An Explicit Construction of Abelian Extensions via Formal Groups

Danielle Li

May 25, 2004

Abstract

We introduce method of approaching local class field theory from the perspective of Lubin-Tate formal groups. Our primarily aim is to demonstrate how to construct abelian extensions using these groups.

1 Introduction

Local class field theory centers about the study of abelian extensions of local fields, most notably the p-adic numbers. Traditionally, local class field theory has been approached either as an offshoot of global, or classical class field theory, or in more recent tradition of Nakayama and Hochschild, from a cohomological perspective as in Artin [1] or Serre [5]. In the mid 1960s, Lubin and Tate [3] showed that many theorems of local class field theory could be deduced from formal groups over local fields, particularly their valuation rings. This paper seeks to provide a basic introduction to that approach.

Although all the results we present are by Lubin and Tate, we follow primarily the exposition of Iwasawa [2] and Milne [4]. Iwasawa's work follows more closely the original Lubin-Tate paper and does so in more generality. He begins with the maximal unramified extension of K, which we, like Milne, exclude when introducing formal group constructions. The primary benefit of this approach is that it makes our notation less cumbersome.[1] Our expository innovation is to begin with a motivational example of how formal groups can be used to generate abelian extensions, presented in Section 2. Section 3 provides an introduction to formal groups in general and specifically Lubin-Tate formal groups. Finally, Section 4 uses these formal groups to construct abelian extensions of a local field K.

[1] In general, I found Milne's exposition to be more clear, although both works cover the preliminarly material in roughly the same detail. Iwasawa, however, relies on formal groups in the rest of his book, proving the main theorems of local class field theory from this perspective, while Milne's discussion is primarily a digression on the construction of abelian groups.

2 Motive

To get a feel for Lubin and Tate's insight about how formal groups can generate abelian extensions, we first consider an incomplete, unrigorous, but enlightening example.

Let K be a locally compact non-archimeadean field. We define the following objects that act on K.

Definition 1 *The multiplicative group G_m is a functor from the category of fields to the category of groups which gives us the units in a field. That is,*

$$G_m(L) = L^*$$

where L^* is the group of units.

We also define a subfunctor, μ_{p^n} that takes fields to their roots of unity. That is, $\mu_{p^n}(L)$ is group of p^nth roots of unity contained in L. When we write μ_{p^n}, we mean all roots of unity.

We say that μ_{p^n} is the p^n-torsion of G_m because $\mu_{p^n}(L)$ is the p^nth torsion of $G_m(L)$. These are exactly the elements that are killed when we raise to the p^nth power in the image of G_m.

Now, consider $A_n = Aut(\mu_{p^n})$ and let z_n be a primitive nth root of unity. z_n generates μ_{p^n} so that any automorphism of μ_{p^n} is defined by where it sends z_n. The map

$$z_n \to z_n^a$$

defines an automorphism of μ_{p^n} as long as a is a unit in $\mathbb{Z}/p^n\mathbb{Z}$ so that

$$A_n = (Z/p^n)^*$$

Further, we have the reduction map

$$\pi : A_n \to A_{n-1}$$

defined by taking a, a unit mod p^n and mapping it to a mod p^{n-1}. Letting n vary, we choose z_n, z_{n+1}, etc., such that

$$z_n^p = z_{n-1}$$

In this way, we define all the A_n's to be compatible. The advantage of this construction is that we can now take the inverse limit.

Definition 2 *Consider a sequence of groups $\{G_i\}_{i=1}^{\infty}$ which are related by surjective homomorphisms $f_i : G_i \to G_{i-1}$ such that:*

$$G_1 \overset{f_2}{\leftarrow} G_2 \overset{f_3}{\leftarrow} G_3 \ldots$$

We define the inverse limit *of* (G_i, f_i)*, denoted* $\liminf G_i$ *to be the subset of* $\prod_{i=1}^{\infty} G_i$ *consisting of sequences*

$$(g_1, g_2, g_3, \ldots)$$

such that $f_i(g_i) = g_{i-1}$*.*

We define another function associated with inverse limits.

Definition 3 *We define the Tate Module* T_p *which takes a group to the inverse limit of its* p^n*-torsion.*

In our case,

$$T_p G_m = \liminf \mu_{p^n}.$$

It consists of infinite sequences $x = (x_1, x_2, \ldots)$ such that x_i is a p^ith root of unity and $x_i^p = x_{i-1}$.

Now let $G =$Gal$(\bar{K}/K)$ for some field K of char$\neq p$. We have that $x_i \in \bar{K}$ for all i. Thus, any element $g \in G$ acts on x_i by the Galois action. Using this, we can define a natural Galois action on $T_p G_m$ by

$$gx = g(x_1, x_2, \ldots) = (gx_1, gx_2, \ldots)$$

Further, we have that every element of G induces an automorphism of mu_{p^n} since $g \in G$ is a Galois automorphism of $\bar{K}$ and thus respects multiplication in μ_{p^n}. So we get the maps:

$$\phi_n : G \to Aut(\mu_{p^n}) = (Z/p^n)^*$$

This formulation gives us a bit more in fact. Let $Ker(\phi_n) = G_n$ be a subgroup of the Galois group G. Let K_n be the fixed field of G_n. From group theory, we have that $G/Ker(\phi_n) = G/G_n = Im(G)$. But since we are also dealing with Galois groups, we also have that $G/G_n = Gal(K_n/K)$. So we have that

$$Gal(K_n/K) = Im(G)$$

a subgroup of $(Z/p^n)^*$. But subgroups of abelian groups are abelian and so we have constructed an abelian extension of K.

The inverse limit allows us to recover all this information from the map:

$$\phi : G \to Aut(T_p G_m) = Z_p^*$$

Thus, we can get these abelian extensions back as well.

We now show that we can get these same abelian extensions from a formal group law as well. This is desireable because $T_p G_m$ is pretty unwieldy, but the formal group we will find is very explicit. Although the abelian extensions we just found do not represent all possible abelian extensions, (although, by Kronecker-Weber, this is true in the case of $\mathbb{Q}$), this is a good starting point for the remainder of the paper where we do construct an arbitrary extension.

Recall that we are in K a locally compact non-archimedean field. Note that this means K is complete, discrete, and has finite residue field. Further, its finite extensions L are complete with respect to the unique extension of our underlying valuation.

We will define a formal group in more generality later, but for now, consider the function:

$$f(X,Y) = X + Y + XY$$

Loosely, we call something a formal group as opposed to a group because a formal group is just the composition law, without the actual set. Thus, we can consider $f(X,Y)$ as a way of defining a binary operation on a set by:

$$x +_f y = f(x,y) = x + y + xy$$

We will take our x,y as elements of $\mathfrak{m}_L$, the maximal ideal in the valuation ring $\mathcal{O}_L$ of a finite extension of K. Recall that we define $\mathcal{O}_L = \{x \in L | |x| \leq 1\}$ and $\mathfrak{m}_L = \{x \in L | |x| < 1\}$.

Proposition 1 *$\mathfrak{m}_L$ together with the composition defined by $f(X,Y)$ is a group.*

Proof:
1. Closure. $|x + y + xy| \leq max\{|x|, |y|, |x||y|\} < 1$
2. Inverses. If $|x| \leq 1$, then $|1/x| = 1/|x| < 1$
3. Identity. 0 works.

Thus, we can define F as the functor from the category of finite extensions, L, to the category of groups $(\mathfrak{m}_L, +_f)$ where f defines a binary operation on the set $\mathfrak{m}_L$, the maximal ideal of $\mathcal{O}_L$. That is,

$$F(L) = (\mathfrak{m}_L, +_f)$$

Theorem 1 *T_pF, the inverse limit of the p^n-torsion of F is isomorphic to T_pG_m.*

Proof:
Here is a roadmap of our proof.
1. We show that the set $1 + \mathfrak{m}_L$ with multiplication is a subgroup of $L^* = G_m(L)$.
2. We show that $(\mathfrak{m}_L, +_f) \cong (1 + \mathfrak{m}_L, *)$
3. We show that the p^n-torsion of $F(L) = (\mathfrak{m}_L, +_f)$ is contained in the p^n-torsion of $G_m(L) = L^*$.
4. We show the other inclusion.

This will allow us to conclude that T_pG_m is isomorphic to T_pF because we defined them to be the inverse images of the p^n torsion.

Proof of 1. The set $1 + \mathfrak{m}_L$ with multiplication is a subgroup of $L^* = G_m(L)$.
It is clearly a subset so we just need to show that it's a group.
1. Closure. Consider $x, y \in \mathfrak{m}_L$. So $1 + x$, $1 + y$ are in $1 + \mathfrak{m}_L$. Then $(1 + x)(1 + y) = 1 + x + y + xy$ but $x + y + xy \in \mathfrak{m}_L$ by the composition law on $\mathfrak{m}_L$. Thus, the product is in $1 + \mathfrak{m}_L$.
2. Inverses. $\frac{1}{1+x} = 1 - x + x^2 - x^3 + \ldots$ but $-x + x^2 - x^3 + \ldots$ converges in $\mathfrak{m}_L$ because $|x| < 1$

and we know that L is complete.
3. Identity. 1=1+0 and $0 \in \mathfrak{m}_L$.

Proof of 2. $(\mathfrak{m}_L, f) \cong (1+\mathfrak{m}_L, *)$ by the map $h : x \to 1+x$. The map is clearly bijective and $h(x +_f y) = h(x+y+xy) = 1+x+y+xy = (1+x)(1+y) = h(x) * h(y)$.

Proof of 3. From 1, and 2, we have that $F(L) = (\mathfrak{m}_L, +_f) \cong (1+\mathfrak{m}_L, *) \subset L^*$. Thus the p^n torsion of $F(L)$ must be contained in the p^n torsion of $G_m(L) = L^*$, which we already said is $\mu_{p^n}(L)$.

Proof of 4. We need to show the other inclusion, that the p^n torsion of $G_m(L)$ is contained in the p^n torsion of $F(L)$. To show this, consider the map

$$\phi : O_L \to O_L/\mathfrak{m}_L$$

the reduction to the residue field. This induces another map from $\phi' : O_L^* \to (O_L/\mathfrak{m}_L)^*$ because we know that a ring homomorphism maps units to units. Here, $1+\mathfrak{m}_L$ is exactly the kernel of ϕ'. Since K is a local field, we know that both O_K/m_K and $O_L/\mathfrak{m}_L$ are finite fields, and further, $O_L/\mathfrak{m}_L$ is a field extension of O_K/m_K. Since O_K/m_K is finite, it has character p, as does $O_L/\mathfrak{m}_L$, its extension. But then it has no nontrivial p^nth roots of unity. To see this, notice that $x^p - 1 = (x-1)^p$ mod p. Thus, in going from O_L^* to $(O_L/\mathfrak{m}_L)^*$, we've lost all the p^n torsions of $G_m(L) = L^*$. They must be in the kernel then. This shows that the p^n torsion of $G_m(L) = L^*$ is contained in $1+\mathfrak{m}_L$. This concludes the proof.

Thus, we have that $T_pG_m \cong T_pF$. This is a remarkable result because we can use T_pG_m to recover the the specific class of abelian extension of our local field K that we constructed in the beginning. But the whole point of local class field theory is to study the abelian extensions of K. Using our formal group, we can recover the exact abelian extension we looked at earlier and get a far more explicit description!

So now we try to do this in more generality.

3 Formal Groups

In general, a formal group is a law of composition that satisfies the group axioms, but without the set. We can use them to create groups from sets as we did with $\mathfrak{m}_L$ and the operation defined by $f(X) = X+Y+XY$ in section 2.

Definition 4 *Let R be a commutative ring with unit. A power series $F(X,Y)$ in $R[[X,Y]]$ is called a* formal group *over R if it satisfies:*

1. $F(X,Y) \equiv X + Y mod \deg 2$

2. $F(F(X,Y),Z) = F(X,F(Y,Z))$

3. $F(X,Y) = F(Y,X)$

Note that these definitions tell us that the operation is associative and commutative. We will be especially interested in the case where $A = \mathcal{O}_K$ where K is a nonarchimedean local field (that is, K is locally compact with respect to a nontrivial valuation - this also means that K is complete, $|\cdot|$ is discrete, and has finite residue field).

Definition 5 *For each prime element, π, of K, let $\mathcal{F}_\pi$ denote the family of power series $f(X)$ in $A[[X]]$ such that :*

$$f(X) \equiv \pi X mod \deg 2 \qquad f(X) \equiv X^q mod \pi$$

For example, the polynomial $\pi X + X^q$ is an element of $\mathcal{F}_\pi$.

Proposition 2 *Let f, g be power series in $\mathcal{F}_\pi$ and let $\phi_1(X_1,\ldots,X_n)$ be a linear form with coefficients in A. Then there is a unique $\phi \in A[[X_1,\ldots,X_n]]$ such that:*

$$\phi(X_1,\ldots,X_n) = \phi_1 mod \deg 2$$

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

Proof: See [4], [2], or [3].

Proposition 3 *For each $f \in \mathcal{F}_\pi$, there exists a unique formal group $F_f(X,Y)$ over A admitting f as an endomorphism.*

Proof: We apply Propostion 2 for $f = g$, and $L(X,Y) = X + Y$ to get that there exists a unique power series $F_f(X,Y)$ in $A[[X,Y]]$ such that:

$$F_f(X,Y) \equiv X + Y mod \deg 2$$

$$f(F_f(X,Y)) = F_f(f(X), f(Y)).$$

If $F_f(X,Y)$ defines a formal group, we are done because the above means that f acts as an endomorphism on $F_f(X,Y)$. We claim that this $F_f(X,Y)$ is a formal group law.
1. Commutativity. We let $G = F_f(Y,X)$ then we have that:

$$G(X,Y) \equiv X + Y mod \deg 2$$

$$f(G(X,Y)) = f(F_f(Y,X)) = F_f(f(Y), f(X)) = G(f(X), f(Y)).$$

But by Proposition 2, $F_f(X,Y)$ is the only power series with this property, so we must have that $G(X,Y) = F_f(Y,X) = F_f(X,Y)$.

2. Associativity. Now let

$$G_1(X,Y,Z) = F_f(X, F_f(Y,Z)), \qquad G_2(X,Y,Z) = F_f(F_f(X,Y), Z)$$

Then, for $i = 1, 2$,

$$G_i(X,Y,Z) \equiv X + Y + Z mod \deg 2$$

$$G_i(f(X), f(Y), f(Z)) = f(G_i(X,Y,Z)).$$

Proposition 2 says that for $\phi(X,Y,Z) = X + Y + Z$, there is a unique power series $G(X,Y,Z)$ that satisfies these criterion. Thus, $G_1 = G_2$.

Thus, $F_f(X,Y)$ satisfies all the axioms of a formal group over A. This concludes the proof of the theorem.

These $F_f(X,Y)$ are the *Lubin-Tate formal group laws.*

Example 1 *Let $K_v = \mathbb{Q}_p$ and $\pi = p$. We define $f = (1+X)^p - 1$. Notice that $f \in \mathcal{F}_p$. We also define $F_f(X,Y) = X + Y + XY$. As we showed in section 1, $F_f(X,Y)$ admits f as an endomorphism. By the above proposition, we now know that $F_f(X,Y)$ is unique.*

4 Constructing Extensions with Formal Groups

Now, let $a \in A$ and let f, g again be a power series in $\mathcal{F}_\pi$. Applying Proposition 2 for $\phi(X) = aX$, we get that there exists a unique power series, call it $[a]_{g,f}$ in $A[[X]]$ such that

$$[a]_{g,f}(X) \equiv aX mod \deg 2$$

$$g \circ [a]_{g,f} = [a]_{g,f} \circ f.$$

Proposition 4 *$[a]_{g,f}$ is a homomorphism from $F_f(X,Y) \to F_g(X,Y)$.*

Proof:
Since I am lazy, let's denote $[a]_{g,f}$ by h. We want to show that

$$h(F_f(X,Y)) = F_g(h(X), h(Y)).$$

It follows from the definition of h that $h(F_f(X,Y)) \equiv aX + aY mod \deg 2 \equiv F_g(h(X), h(Y))$. We also have that:

$$h(F_f(f(X), f(Y))) = (h \circ f)(F_f(X,Y)) = g(h(F_f(X,Y)))$$

$$F_g(f(f(X)), h(f(Y))) = F_g(g(h(X), g(h(Y))) = g(F_g(h(X), h(Y))).$$

Again, we can use Proposition 2 to get uniqueness.

Further, we have that:

$$[a+b]_{g,f} = [a]_{g,f} +_{F_g} [b]_{g,f}, \qquad [ab]_{g,f} = [a]_{h,g} \circ [b]_{g,f}$$

and that for $u \in A^*$ a unit, $[u]_{f,g}$ and $[u^{-1}]_{g,f}]$ are inverse isomorphisms. The proofs of these assertions follow by writing out the properties of the associated power series and using uniqueness as we did in the last few proofs.

This means that for $f, g \in \mathcal{F}_\pi$, $F_f(X,Y) \cong F_g(X,Y)$. If we take $f = g$, then we get that there exists a unique endomorphim $[a]_f : F_f \to F_f$ such that

$$[a]_f(X) \equiv aX mod \deg 2$$

and

$$f \circ [a]_f = [a]_f \circ f.$$

Thus we get an injection $A \to End(F_f)$ given by $a \to [a]_f$.

Now consider $\mathfrak{m}_{\bar{K}}$ where $\bar{K}$, the algebriac closure of K and $\mathfrak{m}_{\bar{K}}$ is the maximal ideal of the valuation ring. As in section 2, we use $\mathfrak{m}_{\bar{K}}$ as the set on which we define operations derived from our formal group.

Proposition 5 *$\mathfrak{m}_{\bar{K}}$ is an A-module with the operations:*
1. For $x, y \in \mathfrak{m}_{\bar{K}}$, let $x + F_f y = F_f(x,y)$.
2. For $a \in A$ and $x \in \mathfrak{m}_{\bar{K}}$, let $a * x = [a]_f x$. When we refer to $\mathfrak{m}_{\bar{K}}$ as an A-module, we call it W_f.

Proof: To show this, we need to show that $\mathfrak{m}_{\bar{K}}$ under addition forms an abelian group. The proof is identical to the one given in section 2, except that we are working with a more general power series. The only thing we need to add is that we can be assured that $F_f(x,y)$ converges because $|x|, |y| < 1$. To show that it satisfies the rest of the module axioms is straightforward if we keep the fact of convergence in mind.

Associated to W_f, we define:

Definition 6 *Denote by W_f^n the submodule of W_f defined as the set:*

$$W_f^n = \{x \in W_f | [\pi]_f^n *_{F_f} x = 0\}$$

where $[\pi]_f$ is defined to be unique power series in $A[[X]]$ such that

$$[\pi]_f(X) \equiv \pi X mod \deg 2$$

$$f \circ [\pi]_f = [\pi]_f \circ f.$$

However, note that this means $[\pi]_f(X) = f(X)$ because we defined $f(X) \in \mathcal{F}_\pi$ to satisfy these requirements. We have uniqueness as a consequence of Proposition 4.

W_f^n is, in fact, exactly the $[\pi]_f^n$-torsion of W_f! We can also notice that W_f^n is equivalently the set of roots of $[\pi]_f^n = f^n$ in $\mathfrak{m}_{\bar{K}}$.

Example 2 *Continuing our previous example, we now take*

$$W_f^n = \{x \in \bar{\mathbb{Z}}_p | (x-1)^{p^n} = 1\} = \{\zeta | \zeta^{p^n} - 1\}$$

this is exactly equal to μ_{p^n}.

Lemma 1 $[\pi]_f^n = f^n(X)$ *is a monic, separable polynomial of degree q^n in $A[X]$ and W_f^n is the set of all roots of $f^n(X)$ in $\bar{K}$. So the order of W_f^n is q^n.*

Proof: We know that W_f^n consists of the roots of f^n in W_f, equal to $\mathfrak{m}_{\bar{K}}$ as a set. We claim that W_f^n is actually the set of all roots of f^n in $\bar{K}$. First, recall that

$$f^n = f \circ \ldots \circ f$$

For illustrative purposes,footnotewe don't need this form to prove the proposition - all we require is that $f(X) \in \mathcal{F}_\pi$, but it is easier to the calculation this way. suppose that $f(X)$ takes the form:

$$f(X) = \pi X + \ldots + X^q$$

Then we have

$$(f \circ f)(X) = f(f(X)) = \pi(\pi X + \ldots + X^q) + \ldots + (\pi X + \ldots + X^q)^q = \pi X^2 + \ldots + X^{q^2}$$

By induction, we get that:

$$f^n = \pi^n X + \ldots + X^{q^n}$$

Now suppose that $x \in \bar{K}$ were a root. We would have $|\pi^n x + \ldots + x^{q^n}| = 0$ which implies that $|x|^{q^n} \leq max\{|x|^{lesserpowers}\}$ and so $|x| \leq 1$ so $x \in \mathfrak{m}_{\bar{K}}$.

The following is a structure theorem for certain modules that we will take for granted:

Proposition 6 *Let A be a principal ideal domain with only one prime up to conjugation (notice that $A = \mathcal{O}_K$ satisfies these conditions). Then every finitely generated torsion A-module, M, decomposes into a direct sum of cyclic modules:*

$$M \cong A/(\pi^{n_1}) \oplus \ldots \oplus A/(\pi^{n_r}), \qquad n_1 \leq \ldots \leq n_r$$

and the sequence $n_1, \ldots, n_r$ is uniquely determined.

Lemma 2 *Let M be an A-module, and let $M_n = Ker(\pi^n : M \to M)$. If we have that:*
1. If M_1 has $q := (A : (\pi))$ elements, and
2. $\pi : M \to M$ is surjective,
then $M_n \cong A/(\pi^n)$; and thus it has q^n elements.

It is worth clarifying that by the map $\pi^n : M \to M$, we mean the map that takes $x \in M$ to $\pi * x = [\pi]_f^n(x)$. *Proof*:
This is done by induction on n.
Base case: $n = 1$. We want to show that $M_1 \cong A/(\pi)$. From 1, we have that M_1 has q elements. Thus, applying the structure theorem for modules, we can write M_1 as a product of cyclic modules. The only way to do this to write $M_1 \cong A/(\pi)$ because it has q elements (since (π) is a prime and thus maximal ideal so $A/(\pi)$ is the residue field which we assumed has order q).
More generally, note that $A/(\pi^n)$ has q^n elements.
Induction case: We assume that $M_{n-1} \cong A/(\pi^{n-1})$. Now consider the sequence:

$$0 \to M_1 \to M_n \to_\pi M_{n-1} \to 0$$

Condition 2. implies that this sequence is exact. By the first isomorphism theorem, then, we have:

$$M_n/M_1 \cong M_{n-1}$$

Using our hypotheses, this gives:

$$M_n/(A/(\pi)) \cong (A/\pi^{n-1})$$

and so M_n has q^n elements. Further, M_n must be cyclic because M_1 and M_{n-1} are (we need the above equation to hold). We know from the structure theorem that $A/(\pi^n)$ is the unique module that satisfies these conditions.

Proposition 7 *The A-module, W_f^n is isomorphic to $A/(\pi^n)$. Thus we have that $End_A(W_f^n) = A/(\pi^n)$ and $Aut_A(W_f^n) = (A/(\pi^n))^\times$.*

Proof: We will prove this by showing that W_f satisfies the hypothesis for M in the previous lemma. We already showed that W_f is an A-module. We need to show that:
1. $W_{f_1} = Ker(\pi : W_f \to W_f)$ has q elements. Note that W_{f_1} is just W_f^1 by definition. The kernel of π is precisely the roots of $[\pi]_f(X) = f(X)$ for $f(X) \in \mathcal{F}_\pi$. It does not matter which $f(X)$ we pick because an A-isomorphism $h : F_{f(X,Y)} \to F_{g(X,Y)}$ of formal groups induces an isomorphism

of A-modules $W_f \to W_g$. Thus, we can take $f(X)$ to be of the form $\pi X + \ldots + X^q$. This is an Eisenstein polynomial so it has q distinct roots. we have already shown that these roots all have valuation less than 1 and so they lie in W_f. This means that the kernel of the map π has exactly q elements, all in W_f.
2. $\pi : W_f \to W_f$ is surjective. This follows because $[\pi]_f = f(X)$ which we showed is an automorphism.

Thus, we apply the lemma on W_f to get that $W_f^n \cong A/(\pi^n)$. It follows immediately that the action of A on W_f^n induces an isomorphism $A/(\pi^n) \to End_A(W_f^n)$. The automorphisms, then, are the subset which are isomorphisms, that is, $(A/(\pi^n))^\times$.

Lemma 3 *Let L be a finite Galois extension of K, a local field with Galois group G. The, for any $F \in \mathcal{O}_K[[X_1, \ldots, X_n]]$ and $x_1, \ldots, x_n \in \mathfrak{m}_L$, we have that:*

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

for all $\tau \in G$

Proof: We know that the valuation on K extends uniquely to L. We also know that $|\cdot|$ makes L a topological field (addition, multiplication, and inverses are continuous). Thus τ is a field isomorphism that fixes $\mathcal{O}_K$. For F a polynomial (not infinite), this is enough to show that F behaves properly. Now if F is a power series, we use the fact that τ is continuous. So it preserves limits:

$$\lim_{m\to\infty} x_m = L \to \lim_{m\to\infty} \tau x_m = \tau L.$$

We approximate F by the polynomials F_m such that $F = F_m + \deg \geq m+1$. Then we have:

$$\tau(F(x_1,\ldots)) = \tau(\lim_{m\to\infty} F_m(x_1,\ldots)) = \lim_{m\to\infty} \tau F(x_1,\ldots) = \lim_{m\to\infty} F(\tau x_1,\ldots) = F(\tau x_1,\ldots).$$

Theorem 2 *Consider $K[W_f^n]$ a field extension of K a non-archimedean local field with residue field F_q. The following holds:*

1. *For each n, $K[W_f^n]/K$ is of degree $(q-1)q^{n-1}$*

2. *The action of $\mathcal{O}_K$ on W_f^n defines an isomorphism:*

   $$(\mathcal{O}_K/\mathfrak{m}_K)^\times \to Gal(K[W_f^n]/K).$$

   In particular, $K(W_f^n)/K$ is an abelian extension.

Proof:
We assume that f is a polynomial of the form $\pi X + \ldots + X^q$ (this is okay because any other $f \in \mathcal{F}_\pi$ would result in an isomorphic result). Choose a nonzero root, π_1 of $f(X)$. The choose a nonzero root π_2 of $f(X) - \pi_1$. π_2 is an element of W_f as well (by Newton's polygon, which is an application

of Hensel's Lemma). Inductively, we choose π_n a nonzero root of $f(X) - \pi_{n-1}$. We get the chain of extensions:

$$K \subset K[\pi_1] \subset \ldots \subset K[\pi_n] \subset K[W_f^n]$$

where the first extension is of degree $q-1$ and the rest are of degree q. By the Tower Law, $[K[W_f^n] : K] = (q-1)q^{n-1}$.

To show 2, remember that W_f^n is the set of roots of f^n in $\bar{K}$. Thus, $K[W_f^n]$ is the splitting field of f^n. Thus, $K[W_f^n]/K$ is a Galois extension and we can identify $Gal(K[W_f^n]/K)$ with the group of permutations of W_f^n (because these are exactly the roots of f). Now we can apply Lemma 3. This allows us to think of each element of $Gal(K[W_f^n]/K)$ as $\mathcal{O}_K$-module isomorphism acting on W_f^n. Because of this, the image of $Gal(K[W_f^n]/K)$ in $Sym(W_f^n)$ must be contained in

$$End_{\mathcal{O}_K}(W_f^n) = (\mathcal{O}_K/(\pi^n))^\times.$$

Thus,

$$(q-1)q^{n-1} \geq \#Gal(K[W_f^n]/K) = [K(W_f^n) : K]$$

But we also have:

$$[K[W_f^n : K] \geq [K[W_f^n] : K] = (q-1)q^{n-1}$$

So $\#Gal(K[W_f^n]/K) = [K(W_f^n) : K] = (q-1)q^{n-1}$

But if the order of $Gal(K[W_f^n)]K)$ is exactly $(q-1)q^{n-1}$ and it fits inside $End_{\mathcal{O}_K}(W_f^n) = (\mathcal{O}_K/(\pi^n))^\times$, then they must be isomorphic. Thus, $K[W_f^n]/K$ is an abelian extension.

References

[1] Artin, Emil. *Algebriac Numbers and Algebraic Functions*, Gordon and Breach: New York, 1967.

[2] Iwasawa, Kenkichi. *Local Class Field Theory*, Oxford University Press: Oxford, 1986.

[3] Lubin, Jonathan and John Tate. "Formal Complex Multiplication in Local Fields," *Annals of Math*, 81, 1965.

[4] Milne, J.S. *Class Field Theory*, Online coursenotes, available: http://www.jmilne.org/math/, 1997.

[5] Serre, Jean-Paul. *Corps Locaux*, Hermann: Paris, 1962.