Algebraic Number Theory Notes: Local Fields

Sam Mundy

These notes are meant to serve as quick introduction to local fields, in a way which does not pass through general global fields. Here all topological spaces are assumed Hausdorff.

1 $\mathbb{Q}_p$ and $\mathbb{F}_q((x))$

The basic archetypes of local fields are the p-adic numbers $\mathbb{Q}_p$, and the Laurent series field $\mathbb{F}_q((t))$ over the finite field with q elements. These fields come with a natural topology which is intertwined with their algebraic structure. As such, they should be viewed through not only an algebraic lens, but also a geometric lens as well. Before defining these fields and their topology, let us give a general definition.

Definition 1.1. A *topological field* is a field K equipped with a topology such that all four field operations are continuous, i.e., the functions

$$\begin{aligned} + &: K \times K \to K, \\ - &: K \to K, \\ \cdot &: K \times K \to K, \\ (\cdot)^{-1} &: K^\times \to K \end{aligned}$$

are all continuous. Here, of course, $K \times K$ has the product topology and $K^\times$ the subspace topology.

One way to give a field a topology is to give it an absolute value, which will induce a metric on the field:

Definition 1.2. Let K be a field. An *absolute value* on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying the following properties:
(1) [Positive Definiteness] $|x| = 0$ if and only if $x = 0$.
(2) [Multiplicativity] $|ab| = |a| \cdot |b|$ for all $a, b \in K$.
(3) [Triangle Inequality] $|a + b| \leq |a| + |b|$ for all $a, b \in K$.

If K is a field with an absolute value, one can define a metric d on K by setting $d(a, b) = |b - a|$. One checks easily that this does indeed define a metric on K. Furthermore, the four field operations are continuous with respect to this metric. In fact, essentially the same proofs from calculus, which show this fact for $K = \mathbb{R}$, work for any field with an absolute value.

Let us now discuss absolute values on $\mathbb{Q}$. Of course, we have the standard absolute

value on $\mathbb{Q}$ which assigns to $a \in \mathbb{Q}$ the value a if $a \geq 0$, and $-a$ otherwise. But there are many other absolute values as well. For instance, let p be a prime number. If n is a nonzero integer, write $v_p(n)$ for the largest integer m for which $p^m | n$. That is, v_p extracts the exact power of p occurring in the factorization of n. Let $x \in \mathbb{Q}$ be nonzero, and write x as a fraction $x = a/b$ with $a, b \in \mathbb{Z}$. Then we set $|x|_p = p^{v_p(b)-v_p(a)}$ and $|0|_p = 0$. It is an easy exercise to check that the assignment $x \mapsto |x|_p$ is an absolute value on $\mathbb{Q}$. It is called the *p-adic absolute value.* In fact, one checks that it satisfies the *ultrametric inequality,* namely the inequality

$$|x + y| \leq \max\{|x|, |y|\} \tag{1}$$

holds for $|\cdot| = |\cdot|_p$.

The ultrametric inequality has some funny consequences for the metric topology on $\mathbb{Q}$ induced by $|\cdot|_p$. For instance, two metric balls intersect if and only if one contains the other. (This is true more generally for any metric space with metric d satisfying $d(x, y) \leq \max\{d(x, z), d(z, y)\}$.)

Proposition/Definition 1.3. *Let K be a field with an absolute value $|\cdot|$. Then $|\cdot|$ satisfies the ultrametric inequality* (1) *if and only if the set $\{|n \cdot 1| \mid n \in \mathbb{Z}\}$ is bounded in K. In either case we say K is* nonarchimedean.

Proof. The proof is not enlightening. It is in Milne's algebraic number theory notes [4] Theorem 7.2 if you want to see it. □

We are ready to define $\mathbb{Q}_p$. Let R be the set of *Cauchy sequences* in $\mathbb{Q}$ with respect to the p-adic absolute value. That is,

$$R = \{\{x_n\}_{n=1}^{\infty} \mid \text{for any } \epsilon > 0, \text{ there is an } N \text{ such that } |x_m - x_n|_p < \epsilon \text{ for } n, m > N\}.$$

This is a ring under termwise addition and multiplication. Let M be the set of p-adic Cauchy sequences converging to 0. Then M is an ideal and we define

$$\mathbb{Q}_p = R/M.$$

We call $\mathbb{Q}_p$ the field of *p-adic numbers.* It is simply the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. This field inherits an absolute from $\mathbb{Q}$ in the obvious way: If $x, y \in \mathbb{Q}_p$ and assume x is the class of the Cauchy sequence $\{x_n\}$. Then we define

$$|x| = \lim_{n \to \infty} |x_n|_p,$$

which is well defined because $\{x_n\}$ is Cauchy. It is not hard to check that this is indeed an absolute value on $\mathbb{Q}_p$. The ultrametric inequality still holds for $\mathbb{Q}_p$ by Proposition 1.3. Finally we note that $\mathbb{Q}_p$ is complete (as a metric space) by construction.

Before we go any further, we note one important property about the p-adic absolute value, namely that its nonzero values are all integral powers of p. In particular, the image of $\mathbb{Q}^\times$ under $|\cdot|_p$ is discrete in $\mathbb{R}_{>0}$, and so it follows that the image of $\mathbb{Q}_p^\times$ under its absolute value is also the integral powers of p.

We will discuss properties of $\mathbb{Q}_p$ in a moment, but first, we repeat this process for the rational function field $\mathbb{F}_q(x)$ in place of $\mathbb{Q}$. For a nonzero polynomial $f \in \mathbb{F}_q[x]$, let $v_x(f)$ be

the exact power of x dividing f. So $v_x(f)$ is the index of the first nonzero coefficient of f. Let $h \in \mathbb{F}_q(t)$ be nonzero, and write $h = f/g$ with $f, g \in \mathbb{F}_q[t]$. Then define $|h|_x = q^{v_x(g)-v_x(f)}$, and $|0|_x = 0$. Then $|\cdot|_x$ is an absolute value on $\mathbb{F}_q(x)$. The field $\mathbb{F}_q(x)$ is nonarchimedean because the image of $\mathbb{Z}$ is bounded (indeed, it is finite.)

We can then let R be the ring of Cauchy sequences in $\mathbb{F}_q(t)$ with respect to $|\cdot|_x$, and M the ideal of sequences converging to 0. Then one can check that

$$R/M \cong F_q((x)).$$

Here $\mathbb{F}_q((x))$ is the field of Laurent series with coefficients in $\mathbb{F}_q$,

$$\mathbb{F}_q((t)) = \left\{ \sum_{i=n}^{\infty} a_i x^i \;\middle|\; a_i \in \mathbb{F}_q, n \in \mathbb{Z} \right\}.$$

In this way, we get an absolute value, and hence a metric topology, on $\mathbb{F}_q((x))$ under which $\mathbb{F}_q((x))$ is complete. This absolute value has an easy description, however: Let $f = \sum a_i x^i \in \mathbb{F}_q((x))$, and let n be the smallest index for which $a_n \neq 0$. Then $|f| = q^{-n}$.

$\mathbb{Q}_p$ and its absolute value have a similar description. One can check that every p-adic number $a \in \mathbb{Q}_p$ can be written in a unique way as

$$a = \sum_{i=-n}^{\infty} a_i p^i$$

where $n \in \mathbb{Z}$ and $a_i \in \{0, \ldots, p-1\}$. Here the series is interpreted at the p-adic limit of its partial sums:

$$\sum_{i=-n}^{\infty} a_i p^i = \lim_{m \to \infty} \sum_{i=-n}^{m} a_i p^i.$$

In order to add or multiply two such series, one must "carry" as if dealing with base-p expansions of integers. Finally, we have $|\sum a_i p^i| = p^{-n}$ where n is the smallest index for which $a_i \neq 0$.

2 Local Fields

Now that we have constructed some basic examples, let us now define the notion of local field.

Definition 2.1. A *local field* is a topological field K whose topology is locally compact and not discrete (and Hausdorff; recall we are assuming all topological spaces are Hausdorff.) By *locally compact* we mean that every point in K has an open neighborhood U such that the closure $\overline{U}$ is compact.

As a good example of some of the basic techniques involved in working with topological algebraic objects, you should do the following exercise.

Exercise 1. (i) Prove that a topological group G (defined in the obvious way; multiplication and inversion are continuous) is Hausdorff if and only if $\{1\}$ is closed in G.

(ii) Prove that a (Hausdorff) abelian topological group G is locally compact if and only if the following condition holds: There is a basis $\mathcal{B}$ of neighborhoods about 0 such that $\overline{U}$ is compact for all $U \in \mathcal{B}$. In particular, if this condition is satisfied for the underlying additive group of a topological field K, then K is a local field.

This definition of local field is hard to work with at first, so we state some equivalent conditions for a field to be a local field.

Theorem 2.2. *The following are equivalent conditions on a topological field K:*

(1) K is a local field.

(2) K has an absolute value $|\cdot|$ which induces a topology on K that makes K complete and locally compact.

(3) K is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((x))$, or $K = \mathbb{R}$ or $K = \mathbb{C}$.

Note that at the moment we have not defined absolute values on the finite extensions of $\mathbb{Q}_p$ or $\mathbb{F}_q((x))$. This will be done in Section 4. For now we remark on the proof of this theorem.

The proof of (1)⇒(2) is somewhat involved. One uses heavily the Haar measure on the locally compact abelian group K (viewed additively.) For the reader who knows a little about this, one defines the *module* of an element $a \in K^\times$ as follows. Let μ be the Haar measure on K. Then by the uniqueness of the Haar measure, the new measure ν on K defined by $\nu(E) = \mu(aE)$ differs from μ by a nonzero constant which we denote $\mathrm{mod}(a)$. This is the module of a. We can then define $|a| = \mathrm{a}$ for $a \in K^\times$ and $|0| = 0$. This recovers the absolute value on K, but the proof is by no means trivial. See Ramakrishnan and Valenza [6], or Weil [9].

In any case we will assume (1)⇒(2), i.e., we will really take (2) as our working definition of local field. We will not assume that we know (3) in these notes, but (3) does provide a convenient way to think of local fields.

Let us show that $\mathbb{Q}_p$ and $\mathbb{F}_q((x))$ are locally compact with respect to the topology induced by their absolute values, so that we know they are local fields (They are Hausdorff, since they are metric.) We do the proof for $\mathbb{Q}_p$; the case of $\mathbb{F}_q((x))$ is formally similar.

First we define a particular subring of $\mathbb{Q}_p$ as follows. Let

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a| \leq 1\}.$$

This is a ring by the fact that $\mathbb{Q}_p$ is nonarchimedean: If $a, b \in \mathbb{Z}_p$, so that $|a|, |b| \leq 1$, then $|a+b| \leq \max\{|a|, |b|\} \leq 1$, hence $(a+b) \in \mathbb{Z}_p$. Also $|-a| = |a|$ implies that $\mathbb{Z}_p$ has additive inverses.

The ring $\mathbb{Z}_p$ is called the ring of *p-adic integers,* and it is a very important structure attached to $\mathbb{Q}_p$. (The analogue of this in the case of $\mathbb{F}_q((x))$ is the subring $\mathbb{F}_q[[x]]$ of formal power series.)

Exercise 2. Prove that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

By definition, $\mathbb{Z}_p$ is closed in $\mathbb{Q}_p$ (it is a closed metric ball.) By discreteness of the absolute value, it is also open: Let $c \in \mathbb{R}$ with $1 < c < p$. Then $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a| < c\}$.

We will show that $\mathbb{Z}_p$ is compact, which will imply that $\mathbb{Q}_p$ is locally compact because any open neighborhood of 0 in $\mathbb{Z}_p$ will have compact closure in $\mathbb{Z}_p$. In particular, the intersection of any basis about 0 with the open set $\mathbb{Z}_p$ will satisfy the condition of Exercise 1, (ii).

To prove compactness of $\mathbb{Z}_p$, it is enough to prove sequential compactness since $\mathbb{Z}_p$ is metric. We will do this by considering the "base-p" expansions from the end of the last section. Note that if $a \in \mathbb{Z}_p$, since $|a| \leq 1$, its expansion starts after the 0th place. So let $a_n \in \mathbb{Z}_p$ be a sequence, and write

$$a_n = \sum_{i=0}^{\infty} a_{i,n} p^i$$

with $a_{i,n} \in \{0, \ldots, p-1\}$ (the digit $a_{0,n}$ may be zero. For $\mathbb{F}_q[[x]]$, the "digits" are none other than the coefficients of a given power series.) Then there are infinitely many a_n with the same first digit $a_{0,n}$. Choose a subsequence of the a_n with the same first digit, call it a_{n_0}. Then repeat this process for the digit a_{1,n_0} to get another subsequence a_{n_1}, and so on. Then the sequence $\{a_{1_k}\}_{k=0}^{\infty}$ converges. Therefore $\mathbb{Z}_p$ is (sequentially) compact, and as we pointed out, this proves that $\mathbb{Q}_p$ is locally compact, hence a local field.

3 Structure of Local Fields

Now that we have shown that $\mathbb{Q}_p$ and $\mathbb{F}_q((t))$ are local fields, let us study local fields in general. *We will assume from now on that all local fields in question are nonarchimedean.* After all, this assumption only rules out the cases of $\mathbb{R}$ and $\mathbb{C}$ in the end.

We begin by attaching three pieces of data to a local field. These data will not exist in the archimedean case. Recall that we are taking for granted that every local field has an absolute value which determines its topology.

Proposition/Definition 3.1. *Let K be a local field.*

(1) We define the valuation ring *of K to be*

$$\mathcal{O}_K = \{a \in K \mid |a| \leq 1\}.$$

This is a discrete valuation ring. In particular, $\mathcal{O}_K$ is a local ring. Furthermore $\mathcal{O}_K$ is compact.

(2) The prime *of K is the set*

$$\mathfrak{p} = \{a \in K \mid |a| < 1\}.$$

The set $\mathfrak{p}$ is the principal prime ideal in the discrete valuation ring $\mathcal{O}_K$. Its generator is called a uniformizer *for K. Such a uniformizer is generally denoted π.*

(3) The residue field *of K is the residue field k of $\mathcal{O}_K$, i.e.,*

$$k = \mathcal{O}_K/\mathfrak{p}.$$

The field k is finite.

Proof. We proceed in several steps.

Step 1. We must first show that $\mathcal{O}_K$ is a ring. But this follows easily from the ultrametric

inequality, as it did for $\mathbb{Z}_p$ above. Similarly $\mathfrak{p}$ is an ideal in $\mathcal{O}_K$.

Step 2. Let us show that $\mathcal{O}_K$ is a local ring with maximal ideal $\mathfrak{p}$. Well, consider the set $\mathcal{O}_K \backslash \mathfrak{p}$. By definition,

$$\mathcal{O}_K \backslash \mathfrak{p} = \{a \in K \mid |a| = 1\}.$$

Therefore it follows from the multiplicativity of the absolute value on K that for any $a \in \mathcal{O}_K \backslash \mathfrak{p}$, we have $a^{-1} \in \mathcal{O}_K \backslash \mathfrak{p}$. Conversely, and for similar reasons, any element $b \in \mathfrak{p}$ has $|b^{-1}| > 1$, and is therefore not invertible in $\mathcal{O}_K$. Thus $\mathcal{O}_K \backslash \mathfrak{p} = \mathcal{O}_K^\times$. If follows that $\mathcal{O}_K$ is local with maximal ideal $\mathfrak{p}$.

Step 3. We now prove that $\mathcal{O}_K$ is compact. This will be a consequence of the local compactness of K. In fact, consider the metric balls

$$B_r = \{a \in K \mid |a| < r\}$$

for $r > 0$. By basic metric space theory, the B_r form a basis of neighborhoods about 0 in K. Therefore one of them, say B_s, is contained in a compact set E. Let $t = s/2$. Then the closed metric ball $C_t = \{a \in K \mid |a| \leq t\}$ is contained in E and is therefore compact. Let $t' = \max\{|a| \mid a \in C_t\}$, so that $C_t = C_{t'}$. Let $\alpha \in C_{t'}$ be an element of absolute value t'. Then multiplication by α^{-1} is a continuous map $C_{t'} \to \mathcal{O}_K$ which is easily seen to be a homeomorphism (its inverse is multiplication by α.) Since $C_{t'} = C_t$ is compact, so must be $\mathcal{O}_K$.

Step 4. Next we show that k is finite. This is not hard now that we have the compactness of $\mathcal{O}_K$: k is the set of cosets of $\mathfrak{p}$ in $\mathcal{O}_K$, and therefore $\mathcal{O}_K$ is the disjoint union of translates of $\mathfrak{p}$ indexed by k. Since $\mathfrak{p}$ is open and $\mathcal{O}_K$ is compact, the number of such translates must be finite; i.e., k is finite.

Step 5. Finally, we show that $\mathfrak{p}$ is principal, from which it follows that $\mathcal{O}_K$ is a discrete valuation ring. For this it is enough to show that the maximum

$$\max\{|a| \mid a \in \mathfrak{p}\}$$

exists. Indeed, if this is the case, let π be an element of $\mathfrak{p}$ whose absolute value is maximal. Then, similarly to what we saw at the end of Step 3, multiplication by π is a homeomorphism between $\mathcal{O}_K$ and $\mathfrak{p}$, i.e., $\mathfrak{p} = \pi\mathcal{O}_K$, as desired.

Now to show that the maximum above exists, it suffices to show that $\mathfrak{p}$ is compact. But this is not hard: We just saw that $\mathcal{O}_K$ is a finite disjoint union of copies of $\mathfrak{p}$. Therefore, $\mathfrak{p}$ is compact if and only if $\mathcal{O}_K$ is compact, which we know from Step 3. So we are done. □

Corollary 3.2. *Let K be a local field and $\pi \in K$ a uniformizer. Then every element of $K^\times$ can be written uniquely as $u\pi^n$ for $u \in \mathcal{O}_K^\times$ a unit and $n \in \mathbb{Z}$. Thus we have an isomorphism*

$$K^\times \cong \mathcal{O}_K^\times \times \mathbb{Z}.$$

(This isomorphism is not canonical because the $\mathbb{Z}$ factor depends on the choice of π.)

In the context above, it follows from this corollary that

$$K = \operatorname{Frac} \mathcal{O}_K = \mathcal{O}_K[\pi^{-1}].$$

Exercise 3. For $K = \mathbb{Q}_p$, we have that, by definition, $\mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p$. Prove that $\mathfrak{p} = p\mathbb{Z}_p$, and $k \cong \mathbb{F}_p$. Similar exercise for $\mathbb{F}_q((x))$.

Next, we come to the celebrated Lemma of Hensel.

Theorem 3.3 (Hensel's Lemma)**.** *Let K be a local field, and let $f(T) \in \mathcal{O}_K[T]$ be a polynomial with coefficients in $\mathcal{O}_K$. Let $\tilde{f}(T) \in k[T]$ be the reduction of this polynomial modulo $\mathfrak{p}$, i.e., reduce the coefficients of f modulo $\mathfrak{p}$. Assume $\alpha \in k$ is simple root of $\tilde{f}$, i.e., $\tilde{f}(\alpha) = 0$ and $\tilde{f}'(\alpha) \neq 0$. Then there exists $a \in \mathcal{O}_K$ such that $f(a) = 0$ and $a \equiv \alpha \pmod{\mathfrak{p}}$*

Proof. See Milne [4], Theorem 7.33 for a proof of a more general statement. □

As a nice application of Hensel's Lemma, we have the following exercise, which I highly recommend doing if you have not seen it already.

Exercise 4. Show that $\mathbb{Z}_p$ contains the $(p-1)$st roots of unity, and they are all distinct modulo p.

4 Extensions of Local Fields

We begin by stating a theorem which says, for one, that extensions of local field are still local fields.

Theorem 4.1. *Let K be a (nonarchimedean) local field with absolute value $|\cdot|$, and let L/K be a finite extension. Then there is a unique absolute value $|\cdot|_L$ on L which extends the one on K, and it makes L a local field. Furthermore, $|\cdot|_L$ is given by the formula*

$$|\alpha|_L = |\operatorname{Nm}_{L/K}(\alpha)|^{1/n}$$

where $n = [L : K]$.

Proof. The best proof of this fact that I have found, given what has been developed so far in these notes, is in Neukirch [5], Chapter II, Theorem 4.8. I may come back and include a proof later. □

Let L/K be a extension of local fields which, for safety, I will assume to be separable. There are two useful pieces of data which one can attach to L/K. Let π_K be a uniformizer for K and π_L one for L. Then by Corollary 3.2 we can write $\pi_K = u\pi_L^e$ for unique $u \in \mathcal{O}_L^\times$ and $e \in \mathbb{Z}$. In fact, it is easy to see that we must have $e \geq 1$. If we change π_K or π_L, then this formula will only change by a unit, so e does not depend on the choice of uniformizers. The number e is called the *ramification index* of L/K.

Another useful piece of information comes from the residue fields. Let $\mathfrak{p}_K$ be the prime in K and $\mathfrak{p}_L$ that in L. Note that $\mathcal{O}_K \subset \mathcal{O}_L$ and $\mathfrak{p}_K \subset \mathfrak{p}_L$ (because, by the uniqueness in Theorem 4.1, if $a \in K$ with $|a| \leq 1$, then $|a| \leq 1$ in L also. Similarly for strict inequality.) Thus there is an inclusion of fields $\mathcal{O}_K/\mathfrak{p}_K \subset \mathcal{O}_L/\mathfrak{p}_L$. The degree $[\mathcal{O}_L/\mathfrak{p}_L : \mathcal{O}_K/\mathfrak{p}_K]$ is called the *inertia degree* of L/K, and it is traditionally denoted by f.

We have the following theorem, which holds for general Dedekind domains.

Theorem 4.2. *Let L/K be a finite separable extension of local fields, and let e and f be, respectively, the ramification index and inertia degree. Then*

$$[L/K] = ef.$$

Proof. We will see this in a more general context later, so I will omit the proof. □

Definition 4.3. Let L/K be a finite separable extension of local fields with ramification index e. We call L/K *unramified* if $e = 1$. We say L/K is *totally ramified* if $e = [L : K]$.

Example 4.4. For an example of a totally ramified extension of local fields, consider the extension field $K = \mathbb{Q}_p(p^{1/n})$ of $\mathbb{Q}_p$. Let $|\cdot|$ denote the absolute value on $\mathbb{Q}_p$ which we have been using above, and let $|\cdot|$ also denote its unique extension to K. We will compute the uniformizer of K and its residue field. We know from Exercise 3 that p is a uniformizer for $\mathbb{Q}_p$. Also we have $(p^{1/n})^n = p$. We can therefore conclude that the ramification index e of $K/\mathbb{Q}_p$ is at least n: if $p^{1/n}$ is a uniformizer then e is exactly n by definition. Otherwise $p^{1/n}$ is, up to unit, a power of a uniformizer of K, in which case e is even bigger. However, $[K : \mathbb{Q}_p] \leq n$. Thus we have

$$n \leq e \leq ef = [K : \mathbb{Q}_p] \leq n,$$

which forces all of these quantities to be equal. Thus we conclude

$$[K : \mathbb{Q}_p] = n, \qquad e = n, \qquad f = 1$$

and also that $p^{1/n}$ is a uniformizer of K, and finally that the residue field of K is $\mathbb{F}_p$.

Example 4.5. For an example of an unramified extension of local fields, consider $\mathbb{F}_{q^n}((x))/\mathbb{F}_q((x))$. Since $\mathbb{F}_{q_n}/\mathbb{F}_q$ is an extension of degree n, tensoring with $\mathbb{F}_q((x))$, for instance, shows that $\mathbb{F}_{q^n}((x))/\mathbb{F}_q((x))$ is an extension of degree n. We see easily that $f = n$ for this extension, and therefore $e = 1$, i.e., this extension is unramified.

The analogue of this extension in characteristic zero is $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ where $p \nmid n$ and ζ_n is a primitive nth root of unity. Indeed, such an extension is unramified. I will omit the proof of this fact since I cannot think of one at the moment which does not pass through the theory of number fields.

5 Some Galois Theory of Local Fields

The goal of this section is to prove the following theorem.

Theorem 5.1. *Let L/K be an unramified Galois extension of local fields. Then L/K is cyclic.*

Proof. Since L/K is unramified, $f = [L : K]$ and $e = 1$, where e and f are, respectively, the ramification index and inertia degree. Let π be a uniformizer for K. Then this says π is a uniformizer for L and $[\mathcal{O}_L/\pi\mathcal{O}_K : \mathcal{O}_K/\pi\mathcal{O}_K] = [L : K]$. For convenience, write $l = \mathcal{O}_L/\pi\mathcal{O}_K$ and $k = \mathcal{O}_K/\pi\mathcal{O}_K$ for the residue fields.

Now let $\sigma \in \mathrm{Gal}(L/K)$. From the explicit description of the absolute value of L in

Theorem 4.1, it is easy to see that $|\sigma a| = |a|$ for all $a \in L$. Thus σ restricts to an automorphism of $\mathcal{O}_L$ preserving $\mathcal{O}_K$ pointwise. Since $\pi \in K$, $\sigma\pi = \pi$, and hence, reducing modulo π, we see that σ induces an automorphism of l over k which fixes k. In other words, we have defined a homomorphism $\varphi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(l/k)$. We want to show that this is an isomorphism. Since these groups have the same order f, it is enough to show injectivity of φ.

To see this, let g be the minimal polynomial over k of a generator α of $l^\times$. Then $g(x) = (x-\alpha)(x-\sigma\alpha)\cdots(x-\sigma^{f-1}\alpha)$ and all the $\sigma^i\alpha$ are distinct in l, and none of them are in k. Let G be a polynomial in $\mathcal{O}_K[x]$ which reduces to g modulo π. The G is irreducible because its reduction modulo π is. By Hensel's Lemma, G has n distinct roots in $\mathcal{O}_L$ which are congruent to the roots of g modulo π. Thus, if a is a root of G, then $L = K(a)$. But $\mathrm{Gal}(L/K)$ permutes the roots of G transitively, and hence the image of $\mathrm{Gal}(L/K)$ in $\mathrm{Gal}(l/k)$ permutes the roots of g transitively. Thus since there are f roots g and f elements in $\mathrm{Gal}(L/K)$, it follows that φ is injective, hence an isomorphism. Since $\mathrm{Gal}(l/k)$ is cyclic, this completes the proof. □

In the setting of the above proof, let $\tau \in \mathrm{Gal}(l/k)$ be the element $\alpha \mapsto \alpha^q$, where $q = |k|$. Then τ generates $\mathrm{Gal}(l/k)$. The element $\varphi^{-1}(\tau) \in \mathrm{Gal}(L/K)$ is called the *Frobenius element*. It is denoted by Frob and it characterized by the condition that $\mathrm{Frob}\, a \equiv a^q \pmod{\pi}$. This element plays a very important role in class field theory.

I have included more references than those cited above. They are all good sources for reading about algebraic number theory and related topics.

References

[1] J. W. S. Cassels and A. Frohlich, *Algebraic Number Theory*. Academic Press, London, 1967

[2] S. Lang, *Algebraic Number Theory*, Second Edition. Graduate Texts in Mathematics 84. Springer-Verlag, Berlin, 1994.

[3] D. Marcus, *Number Fields*. Universitext. Springer-Verlag, Berlin, 1977.

[4] J. S. Milne, *Algebraic Number Theory*. http://www.jmilne.org/math/CourseNotes/ANT.pdf.

[5] J. Neukirch, *Algebraic Number Theory*. Grundlehren der Mathematischen Wissenschaften 322. Springer-Verlag, Berlin, 1999.

[6] D. Ramakrishnan and R. Valenza, *Fourier Analysis on Number Fields*. Graduate Texts in Mathematics 186. Springer-Verlag, Berlin, 1999.

[7] M. Rosen, *Number Theory in Function Fields*. Graduate Texts in Mathematics 210. Springer-Verlag, Berlin, 2002.

[8] J.-P. Serre, *Local Fields*. Graduate Texts in Mathematics 67. Springer-Verlag, Berlin, 1979.

[9] A. Weil, *Basic Number Theory*. Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete 144. Springer-Verlag, Berlin, 1967.