Local Class Field Theory and Lubin-Tate Extensions: An Explicit Construction of the Artin Map.

Siddharth Mathur

Department of Mathematics and its Applications

Central European University

In partial fulfillment of the requirements for the degree of Master of Sciences

Supervisor:
Professor Gergely Zábrádi
ELTE

Budapest, Hungary

2012

Acknowledgements

I would like to thank all the Professors who have taught me Number theory: Oliver Schirokauer, Gergely Harcos, Tamás Szamuely and most especially Gergely Zábrádi whose guidance and patience was an invaluable part of this thesis.

I would like to thank Professor Pál Hegedűs for his academic advice throughout the Masters program. Finally I'd like to express my gratitude to Professor Robert Young whose impassioned lectures first inspired my love for Mathematics.

Last but not least I'd like to thank my friends and family for their love and support.

Introduction

The aim of this paper is to give an exposition of the main theorems of local class field theory using Lubin-Tate extensions. The existence of the Artin map is one of the main results of local Class Field theory and our approach will be only one of many. Each one of the available proofs has its own benefits e.g. the cohomological approach yields information about the cohomology groups. In contrast the rationale behind using Lubin-Tate theory is that the constructions here are explicit.

The Local Artin map of a local field K is between K^* and $G_{K^{ab}/K}$ and it satisfies certain arithmetic conditions which will allow us to better understand the Galois group of the maximal abelian extension of K: K^{ab}. We will see how this map induces isomorphisms between finite quotients of K^* and $G_{K^{ab}/K}$ and then this will yield a correspondence between certain subgroups of the multiplicative group K^* and its abelian extensions.

Like many other approaches to the subject, the proof of existence will need to be handled carefully - we will separate the cases into two parts, the ramified and unramified extensions. The unramified extensions are fairly well understood for local fields and will not take much time to dispense of. However the ramified case requires more care and this is where we use Lubin-Tate theory.

We begin by introducing the theory of local fields and arithmetic properties of their extensions, these results will be mostly preliminary and will have been covered in a first course in Algebraic Number Theory, proofs will be ommited. We will then consider Formal Group laws, which are, informally speaking, a formal analogue of a group structure. After we have proven what we've needed for Lubin-Tate group laws we shall explicitly construct maximal totally ramified extensions of K. This will set the stage for an explicit description of the Artin map. A large part of the proof will be to show that the composition of the maximal unramified extension with a maximal totally ramified extension is in fact the maximal abelian extension. After this we will need to determine the norm groups of certain fields and establish the functoriality of the Artin map.

We should mention that while we have striven for a self-contained exposition we have found that ommiting certain proofs increased the readibility and flow of the paper. The proofs we omit are largely technical results whose proofs are of an unenlightening nature. The one exception to this is The Hasse-Arf theorem which we do not include because its proof is elementary, complicated, and outside the framework of Lubin-Tate theory. In the beginning we will state the results needed from Algebraic Number Theory but we will assume as known many algebraic concepts. In particular Galois theory and its infinite analogue will be assumed.

For the preliminaries we refer to [3] and [2]. Our exposition of Formal Group Laws follows that of [4] as Milne does an excellent job of presenting the main facts quickly. We continue to follow his exposition, with some help form [6] up until the Local Kronecker-Weber theorem. To prove the remaining theorems of Local Class Field Theory we found it necessary to consult [5] and [1].

Contents

1 Preliminaries from Algebraic Number Theory

Definition 1.1. An absolute value on a field K is a nonnegative function $|\cdot|\colon K \to \mathbf{R}$ satisfying the following properties: it should attain positive values on nonzero elements and zero on the zero, it should be multiplicative and lastly it should satisfy the triangle inequality: $|x+y| \leq |x| + |y|$ for all $x, y, z \in K$. If in fact the absolute value satisfies the stronger condition that $|x+y| \leq \max\{|x|, |y|\}$ then we say the absolute value is non-archimedean on K. Moreover if $|K^*|$ is discrete in $\mathbb{R}_{>0}$ then we say $|\cdot|$ is a discrete absolute value.

Definition 1.2. By a local field we mean a field K with a discrete absolute value that induces a topology with respect to which K is locally compact. We will call a local field whose topology is induced by a non-archimedean absolute value a non-archimedian local field.

Theorem 1.3. Let K be a nonarchimdean local field, then K is either finite extension of $\mathbb{Q}_p$ for some p or a finite extension of $\mathbb{F}_p((x))$ the Laurent series field over a finite field.

Proof: [2] Chapter 2, Proposition 5.2
♣

Definition 1.4. If K is a non-archimedean local field then define $\mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$ to be the ring of integers of K.

Note that although we defined a valuation to be multiplicative most people who have studied valuations on rings will have seen an additive definition. However, one can pass from (non-archimeadean) multiplicative valuations to their additive analogue using the logarithm and the exponential functions to go backwards - using this we will see that $\mathcal{O}_K$ is in fact a discrete valuation ring.

Proposition 1.5. If K is a non-archimedean local field with absolute value $|\cdot|$ then $log|\cdot|$ is an additive valuation with respect to which $\mathcal{O}_K$ is a discrete valuation domain whose unique prime ideal is $\{x \in K||x| < 1\}$.

Proof: [3] Propositions 7.5 and 7.6
♣

Proposition 1.6. If K is a non-archimedean local field with absolute value $|\cdot|$ then $|K|$ is a subset of the real numbers with only zero as a limit point.

Proof: [3] Proposition 7.6
♣

Definition 1.7. Any generator of the maximal ideal of $\mathcal{O}_K$ is called a prime element. Note that such elements exist as discrete valuation rings are principal rings.

Proposition 1.8. If K is a nonarchimedean local field and L a finite extension of K, then there is a unique extension of the additive valuation on K to L. This additive valuation induces a metric on L making it a local field. Also, the valuation ring of L is the integral closure of $\mathcal{O}_K$ in L.

Proof: [2] Chapter 2, Theorem 4.8
♣

Proposition 1.9. If K is a nonarchimdean local field and $a_i \in L$ some sequence then $\lim_{n\to\infty} \sum_{i=1}^{n} a_i$ converges if and only if $a_i \to 0$.

Proof: One can immediately recognize the forward direction as the well known convergence test. It therefore remains to show $a_i \to 0$ is sufficient to guarantee the sum converges. We will show the sequence of partial sums, $s_n = a_1 + ... + a_n$, is Cauchy and completeness will give the result. Recall that K is complete since it is locally compact and compact neighborhoods are complete. Since the norm is non-archimdean we have:

$$|s_n - s_m| = |\sum_{i=m+1}^{n} a_i| \leq \min\{|a_{m+1} + ... + a_{n-1}|, |a_n|\}$$

but using the non-archimedean property again we know the the term on the right is less than or equal to

$$\min\{|a_{m+1} + ... + a_{n-2}|, |a_{n-1}|, |a_n|\}$$

and proceeding in this way we obtain

$$|s_n - s_m| = |\sum_{i=m+1}^{n} a_i| \leq \min\{|a_{m+1}|, ..., |a_n|\}$$

Now, we use the fact that $a_i \to 0$ and choose m, n to be large enough so that $|s_n - s_m|$ is small. This shows that the partial sums are Cauchy and therefore convergent.
♣

Proposition 1.10. Given an extension of local fields L/K we know that we have a corresponding integral extension of $\mathcal{O}_L/\mathcal{O}_K$ of discrete valuation rings. From the basic theory of integral extensions of Dedekind rings we know that if m_K and m_L are the maximal prime ideals of $\mathcal{O}_K$ and $\mathcal{O}_L$ then $m_K = m_L^e$ for some e. Moreover that if $|\mathcal{O}_L/m_L : \mathcal{O}_K/m_K| = f$ is the degree of residue field extensions then $ef = |L : K|$.

Proof: [3] Theorem 3.34
♣

Definition 1.11. As in the proposition above call e the ramification index of L/K and f the residue class degree. ♣

Definition 1.12. : If L/K is an extension with ramification index equal to 1 then we say L is an unramified extension of K, however if the ramification index equals $|L : K|$ then we call the extension totally ramified. An infinite extension is unramified (totally ramified) if every finite subextension is unramified (totally ramified).

Proposition 1.13. If L_1, L_2 are unramified extensions of K then L_1L_2 is as well.

Proof: [2] Chapter 2, Corollary 7.3 ♣

Corollary 1.14. If K is a local field then there exists a unique maximal unramified extension of K, we call it K^{un}.

Proof: Zorn's lemma tells us that a maximal unramified extension exists, so assume L_1 and L_2 are examples. Then by the previous result L_1L_2 is also unramified and by maximality we have that $L_1 = L_1L_2 = L_2$ as desired. ♣

Proposition 1.15. Unramified extensions have a Galois group isomorphic to that of the residue field extensions and are thus cyclic.

Proof: [3] Theorem 7.50 ♣

Definition 1.16. : If L/K is a unramified extension and l/k the corresponding residue field extension with $|k| = q$ then by the previous proposition there exists a unique element $\sigma \in Gal(L/K)$ such that $\sigma a = a^q \mod m_L$ for every $a \in L$. This element is called the Frobenius of the Galois group $Gal(L/K)$.

We will need the following lemma regarding finitely generated modules over principal ideal domains. For the following lemma suppose that A is a principal ideal domain with a unique prime ideal generated by some $\pi \in A$.

Lemma 1.17. Let M be a A-module and put $M_n = \ker \pi_n$ where $\pi^n : M \to M$ is the endomorphism $m \mapsto \pi^n \cdot m$. If $|M_1| = |A/(\pi)|$ and $\pi : M \to M$ is surjective then $M_n \cong A/(\pi)^n$ as A-modules.

Proof: We proceed by induction on n. Note that M_1 has the same size as $A/(\pi)$. Since A has a unique prime ideal the structure theorem of finitely generated A-modules tells us that every A-module will be isomorphic to $A/(\pi)^{n_1} \oplus A/(\pi)^{n_2} \oplus \cdots \oplus A/(\pi)^{n_k}$ where the n_i form an increasing sequence of natural numbers. This forces $M_1 \equiv A/(\pi)$ which completes the base case. Next consider the following chain complex

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

where the second map is multiplication by π and $M_{n-1} \cong A/(\pi^{n-1})$. The fact that $\pi : M \to M$ is surjective tells us that every element in M_{n-1} is of the form $\pi \cdot x$ where $x \in M$. Since $\pi \cdot x \in M_{n-1}$ we know that $\pi^n \cdot x = 0$ so that $x \in M_n$, this tells us that the above sequence is in fact exact. So M_n has q^n many elements and is of the form stated above. If it isn't cyclic (i.e. of the form $A/(\pi)^n$ for some n) then it is impossible for $M_{n-1} \cong A/(\pi)^{n-1}$ which we have assumed. Therefore $M_n \cong A/(\pi)^n$ as desired. ♣

We are now in a position to describe the Local Artin map.

Theorem 1.18. If K is a local field a and $Gal(K^{ab}/K)$ the Galois group of the maximal abelian extension of K then there exists a unique map $\phi : K^* \to Gal(K^{ab}/K)$ such that for each prime element $\pi \in K$, $\phi(\pi)|_{K^{un}}$ is the Frobenius element. Moreover, for any finite abelian extension L/K, ϕ induces an isomorphism: $\phi_{L/K} : K^*/N_{L/K}(L^*) \to Gal(L/K)$.

Recall from infinite Galois theory that there is a one to one correspondence between open subgroups of $Gal(K^{ab}/K)$ and finite abelian extensions of K. The theorem gives us a link between the norm subgroup of that field and its fixed field. We will see that this is actually a bijection and that what we have is a one-to-one order-reversing correspondence between norm subgroups and finite field extensions. Note that by the above theorem every norm subgroup is of finite index in K^*. It is not difficult to show that it is open in K^*. The converse of the previous two statements is the content of the next major theorem of Local Class Field theory:

Theorem 1.19. (Local existence): Every open subgroup of finite index in K^* is a norm subgroup.

In constructing the Artin map it will be useful to define the action of $\phi(K^*)$ over two subfields, the maximal unramified extension K^{un} and some maximal totally ramified extension separately. We will then use the Hasse-Arf theorem from classical algebraic number theory to show that the composition of these two subfields equals K^{ab}.

Proposition 1.20. Let $\mathcal{O}_K^*$ denote the group of multiplicative units in $\mathcal{O}_K$, then we have an isomorphism $K^* \cong \mathbb{Z} \times \mathcal{O}_K^*$.

Proof: Fix a prime element $\pi \in \mathcal{O}_K^*$ and note that $\mathcal{O}_K^* = \mathcal{O}_K - m_K = \{x \in K || x| = 1\}$, now we know every element in $\mathcal{O}_K^*$ can be written as $u\pi^m$ with $u \in \mathcal{O}_K^*$ since it is a discrete valuation domain with maximal ideal equal to (π). Send this element to $(m, u) \in \mathbb{Z} \times \mathcal{O}_K^*$. It is easy to verify that it is a group isomorphism. ♣

Proposition 1.21. Let L/K be a Galois extension of local fields then because $Gal(L/K)$ fixes the prime ideal $m_L \subset \mathcal{O}_L$ setwise there is an induced action on $\mathcal{O}_L/m_L = l$. Putting $k = \mathcal{O}_K/m_K$. This yields a surjective homomorphism $Gal(L/K) \to Gal(l/k)$.

Proof: [3] Propositions 7.50 and 8.10 ♣

Definition 1.22. The kernel of the above map is denoted $(Gal(L/K))_0$ and is called the inertia subgroup of $Gal(L/K)$. By the above proposition we have $Gal(L/K)/(Gal(L/K))_0 \cong Gal(l/k)$

Proposition 1.23. The fixed field of the inertia subgroup is the maximal unramified extension of L/K.

Proof: [3] Proposition 7.58 ♣

Proposition 1.24. Given an algebraic extension of local fields L/K there is a one to one correspondence between unramified subextensions and residue field subextensions of l/k.

Proof: [3] Proposition 7.50 ♣

Proposition 1.25. Given an extension of local fields L/K, the corresponding extension of integer rings, $\mathcal{O}_L/\mathcal{O}_K$ is monogenic, that is, there is a $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_K[\alpha] = \mathcal{O}_L$.

Proof: [6] Chapter 3, Section 6, Proposition 12 ♣

Definition 1.26. A polynomial $f \in \mathcal{O}_K$ of degree n

$$f(X) = a_n X^n + ... + a_1 X + a_0$$

is called Eisenstein if $a_i \in m_K$ exactly when $i < n$ and if $0 = |\pi|$ for some prime element π of $\mathcal{O}_K$.

Proposition 1.27. A finite extension of local fields L/K is totally ramified if and only if $L \cong K[\alpha]$ where α is the root of an Eisenstein polynomial.

Proof: [3] Proposition 7.55 ♣

Definition 1.28. Given a finite extension L/K, each $a \in L$ induces a K-linear map, σ_a, on L viewed as a K-vector space: $b \mapsto ab$. Define the norm of $a \in L$ with respect to L/K to be $\det(\sigma_a)$. We denote this quantity $N_{L/K}(a)$. More generally if L/K is not finite, then set $N_{L/K}(L^*) = \bigcap K'/K N_{K'/K}(K'^*)$ where K' runs through the finite subextensions of L/K.

Proposition 1.29. The norm operator is transitive, that is if $M/L/K$ are finite extensions then $N_{M/L} = N_{L/K} \circ N_{M/L}$. Moreover if, L/K is Galois then $N_{L/K}(a) = \Pi_{\sigma \in G_{L/K}} \sigma(a)$.

Proof: [2] Chapter 1, Corollary 2.7 ♣

Theorem 1.30. An algebraic extension L/K is totally ramified if and only if its Norm group $N_{L/K}(L^*)$ contains a prime element of K.

Proof: For finite extensions L/K this follows from proposition 1.27 and the fact that the norm of an element is, upto sign, the constant term of its minimal polynomial. So L/K being totally ramified implies the extension is of the form $K[\alpha]/K$ where the minimal polynomial of α is Eisenstein and the norm of α is a prime element of K. Recall that e denotes the ramification index of L/K. Conversely, if a prime element of K, π, is the norm of an element in L, Π, then because the normalized valuation of L, when restricted to K, is equal to ev_K, we have

$$1 = v_K(N_{L/K}(\Pi)) = \frac{v_L(N_{L/K}(\Pi))}{e} = \frac{|L:K| v_L(\Pi)}{e} \geq \frac{|L:K|}{e}$$

Since $|L : K| \geq e$ this forces equality so that L/K must be totally ramified. The infinite case now follows easily. ♣

2 Formal Group Laws

We now introduce the Lubin-Tate formal group laws but before this we give a quick review of formal power series rings.

Definition 2.1. If A is a ring then $A[[x]]$ consists of elements of the form $\sum_{i=0}^{\infty} a_i x^i$ where $a_i \in A$. Moreover, it can be given a ring structure where multiplication and addition are defined formally, that is:

$$\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i$$

and

$$\sum a_i x^i \sum b_j x^j = \sum c_k x^k$$

where $c_k = \sum_{i+j=k} a_i b_j$. We call $A[[x]]$, endowed with the aforementioned ring structure, the formal power series ring.

Note that A will usually just be a ring without any topological structure and as such the notion of an infinite sum over A will be meaningless. This is why we call $A[[x]]$ the ring of *formal* power series because multiplication and addition between two such elements is considered in a formal manner and as such the infinitude of their coefficients pose no problem. However, in what follows we will need to compose two such series that is, given $f, g \in A[[x]]$ can we say what $f(g(x))$ is? If $g(x)$ has a nonzero constant term then the composition will almost always (unless f is a polynomial) require us to sum infinitely many terms because $f(g(x)) = a_0 + a_1(b_0 + ..) + a_2(b_0 + ...)^2 + ...$ where $f = \sum_{i=0}^{\infty} a_i x^i$. In general, over an arbitrary ring A this would be meaningless - so we define $f \circ g$ only when g has no constant term. In this case to calculate the coefficient of x^i in $f(g(x))$ we only need to calculate at the most of the first ith powers of g and then collect the coefficients belonging to x^i in each of $a_j g^j$ $(1 \leq j \leq i)$.

In our discussion about formal group laws we follow [4].

Proposition 2.2. For $f, g, h \in A[[x]]$ where g and h have no constant term then $f \circ (g \circ h) = (f \circ g) \circ h$.

Proof: [4] Chapter 1, Proposition 2.1. ♣

One can define power series in several variables in exactly the same way. Also if $f \in A[[x_1, ..., x_n]]$ and $h_1, ..., h_n$ have no constant terms then we can make sense out of the composition $f(h_1, ..., h_n)$ just as we did in the one variable case so that $f(h_1, ..., h_n) \in A[[x_1, ..., x_n]]$. This brings us to our first new definition

Definition 2.3. Let A be a commutative ring, then a commutative formal group law is a power series $F \in A[[X, Y]]$ such that $F(X, 0) = X$, $F(0, Y) = Y$, $F(X, F(Y, Z)) = F(F(X, Y), Z)$ and $F(X, Y) = F(Y, X)$. Lastly, we require that there be a unique $i_F \in A[[X]]$ with no constant term such that $F(X, i_F(X)) = 0$.

Note that the first two properties imply that F has no constant term and so $F(X, F(Y, Z))$ and $F(F(X, Y), Z)$ make sense. We note the following

Proposition 2.4. Suppose $F \in A[[X, Y]]$ satisfies all of the above requirements for being a formal group law except that instead of $F(X, 0) = X$ and $F(0, Y) = Y$ we have that $F(X, Y) = X + Y + F_2$ where F_2 is a power series with degree ≥ 2 terms. Then F is a formal group law.

Proof: [4] Chapter 1, Remark 2.4. ♣

Proposition 2.5. Suppose $F \in A[[X,Y]]$ satisfies all of the above requirements for being a formal group law except for the existence of an i_F with $F(X, i_F(X)) = 0$, then F is still a formal group law.

Proof: [5] Lemma 3.1. ♣

We now specialize to the local number theoretic situation. Suppose that our commutative ring is actually $\mathcal{O}_K$, the ring of integers in a nonarchimedean local field, we now have the notion of convergence! Let $F = \sum_{i,j\geq 0} a_{ij}X^iY^j$ be a formal group law over $\mathcal{O}_K$. Proposition 1.9 says that a series converges if and only if its summands converge to zero in such fields. As such if $c, d \in m_K$ then the series $\sum_{i,j\geq 0} a_{ij}c^id^j$ converges to some element in $\mathcal{O}_K$. That the series converges in m_K follows because it is closed. From here onwards we will call this element $c+_F d$. Since $F(X,Y)$ is a formal group law m_K is an abelian group under $+_F$. Another set we can turn into a group using F is the collection of all formal power series in one or more variables without constant terms: if $f, g \in ZA[[Z]]$ then define $f +_F g = F(f(Z), g(Z)) \in ZA[[Z]]$. Now we define the morphisms between these group laws

Definition 2.6. Given two formal group laws F, G over A a homomorphism $F \to G$ is an element $f \in ZA[[Z]]$ with the property that $f(F(X,Y)) = G(f(x), f(y))$. If there is a homomorphism $G \to F$ with $f \circ g = g \circ f = Z$ then we say that f is an isomorphism of formal group laws. A homomorphism from F to itself is called an endomorphism.

Proposition 2.7. For any two formal group laws F, G the set of homomorphism from F to G is a group under $+_G$, we call this set $Hom(F,G)$. Moreover, the set of endomorphism of a group law forms a ring $End(F)$ with multiplication being the composition of power series.

Proof: First we show that the set is closed under addition, let $f, g \in Hom(F,G)$ and consider $h = f +_G g$ then note that

$$h(F(X,Y)) = G(f(F(X,Y)), g(F(X,Y))) = G(G(f(X), f(Y)), G(g(X), g(Y)))$$

which is

$$f(X) +_G f(Y) +_G g(X) +_G g(Y)$$

and now because G satisfies associativity and commutativity this is equal to

$$(f(X) +_G g(X)) +_G (f(Y) +_G g(Y)) = G(h(X), h(Y))$$

this tells us that h is in fact a homomorphism from $F \to G$. Now we would like to show that if $f \in Hom(F,G)$ then $i_G \circ f \in Hom(F,G)$. To see this we first show that $i_G \circ G = G \circ i_G$. Note that $G(G(X,Y), G(i_G(X), i_G(Y))) = X +_G Y +_G i_G(Y) +_G i_G(X) = 0$ (using associativity and commutativity of $+_G$) so that $G \circ i_G$ kills $G(X,Y)$ but $i_G \circ G$ also has this property and since there is only one power series with this property they must be the same. This means $i_G \circ f(F(X,Y)) = i_G \circ (G(f(X), g(Y))) =$

$G(i_G(f(X)), i_G(f(Y)))$ as desired. It is clear that $0 \in Hom(F, G)$ so the first statement is proved. To show that the endomorphisms form a ring we need only show distributivity, i.e. that $f \circ (g +_G h) = f \circ g +_G f \circ h$ since Z is the multiplicative identity and is clearly an endomorphism. But $f \circ (g +_G h) = f \circ G(g(Z), h(Z)) = G(f \circ g(Z), f \circ h(Z)) = f \circ g +_G f \circ h$ as desired. Distributivity from the other side is proved in the exact same way. ♣

Definition 2.8. Consider the ring of formal power series over $\mathcal{O}_K$, the ring of integers in a nonarchimedean local field and a prime element $\pi \in K$. Then let $\mathcal{F}_\pi$ denote the set of all $f \in \mathcal{O}_K[[X]]$ such that $f(X)$ has no constant term, $f \equiv \pi X \mod$ degree two terms, and $f \equiv X^q \mod (\pi)$. Here $q = |\mathcal{O}_K/m_K|$ is the size of the residue field of K.

The following lemma will be essential in endowing the Lubin-Tate group laws with an $\mathcal{O}_K$-module structure. It is a special case of another lemma we will state but not prove.

Lemma 2.9. Given $f, g \in \mathcal{F}_\pi$ and any linear polynomial $\phi_1(X_1, ..., X_n)$ over $\mathcal{O}_K$ there exists a unique $\phi \in \mathcal{O}_K[[X_1, ..., X_n]]$ such that ϕ has linear part equal to ϕ_1 and no constant terms with $f(\phi) = \phi(g)$.

Proof: We inductively construct our ϕ degree by degree. Let ϕ_1 be as in the statement of the theorem. We shall construct ϕ_r such that

$$f(\phi_r(X_1, ..., X_n) = \phi_r(g(X_1), ..., g(X_n)) + \epsilon_{r+1}$$

where ϵ_{r+1} consists of $r+1$-degree terms. In what follows ϵ_i will be a generic term for formal power series that have minimal degree greater than or equal to i. For ϕ_1 note that because ϕ_1 is linear we have

$$f(\phi_1) = \pi(\phi_1(X_1, ..., X_n) + \epsilon_2 = \phi_1(\pi(X_1), ..., \pi(X_n)) + \epsilon_2$$

which is, modulo degree ≥ 2 terms:

$$\phi_1(\pi X_1 + \epsilon_2, ..., \pi X_n + \epsilon_2) + \epsilon_2 = \phi_1(g(X_1), ..., g(X_n)) + \epsilon_2$$

So the case $r = 1$ is complete and we assume that ϕ_r exists satisfying the above properties, that is: it is the unique degree r polynomial with coefficients in $\mathcal{O}_K$ satisfying $f \circ \phi_r = \phi_r(g) + \epsilon_{r+1}$ and $\phi_r = \phi_1 + \epsilon_2$. We have to show the existence of ϕ_{r+1} and if it were to exist then we'd have that $\phi_r + Q = \phi_{r+1}$ for some homogenous degree $r+1$ polynomial Q. This is because if we chopped off the degree $\geq r+1$ terms of ϕ_{r+1} we'd get a suitable replacement for ϕ_r, but by uniqueness they must be the same modulo degree $r+1$ terms. In other words we get ϕ_{r+1} by adding to ϕ_r a homogenous polynomial, Q, of degree $r+1$.

What we want is a ϕ_{r+1} with

$$f(\phi_{r+1}(X_1, ..., X_n)) = f(\phi_r(X_1, ..., X_n) + Q) = f(\phi_r(X_1, ..., X_n)) + \pi Q + \epsilon_{r+2}$$

which should equal

$$\phi_{r+1}(g) = \phi_r(g(X_1), ..., g(X_n)) + Q(g(X_1), ..., g(X_n) = \phi_r(g) + Q(\pi X_1, ..., \pi X_n) + \epsilon'_{r+2}$$

So if Q is to make both quantities equal we will need it to satisfy

$$Q(\pi X_1, ..., \pi X_n) - \pi Q = f(\phi_r) - \phi_r(g) + \epsilon''_{r+2}$$

but because Q is homogenous of degree $r+1$ the above equation becomes

$$(\pi^{r+1} - \pi)Q = f(\phi_r) - \phi_r(g) + \epsilon''_{r+2}$$

so Q must equal the sum of the degree $r+1$ terms in the power series

$$\frac{f \circ \phi_r - \phi_r \circ g + \epsilon''_{r+2}}{\pi(\pi^r - 1)}$$

It remains to show that Q has coefficients in $\mathcal{O}_K$. To do this it suffices to prove that $f \circ \phi_r - \phi_r(g)$ is divisible by π. Since $f, g \in \mathcal{F}_\pi$ we know that the coefficient of every ith degree term of f and g (except for $i = q = |\mathcal{O}_K/m_K|$) is divisible by π so:

$$f(\phi_r) = \sum_{i \neq q} \pi a_i (\phi_r)^i + \phi_r^q$$

and

$$\phi_r(g) = \phi_r(\sum_{i \neq q} \pi b_i X_1^i + X_1^q, ..., \sum_{i \neq q} \pi b_i X_n^i + X_n^q)$$

now when we pass to the residue field (mod out by (π)) of characteristic p we get

$$f(\phi_r) \equiv \phi_r(X_1, ..., X_n)^q \equiv \phi_r(X_1^q, ..., X_n^q)$$

and

$$\phi_r(g) \equiv \phi_r(X_1^q, ..., X_n^q)$$

so that their difference mod π is 0. Since $\pi - 1$ is a unit in $\mathcal{O}_K$ this completes the proof that Q is a polynomial in $\mathcal{O}_K$. Now take $\phi_{r+1} = \phi_r + Q$ and by the construction of Q it is obvious it satisfies the required properties. Now we define ϕ to be the unique power series extending each of the ϕ_r's. It will satisfy $f \circ \phi = \phi \circ g$ because it does so modulo degree r terms for each natural number r. ♣

Proposition 2.10. For each $f \in \mathcal{F}_\pi$ there exists a unique formal group law $F_f \in \mathcal{O}_K[[X, Y]]$ such that $f \in End(F_f)$.

Proof: Use the lemma above with $\phi_1 = X+Y$ and $f = f = g$ to get some $\phi(X, Y) \in \mathcal{O}_K[[X, Y]]$ which we will call F_f. It remains to check that it is a formal group law. We need to check first commutativity, put $F_f(Y, X) = G(X, Y)$. Note then that $G = \phi_1$ modulo degree two terms and that $f(G(X, Y)) = f(F_f(Y, X)) = F_f(f(Y), f(X)) = G(f(X), f(Y))$. But then G and F_f satisfy the properties of the above lemma (with $f = f = g$ and $\phi_1 = X + Y$) and so by uniqueness they must be the same. For associativity we proceed similarly by considering $G(X, Y, Z) = F_f(F_f(X, Y), Z)$ and $H(X, Y, Z) = F_f(X, F_f(Y, Z))$. Then note that both G and H equal $X + Y + Z$ plus

some degree ≥ 2 terms. It is also easy to see that $f \circ G = G \circ f$ and $f \circ H = H \circ f$ so again by uniqueness they must be the same. By the propositions 2.4 and 2.5 we see that F_f is a formal group law and that $f \in End(F_f)$. ♣

The formal group laws F_f whose existence we have just proven are called the Lubin-Tate formal group laws and will be essential in constructing totally ramified extensions of a nonarchimdean local field K. Now let $f, g \in \mathcal{F}_\pi$ and let $a \in \mathcal{O}_K$ then Lemma 2.9 guarantees the existence of an $[a]_{f,g} \in Z\mathcal{O}_K[[Z]]$ whose linear term is exactly aZ and satisfying $g \circ [a]_{g,f} = [a]_{g,f} \circ f$.

Proposition 2.11. $[a]_{g,f}$ is a homomorphism of formal group laws $F_f \to F_g$.

Proof: We need to show that $[a]_{g,f}(F_f(X,Y)) = F_g([a]_{g,f}(X), [a]_{g,f}(Y))$. Their linear terms agree since they are both equal to $aX + aY$. Now notice

$$[a]_{g,f}(F_f(f(X), f(Y))) = [a]_{g,f} \circ f(F_f(X,Y)) = g \circ [a]_{g,f}(F_f(X,Y))$$

To proceed, observe

$$[a]_{g,f}(F_f([a]_{g,f}(X), [a]_{g,f}(Y))) = \phi$$

satisfies $\phi(f) = g(\phi)$ since

$$\phi \circ f = F_g(g([a]_{g,f}(X)), g([a]_{g,f}(Y))) = g \circ F_g([a]_{g,f}(X), [a]_{g,f}(Y)) = g \circ \phi$$

and also that $\phi' = [a]_{g,f}(F_f(X,Y))$ satisfies $\phi'(f) = g(\phi')$ because

$$\phi' \circ f = [a]_{g,f}(F_f(f(X), f(Y))) = [a]_{g,f} \circ f \circ (F_f(X,Y)) = g \circ [a]_{g,f}(F_f(X,Y)) = g \circ \phi'$$

so by the uniquness in Lemma 2.10 they must be the same power series as desired. ♣

Our aim is to prove that there is a ring morphism $\mathcal{O}_K \to End(F_f)$ taking $a \mapsto [a]_{f,f}$ so that we can consider think of F_f as an abstract $\mathcal{O}_K$-module. By this we mean that if we regard some subset of a ring B with $\mathcal{O}_K \subset B$ as a group under the group law $+_{F_f}$ then it would have an accompanying $\mathcal{O}_K$-module structure compatible with the group law.

Proposition 2.12. The map considered above $\mathcal{O}_K \to End(F_f)$ is an injective ring homomorphism.

Proof: We will prove something slightly more general, i.e. that for any $a, b \in A$ we have $[a+b]_{g,f} = [a]_{g,f} +_{F_g} [b]_{g,f}$ and $[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}$. Once we have proven these two identities then the proposition follows when we set $g = h = f$.

The plan of the proof will be to show that both sides of both equations satisfy the same properties and then use uniqueness in Lemma 2.9 to show that they must be the same. For the first one we know that $[a+b]_{g,f}$ is the unique power series satisfying both $[a+b]_{g,f}(T) = (a+b)T + \sum_{i=2}^{\infty} c_i T^i$ and $g \circ [a+b]_{g,f} = [a+b]_{g,f} \circ f$. But it is obvious that $g \circ ([a]_{g,f} +_{F_g} [b]_{g,f}) = g \circ F_g([a]_{g,f}, [b]_{g,f}) = F_g(g \circ [a]_{g,f}, g \circ [b]_{g,f}) = F_g([a]_{g,f} \circ f, [b]_{g,f} \circ f)$ but this last power series is actually just $([a]_{g,f} +_{F_g} [b]_{g,f}) \circ f$. By uniqueness we see that they must be the same. Similarly note that $h \circ [ab]_{h,f} = [ab]_{h,f} \circ f$ and that $[ab]_{h,f}$ has abT as its linear term. Now $h \circ [a]_{h,g} \circ [b]_{g,f} = [a]_{h,g} \circ g \circ [b]_{g,f} = [a]_{h,g} \circ [b]_{g,f} \circ f$

and its not hard to see that $[a]_{h,g} \circ [b]_{g,f}$ has abT as its linear term as well. Again, by uniqueness we see that these two power series are the same.

To complete the proof that it is a ring homomorphism we need to check that $1 \mapsto T$ under this mapping but clearly the linear term of T and $[1]_{f,f}$ are the same and also both commute with f, so in fact $[1]_{f,f} = T$. That the map is injective is clear since if $a \neq 0$ then $[a]_{f,f}$ will have a nonzero linear term and hence cannot be the zero power series. ♣

3 Lubin-Tate Extensions and their Galois groups

Fixing some prime element $\pi \in \mathcal{O}_K$ we will construct a totally ramified abelian extension K_π which will satisfy certain nice properties. Namely π will be a norm for any finite subextension of K_π, we will have $K_\pi = \bigcup_{i=1}^{\infty} K_{\pi,n}$ where $K_{\pi,n}$ is totally ramified with degree over K equal to $q^{n-1}(q-1)$. Moreover, $K_{\pi,n}$ will have a Galois group isomorphic to $(\mathcal{O}_K/(\pi)^n)^* \cong \mathcal{O}_K^*/(1+(\pi)^n)$ (this last isomorphism will become clear later). We proceed in steps.

Note that the valuation on a nonarchimedean local field K extends uniquely to any finite extension of K and thus using a maximality argument we see that it must extend to the entire algebraic closure of K, $\bar{K}$. Fix $f \in \mathcal{F}_\pi$. Given any two elements $x, y \in \bar{K}$ with valuation strictly less than one we see that $F_f(x,y)$ converges (since its summands goto zero). Moreover since F_f was constructed to have no constant term it converges to an element with valuation strictly less than one. Note that we are using the fact that a nonarchimedean valuation is a group homomorphism sending K^* to a set of points in $\mathbb{R}$ with only zero as the limit point. In this way we endow $m_{\bar{K}} = \{x \in \bar{K} || x| < 1\}$ with the group structure induced by the group law $+_{F_f}$. As remarked above this also endows $m_{\bar{K}}$ with an $\mathcal{O}_K$-module structure where $a \cdot x = [a]_{f,f}(x)$. We will let $m^f_{\bar{K},n}$ denote the set of elements killed by $[\pi]^n_{f,f}$. But clearly $f = [\pi]_{f,f}$ since its linear term is πT and it commutes with F_f. We will set $K_{\pi,n} = K[m^f_{\bar{K},n}]$ and later show it has the required properties. The next proposition illustrates why which $f \in \mathcal{F}_\pi$ we choose does not matter.

Proposition 3.1. If we have two polynomials $f, g \in \mathcal{F}_\pi$ then we have $K[m^f_{\bar{K},n}] = K[m^g_{\bar{K},n}]$ as field extensions of K.

Proof: By lemmas 2.11 and 2.12 there is a power series $[1]_{g,f} \in \mathcal{O}_K[[X]]$ with $[1]_{g,f}(f) = g([1]_{g,f})$. Thus we have $[1]_{g,f} : m^f_{\bar{K},n} \to m^g_{\bar{K},n}$ which is $\mathcal{O}_K$-module map, it is invertible because 1 is. Since $K[m^f_{\bar{K},n}]$ is a finite extension K it is complete and therefore $[1]_{g,f}(a) \in K[m^f_{\bar{K},n}]$ for $a \in m^f_{\bar{K},n}$. This shows $m^g_{\bar{K},n} \subset K[m^f_{\bar{K},n}]$ completing the proof. ♣

This allows us to choose $f = \pi T + T^q$ for simplicity. And $m^f_{\bar{K},n}$ will consist of the roots of $f^{(n)} = f \circ f \circ \cdots \circ f$ (n times) whose absolute value, as the next proposition shows, is strictly less than one.

Proposition 3.2. The polynomial, $f^{(n)}$, above has as roots elements with valuation strictly less than one.

Proof: The roots of $f^{(2)}$ are the roots of the polynomial $f(X) - a$ where a is a root of $f(X)/X$. Note that a is a root of the Eisenstein (hence irreducible) polynomial $X^{q-1} + \pi$. Thus in $K[a]$, a has, with respect to the normalized valuation, valuation one, i.e. it is in $m_{K[a]}$ but not $m^2_{K[a]}$. Now lemma 3.3 applies to show that the roots of $f(X) - a$ have valuation strictly less than one. Using lemma 3.3 again we see that if we replace a with any of the roots of $f(X) - a$ we can repeat this whole argument

with $f^{(3)}$ in place of $f^{(2)}$. The argument for $f^{(n)}$ now follows by an easy inductive argument. ♣

The set $m^f_{\bar{K},n}$ consists of the roots of $f^{(n)}$ and is closed under the operation $+_{F_f}$ since $f(F_f(x,y)) = F_f(f(x), f(y)) = F(0,0) = 0$ (since F_f has no constant term) when $x, y \in m^f_{\bar{K},n}$. It is also closed under $[a]_{f,f}$ because $f([a]_{f,f}(x)) = [a]_{f,f}(f(x)) = [a]_{f,f}(0) = 0$ since $[a]_{f,f}$ is a power series with no constant term. Thus we know that $m^f_{\bar{K},n}$ has an $\mathcal{O}_K$-module structure. Note that $m^f_{\bar{K},n}$ is a torsion $\mathcal{O}_K$-module that is finitely generated since it is finite and is killed by $f^{(n)} = [\pi]^n_{f,f}$. Since $\mathcal{O}_K$ is a discrete valuation ring we can apply the theory of finitely generated modules over principal ideal domains.

Lemma 3.3. The polynomials $\pi T + T^q - a$ where $a \in m_K$ but not in m_K^2 are Eisenstein polynomials and therefore have q distinct roots each of which has absolute value strictly less than one. Moreover if b is a root then $b \in m_{K[b]}$ but not in $m^2_{K[b]}$.

Proof: [3] Proposition 3.53 ♣

Theorem 3.4. The $\mathcal{O}_K$-module $m^f_{\bar{K},n}$ is isomorphic to $\mathcal{O}_K/(\pi)^n$.

Proof: For any two $f, g \in \mathcal{F}_\pi$ there is a formal group isomorphism $F_f \to F_g$. As we remarked earlier this really means that any two sets that form $\mathcal{O}_K$-modules under the group laws $+_{F_f}$ and $+_{F_g}$ respectively are actually isomorphic as $\mathcal{O}_K$-modules. In this way we see that it doesn't matter which $f \in \mathcal{F}_\pi$ we choose. So suppose that $f = \pi X + T^q$ this has q distinct roots with valuation smaller than one. Moreover if $a \in m_{\bar{K}}$ the preceding lemma tells us that $f - a$ is has q distinct roots all of which lie in $m_{\bar{K}}$. Since $f(a) = [\pi]_{f,f} \cdot a$ we see that the map $m_{\bar{K}} \to m_{\bar{K}}$ is actually surjective since $f(x) - a$ has roots in $m_{\bar{K}}$. Thus the hypothesis of proposition 1.16 are satisfied and the result follows. ♣

We set $K[m^f_{\bar{K},n}] = K_{\pi,n}$. Recall that we remarked earlier the $f \in \mathcal{F}_\pi$ we chose doesn't matter since $K[m^f_{\bar{K},n}]$ is the same extension for any such f. Finally we come to the following

Theorem 3.5. $K_{\pi,n}$ has the three desired properties, that is, it is totally ramified of degree $q^{n-1}(q-1)$, has π as a norm, and $Gal(K_{\pi,n}/K) \cong (\mathcal{O}_K/(\pi)^n)^*$.

Proof: Since our choice of $f \in F_\pi$ doesn't matter we will choose $f(x) = \pi X + X^q$. Choose a nonzero root of f and call it a_1, then let a_2 be a root of $f - a_1$ and in this fashion let a_n be a root of $f - a_{n-1}$. Now because a_1 is the root of an eisenstein polynomial it has positive valuation and therefore is divisible by π which means $f - a_1$ is also eisenstein (hence irreducible of degree q) and so its root a_2 is also divisible by π. In this way we see that each of the polynomials $f - a_i$ are irreducible of degree q. Note also that $f(f(a_2)) = f(a_1) = 0$ and in general $f^{(i)}(a_i) = f^{(i-1)}(a_{i-1}) = ... = f(a_1) = 0$ so that a_i is a root of $f^{(i)}$. Also since $f \in K[X]$ and a_i is a root of $f - a_{i-1}$ we see that $K[a_1, ..., a_k] = K[a_k]$ because $f(a_k) = a_{k-1}$, and so $f^{(j)}(a_k) = a_{k-j}$. Thus we get a sequence of fields

$$K \subset K[a_1] \subset K[a_2] \subset ... \subset K[a_n] \subset K[m^f_{\bar{K},n}] = K_{\pi,n}$$

where the first extension is of degree $q-1$ (since $f = X(\pi + X^{q-1})$ and is Eisenstein) and the other $n-1$ extensions are of degree q, telling us that $q^{n-1}(q-1) \leq |K_{\pi,n} : K|$. To see that each extension is totally ramified just note that the valuation of a_1 is simply $1/(q-1)$ since $a_1^{q-1} = \pi$ and so $(q-1)v(a_1) = v() = 1i$. Similarly $a_2^q + \pi a_2 = a_1$ so $v(a_2^q + \pi a_2) = \frac{1}{q-1}$ and because $v(a_2^q) = qv(a_2) \neq 1 + v(a_2) = v(\pi a_2)$ we must have $v(a_2^q + \pi a_2) = \min(qv(a_2), 1 + v(a_2))$. But which is smaller? If $1 + v(a_2) < qv(a_2)$ then $q - 1v(a_2) > 1$ in other words a_2^{q-1} wouldn't be an algebraic integer, but it is! In this way we see that $v(a_2) = v(a_1)/q$. In exactly the same fashion one can prove that $v(a_i) = \frac{v(a_{i-1})}{q}$ for every other $i \geq 2$. This implies that the extensions $K[a_i]/K$ are totally ramified because the prime ideal (π) factors into $(a_i)^{(q-1)(q^{i-1})}$. By construction $K_{\pi,n}$ is the splitting field of $f^{(n)}$ and as such it's Galois group $Gal(K_{\pi,n}/K)$ faithfully permutes the roots of $f^{(n)}$: $m^f_{\bar{K},n}$. It is useful to note that each element $\sigma \in Gal(K_{\pi,n}/K)$ has an action that is compatible with the given $\mathcal{O}_K$-module structure on $m^f_{\bar{K},n}$. To see this consider that σ acts continuously with respect to the topology induced by $|\cdot|$ since it fixes the ideals $(\pi)^j$ (setwise) for every j. Thus, by continuity, if we take $a \in \mathcal{O}_K$ and consider $[a]_{f,f}$ then $\sigma([a]_{f,f}(x)) = [a]_{f,f}(\sigma(x))$. This follows since σ commutes with limits by continuity i.e.

$$\sigma([a]_{f,f}(x)) = \sigma(\lim_{i\to\infty} \sum^{i} a_i x^i) = \lim_{i\to\infty} \sum^{i} a_i \sigma(x)^i$$

as desired. So each $\sigma \in Gal(K_{\pi,n}/K)$ is a $\mathcal{O}_K$-isomorphism of $m^f_{\bar{K},n}$. But we know the latter is isomorphic to $\mathcal{O}_K/(\pi)^n$ thereby implying its endomorphism ring is isomorphic to $\mathcal{O}_K/(\pi)^n$). This tells us that we have an injection of groups: $Gal(K_{\pi,n}/K) \to (\mathcal{O}_K/(\pi)^n)^*$. The latter group has order equal to $(q-1)q^{n-1}$ (because there are $q-1$ cosets in $\mathcal{O}_K/(\pi)$ and q cosets in each of $(\pi)^i/(\pi)^{i+1}$ for $i \geq 1$) telling us that $|K_{\pi,n} : K| = |Gal(K_{\pi,n}/K)| \leq q^{n-1}(q-1)$, but earlier we had the reverse inequality. It follows that $K[a_n] = K_{\pi,n}$ and that the map $Gal(K_{\pi,n}/K) \to (\mathcal{O}_K/(\pi)^n)^*$ mentioned above is actually an isomorphism.

We now only need to show that π is the norm of some element in $K[a_n]$. Note that a_1 is a root of $f(X)/X = \pi + X^{q-1}$ and that $f^{n-1}(a_n) = a_1$ meaning a_n is a root of $f(X)/X \circ f^{(n-1)}(X)$ which looks like $\pi + ... + X^{q^{n-1}(q-1)}$. The minimal polynomial of a_n over K must divide this and have degree equal to $q^{n-1}(q-1)$. Since this polynomial has the same degree it must be the minimal polynomial of a_n and hence we know the constant term is the product of the Galois conjugates of a_n. This is the norm of a_n and is equal to $(-1)^{(q-1)q^{n-1}}\pi = \pi$. ♣

4 The fields $K^{un} \cdot K_\pi$ and the maps ϕ_π

We are getting closer to the main theorem of local class field theory. We are now in a position to explicitly construct the local Artin map. Fix a prime element $\pi \in K$ and consider $K_\pi = \bigcup_{i=1}^{\infty} K_{\pi,n}$. We will define a map $\phi_\pi : K^* \to Gal(K_\pi \cdot K^{un}/K)$ which will turn out to be the Artin map. Before we proceeding with the proof we need two important facts: that ϕ_π and the field $K_\pi \cdot K^{un}$ are independent of our choice of π.

First, the construction. We would like to define how $\phi_\pi(a)$ acts on $K^{un} \cdot K_\pi$ for some $a \in K^*$. Since $K^{un} \cap K_\pi = K$ it suffices to define its image in each of $Gal(K^{un}|K)$ and $Gal(K_\pi|K)$. We know every $a \in K^*$ can be written in the form $u\pi^n$ for some $u \in \mathcal{O}_K^*$ and some integer n, so put $\phi_\pi(u\pi^n)|_{K^{un}} = \varphi^m$ (here φ is the Frobenius over K) and $\phi_\pi(u\pi^n)|_{K_\pi} = [u^{-1}]_{f,f}$ where $f \in \mathcal{F}_\pi$. Note that since u is a unit $\phi_\pi(a)|_{K_\pi}$ is in fact an automorphism of the $\mathcal{O}_K$-module K_π. The main theorem of the chapter is

Theorem 4.1. The $K_\pi \cdot K^{un}$ and ϕ_π as defined above are independent of our choice of prime element $\pi \in K$.

The proof will be long, technical and rather unilluminating and the reader who is willing to accept it is encouraged to skip it and move forward. For the sake of completeness we will present the proof as found in [4].

Remarks: It is a fact that $\bar{K}$ is not complete and neither is K^{un}. So we let $\hat{K^{un}}$ denote its completion. It's clear that the absolute value on $\hat{K}$ extends uniquely to $\hat{K^{un}}$ so we let B denote the set of elements in $\hat{K^{un}}$ with absolute value no larger than 1. Because the Frobenius automorphism, φ, is continuous with respect to this absolute value, it can be extended uniquely to the completion of K^{un} since K^{un} is dense in $\hat{K^{un}}$. For any $\theta(T) = \sum b_i T^i \in B[[T]]$ as before we put $\theta^\varphi(T) = \sum \varphi(b_i)T^i$.

Lemma 4.2. Given $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\nu$ where π and ν are prime elements in K with $u\pi = \nu$ then F_f and F_g become isomorphic as $\mathcal{O}_K$-modules over the ring B. That is, there is an $\epsilon \in B^*$ with $\epsilon^\varphi = \epsilon u$ and an element, θ of the power series ring $B[[T]]$ satisfying

$$a) \quad \theta(T) = \epsilon T + \sigma_{i \geq 2} a_i T^i$$

$$(b) \quad \theta^\varphi = \theta \circ [u]$$

$$(c) \quad \theta(F_f(X,Y)) = F_g(\theta(X), \theta(Y))$$

$$(d) \quad \theta \circ [a]_{f,f} = [a]_{g,g} \circ \theta$$

The last two conditions are another way of saying that θ is a homomorphism $F_f \to F_g$ as (abstract) $\mathcal{O}_K$-modules. That $\epsilon \in B^*$ implies that $\theta \in B[[T]]$ is actually invertible, i.e. that there is a $\theta^{-1} \in B[[T]]$ with $\theta \circ \theta^{-1} = \theta^{-1} \circ \theta = T$. The inverse can be found by solving for θ^{-1} coefficients inductively.

Proof: [4] Chapter 1, Proposition 3.10 ♣

Proof: (Of theorem 4.1) As in the statement of the previous lemma suppose that $\nu = u\pi$ are two prime elements of K. By the lemma there exists a $\theta \in B[[T]]$ such that

$$\theta^{\varphi} \circ [\pi]_{f,f} = \theta \circ [u]_{f,f} \circ [\pi]_{f,f} = \theta \circ [\nu]_{f,f} = [\nu]_{g,g} \circ \theta$$

since $f = [\pi]_{f,f}$ and $g = [\nu]_{g,g}$ we can rewrite the above line as $\theta^{\varphi}(f(T)) = g(\theta(T))$. This tells us that given any element $a \in \bar{K}$ with $f(a) = 0$ then $\theta^{\varphi}(f(a)) = 0$ (since θ^{φ} is a power series with no constant term) but this is equal to $g(\theta(a))$. We have just shown that $f(a) = 0$ implies that $g(\theta(a)) = 0$. Now consider θ^{-1}, it is in $Hom(F_g, F_f)$ and satisfies the following four properties:

$$\theta^{-1}(T) = \epsilon^{-1} + \Sigma_{i \geq 2} c_i T^i$$

$$\theta^{\varphi} = \theta \circ [u^{-1}]_{g,g}$$

$$\theta^{-1}) F_g(X, Y) = F_f(\theta^{-1}(X), \theta^{-1}(Y))$$

$$\theta^{-1} \circ [a]_{g,g} = [a]_{f,f} \circ \theta$$

The first, third and fourth are all follow from the fact that $\theta^{-1} \circ \theta(T) = \theta \circ \theta^{-1}(T) = T$. For example $\theta^{-1}(F_g(X, Y)) = \theta^{-1}(F_g(\theta \circ \theta^{-1}(X), \theta \circ \theta^{-1}(Y))) = \theta^{-1} \circ \theta(F_f(\theta^{-1}(X), \theta^{-1}(Y))) = F_f(\theta^{-1}(X), \theta^{-1}(Y))$ as desired. The second follows since $T = (\theta \circ \theta^{-1}(T))^{\varphi} = \theta^{\varphi} \circ (\theta^{-1})^{\varphi}(T)$ since the composition is compatible with the action of the Frobenius. This fact is easy to see once one realizes that determining the coefficients of the composition of two power series involves calculating finitely many terms at each step. Obviously $\theta^{-1} \circ [u^{-1}]_{g,g}$ is the inverse (with respect to composition) of $\theta \circ [u]_{f,f}$ and since these are uniquely determined we se that $\theta^{-1} \circ [u^{-1}]_{g,g} = (\theta^{-1})^{\varphi}$.

Now we have the following:

$$(\theta^{-1})^{\varphi} \circ [\nu]_g = \theta^{-1} \circ [u^{-1}]_{g,g} \circ [\nu]_{g,g} = \theta^{-1} \circ [\pi]_{g,g}$$

which is simply $[\pi]_{f,f} \circ \theta^{-1}$. In other words $\theta^{\varphi} \circ g(a) = f(\theta^{-1}(a))$. So if $g(a) = 0$ then $f(\theta^{-1}(a)) = 0$. Thus θ establishes a one to one correspondence between $m^f_{\bar{K},1}$ and $m^g_{\bar{K},1}$. From this and the completeness of $\hat{K^{un}}[m^f_{\bar{K},1}]$ and $\hat{K^{un}}[m^f_{\bar{K},1}]$ we deduce the following

$$\hat{K^{un}}[m^g_{\hat{K},1}] = \hat{K^{un}}[\theta(m^f_{\bar{K},1})] \subset \hat{K^{un}}[m^f_{\bar{K},1}] = \hat{K^{un}}[\theta^{-1}(m^g_{\bar{K},1})] \subset \hat{K^{un}}[m^g_{\bar{K},1}]$$

so that we have equality throughout. Note where we use completeness: if $\theta(a) \in m_L \subset L$ a complete field, then so is $a = \theta^{-1}(\theta(a))$ since θ^{-1} has coefficients in L and L is complete. This tells us that $\hat{K^{un}}[m^g_{\bar{K},1}] = \hat{K^{un}}[m^f_{\bar{K},1}]$. The next lemma will tell us that $\hat{K^{un}}[m^g_{\bar{K},1}] \cap \bar{K} = K^{un}[m^g_{\bar{K},1}]$ and $\hat{K^{un}}[m^f_{\bar{K},1}] \cap \bar{K} = K^{un}[m^f_{\bar{K},1}]$ thereby implying

$$K^{un}[m^f_{\bar{K},1}] = K^{un}[m^g_{\bar{K},1}]$$

The proof generalizes without difficulty to yield

$$K^{un}[m^f_{\bar{K},n}] = K^{un}[m^g_{\bar{K},n}]$$

for all $n \geq 1$. This proves that $K_\nu \cdot K^{un} = K_\pi \cdot K^{un}$. ♣

Lemma 4.3. Let E be an algebraic extension of K and let $\hat{E}$ be its completion, then $\hat{E} \cap \bar{K} = E$.

Proof: Consider the Galois group $Gal(\bar{K}|E)$. We know it fixes E and since E is dense in $\hat{E} \cap \bar{K}$ the fact that $Gal(\bar{K}|E)$ acts continuously on $\bar{K}$ tells us that it must also fix $\hat{E} \cap \bar{K}$. By Galois theory this tells us that $\hat{E} \cap \bar{K} \subset E$. The opposite inclusion is obvious. ♣

Proof: (ϕ_π in independent of π) To prove the theorem it suffices to show that for any two prime elements ν and π we have $\phi_\pi(\nu) = \phi_\nu(\nu)$. To see why this is enough, consider any other prime element μ then we would have that $\phi_\pi(\mu) = \phi_\mu(\mu) = \phi_\nu(\mu)$ since ν and π were arbitrary. Now because the prime elements generate K^* this shows that $\phi_\pi = \phi_\nu$. That the prime elements generate K^* is easy to see: any unit can be written as $u = (u\pi)\pi^{-1}$ where π is a prime element so that $u\pi$ is one too.

By construction we have that $\phi_\pi(\nu)|_{K^{un}} = \phi_\nu(\nu)|_{K^{un}} = \varphi$ (the Frobenius) so it remains to show the action of $\phi_\pi(\nu)$ and $\phi_\nu(\nu)$ is the same on K_ν. Take a θ as in Lemma 4.2 that gives an isomorphism of formal group laws $F_f \to F_g$ for $f \in \mathcal{F}_\pi$, $g \in \mathcal{F}_\nu$ ($\nu = \pi u$). This yields an isomorphism of $\mathcal{O}_K$-modules $m^f_{\bar{K},n} \to m^g_{\bar{K},n}$ so that we can say $K_{\nu,n}$ is generated over K by the elements $\theta(a)$ for $a \in m^f_{\bar{K},n}$. Since $\phi_\nu(\nu)$ acts as the identity on K_ν we have to show $\phi_\pi(\nu)(\theta(a)) = \theta(a)$ for any $a \in m^f_{\bar{K},n}$. Write $\phi_\pi(\nu) = \phi_\pi(u)\phi_\pi(\pi)$, now $\phi_\pi(u)$ acts as the identity on K^{un} and as $[u^{-1}]_{f,f}$ on $a \in K_{\pi,n}$. Also $\phi_\pi(\pi)$ acts as the Frobenius on K^{un} and as the identity on $a \in K_{\pi,n}$. Note that we extend the action of the Frobenius and $\phi_\pi(u)$ to $\hat{K^{un}}$, each of which can only be done continuously in one way sinceK^{un} is dense in its completion. From here, we have

$$\phi_\pi(\nu)(\theta(a)) = \phi_\pi(\pi)\phi_\pi(u)(\theta(a)) = \phi_\pi(\pi)\theta(\phi_\pi(u)a)$$

where the last equality holds since $\phi_\pi(u)$ acts as the identity on K^{un} and hence on its completion which is where θ has its coefficients. Continuing, we obtain

$$\phi_\pi(\pi)\theta([u^{-1}]_{f,f}(a)) = \theta^\varphi([u^{-1}]_{f,f}(a)) = \theta \circ [u]_{f,f} \circ [u^{-1}]_{f,f}(a) = \theta(a)$$

Since φ fixes $[u^{-1}]_{f,f}(a)$: $[u^{-1}]_{f,f}$ has coefficients in $\mathcal{O}_K$ and $a \in K_{\pi,n}$. We have thus shown that $\phi_\pi(\nu) = \phi_\nu(\nu)$ yield the same action on $K_\nu \cdot K^{un}$ as desired. ♣

5 Ramification Groups and a proof that $K^{un} \cdot K_\pi = K^{ab}$

Before we can reasonably say that ϕ_π as constructed is the Artin map we need to prove that $K_\pi \cdot K^{un}$ is actually the maximal abelian extension of K, K^{ab}. Note that one inclusion is clear: $K_\pi \cdot K^{un} \subset K^{ab}$ because $K_\pi \cap K^{un} = K$ so that $Gal(K_\pi \cdot K^{un}|K) \cong Gal(K_\pi|K)| \times Gal(K^{un}|K)$ and hence is abelian. The other inclusion is much more difficult and we will prove it now. We begin with an analysis of the ramification groups of $K_{\pi,n}$.

Definition: If L/K is any finite Galois extension with Galois group G then we define the *ith* ramification group to be

$$G_i = \{\sigma \in G|\ v(\sigma(a) - a) \geq i + 1\ \forall a \in \mathcal{O}_K\}$$

where v denotes the normalized extension of the additive valuation on K to L. By normalized we mean that $v(L) = \mathbb{Z}$. Note that G_0 is simply the inertia group, i.e. those elements $\sigma \in G_0$ that act trivially on the residue field extension corresponding to L/K. From now onwards we will call the residue field of L, l and that of K, k. It's clear that we have $G_i \subset G_{i-1}$ and moreover that

$$G_i = \{\sigma \in G_0 | v(\sigma(\pi) - \pi) \geq i + 1\}$$

for some fixed prime element, π of L for all $\imath \geq 1$. This is saying that if $i \geq 1$ then to check if a field automorphism is in G_i it suffices to check two things: whether or not it is in G_0 and if it satisfies the condition for a single prime element of L instead on all of O_L. This is true because:

$$v(\sigma(u\pi) - u\pi) = v(\sigma(u)\sigma(\pi) - u\pi) = v((u + u'\pi)\sigma(\pi) - u\pi)$$

which is $v(\sigma(\pi) - \pi)$. So satisfying $v(\sigma(\pi) - \pi) \geq i + 1$ for a single prime element means it is true for all prime elements. From algebraic number theory we have that $G/G_0 \cong Gal(l|k)$. In what follows π, and Π will denote prime elements of K and L respectively. Consider the following

Lemma 5.1. Then there are injections $G_0/G_1 \to l^*$ and $G_i/G_{i+1} \to l$ $(i \geq 1)$ where the first map is given by $\sigma \mapsto \frac{\sigma(\Pi)}{\Pi} \mod \Pi$ and the second by $\sigma \mapsto \frac{\sigma(\Pi)-\Pi}{\Pi^{i+1}} \mod \Pi$.

Proof: First we need to see the maps are well defined i.e. that if $\sigma \in G_1$ then $\frac{\sigma(\Pi)}{\Pi} \equiv 1$ in l^* but since Π^2 divides $\sigma(\Pi) - \Pi$. Similarly if $\sigma \in G_{i+1}$ then $\frac{\sigma(\Pi)}{\Pi^{i+1}} \equiv \frac{\Pi}{\Pi^{i+1}}$ because $\sigma(\Pi) - \Pi$ is divisible by Π^{i+2}. That the first map is a homomorphism follows since we have:

$$\frac{\sigma \circ \tau(\Pi)}{\Pi} = \frac{\sigma \circ \tau(\Pi)}{\Pi} \cdot \frac{\tau(\Pi)}{\tau(\Pi)} = \frac{\sigma(\tau(\Pi)}{\tau(\Pi)} \cdot \frac{\tau(\Pi)}{\Pi}$$

and the first term is simply $\frac{\sigma(\Pi}{)}\Pi$ because $\tau(\Pi) = u\Pi$ for some $u \in \mathcal{O}_L^*$ and σG_0 acts trivially on u modulo Π.

That the second map is a homomorphism is similar:

$$\sigma \circ \tau \mapsto \frac{\sigma(\tau(\Pi)) - \Pi}{\Pi^{i+1}} = \frac{\sigma(\tau(\Pi)) - \tau(\Pi) + \tau(\Pi) - \Pi}{\Pi^{i+1}}$$

which is equal to the sum of the images of σ and τ since $\frac{\tau(\Pi)}{\Pi} = 1 \mod (\Pi)$. ♣
Recall that $|k| = q$. From this we obtain two facts, namely that $|G_0 : G_1|$ divides $q-1$ and for $i \geq 1$ $|G_i : G_{i-1}|$ divides q. One can also see that for a sufficiently large i, G_i will be the one element group. This follows from the finiteness of G_0: we simply choose a prime element Π of L and note that a nonidentity element $\sigma \in G_0$ cannot fix some prime element Π. If it did then it would fix every unit as well and hence all of O_L and L. Thus for each $\sigma \in G_0$ there is a n_σ such that $\sigma(\Pi) - \Pi$ is not in $(\Pi)^{n_\sigma}$. If i denotes the largest of the n_σ plus one, then it is easy to see that $G_i = \{1\}$.

To better understand the ramification groups of $K_{\pi,n}$ it will help to discuss the well understood unit groups of $\mathcal{O}_K$ then to show that, under a certain isomorphism, the two objects are related.

Definition 5.2. Let π be a prime element of $\mathcal{O}_K$ then set $U^{(0)} = \mathcal{O}_K^*$ and for all $i \geq 1$ put $U^{(i)} = 1 + (\pi)^i$. $U^{(i)}$ is called the ith unit group of $\mathcal{O}_K$.

We have a filtration:

$$0 = U^{(n)}/U^{(n)} \subset U^{(n-1)}/U^{(n)} \subset .... \subset U^{(0)}/U^{(n)}$$

Remarks: Recall in the previous chapter that we proved $K_{\pi,n}$ was an $\mathcal{O}_K$ module isomorphic to $\mathcal{O}_K/(\pi^n)$. Moreover we showed that because the Galois group $Gal(K_{pi,n}/K)$ induced $\mathcal{O}_K$-module isomorphisms that it could be embedded into

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

Then using order considerations we proved that this map actually yields the isomorphism

$$Aut_{\mathcal{O}_K}(\mathcal{O}_K/(\pi)^n) = (\mathcal{O}_K/(\pi)^n)^* \cong Gal(K_{\pi,n}/K).$$

Note that we also have the map $\mathcal{O}_K^*/U^{(n)} \to Aut_{\mathcal{O}_K}(\mathcal{O}_K/(\pi)^n) \subset End_{\mathcal{O}_K}(\mathcal{O}_K/(\pi)^n)$ sending $u \mapsto [a \mapsto ua]$. It is easy to see that this is in fact a well defined map of groups. That it is injective is not difficult either: $u \in \mathcal{O}_K$ will fix $\mathcal{O}_K/(\pi)^n$ if and only if we have $u \cdot 1 - 1 \equiv 0$ or when $u - 1 \in (\pi^n)$ i.e. $u \in U^{(n)}$. This means we have an injective map $\mathcal{O}_K^*/U^{(n)} \to Aut_{\mathcal{O}_K}(\mathcal{O}_K/(\pi)^n) \cong Gal(K_{\pi,n}/K)$ but a quick glance at the $U^{(i)}$ show that they both have the same order. Thus we get

$$\mathcal{O}_K^*/U^{(n)} \cong Aut_{\mathcal{O}_K}(\mathcal{O}_K/(\pi)^n) \cong Gal(K_{\pi,n}/K)$$

Now we can state the precise relationship between the unit groups of K^* and the ramification groups of $K_{\pi,n}$.

Proposition 5.3. Under the above isomorphism $\mathcal{O}_K^*/U^{(n)} \cong G_{K_{\pi,n}|K}$ the restriction to $U^{(i)}/U^{(n)}$ induces the isomorphisms $U^{(i)}/U^{(n)} \cong G_{q^i-1}$.

Proof: As in the previous chapter, for simplicity we choose $f(X) = X^q + \pi X \in \mathcal{F}_\pi$. Since $K_{\pi,n}$ is totally ramified the Galois action fixes every element in $l = k$, thus

$G_0 = G$. The isomorphism above can be rewritten as $U^{(0)}/U^{(n)} \cong G_0$. Now we work with the case when $i \geq 1$ and suppose $u \in U^{(i)} - U^{(i+1)}$ so that $u = 1 + v\pi^i$ where v is a unit in $\mathcal{O}_K$. Recall that we constructed a sequence of fields

$$K \subset K[a_1] \subset K[a_2] \subset ... \subset K[a_n] = K_{\pi,n}$$

where a_1 is a root of f, a_2 a root of $f - a_2$ and in general a_i a root of $f - a_{i-1}$. In this way a_i is a root of $f^{(i)}$ and $f(a_i) = a_{i-1}$. Thus for $u = 1 + v\pi^i$ we have

$$u \cdot a_n = [u]_{f,f}(a_n) = [1 + v\pi^i]_{f,f}(a_n) = [1]_{f,f}(a_n) + [v] \circ [\pi]^i_{f,f}(a_n)$$

which is

$$a_n + [v]_{f,f}(f^{(i)}(a_n))) = a_n + [v]_{f,f}(a_{n-i})$$

but

$$[v](a_{n-i}) = v(a_{n-i}) + v_2(a_{n-i})^2 + v_3(a_{n-i})^3 + ... = a_{n-i}(v + v_2(a_{n-i}) + v_3(a_{n-i})^2 + ...)$$

where the term in brackets is a unit since $v \in \mathcal{O}_K$ is. In other words $[u]_{f,f}(a_n) = a_n + v'a_{n-i}$ for some unit $v' \in \mathcal{O}_K^*$. We also have:

$$a_i = f(a_{i+1}) = \pi(a_{i+1}) + a_{i+1}^q = a_{i+1}^q(\frac{\pi}{a_{i+1}^{q-1}} + 1) = a_{i+1}^q(v'')$$

where v'' is a unit since $\frac{\pi}{a_{i+1}^{q-1}}$ has absolute value strictly less than one. In other words the valuation of π is strictly larger than that of a_{i+1}^{q-1} since $i \geq 1$ and $v(\pi) = q^{i-1}(q-1)v(a_i)$ where v is the valuation on K extended to $K_{\pi,n}$. Thus we see that $a_{n-i} = a_{n-i+1}v''' = a_{n-i+2}^q v'''' \cdot v''' = ... = a_n^{q^i} v_0$ where v_0 is some unit in $\mathcal{O}_{K_{\pi,n}}$. We've shown that

$$u \cdot a_n - a_n = [u]_{f,f}(a_n) - a_n = a_n^{q^i} v_0'$$

for some unit v_0 so $[u]_{f,f} \in G_{q^i-1}$ but is not in G_{q^i}. Let $\sigma \in G_{q-1}$ be the image of some $u \in U^{(0)}/U^{(n)}$ then we know $ord_L(\sigma(\Pi) - \Pi) \geq q$. In other words $[u]_{f,f}(\Pi) - \Pi = u\Pi + (\Sigma_{i=2}^{\infty} u_i \Pi^i) - \Pi = 0 = u\Pi - \Pi \mod (\Pi)^2$ so that $u - 1 = k\Pi \in (\Pi) = m_L$ but $u - 1 \in \mathcal{O}_K$ as well so $u - 1 \in m_K$ i.e. $u \in U^{(1)}$. So far we've shown that $U^{(1)}$ maps onto G_{q-1} and that $U^{(0)}$ maps onto G_0. The discussion above shows that for $i \geq 1$ if $x \in U^{(i)} - U^{(i+1)}$ then its image lies in G_{q^i-1} but not in G_{q^i}. So let $\sigma \in G_{q^2-1}$ then we know it is the image of some $u \in U^{(1)}$, if u isn't in $U^{(2)}$ then its image lies in G_{q-1} but not in G_q. However this is impossible since its image is in $G_{q^2-1} \subset G_q$. This means $u \in U^{(2)}$ and that it maps onto G_{q^2-1}. The exact same proof works for the rest of the i. ♣

Corollary 5.4. : Consider the extension $K_{\pi,n}$ of K, then a complete list of distinct ramification groups are as follows:

$$G_0 = G$$
$$G_{q-1} = G_{q-2} = ... = G_1$$
$$G_{q^2-1} = G_{q^2-2} = ... = G_q$$
$$\vdots$$
$$G_{q^n-1} = \{1\}$$

Proof: In each of the rows above we have a line of inclusions like

$$G_{q-1} \subset G_{q-2} \subset ... \subset G_1$$

Let $x \in G_1$ so that it is the image of some $u \in U^{(0)}$ where $[u]_{f,f}(\Pi) - \Pi \equiv 0 \mod (\Pi)^2$. But $[u]_{f,f}(\Pi) - \Pi = u\Pi + (\Sigma_{i=2}^{\infty} u_i \Pi^i) - \Pi \equiv u\Pi - \Pi \mod (\Pi)^2$ so that $u\Pi - \Pi = k\Pi^2$ or $u - 1 = k\Pi \in m_L \cap \mathcal{O}_K = m_K$ because $u - 1 \in K$. This implies $u \in U^{(1)}$ but we know from above that $U^{(1)}$ maps onto G_{q-1} so that $x \in G_{q-1}$ and the inclusions above all become equalities. Now let $\sigma \in G_q$ then since $G_q \subset G_{q-1}$ and $U^{(1)}$ maps onto the latter we know there is a $u \in U^{(1)}$ such that $u \mapsto \sigma$. Moreover if $u \in U^{(1)} - U^{(2)}$ then the proof of the above theorem shows that $u \mapsto \sigma \in G_{q-1} - G_q$ but this is contrary to our assumption that $\sigma \in G_q$, therefore $u \in U^{(2)}$. However, the above theorem tells us that $U^{(2)}$ maps onto G_{q^2-1} so that $\sigma \in G_{q^2-1}$ i.e. $G_q \subset G_{q^2-1}$ and we have the equalities:

$$G_{q^2-1} = G_{q^2-2} = ... = G_q$$

The remaining $i < n$ are proved in the exact same way. The fact that G_{q^n-1} is the trivial group follows because we know by the previous theorem that the trivial group $U^{(n)}/U^{(n)}$ maps onto it. ♣

Corollary 5.5. Consider the extension $K_{\pi,n}$ of K, then for each $i \geq 0$ we have

$$U^{(i)}/U^{(i+1)} \cong G_{q^i-1}/G_{q^i}$$

In particular $|G_0 : G_1| = q - 1$ and $|G_{q^i-1} : G_{q^i}| = q$ for $i \geq 1$.

Proof: We have the surjective map $U^{(0)}/U^{(n)} \to G_0 \to G_0/G_1$ and by the proof of the theorem above we know the kernel is exactly $U^{(1)}/U^{(n)}$. Similarly for each $i \geq 1$ we have the surjective map $U^{(i)}/U^{(n)} \to G_{q^i-1} \to G_{q^i-1}/G_{q^i}$ and by the calculation in the proof of the theorem above we see that the kernel is exactly $U^{(i+1)}$. The result follows. ♣

We now define a so-called upper numbering on ramification groups since they will be convenient when passing to quotients.

Definition 5.6. Let L be a finite Galois extension of a local field K with Galois group G. We extend the definition of a ramification group to any real number $r \geq -1$ we extend the definition of a ramification group to

$$G_r = G_i$$

where i is the least integer greater than or equal to r. Let $\varphi : \mathbb{R}_{\geq 0} \to \mathbb{R}$ be the unique continuous piecewise function with $\varphi(0) = 0$ and $\varphi'(u) = \frac{1}{|G_0 : G_u|}$, φ is called the Hasse-Herbrand function of the extension L/K. Finally, we define $G^v = G_u$ when $\varphi(u) = v$. We shall call these groups the upper ramification groups. It is useful to note that φ is strictly increasing and continuous and therefore a homeomorphism from $[0, \infty)$ to itself. This forces the existence of an inverse which we denote ψ.

Example 5.7. It turns out that the knowledge of the upper ramification groups is equivalent to that of the lower ramification groups. The example we need is that of $K_{\pi,n}$, we know by the previous result that $|G_0 : G_1| = q - 1$ and $G_1 = ... = G_{q-1}$ so since $\varphi(0) = 0$ we see that $\varphi'(u) = \frac{1}{q-1}$ for $0 < u < q - 1$. This tells us that the graph of φ on $(0, q - 1)$ is the line connecting $(0, 0)$ to $(q - 1, 1)$. By definition of the upper numbering we see that $G^1 = G_{q-1}$. On the interval $(q - 1, q^2 - 1)$ we know that $\varphi'(u) = \frac{1}{|G_0:G_u|} = \frac{1}{|G_0:G_{q^2-1}|}$ because $G_q = ... = G_{q^2-1}$, and we know this value is simply $\frac{1}{|G_0:G_1||G_1:G_q|} = \frac{1}{q(q-1)}$. A simple calculation shows that the graph of φ on the interval $(q - 1, q^2 - 1)$ is the line segment connecting $(q - 1, 1)$ and $(q^2 - 1, 2)$. It is not difficult to see that if we go on in this manner that the graph of φ on $(q^i - 1, q^{i+1} - 1)$ is the line segment connecting $(q^i - 1, i)$ to $(q^{i+1} - 1, i + 1)$. In this way we see that $G^i = G_{q^i-1}$ for all i. Thus for $K_{\pi,n}$ we have that $|G^i : G^{i+1}|$ is equal to q or $q - 1$ and that G^n is the trivial group. Note that the G^i's encode all the information given by the G_{q^i-1}.

We now come to an important but highly technical theorem that will allow us to define the upper ramification groups of infinite extensions. The proof will follow the exposition given in [6] but we'll simplify it somewhat by supposing all extensions involved are abelian and totally ramified since this is the only case with which we are concerned.

Theorem 5.8. Consider the abelian totally ramified Galois extensions $K \subset L \subset M$ with $G = Gal(M/K)$ and $Gal(M/L) = H \triangleleft G$ so that we have $G/H \cong Gal(L/K)$. Then the ramification group of G/H (with the upper numbering) is equal to the image of the upper ramification group of G. More precisely for any v we have $(G/H)^v = G^v H/H$.

The proof will proceed in steps, it will be convenient to introduce the following:

Definition 5.9. : Let L/K be an extension of local fields with Galois group G and Π a prime element of L then define $i_G : G \to \mathbb{R}$ to be $\sigma \mapsto v_L(\sigma(\Pi) - \Pi)$ where v_L here is the normalized extension of v_K so that $v_L(L) = \mathbb{Z}$.

Now suppose that all our extensions are totally ramified and abelian. We have $i_G(\sigma) \geq i + 1$ exactly when $\sigma \in G_i$. Moreover $i_G(\sigma\tau) \geq min(i_G(\sigma), i_G(\tau))$. To see this last fact suppose that $i_G(\sigma) = k \geq l = i_G(\tau)$ so that Π^k divides $\sigma(\tau^{-1}(\Pi)) - \tau^{-1}(\pi)$ so that it must also divide $\tau(\sigma(\tau^{-1}(\Pi)) - \tau(\Pi)) = \tau\sigma(\tau^{-1}(\Pi)) - \Pi$ so Π^l divides it as well. But Π^l divides $\Pi - \tau(\Pi)$ and so it divides their sum as well. There sum is $\tau\sigma(\tau^{-1}(\Pi) - \tau^{-1}(\Pi)$, this means $i_G(\tau\sigma) \geq l$ as desired. Note that this proof shows we have $i_G(\sigma\tau) = min(i_G(\sigma), i_G(\tau))$ if $l < k$. The next two propositions describe how the function i_G behaves when restricted to subgroups or passing to quotients.

Proposition 5.10. If $H \triangleleft G = Gal(L/K)$ with K' the fixed field of H then for every $\sigma \in H$ we have $i_G(\sigma) = i_H(\sigma)$.

Proof: This follows trivially since the valuation of K extends uniquely to K' and so the valuation of K' extended (and normalized) to L is exactly the normalization of

the extension of the original valuation on K. Thus for $\sigma \in H$: $ord_L(\sigma(\Pi) - \Pi) = j+1$ exactly when $\sigma \in H_j$ or $\sigma \in G_j$, in other words $G_j \cap H = H_j$. ♣

Proposition 5.11. If $H \triangleleft G = Gal(L/K)$ with K' the fixed field of H then for every $\sigma \in G/H = Gal(K'/K)$ we have

$$i_{G/H}(\sigma) = \frac{1}{|L:K|}\Sigma_{\tau \mapsto \sigma} i_G(\tau)$$

where τ runs through the possible coset representatives of σ in G.

Proof: Note that here $|L : K'| = e$ is the ramification index since our extensions are all totally ramified. If σ is the identity of G then we know that both sides equal $v_L(0) = v'_K(0) = \infty$ so we suppose $\sigma \neq 1$. Let Π_L and $\Pi_{K'}$ denote prime elements of L and K' respectively. Then because our valuations are all normalized we see that $i_{G/H}(\sigma)|L : K'| = v_L(\sigma(\Pi_{K'}) - \Pi_{K'})$ and $i_G(\tau) = v_L(\tau(\Pi_L) - \Pi_L)$. Fixing some representative $\tau \in G$ representing the coset corresponding to σ we know all others will be of the form τh for $h \in H$. Thus it suffices to show that the two elements

$$a = \tau(\Pi_{K'}) - \Pi_{K'}$$

and

$$b = \Pi_{h \in H}(\tau h(\Pi_L) - \Pi_L)$$

generate the same ideal in $\mathcal{O}_L$ since that would mean they have the same valuation v_L and then using the fact that the valuation is a homomorphism to $\mathbb{Z}$ we would get

$$\sigma = \frac{1}{|L:K'|} i_{G/H} \sum_{\tau \mapsto \sigma} i_G(\tau)$$

as desired.

Now let $f \in \mathcal{O}_{K'}[X]$ be the minimal polynomial for Π_L over K. Then we have $f = \Pi_{h \in H}(X - h(\Pi_L))$ and if we apply τ to its coefficients we get $\tau(f) = \Pi_{h \in H}(X - \tau h(\Pi_L)$. Now because $\mathcal{O}_K[\Pi_{K'}] = \mathcal{O}_{K'}$ its clear that $a = \tau(\Pi_{K'}) - \Pi_{K'}$ divides the coefficients of $\tau(f) - f$. To see this write $\sum a_i X^i = f(X)$ and note that $a_i = \sum b_i \Pi_{K'}$ where $b_i \in \mathcal{O}_K$. Then $\tau(a_i) - a_i = \sum b_j(\tau(\Pi_{K'})^j - \Pi^j_{K'})$ which is easily seen to be divisible by $(\tau(\Pi_{K'}) - \Pi_{K'}) = a$. However, this means $b = \tau(f)(\Pi_L) - f(\Pi_L)$ is divisible by a. Now we need to show that b divides a. Using the fact that $\mathcal{O}_L/\mathcal{O}_{K'}$ is monogenic we can write $\Pi_{K'}$ as a polynomial in Π_L over K, i.e. $g(\Pi_L) = \Pi_{K'}$ with $g(X) \in \mathcal{O}_K$. Then $g(X) - \Pi_{K'}$ has Π_L as a root and is therefore divisible by its minimal polynomial, f: $g(X) - \Pi_{K'} = f(X)h(X)$. Then applying τ to both sides of this equation we get

$$g(X) - \tau(\Pi_{K'}) = \tau(f)(X)\tau(h(X))$$

and substituting Π_L yields

$$\Pi_{K'} - \tau(\Pi_{K'}) = \tau(f)(\Pi_L)\tau h(\Pi_L) = b\tau(h(\Pi_L))$$

showing that b divides a. ♣

Lemma 5.12. We have $\varphi(u) = -1 + \frac{1}{|G_0|}\sum_{s\in G}\min(i_G(s), u+1)$

Proof: It's easy to see that the right hand side is a piecewise linear continuous function. It also vanishes at zero because all the summands are zero when $s \in G - G_0$ and is 1 at each $s \in G_0$. This is because at those elements $i_G(s) \geq 1$ and $u + 1 = 1$ so their minimum is 1 and at elements not in G_0 we know $ord_L(s(\Pi) - \Pi) = 0$. If we let m be an integer then for $m < u < m + 1$ we see that the sum on the right simplifies into two parts: a constant part for each group element not in G_{m+1} and a linear term in u for each group element in G_{m+1}. This means the derivative of the right hand side is $\frac{1}{|G_0:G_{m+1}|}$. Since this is the derivative of φ at such u as well we see that they must actually be same functions. ♣

Lemma 5.13. Choose $\sigma \in G/H$ and let $j(\sigma)$ denote the upper bound of the integers $i_G(s)$ for any s in the preimage of σ in the natural map $G \to G/H$. Then

$$i_{G/H}(\sigma) - 1 = \varphi_{L/K'}(j(\sigma) - 1)$$

Proof: : Let $s \in G$ be an element that represents the coset σ with the property that $j(\sigma) = i_G(s) = m$. We know the other preimages of σ are of the form sh for $h \in H$. Suppose that $h \in H_{m-1}$, then $i_G(h) \geq m$ so that $i_G(sh) \geq m$ and therefore equal to it since m is the maximum value it can attain. If h isn't in H_{m-1} then $i_G(h) < m$ and therefore $i_G(sh) = i_G(h)$ so that we have $i_G(sh) = \min(i_G(h), m)$ then applying lemma 5.12 we get

$$i_{G/H}(\sigma) = \frac{1}{e_{L/K'}}\sum_{h\in H}\min(i_G(h), m)$$

Recall that $i_G(h) = i_H(h)$ and that our extensions are totally ramified so that $e_{L/K'} = |H_0| = |H| = |L : K'|$. Now apply the last lemma to the extension L/K' to get

$$\varphi(m-1) = -1 + \frac{1}{|H_0|}\sum_{h\in H}\min(i_H(s), m) = i_{G/H}(\sigma) - 1$$

as desired. ♣

Lemma 5.14. Let φ be as above then $G_uH/H = (G/H)_{\varphi_{L/K'}(u)}$

Proof: If $\sigma \in G_uH/H$ then this means its the image of some $\tau \in G_u$ i.e. that $j(\sigma) - 1 \geq u$. Now since $\varphi_{L/K'}$ is a strictly increasing function this is equivalent to $\varphi_{L/K'}(j(\sigma) - 1) \geq \varphi_{L/K'}(u)$ but by the previous lemma this implies $i_{G/H}(\sigma) - 1 \geq \varphi_{L/K'}(u)$ which means $\sigma \in (G/H)_{\varphi_{L/K'}(u)}$. The implications just stated are reversible and therefore equality holds. ♣

Lemma 5.15. Let ψ be the inverse of φ, then both functions satisfy the following transitivity relations for a tower of extensions $K \subset K' \subset L$

$$\varphi_{L/K} = \varphi_{K'/K} \circ \varphi_{L/K'}$$

and

$$\psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}$$

Proof: We begin with with the first assertion: it is clear that both sides vanish at 0 and are both piecewise linear continuous functions therefore it remains to show they have the same derivative everywhere if the derivative exists. Suppose $u > -1$ is not an integer then using the chain rule the derivative of the composition $\varphi_{K'/K} \circ \varphi_{L/K'}$ is simply

$$\varphi'_{K'/K}(\varphi_{L/K'}(u)) \cdot \varphi'_{L/K'}(u)$$

And we know from the proof of lemma 5.12 that these derivatives are related to the cardinalities of certain ramification groups, more precisely, the above is equal to

$$\frac{|(G/H)_{\varphi_{L/K'}(u)}|}{|G/H|} \cdot \frac{|H_u|}{|H|}$$

Referring to the previous lemma its easy to see this quantity is equal to $\frac{|G_u|}{|L:K|}$ since our extensions are totally ramified. But this is exactly equal to the derivative of φ at u. The transitivity formula for the inverse ψ now follows easily. ♣

We are finally in a position to prove theorem 5.8. It will allow us to define ramification groups for the infinite extensions K_π, and more generally, totally ramified abelian extensions L/K.

Proof: (of Theorem 5.8) By definition we have $(G/H)^v = (G/H)_u$ with $u = \psi_{K'/K}(v)$ and by lemma 5.14 we know that $(G/H)_u = G_w H/H$ where $w = \psi_{L/K'}(u) = \psi_{L/K'} \circ \psi_{K'/K}(v) = \psi_{L/K}(v)$ by the transitivity above. Thus $G_w = G^v$ and we have $(G/H)^v = G^v H/H$ and the theorem holds. ♣

The above theorem will allow us to define ramification groups (via an upper numbering) of infinite totally ramified abelian extensions by doing so at each finite step. More precisely,

Definition 5.16. Let L be the totally ramified infinite extension defined in the previous sections and suppose that $G = Gal(L/K)$. Then define G^v to be the set of elements σ whose image is in $(G/H)^v$ for every open normal subgroup H of G. By infinite Galois theory this is equivalent to saying that σ is in $Gal(L'/K)^v$ for every finite Galois subextension L' of L/K

Recall the description above of the the upper ramification groups of $K_{\pi,n}$: $G^i = G_{q^i-1}$ and as such $|G^i : G^{i+1}|$ is equal to either q or $q-1$. Recall that for an arbitrary finite Galois extension L/K we had the injections $G_0/G_1 \hookrightarrow l^*$ and $G_i/G_{i+1} \hookrightarrow l$ for $i \geq 1$: this tells us that $|G_0 : G_1||q-1$ and $|G_i : G_{i+1}||q$, and in particular that $|G_0 : G_1| \leq q-1$ and $|G_i : G_{i+1}| \leq q$. We will now need a result that we shall not prove as its proof is highly technical and outside the framework of the paper.

Theorem 5.17. (Hasse-Arf) If L/K is abelian and if the G_u, $u \in \mathbb{R}$ stand for the ramification groups of $Gal(L/K)$ then whenever $G_u \neq G_{u+1}$, $\varphi(u)$ must be an integer.

Proof: [6] Chapter 5, Section 7. ♣

Corollary 5.18. Let L/K be any abelian extension with Galois group G. Then there is a subsequence of the natural numbers $\{i_j\}_{j\in\mathbb{Z}}$ such that

$$\cdots G^{i_l} \subsetneq G^{i_{l-1}} \subsetneq \cdots G^{i_2} \subsetneq G^{i_1} \subsetneq G^{i_0}$$

form a complete list of distinct upper ramification groups. Also $|G^{i_k} : G^{i_{j+1}}|$ divides q or $q-1$ and $G^n = \{1\}$ for some $n \in \mathbb{Z}$.

Proof: For the first statement let

$$G_0 = ... = G_{j_0} \neq G_{j_0+1} = ...G_{j_1} \neq G_{j_1+1} = ... =$$

be a complete list of the distinct ramification groups with the jumps occuring at the subsequence $\{j_k\}_{k\in\mathbb{N}}$. Then by the Hasse-Arf theorem $\varphi(j_k) = i_k \in \mathbb{Z}$ and so

$$G^{i_0} \supsetneq G^{i_1} \supsetneq G^{i_2} \supsetneq G^{i_3} \supsetneq ...$$

forms a complete list of distinct upper ramification groups. Note that $|G^{i_k} : G^{i_{j+1}}| = |G_{j_k} : G_{j_k+1}|$ and by the remark above we know this divides either q or $q-1$. Similarly since G_n is the trivial group for a large enough n by definition $G^{\varphi(n)}$ will be too, choosing the n so that it is the smallest integer with this property guarantees, by the Hasse-Arf theorem, that $\varphi(n) \in \mathbb{Z}$. ♣

Now consider the case when our totally ramified abelian extension, K'/K, is infinite. Let G be the Galois group this infinite extension. For convenience shorten $Gal(L/K) = G_{L/K}$. Then, consider $G^{i_j}/G^{i_{j+1}}$. It is easy to see this is simply the inverse limit of the groups $G^{i_j}_{L/K}/G^{i_{j+1}}_{L/K}$ as L/K varies over the finite Galois subextensions L/K. Since K'/K is totally ramified they have the same residue fields. By the remark above this says that each group in the limit divides $q = |k|$ or $q-1$ (q if $j \geq 1$ and $q-1$ otherwise) so the maximum cardinality must be attained at some finite level, say at L/K. But then for all $L'/L/K$ the natural projections $G^{i_j}_{L'/K}/G^{i_{j+1}}_{L'/K} \to G^{i_j}_{L/K}/G^{i_{j+1}}_{L/K}$ must be isomorphisms, being surjective maps between two groups of the same cardinality. Thus the inverse limit will simply be $G^{i_j}_{L/K}/G^{i_{j+1}}_{L/K}$ and so we see that the above statement applies to infinite extensions as well i.e. that $|G^{i_j} : G_{i_{j+1}}| \leq q$. Now suppose that $\sigma \in G^n$ for every natural number n and pick any open normal subgroup $N \triangleleft G$. Then by the previous corollary there exists an n_N such that $(G/N)^{n_N} = \{1\}$ but $\sigma \in G^{n_N}$ so $\sigma|_{K'^N} = 1$ i.e. $\sigma \mapsto \sigma_{|_{K'^N}} \in N$ under the natural map $G \to G/N$. Since N was an arbitrary open normal subgroup and $\bigcap N = \{1\}$ is the trivial subgroup of G we get that σ is the identity of G. We have shown that $\bigcap_{n\in\mathbb{N}} G^n = \{1\}$.
We can finally proceed with a few lemmas which will culminate in main theorem of this chapter.

Theorem 5.19. Let π be a prime element of K and suppose K_π is the corresponding Lubin-Tate extension, then

$$K^{un} \cdot K_\pi = K^{ab}$$

Lemma 5.20. Let L be any abelian totally ramified extension containing K_π, then $L = K_\pi$ i.e. the Lubin-tate extension is a maximal totally ramified extension.

Proof: Put $G = Gal(L/K)$, $H = Gal(L/K_\pi)$ so that $G/H = Gal(K_\pi/K)$. Consider the following commutative diagram of abelian groups:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G^{n+1} \cap H & \longrightarrow & G^{n+1} & \longrightarrow & (G/H)^{n+1} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G^{n} \cap H & \longrightarrow & G^{n} & \longrightarrow & (G/H)^{n} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \frac{G^n \cap H}{G^{n+1} \cap H} & \longrightarrow & \frac{G^n}{G^{n+1}} & \longrightarrow & \frac{(G/H)^n}{(G/H)^{n+1}} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

It's clear that the columns are exact, that the first two rows are exact follows because of theorem 5.8 i.e. that $(G/H)^v = G^v H$. A diagram chasing argument easily shows that the third row must be exact. This tells us that

$$|G^n : G^{n+1}| = |(G/H)^n : (G/H)^{n+1}||G^n \cap H : G^{n+1} \cap H|$$

but the left hand side is less than q and $|(G/H)^n : (G/H)^{n+1}| = q$ or $q-1$. This tells us that $|G^n \cap H : G^{n+1} \cap H|$ must equal one i.e. $G^n \cap H = G^{n+1} \cap H$ for arbitrary n. But for $n = 0$ we have $G^0 = G_0 = G$ (because L is totally ramified) so

$$G^n \cap H = G^{n-1} \cap H = .. = G^0 \cap H = H$$

so $H \subset G^n$ for every n. Since $\bigcap G^n = \{1\}$ we see that H is trivial and by infinite Galois theory $L = K_\pi$. ♣

Lemma 5.21. Any finite unramified extension of K_π is contained in $K_\pi \cdot K^{un}$.

Proof: Suppose that L is some unramified extension of $K_\pi = \bigcup_{i=1}^{\infty} K_{\pi,n}$, then L is an unramified extension of $K_{\pi,n}$ for some n. Consider the Galois group G of $K_{\pi,n}L/K$, we know the fixed field of the inertia subgroup $G_0 \leq G$ is the maximal unramified extension contained in $K_{\pi,n}L$, call it L'. Its clear that $L'K_{\pi,n} \subset LK_{\pi,n}$ moreover that $L'K_{\pi,n}$ is an unramified extension of $K_{\pi,n}$. This follows because

$$|L'K_{\pi,n} : K_{\pi,n}| = |L' : K_{\pi,n} \cap L'| = |L' : K|$$

since $K_{\pi,n} \cap L' = K$ (since the only totally ramified unramified extension of K is K). Also the residue field of $L'K_{\pi,n}$ contains that of L' and the residue field of $K_{\pi,n}$ is the same as that of K. So the degree of the residue field extension corresponding to $L'K_{\pi,n}/K_{\pi,n}$ is at least the degree of the residue field extension corresponding to L'/K. But this latter extension is unramified so for it the degree of the residue field extension is $|L' : K| = |L'K_{\pi,n} : K_{\pi,n}|$. This means the degree of the residue field

extension of $L'K_{\pi,n}/K_{\pi,n}$ must equal $|L'K_{\pi,n} : K_{\pi,n}|$ since it is also bounded above by it (by Proposition 1.10). Its residue field extension is equal to that of $LK_{\pi,n}$. But since they are both unramified we see that they must be equal (Proposition 1.23). This shows that $LK_{\pi,n} \subset K^{un} \cdot K_\pi$ since K^{un} denotes the maximal unramified extension K i.e. the union of all unramified extensions of K. ♣

Lemma 5.22. Suppose that L is a finite abelian extension of K_π whose Galois group $Gal(L/K_\pi)$ has exponent m and let $(K_\pi)_m$ be the unramified extension of K_π of degree m. Then there is a totally ramified abelian extension L_t of K_π with the property that $L_t \cdot (K_\pi)_m = L \cdot (K_\pi)_m$. ♣

Proof: Note that for any $\sigma \in Gal(L(K_\pi)_m)$ we have that σ^m is the identity since by hypothesis its restriction to L is the identity and its restriction to (K_π) is simply $\sigma|^m_{(K_\pi)_m}$. This is the identity because the unramified extension of degree m of K_π has a cyclic Galois group of degree m which is obviously of exponent m. We've shown that $Gal(L(K_\pi)_m)$ is a group of exponent m. Let $\sigma \in Gal(L(K_\pi)_m)$ denote an element whose restriction to $(K_\pi)_m$ is the Frobenius automorphism. This element has order at least m (since the Frobenius does) and at most m since it is in a group of exponent n. Now consider the subgroup $\langle\sigma\rangle \leq Gal(L(K_\pi)_m)$. We have the homomorphism $|_{(K_\pi)_m} : Gal(L(K_\pi)_m) \to Gal((K_\pi)_m/K_\pi) =< \sigma$ so clearly $\langle\sigma\rangle$ is an image of the group $Gal(L(K_\pi)_m)$. The subgroup fixing $(K_\pi)_m$ is therefore a normal subgroup complimenting $\langle\sigma\rangle$ in G, call this subgroup H. Its clear that $\langle\sigma\rangle \cap H$ intersect trivially since no power of the Frobenius fixes $(K_\pi)_m$ unless it is the identity. Since $Gal(L(K_\pi)_m)$ is abelian (the composition of abelian extensions is abelian) we see that $\langle\sigma\rangle$ is normal too and that we can write $Gal(L(K_\pi)_m) \cong \langle\sigma\rangle \times H$. Put $L_t = L^{\langle\sigma\rangle}$, we will show L_t is totally ramified. If it wasn't then for some n which divides m there would be an unramified extension $(K_\pi)_n \subset L_t$. Its necessary that n divides m because $Gal(L_t/K_\pi)$ is of exponent m. By the 1-1 correspondence between residue field extensions and unramified extensions we see that $(K_\pi))_n) \subset (K_\pi)_m$. This implies $(K_\pi)_n \subset L_t \cap (K_\pi)_m$ and therefore is fixed by both $\langle\sigma\rangle$ and H so all of $Gal(L(K_\pi)_m)$. Galois theory now tells us that $(K_\pi)_n = K_\pi$ or that $n = 1$ and L_t is in fact totally ramified. Note that if an element $\tau \in Gal(L(K_\pi)_m)$ fixes $L_t(K_\pi)_m$ then it is in $H \cap \langle\sigma\rangle = \{1\}$ and therefore Galois theory says $L_t(K_\pi)_m = L(K_\pi)_m$ as desired. ♣

Proof: (that $K_\pi \cdot K^{un} = K^{ab}$): To show that $K^{ab} = K^{un} \cdot K_\pi$ we show that any finite abelian extension L of K is contained in $K^{un} \cdot K_\pi$. Consider the extension LK_π/K_π, it has a maximal unramified part, say $(K_\pi)_m$ and the Lemma above says that there is a totally ramified extension L_t of K_π with $L_t \cdot (K_\pi)_m = L \cdot (K_\pi)_m$. In particular $L \subset L_t \cdot (K_\pi)_m$. Now L^t/K is itself a totally ramified extension because it is a totally ramified extension of K_π, another totally ramified extension of K. To see this clearly just note that the residue fields of L_t, K_π and K must all be the same so that no nontrivial unramified extension can occur in L_t/K. Thus by lemma 5.20 we see that $L_t \subset K_\pi$ and lemma 5.21 tells us that $(K_\pi)_m \subset K_\pi \cdot K^{un}$. All in all we get that $L \subset L_t \cdot (K_\pi)_m \subset K_\pi \cdot K^{un}$ completing the proof. ♣

6 Norm Groups

Thus far we have constructed a $\phi : K^* \to Gal(K^{ab}|K)$ satisfying the first property of the Artin map, namely that $\phi(\pi)$ acts as the Frobenius automorphism on K^{un} for any prime element $\pi\ in K^*$. It remains to check that $\ker \phi|_L = N_{L/K}$ and that this induces an isomorphism

$$K^*/N_{L/K}(L^*) \cong Gal(L/K)$$

We begin by determining the norm groups of the $K_{\pi,n}$. From here onwards φ will denote the Frobenius.

Theorem 6.1. Consider the extension $K_{\pi,n}/K$, then its norm group, $N_{K_{\pi,n}/K}(K_{\pi,n}) = \pi^{\mathbb{Z}} \cdot (1 + (\pi)^n)$ where $\pi^{\mathbb{Z}}$ denotes the cyclic subgroup of K^* generated by π, and, as usual, (π) is the maximal ideal in $\mathcal{O}_K$.

This is a nontrivial proof and before we can attack it we will need some preliminary results. The first is adapted from [1] and [5].

Proposition 6.2. If $\pi' = u\pi$ are two prime elements of K^* with $u \in 1 + (\pi)^n$ then $K_{\pi',n} = K_{\pi,n}$.

Proof: We shall proceed in steps. Step one will be to show that there exists a unit $\mu \in \mathcal{O}_{\bar{K}}$ with $\frac{\mu^\varphi}{\mu} = u$. By hypothesis we have $u = 1 + \pi^n a$ for some $a \in \mathcal{O}_{K_{\pi,n}}$ and we are looking for a $\mu = 1 + \pi^n b$ for some algebraic integer b. We will proceed inductively by showing the equation

$$\frac{\mu^\varphi}{\mu} = \frac{1 + (\pi^n b)^\varphi}{1 + \pi^n b}$$

can be solved modulo π^{n+1} for some b. We know that

$$\frac{1}{1 + \pi^n b} = 1 - \pi^n b + (\pi^n b)^2 + ...$$

since $\mod \pi^k$ for all $k \geq 0$ they are the same. Note then that modulo π^{n+1} combining the two equations yields

$$\frac{\mu^\varphi}{\mu} \equiv 1 + (\pi^n b)^\varphi - \pi^n b \mod \pi^{n+1}$$

and we want this to equal $u = 1 + \pi^n a$ i.e. $(\pi^n b)^\varphi - \pi^n b \equiv u - 1 = \pi^n a \mod \pi^{n+1}$. Putting $w = \frac{\pi^{n\varphi}}{\pi^n}$ and dividing out by π^n this amounts to finding a b satisfying the equation $wb^\varphi - b + a$ modulo (π). Note however that modulo (π) the Frobenius acts as taking the q-th power where, as usual, q denotes the order of the base residue field so we need b to be a root of the polynomial $wx^q - x + a$ modulo (π). Since w is a unit its roots will be algebraic integers, so we can find a b modulo (π) satisfying this equation. If we continue in this way we can find what b should be modulo π^2, then modulo π^3 and so on. By induction there is an algebraic integer μ with the desired property.

We will now construct a homomorphism $\rho : F_f \to F_{f'}$ where $f' \in \mathcal{F}_{\pi'}$, $f \in \mathcal{F}_\pi$ with $\rho \in \bar{K}[[X]]$. We want ρ to be μX modulo degree 2 terms and to have the property that $f' \circ \rho = \rho^\varphi \circ f$ where φ is the Frobenius automorphism. Here ρ^φ is the power series obtained by applying φ to the coefficients of ρ, here we can extend φ to all of $\bar{K}$ so that it acts trivially on K_π. This can be done because $K_\pi \cap K^{un} = K$. To obtain such a power series ρ we appeal to a Lemma that will follow. Note that any such power series will be unique. To check that ρ as defined is a homomorphism $F_f \to F_{f'}$ we will make use of the uniqueness statement in the Lemma to follow. To use the uniqueness note that $\rho \circ F_f \equiv F_{f'} \circ \rho = \mu(X+Y)$ modulo degree two terms and the following two facts

$$f' \circ (\rho \circ F_f) = \rho^\varphi \circ f \circ F_f = \rho^\varphi \circ F_f^\varphi \circ f = (\rho \circ F_f)^\varphi \circ f$$

since $F_f \in \mathcal{O}_K$ and so $F_f^\varphi = F_f$. Also that

$$f' \circ (F_{f'} \circ \rho) = F_{f'}^\varphi \circ f' \circ \rho = F_{f'}^\varphi \circ \rho^\varphi \circ f' = (F_{f'} \circ \rho)^\varphi \circ f'$$

so that uniqueness applies to get $\rho \circ F_f = F_{f'} \circ \rho$. This means that ρ induces a group homomorphism $m_{\bar{K},n}^f \to m_{\bar{K},n}^{f'}$, that it is an isomorphism follows since the coefficient of its degree one term, μ, is a unit. Thus given $a' \in m_{\bar{K},n}^{f'}$ there exists a $a \in m_{\bar{K},n}^f$ with $\rho(a) = a'$. Recall that $[\pi']_{f',f'} = f'$ so we have

$$\rho \circ [u]_{f,f} \circ [\pi]_{f,f} = \rho \circ [\pi']_{f,f} = [\pi']_{f',f'} \circ \rho = f' \circ \rho = \rho^\varphi \circ f = \rho^\varphi \circ [\pi]_{f,f}$$

because ρ is a $\mathcal{O}_K$-module homomorphism from $F_f \to F_{f'}$. An easy induction argument shows that this implies the coefficients of $\rho \circ [u]_{f,f}$ are equal to that of ρ^φ i.e that they are the same. This implies that $\rho^\varphi(a) = \rho([u]_{f,f}(a)) = \rho(a)$. This is because $[u]_{f,f}$ acts trivially on $a \in m_{\bar{K},n}^f$: since $u \in 1+(\pi)^n$ and we have $Aut(m_{\bar{K},n}^f) \cong \mathcal{O}_K^*/(1+(\pi)^n)$. Recall that φ acts trivially on K_π now we denote $\varphi_{K^{un}.K_{\pi,n}} = \sigma$. Alternatively we can define σ to be the unique extension of the Frobenius to $K^{un} \cdot K_{\pi,n}$ that acts as the identity on $K_{\pi,n}$. This means the fixed set of the subgroup generated by σ is exactly $K_{\pi,n}$, now because $a \in m_{\bar{K},n}^f$ is fixed by the Frobenius. We see that $\rho^\varphi(a) = (\rho(a))^\sigma = \rho(a)$, in other words $\rho(a) = a'$ is fixed by σ thereby implying that $m_{\bar{K},n}^{f'} \subset K_{\pi,n}$. This shows $K_{\pi',n} \subset K_{\pi,n}$ and since they have the same degrees they must be equal. ♣

Lemma 6.3. Let π and π' be two prime elements in $\mathcal{O}_K$ and $f, f' \in \mathcal{O}_{\bar{K}}[[X]]$ be two power series whose coefficient modulo degree two terms are π and π' respectively. Also assume $f \equiv f' \equiv X^q$ modulo the unique maximal ideal in $\mathcal{O}_{\bar{K}}$ and that $L(X_1, ..., X_m)$ is some linear form in m variables satisfying

$$\pi L(X_1, ..., X_m) = \pi' L^\varphi(X_1, ..., X_m)$$

then there exists a unique power series $\rho \in \mathcal{O}_{\bar{K}}$ congruent to L modulo degree two terms and that

$$f \circ \rho = \rho^\varphi \circ f'$$

Proof: [1] Proposition 3.12. ♣

Lemma 6.4. Let $g(X)$ be a power series in $\mathcal{O}_K[[X]]$ whose constant term isn't in m_K. If g satisfies $g(X +_{F_f} \gamma) = g(X)$ for all $\gamma \in m^f_{\bar{K},1}$ then there is a unique h with $h(0)$ not in m_K with $g(X) = h \circ f$

Proof: [1] Lemma 5.6 ♣

Theorem 6.5. The norm groups of $K_{\pi,n}$ and K_π are $\pi^{\mathbb{Z}} \times (1+(\pi)^n)$ and $\pi^{\mathbb{Z}}$ respectively.

Proof: We first show that $N_{K_{\pi,n}/K}(K^*_{\pi,n}) = \pi^{\mathbb{Z}} \times (1 + (\pi)^n)$. Theorem 3.5 shows that $\pi \in N_{K_{\pi,n}/K}(K_{\pi,n})$ and that $u\pi \in N_{K_{u\pi,n}/K}(K_{u\pi,n})$ for $u \in 1 + (\pi)^n$ and by proposition 4.1 we know they are the same thing so that $\pi, u\pi \in N_{K_{\pi,n}/K}(K_{\pi,n})$. This implies $u = \frac{u\pi}{\pi}$ is in the norm group i.e. $1 + (\pi)^n \subset N_{K_{\pi,n}/K}(K_{\pi,n})$ also that $\pi \in N_{K_{\pi,n}/K}$. Now because $N_{K_{\pi,n}/K} \leq K^* = \pi^{\mathbb{Z}} \times \mathcal{O}_{\mathcal{K}}{}^*$ we need to show that the units in $N_{K_{\pi,n}/K}(K_{\pi,n})$ are in $1 + (\pi)^n$. Note that the only norms which are units are the norms of units: look at valuations at valuations and recall that the norm of an element in a Galois extension is simply the product of all its Galois conjugates. Thus we need to show that $N_{K_{\pi,n}/K}(\mathcal{O}_{K_{\pi,n}}) \subset 1 + (\pi)^n$.

Choose a $u \in \mathcal{O}^*_{K_{\pi,n}}$ and let $a \in m^f_{\bar{K},n} - m^f_{\bar{K},n-1}$ so that a is a generator for the maximal ideal in $\mathcal{O}_{K_{\pi,n}}$. Then then by proposition 1.24 $\mathcal{O}_{K_{\pi,n}} = \mathcal{O}_K[a]$. This means that $u = h(a)$ for some polynomial (and hence power series) $h(X) \in \mathcal{O}_K[[X]]$ and because u is a unit we know that modulo (π) $u \equiv h(0)$ and that they cannot be congruent to zero. This implies that the constant term of $h(X)$ is a unit in $\mathcal{O}_K$ and hence invertible in $\mathcal{O}_K[[X]]$.

Choose $\gamma, \gamma' \in m^f_{\bar{K},1}$ then by the associativity axiom satisfied by Formal groups we have $(X +_{F_f} \gamma) +_{F_f} \gamma' = X +_{F_f} (\gamma +_{F_f} \gamma')$. This shows that a power series of the form $h_1(X) = \Pi_{\gamma \in m^f_{\bar{K},n}} h(X +_{F_f} \gamma)$ satisfies the identity $h_1(X + F_f\gamma) = h_1(X)$. This is easy to see because of the associativity law and the fact that $m^f_{\bar{K},1}$ forms a group under $+_{F_f}$ so that adding by some $\gamma \in m^f_{\bar{K},1}$ inside just permutes the terms in the product. By lemma 6.4 there exists a unique power series $h_2(X)$ with $h_1 = h_2 \circ f$. We define $N(g)$ for some power series $g \in \mathcal{O}_K[[X]]$ to be the unique power series such that

$$N(h) \circ f = \Pi_{\gamma \in m^f_{\bar{K},1}} h(X +_{F_f} \gamma)$$

whose existence, again, is guaranteed by the previous lemma. Recall that $m^f_{\bar{K},1}$ consists of the roots of the polynomial $f \in \mathcal{O}[X]$ and is therefore closed under the action of the Galois group. For any $\sigma \in Gal(K_{\pi,n}/K)$ this shows that for $g \in \mathcal{O}_K[X]$

$$(N(g) \circ f)^\sigma = \Pi_{\gamma \in m^n_{\bar{K},f}} g(X +_{F_f} \gamma)^\sigma = \Pi_{\gamma \in m^n_{\bar{K},f}} g(X +_{F_f} \gamma^\sigma) = \Pi_{\gamma \in m^n_{\bar{K},f}} g(X +_{F_f} \gamma)$$

or that $N(g) \circ f$ is invariant under $Gal(K_{\pi,n}/K)$ and hence has coefficients in K. Then, using the fact that f itself has coefficients in $\mathcal{O}_K$, its easy to see that $N(g)$ must as well. We define $N^k(h) = N^{k-1}(N(h))$ where $N^0(h) = h$. We shall prove some properties of this operator N. Before anything else, note that by definition it is multiplicative. Secondly, we have $N(g) \equiv g \mod (\pi)$. To see this recall that $f(X) \equiv X^q$ modulo (π) so that $N(h) \circ f \equiv N(h) \circ X^q$ modulo (π). Now because $\gamma \in m^f_{\bar{K},1} \subset (\pi_{K_{\pi,1}})$ we have $X +_{F_f} \gamma \equiv X$ modulo $(\pi_{K_{\pi,1}})$ because $X +_{F_f} \gamma =$

$F_f(X,\gamma) \equiv X + \gamma$ modulo degree two terms and the γ goes to zero modulo $(\pi_{K_{\pi,1}})$. This means $\Pi_{\gamma \in m_{\bar{K},1}} g(X +_{F_f} \gamma) \equiv g(X)^q \equiv g(X^q)$ modulo $(\pi_{K_{\pi,1}})$. But these are all polynomials over $\mathcal{O}_K$ and so they must be congruent modulo $(\pi_{K_{\pi,1}}) \cap K_{\pi,n} = (\pi)$. This tells us that $N(g) \circ X^q \equiv N(g) \circ f \equiv g(X^q) = g \circ X^q$ modulo (π). It is easy to see this implies $N(g) \equiv g$ modulo π as desired. This immediately implies that if $g \in \mathcal{O}_K[[X]]^*$ then so is $N(g)$.

Next we will show that if $g \equiv 1$ modulo $(\pi)^i$ then $N(g) \equiv 1$ modulo $(\pi)^{i+1}$. Write $g = 1 + \pi^i g_1$ with $g_1 \in \mathcal{O}_K[X]$. Then we have

$$N(g) \circ f = \Pi_{\gamma \in m^f_{\bar{K},1}} (1 + \pi^i g_1(X +_{F_f} \gamma)) \equiv (1 + \pi^i g_1(X))^q$$

modulo π^{i+1} since $\pi^i(g_1(X +_{F_f} \gamma) - g_1(X)) \in (\pi)^{i+1}$ because, as we showed in the previous paragraph $g_1(X +_{F_f} \gamma) = g_1(X)$ are congruent modulo (π). But then we have

$$(1 + \pi^i g_1(X))^q \equiv 1 + q\pi^i g_1(X) + ... + \pi^{iq} g_1(X)^q \equiv 1$$

modulo $(\pi)^{i+1}$ since each term besides the first two is a multiple of π^{i+1} and the second term is in $(q)(\pi)^i$ which is itself in $(\pi)^{i+1}$. Now, using multiplicativity, note that since $\frac{N(g)}{g} \equiv 1$ modulo (π) that $\frac{N^2(g)}{N(g)} \equiv 1$ modulo $(\pi)^2$ i.e. that $N^2(g) \equiv N(g)$ modulo $(\pi)^2$. Proceeding in this fashion we see that in general $N^{k-1}(h) \equiv N^k(h)$ modulo $(\pi)^k$. Coming back to the situation we have that $N(h)$ is not zero modulo (π), moreover that neither is $N^{n-1}(h)$ nor $N^n(h)$. Also we have that $N^{n-1}(h)(0) = u_1 \equiv u_2 = N^{n-2}(h)(0) \in \mathcal{O}_K^*$ modulo $(\pi)^n$. We shall show by induction that

$$N^n(h) \circ f^{(n)} = \Pi_{\beta \in m^f_{\bar{K},n}} h(X +_{F_f} \beta)$$

for $n = 1$ this is the definition. Our induction hypothesis will assume that the equality holds for $n-1$. Let A be a set of coset representatives for the group $m^f_{\bar{K},n}/m^f_{\bar{K},1}$ which means every element in $m^f_{\bar{K},n}$ can be written uniquely as $a + \gamma$ for some $a \in A$ and some $\gamma \in m^f_{\bar{K},1}$. Then we can write

$$\Pi_{\beta \in m^f_{\bar{K},n}} h(X +_{F_f} \beta) = \Pi_{\beta \in A} \Pi_{\gamma \in m^f_{\bar{K},1}} h(X +_{F_f} \beta +_{F_f} \gamma) = \Pi_{\beta \in A} N(h) \circ f(X +_{F_f} \beta)$$

Note that f is an endomorphism of F_f which implies $f(X +_{F_f} \beta) = f(X) +_{F_f} f(\beta)$ except now $f(\beta) \in m^f_{\bar{K},n-1}$. In fact, it is easy to see that as β runs through A $f(\beta)$ runs through the complete list of elements in $m^f_{\bar{K},n-1}$. This tell us that

$$\Pi_{\beta \in m^f_{\bar{K},n}} h(X +_{F_f} \beta) = \Pi_{\zeta \in m^f_{\bar{K},n-1}} N(h)(f(X) +_{F_f} \zeta)$$

and by the induction hypothesis this is exactly $N^{n-1}(h)(N(h)) \circ f^{(n-1)}(f(X)) = N^n(h) \circ f^{(n)}(X)$ thereby completing the induction.

This means that $u_1 = \Pi_{\gamma \in m^f_{\bar{K},n-1}} h(\gamma)$ and that $u_2 = \Pi_{\gamma \in m^f_{\bar{K},n}} h(\gamma)$ so that

$$\frac{u_2}{u_1} = \Pi_{\gamma \in m^f_{\bar{K},n} - m^f_{\bar{K},n-1}} h(\gamma)$$

Now, because $m^f_{K,n} - m^f_{K,n-1}h(\gamma)$ is a complete set of Galois conjugates we see that $\frac{u_2}{u_1} = N_{K_{\pi,n}/K}(h(\gamma)) = N_{K_{\pi,n}/K}(h(a)) = N_{K_{\pi,n}/K}(u)$ is in the norm group of $K_{\pi,n}$. The fact that $u_1 \equiv u_2$ modulo $(\pi)^n$ tells us that $N_{K_{\pi,n}/K}(u) \in 1 + (\pi)^n$ as claimed.

It remains to show that $N_{K_\pi/K}(K_\pi) = \pi^{\mathbb{Z}}$. However, this follows easily from the first fact since $\bigcap_{i=1}^{\infty} 1 + (\pi)^i = \{1\}$ and by definition the norm group of an infinite extension is the intersection of the norm groups of the finite subextensions. This shows that $N_{K_\pi/K}(K^*_\pi) = \pi^{\mathbb{Z}}$. ♣

7 The Main Theorems of Local Class Field Theory

Now we will show that the Artin map we constructed is functorial, more precisely:

Theorem 7.1. Let L/K be a finite extension of local fields, and let ϕ_K and ϕ_L be the respective Artin maps, then the following diagram commutes

$$\begin{array}{ccc} L^* & \xrightarrow{\phi_L} & Gal(L^{ab}/L) \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle |_{K^{ab}}} \\ K^* & \xrightarrow{\phi_K} & Gal(K^{ab}/K) \end{array}$$

Proof: Let E be a subextension of L/K i.e. $K \subset E \subset L$. If we show the theorem holds for the two extensions E/K and L/E then, because the norm and restriction maps are functorial i.e. $N_{L/K} = N_{E/K} \circ N_{L/E}$ then the theorem holds for L/K. Setting E equal to the fixed field of the inertia group makes L/E is totally ramified and E/K unramified. Thus we have reduced the proof to the cases where L/K is totally ramified and unramified. We deal with them separately.

First suppose that L/K is totally ramified. Since the prime elements of L^* generate L^* we only need to show that $\phi_K(N_{L/K}(\pi')) = \phi_L(\pi')|_{K^{ab}}$ for every prime element $\pi' \in L^*$. We extend $\phi_L(\pi')$ to an automorphism τ of $\bar{K} = \bar{L}$, and we know that the fixed field of τ, F, intersects $L^{un} \cdot L_{\pi'}$ exactly at $L_{\pi'}$. This is because the fixed field of $\langle\tau\rangle$ will have a residue field that is fixed by τ. Moreover, τ acts on the residue field extension as the Frobenius over L. Therefore the residue field extension must be trivial. This tells us that the fixed field,F, of τ is totally ramified and so its intersection with $L^{ab} = L^{un} \cdot L_{\pi'}$ is a totally ramified extension containing L_π. Lemma 5.20 implies it is equal to L_π. By proposition 1.30 we know that an extension is totally ramified if and only if it contains a prime element of the ground field. By the previous result we know that $N_{L_{\pi'}/L}(L^*_{\pi'}) = \pi'^{\mathbb{Z}}$ and because $N_{F/L}(F^*) \subset N_{L_{\pi'}/L}(L^*_{\pi'}) = \pi'^{\mathbb{Z}}$ must contain a prime element we must have equality i.e. $N_{F/L}(F^*) = \pi'^{\mathbb{Z}}$.

Since τ extends $\phi_L(\pi')$ we know it acts as the Frobenius automorphism on L^{un} and because L/K is totally ramified (i.e. the corresponding residue field extension is trivial) we see that $\phi_L(\pi')$ acts as the Frobenius on K^{ab} as well. Put $\sigma = \tau|_{K^{ab}}$ and since it acts as the Frobenius, the following Lemma tells us that it is equal to some $\phi_K(\pi)$ for a prime element $\pi \in K^*$. As in the previous paragraph the intersection of the fixed field of $\phi_K(\pi) = \sigma$ and K^{ab} is a totally ramified extension containing K_π and thus must be equal to K_π. Since σ is the restriction of τ and F is the fixed field of τ, K_π must be contained in F. Now because F/L and L/K are totally ramified we see that F/K is as well and thus its norm group must contain a prime element of the ground field. Now because $N_{F/K}(F^*) \subset N_{K_\pi/K}(K^*_\pi) = \pi^{\mathbb{Z}}$, as in the previous paragraph, we must have equality i.e. $N_{F/K}(F^*) = \pi^{\mathbb{Z}}$.

Now we combine the two statements, namely that $N_{F/L} = \bigcap_{L \subset M \subset F} N_{M/L}(M^*) = \pi'^{\mathbb{Z}}$ (as M/L ranges through the finite subextensions) and $N_{F/K}(F^*) = \pi^{\mathbb{Z}}$. Firstly, by definition and the transitivity of the norm $N_{F/K} = \bigcap_{K \subset M \subset F} N_{M/K} \subset \bigcap_{L \subset M \subset F} N_{L/K} \circ N_{M/L}$. Now given any M/K, we consider ML/L, and note that $N_{L/K} \circ N_{ML/L} =$

$N_{ML/K} \subset N_{M/K}$ because $N_{ML/K} = N_{M/K} \circ N_{ML/M}$. This tells us that actually

$$N_{F/K} = \bigcap_{L \subset M \subset F} N_{L/K} \circ N_{M/L}$$

as M ranges through all finite subextensions of F/L. Applying this fact to our case we see that $N_{F/K}(F^*) = \bigcap_{L \subset M \subset F} N_{L/K} \circ N_{M/L}(M^*) = \pi^{\mathbb{Z}}$ where $\pi' \in N_{M/L}(M^*)$ for all finite subextensions M of F/L. This tells us that $N_{L/K}(\pi') \in N_{F/K}(F^*) = \pi^{\mathbb{Z}}$ but since L/K is totally ramified we know that the norm of a prime element of L must be prime in K. From this we see that $N_{L/K}(\pi') = \pi$. What we've shown is that

$$\phi_K(N_{L/K}(\pi')) = \phi_K(\pi) = \sigma = \tau|_{K^{ab}} = \phi_L(\pi')|_{K^{ab}}$$

for L/K totally ramified.

Now we proceed to the case where L/K is unramified. Suppose that L is the unique unramified extension of K with $|L : K| = m$. As above only need to prove this for prime elements, π' of L. Consider $L_{\pi',n}/L$, the totally ramified Lubin-Tate extension of L. Since $\pi' \in L$ is a prime element the previous argument shows $\pi' = N_{L_{\pi',n}}(L^*_{\pi,n})$ and that $\phi_L(\pi')$ is equal to the restriction of an element from $Gal(L^{ab}_{\pi,n}/L_{\pi',n})$. This means its restriction to $L_{\pi',n}$ is the identity. Since n was arbitrary we see that $\phi_L(\pi')|_{L_{\pi'}} = 1$. But we know the action of $\phi_L(\pi')$ is the Frobenius over L, that is, the m-th power of the Frobenius over K because L/K is unramified of degree m. Moreover, $\phi_K(N_{L/K}(\pi'))|_{K^{un}}$ is the mth power of the Frobenius because $N_{L/K}(\pi')$ is the product of m prime elements of K. So $\phi_K(N_{L/K}(\pi'))$ and $\phi_L(\pi')$ agree on K^{un}. Note $L_{\pi'} \subset K^{ab}$, moreover that $L^{un} = K^{un}$ so

$$K^{ab} = L^{ab} = L_{\pi'}L^{un} = L^{\pi'}K^{un}$$

Thus, it remains to show that the action of $\phi_K(N_{L/K}(\pi'))$ is trivial on $L_{\pi'}$. The proof is long and unenlightening, the interested reader can consult [1] Lemma 6.1. ♣

Lemma 7.2. The map $\phi_K|_{\mathcal{O}_K^*} : \mathcal{O}_K^* \to Gal(K^{ab}/K)$ induces an isomorphism $\mathcal{O}_K^* \to Gal(K_\pi/K)$. Therefore the set $\phi_K(K^*)$ consists of all elements in $Gal(K^{ab}/K)$ whose restriction to K^{un} is an integer power of the Frobenius.

Proof: For any unit $u \in \mathcal{O}_K^*$ we know $\phi_K(u)$ acts trivially on K^{un}. Note that $K^{un} \cap K_\pi = K$ so $Gal(K^{ab}/K) \cong Gal(K^{un}/K) \times Gal(K_\pi/K)$. So we obtain the induced map by composing

$$\mathcal{O}_K^* \to Gal(K^{ab}/K) \cong Gal(K_\pi/K) \times Gal(K^{un}/K) \to Gal(K_\pi/K)$$

where the first map is ϕ_K and the second is the projection onto the first coordinate. This map takes $u \mapsto [u^{-1}]_{f,f}$ for some $f \in \mathcal{F}_\pi$ and it induces the isomorphisms $\mathcal{O}_K^*/(1+(\pi)^n) \to Gal(K_{\pi,n}/K)$. Moreover its easy to see that the map $\mathcal{O}_K^* \to Gal(K_\pi/K)$ can be recovered as the limit of these isomorphisms and hence yields an isomorphism

$$\varprojlim_{n \in \mathbb{N}} \mathcal{O}_K^*/(1+(\pi)^n) \cong \varprojlim_{n \in \mathbb{N}} Gal(K_{\pi,n}/K) \cong Gal(K_\pi/K)$$

But $1+(\pi)^n$ forms a system of neighborhoods for $\mathcal{O}_K^*$ in the topology induced by the π-adic topology since they are the translates of the $(\pi)^n$. This means its completion with respect to the topology generated by the $1+(\pi)^n$ is the same as the completion with respect to the π-adic topology. But the latter is simply $\mathcal{O}_K^*$ itself because it is a closed subset of a complete space. Thus we see that the map defined above is actually an isomorphism as claimed. The second statement now follows easily: let $(\varphi^m, \sigma) \in Gal(K^{ab}/K)$ where $\sigma \in Gal(K_\pi/K)$ and φ is the Frobenius. Then take a $u \in \mathcal{O}_K^*$ as above that gets sent to σ under the projection map, then $u\pi^m$, gets sent to $\phi_K(u\pi^m) = (\varphi^m, \sigma)$ as desired. ♣

Lemma 7.3. For any finite abelian extension L/K the map $K^* \to Gal(K^{ab}/K) \to Gal(L/K)$ induced by ϕ_K is surjective and has $N_{L/K}(L^*)$ as its kernel. This map will be denoted $\phi_{L/K}$.

Proof: By the previous lemma $\phi_K(K^*)$ consists of all the automorphisms of K^{ab} whose restriction to K^{un} is an integer power of the Frobenius. We can write $K^{ab} = \bigcup_{i=1}^{\infty} K_i K_{\pi,i}$ where K_i is the unique unramified extension of degree i. Thus we have

$$\varprojlim_{i\in\mathbb{N}} (Gal(K_{\pi,i}/K) \times Gal(K_i/K)) \cong \varprojlim_{i\in\mathbb{N}} Gal(K_{\pi,i}/K) \times \varprojlim_{i\in\mathbb{N}} Gal(K_i/K)$$

and by theorem 3.5 and proposition 1.15 this is isomorphic to

$$\varprojlim_{n\in\mathbb{N}} \mathcal{O}_K^*/(1+(\pi)^n) \times \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/(n) \cong \mathcal{O}_K^* \times \hat{\mathbb{Z}}$$

where the last isomorphism follows from the previous lemma and the definition of $\bar{Z}$. Now it is obvious that the image of ϕ_K, $\mathcal{O}_K^* \times \mathbb{Z}$, is dense in this group. This implies that its image in $Gal(K^{ab}/K)/Gal(K^{ab}/L) \cong Gal(L/K)$ is also dense. Since the topology on the latter (finite) group is discrete this means $\phi_{L/K}$ onto.

It is obvious from theorem 7.1 that $N_{L/K}(L^*) \subset \ker \phi_{L/K}$. This is because

$$\phi_K(N_{L/K}(x)) = \phi_L(x)|_{K^{ab}}$$

but ϕ_L takes has its image in $Gal(L^{ab}/L)$ and so fixes L. Now suppose $x \in \ker \phi_{L/K}$, then $\phi_K(x)|_{L\cap K^{un}} = 1$. Note that $L \cap K^{un} = K_m$ for some natural number m where K_m is the unique unramified extension of degree m. Using the previous lemma we see that $\phi_K(x)|_{K_m} = 1$ implies $\phi_K(x)|_{K^{un}}$ is a power of the m-th power of the Frobenius over K i.e. $\phi_K(x)|_{K^{un}} = (\varphi_K^m)^i$. By basic Galois theory we know that

$$Gal(LK^{un}/K_m) \cong Gal(L/K_m) \times Gal(K^{un}/K_m)$$

and

$$Gal(LK^{un}/L) \cong Gal(K^{un}/K_m)$$

L and K_m have the same residue fields and so do K^{un} and LK^{un}. So the inertia subgroups of $Gal(LK^{un}/L)$ and $Gal(K^{un}/K_m)$ are mapped isomorphically onto one another. Since K^{un}/K_m is unramified $Gal(K^{un}/K_m)$ has a trivial inertia subgroup and so $Gal(LK^{un}/L)$ does as well. This tells us that LK^{un} is unramified over L and

since it has the same residue field as L^{un} proposition 1.24 tells us $LK^{un} = L^{un}$. From the above discussion we obtain the isomorphism: $Gal(L^{un}/L) \cong Gal(K^{un}/K_m)$. This shows $\phi_K(x)|_{L^{un}} = \varphi_L^i$ is some power of the Frobenius over L. Thus, by the previous lemma this implies $\phi_K(x) = \phi_L(x')$ for some $x' \in L$. Finally by theorem 7.1 we can say $\phi_K(x) = \phi_K(N_{L/K}(x'))$ and the injectivity of ϕ_K yields $x = N_{L/K}(x')$, as desired. For the injectivity of ϕ_K: suppose $\phi_K(u\pi^m) = 1$, then $\phi_K(u\pi^m)|_{K^{un}} = \varphi^m = 1$ implying that $m = 0$. Lastly, lemma 7.2 shows that $\phi_K(u) = 1$ implies $u = 1$. ♣

With the above lemma we have proven the main theorem of Local Class Field Theory, Theorem 1.18. Now we will prove the Local Existence theorem. In classical proofs of Local Class field theory this was the result proven first and the Artin map was then deduced from it. The result will give a one to one order reversing correspondence between open subgroups in K^* of finite index and finite abelian extensions of K^*. In this return to the exposition given in [4].

Theorem 7.4. Let K be a nonarchimedean local field. Then the following statements are true

(a) There is a one-to-one correspondence between finite abelian extensions of K and subgroups of K^* that are open and of finite index. The correspondence is given by $L \leftrightarrow N_{L/K}(L^*)$.

(b) This correspondence is order reversing i.e. $L \subset M$ if and only $N_{M/K}(M^*) \subset N_{L/K}(L^*)$.

(c) $N_{LM/K}((LM)^*) = N_{M/K}(M^*) \cap N_{L/K}(L^*)$

(d) $N_{(L\cap M)/K}((L \cap M)^*) = N_{L/K}(L^*) \cdot N_{M/K}(M^*)$

(e) Any subgroup that contains a norm subgroup must itself be a norm subgroup.

Proof: We will prove the middle three statements first. The forward direction in (b) is obvious since the norm is transitive: $N_{M/K}(M^*) = N_{L/K}(N_{M/L}(M^*))$. Since L and M are in LM this tells us that $N_{LM/K}((LM)^*) \subset N_{L/K}(L^*) \cap N_{M/K}(M^*)$. Now if $a \in N_{L/K}(L^*) \cap N_{M/K}(M^*)$ then we know that $\phi_{L/K}(a) = 1 = \phi_{M/K}(a)$ and because of theorem 7.1 this tells us that $\phi_K(a)$ acts trivially on ML i.e. $a \in N_{ML/K}((ML)^*)$. Note that here we are using the fact that an element of $Gal(ML/K)$ is uniquely determined by its action on M and L. Thus (c) holds and we can now finish the proof of (b). Suppose $N_{M/K}(M^*) \subset N_{L/K}(L^*)$ then (c) says $N_{ML/K}((ML)^*) = N_{M/K}(M^*)$. The Artin map induces an isomorphism, $\phi_{LM/K}$, between the groups $K^*/N_{ML/K}((ML)^*)$ and $Gal(ML/K)$, it also induces an isomorphism $\phi_{M/K}$ from $K^*/N_{M/K}(M^*)$ to $Gal(M/K)$. Therefore the indices of $N_{ML/K}((ML)^*)$ and $N_{M/K}(M^*)$ in K^* are the same and equal the degrees of ML/K and M/K. Since $M \subset ML$ this means $|ML : M| = 1$ or that $L \subset M$ as desired. Part (a) now follows easily since by definition the set map $L \to N_{L/K}(L^*)$ is surjective, injectivity is easily deduced from (b). We now prove (e). Suppose that $N_{L/K}(L^*) \subset I$ then the Artin map induces an isomorphism $\phi_{L/K} : K^*/N_{L/K}(L^*) \to Gal(L/K)$ then let M be the fixed field of $\phi_{L/K}(I/N_{L/K}(L^*))$. By the previous lemma we have the following commutative diagram

$$\begin{array}{ccc} K^* & \xrightarrow{\phi_{L/K}} & Gal(L/K) \\ \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle |_M} \\ K^* & \xrightarrow{\phi_{M/K}} & Gal(M/K) \end{array}$$

where the kernel of $\phi_{M/K}$ is exactly $N_{M/K}(M^*)$ but we know I is contained in the kernel as well so $I \subset N_{M/K}(M^*)$. Note that I and $N_{M/K}(M^*)$ contain $N_{L/K}(L^*)$. Galois theory gives us that $\phi_{L/K}(I) = \phi_{L/K}(N_{M/K}(M^*))$ so they must have the same preimages i.e. $I = N_{M/K}(M^*)$ as desired. Finally we prove (d): by (b) we see that $N_{L/K}(L^*)$ and $N_{M/K}(M^*)$ are inside $N_{(L\cap M)/K}((L \cap M)^*)$. By (e) we know $N_{L/K}(L^*) \cdot N_{M/K}(M^*)$ is itself is a norm group, say $N_{N/K}(N^*)$. By (b) $N \subset L \cap M$ and by (b) again $N_{(L\cap M)/K}((L \cap M)^*) \subset N_{N/K}(N^*) = N_{L/K}(L^*) \cdot N_{M/K}(M^*)$ thereby completing the proof. ♣

Proof (Local Existence Theorem): We will show that the open subgroups of finite index of K^* are exactly the norm subgroups of finite abelian extensions L/K. First, let L/K be a finite abelian extension, then lemma 7.3 says $N_{L/K}(L^*)$ has finite index in K^*. Note that the norm map $N_{L/K} : L^* \to K^*$ is continuous: it is the composition of the maps

$$L^* \to L^* \times \cdots \times L^* \to L^*$$

where the first is the map $a \mapsto (a, \sigma_1(a), ..., \sigma_n(a))$ where the σ_i run through the non-identity elements of $Gal(L/K)$. The second map is multiplication. These two maps are clearly continuous so their composition, the norm, is continuous as well. Note that we've used the fact that the topology on K^* is the same as the induced topology from L^*. This implies that the image of the compact set U_L (the set of units in $\mathcal{O}_L$) is itself compact and hence closed. We also see that $N_{L/K}(L^*) \cap U_K = N_{L/K}(U_L)$ since an element that is in a norm group can have zero valuation if and only if it is the norm of an element with zero valuation. This tells us that there is an injection $U_K/N_{L/K}(U_L) \hookrightarrow K^*/N_{L/K}(L^*)$ so that $N_{L/K}(U_L)$ must have finite index in U_K. Since it is also closed in U_K it must be open there too: it is the complement of a finite union of closed cosets. Since U_K is itself open this implies $N_{L/K}(U_L)$ must also be open in K^*. Since $N_{L/K}(L^*)$ contains an open subgroup it is the union of open cosets and therefore is itself open.

We now prove the converse, suppose O is an open set in K^* of finite index. Its intersection with U_K must contain an open set, $(1 + m_K^n)$ say, since these sets form a system of neighborhoods for U_K. It must also intersect $\pi^{\mathbb{Z}}$ nontrivially because it has finite index. This means O contains the subgroup $\langle \pi^m \rangle \cdot (1 + m_K^n)$ for some positive numbers m, n. Note that the norm group of the unique unramified extension of K of degree m, K_m, is $\langle \pi^m \rangle \times \mathcal{O}^*$. This follows because by the construction of ϕ_K and theorem 4.1, $\phi_K(u)$ acts trivially on K^{un}. Moreover, by lemma 7.3 order considerations force $N_{K_m/K}(K_m) = \langle \pi^m \rangle \times \mathcal{O}_K$. Then by theorem 7.4 (c) and 6.5 we see that $\langle \pi^m \rangle \cdot (1 + m_K^n) = N_{L/K}(L^*)$ where $L^* = K_m \cdot K_{\pi,n}$. This means O contains a norm subgroup, now by part (e) of the previous lemma it itself must be a norm subgroup. ♣

8 A Concrete Realization of $\mathbf{Gal(K}^{ab}/K)$

We begin by collecting the facts proven. We have constructed the Local Artin map for a local field K:

$$\phi_K : K^* \to Gal(K^{ab}/K)$$

which induces isomorphisms $\phi_{L/K}$ for finite abelian extensions L/K

$$\phi_{L/K} : K^*/N_{L/K}(L^*) \to Gal(L/K)$$

Fixing a prime element $\pi \in K^*$ we can rewrite these isomorphisms as

$$\phi_{L/K} : (\pi^{\mathbb{Z}} \times \mathcal{O}_K^*)/N_{L/K}(L^*) \to Gal(L/K)$$

Taking the inverse limit of both sides as L/K runs through all the finite abelian extensions induces the isomorphism

$$\varprojlim_{L/K} (\pi^{\mathbb{Z}} \times \mathcal{O}_K^*)/N_{L/K}(L^*) \to Gal(K^{ab}/K)$$

The Local existence theorem says that $K^* \cong \pi^{\mathbb{Z}} \times \mathcal{O}_K^*$, with the π-adic topology, is a finer space than K^* with the norm topology. In other words the identity map

$$K^* \to K^*$$

is continuous when the right hand side is endowed with the topology induced by the norm groups and the left hand side is the regular π-adic topology. By the functoriality of taking completions this continuous map induces a map $K^* \to \hat{K^*}$ on the completions. Here K^* denotes the multiplicative group we began with since it is already complete with respect to the π-adic topology. $\hat{K^*}$ denotes the completion of K^* with respect to the norm topology. In $\mathcal{O}_K^*$ the norm topology and the π-adic topology are the same, so passing to a completion leaves it unchanged. On the other hand, completing $\pi^{\mathbb{Z}}$ over all subgroups of finite index yields $\pi^{\hat{\mathbb{Z}}}$. In other words we have exhibited the isomorphism

$$\hat{K^*} \cong \mathcal{O}_K^* \times \pi^{\hat{\mathbb{Z}}} \cong Gal(K^{ab}/K)$$

which yields a concrete realization of the Galois group of the maximal abelian extension over K.

References

[1] K. Iwasawa. Local Class Field theory. Oxford Science Publications. The Clarendon Press Oxford University Press, New York. Oxford Mathematical Monographs, 1986.

[2] J. Neukirch, Algebraic Number Theory, Grundlehren der mathematischen Wissenschaften, 322, Berlin: Springer-Verlag, 1999.

[3] J.S. Milne, Algebraic Number Theory, http://www.jmilne.org/math, 2012.

[4] J.S. Milne, Class Field Theory, http://www.jmilne.org/math, 2011.

[5] E. Riehl, Lubin-Tate Formal Groups And Local Class Field Theory, http://www.math.harvard.edu/ eriehl/, 2006.

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