcal{O}^\times \xrightarrow{\sim} k^\times \times (1+\mathfrak{m})$.*

Proof. By the construction given above, the map $a \mapsto \overline{a}$ from $a \in \mathcal{O}^\times$ to its Teichmüller representative in $\mathcal{O}^\times$ is a multiplicative homomorphism. By construction, the set of Teichmüller representatives is isomorphic to $k^\times$, and so $\overline{a} \xmapsto{\sim} \overline{a} \bmod \mathfrak{m}$, which we consider as an element of $k^\times$. Because $\overline{a} = \lim_{n\to\infty} a^{q^n}$, $\overline{a} \equiv a \bmod \mathfrak{m}$, so in particular, $\overline{a}/a \in 1+\mathfrak{m}$. Hence, the map $a \to a \bmod \mathfrak{m} \times (\overline{a}/a + \mathfrak{m})$ gives a homomorphism from $\mathcal{O}^\times$ to $k^\times \times (1+\mathfrak{m})$, which is easily seen to be an isomorphism. □

2.2 Extensions of Local Fields

An algebraic extension E/K is *separable* if the minimal polynomial of every $\alpha \in E$ does not have any multiple roots. An algebraic extension is *normal* if every irreducible polynomial over K with a root in E splits in E. When an extension is both normal and separable, for each $\alpha \in E$, the number of distinct automorphisms of $K(\alpha)/K$ equals the degree of this extension, and E/K is said to be *Galois*. When a separable extension fails to be normal, it can be embedded in its Galois closure by taking a splitting field. However, when an extension fails to be separable, this presents a more serious problem, because there is no larger field

in which an irreducible polynomial with multiple roots will yield the appropriate number of distinct automorphisms. As a result, it is customary to assume separability from the beginning; thus, requiring an extension E/K to be Galois simply amounts to replacing E with its Galois closure if necessary.

When K has characteristic zero, then every algebraic extension is separable, and K is what is called a *perfect* field. When K has characteristic p, K may not be perfect, so the additional hypothesis that extensions of K are separable will be required. Fix a separable, algebraic closure K^{s} of K, which is equal to the algebraic closure K^{al} in the case where K is a perfect field. Throughout this thesis, "an extension of K" will mean "a subfield of K^{s}." In particular, all extensions will be assumed to be algebraic and separable.

Let L be a finite extension of a local field K of degree n. If $\sigma_1, \ldots, \sigma_n$ denote the n distinct embeddings of L into its Galois closure over K, then there exist homomorphisms $\mathrm{Tr}_{L/K} : L \to K$ and $N_{L/K} : L^\times \to K^\times$ defined by

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha), \qquad N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

called the *trace map* and *norm map* respectively. The norm map will prove particularly important, and its image will be abbreviated by $N(L^\times)$ whenever there can be no confusion about the ground field K. This group will be characterized as a subgroup of $K^\times$ by Theorem 6.9.

The valuations v and $|\cdot|$ can be extended uniquely to L by the formulas (see [5, pg 105-106]):

$$v_L(\alpha) = \frac{1}{n} v(N_{L/K}(\alpha)), \qquad |\alpha|_L = \sqrt[n]{|N_{L/K}(\alpha)|}.$$

In particular, field automorphisms preserve v and $|\cdot|$. Note that if $\alpha \in K^\times$, then $N_{L/K}(\alpha) = \alpha^n$, so $v_L = v$ on $K^\times$ and likewise for $|\cdot|_L$. It will most often be convenient to normalize v so that $v(\pi) = 1$ for primes $\pi \in K$ even though the image of v_L may not be contained in $\mathbb{Z}$.

Infinite extensions of local fields are not themselves local, yet a local ring and maximal ideal can nonetheless be defined. If $[E : K]$ is infinite, define $\mathcal{O}_E = \bigcup \mathcal{O}_L$ and $\mathfrak{m}_E = \bigcup \mathfrak{m}_L$ where the unions are taken over all $K \subset L \subset E$ such that L/K is finite. Because v and $|\cdot|$ extend uniquely to each finite L/K, they also extend to E, although v may no longer be discrete. As in the finite case, $\mathcal{O}^{\mathrm{s}} = \{\alpha \in K^{\mathrm{s}} \mid |\alpha| \leq 1\}$ and $\mathfrak{m}^{\mathrm{s}} = \{\alpha \in K^{\mathrm{s}} \mid |\alpha| < 1\}$, giving further justification to these names.

For any Galois extension E/K, which may or may not be infinite, define a topology on $\mathrm{Gal}(E/K)$ where the sets

$$\mathrm{Gal}(E/L), \quad E \supset L \supset K, \quad [L : K] < \infty$$

form a fundamental system of neighborhoods of the identity. It follows that two elements of $\mathrm{Gal}(E/K)$ are "close" if they agree on a large subfield of E that is finite over K. If E/K is finite, then $\mathrm{Gal}(E/E) = \{1\}$ is open and the topology on $\mathrm{Gal}(E/K)$ is discrete. If E/K is infinite, then this is not the case.

It follows from this definition that $\mathrm{Gal}(E/K)$ is compact. To see this, consider the map $\mathrm{Gal}(E/K) \to \prod \mathrm{Gal}(L/K)$ where each component is the canonical projection map $\sigma \mapsto \sigma|_L$ and the product is taken over all $L \subset E$ that are finite and Galois over K. Because E is the union of finite Galois extensions, the map is injective. The topology described above is induced on $\mathrm{Gal}(E/K)$ via this map by endowing each $\mathrm{Gal}(L/K)$ with the discrete topology and the product with the product topology. Any closed subset of this product is compact, so to show that $\mathrm{Gal}(E/K)$ is compact it suffices to show that its image in $\prod \mathrm{Gal}(L/K)$ is closed. For every point $(\ldots, \sigma_L, \ldots)$ not in the image, there must be some components $\sigma_{L'}$ and $\sigma_{L''}$ such that $L' \subset L''$ and $\sigma_{L''}|L' \neq \sigma_{L'}$. Let $U = \prod_{L \neq L', L''} \mathrm{Gal}(L/K) \times \{\sigma_{L'}\} \times \{\sigma_{L''}\}$. Then U is an open subset of $\prod \mathrm{Gal}(L/K)$ that separates this point from the image of $\mathrm{Gal}(E/K)$. So the image of $\mathrm{Gal}(E/K)$ in this product is closed, and therefore, $\mathrm{Gal}(E/K)$ is compact.

Local class field theory studies the abelian extensions of a local field. The composite of two abelian extensions is again abelian because the group $\mathrm{Gal}(L_1 \cdot L_2/K)$ is a subgroup of the product $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ via the homomorphism $\sigma \mapsto (\sigma\,|_{L_1}, \sigma\,|_{L_2})$. Hence, it makes sense to define a maximal abelian extension K^{ab} of K as the composite of all finite ones.

One natural way to describe an abelian extension L/K is to separate it into a tower of its unramified and totally ramified parts. As a consequence of Lemma 2.4 below, L contains a canonical unramified extension F of K obtained by adjoining the Teichmüller representatives of the residue field k_L to K. The extension L/F will be totally ramified. By contrast, no canonical totally ramified subextension of L exists, a fact that will motivate the construction of K_π in Section 5.

There are many equivalent definitions of when an extension is ramified. In the local context, an extension L/K is *unramified* if a prime element π of K remains prime in L, i.e., if every $\alpha \in L$ can be written as $u\pi^n$ for some $u \in \mathcal{O}_L^\times$ and $n \in \mathbb{Z}$. The extension is *ramified* otherwise. For finite extensions, the *ramification degree* of L/K is the unique positive integer e such that the image of the extension of the normalized valuation v of K to $L^\times$ is $\frac{1}{e}\mathbb{Z}$. A prime element of K would have valuation 1, while a prime element of L would have valuation $\frac{1}{e}$. Note that if $e = 1$, then prime elements of K are prime in L and the extension is unramified. If $e = [L : K]$ then L/K is *totally ramified*. Equivalently, it follows from the definition of v_L that L/K is totally ramified if and only if $N(L^\times)$ contains a prime of K. If p does not divide e then the extension is *tamely ramified*, and it is *wildly ramified* otherwise.

2.2.1 Unramified Extensions

Unramified extensions are characterized through the following important lemma.

Lemma 2.4. *Let L/K be a finite, Galois extension. If L/K is unramified, then there is a canonical isomorphism $\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(k_L/k)$ where k_L is the residue field of L. Conversely, if $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(k_L/k)$, the L/K is unramified.*

Proof. Let L/K be finite and Galois, let $k_L = k[a]$, and let $\overline{g}(X)$ be the minimal polynomial for a. Because k is finite, it is perfect, and $\overline{g}(X)$ has distinct roots. If $g(X)$ is any lift of

$\overline{g}(X)$ to L, then by Hensel's Lemma there exists a unique $\alpha \in L$ such that $g(\alpha) = 0$ and $\alpha \equiv a \bmod \mathfrak{m}$. Because L is Galois, g splits in L, so $\overline{g}$ splits in k_L, and k_L/k is Galois.

Automorphisms of L/K preserve $\mathcal{O}_L$ and $\mathfrak{m}_L$, so there is a well-defined homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$. When L/K is unramified, $[L : K] = [\mathcal{O}_L : \mathcal{O}] = [\mathcal{O}_L/(\pi) : \mathcal{O}/(\pi)] = [k_L : k]$, so $L = K(\alpha)$ and each $\sigma \in \mathrm{Gal}(L/K)$ maps α to a distinct conjugate. The conjugates of α are distinct in k_L, because finite fields are perfect, which means that $\overline{g}$ is separable. Thus, by Hensel's Lemma, the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ is surjective, and therefore an isomorphism.

Conversely, if $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(k_L/k)$, then $[\mathcal{O}_L/\mathfrak{m}_L : \mathcal{O}/\mathfrak{m}] = [k_L : k] = [L : K] = [\mathcal{O}_L/\mathcal{O}] = [\mathcal{O}_L/(\pi) : \mathcal{O}/(\pi)]$. As $\mathcal{O}_L$ has only one ideal of each index, this implies that $\mathfrak{m}_L = (\pi)$. In particular, π remains prime in L, so L/K is unramified. □

The composite of two unramified extensions is again unramified, so it makes sense to define a maximal unramified extension K^{ur} of K as the union of all finite unramified extensions. One natural question is whether $K^{\mathrm{ur}} \subset K^{\mathrm{ab}}$. This is true, and follows as a consequence of the following lemma.

Lemma 2.5. *For any local field K and positive integer n, there exists a unique unramified extension L of degree n over K, which is Galois with cyclic Galois group.*

Proof. It is well known that the elements of the finite field k of order q are precisely the roots of $X^q - X$ in the separable closure of $\mathbb{Z}/p$. Furthermore, there exists a unique cyclic extension of degree n over k consisting of the roots of $X^{q^n} - X$. Let $\overline{g}(X)$ be the minimal polynomial for a primitive $(q^n - 1)$-st root of unity over k and let $g(X)$ be any lift of $\overline{g}(X)$ to K. Then g is irreducible because it is irreducible mod $\mathfrak{m}$. Let L be the splitting field of g over K. By the theory of Teichmüller representatives, the roots of g in L are in bijection with the roots over k, so they are distinct. Hence, L/K is separable and Galois, and because the degree of g is equal to the degree of $\overline{g}$, $[L : K] = [\mathbb{F}_{q^n} : k] = n$. Let k_L be the residue field of L. By construction, $k_L \supset \mathbb{F}_{q^n}$, so $[k_L : k] \geq n$. But $[L : K]$ is always greater than or equal to $[k_L : k]$, so $k_L = \mathbb{F}_{q^n}$. Because $\mathrm{Gal}(L/K)$ maps onto $\mathrm{Gal}(k_L/k)$ and these groups have the same order, they are isomorphic, so from Lemma 2.4, L/K is an unramified extension of degree n, as desired. In particular, $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(k_L/k)$, which is cyclic because k_L/k is a finite Galois extension of finite fields.

For uniqueness, assume two distinct unramified extensions L, L' existed. Then the composite extension LL' would also be unramified over K. By the above observation that the Galois groups of L/K and L'/K are both $\mathbb{Z}/n$, and the Galois group of LL'/K must be a finite cyclic group as well. Let $E = L \cap L'$, also an unramified extension of K of order n/m. Then $\mathrm{Gal}(L/E) \simeq \mathrm{Gal}(L'/E) = \mathbb{Z}/m$, because this extension is unramified. Because $L \cap L' = E$, $\mathrm{Gal}(LL'/E) \simeq \mathbb{Z}/m \times \mathbb{Z}/m$, which is not cyclic, contradicting the fact that this extension is unramified. This contradiction guarantees uniqueness. □

Not only is $\mathrm{Gal}(L/K)$ cyclic when L/K is unramified, but it has a canonical generator. Let $r = [k_L : k]$, where k is a finite field of order $q = p^f$. Then the map $\mathrm{Frob}(x) = x^q$ is an automorphism of k_L/k called the *Frobenius* automorphism. Because k_L has order q^r,

$\mathrm{Frob}^r(x) = x^{q^r} = x$ for all $x \in k_L$ so Frob has order dividing r. If Frob^d were the identity for some $d < r$, then the elements of k_L would all be roots of $X^{q^d} - X$, which cannot be because $q^d < \#k_L$. So Frob has order r and thus generates $\mathrm{Gal}(k_L/k)$. By the isomorphism, for unramified extensions there is a unique automorphism $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma x \equiv x^q \pmod{\pi}$ for all $x \in L$ and that generates $\mathrm{Gal}(L/K)$. This automorphism is denoted by $\mathrm{Frob}_{L/K}$.

It follows from Lemma 2.5 that $K^{\mathrm{ur}} = \cup K_n$ where K_n denotes the unique unramified extension of K of degree n. By the theory of Teichmüller representatives, K_n is in fact the splitting field of $X^{q^n} - X$ over K. Furthermore, the Frobenius automorphism extends to K^{ur} and can be identified as the image of the generators of $\mathrm{Gal}(K_n/K) = \mathbb{Z}/n$ in

$$\mathrm{Gal}(K^{\mathrm{ur}}/K) = \widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}.$$

2.2.2 Ramified Extensions

In general, ramified extensions are more complicated than their unramified counterparts. To study these extensions, it is useful to keep more precise track of the behavior of elements of its Galois group. For any Galois extension L/K, there exist subgroups

$$I_n = \{\sigma \in \mathrm{Gal}(L/K) \mid v(x - \sigma x) \geq n + 1 \ \forall x \in L\}$$

called *higher ramification groups* for each $n \in \mathbb{N}$. The higher ramification groups clearly form a chain of decreasing subgroups $\mathrm{Gal}(L/K) \supseteq I_0 \supseteq I_1 \supseteq \cdots$. The group I_0 is the inertia group I that arises as the kernel of the exact sequence

$$0 \to I \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k) \to 0$$

because $\sigma \in I_0$ if and only if σ acts trivially on the residue field.

When L/K is unramified, $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(k_L/k)$ by Lemma 2.4, so the inertia group is trivial. Conversely, if the inertia group is trivial, then $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(k_L/k)$, which implies that L/K is unramified. In general, $\mathrm{Gal}(L/K)/I_0 \simeq \mathrm{Gal}(k_L/k)$ is the Galois group of the largest unramified subextension of L/K.

When L/K is totally ramified, the index $[\mathfrak{m}_L : \mathfrak{m}] = n$, which means that $[k_L : k] = [\mathcal{O}_L/\mathfrak{m}_L : \mathcal{O}/\mathfrak{m}] = [L : K]/[\mathfrak{m}_L : \mathfrak{m}] = n/n = 1$. So $k_L = k$ and $\mathrm{Gal}(k_L/k)$ is trivial, which means that $I_0 = \mathrm{Gal}(L/K)$. In this case, the higher ramification groups can be identified by computing $v(\pi - \sigma\pi)$ for a fixed prime $\pi \in L$, a fact that is proven in the following lemma.

Lemma 2.6. *Let L/K be totally ramified and let $\pi \in L$ be any prime element. Then the group $I_n = \{\sigma \in \mathrm{Gal}(L/K) \mid v(\pi - \sigma\pi) \geq n + 1\}$.*

Proof. If $\sigma \in I_n$, then from the original definition, it is clear that $v(\pi - \sigma\pi) \geq n+1$. To show conversely that if $v(\pi - \sigma\pi) \geq n+1$ then $\sigma \in I_n$, it suffices to show that $v(\pi - \sigma\pi) \leq v(x - \sigma x)$ for all $x \in L$.

Let $a_1, \ldots, a_q \in L$ denote any lift of the residue field k_L such that the a_i are distinct modulo $\mathfrak{m}_L$. Then any $x \in L$ can be written uniquely as $b_{-n}\pi^{-n} + \cdots + b_0 + b_1\pi + \cdots$

where the coefficients b_i are in the set $\{a_1, \ldots, a_q\}$. Choose the set $\{a_1, \ldots, a_q\}$ to be the Teichmüller representatives in L. Then the a_i are fixed by $\mathrm{Gal}(L/K) = I_0$. So given $x \in L$ and $\sigma \in \mathrm{Gal}(L/K)$, $x - \sigma x = b_1(\pi - \sigma\pi) + b_2(\pi^2 - (\sigma\pi)^2) + \cdots$, because the terms of valuation less than one must vanish because $\mathrm{Gal}(L/K) = I_0$. This expression can be factored to yield $x - \sigma x = (\pi - \sigma\pi)(b_1 + b_2(\pi + \sigma\pi) + \cdots)$. As $x - \sigma x$ is the product of $\pi - \sigma\pi$ and an integer, it follows that $v(\pi - \sigma\pi) \leq v(x - \sigma x)$, completing this proof. □

The following lemma will prove useful later on.

Lemma 2.7. *Let L/K be a finite Galois extension of local fields. Then if the residue field of L has order q', $[I_0 : I_1] \mid (q' - 1)$ and $[I_n : I_{n+1}] \mid q'$ for $n \geq 1$. Furthermore, for large enough m, $I_n = \{1\}$ for all $n > m$, so I_1 has p-power order.*

Proof. For the first claim, we will prove something slightly stronger: namely, that there is a homomorphism $I_0 \to \mathcal{O}_L^\times/(1 + \mathfrak{m}_L)$ with kernel I_1 given by $\sigma \mapsto \sigma\pi/\pi$ where π is a fixed prime in L. To see this, note that $\sigma\pi$ and π have the same valuation, so this element is indeed a unit. For $\sigma, \tau \in I_0$, $\tau(\sigma\pi/\pi) \equiv \sigma\pi/\pi \bmod \mathfrak{m}_L$, so $\tau\sigma\pi/(\tau\pi) \equiv \sigma\pi/\pi$ and hence $\tau\sigma\pi/\pi \equiv (\tau\pi/\pi)(\sigma\pi/\pi) \bmod \mathfrak{m}_L$. In particular, this map is a homomorphism, as claimed. If $\sigma \in I_1$, then $\sigma\pi \equiv \pi \bmod \mathfrak{m}_L^2$, which by division implies that $\sigma\pi/\pi \in 1 + \mathfrak{m}_L$, so I_1 is contained in the kernel of this map. For the converse, if $\sigma\pi/\pi \in 1 + \mathfrak{m}_L$, then $\sigma\pi \equiv \pi \bmod \mathfrak{m}_L^2$. By definition I_0 acts trivially on the residue field. Hence, because σ fixes $\pi \bmod \mathfrak{m}_L^2$, $\sigma \in I_1$, proving that this is the kernel of the homomorphism. It follows that $I_0/I_1 \hookrightarrow \mathcal{O}_L^\times/(1 + \mathfrak{m}_L) \simeq k_L^\times$, so in particular, this quotient has order dividing $q' - 1$.

More generally, there is an injective homomorphism $I_n/I_{n+1} \hookrightarrow (1+\mathfrak{m}_L^n)/(1+\mathfrak{m}_L^{n+1})$ given by the map $\sigma \mapsto \sigma\pi/\pi$ for any $n \geq 0$. From this map, it is clear that I_n/I_{n+1} has p-power order if and only if every element $1 + \pi^n u$ of $(1 + \mathfrak{m}_L^n)/(1 + \mathfrak{m}_L^{n+1})$ does. The latter follows immediately from the isomorphism $(1+\mathfrak{m}_L^n)/(1+\mathfrak{m}_L^{n+1}) \to k_L$ given by the map $1+\pi^n u \mapsto u$.

Finally, we show that for large enough index, I_n is trivial. For each $\sigma \in \mathrm{Gal}(L/K)\backslash\{1\}$, there is some $x \in K$ not fixed by σ. Let $s_\sigma = v(x - \sigma x)$ for this particular x. As $\mathrm{Gal}(L/K)$ is finite there is some integer m greater than s_σ for each non-trivial σ. For all $n > m$, I_n is clearly trivial. It follows that I_1 has p-power order, completing this proof. □

3 Formal Group Laws

For any commutative ring A with identity, we define $A[[T]]$ to be the ring of formal power series $\sum_{i \geq 0} a_i T^i$, where addition and multiplication of two power series are defined in the usual way. Power series in several variables can be defined similarly. When $f \in A[[T]]$ and $g \in TA[[T]]$ then the composition $f(g(T))$ makes sense. However, if g has a nonzero constant term, then computing the constant term of $f(g(T))$ would require an infinite sum; because we are dealing with purely formal sums, we have no notion of convergence, and this is not possible.

A *commutative formal group law* is a power series $F \in A[[X, Y]]$ such that

(a) $F(X, Y) = F(Y, X)$ in $A[[X, Y]]$;

(b) $F(0,Y) = Y$ and $F(X,0) = X$;
(c) $F(X,F(Y,Z)) = F(F(X,Y),Z)$ in $A[[X,Y,Z]]$.

Here $0 \in A$ is the additive identity in $A[[T]]$. Note that substitution is permitted in (c) because (b) implies that $F(X,Y)$ has no constant term.

The power series F can be thought of as providing a group operation for the variables X and Y prior to identifying a group in which these elements belong. Indeed, the notation $X +_F Y := F(X,Y)$ is sometimes adopted to make idea more obvious. In this light, property (a) gives commutativity, (b) identity, and (c) associativity for elements of $TA[[T]]$. Property (b) is often given as $F(X,Y) \equiv X + Y$ (mod deg. 2), and this substitution is equivalent (see [3, pg 50] or [6, pg 16-17] for the non-obvious implication).

A simple but important example of a commutative formal group law is the polynomial $F(X,Y) = X + Y + XY$. We will return to this example later.

To show that inverses exist in $TA[[T]]$ for the group law $F(X,Y)$, it suffices to show that the indeterminate T is invertible. This is accomplished by the following lemma.

Lemma 3.1. *There is a unique $h(T) \in TA[[T]]$ such that $F(T,h(T)) = 0$.*

Proof. From property (b), it is clear that $F(X,Y) = X+Y+\sum_{i,j\geq 1} a_{ij}X^iY^j$; i.e., F contains no higher order terms in only one variable. Hence, the equation $F(T,h(T)) = 0$ can be solved by inductively constructing polynomial solutions $h_n(T)$ to the equations $F(T,h_n(T)) \equiv 0$ (mod deg. n). It is easy to see that $h_2(T) = -T + a_{11}T^2$. Given a polynomial $h_n(T)$ such that $F(T,h_n(T)) \equiv 0$ (mod deg. n), then the equation $F(T,h_n(T) + b_{n+1}T^{n+1}) \equiv 0$ (mod deg. $n+1$) amounts to a one-variable linear equation in the coefficients of h_n and F, which can certainly be solved. □

Note that if $f(T) \in TA[[T]]$, then $F(f(T), h \circ f(T)) = 0$. Hence, for any commutative formal group law F, the addition law $f +_F g := F(f(T), g(T))$ makes $TA[[T]]$ into an abelian group. In what follows, let $i_F : TA[[T]] \to TA[[T]]$ be the map that takes a power series f to its inverse $i_F \circ f$ with respect to the commutative formal group law $+_F$.

Let $F(X,Y)$ and $G(X,Y)$ be two commutative formal group laws over the same ring A. A power series $f \in TA[[T]]$ such that $f(F(X,Y)) = G(f(X), f(Y))$, or, more familiarly, $f(X +_F Y) = f(X) +_G f(Y)$, is called a *homomorphism* and written as $f : F \to G$. If there exists a power series $g \in TA[[T]]$ such that $g : G \to F$ and $f \circ g = g \circ f = T$, then f is an *isomorphism*. As usual, a homomorphism $f : F \to F$ is called an *endomorphism*. For example, when $F(X,Y) = X + Y + XY$, $f(T) = (1+T)^p - 1$ is an endomorphism. In general:

Lemma 3.2.
(a) The set $\mathrm{Hom}(F,G)$ *is a subgroup of $TA[[T]]$ with respect to the addition law $+_G$.*
(b) $\mathrm{End}(F)$ *forms a ring with respect to the addition law $+_F$ and the multiplication law of composition.*

The proof of this lemma will require the associativity of composition in the ring $TA[[T]]$, which we might as well check now. This particularly clever proof of associativity is given in Milne [6, pg 15].

Lemma 3.3. *Let $f, g, h \in TA[[T]]$. Then $f \circ (g \circ h) = (f \circ g) \circ h$.*

Proof. For any $f, g, h \in TA[[T]]$, $(fg) \circ h = (f \circ h)(g \circ h)$. In particular, $f^n \circ g = (f \circ g)^n$. When $f = T^n$, both $(f \circ g) \circ h$ and $f \circ (g \circ h)$ equal $(g \circ h)^n$, and when $f = \sum_{n \geq 1} a_n T^n$, both equal $\sum_{n \geq 1} a_n (g \circ h)^n$. □

When dealing with power series in multiple variables, we will abuse notation slightly and write $G \circ f$ for $G(f(X), f(Y))$. For example, $f : F \to G$ is a homomorphism if and only if $f \circ F = G \circ f$.

Proof of Lemma 3.2. Let $f, g \in \mathrm{Hom}(F, G)$ and let $h = f +_G g$. Then $h \circ F = f \circ F +_G g \circ F = G \circ f +_G G \circ g = (f(X) +_G f(Y)) +_G (g(X) +_G g(Y))$. By associativity and commutativity in $TA[[T]]$, this equals $(f(X) +_G g(X)) +_G (f(Y) +_G g(Y)) = h(X) +_G h(Y) = G \circ h$. Hence, $h \in \mathrm{Hom}(F, G)$. Using associativity and commutativity again, it follows that $G(G, G \circ i_G) = (X +_G Y) +_G (i_G(X) +_G i_G(Y)) = (X +_G i_G(X)) +_G (Y +_G i_G(Y)) = 0 +_G 0 = 0$, so $G \circ i_G = i_G \circ G$. Hence, for any $f \in \mathrm{Hom}(F, G)$, $G \circ (i_G \circ f) = (G \circ i_G) \circ f = i_g \circ (G \circ f) = i_g \circ (f \circ F) = (i_g \circ f) \circ F$. So $i_G \circ f \in \mathrm{Hom}(F, G)$. Trivially, $0 \in \mathrm{Hom}(F, G)$, so it is indeed a subring under $+_G$.

Associativity of composition is given in Lemma 3.3, so to show that $\mathrm{End}(F)$ is a ring, it remains to only check distributivity. For any $f \in \mathrm{End}(F)$, $f \circ (g +_F h) = f \circ F(g(X), h(Y)) = F(f(g(X)), f(h(Y)) = f \circ g +_F f \circ h$. With the note that T acts as the multiplicative identity for $\mathrm{End}(F)$, the proof is complete. □

Now let $A = \mathcal{O}$, the ring of integers of a local field K, and $F \in A[[X, Y]]$ be a commutative formal group law. For any $x, y \in \mathfrak{m}_L \subset \mathcal{O}_L$, the maximal ideal in the ring of integers of a finite extension L of K, the series $F(x, y)$ converges. So $\mathfrak{m}_L$ becomes a commutative group with addition $x +_F y := F(x, y)$. For example, if $F(X, Y) = X + Y + XY$, then the operation $+_F$ on $\mathfrak{m}$ is simply the multiplicative group law of $1 + \mathfrak{m}$. Furthermore, because $f(T) = (1 + T)^p - 1$ is an endomorphism of F, the following diagram commutes,

$$\begin{array}{ccc} \mathfrak{m} & \xrightarrow{f} & \mathfrak{m} \\ \downarrow{\scriptstyle a \mapsto 1+a} & & \downarrow{\scriptstyle a \mapsto 1+a} \\ 1 + \mathfrak{m} & \xrightarrow{a \mapsto a^p} & 1 + \mathfrak{m} \end{array}$$

where $\mathfrak{m}$ is an abelian group under $+_F$ and $1 + \mathfrak{m}$ is an abelian group under the usual multiplication in $K^\times$.

4 Lubin-Tate Formal Groups

For the remainder of this paper, let K be a local field and $A = \mathcal{O}$. For each prime element $\pi \in K$, let $\mathcal{F}_\pi$ be the set of power series $f \in \mathcal{O}[[X]]$ such that:

(a) $f(X) \equiv \pi X \pmod{\text{deg. } 2}$

(b) $f(X) \equiv X^q \pmod{\pi}$

where q is the order of the residue field k of K. The second condition means that the image

of f under the homomorphism $\mathcal{O}[[X]] \to k[[X]]$ that maps each coefficient to its residue modulo π is X^q. In other words, the elements of $\mathcal{F}_\pi$ are precisely those power series whose derivative at 0 is π and which reduce modulo $\mathfrak{m}$ to the Frobenius map.

For example, the polynomial $f(X) = \pi X + X^q$ always lies in $\mathcal{F}_\pi$. When $K = \mathbb{Q}_p$ and $\pi = p$, then $f(X) = (1+X)^p - 1$ lies in $\mathcal{F}_\pi$ as well.

Proposition 4.1. *For each $f \in \mathcal{F}_\pi$ there exists a unique commutative formal group law F_f with coefficients in $\mathcal{O}$ such that f is an endomorphism.*

This F_f is the *Lubin-Tate formal group law* for f. Proof of Proposition 4.1 requires the following lemma.

Lemma 4.2. *Let $f, g \in \mathcal{F}_\pi$ and let $\phi_1(X_1, \ldots, X_n)$ be a linear form over $\mathcal{O}$. There is a unique $\phi \in \mathcal{O}[[X_1, \ldots, X_n]]$ such that*

(a) $\phi \equiv \phi_1$ (mod deg. 2)

(b) $f(\phi(X_1, \ldots, X_n)) = \phi(g(X_1, \ldots, X_n))$.

Proof. The idea is to construct ϕ by successive polynomial approximations ϕ_r that satisfy (a) and (b) (mod deg. $r+1$) and are unique (mod deg. $r+1$). Note that $f \circ \phi_1 \equiv \phi_1 \circ g$ (mod deg. 2) and, by condition (a), ϕ_1 is unique, so this linear form is appropriately named. Given the existence of a unique ϕ_r, let $\phi_{r+1} = \phi_r + h$, where $h \in \mathcal{O}[X_1, \ldots, X_n]$ is homogeneous of degree $r+1$. As $f \in \mathcal{F}_\pi$, $f \circ \phi_{r+1} \equiv f \circ \phi + \pi h$ (mod deg. $r+2$). Similarly, $\phi_{r+1} \circ g \equiv \phi_r \circ g + h(\pi X_1, \ldots, \pi X_n) \equiv \phi_r \circ g + \pi^{r+1} h$. So condition (b) is satisfied if $(\pi^{r+1} - \pi)h = f \circ \phi_r - \phi_r \circ g$ (mod deg. $r+2$). Modulo π, $f(X) \equiv g(X) \equiv X^q$, so $f \circ \phi_r - \phi_r \circ g \equiv \phi_r(X_1, \ldots, X_n)^q - \phi_r(X_1^q, \ldots, X_n^q)$, and this is equivalent to 0 mod π because we are working in characteristic p. So π divides $f \circ \phi_r - \phi_r \circ g$. Because $\pi^r - 1 \in \mathcal{O}^\times$, h does indeed have coefficients in $\mathcal{O}$, so our construction of ϕ_{r+1} is valid. In this manner, we inductively construct a power series ϕ such that $f \circ \phi = \phi \circ g$ (mod deg. r) for all r. Clearly, $\phi \equiv \phi_1$ (mod deg. 2), completing the proof. □

The characterization of Lubin-Tate formal group laws now follows.

Proof of Proposition 4.1. By Lemma 4.2, for each $f \in \mathcal{F}_\pi$, there exists a unique power series $F_f \in \mathcal{O}[[X, Y]]$ such that $F_f(X, Y) \equiv X + Y$ (mod deg. 2) and $f \circ F_f = F_f \circ f$. It remains to show that F_f is a commutative formal group law. It is clear that $F_f(X, F_f(Y, Z)) \equiv X + Y + Z \equiv F_f(F_f(X, Y), Z)$ (mod deg. 2). Furthermore, $f \circ F_f(X, F_f(Y, Z)) = F_f(f(X), f \circ F_f(Y, Z)) = F_f(f(X), F_f(f(Y), f(Z)))$ and similarly $f \circ F_f(F_f(X, Y), Z) = F_f(F_f(f(X), f(Y)), f(Z))$. So by the uniqueness statement in Lemma 4.2, $F_f(X, F_f(Y, Z)) = F_f(F_f(X, Y), Z)$. As $F_f(X, 0) \equiv X$ and $F_f(0, Y) \equiv Y$ (mod deg. 2) and each power series commutes with f, the uniqueness statement in Lemma 4.2 again shows that $F_f(X, 0) = X$ and $F_f(0, Y) = Y$. Similarly, as $F_f(X, Y) \equiv F_f(Y, X) \equiv X + Y$ (mod deg. 2) and f commutes with each series, $F_f(X, Y) = F_f(Y, X)$, completing the proof. □

Let $f \in \mathcal{F}_\pi$ and let F_f denote the corresponding Lubin-Tate formal group law given by Proposition 4.1. By Lemma 4.2 for each $a \in \mathcal{O}$, there exists a unique $[a]_f \in \mathcal{O}[[X]]$ such that

(a) $[a]_f \equiv aX \pmod{\text{deg. } 2}$;
(b) $[a]_f \circ f = f \circ [a]_f$.
Note, for example, that $[\pi]_f = f$.

Proposition 4.3. *For each $a \in \mathcal{O}$, $[a]_f \in \mathrm{End}(F_f)$. Furthermore, the map $a \mapsto [a]_f$ defines an injective ring homomorphism $\mathcal{O} \hookrightarrow \mathrm{End}(F_f)$.*

Proof. Once again, this proof is an easy exercise in the application of Lemma 4.2. As $[a]_f \equiv aX \pmod{\text{deg. } 2}$, $[a]_f \circ F_f \equiv aX + aY \equiv F_f \circ [a]_f \pmod{\text{deg. } 2}$. Because both F_f and $[a]_f$ commute with f, $f \circ ([a]_f \circ F_f) = [a]_f \circ f \circ F_f = ([a]_f \circ F_f) \circ f$ and similarly, $f(F_f([a]_f(X), [a]_f(Y))) = F_f(f([a]_f(X)), f([a]_f(Y))) = F_f([a]_f(f(X)), [a]_f(f(Y)))$. By the uniqueness statement in Lemma 4.2, $[a]_f \circ F_f = F_f \circ [a]_f$, so $[a]_f \in \mathrm{End}(F_f)$.

It remains to check the three properties of a ring homomorphism, beginning with the obvious fact that $[1]_f = T$. Recall that the binary operations on the ring $\mathrm{End}(F_f)$ are $+_{F_f}$ and composition. Hence, it remains to show that $[a]_f +_{F_f} [b]_f = [a+b]_f$ and $[ab]_f = [a]_f \circ [b]_f$. For the former, $[a]_f +_{F_f} [b]_f \equiv (a+b)X \pmod{\text{deg. } 2}$ because F_f is a formal group law, and the same is true of $[a+b]_f$ by definition. As $[a]_f, [b]_f, f \in \mathrm{End}(F_f)$, which is a ring by Lemma 3.2, distributivity shows that f commutes with $[a]_f +_{F_f} [b]_f$ as well as $[a+b]_f$, so by the uniqueness statement in Lemma 4.2 once again, $[a]_f +_{F_f} [b]_f = [a+b]_f$. A similar proof shows that $[a]_f \circ [b]_f = [ab]_f$. Finally, the homomorphism is injective because a can be recovered as the leading coefficient of $[a]_f$. □

We are now prepared to give the following definition. A *formal $\mathcal{O}$-module* over an $\mathcal{O}$-algebra A is:
(a) a commutative formal group law F_f;
(b) an injective ring homomorphism $\mathcal{O} \hookrightarrow \mathrm{End}_A(F_f)$, $a \mapsto [a]_f(X)$.
The Lubin-Tate formal group law F_f gives an actual abelian group $(\mathfrak{m}_L, +_{F_f})$ for any finite extension L of K. Furthermore, the group $(\mathfrak{m}_L, +_{F_f})$ has a natural $\mathcal{O}$ module structure with scalar multiplication $a \cdot x$ defined as $[a]_f(x)$ for all $a \in \mathcal{O}$, $x \in \mathfrak{m}_L$. This module structure will be used in Section 5 to provide a Galois action of $K^\times$ on large abelian extensions of K.

More generally, for any $f, g \in \mathcal{F}_\pi$ and $a \in \mathcal{O}$, there exists a unique $[a]_{g,f} \in \mathcal{O}[[X]]$ such that
(a) $[a]_{g,f} \equiv aX \pmod{\text{deg. } 2}$;
(b) $[a]_{g,f} \circ f = g \circ [a]_{g,f}$,
again by Lemma 4.2. As in the proof of Proposition 4.3, an easy application of Lemma 4.2 shows that $[a]_{g,f} \in \mathrm{Hom}(F_f, F_g)$ and $[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}$.

Proposition 4.4. *For any $f, g \in \mathcal{F}_\pi$, $F_f \simeq F_g$ as formal $\mathcal{O}$-modules over $\mathcal{O}$.*

Proof. Let $u \in \mathcal{O}^\times$ be a unit. Then $X = [1]_f = [1]_{f,f} = [u^{-1}]_{f,g} \circ [u]_{g,f}$, so $[u]_{g,f}$ and $[u^{-1}]_{f,g}$ are inverse isomorphisms. In particular, $[1]_{g,f} : F_f \to F_g$ gives a canonical isomorphism. □

It follows from this proposition that the choice of endomorphism $f \in F_\pi$ is unimportant because the resulting formal group laws are isomorphic. However, the choice of uniformizer $\pi \in K$ does matter, as we shall see in Section 5.

5 Main Theorems

The point of studying Lubin-Tate formal groups is that they allow for a straightforward construction of totally ramified abelian extensions, which will be used to prove the following theorem.

Theorem 5.1. *Let K be a local field. There is a unique group homomorphism $\phi : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ such that*

(a) for any uniformizer π of K and any finite unramified extension L of K, $\phi(\pi)|_L = \mathrm{Frob}_{L/K}$;

(b) for any finite abelian extension L of K, ϕ induces an isomorphism $K^\times/N(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$ via the map $a \mapsto \phi(a)|_L : K^\times \to \mathrm{Gal}(L/K)$.

The map ϕ is called the *Artin map* or the *local reciprocity map*. For the remainder of this section, the goal will be to construct, for a fixed prime element $\pi \in K$, a maximal totally ramified extension K_π with $N(K_\pi^\times) = \pi^{\mathbb{Z}}$ and then explicitly describe a Galois action of $K^\times$ on $L_\pi := K_\pi \cdot K^{\mathrm{ur}}$ via a homomorphism ϕ_π. This section will conclude by showing that both $L_K = L_\pi$ and $\phi_K = \phi_\pi$ are independent of the choice of uniformizer. The goal of Section 6 will then be to show that $K^{\mathrm{ab}} = L_K$ and that $\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfies properties (a) and (b) and is unique.

5.1 Constructing Abelian Extensions

Fix a prime $\pi \in K$ and choose some $f \in \mathcal{F}_\pi$. By Proposition 4.4 the choice of f is unimportant, because all resulting group laws F_f are isomorphic. Let $\Lambda_f = \mathfrak{m}^{\mathrm{s}} = \{\alpha \in K^{\mathrm{s}} \mid |\alpha| < 1\}$, given the structure of an $\mathcal{O}$-module with addition $\alpha +_{\Lambda_f} \beta = F_f(\alpha, \beta)$ and multiplication $a \cdot \alpha = [a]_f(\alpha)$. Note that for $\alpha, \beta \in \Lambda_f$ all power series in this definition converge.

Let $\Lambda_{f,n}$ be the submodule of Λ_f killed by π^n, i.e., $\Lambda_{f,n}$ is the set of roots of $[\pi^n]_f = f^{(n)} = f \circ f \circ \cdots \circ f$ (n times) in Λ_f. The fact that $\Lambda_{f,n}$ is indeed a submodule follows because F_f and $[a]_f$ commute with f.

Proposition 5.2. *The $\mathcal{O}$-module $\Lambda_{f,n}$ is isomorphic to $\mathcal{O}/(\pi^n)$. Hence, $\mathrm{End}(\Lambda_{f,n}) \simeq \mathcal{O}/(\pi^n)$ and $\mathrm{Aut}(\Lambda_{f,n}) \simeq (\mathcal{O}/(\pi^n))^\times$.*

Proof. It is easy to see that an isomorphism $h : F_f \to F_g$ induces an isomorphism of $\mathcal{O}$-modules $\Lambda_f \to \Lambda_g$, so the choice of $f \in \mathcal{F}_\pi$ is unimportant. Hence, for simplicity, choose f to be the polynomial $f(X) = \pi X + X^q$. In this case, $f^{(n)}$ has finitely many roots, so it is clear that $\Lambda_{f,n}$ is finitely generated. The ring $\mathcal{O}$ is a principal ideal domain, so by the structure theorem for finitely generated modules

$$\Lambda_{f,n} \simeq \mathcal{O}/(\pi^{d_1}) \times \cdots \times \mathcal{O}/(\pi^{d_r}), \quad d_1 \leq d_2 \leq \cdots \leq d_r.$$

By elementary field theory, f has q distinct roots, and the non-zero roots are conjugates, which must have the same valuation. Because the product of the non-zero roots is π, this

valuation is positive and non-zero, so all of the roots of f lie in Λ_f. Hence, $\Lambda_{f,1}$ has $q = \#k = [\mathcal{O} : (\pi)]$ elements, and, by the structure theorem, $\Lambda_{f,1} \simeq \mathcal{O}/(\pi)$.

For $n > 1$, consider the exact sequence

$$0 \to \Lambda_{f,1} \to \Lambda_{f,n} \xrightarrow{\pi} \Lambda_{f,n-1} \to 0.$$

For any $\alpha \in \Lambda_f$, the roots of the polynomial $f(X) - \alpha$ have a norm with positive valuation, which means that these roots lie in Λ_f. Hence, the map $\pi : \Lambda_f \to \Lambda_f$ is surjective, which means that $\pi : \Lambda_{f,n} \to \Lambda_{f,n-1}$ is surjective as well. It follows by induction that $\#\Lambda_{f,n} = q^n$. Furthermore, an inductive argument shows that $\Lambda_{f,n}$ must be cyclic. The only way that the map π from $\Lambda_{f,n}$ can have $\mathcal{O}/(\pi^{n-1})$ as its image is if $\Lambda_{f,n}$ contains $\mathcal{O}/(\pi^n)$ as a subgroup. Therefore, $\Lambda_{f,n} \simeq \mathcal{O}/(\pi^n)$ as claimed. □

Let $F \in \mathcal{O}[[X_1, \ldots, X_n]]$ be a power series. Then for any finite Galois extension L of K, the elements $\sigma \in \mathrm{Gal}(L/K)$ commute with F, i.e.,

$$F(\sigma\alpha_1, \ldots, \sigma\alpha_n) = \sigma F(\alpha_1, \ldots, \alpha_n)$$

for all $\alpha_1, \ldots, \alpha_n \in \mathfrak{m}$. When F is a polynomial, this follows directly from the fact that σ is a field automorphism fixing the elements of $\mathcal{O}$. In general σ acts continuously on L because it preserves valuation. Hence, it preserves limits as well. Let F_m be the unique polynomial of degree m congruent to F (mod deg. m). Thus

$$\sigma F(\alpha) = \sigma \lim_{m\to\infty} F_m(\alpha) = \lim_{m\to\infty} \sigma F_m(\alpha) = \lim_{m\to\infty} F_m(\sigma\alpha) = F(\sigma\alpha).$$

In particular, the elements of $\mathrm{Gal}(L/K)$ act as an $\mathcal{O}$-module isomorphism on $\Lambda_{f,n}$.

Let $K_{\pi,n} = K[\Lambda_{f,n}]$, the subfield of K^{s} generated over K by the elements of $\Lambda_{f,n}$. Note that the module $\Lambda_{f,n}$ depends on the choice of $f \in F_\pi$, but $K_{\pi,n}$ does not because all such modules are isomorphic, and the extension $K_{\pi,n}/K$ is a splitting field, and hence Galois.

Theorem 5.3.

(a) For each n, $K_{\pi,n}$ is totally ramified of degree $(q-1)q^{n-1}$.

(b) The action of $\mathcal{O}$ on $\Lambda_{f,n}$ defines an isomorphism $(\mathcal{O}/\mathfrak{m}^n)^\times \to \mathrm{Gal}(K_{\pi,n}/K)$.

(c) For each n, π is a norm from $K_{\pi,n}$ to K.

In particular, it follows from (b) that $K_{\pi,n}/K$ is abelian.

Proof. Again, for convenience, choose $f(X) = \pi X + X^q$. Let α_1 be a non-zero root of f. Then inductively construct a sequence of roots $\alpha_2, \ldots, \alpha_n$ such that α_i is a root of $f(X) - \alpha_{i-1}$. By construction, α_i is a root of $f^{(i)}$ but not a root of $f^{(i-1)}$. Consider the sequence of fields

$$K \subset K[\alpha_1] \subset \cdots \subset K[\alpha_n] \subset K[\Lambda_{f,n}].$$

Each extension, excepting $K[\Lambda_{f,n}]$, is obtained by adjoining the root of an Eisenstein polynomial. Hence, the first extension has degree $q-1$ and the $n-1$ remaining extensions are each

of degree q. In particular, $[K[\Lambda_{f,n}] : K] \geq (q-1)q^{n-1}$. By construction $v(\alpha_1) = 1/(q-1)$ and $v(\alpha_i) = v(\alpha_{i-1})/q$ for $i \geq 2$, so the extensions $K[\alpha_i]/K$ are totally ramified as well.

By definition $K[\Lambda_{f,n}]$ is the splitting field of $f^{(n)}$, so $\mathrm{Gal}(K[\Lambda_{f,n}]/K)$ can be identified with a subgroup of the group of permutations of the set $\Lambda_{f,n}$. Furthermore, because each element of $\mathrm{Gal}(K[\Lambda_{f,n}]/K)$ acts as an $\mathcal{O}$-module isomorphism on $\Lambda_{f,n}$, this subgroup is contained in $\mathrm{Aut}(\Lambda_{f,n}) \simeq (\mathcal{O}/\mathfrak{m}^n)^\times$, which has order $(q-1)q^{n-1}$. Hence, $(q-1)q^{n-1} \geq \#\mathrm{Gal}(K[\Lambda_{f,n}]/K)$, which shows that $K[\Lambda_{f,n}] = K[\alpha_n]$, the extension $K_{\pi,n}/K$ has degree $(q-1)q^{n-1}$, and $K_{\pi,n}/K$ is totally ramified. Additionally, $\mathrm{Gal}(K_{\pi,n}/K) \simeq (\mathcal{O}/\mathfrak{m}^n)^\times$ because they have the same order.

By construction α_n is a root of the polynomial $(f(X)/X) \circ f^{(n-1)} = \pi + \cdots + X^{(q-1)q^{n-1}}$. As $K[\alpha_n]$ has degree $(q-1)q^{n-1}$ over K, this polynomial must be the minimal polynomial for α_n. The norm of α_n over K is defined to be the product of its conjugates, which means that $N_{K_{\pi,n}/K}\alpha_n = (-1)^{(q-1)q^{n-1}}\pi = \pi$. □

Let $K_\pi = \cup K_{\pi,n}$. As a consequence of Theorem 5.3, $\mathrm{Gal}(K_\pi/K) = \varprojlim \mathrm{Gal}(K_{\pi,n}/K) \simeq \varprojlim (\mathcal{O}/\mathfrak{m}^n)^\times = \mathcal{O}^\times$. The extensions $K_{\pi,n}$ and K_π are non-canonical. For example, $K_{\pi,1} = K_{\pi',1}$ if and only if the unit π'/π has a $q-1$-st root in K. This is the case if and only if $\pi \equiv \pi' \bmod \mathfrak{m}$. In general, the fields $K_{\pi,n}$ and $K_{\pi',n}$ are less likely to be equal as n gets large, and for each $\pi \in K$, the field K_π is distinct. The following proposition makes this more precise.

Proposition 5.4. *Let $u \in 1 + \mathfrak{m}^n$ and $\pi' = u\pi$. Then $K_{\pi,n} = K_{\pi',n}$.*

Proof. We claim, there exists a unit $\eta \in \mathcal{O}^{\mathrm{s}}$ such that $u = \mathrm{Frob}\,(\eta)/\eta$, that can be constructed recursively. Let $u = 1 + \pi^n a$ and write $\eta = 1 + \pi^n v$, where v will be chosen to satisfy this equation mod π^{n+1}. We have

$$\frac{\mathrm{Frob}\,(\eta)}{\eta} = \frac{1 + \mathrm{Frob}(\pi^n v)}{1 + \pi^n v} \equiv 1 + \mathrm{Frob}(\pi^n v) - \pi^n v \bmod \pi^{n+1}.$$

Thus, we wish to solve the equation $\mathrm{Frob}(\pi^n v) - \pi^n v \equiv \pi^n a \bmod \pi^{n+1}$. Let $\mathrm{Frob}(\pi^n) = \pi^n w$. Then, this equation is equivalent to $w\,\mathrm{Frob}(v) - v - a \equiv 0 \bmod \pi$. Modulo $\mathfrak{m}$, the Frobenius acts as by exponentiation, so this becomes $wv^p - v - a \equiv 0 \bmod \pi$. A root of $wX^p - X - a$ exists in $\mathcal{O}^{\mathrm{s}}$, and η can be constructed by proceeding inductively.

Let $f' \in F_{\pi'}$ and $\alpha' \in \Lambda_{f',n}$. We claim that there exists a unique power series ρ such that $\rho(X) \equiv \eta X \bmod$ deg. 2 and $f' \circ \rho = \rho^\varphi \circ f$, where ρ^φ is the power series that results when the Frobenius automorphism is applied to the coefficients of ρ. This last equality certainly holds mod deg. 2, and ρ can be constructed through a complicated inductive argument (see [3, pg 47-49]). From the uniqueness of this power series, it follows that $\rho : F_f \to F_{f'}$ is a homomorphism. Note that $\rho \circ F_f \equiv F_{f'} \circ \rho \equiv \eta(X+Y) \bmod$ deg. 2. Because F_f has coefficients in $\mathcal{O}$ which are fixed by the Frobenius, $f' \circ \rho \circ F_f = \rho^\varphi \circ f \circ F_f = \rho^\varphi \circ F_f^\varphi \circ f = (\rho \circ F_f)^\varphi \circ f$. Similarly, $f' \circ F_{f'} \circ \rho = F_{f'}^\varphi \circ f' \circ \rho = F_{f'}^\varphi \circ \rho^\varphi \circ f = (F_{f'} \circ \rho)^\varphi \circ f$. By uniqueness of the power series ρ, $\rho \circ F_f = F_{f'} \circ \rho$, and in particular, $\Lambda_{f',n} = \rho(\Lambda_{f,n})$ and there exists $\alpha \in \Lambda_{f,n}$ such that $\alpha' = \rho(\alpha)$.

By definition $f'(X) \equiv u\pi X$ mod deg. 2, and because f' has coefficients in $\mathcal{O}$, $f'^{\varphi} = f'$. Hence, the homomorphism $\rho : F_f \to F'_f$ must map $[\pi']_f$ to f'. This means that $\rho \circ [u]_f \circ [\pi]_f = \rho \circ [\pi']_f = f' \circ \rho = \rho^{\varphi} \circ f = \rho^{\varphi} \circ [\pi]_f$. It follows that $\rho^{\varphi} = \rho \circ [u]_f$, and therefore $\rho^{\varphi}(\alpha) = \rho([u]_f(\alpha))$. Because $u \equiv 1$ mod $\mathfrak{m}^n$ and $\mathrm{Aut}(\Lambda_{f,n}) \simeq (\mathcal{O}/(\pi^n))^{\times} \simeq \mathcal{O}^{\times}/(1+\mathfrak{m}^n)$, $[u]_f$ acts trivially in $\mathrm{Aut}(\Lambda_{f,n})$. Therefore, $\alpha \in \Lambda_{f,n}$ implies that $[u]_f(\alpha) = \alpha$, which means that $\rho^{\varphi}(\alpha) = \rho(\alpha)$.

Because $K^{\mathrm{ur}} \cap K_{\pi,n} = K$, the Frobenius automorphism can be extended to an automorphism φ of $L_n = K^{\mathrm{ur}} \cdot K_{\pi,n}$ such that $L^{\varphi} = K_{\pi,n}$. Because the Frobenius fixes $K_{\pi,n} \ni \alpha$, $(\rho(\alpha))^{\varphi} = \rho^{\varphi}(\alpha) = \rho(\alpha)$. Hence, φ fixes $\alpha' = \rho(\alpha)$. Therefore, $K_{\pi',n} \subset K_{\pi,n}$. A similar argument with u^{-1} shows that $K_{\pi,n} \subset K_{\pi',n}$, so these fields are equal. □

The next two results describe the norm groups of $K_{\pi,n}$ and K_{π} more explicitly.

Proposition 5.5. *The group $N(K_{\pi,n}^{\times})$ is the subgroup of $K^{\times}$ generated by π and units congruent to 1 mod π^n.*

Proof. Note that if we assume the existence of the Artin map, this result follows immediately. By Theorem 5.1, $K^{\times}/N(L^{\times}) \simeq \mathrm{Gal}(K_{\pi,n}/K) \simeq \mathcal{O}^{\times}/(1+\mathfrak{m}^n) \simeq K^{\times}/(\pi, 1+\mathfrak{m}^n)$, so $N(L^{\times})$ is generated by π and $1+\mathfrak{m}^n$ as claimed. Without assuming such a map exists, however, this result is considerably more difficult.

By Theorem 5.3, π is a norm from $K_{\pi,n}$ to K, so it remains to describe the units in $N(K_{\pi,n}^{\times})$. Let $u \in 1+\mathfrak{m}^n$. By Proposition 5.4, $K_{u\pi,n} = K_{\pi,n}$, so by Theorem 5.3, $u\pi \in N(K_{\pi,n}^{\times})$ as well. So $u = u\pi/\pi \in N(K_{\pi,n}^{\times})$. Hence, $N(K_{\pi,n}^{\times})$ contains the group generated by π and $1+\mathfrak{m}^n$.

To show that these groups are equal, it suffices to show that the units in $N(K_{\pi,n}^{\times})$ are contained in $1+\mathfrak{m}^n$. Because the only norms which are units are units of norms, what we need to show is that $N(\mathcal{O}_{\pi,n}^{\times}) \subset 1+\mathfrak{m}^n$. Let $\zeta \in N(\mathcal{O}_{\pi,n}^{\times})$, and fix a root α of $f^{(n)}$ such that α is not a root of $f^{(n-1)}$ for fixed $f \in F_{\pi}$. The ring $\mathcal{O}_{\pi,n} \subset \mathcal{O}[\alpha]$ because α is a uniformizer and $K_{\pi,n}$ is totally ramified, which means there is a lift of $k_{\pi,n}$ in $\mathcal{O}$. So $\zeta = h(\alpha)$ for some power series $h(x) \in \mathcal{O}[[X]]$. Because ζ is a unit, $h(0) \neq 0$ mod $\mathfrak{m}$, so $h(X)$ is invertible in $\mathcal{O}[[X]]$.

Let $\gamma, \gamma' \in \Lambda_{f,1}$. By associativity of addition for formal groups, $(X +_{F_f} \gamma) +_{F_f} \gamma' = X +_{F_f} (\gamma +_{F_f} \gamma')$. It follows that a power series of the form $h_1(X) = \prod_{\gamma \in \Lambda_{f,1}} h(X +_{F_f} \gamma)$ satisfies $h_1(X +_{F_f} \gamma) = h_1(X)$. For any power series h_1 such that this is the case, it can be shown that there exists some power series $h_2(X)$ such that $h_1 = h_2 \circ f$ and that h_2 is unique (see [3, pg 70-71]). Define $\rho(h)$ to be the unique power series such that

$$\rho(h) \circ f = \prod_{\gamma} h(X +_{F_f} \gamma), \quad \text{where } \gamma \in \Lambda_{f,1}.$$

Because $\Lambda_{f,1}$ contains a complete set of conjugates, the coefficients of $\rho(h)$ are fixed by the Galois group, so $\rho(h) \in \mathcal{O}[[X]]$. Define $\rho^n(h)$ to be $\rho(\rho^{n-1}(h))$ where $\rho^0(h) = h$.

Recall that $f(X) \equiv X^q$ mod $\mathfrak{m}$. Thus $\rho(h) \circ f \equiv \rho(h) \circ X^q$ mod $\mathfrak{m}$. On the other hand, $\gamma \in \Lambda_{f,1} \subset \mathfrak{m}_{\pi,1}$, so $X +_{F_f} \gamma \equiv X$ mod $\mathfrak{m}_{\pi,1}$. Hence, $\prod_{\gamma} h(X +_{F_f} \gamma) \equiv h(X)^q \equiv h(X^q)$ mod $\mathfrak{m}_{\pi,1}$. Because $\prod_{\gamma} h(X +_{F_f} \gamma)$ and $h(X^q)$ are polynomials over $\mathcal{O}$, these must be equivalent modulo $\mathfrak{m} = \mathcal{O} \cap \mathfrak{m}_{\pi,1}$ as well. Therefore, $\rho(h) \circ X^q \equiv h(X^q)$ mod $\mathfrak{m}$, which means that

$\rho(h) \equiv h \bmod \mathfrak{m}$. In particular, because $h \in \mathcal{O}[[X]]^\times$, the same is true of $\rho^{n-1}(h)$ and $\rho^n(h)$, and furthermore $\rho^{n-1}(h_1) \equiv \rho^n(h_1) \bmod \mathfrak{m}^n$. Let $u_1 = \rho^{n-1}(h_1)(0)$ and $u_2 = \rho^n(h_1)(0)$. Then it clearly follows that $u_1, u_2 \in \mathcal{O}^\times$ with $u_1 \equiv u_2 \bmod \mathfrak{m}^n$.

We claim that

$$\rho^n(h) \circ f^{(n)} = \prod_{\beta \in \Lambda_{f,n}} h(X +_{F_f} \beta).$$

For $n = 0, 1$, this is trivial, so we assume inductively assume that it holds for $n-1$. Let Λ be a set of coset representatives for $\Lambda_{f,n}/\Lambda_{f,1}$, so that $\Lambda_{f,n} = \{\beta +_{F_f} \gamma \mid \beta \in \Lambda, \gamma \in \Lambda_{f,1}\}$. Then

$$\prod_{\beta \in \Lambda_{f,n}} h(X +_{F_f} \beta) = \prod_{\Lambda} \prod_{\Lambda_{f,1}} h(X +_{F_f} \beta +_{F_f} \gamma) = \prod_{\beta \in \Lambda} \rho(h) \circ f \circ (X +_{F_f} \beta).$$

Because f is an endomorphism of F_f, $f \circ (X +_{F_f} \beta) = f(X) +_{F_f} f(\beta)$, where $\beta \in \Lambda_{f,n}$ implies that $f(\beta) \in \Lambda_{f,n-1}$, and in fact, $f(\Lambda) = \Lambda_{f,n-1}$. Hence,

$$\prod_{\beta \in \Lambda_{f,n}} h(X +_{F_f} \beta) = \prod_{\beta' \in \Lambda_{f,n-1}} \rho(h)(f(X) +_{F_f} \beta').$$

By the inductive hypothesis, this last term equals $\rho^{n-1}(\rho(h)) \circ f^{(n-1)}(f(X)) = \rho^{(n)}(h) \circ f^{(n)}$; hence, $\rho^n(h) \circ f^{(n)} = \prod_{\beta \in \Lambda_{f,n}} h(X +_{F_f} \beta)$ as claimed.

In particular, this implies that $u_1 = \prod_{\beta \in \Lambda_{f,n-1}} h_1(\beta)$ and $u_2 = \prod_{\beta \in \Lambda_{f,n}} h_1(\beta)$. Hence

$$u_2/u_1 = \prod_{\beta} h_1(\beta) \quad \text{where } \beta \in \Lambda_{f,n} - \Lambda_{f,n-1}.$$

Because the set $\Lambda_{f,n} - \Lambda_{f,n-1}$ is a complete set of conjugates in the extension $K_{\pi,n}/K$, $u_2/u_1 = N_{K_{\pi,n}/K}(h_1(\alpha)) = N_{K_{\pi,n}/K}(\zeta) = u \in N(K_{\pi,n}^\times)$. Clearly $u_2 \equiv u_1 \bmod \mathfrak{m}^n$ implies $u \equiv 1 \bmod \mathfrak{m}^n$, so this shows that $N(\mathcal{O}_{\pi,n}^\times) \subset 1 + \mathfrak{m}^n$, as desired. □

Corollary 5.6. *The group $N(K_\pi^\times)$ is the cyclic subgroup of $K^\times$ generated by π, which will be denoted $\pi^{\mathbb{Z}}$.*

Proof. The norm group of an infinite extension is the intersection of the norm groups of its finite subextensions. Because the intersection of $1 + \mathfrak{m}^n$ for all $n \geq 1$ is 1, this result follows immediately. □

In particular, the fields K_π are distinct for each $\pi \in K$. However, we will show that the field $K_\pi \cdot K^{\mathrm{ur}}$ is independent of the choice of uniformizer. In other words, there is no canonical maximal totally ramified abelian extension over K, but there do exist canonical totally ramified extensions $K_{\pi,n} \cdot K^{\mathrm{ur}}$ of K^{ur} for each n, as we shall see below.

Consider the field $L_\pi = K_\pi \cdot K^{\mathrm{ur}}$. Because $K_\pi \cap K^{\mathrm{ur}} = K$,

$$\mathrm{Gal}(L_\pi/K) \simeq \mathrm{Gal}(K_\pi/K) \times \mathrm{Gal}(K^{\mathrm{ur}}/K),$$

so it suffices to describe the action of $\sigma \in \mathrm{Gal}(L_\pi/K)$ on K_π and K^{ur} separately. With this in mind, define a homomorphism

$$\phi_\pi : K^\times \to \mathrm{Gal}(L_\pi/K)$$

as the composition of the following homomorphisms:

$$K^\times \to \mathcal{O}^\times \times \mathbb{Z} \to \mathrm{Gal}(K_\pi/K) \times \mathrm{Gal}(K^{\mathrm{ur}}/K) \simeq \mathrm{Gal}(L_\pi/K)$$

$$u\pi^m \longmapsto (u, m) \longmapsto ([u^{-1}]_f, \mathrm{Frob}^m) =: \phi_\pi(u\pi^m).$$

The goal is to prove that both ϕ_π and L_π are independent of the choice of a uniformizer $\pi \in K$. Let $\varpi = u\pi$ be another prime element of K, and let $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\varpi$. If F_f were isomorphic to F_g over $\mathcal{O}$, then the field $K_{\pi,n}$ and $K_{\varpi,n}$ would be the same for all n. Because π and ϖ are distinct there is some $n \in \mathbb{Z}$ such that $\pi/\varpi \neq 1 \bmod \mathfrak{m}^n$. Then by Proposition 5.5, π is a norm from $K_{\pi,n}$ to K but not from $K_{\varpi,n}$, so these fields cannot be equal. This, together with Proposition 5.4, shows that $K_{\pi,n} = K_{\varpi,n}$ if and only if $\pi = u\varpi$ with $u \in 1 + \mathfrak{m}^n$. However, we hope to show that over K^{ur}, the extensions $K_{\pi,n} \cdot K^{\mathrm{ur}}$ are canonical, that is independent of the choice of uniformizer. To do so, we must show that F_f and F_g are isomorphic over K^{ur}.

The field K^{ur} is an increasing union of complete fields, but is not itself complete. This is true more generally for any infinite extension of K constructed as an increasing union of finite extensions. It is not terribly difficult to construct a series, in which the partial sums form a Cauchy sequence of elements in extensions of increasing finite degree, but the limit cannot be in any finite extension and consequently is not in the union of such extensions. In other words, K^{ur} is not complete, so power series evaluated at $\mathfrak{m}^{\mathrm{ur}}$ might not converge. Thus, it is necessary to work over its completion $\widehat{K}^{\mathrm{ur}}$. The Frobenius automorphism of the extension K^{ur}/K extends to $\widehat{K}^{\mathrm{ur}}$ by continuity.

Lemma 5.7. *There exists a power series $\rho \in \widehat{\mathcal{O}}^{\mathrm{ur}}[[X]]$ such that*
(a) $\rho(X) \equiv \epsilon X$ (mod deg. 2) for some unit ϵ;
(b) $\mathrm{Frob}\ \rho = \rho \circ [u]_f$;
(c) $\rho \circ F_f = F_g \circ \rho$;
(d) $\rho \circ [a]_f = [a]_g \circ \rho$ for all $a \in \mathcal{O}$.

Properties (a) and (c) say that ρ is an isomorphism $F_f \to F_g$, and (d) says that ρ commutes with the actions of $\mathcal{O}$. A self-contained proof of this result is given in Milne [6, pg 27-28].

As F_f and F_g are isomorphic over $\widehat{K}^{\mathrm{ur}}$, the extensions of this field generated by the roots of $f^{(n)}$ and $g^{(n)}$ are the same. Hence, $K_\pi \cdot \widehat{K}^{\mathrm{ur}} = K_\varpi \cdot \widehat{K}^{\mathrm{ur}}$. By taking the completions, $\widehat{K_\pi \cdot K^{\mathrm{ur}}} = \widehat{K_\varpi \cdot K^{\mathrm{ur}}}$ as well. The following lemma completes the argument that $L_\pi = L_\varpi$.

Lemma 5.8. *Let E be any algebraic extension of a local field K considered as a subfield of K^{s} and let $\widehat{E}$ be its completion. Then $\widehat{E} \cap K^{\mathrm{s}} = E$.*

Proof. By definition, $\mathrm{Gal}(K^{\mathrm{s}}/E)$ fixes every element of E, so by continuity, it fixes $\widehat{E} \cap K^{\mathrm{s}}$ as well. Hence, by Galois theory, $\widehat{E} \cap K^{\mathrm{s}}$ must be contained in E, but $E \subset \widehat{E} \cap K^{\mathrm{s}}$ so these fields are equal. $\square$

It follows that $K_\pi \cdot K^{\mathrm{ur}} = \widehat{K_\pi \cdot K^{\mathrm{ur}}} \cap K^{\mathrm{s}} = \widehat{K_\varpi \cdot K^{\mathrm{ur}}} \cap K^{\mathrm{s}} = K_\varpi \cdot K^{\mathrm{ur}}$, so $L_\pi = L_\varpi$, as desired.

To show that ϕ_π is independent of the choice of uniformizer, we shall show that $\phi_\pi(\varpi) = \phi_\varpi(\varpi)$. Consequently, for any uniformizers $\pi, \pi', \varpi \in K$, $\phi_\pi(\varpi) = \phi_\varpi(\varpi) = \phi_{\pi'}(\varpi)$. The set of uniformizers generates $K^\times$, so it follows that $\phi_\pi = \phi_{\pi'}$.

On K^{ur} both $\phi_\pi(\varpi)$ and $\phi_\varpi(\varpi)$ induce the Frobenius automorphism, so it remains only to show that they yield the same automorphism of K_ϖ. Let $f \in F_\pi$ and $g \in F_\varpi$. On K_ϖ, $\phi_\varpi(\varpi)$ is the identity. Let ρ be as in Lemma 5.7. Recall $\rho : F_f \to F_g$ is an isomorphism, which means that it is also an isomorphism of $\Lambda_{f,n} \to \Lambda_{g,n}$ as $\mathcal{O}$-modules. To show that $\phi_\pi(\varpi)$ is the identity on K_ϖ, it suffices to show that $\phi_\pi(\varpi)$ is the identity on $\Lambda_{g,n}$ for all n, i.e., for all $\alpha \in \Lambda_{f,n}$, that $\phi_\pi(\varpi)(\rho(\alpha)) = \rho(\alpha)$. Because $\varpi = u\pi$, $\phi_\pi(\varpi) = \phi_\pi(u)\phi_\pi(\pi)$. By definition, $\phi_\pi(\pi)$ fixes K_π and acts as the Frobenius automorphism on K^{ur}, while $\phi_\pi(u)$ fixes K^{ur} and acts as $[u^{-1}]_f$ on K_π. Both actions on K^{ur} extend to $\widehat{K}^{\mathrm{ur}}$ by continuity. Recalling that ρ has coefficients in $\widehat{K}^{\mathrm{ur}}$,

$$\phi_\pi(\varpi)(\rho(\alpha)) = \phi_\pi(u)\phi_\pi(\pi)(\rho(\alpha)) = (\phi_\pi(\pi)(\rho))(\phi_\pi(u)(\alpha)) = \mathrm{Frob}\ \rho \circ [u^{-1}]_f(\alpha) = \rho(\alpha)$$

by statement (b) of Lemma 5.7. Hence $\phi_\pi(\varpi) = \phi_\varpi(\varpi)$, completing the proof.

6 Existence of the Artin Map

Write L_K for L_π and ϕ_K for ϕ_π now that we know both are independent of the choice of $\pi \in K$. To show that there exists a homomorphism $\phi : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfying condition (a) of Theorem 5.1, it suffices to show that $K^{\mathrm{ab}} = L_K$ so that we can take ϕ to be ϕ_K. A further argument will show that ϕ_K satisfies condition (b) as well. At this point, it will be easy to show that ϕ_K is the unique map satisfying both conditions, completing the proof of Theorem 5.1.

6.1 Proof that $K^{\mathrm{ab}} = L_K$

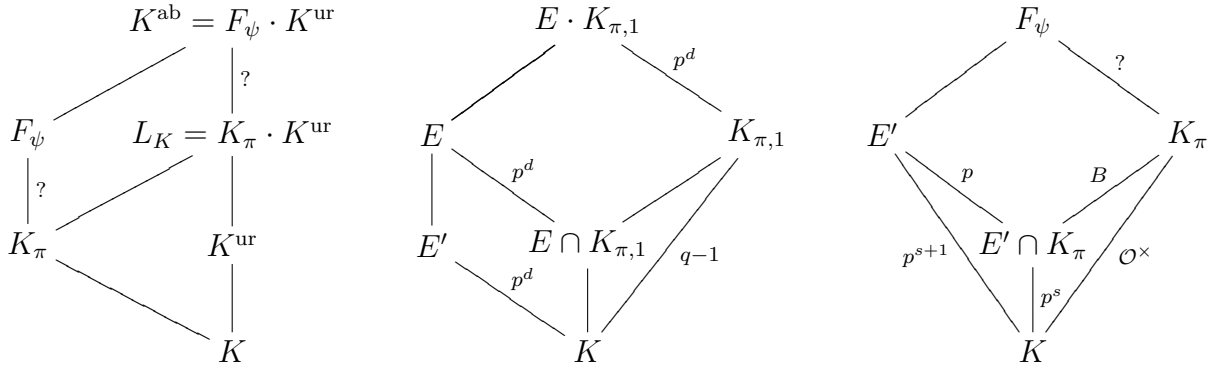
Because $K^{\mathrm{ur}} \subset K^{\mathrm{ab}}$, the Frobenius automorphism of K^{ur} can be extended non-uniquely to an automorphism ψ of K^{ab}. Let F_ψ denote the fixed field of ψ. Clearly $F_\psi \cap K^{\mathrm{ur}} = K$, the fixed field of $\psi|_{K^{\mathrm{ur}}}$, and the following lemma will show that $F_\psi \cdot K^{\mathrm{ur}} = K^{\mathrm{ab}}$. To show that $K^{\mathrm{ab}} = L_\pi$, we will show that $F_\psi = K_\pi$ for some prime π of K whose choice corresponds to the choice of the extension ψ of the Frobenius.

Lemma 6.1. *Let ψ be an extension of the Frobenius element of K^{ur} to K^{ab} and let F_ψ be the fixed field of ψ. Then $F_\psi \cdot K^{\mathrm{ur}} = K^{\mathrm{ab}}$.*

Proof. Let E be any field such that $F_\psi \subset E \subset K^{\mathrm{ab}}$ and $[E : F_\psi] < \infty$. If $[E : F_\psi] = n$, then let $F' = F_\psi \cdot K_n$ and $F'' = E \cdot K_n \supset F_\psi \cdot K_n = F'$ where K_n is the unique unramified extension of K of degree n. Because $F_\psi \cap K^{\mathrm{ur}} = K$, $[F' : F_\psi] = [K_n : K] = n$. Hence, F'' is a finite extension of F_ψ that contains two extensions of degree n. Because the fixed field of ψ in K^{ab} is F, $\mathrm{Gal}(F''/F)$ must be a finite cyclic group generated by $\psi|_{F''}$, for if this were not the case, ψ would fix some finite extension of F. The only way that a finite cyclic Galois extension can contain two subfields of the same order is if they are equal. So $E = F_\psi \cdot K^n \subset F_\psi \cdot K^{\mathrm{ur}}$. As this is true for any $E \subset K^{\mathrm{ab}}$ that is finite over F_ψ, $F_\psi \cdot K^{\mathrm{ur}} = K^{\mathrm{ab}}$ as claimed. □

The image of ϕ_K consists of precisely those automorphisms σ such that $\sigma|_{K^{\mathrm{ur}}}$ is an integer power of the Frobenius automorphism, and this subset is dense in $\mathrm{Gal}(L_K/K)$ because the Frobenius generates a dense subset of $\mathrm{Gal}(K^{\mathrm{ur}}/K) = \widehat{\mathbb{Z}}$. Because $K^{\mathrm{ur}} \subset L_K \subset K^{\mathrm{ab}}$, $\sigma = \psi|_{L_K}$ also restricts to Frob on K^{ur}. So $\sigma = \phi_K(\pi)$ for some uniformizer π depending on the extension ψ of the Frobenius automorphism of K^{ur}.

Because $K_\pi \subset K^{\mathrm{ab}}$ is fixed by $\sigma = \psi|_{L_K}$, $K_\pi \subset F_\psi$. If these fields are not equal, then there exists some finite cyclic extension E of K that is contained in F_ψ but is not contained in K_π. Because $E \cap K^{\mathrm{ur}} = K$, E is totally ramified. Hence, $\mathrm{Gal}(E/K) = I_0$, $k_E = k = \mathbb{F}_q$, and Lemma 2.7 implies that the degree $[E : K]$ is the product of a factor of $q-1$ and a power of p. Because $[K_{\pi,1} : K] = q - 1$, the degree $[E : E \cap K_{\pi,1}] = [E \cdot K_{\pi,1} : K_{\pi,1}]$ is a power of p, while $[E \cap K_{\pi,1} : K]$ is prime to p because it is a subextension of $K_{\pi,1}/K$, and $[K_{\pi,1} : K]$ is prime to p. It follows that there exists a cyclic extension E' of K of p-power degree such that $E' \cap (E \cap K_{\pi,1}) = K$ and $E' \cdot (E \cap K_{\pi,1}) = E$. Because $(E \cap K_{\pi,1}) \subset K_\pi$ but E is not, $E' \nsubseteq K_\pi$. Replacing E' with a subfield if necessary, there exists by construction a finite cyclic p-power extension E' of K such that $K \subset E' \subset F_\psi$ and $[E' : E' \cap K_\pi] = p$.



To show that $K_\pi = F_\psi$, we will use the field E' to construct a totally ramified cyclic extension L/K of degree p such that $N(L^\times) = K^\times$. This contradicts the following lemma, which implies that no such E' can exist, and hence, that $K_\pi = F_\psi$.

Lemma 6.2. *Let L/K be a cyclic extension of degree p. Then $N(L^\times) \neq K^\times$.*

Proof. Let $G = \mathrm{Gal}(L/K)$ and let I_n be the inertia groups defined in Section 2.2. Because G is cyclic of order p, each I_n is either G or 1. If $I_0 = 1$ then L/K is unramified, and if ϖ is a prime in L, then $v_L(\varpi) = 1$. Hence, $v(N_{L/K}(\varpi)) = p$, because the valuation is an additive homomorphism, and the valuation is preserved by field automorphisms. In particular, there are no primes of K in $N(L^\times)$, so this result is obvious.

When $I_0 = G$, L/K is totally ramified, and by Lemma 2.7, the quotient I_0/I_1 has order prime to p. As $\#I_0 = p$ and $\#I_1$ is either 1 or p, it must be that $I_1 = I_0 = G$. Hence, there is some integer $s \geq 1$ such that

$$G = I_0 = I_1 = \cdots = I_s, \quad I_{s+1} = I_{s+2} = \cdots = 1.$$

Let $1+x \in 1+\mathfrak{m}_L^{s+1}$. Then $N_{L/K}(1+x) = \prod_{\sigma\in G}(1+\sigma(x)) = 1+\sum_\lambda x^\lambda + N_{L/K}(x)$ where λ ranges over all elements of the form $\sigma_1+\ldots+\sigma_t$, $1 \leq t \leq p-1$ in the group ring $\mathbb{Z}[G]$ where the σ_i are distinct. Since p is prime, left multiplication of λ by any non-identity group element has no stabilizer. In particular, $\lambda, \sigma\lambda, \ldots, \sigma^{p-1}\lambda$ are distinct elements of $\mathbb{Z}[G]$, so $\sum_\lambda x^\lambda$ can be decomposed into sums of the form $\sum_{\sigma\in G} x^{\sigma\lambda} = \mathrm{Tr}_{L/K}(x^\lambda)$. For totally ramified extensions, it follows from the definition of the extension of the valuation v on K to L that $N_{L/K}(\mathfrak{m}_L^{s+1}) \subset \mathfrak{m}^{s+1}$. Hence, if we can show that $\mathrm{Tr}_{L/K}(x^\lambda) \in \mathfrak{m}^{s+1}$, then $N_{L/K}(1+\mathfrak{m}_L^{s+1}) \subset 1+\mathfrak{m}^{s+1}$, and the norm map $N_{L/K}$ induces a homomorphism $\varphi : \mathcal{O}_L^\times/(1+\mathfrak{m}_L^{s+1}) \to \mathcal{O}^\times/(1+\mathfrak{m}_K^{s+1})$.

To show that the trace maps $\mathfrak{m}_L^{s+1}$ into $\mathfrak{m}^{s+1}$ when L/K is totally ramified, we define the *different* $\mathcal{D} = \mathcal{D}_{L/K}$ as follows. Let $\mathfrak{p} = \{z \in L : \mathrm{Tr}(z) \in \mathcal{O}\}$. Clearly $\mathcal{O}_L \subset \mathfrak{p}$, so $\mathcal{D} = \mathfrak{p}^{-1}$ is a non-zero ideal of $\mathcal{O}_L$. Fix a prime $\varpi \in L$ and let $f(X)$ be its minimal polynomial over K. The derivative $f'(X)$ may be computed algebraically and gives a polynomial over K. A rather ugly computation shows that $\mathcal{D} = f'(\varpi)\mathcal{O}_L$ (see [3, pg 30-31]). It is clear that $f'(\varpi) = \prod(\varpi - \sigma(\varpi))$ where the product is taken over $G - \{1\}$. Because $I_s = G$ and $I_{s+1} = 1$, it follows from Lemma 2.6 that $v(\varpi - \sigma(\varpi)) = s+1$ for all $\sigma \neq 1 \in G$. So $v(f'(\varpi)) = (p-1)(s+1)$, and $\mathcal{D} = \mathfrak{m}_L^{(p-1)(s+1)}$. Clearly if $x \in \mathfrak{m}_L^{s+1}$, then $\lambda x \in \mathfrak{m}_L^{s+1}$. Hence, $\mathrm{Tr}(\lambda(x)) \in \mathrm{Tr}(\mathfrak{m}_L^{s+1}\mathcal{D}\mathcal{D}^{-1}) = \mathrm{Tr}(\mathfrak{m}_L^{s+1}\mathfrak{m}_L^{(p-1)(s+1)}\mathfrak{p}) = \mathfrak{m}_L^{p(s+1)}\mathrm{Tr}(\mathfrak{p}) \subset \mathfrak{m}_L^{p(s+1)}$. When L/K is totally ramified, $\mathfrak{m}_L^p = \mathfrak{m}$, so $\mathrm{Tr}(\lambda(x)) \in \mathfrak{m}^{s+1}$ as desired, and the norm map $N_{L/K}$ induces a homomorphism $\varphi : \mathcal{O}_L^\times/(1+\mathfrak{m}_L^{s+1}) \to \mathcal{O}^\times/(1+\mathfrak{m}^{s+1})$.

Let $u = \sigma\varpi/\varpi$. It is clear that $N_{L/K}(u) = 1$, so u is in the kernel of this map. But $v(\varpi - \sigma(\varpi)) = s+1$ implies that $v(1-u) = s$, so $u \in 1+\mathfrak{m}_L^s$ but $u \notin 1+\mathfrak{m}_L^{s+1}$, and φ is not injective. However, since L/K is totally ramified, their residue fields are equal, and $1+\mathfrak{m}_L^{s+1}$ and $1+\mathfrak{m}^{s+1}$ have the same indices in $\mathcal{O}_L^\times$ and $\mathcal{O}^\times$, respectively. Hence, φ is not surjective, which means that $N(\mathcal{O}_L^\times) \neq \mathcal{O}^\times$. Because only units have norms that are units, it follows that $N(L^\times) \neq K^\times$. □

Restriction of the map ϕ_K to $\mathcal{O}^\times$ induces an isomorphism with $\mathrm{Gal}(K_\pi/K)$. Let $B \subset \mathcal{O}^\times$ be the subgroup isomorphic to $\mathrm{Gal}(K_\pi/K^*)$ under this map, where $K^* = E' \cap K_\pi$. As $K^* \subset K^{\mathrm{ab}}$, B is normal, and $\mathcal{O}^\times/B \simeq \mathrm{Gal}(K^*/K)$, a cyclic group of order p^s. In particular, there is a continuous character χ of $\mathcal{O}^\times/B$ with order p^s. The set $\mathcal{O}^\times$ is clearly complete and totally bounded, the latter because it can be covered by neighborhoods $a+\mathfrak{m}^n$ where a is indexed by the set $k^n - \{0\}$. Hence, $\mathcal{O}^\times$ is compact, and χ can be lifted to a continuous character on the group $\mathcal{O}^\times$ with kernel B.

We wish to show that there is a continuous character λ of $\mathcal{O}^\times$ such that $\lambda^p = \chi$. The kernel of this map will give an extension K'/K^* of degree p that is distinct from E'/K^*, another extension of degree p. These two extensions will be used to produce a field L of degree p over K with $N(L^\times) = K^\times$, which will lead to a contradiction.

Lemma 6.3. *Let χ be a continuous character of $\mathcal{O}^\times/B \simeq \mathrm{Gal}(K^*/K)$ of order p^s. Then there exists a continuous character λ of $\mathcal{O}^\times$ of order p^{s+1} such that $\lambda^p = \chi$.*

Proof. By Lemma 2.3, $\mathcal{O}^\times \simeq k^\times \times (1+\mathfrak{m})$, and $\chi(k^\times)$ must equal 1, because $k^\times$ has order prime to p. So it suffices to consider the characters of $1+\mathfrak{m}$. The structure of this module depends on whether it has torsion elements, which depends on whether or not K contains a primitive p-th root of unity. Thus, we will consider these cases separately.

If K contains no primitive p-th roots of unity, then the group $1+\mathfrak{m}$ is a free $\mathbb{Z}_p$ module of possibly infinite rank (see [3, pg 23-25]; Proposition 7.6 proves this result in the characteristic 0 case). Characters on $\mathbb{Z}_p$ have the form $\nu_y : \mathbb{Z}_p \to S^1$, $x \mapsto e^{2\pi i[xy]}$ where $[\cdot]$ is the p-adic floor function, i.e., $z - [z] \in \mathbb{Z}_p$ for all $z \in \mathbb{Q}_p$, and $y \in \mathbb{Q}_p$ is fixed. The map $y \mapsto \nu_y$ has kernel $\mathbb{Z}_p$, so the character group of $\mathbb{Z}_p$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$. Because $\mathbb{Q}_p$ is a divisible group and quotients of divisible groups are divisible, $\mathbb{Q}_p/\mathbb{Z}_p$ is divisible. Hence, the desired character λ must exist.

If, on the other hand, K contains a primitive p-th root of unity ζ_p, this root will generate a torsion submodule of $1+\mathfrak{m}$. To prove that χ has a p-th root, we will show that $\chi(\zeta_p) = 1$, so that χ is determined by its action on a free $\mathbb{Z}_p$ module as before. Note that if K contains a p-th root of unity, it must have characteristic 0, for no such roots are found in fields of the form $k((T))$. This case requires the following two lemmas.

Lemma 6.4. *Let $K \overset{p^s}{\subset} K^* \overset{p}{\subset} E'$ with E'/K cyclic and K of characteristic 0. Then $\zeta_p \in N(K^{*\times})$.*

Proof. If σ is a generator for $\mathrm{Gal}(E'/K)$, then $\tau = \sigma^{p^s}$ generates $\mathrm{Gal}(E'/K^*)$. Because $\zeta_p \in K^*$, Kummer theory shows that there is some $\alpha \in E'$ such that $E' = K^*(\alpha)$ and $\alpha^{\tau-1} = \zeta_p$. Let $\beta = \alpha^{\sigma-1}$. Then $\beta^{\tau-1} = (\alpha^{\tau-1})^{\sigma-1} = \zeta_p^{\sigma-1} = 1$. Hence, β is fixed by $\mathrm{Gal}(E'/K^*)$ and must lie in K^*. By simple division,

$$\tau - 1 = (\sigma - 1)\sum_{i=0}^{p^s-1} \sigma^i.$$

Hence $N(\beta) = \prod_{i=0}^{p^s} \beta^{\sigma^i - 1} = \alpha^{\tau-1} = \zeta_p \in N(K^{*\times})$, as desired. □

Note that K^*/K is totally ramified because E' and K_π are totally ramified extensions of K. By hypothesis, $[K^* : K]$ is finite, so the following lemma applies.

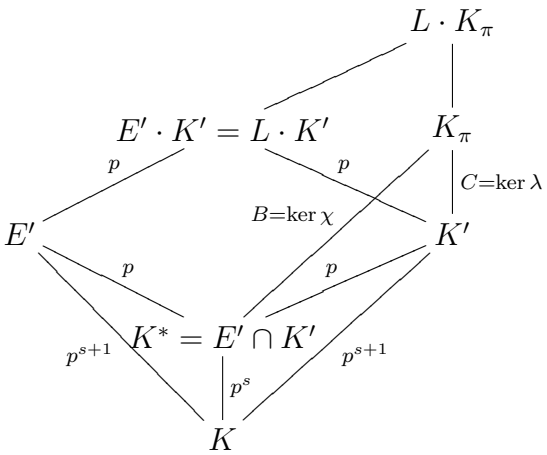
Lemma 6.5. *For any finite, totally ramified extension K^* of K and any non-zero element α of K^*, $\phi_K(N_{K^*/K}(\alpha))|_{K^*} = \phi_{K^*}(\alpha)|_{K^*} = 1$.*

Proof. It suffices to prove this for uniformizers π^* of K^*, because these generate the multiplicative group. Extend $\phi_{K^*}(\pi^*)$ to an automorphism τ of the algebraic closure K^{s}/K. Let F denote the fixed field of τ in K^{s}. By construction, the fixed field of τ in L_{K^*} is $K^*_{\pi^*}$, so $F \cap L_{K^*} = K^*_{\pi^*}$ and $F \cap K^{*\mathrm{ur}} = K *_{\pi^*} \cap K^{*\mathrm{ur}} = K^*$. So F/K^* is totally ramified, and F contains $K*_{\pi^*}$. As discussed in Section 2.2, an extension is totally ramified if and only if its norm group contains a uniformizer of the ground field. By Corollary 5.6 $N_{K^*_\pi/K^*}(K^{*\times}_{\pi^*}) = (\pi^*)^{\mathbb{Z}}$, so $N_{F/K^*}(F^\times) \subset N_{K^*_\pi/K^*}(K^{*\times}_{\pi^*})$ implies that π^* is this uniformizer. But then $N_{F/K^*}(F^\times) = (\pi^*)^{\mathbb{Z}}$ as well.

By the definition of ϕ_{K^*}, τ acts as the Frobenius automorphism on $K^{*\mathrm{ur}}$. Because K^*/K is totally ramified, $\mathrm{Gal}(K^{*\mathrm{ur}}/K^*) \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ur}}/K)$, so τ acts as the Frobenius on K^{ur} as well. Let $\sigma = \tau|_{L_K}$. So σ acts as the Frobenius on K^{ur}, which means that $\sigma = \phi_K(\pi)$ for some prime $\pi \in K$. The fixed field of σ in L_K is K_π, which must be contained in F. As F/K^* and K^*/K are totally ramified, F/K must be as well, which by the discussion above means that $N_{F/K}(F^\times) = \pi^{\mathbb{Z}}$. Because $N_{F/K^*}(F^\times) = (\pi^*)^{\mathbb{Z}}$, $N_{K^*/K}(\pi^*) \in N_{F/K}(F^\times) = \pi^{\mathbb{Z}}$. But because K^*/K is totally ramified and π^* is a prime in K^*, $N_{K^*/K}(\pi^*)$ must be a prime in K. Hence, $N_{K^*/K}(\pi^*) = \pi$, completing the proof. □

By definition, ϕ_{K^*} maps $K^{*\times}$ to automorphisms over $K*$, so the restriction of any of these maps to $K*$ must be the identity. Hence, by Lemmas 6.4 and 6.5, $\phi_K(\zeta_p)|_{K*} = \phi_{K*}(\beta)|_{K*} = 1$. Therefore, $\zeta_p \in B$, and $\chi(\zeta_p) = 1$. It follows that the character χ of $\mathcal{O}^\times$ is determined by its action on a free $\mathbb{Z}_p$ module, and as in the previous case, λ exists. □

Let C be the kernel of λ in $\mathcal{O}^\times$ and let $K' \subset K_\pi$ be the field such that C is isomorphic to $\mathrm{Gal}(K_\pi/K')$. Because $K^* = E' \cap K_\pi$ and $K^* \subset K' \subset K_\pi$, $K^* = E' \cap K'$. By construction, $[\ker\chi : \ker\lambda] = p$, so both E'/K and K'/K are cyclic extensions of degree p^{s+1} over K and degree p over K^*. It follows that there is a cyclic extension L/K of degree p such that $E' \cdot K' = L \cdot K'$.



Lemma 6.6. $L \subset L_K$.

Proof. Assume $L \not\subseteq L_K$. Then the fact that $[L : K] = p$ implies that $L \cap L_K = K$, and hence $\mathrm{Gal}(L \cdot L_K/K) \simeq \mathrm{Gal}(L/K) \times \mathrm{Gal}(L_K/K) \simeq \mathrm{Gal}(L/K) \times \mathrm{Gal}(K_\pi/K) \times \mathrm{Gal}(K^{\mathrm{ur}}/K)$ for

any prime $\pi \in K$. In particular, $(L \cdot K_\pi) \cap K^{\text{ur}} = K$, so $L \cdot K_\pi$ is a totally ramified extension of K. As discussed in Section 2.2, an extension is totally ramified if and only if its norm group contains a uniformizer of K. Because $N((L \cdot K_\pi)^\times) \subset N(K_\pi^\times) = \pi^{\mathbb{Z}}$, we must have $\pi \in N((L \cdot K_\pi)^\times)$. This norm group is a subgroup of $N(L^\times)$ as well, so $\pi \in N(L^\times)$. Because any uniformizer could have been chosen for the decomposition $L_K = K_\pi \cdot K^{\text{ur}}$, this implies that $N(L^\times)$ contains every prime of K, and hence $N(L^\times) = K^\times$. This contradicts Lemma 6.2, so L must be contained in L_K as claimed. □

Because $[L : K] = p$ and $L \cdot K' \neq K'$, $L \cap K'$ must equal K. Hence, the fact that $E' \cdot K' = L \cdot K'$ implies that $L \subset E' \subset F_\psi$. By Lemma 6.6, $L \subset F_\psi \cap L_K = F_\pi$. But by construction $K' \subset K_\pi$, so $E' \subset E' \cdot K' = L \cdot K' \subset K_\pi$, contradicting our previous claim. Hence, $F_\psi = K_\pi$ which means that $L_K = K^{\text{ab}}$, so our proof is finally complete.

6.2 Norms

Let L/K be any finite extension of K. As L is also local, the above results give a map $\phi_L : L^\times \to \text{Gal}(L^{\text{ab}}/L)$ satisfying condition (a) of Theorem 5.1. A natural question, explored partially in Lemma 6.5, is how the map ϕ_L relates to ϕ_K, and the answer to this question will show that ϕ_K satisfies condition (b) as well.

Theorem 6.7. *Let L/K be a finite extension of local fields and let ϕ_K and ϕ_L be the maps constructed in Section 5. Then the following diagram is commutative*

$$\begin{array}{ccc} L^\times & \xrightarrow[\phi_L]{} & \text{Gal}(L^{\text{ab}}/L) \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \rho} \\ K^\times & \xrightarrow[\phi_K]{} & \text{Gal}(K^{\text{ab}}/K) \end{array}$$

where $N_{L/K}$ is the norm map and $\rho : \text{Gal}(L^{\text{ab}}/L) \to \text{Gal}(K^{\text{ab}}/K)$ is restriction. In other words, $\phi_L(x)|_{K^{\text{ab}}} = \phi_K(N_{L/K}(x))$ for all $x \in L^\times$.

Proof. It is clear that if this theorem holds for two intermediate extensions F/K and L/F, then it holds for L/K as well. In particular, take $F = L \cap K^{\text{ur}}$, so that F/K is unramified and L/F is totally ramified. For a totally ramified extension, this theorem follows immediately from the proof of Lemma 6.5. Hence, it remains to consider the case where L/K is unramified. Let $[L : K] = m$ so that L is the unique unramified extension of degree m (see Lemma 2.5). As before, it suffices to show that $\phi_L(\pi')|_{K^{\text{ab}}} = \phi_K(N_{L/K}(\pi'))$ for some prime $\pi' \in L$. Consider $L_{\pi',n}$, a totally ramified extension of L, which by Theorem 5.3 is such that $\pi' \in N_{L_{\pi,n}/L}(L_{\pi,n}^\times)$. So again, Lemma 6.5 shows us that $\phi_L(\pi')|_{L_{\pi,n}} = 1$ for all $n \geq 0$. In particular, $\phi_L(\pi')|_{L_\pi} = 1$. On the other hand, on K^{ur}, $\phi_L(\pi')$ acts as the Frobenius over L, i.e., the m-th power of the Frobenius over K, because π' is a prime element. Because L/K is unramified, $v(N_{L/K}(\pi')) = m$, so $\phi_K(N_{L/K}(\pi'))$ has the same action on K^{ur}. Hence, $\phi_L(\pi')|_{K^{\text{ab}}} = \phi_K(N_{L/K}(\pi'))$, and the proof is complete. □

Let L/K be a finite abelian extension of local fields. Define a map

$$\phi_{L/K} : K^\times \to \mathrm{Gal}(L/K) \quad \text{by} \quad a \mapsto \phi_K(a)|_L$$

to be the composition of ϕ_K and the canonical projection homomorphism $\mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$.

Theorem 6.8. *The map $\phi_{L/K}$ induces an isomorphism*

$$K^\times/N(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Proof. As a corollary to Theorem 6.7, the kernel of $\phi_{L/K}$ is $N(L^\times)$. The image of ϕ_K is a dense subgroup of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ because it contains precisely those automorphisms whose restriction to K^{ur} is an integer power of the Frobenius, and these automorphisms are dense in $\mathrm{Gal}(K^{\mathrm{ur}}/K) = \widehat{\mathbb{Z}}$. Because $\mathrm{Gal}(K^{\mathrm{ab}}/L)$ is an open normal subgroup, this implies that $\phi_{L/K}$ is surjective. Hence, $K^\times/N_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$. □

Theorem 6.8 completes the proof of Theorem 5.1, modulo the claim about uniqueness of the Artin map. For this, let $\phi : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ be a map satisfying conditions (a) and (b) of Theorem 5.1. By construction, $\pi \in N(K^\times_{\pi,n})$ for each n, so condition (b) implies that $\phi(\pi)$ is the identity on $K_{\pi,n}$, and thus also for K_π. Meanwhile, condition (a) completely determines the action of $\phi(\pi)$ on K^{ur}. Hence, the action of $\phi(\pi)$ on K^{ab} is completely determined, and as the prime elements generate $K^\times$, the map described in Theorem 5.1 is unique.

An obvious consequence of Theorem 6.8 is that for a finite abelian extension L/K of local fields, $[K^\times : N(L^\times)] = [L : K]$, a result called the fundamental equality in local class field theory. The pre-Lubin-Tate perspective used this result as a building block for local class field theory. This theorem also illustrates why the Artin map is sometimes called the *norm residue map*: because it induces an isomorphism of the quotient group of $K^\times$ modulo the norm group $N(L^\times)$ onto $\mathrm{Gal}(L/K)$.

A final important result, called the Existence Theorem, gives a topological characterization of the subgroups of $K^\times$ that are norm groups for some finite abelian extension L of K.

Theorem 6.9 (Existence Theorem)**.** *A subgroup N of $K^\times$ is of the form $N(L^\times)$ for some finite abelian extension L of K if and only if N is of finite index and open in $K^\times$.*

Proof. Because N has finite index, there are only a finite number of cosets of the form $\pi^j N$, which means that for some $m \geq 1$, $\pi^m \in N$. Furthermore, it is easy to see that the set $\{1 + \mathfrak{m}^n : n \in \mathbb{N}\}$ forms a neighborhood basis for the identity in $K^\times$; hence for sufficiently large n, $1 + \mathfrak{m}^n \subset N$ because N is open. Hence, N contains the subgroup $H_{n,m}$ generated by π^m and the set $1 + \mathfrak{m}^n$. Let K_m denote the unique unramified extension of degree m over K, and consider the subfield $K_{n,m} = K_{\pi,n} \cdot K_m$ of K^{ab}. By the definition of the Artin map, $\phi(a)$ acts trivially on $K_{n,m}$ for all $a \in H_{n,m}$. Hence, $H_{n,m}$ is contained in the kernel of the quotient map $\phi_{L/K} : K^\times \to \mathrm{Gal}(L/K)$, i.e., by Theorem 6.8, $H_{n,m} \subset \mathbb{N}(L^\times)$. However the

index $[K^\times : H_{n,m}] = [\mathcal{O}^\times : 1+\mathfrak{m}^n] \cdot [\mathfrak{m} : \mathfrak{m}^m] = (q-1)q^{n-1}m = [K_{\pi,n} : K][K_m : K] = [K_{n,m} : K] = [K^\times : N(K_{n,m}^\times)]$, so $N(K_{n,m}^\times) = H_{n,m}$.

In particular, any open subgroup $N \subset K^\times$ of finite index contains a norm group $N(K_{n,m}^\times)$ as a subgroup. Let L be the subfield of $K_{n,m}$ fixed by $\phi_{K_{n,m}/K}(N)$. Then N is the kernel of $\phi : K^\times \to \mathrm{Gal}(L/K)$; therefore, by Theorem 6.8, $N = N(L^\times)$.

Conversely, of L is a finite abelian extension of K, the map $\phi_{L/K}$ gives an isomorphism $K^\times/N(L^\times) \simeq \mathrm{Gal}(L/K)$, which means that $N(L^\times)$ has finite index in $K^\times$. To show that $N(L^\times)$ is open, it suffices to show that it contains an open subgroup. The set $\mathcal{O}_L^\times$ is compact, so its image under the norm map is closed in $K^\times$. Only units have norms which are units, so the quotient $\mathcal{O}^\times/N(\mathcal{O}_L^\times)$ injects into $K^\times/N(L^\times)$. So $N(\mathcal{O}_L^\times)$ has finite index and is open as well, which means that $N(L^\times)$ is open. □

6.3 Summary

It is worth pausing for a moment to take note of what we have accomplished with the proof of Theorem 5.1. We have shown that there exists a canonical homomorphism $\phi : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ and that, for each finite abelian extension L/K, the diagram

$$\begin{array}{ccc} K^\times & \xrightarrow[\phi]{} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \downarrow & & \downarrow{\scriptstyle \sigma \mapsto \sigma|_L} \\ K^\times/N(L^\times) & \xrightarrow{\sim} & \mathrm{Gal}(L/K) \end{array}$$

is commutative, with $K^\times/N(L^\times) \to \mathrm{Gal}(L/K)$ an isomorphism. Furthermore, for any prime $\pi \in K$, $\phi(\pi)|_{K^{\mathrm{ur}}}$ is the Frobenius element. As a consequence of this last statement, for any $u \in \mathcal{O}^\times$, $\phi(u)|_{K^{\mathrm{ur}}} = \phi(u\pi)|_{K^{\mathrm{ur}}} \cdot \phi(\pi)^{-1}|_{K^{\mathrm{ur}}} = 1$. So $\mathcal{O}^\times$ is contained in the kernel of the map

$$K^\times \xrightarrow{\phi} \mathrm{Gal}(K^{\mathrm{ab}}/K) \xrightarrow{\sigma \mapsto \sigma|_{K^{\mathrm{ur}}}} \mathrm{Gal}(K^{\mathrm{ur}}/K).$$

In fact, $\mathcal{O}^\times$ is the kernel of this map, because any $x \in K^\times$ with non-zero valuation will act as an integer power of the Frobenius on K^{ur}. In other words, this map factors into

$$K^\times \xrightarrow{v} K^\times/\mathcal{O}^\times \simeq \mathbb{Z} \xrightarrow{n \mapsto \mathrm{Frob}^n} \mathrm{Gal}(K^{\mathrm{ur}}/K).$$

The isomorphisms $K^\times/N(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$ form a projective system as L ranges over all finite abelian extensions of K. Therefore, in passing to the projective limit, we obtain an isomorphism

$$\widehat{\phi} : \widehat{K^\times} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K) \quad \text{where} \quad \widehat{K^\times} = \varprojlim K^\times/N(L^\times).$$

The topology of the projective limit $\widehat{K^\times}$ is the topology inherited by this group as a subgroup of the product $\prod K^\times/N(L^\times)$ over all finite abelian extensions L, where each quotient is given the discrete topology and the product is given the product topology. In other words, $\widehat{K^\times}$ is the completion of $K^\times$ with respect to the topology for which the norm groups $N(L^\times)$ form a fundamental system of neighborhoods of 1. By the Existence Theorem, this topology, called

the *norm topology*, is contained in the usual topology from the multiplicative valuation on $K^\times$, and, in fact, it is coarser. For example $\mathcal{O}^\times$ is not open in the norm topology because all subgroups $N(L^\times)$ have finite index by Theorem 6.9, and $\mathcal{O}^\times$ does not. However, the norm topology induces the usual topology on $\mathcal{O}^\times$. To see this, recall that the sets $1+\mathfrak{m}^n$ form a fundamental system of neighborhoods of unity in the valuation topology. While these sets are not open in $\widehat{K^\times}$, they are open in $\mathcal{O}^\times$ because $1+\mathfrak{m}^n = \mathcal{O}^\times \cap N(K^\times_{\pi,n})$ by Proposition 5.5. Therefore, when we complete the terms in the exact sequence

$$0 \to \mathcal{O}^\times \to K^\times \xrightarrow{v} \mathbb{Z} \to 0$$

with respect to the norm topology, the result is an exact sequence

$$0 \to \mathcal{O}^\times \to \widehat{K^\times} \to \widehat{\mathbb{Z}} \to 0.$$

In this context, $\widehat{\mathbb{Z}}$ denotes the completion of $\mathbb{Z}$ with respect to the topology defined by subgroups of finite index, which is the same as the definition $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ given previously. Hence, the choice of a prime element $\pi \in K$ determines a decomposition $\widehat{K^\times} \simeq \pi^{\widehat{\mathbb{Z}}} \times \mathcal{O}^\times$, which gives a decomposition $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{ur}}$, where K_π is the fixed field of $\phi(\pi)$ and K^{ur} is the fixed field of $\phi(\mathcal{O}^\times)$. The image of the homomorphism ϕ in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is dense because $\mathbb{Z}$ is dense in $\widehat{\mathbb{Z}}$, so the Artin map encodes all of the information provided by $\widehat{\phi}$.

7 Classifying Galois Groups

One application of the correspondence provided by the Artin map and the categorization of norm groups of finite extensions given in the Existence Theorem is to the problem of counting and classifying the Galois extensions of a local field with a particular automorphism group. The following sections will consider this problem for Galois groups of increasing complexity.

7.1 Prime-Order Cyclic Groups

Let K be a local field with residue field k of order $q = p^f$. Given a prime l, what are the extensions L/K with Galois group $\mathbb{Z}/l$? How many are there?

By the Artin map described in Theorem 5.1, $\mathrm{Gal}(L/K) \simeq K^\times/N(L^\times)$. For any Galois extension of degree l, $(K^\times)^l \subset N(L^\times)$ because this is the set of norms of $K^\times \subset L^\times$. So $\mathrm{Gal}(L/K)$ can be identified via the Artin map with a quotient of $K^\times/(K^\times)^l$. By the Existence Theorem, every quotient of order l will correspond to a norm group and hence to $\mathbb{Z}/l$ extension of K. Conversely, Theorem 5.1 guarantees that every $\mathbb{Z}/l$ extension of K corresponds to a distinct quotient of $K^\times/(K^\times)^l$ of order l.

By choosing a uniformizer, $K^\times$ is non-canonically isomorphic to the direct product $\mathbb{Z} \times \mathcal{O}^\times$. The subgroup of l-th powers of a direct product is simply the product of l-th powers of each group; hence, $(K^\times)^l \simeq l\mathbb{Z} \times (\mathcal{O}^\times)^l$. So $K^\times/(K^\times)^l \simeq \mathbb{Z}/l \times \mathcal{O}^\times/(\mathcal{O}^\times)^l$. By definition, the residue field $k \simeq \mathcal{O}/\mathfrak{m}$ and $k^\times \simeq (\mathcal{O}/\mathfrak{m})^\times \simeq \mathcal{O}^\times/(1+\mathfrak{m})$, as both of the latter

are multiplicative groups of non-trivial cosets of $\mathfrak{m}$ modulo the equivalence $a+\mathfrak{m} \sim b+\mathfrak{m}$ if and only if $a-b \in \mathfrak{m}$. Hence, there is an exact sequence

$$1 \to 1+\mathfrak{m} \to \mathcal{O}^\times \to k^\times \to 1.$$

By Lemma 2.3, $\mathcal{O}^\times \simeq k^\times \times (1+\mathfrak{m})$ via the map $a \to a \bmod \mathfrak{m} \times (\overline{a}/a+\mathfrak{m})$, where $\overline{a} = \lim_{n\to\infty} a^{q^n}$ is the Teichmüller representative for a. So $(\mathcal{O}^\times)^l \simeq (k^\times)^l \times (1+\mathfrak{m})^l$, and

$$K^\times/(K^\times)^l \simeq \mathbb{Z}/l \times k^\times/(k^\times)^l \times (1+\mathfrak{m})/(1+\mathfrak{m})^l.$$

To compute $K^\times/(K^\times)^l$ it remains to compute $k^\times/(k^\times)^l \times (1+\mathfrak{m})/(1+\mathfrak{m})^l$. This is easiest when l is not equal to p, and the result is captured in the following proposition. Let ζ_l be a primitive l-th root of unity.

Proposition 7.1. *Let $l \neq p$ be a prime. Then if $\zeta_l \notin K$, $K^\times/(K^\times)^l \simeq \mathbb{Z}/l$ and there exists a unique cyclic extension of degree l. If $\zeta_l \in K$, then $K^\times/(K^\times)^l \simeq (\mathbb{Z}/l)^2$ and there exist $l+1$ cyclic extensions of degree l.*

Proof. When $l \neq p$, it is easy to see by direct computation that $(1+\mathfrak{m})^l = 1+\mathfrak{m}$. For any $1+a\pi^n \in 1+\mathfrak{m}$ with a a unit, consider the polynomial $f(X) = X^l - (1+a\pi^n)$. Because $l \in \mathcal{O}^\times$, $1+(a/l)\pi^n$ is a root of this polynomial mod $\mathfrak{m}^{n+1}$. By Hensel's Lemma and the fact that $v(l)=0$, this implies that there is a root in $z \in \mathcal{O}$ that is congruent to $1+(a/l)\pi^n$ mod $\mathfrak{m}^{n+1}$, so in particular $z \in 1+\mathfrak{m}$.

Therefore, when $l \neq p$, $K^\times/(K^\times)^l \simeq \mathbb{Z}/l \times k^\times/(k^\times)^l$. Because $k^\times$ is a cyclic group of order $q-1$, if $l \nmid q-1$, then $(k^\times)^l$ is simply $k^\times$ and $K^\times/(K^\times)^l \simeq \mathbb{Z}/l$. When $l \mid q-1$, then $k^\times/(k^\times)^l \simeq \mathbb{Z}/l$ and $K^\times/(K^\times)^l \simeq (\mathbb{Z}/l)^2$.

When $l \nmid q-1$, there are no l-th roots of unity in the residue field k. Hence, the polynomial $X^l - 1 = 0$ has no roots mod $\mathfrak{m}$, which means it also has no roots in K, and $\zeta_l \notin K$. Thus, the splitting field L of this polynomial over K also yields an extension of k of degree l, which means that L/K is unramified. Hence, the unique cyclic quotient of $\mathbb{Z}/l$ of order l corresponds to the unique unramified extension of degree l, which makes sense.

When $l \mid q-1$, Hensel's Lemma implies that $\zeta_l \in K$. In this case, $K^\times/(K^\times)^l \simeq (\mathbb{Z}/l)^2$, which has has $l+1$ distinct cyclic subgroups of order l and thus also $l+1$ distinct quotients of order l. To see this, consider the group as a vector space over the finite field of order l and count the number of one dimensional subspaces. There exist l "normalized" vectors $(1,a)$, $a \in \mathbb{Z}/l$ together with one "projective" vector $(0,1)$. Thus, when $\zeta_l \in K$, there exists one unramified extension and l totally ramified extensions with Galois group $\mathbb{Z}/l$. □

When $l = p$, computing $(\mathcal{O}^\times)^p$ is a bit more complicated. Immediately, $(k^\times)^p = k^\times$ because the latter is the image of the former under the familiar Frobenius automorphism. So $K^\times/(K^\times)^p \simeq \mathbb{Z}/p \times (1+\mathfrak{m})/(1+\mathfrak{m})^p$. The structure of $(1+\mathfrak{m})^p$ varies widely based on certain characteristics of the local field K. For one thing, when K has characteristic p, the quotient $(1+\mathfrak{m})/(1+\mathfrak{m})^p$ is not finite, as we see in the following proposition.

Proposition 7.2. *Let $K = \mathbb{F}_q((T))$ be a local field of characteristic p. Then K has an infinite number of cyclic extensions of degree p.*

Proof. When $K = \mathbb{F}_q((T))$, a generic element of $\mathfrak{m}$ can be written in the form $a(T)T$ where a is a power series over $\mathbb{F}_q$. Immediately, $(1 + a(T)T)^p = 1 + pb(T) + a(T)^pT^p$ where $b(T)$ is another polynomial over $\mathbb{F}_q$, but in this field, $p \equiv 0$, so the middle term vanishes. The map $\mathcal{O} \to \mathcal{O}$ given by $a(T) \mapsto a(T)^p = a(T^p)$ is clearly not surjective, suggesting that the quotient $1 + \mathfrak{m}/(1 + \mathfrak{m})^p$ is infinite. This can be seen by noting that the image of each irreducible polynomial $b(T)$ that is not a polynomial in T^p, is a distinct coset in $1 + \mathfrak{m}/(1 + \mathfrak{m})^p$. It is well known that there exist irreducible polynomials of each degree over $\mathbb{F}_q$, so there are an infinite number of extensions of degree p of $\mathbb{F}_q((T))$. □

Note that when $l \neq p$, the power series $(1 + a(T)T)^l$ may contain non-zero terms of each degree, and the situation is very different. Because there are an infinite number of $\mathbb{Z}/p$ extensions of $\mathbb{F}_q((T))$, however, for the remainder of this paper we will only consider p-adic local fields, i.e., fields K that are finite extensions of $\mathbb{Q}_p$ for some prime p.

When K lies over $\mathbb{Q}_p$, the normalized valuation $v(p) = e \geq 1$, where e is the ramification degree of $K/\mathbb{Q}_p$. The structure of $(1 + \mathfrak{m})/(1 + \mathfrak{m})^p$ will depend on the specific value of e.

Lemma 7.3. *Let e be the ramification degree of $K/\mathbb{Q}_p$ and let $c = \min\{e + 1, p\}$. Then $1 + \mathfrak{m}^{2e+1} \subset (1 + \mathfrak{m})^p \subset 1 + \mathfrak{m}^c$. In particular, the quotient $(1 + \mathfrak{m})/(1 + \mathfrak{m})^p$ is finite.*

Proof. Fix a prime π of K. By definition $(1 + \mathfrak{m})^p = \{(1 + a\pi)^p \mid a \in \mathcal{O}\}$. Expanding this expression, $(1+a\pi)^p \equiv 1+ap\pi+a^p\pi^p \bmod \mathfrak{m}^{e+2}$. Hence, $v((1+a\pi)^p-1) \geq \min\{e+1, p\} = c$, which means that $(1 + \mathfrak{m})^p \subset 1 + \mathfrak{m}^c$.

To find an integer n such that $1 + \mathfrak{m}^n \subset (1 + \mathfrak{m})^p$, we consider the polynomial $f(X) = X^p - (1 + a\pi^n)$ for some $a \in \mathcal{O}^\times$. Let $z = a_0 + a_1\pi$ be a root of this polynomial, assuming such a root exists, where $a_0, a_1 \in \mathcal{O}$. Then $z^p \equiv a_0^p \bmod \mathfrak{m}$. By hypothesis, $z^p - 1 \equiv 0 \bmod \mathfrak{m}$, so it follows that $a_0^p \equiv 1 \bmod \mathfrak{m}$. Because $p \nmid (q-1)$ the map $x \mapsto x^p$ is an automorphism of the residue field k. Hence, $a_0^p \equiv 1 \bmod \mathfrak{m}$ if and only if $a_0 \equiv 1 \bmod \mathfrak{m}$. Therefore, any root of $f(X) = X^p - (1 + a\pi^n)$ in $\mathcal{O}$ lies in $1 + \mathfrak{m}$. By Hensel's Lemma, if there is some $\alpha_0 \in \mathcal{O}$ such that $v(f(\alpha_0)) > 2v(f'(\alpha_0))$, then $f(X)$ has a root in $\mathcal{O}$, and hence in $1 + \mathfrak{m}$. In order for $v(f(\alpha_0))$ to be non-zero, let $\alpha_0 = 1 + b\pi^m$ for some $m \in \mathbb{Z}^+$ and $b \in \mathcal{O}$. Then $v(f(\alpha_0)) = v((1 + b\pi^m)^p - 1 - a\pi^n) = v(bp\pi^m + b^p\pi^{mp} - a\pi^n) \geq \min\{m + e, mp, n\}$. Meanwhile, $v(f'(\alpha_0)) = v(p(1 + b\pi^m)^{p-1}) = v(p) + v((1 + b\pi^m)^{p-1}) = e$. So $v(f(\alpha_0))$ is certainly larger than $2v(f'(\alpha_0))$ if $m > e$ and $n > 2e$. We can choose m to be arbitrary large, so this computation shows that $1 + \mathfrak{m}^{2e+1} \subset (1 + \mathfrak{m})^p$.

It follows that $(1+\mathfrak{m})/(1+\mathfrak{m})^p \subset (1+\mathfrak{m})/(1+\mathfrak{m}^{2e+1})$, which has order q^{2e}, so in particular the order of $K^\times/(K^\times)^p$, and thus also the number of extensions of K with Galois group $\mathbb{Z}/p$, is bounded. □

To determine the order of $(1 + \mathfrak{m})/(1 + \mathfrak{m})^p$ more specifically, we define subgroups

$$G_i = (1 + \mathfrak{m}^i)/[(1 + \mathfrak{m}^i) \cap (1 + \mathfrak{m})^p].$$

Clearly, $1 + \mathfrak{m}^{i+1} \hookrightarrow 1 + \mathfrak{m}^i$, so there exists a group homomorphism

$$1 + \mathfrak{m}^{i+1} \to (1 + \mathfrak{m}^i)/[(1 + \mathfrak{m}^i) \cap (1 + \mathfrak{m})^p].$$

The kernel of this map is $(1+\mathfrak{m}^{i+1})\cap(1+\mathfrak{m})^p$, so $G_{i+1}\hookrightarrow G_i$. Because $1+\mathfrak{m}^{2e+1}\subset(1+\mathfrak{m})^p$, $G_{2e+1}=\{1\}$, so we have a decreasing sequence of groups

$$(1+\mathfrak{m})/(1+\mathfrak{m})^p = G_1 \supset G_2 \supset \cdots \supset G_{2e+1} = \{1\}.$$

It follows that the order of $(1+\mathfrak{m})/(1+\mathfrak{m})^p$ is

$$\#G_1 = \prod_{i=1}^{2e} \#(G_i/G_{i+1}).$$

For $i<c$, $(1+\mathfrak{m})^p\subset 1+\mathfrak{m}^i$, so $G_i/G_{i+1} = [(1+\mathfrak{m}^i)/(1+\mathfrak{m})^p]/[(1+\mathfrak{m}^{i+1})/(1+\mathfrak{m})^p] = (1+\mathfrak{m}^i)/(1+\mathfrak{m}^{i+1})\simeq k$. So the first $c-1$ quotients in the product have order q, and

$$\#G_1 = q^{c-1}\prod_{i=c}^{2e}\#(G_i/G_{i+1}).$$

A finer analysis is needed to determine the orders of the quotients G_i/G_{i+1} for $c\le i<2e$. For this, the specific value of $c=\min\{e+1,p\}$ will be important. In general, the situation is more complex as the ramification degree e increases relative to p. The following proposition completes this computation and determines the structure of $K^\times/(K^\times)^p$.

Proposition 7.4. *Let e be the ramification degree of $K/\mathbb{Q}_p$. If $\zeta_p\notin K$, then $(1+\mathfrak{m})/(1+\mathfrak{m})^p$ has order q^e and if $\zeta_p\in K$, then $(1+\mathfrak{m})/(1+\mathfrak{m})^p$ has order $q^e p$. It follows that*

$$K^\times/(K^\times)^p \simeq \begin{cases} (\mathbb{Z}/p)^{[K:\mathbb{Q}_p]+1} & \text{if } \zeta_p\notin K \\ (\mathbb{Z}/p)^{[K:\mathbb{Q}_p]+2} & \text{if } \zeta_p\in K. \end{cases}$$

Proof. By definition, G_i/G_{i+1} is the set $\{1+b\pi^i \mid b\in k\}$ modulo elements with p-th roots in $\mathcal{O}$. Let $\eta\in\mathcal{O}^\times$ such that $p=\eta\pi^e$. Then for $a\in\mathcal{O}$, $(1+a\pi)^p\equiv 1+a\eta\pi^{e+1}+a^p\pi^p \bmod \mathfrak{m}^{c+1}$.

If $p>e+1$, then $v((1+a\pi)^p-1)=e+1=c$. Let $c\le i\le 2e$ and let $a=u\pi^{i-c}$ with $u\in\mathcal{O}^\times$. Then $(1+a\pi)^p\equiv 1+u\eta\pi^i \bmod \mathfrak{m}^{i+1}$. Because there exist units with residues in each residue class and left multiplication by $\eta\in\mathcal{O}^\times$ is a transitive action on k, G_i/G_{i+1} is trivial. Hence $\#G_1=q^{c-1}=q^e$ when $p>e+1$. In this case, $\zeta_p\notin K$, because the ramification degree of $K/\mathbb{Q}_p$ is less than the ramification degree $e(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)=p-1$. Thus, K cannot contain $\mathbb{Q}_p(\zeta_p)$ as a subfield, so $\zeta_p\notin K$.

Next, assume $p=e+1$. Once again, $(1+a\pi)^p\equiv 1+a\eta\pi^{e+1}+a^p\pi^p \bmod \mathfrak{m}^{e+2}$, although this time we cannot simplify this expression without knowing the value of $v(a)$. If $i>c=p=e+1$, then let $a=u\pi^{i-c}$ where $u\in\mathcal{O}^\times$. Then $v(a)>0$, which means that $v(a^p)>v(a)$. Therefore, $(1+a\pi)^p\equiv 1+u\eta\pi^i \bmod \mathfrak{m}^{i+1}$, so again G_i/G_{i+1} is trivial. It remains to consider the case $i=c$. For $u\in\mathcal{O}^\times$, $(1+u\pi)^p\equiv 1+(u\eta+u^p)\pi^i \bmod \mathfrak{m}^{i+1}$. The map $\rho: k\to k$ given by $u\mapsto u\eta+u^p$ is an additive homomorphism because k has characteristic p. Its kernel consists of the roots of the polynomial $X^p+\eta X = X(X^{p-1}+\eta)=0$ in k, and because k is a field there can be at most p such roots. If $-\eta$ has no $(p-1)$-st root modulo

$\mathfrak{m}$, then $X^p + \eta X$ has no non-trivial roots mod $\mathfrak{m}$, and hence no roots aside from $0 \in k$. Consequently, the map $u \mapsto u\eta + u^p$ is surjective and G_i/G_{i+1} is trivial. Suppose $-\eta$ is a $(p-1)$-st root mod p. Then by Hensel's lemma $-\eta$ is a $(p-1)$-st root in K, and $-\eta = \mu^{p-1}$. The original choice of uniformizer was not canonical, so we could choose $\varpi = \mu\pi$. Then $p = \eta\pi^{p-1} = \eta\varpi^{p-1}/\mu^{p-1} = -\varpi^{p-1}$, and the equation $X^p + \eta X$ is replaced by $X^p - X$, which has p solutions in k, precisely the elements of $\mathbb{F}_p$. Thus, the image of $u \mapsto -u + u^p$ has order q/p, and G_i/G_{i+1} has order p.

Note that in the case where $-\eta$ has a $(p-1)$-st root in K, we have a prime ϖ in K such that $\varpi^{p-1} = -p$. By the following lemma, the field $\mathbb{Q}_p(\varpi) = \mathbb{Q}_p(\zeta_p)$ where ζ_p is a primitive p-th root of unity. Hence, this case occurs exactly when $\zeta_p \in K$. Thus, if $p = e + 1$ and $\zeta_p \notin K$, then $\#G_1 = q^e$, and if $\zeta_p \in K$, then $\#G_1 = q^e p$.

Lemma 7.5. *For any prime p, $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p((-p)^{\frac{1}{p-1}})$.*

Proof. The polynomial $X^{p-1} + p$ satisfies the Eisenstein criterion, so it is irreducible over $\mathbb{Q}_p$. Similarly, the Eisenstein criterion shows that the polynomial $(X^p - 1)/(X - 1)$ is irreducible over $\mathbb{Q}_p$. Hence these fields have the same degree and it suffices to show that $(-p)^{\frac{1}{p-1}} \in \mathbb{Q}_p(\zeta_p)$.

For convenience, take $\pi = 1 - \zeta_p$ to be the uniformizing element of $\mathbb{Q}_p(\zeta_p)$. We compute that $N(\pi) = \prod_{i=1}^{p-1}(1 - \zeta_p^i) = \lim_{x\to 1}\prod_{i=1}^{p-1}(x - \zeta_p^i) = \lim_{x\to 1}\frac{x^p-1}{x-1} = p$ by L'Hôpital's rule. In particular $v(p) = v(\pi^{p-1})$ in this field. Let $p = \eta\pi^{p-1}$ for some unit η. Hence,

$$\eta = \frac{p}{(1-\zeta_p)^{p-1}} = \prod_{i=1}^{p-1}\frac{1-\zeta_p^i}{1-\zeta_p},$$

and because $\frac{1-\zeta_p^i}{1-\zeta_p} = 1 + \zeta_p + \cdots + \zeta_p^i \equiv i \bmod \pi$, $\eta \equiv \prod_{i=1}^{p-1} i \equiv (p-1)! \equiv -1 \bmod p$. In particular, $-p = (-\eta)\pi^{p-1}$ and $-\eta \equiv 1 \bmod p$. By Hensel's Lemma, $-\eta$ has a $(p-1)$-st root in $\mathbb{Q}_p$ and hence also in $\mathbb{Q}_p(\zeta_p)$. So $(-p)^{\frac{1}{p-1}} \in \mathbb{Q}_p(\zeta_p)$ as desired. □

It remains to consider the case $p < e + 1$. When $a = u\pi^{n-1}$, the contributing terms to $v((1 + u\pi^n)^p - 1)$ are $u\eta\pi^{n+e}$ and $u^p\pi^{np}$. Let n be the smallest integer such that $n + e \geq np$ and consider $i \leq n + e$. If i is not a multiple of p, then there are no elements of $\mathcal{O}$ such that $v((1 + a\pi)^p - 1) = i$, so $\#G_i/G_{i+1} = q$. If $\zeta_p \in K$, then the ramification index $e(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ divides $e(K/\mathbb{Q}_p)$. The extension $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ is totally ramified of degree $p-1$ with uniformizer $\zeta_p - 1$, so this implies that $p - 1$ divides e, which means that $n + e = np$. For $i = n + e = np$, then as before G_i/G_{i+1} has order p. If $\zeta_p \notin K$, then either this group is trivial, or $np \neq n + e$ and this case does not need to be considered. If $n + e$ is strictly greater than np and if i is one of the n multiples of p less than $n + e$, then $(1 + u\pi^{i/p})^p \equiv 1 + u^p\pi^i \bmod \mathfrak{m}^{i+1}$. The map $x \mapsto x^p$ is an automorphism of k, so for each residue class there are units in $\mathcal{O}^\times$ with p-th powers in that residue class, which means that G_i/G_{i+1} is trivial. Finally if $i > n + e$, then $(1 + u\pi^{i-e})^p \equiv 1 + u\eta\pi^i \bmod \mathfrak{m}^{i+1}$, and, as above, G_i/G_{i+1} is trivial in this case. Putting this information together, if $p < e + 1$ and $\zeta_p \notin K$, then $\#G_1 = q^{(n+e)-n} = q^e$. If $p < e + 1$ and $\zeta_p \in K$, then $\#G_1 = q^e p$.

The degree $[K : \mathbb{Q}_p]$ is the product of the degree of its totally ramified and unramified subfields, i.e., $[K : \mathbb{Q}_p] = ef$ where e is the ramification degree and $q = p^f$. Hence, we have determined that the order of $(1+\mathfrak{m})/(1+\mathfrak{m})^p$ is $q^e = p^{[K:\mathbb{Q}_p]}$ when $\zeta_p \notin K$ and $q^e p = p^{[K:\mathbb{Q}_p]+1}$ when $\zeta_p \in K$. Furthermore, $(1+\mathfrak{m})/(1+\mathfrak{m})^p$ is an abelian group that is compatible with scalar multiplication by $\mathbb{Z}/p$ because $\mathbb{Z}/p$ is a subfield of the residue field k. So $(1+\mathfrak{m})/(1+\mathfrak{m})^p$ is a $\mathbb{Z}/p$-vector space of order p^n, where $n = [K : \mathbb{Q}_p]$ or $[K : \mathbb{Q}_p] + 1$ depending on the case, which means that $(1+\mathfrak{m})/(1+\mathfrak{m})^p \simeq (\mathbb{Z}/p)^n$ as an additive group. This information, combined with the fact that $K^\times/(K^\times)^p \simeq \mathbb{Z}/p \times (1+\mathfrak{m})/(1+\mathfrak{m})^p$, completes the proof. $\square$

To determine the number of extensions of K with Galois group $\mathbb{Z}/p$ it remains to count the number of cyclic subgroups of $K^\times/(K^\times)^p \simeq (\mathbb{Z}/p)^{n+1}$, where $n = [K : \mathbb{Q}_p]$ or $[K : \mathbb{Q}_p]+1$ depending on the case, because each one dimensional subspace uniquely corresponds to an n dimensional subspace, which uniquely corresponds to a quotient of order p. Computing this number is a simple combinatorial problem, and the result is: $p^n + p^{n-1} + \cdots + 1 = (p^{n+1} - 1)/(p - 1)$.

For example, it can be shown by elementary methods that there exist 7 quadratic extensions of $\mathbb{Q}_2$: $\mathbb{Q}_2(\sqrt{3}), \mathbb{Q}_2(\sqrt{5}), \mathbb{Q}_2(\sqrt{7}), \mathbb{Q}_2(\sqrt{2}), \mathbb{Q}_2(\sqrt{6}), \mathbb{Q}_2(\sqrt{10})$, and $\mathbb{Q}_2(\sqrt{14})$. When $K = \mathbb{Q}_2$, $p = 2$ and $e = v(2) = 1$. By Proposition 7.4, $K^\times/(K^\times)^2 \simeq (\mathbb{Z}/2)^3$, which has 7 cyclic subgroups of order 2, as we would expect.

7.2 l^n-Torsion Groups

Rather than count explicitly the number of Galois extensions with l^n-torsion automorphism groups, it makes sense to consider the maximal abelian l^n-torsion extension, which will be the composite of these. Such an extension somehow captures all l^n-torsion extensions, and then enumerating them becomes a problem in combinatorics rather than number theory.

Let K be a finite extension of $\mathbb{Q}_p$, let $\Gamma = \mathrm{Gal}(K^{\mathrm{ab}}/K)$, and let l be any fixed prime. Define $\Gamma_n = \Gamma/l^n\Gamma$. Then $\Gamma_n = \mathrm{Gal}(E_n/K)$ where E_n is the maximal abelian l^n-torsion extension of K. For each n, $[E_n : K]$ is finite because E_n is the composite of finite cyclic $\mathbb{Z}/l^i$ extensions for $i \leq n$, of which Section 7.1 has shown there is a finite number. Hence, Γ_n is finitely generated and killed by l^n, so by the structure theorem for finitely generated abelian groups,

$$\Gamma_n \simeq (\mathbb{Z}/l)^{a_1} \times (\mathbb{Z}/l^2)^{a_2} \times \cdots \times (\mathbb{Z}/l^{n-1})^{a_{n-1}} \times (\mathbb{Z}/l^n)^{b_n}.$$

The field E_1 is the composite of all $\mathbb{Z}/l$ extensions of K. Hence each quotient of $\Gamma_1 = \mathrm{Gal}(E_1/K)$ of order l corresponds to a distinct $\mathbb{Z}/l$ extension of K. In particular, $\Gamma_1 \simeq (\mathbb{Z}/l)^{b_1}$ must be the group with precisely as many quotients as the number of such extensions, which means that $\Gamma_1 \simeq K^\times/(K^\times)^l$. Hence, b_1 is the value that we computed in Section 7.1. Furthermore, for each n,

$$\Gamma_n/l\Gamma_n \simeq (\mathbb{Z}/l)^{b_n + \sum a_i},$$

and also,

$$\Gamma_n/l\Gamma_n \simeq (\Gamma/l^n\Gamma)/l(\Gamma/l^n\Gamma) \simeq (\Gamma/l^n\Gamma)/(\Gamma/l^{n-1}\Gamma) \simeq (l^{n-1}\Gamma)/(l^n\Gamma) \simeq \Gamma/l\Gamma \simeq \Gamma_1.$$

Consequently,

$$b_n + \sum_{i=1}^{n-1} a_i = b_1$$

for each n.

For all $m < n$ in $\mathbb{Z}^+$, there is a homomorphism $\Gamma_n \to \Gamma_m$ given by the quotient map $\Gamma_n \to \Gamma_n/l^m\Gamma_n \simeq \Gamma_m$. Hence the set $\{\Gamma_n\}$ forms an inverse system. Define

$$\Gamma_\infty = \varprojlim \Gamma_n$$

to be the inverse limit. The limit Γ_∞ must be a $\mathbb{Z}_l$-module because each Γ_n is a $\mathbb{Z}_l$-module. Thus $\Gamma_\infty \simeq \mathbb{Z}_l^r \times T$ where $T = \prod(\mathbb{Z}/l^n)^{c_n}$. As before, $\Gamma_\infty/l\Gamma_\infty \simeq (\mathbb{Z}/l)^{r+\sum c_n} \simeq \Gamma_1$, so $r + \sum_{n=1}^{\infty} c_n = b_1$. In particular, only finitely many of the c_n are non-zero.

Because E_n is the composite of all cyclic extensions of degree dividing l^n, $\Gamma_n \simeq K^\times/(K^\times)^{l^n}$. From this point we consider the cases $l \neq p$ and $l = p$ separately.

When $l \neq p$, $(1+\mathfrak{m})^{l^n} = 1 + \mathfrak{m}$ by Hensel's Lemma. Hence, $(1+\mathfrak{m})/(1+\mathfrak{m})^{l^n}$ is trivial, and

$$\Gamma_\infty = \varprojlim K^\times/(K^\times)^{l^n} = \varprojlim \mathbb{Z}/l^n \times k^\times/(k^\times)^{l^n} = \mathbb{Z}_l \times \mathbb{Z}/l^m\mathbb{Z}$$

where m is the largest power of l such that $l^m \mid q-1$. In this case, $\Gamma_1 \simeq (\mathbb{Z}/l)^2$ if $l \mid q-1$ and $\Gamma_1 \simeq (\mathbb{Z}/l)$ otherwise, which is precisely the result we obtained in Proposition 7.1.

If $l = p$, then $k^\times/(k^\times)^{p^n}$ is trivial, and $\Gamma_n \simeq \mathbb{Z}/p^n \times (1+\mathfrak{m})/(1+\mathfrak{m})^{p^n}$. Hence,

$$\Gamma_\infty = \varprojlim \mathbb{Z}/p^n \times (1+\mathfrak{m})/(1+\mathfrak{m})^{p^n} \simeq \mathbb{Z}_p \times (1+\mathfrak{m}).$$

This implies that the torsion submodule of Γ_∞ must be the torsion submodule of $1+\mathfrak{m}$, which consists of roots of unity. Furthermore, this torsion group is killed by some power of p, so T must be precisely the p-power roots of unity contained in K. The structure of the $\mathbb{Z}_p$-module $1+\mathfrak{m}$ is given by the following proposition.

Proposition 7.6. *Let K be a finite extension of $\mathbb{Q}_p$ and let T be the group of all p-power roots of unity in K. Then T is the torsion submodule of $1+\mathfrak{m}$, $(1+\mathfrak{m})/T \simeq \mathbb{Z}_p^d$ where $d = [K:\mathbb{Q}_p]$, $1+\mathfrak{m} \simeq \mathbb{Z}_p^d \times T$, and T is finite and cyclic.*

Proof. By Lemma 7.3, $(1+\mathfrak{m})/(1+\mathfrak{m})^p$ is finite. Hence, the fact that $1+\mathfrak{m}$ is a compact $\mathbb{Z}_p$-module implies that $1+\mathfrak{m}$ is finitely generated over $\mathbb{Z}_p$, which shows that its torsion submodule is finite. Let m be the largest integer such that there exists a primitive p^m-th root of unity $\zeta_{p^m} \in K$. Then, $T \simeq (\mathbb{Z}/p^m)$. In particular, the torsion submodule T of $1+\mathfrak{m}$ is cyclic.

Because $1+\mathfrak{m}$ is a finitely generated $\mathbb{Z}_p$-module with torsion submodule $T \simeq (\mathbb{Z}/p^m)$, we know that $1+\mathfrak{m} \simeq \mathbb{Z}_p^r \times (\mathbb{Z}/p^m)$. The quotient of a direct product equals the product of the quotients, so $(1+\mathfrak{m})/(1+\mathfrak{m})^p \simeq (\mathbb{Z}/p)^n$ where $n = r$ if K contains no p-power roots of unity and $n = r+1$ if $\zeta_p \in K$. By Proposition 7.4, the quotient $(1+\mathfrak{m})/(1+\mathfrak{m})^p \simeq (\mathbb{Z}/p)^d$ if $\zeta_p \notin K$ and $(1+\mathfrak{m})/(1+\mathfrak{m})^p \simeq (\mathbb{Z}/p)^{d+1}$ if $\zeta_p \in K$. Hence, $r = d = [K:\mathbb{Q}_p]$. So $1+\mathfrak{m} \simeq \mathbb{Z}_p^d \times T$ where T is the finite cyclic group of p-power roots of unity in K, as claimed. □

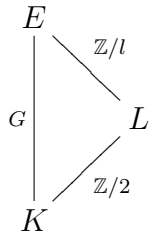
Hence, when $l = p$,

$$\Gamma_\infty \simeq \mathbb{Z}_p^{[K:\mathbb{Q}_p]+1} \times T$$

where T is the cyclic subgroup of K of p-power roots of unity. The torsion part of Γ_∞, if it exists, consists of a single cyclic subgroup, so $b_1 = r + \sum c_n$ reduces to $b_1 = r + 1$ in the case where $\zeta_p \in K$ and $b_1 = r$ in the case $\zeta_p \notin K$. So $\Gamma_1 \simeq (\mathbb{Z}/p)^{[K:\mathbb{Q}_p]+1}$ if $\zeta_p \in K$ and $\Gamma_1 \simeq (\mathbb{Z}/p)^{[K:\mathbb{Q}_p]}$ if $\zeta_p \notin K$. Using the formula $[K : \mathbb{Q}_p] = (q/p)e$, this is precisely the result we obtained in Section 7.1.

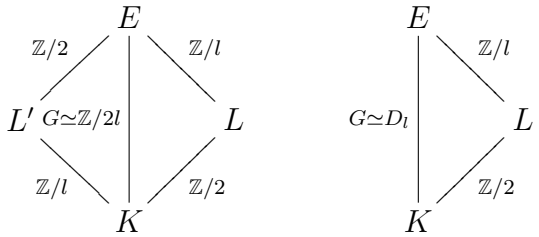
7.3 Dihedral Groups

Similar techniques can be used to count extensions of $K/\mathbb{Q}_p$ with certain non-abelian Galois groups as well. Let $l \neq p$ be an odd prime and let D_l denote the dihedral group of $2l$ elements. Consider a tower of Galois extensions of the form:



The group $G = \mathrm{Gal}(E/K)$ is determined by the action of an element τ in the non-trivial coset of $\mathbb{Z}/2$ in G on σ, the generator of $\mathbb{Z}/l \subset G$. The element $(\sigma\tau)^2$ must be in the kernel of the map $G \to G/(\mathbb{Z}/l) \simeq \mathbb{Z}/2$, so $(\sigma\tau)^2 = \sigma^i$ for some $0 \leq i < l$. If $i \neq 0$, then $\sigma\tau$ has order $2l$ and $G \simeq \mathbb{Z}/2l$ is cyclic. If $i = 0$, then $(\sigma\tau)^2 = 1$, which means that $\tau\sigma\tau = \sigma^{-1}$. In this case, $G \simeq D_l = \langle \sigma\tau \mid \sigma^l = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$.

Equivalently, $G \simeq \mathbb{Z}/2l$ if and only if the subgroup $\langle\tau\rangle \simeq \mathbb{Z}/2$ is normal in G, and $G \simeq D_l$ otherwise. In other words, $G \simeq \mathbb{Z}/2l$ if and only if there exists a cyclic extension L'/K of degree l that is contained in E. If no such L' exists, then E/K is dihedral.



In Section 7.1, we computed the number of $\mathbb{Z}/l$ extensions of local fields in terms of the order of their residue field. Fix a quadratic extension L/K. Because $[L : K] = 2$, either L/K is unramified, in which case $q_L = q_K^2$, or L/K is totally ramified, in which case $q_L = q_K$.

If L/K is totally ramified, then the number of $\mathbb{Z}/l$ extensions of L and and the number of $\mathbb{Z}/l$ extensions of K are the same. Because each $\mathbb{Z}/l$ extension L' of K together with the field L uniquely determines $E = L \cdot L'$, in this case there can be no dihedral extensions of

K containing L. This can be seen another way as well. If a D_l extension E/K contains a totally ramified extension L/K, then E/K must be totally ramified as well; otherwise $L' = E^{\text{ur}}$ certainly exists. As l is neither 2 nor p, E/K is tamely ramified, which means that the subgroup $I_1 \subset \text{Gal}(E/K)$, which is a p-group by Lemma 2.7, must be trivial. Hence, Lemma 2.7 implies that $I_0 \hookrightarrow k_E^\times$. This latter group is cyclic, and consequently $I_0 \simeq \text{Gal}(E/K)$ must be as well, so there are no totally ramified dihedral extensions of K.

When L/K is unramified, $q_L - 1 = (q_K - 1)(q_K + 1)$. If $l \mid q_K - 1$ then $l \mid q_L - 1$ and $K^\times/(K^\times)^l \simeq L^\times/(L^\times)^l \simeq (\mathbb{Z}/l)^2$. Hence, there is a one-to-one correspondence between degree l extensions of L and degree l extensions of K, which means that there are again no dihedral extensions of K. If $l \mid q_K + 1$, however, then $l \nmid q_K - 1$ but $l \mid q_L - 1$. In this case, $K^\times/(K^\times)^l \simeq \mathbb{Z}/l$ but $L^\times/(L^\times)^l \simeq (\mathbb{Z}/l)^2$, so there are $(l+1)$ $\mathbb{Z}/l$ extensions of L but only one $\mathbb{Z}/l$ extension of K. Hence, when $l \mid q_K + 1$ and L/K is unramified, there exist l dihedral extensions of K. Because there is a unique unramified quadratic extension of K, we conclude that K has l D_l extensions in the case that $l \mid q_K + 1$ and none otherwise.

References

[1] J.W.S. Cassels, A. Fröhlich, Algebraic Number Theory, Academic Press, San Diego, 1967.

[2] F. Gouvêa, p-Adic Numbers, An Introduction, Second Edition, Springer, Berlin, 1997.

[3] K. Iwasawa, Local Class Field Theory, Oxford University Press, New York, 1986.

[4] J. Lubin and J. Tate, Formal complex multiplication in local fields, Annals of Mathematics (81), 1965, 380-387.

[5] J. Milne, Algebraic Number Theory, http://www.jmilne.org/math, 1998.

[6] J. Milne, Class Field Theory, http://www.jmilne.org/math, 1997.

[7] J.-P. Serre, Local Fields, Springer-Verlag, New York, 1979.