LOCAL FIELDS AND p-ADIC NUMBERS

HANLEI WEN

Abstract. This paper will use p-adic numbers as a motivation to develop more general results, including investigating Hensel's Lemmas and Ostrowski's Theorem, among others. In doing so, it will attempt to provide a solid foundation for more in-depth algebraic number theory. To avoid overly tedious exposition, this paper will assume basic familiarity with abstract algebra and analysis, at the level of introductory undergraduate courses.

Contents

1. Introduction

I started off the REU program very ambitious, attempting to read Prof. Ngô Bảu Châu's lecture notes on representation of p-adic reductive groups. Then swiftly, very swiftly, I faced a big problem – I did not even understand the first sentence. Trying to comprehend what was going on, I quickly found myself entangled with a much more foundational topic (local fields) that slowly turned out to be very important in algebraic number theory.

This paper will attempt to organize what I have studied in the last two and a half months; it will move toward the final goal of classifying local fields, using the p-adic numbers as a key motivation throughout the process; to avoid being a conglomeration of random but important facts, it will also leave out some important things that I have picked up along the way, including facts about discrete valuation

rings, dedekind domains and a bit of ramification theory. I recommend to read [9] if you are interested.

As this paper ultimately intends to be an introduction for someone beginning in algebraic number theory, it will attempt to be rather self–contained (such as reminding key definitions along the way). For the same purpose, it will use p–adic number examples as a motivation for the more abstract concepts involved. That being said, to avoid being overly tedious, basic familiarity with abstract algebra and analysis will be assumed.

Finally, enjoy! Hope you learn a bit more about p–adic numbers and local fields (or at least find the topic interesting).

2. Basic Ring and Field Theory

There are a few basic definitions that any study of local fields will require. For the sake of reminding the reader, I will briefly overview relevant background material. For more detail, see [4] or [6].

Definition 2.1. Let R be a ring. A subset $I \subset R$ is a **left ideal** if

(i) I is an abelian subgroup of R
(ii) $ra \in I$ for all $a \in I, r \in R$

A right ideal is defined analogously.
A subset is an **ideal** if it is both a left and a right ideal.
An ideal is **principal** if it is generated by 1 element.
An ideal $I \subset R$ is **maximal** if for every other ideal $J \supset I$, then $J = R$.
An ideal is **prime** if for all $a, b \in R, ab \in I$ implies either $a \in I$ or $b \in I$.

The following definition is equally fundamental and important.

Definition 2.2. Let R be a ring. A left $R-$module or a left module over R is a set M together with

(i) a binary operation $+$ on M under which M is an abelian group
(ii) an action of R on M (that is, a map $R \times M \to M$) denoted by rm, for all $r \in R$ and for all $m \in M$ which satisfies
  (a) $(r + s)m = rm + sm$ for all $r, s \in R$ and $m \in M$
  (b) $(rs)m = r(sm)$ for all $r, s \in R$ and $m \in M$
  (c) $r(m + n) = rm + rn$ for all $r \in R$ and $m, n \in M$
  (d) $1m = m$ where $1 \in R$ is the identity and $m \in M$

Note that all ideals $I \subset R$ can be viewed as $R-$modules. Recall also the following definitions.

Definition 2.3. A **field** F is a commutative division ring, i.e. multiplication on F is commutative and all $a \neq 0 \in F$ have inverses.

$\mathbb{R}$ and $\mathbb{C}$ are common examples of fields that we are familiar with.

Definition 2.4. A ring R is an **integral domain** if it is commutative, has a multiplicative identity and has no zero divisors i.e. $ab = 0$ implies either $a = 0$ or $b = 0$. An integral domain R is a **principal ideal domain (PID)** if every ideal is principal.

Definition 2.5. Let R be a ring and M be a module. M is **Noetherian** if every submodule is finitely generated. Equivalently, M is Noetherian if every ascending chain of submodules of M,

$$M_1 \subset M_2 \subset M_3 \subset \dots$$

eventually stabilizes (see pg. 413, [6]). Note that an ideal $I \subset R$ can always be considered as an $R-$module.

It is important the the reader is comfortable with these definitions (and the corresponding related material), as they will be treated as background knowledge in the following exposition.

3. Valued Fields

3.1. **Absolute Values and Valuations.** Given any arbitrary field F, we can assign certain non-negative values in $\mathbb{R}$ to elements of F. The following definitions formalize this idea.

Definition 3.1. Let K be a field. An **absolute value** on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that

(i) $|x| \geq 0 \quad \forall x \in K$ with equality iff $x = 0$
(ii) $|xy| = |x| \cdot |y|$ for all $x, y \in K$
(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in K$

An absolute value is trivial if $|x| = 1$ for all non-zero $x \in K$. Moreover, it follows from the definition above and the property of fields that $|1| = 1, |-1| = 1$ and $|-x| = |x| \quad \forall x \in K$. This definition of absolute value should feel familiar. Criteria (iii) in particular is the common and useful $\triangle$-inequality. We can change the $\triangle-$inequality into a much stronger inequality to obtain interesting results.

Definition 3.2. An absolute value is called non-archimedean if

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

for all $x, y \in K$. Otherwise, it is called archimedean.

Example 3.3. Given any

$$x = p^n \cdot \frac{a}{b} \in \mathbb{Q}^\times$$

with $a, b \in \mathbb{Z}$ not divisible by p, the absolute value defined by $|x|_p = p^{-n}$ is non-archimedean. The usual absolute value on $\mathbb{Q}$, which we may sometimes denote as $|\cdot|_\infty$ in this exposition, is archimedean.

Suppose $|\cdot|$ is non-archimedean and suppose $|x| < |y|$. Then

$$|y| = |y + x - x| \leq \max\{|x + y|, |x|\}$$

In particular, $|y| > |x|$ implies $|y| \leq |x + y|$. By definition of a non-archimedean absolute value, we also have $|x+y| \leq \max\{|x|, |y|\} = |y|$. It follows that $|x+y| = |y|$.

Lemma 3.4. *Let $(K, |\cdot|)$ be a non-archimedian valued field. If (x_n) is a sequence in K such that $|x_n - x_{n+1}| \to 0$ as $n \to \infty$ then (x_n) is Cauchy.*

Proof. Fix $\epsilon > 0$. Find N such that $n > N \implies |x_n - x_{n+1}| < \epsilon$. Then, for any $n, m > N$, we have

$$\begin{aligned} |x_n - x_m| &= |x_n - x_{n+1} + x_{n+1} - x_{n+2} + \ldots + x_{m-1} - x_m| \\ &\leq \max_{i \in [n, m-1]} \{|x_i - x_{i+1}|\} < \epsilon \end{aligned}$$

□

Lemma 3.4 simplifies the verification of whether or not a sequence is Cauchy and provides us with a luxury we do not have with Cauchy sequences in $\mathbb{R}$. The following examples hopefully provide more insight into what fields with non-archimedean absolute values look like.

Example 3.5. Recall from Example 3.3 the absolute value $|\cdot|_p$. Let us verify that this absolute value is non-archimedean. Take $a_1 = p^{k_1} \cdot \frac{b_1}{c_1}, a_2 = p^{k_2} \cdot \frac{b_2}{c_2}$. We know that $|a_1|_p = p^{-k_1}, |a_2|_p = p^{-k_2}$. WLOG, $k_1 \leq k_2$. Then,

$$a_1 + a_2 = p^{k_1} \cdot \left(\frac{b_1 c_2 + p^{k_2 - k_1} b_2 c_1}{c_1 c_2} \right)$$

In particular, $p \nmid c_1, c_2$ implies $|a_1 + a_2|_p \leq p^{-k_1} = |a|_p$.

Exercise 3.6. Which of the following sequences in $\mathbb{Q}$ are Cauchy sequences with respect to the given absolute value? Prove your answer.

1. (n) w.r.t. $|\cdot|_3$
2. $\left(\frac{1}{n}\right)$ w.r.t. $|\cdot|_5$
3. $(5 \cdot 7^n)$ w.r.t. $|\cdot|_5$

There is another rather standard method of thinking about values.

Definition 3.7. A valuation of a field K is a function $v : K^\times \to \mathbb{R}$ such that $\forall x, y \in K$

(i) $v(xy) = v(x) + v(y)$
(ii) $v(x + y) \geq \min(v(x), v(y))$

Observe that in the definition we do not evaluate on 0. Conventionally, however, we set $v(0) = \infty$. To provide more intuition, consider the following example.

Example 3.8. Define $v : \mathbb{Q}^\times \to \mathbb{R}$,

$$v(x) = v\left(p^k \cdot \frac{a}{b}\right) = k$$

for $x = p^k \cdot \frac{a}{b}$ where $p \nmid a, b$. Here, we can think of the function v as simply extracting the power of p contained within a rational number.

It turns out these two definition are actually equivalent. More rigorously, for each absolute value defined on a field K, we can induce a valuation by $v : K^\times \to \mathbb{R}, v(x) = -\log|x|$. Similarly, for each valuation defined on $K^\times$, we can induce an absolute value by fixing some $\alpha > 1$, setting $|0| = 0$ and letting $|x| = \alpha^{-v(x)}$.

Exercise 3.9. Verify that the above definitions satisfy the axioms for absolute values and valuations.

3.2. **Topology of the Valued Field.** Unless otherwise specified, K will represent an arbitrary field for this subsection. From undergraduate analysis class, we know that any absolute value induces a topology on a field – that is, basic open sets are of the form $B(x,r) = \{y \in K \mid |x-y| < r\}$.

Definition 3.10. Let $|\cdot|, |\cdot|'$ be absolute values on K. $|\cdot|, |\cdot|'$ are equivalent if the induced topologies are the same.

The following proposition simplifies the verification of absolute value equivalence.

Proposition 3.11. *Let $|\cdot|, |\cdot|'$ be non-trivial absolute values on K. The following are equivalent:*

(i) $|\cdot|, |\cdot|'$ *are equivalent*
(ii) $|x| < 1$ *iff* $|x|' < 1$ $\forall x \in K$
(iii) $\exists c \in \mathbb{R}_{>0}$ *s.t.* $|x|^c = |x|'$ $\forall x \in K$

Proof. $(i) \implies (ii)$ Observe that $|x| < 1$ iff $x^n \to 0$ w.r.t. $|\cdot|$. It suffices to show that $x^n \to 0$ w.r.t $|\cdot|'$ (the other direction is analogous). Fix $\epsilon > 0$. The ball

$$D(0,\epsilon) = \{x \mid |x|' < \epsilon\}$$

is open by assumption, so we can find some $\epsilon' \leq \epsilon$ such that

$$B(0,\epsilon') = \{x \mid |x| < \epsilon'\} \subset D(0,\epsilon)$$

Find N such that $n > N \implies x^n \subset D_\epsilon(0)$. Then the same N satisfies $n > N \implies x^n \in B(0,\epsilon') \subset B(0,\epsilon)$.

$(ii) \implies (iii)$ Let $a \in K^\times$ such that $|a| > 1$. We want to show that $\frac{\log|x|}{\log|x|'}$ is fixed. It suffices to show that for any $x \in K$, we have

$$\frac{\log|x|}{\log|a|} = \frac{\log|x|'}{\log|a|'}$$

Let $\frac{m}{n} \in \mathbb{Q}$ such that $\frac{\log|x|}{\log|a|} < \frac{m}{n}$. Then, it follows that $|a|^{\frac{m}{n}} = |x| \iff |a|^m = |x|^n \iff \left|\frac{x^n}{a^m}\right| < 1$. By (ii), it follows that $\left|\frac{x^n}{a^m}\right|' < 1$. By the same chain of equivalences, $\frac{\log|x|'}{\log|a|'} < \frac{m}{n}$. This holds for any rational number larger than $\frac{\log|x|}{\log|a|}$, so in fact $\frac{\log|x|'}{\log|a|'} \leq \frac{\log|x|}{\log|a|}$. The other direction holds analogously.

$(iii) \implies (i)$ Clear since $|x|^c$ is cts for any $c \in \mathbb{R} > 0$. □

This proposition establishes that equivalent absolute values on a field are powers of each other. This is a crucial property that will become very useful later in the classification of absolute values on $\mathbb{Q}$. Reverting back to non-Archimedean absolute values, we find interesting results from the unconventional way these absolute values are defined.

Lemma 3.12. *Let $x \in (K, |\cdot|)$ where $|\cdot|$ is non-Archimedean and $r \in \mathbb{R}_{>0}$. Define*

$$B(x,r) = \{y \in K \mid |y-x| < r\}$$
$$\overline{B}(x,r) = \{y \in K \mid |y-x| \leq r\}$$

Then we have:

(i) If $z \in B(x,r)$, then $B(z,r) = B(x,r)$.
(ii) If $z \in \overline{B}(x,r)$, then $\overline{B}(z,r) = \overline{B}(x,r)$.

(iii) $B(x,r)$ *is closed.*
(iv) $\overline{B}(x,r)$ *is open.*

Proof.
(i) Let $y, z \in B(x,r)$. We want to show $y \in B(z,r)$. Observe

$$|y-z| \leq \max\{|y-x|, |x-z|\} \leq r$$

(ii) is analogous.
(iii) Take $y \in B(x,r)^c$. The case $|y-x| > r$ is handled by the $\triangle-$ineq. For $|y-x| = r$, pick $r' < r$. Then for all $z \in B(y,r')$ we have

$$|x-y| = r \leq \max\{|z-x|, |z-y|\}$$

but $|z-y| < r' < r$ and hence $|z-x| \geq r$. Therefore, $z \in B(x,r)^c$.
(iv) follows analogously. □

Observe that we write $\overline{B}(x,r)$ instead of $\overline{B(x,r)}$. Unlike working in $\mathbb{R}$, $\overline{B}(x,r)$ is not the closure of $B(x,r)$. The latter is already closed.

Example 3.13. The p-adic numbers provide some intuition for these results. Take

$$x_1 = p^{n_1} \cdot \frac{a_1}{b_1},\ x_2 = p^{n_2} \cdot \frac{a_2}{b_2},\ x_3 = p^{n_3} \cdot \frac{a_3}{b_3}$$

and suppose that $x_2, x_3 \in B(x_1, r)$. Then $v(x_1 - x_2), v(x_1 - x_3) > -\log(r)$. In other words, both $x_1 - x_2, x_1 - x_3$ have a power of p greater than $-\log(r)$. It follows that their difference $x_2 - x_3$ also has a power of p greater than $-\log(r)$.

Moreover, I will point out that $(iii), (iv)$ imply that all open and closed balls are in fact clopen. Note that because of this reason, we actually have $\overline{B(0,1)} = B(0,1) \neq \overline{B}(0,1)$. With this in mind, let us make the following key definitions.

Definition 3.14. Let $(K, |\cdot|)$ be a non-Archimedean valued field. Let

$$O_K = B(0,1) = \{x \in K \mid |x| \leq 1\} = \{x \in K \mid v(x) \geq 0\}$$

$$m = \overline{B}(0,1) = \{x \in K \mid |x| < 1\} = \{x \in K \mid v(x) > 0\}$$

O_K is called the **valuation ring** of K. It it left to the reader to verify that O_K is a subring of K and that m is the unique maximal ideal of O_K (hint: consider units).

Definition 3.15. A valuation v on K is discrete if $v(K^\times) \cong \mathbb{Z}$. If $\pi \in K^\times$ is such that $v(\pi) > 0$ and $v(\pi)$ generates $v(K^\times)$, then π is called a uniformizer.

Note that such a π always exists, since the definition requires $v(K^\times)$ isomorphic to $\mathbb{Z}$. As a result, we have the following Lemma.

Lemma 3.16. *If v is a discrete valuation on K with uniformizer π, then $\forall x \in K^\times$, $\exists$ unique $n \in \mathbb{Z}, v \in O_K^\times$ such that $x = \pi^n u$.*

Proof.
(Existence) Pick $n = v(x)$, $u = \frac{x}{\pi^n}$ and observe that $v(u) = 0$.
(Uniqueness) Suppose $x = \pi^{n_1} u_1 = \pi^{n_2} u_2$. We have the following chain of implications. Since $u_1, u_2 \in O_K^\times$, then $u_1^{-1}, u_2^{-1} \in O_K$ by definition. Moreover,

$$0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1}) \implies v(x^{-1}) = -v(x)$$

Applied to u_1 we see $v(u_1) \geq 0$ and $-v(u_1) = v(u_1^{-1}) \geq 0$. Hence, $v(u_1) = 0$. The same is true for $v(u_2)$. In particular, this implies $n_1 = v(\pi^{n_1}u_1) = v(\pi^{n_2}u_2) = n_2$. Then we have $\pi^{n_1}u_1 = \pi^{n_1}u_2$ which implies $u_1 = u_2$ by inverting π. □

We end off this section with a proposition that characterizes discretely valued fields.

Proposition 3.17. *Let (K, v) be a valued field. The following are equivalent.*

(i) v is discrete
(ii) O_K is a principal ideal domain (PID)
(iii) O_K is Noetherian
(iv) m is principal

Proof.
$(i) \implies (ii)$ O_K is an integral domain since it is a subring of K. Take ideal I s.t. $0 \neq I \subset O_K$. Let $x \in I$ with $v(x)$ minimal (this is possible since $v(O_K) \cong \mathbb{N} \cup \{0\}$). $xO_K \subset I$ since I is an ideal. Now, take any $y \in I$. We know $v(y) \geq v(x)$ and hence $v(x^{-1}y) = -v(x) + v(y) \geq 0 \implies x^{-1}y \in O_K$. It follows that $y = xx^{-1}y \in xO_K$ and hence $I \subset O_K$. This proves $I = xO_K$ and hence O_K is a PID.

$(ii) \implies (iii)$ by definition.

$(iii) \implies (iv)$ m is finitely generated by hypothesis. Suppose $m = (x_1, \ldots, x_n)$. Let $\min_i \{v(x_i)\} = v(x_j)$. Then observe that $x_j^{-1}x_i \in O_K$ by the same argument of $(i) \implies (ii)$. It follows that $x_i \in x_jO_K$. This holds for all i so in fact m is generated by (x_j). That is, m is principal.

$(iv) \implies (i)$ Let $m = \pi O_K$ and $v(\pi) = c$. If $x \in m$ then $v(x) \geq c \implies v(K^\times) \cap (0, c) = \emptyset \implies v(K^\times) = c\mathbb{Z}$. □

4. p-ADIC NUMBERS

In the previous section, p-adic numbers were used to motivate and provide intuition for many abstract definitions. They will continue to be provide intuition for further topics such as local fields, and so a more rigorous and substantial excursion to the basics of p-adic numbers will prove to be helpful.

Definition 4.1. Let $|\cdot|_p$ be the absolute value defined on $\mathbb{Q}$ in Example 3.2. The p-adic numbers, or $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

When $K = \mathbb{Q}_p$, we say $O_K = \mathbb{Z}_p$. $\mathbb{Z}_p$ is also known as the p-adic integers. Let $a, b \in \mathbb{Z}$. Then $\frac{a}{b} \in \mathbb{Z}_p$ for $p \nmid b$. Moreover, $\frac{a}{b \cdot p^n} \notin \mathbb{Z}_p$ for $n > 0$. Can we say more? The following lemmas and definitions will help us break down $\mathbb{Z}_p$ and $\mathbb{Q}_p$ even more.

Lemma 4.2. *Let (a_n) be a sequence in $\mathbb{Q}_p$. $\sum_{n=0}^{\infty} a_n$ converges iff $\lim_{n\to\infty} a_n = 0$.*

Proof. $(\Rightarrow)$ is trivial (same proof as $\mathbb{R}$). $(\Leftarrow)$ Apply Lemma 3.4. □

Exercise 4.3. Prove: any series in the form $\sum_{n=n_0}^{\infty} a_n p^n$ with $a_n \in \{0, \ldots, p-1\}$ and $n_0 \in \mathbb{Z}$ converges in $\mathbb{Q}_p$.

This exercise provides motivation for the following definition.

Definition 4.4. A p-adic expansion of $a \neq 0 \in \mathbb{Q}_p$ is

$$a = \sum_{n=n_0}^{\infty} a_n p^n$$

where $n_0 \in \mathbb{Z}, a_{n_0} \neq 0$ and $a_n \in \{0, \ldots, p-1\}\ \forall n \geq n_0$. We call a_n the coefficients of the expansion.

For the special case of $a = 0$, a conventional approach is to allow $a_{n_0} = 0$. In this case, any expansion starting at any integer $z \in \mathbb{Z}$ with all coefficients equal to 0 can be viewed as a p-adic expansion of 0. Note that in the case of 0, we do not have $v(0) = n_0$ since n_0 can be completely arbitrary (recall that we set $v(0) = \infty$).

Example 4.5. Write out the 2-adic expansion of -1. Let $-1 = \sum_{n=n_0}^{\infty} a_n 2^n$. We know that $n_0 = 0$ since $v(-1) = 0$. Moreover,

$$1 + (-1) \equiv 0 \pmod 2 \implies 1 + a_0 2^0 \equiv 0 \pmod 2 \implies a_0 = 1$$
$$1 + (-1) \equiv 0 \pmod 2 \implies 1 + 2^0 + a_1 2^1 \equiv 0 \pmod 2 \implies a_1 = 1$$
$$\vdots$$
$$1 + (-1) \equiv 0 \pmod 2 \implies 1 + \sum_{k=0}^{n-1} 2^k + a_n 2^n \equiv 0 \pmod 2 \implies a_n = 1$$

and therefore $-1 = \sum_{n=0}^{\infty} 2^n$.

Observe how -1 has an infinite but periodic expansion. In fact, the following property holds.

Theorem 4.6. *A p-adic number has an eventually periodic p-adic expansion iff it is rational.*

Proof. See [8], pg. 1-2 or [2], pg. 3-5. □

Try the following exercises to familiarize with p-adic expansions and arithmetic.

Exercise 4.7. Compute:

(i) The 5-adic expansion of $\frac{7}{2}$
(ii) $\overline{65351}_7 + \overline{32142}_7$
(iii) $(1222)_3 \cdot (1111)_3$

Note that if $a \in \mathbb{N}$, then the p-adic expansion of a is the same as the base p representation of a. Moreover, it turns out that every p-adic number has a unique p-adic expansion (see [5], pg. 82-83). Observe that any non-zero $x \in \mathbb{Z}_p$ if and only if the $p-$adic expansion of x has $n_0 \geq 0$. It will be left as an exercise to the reader to check that $\mathbb{Z}_p$ is the completion of $\left\{\frac{a}{b},\ a, b \in \mathbb{Z} \mid p \nmid b\right\}$.

Theorem 4.8. *Let $K = \mathbb{Q}_p$, the p-adic field. Then $k = O_K/m = \mathbb{F}_p$ where $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.*

Proof. Any $x \in m$ must have $v(x) \geq 1$ and so $v(xp^{-1}) \geq 0$. This implies $x \in p\mathbb{Z}_p$. We also know that m is an ideal so in fact $m = p\mathbb{Z}_p$. Since $O_K = \mathbb{Z}_p$, we have $k = \mathbb{Z}_p/p\mathbb{Z}_p$. Therefore, it simply suffices to show that $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$.

Take any $x \in \mathbb{Z}_p$. We know that any such x can be written as $\sum_{n=0}^{\infty} a_n p^n$. Define $\pi(x) : \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$ by

$$\pi(x) = \pi\left(\sum_{n=0}^{\infty} a_n p^n\right) = a_0$$

π is a surjective ring homomorphism (verifying this is a matter of addition and multiplication practice in $\mathbb{Q}_p$). The kernel of π is $p\mathbb{Z}_p$. By the First Ring Isomorphism Theorem (see pg. 243, [4] if unfamiliar), we have $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ as desired. □

Proposition 4.9. *In $\mathbb{Q}_p$, any open ball is closed (and vice versa). Therefore, $\mathbb{Q}_p$ is totally disconnected and $\mathbb{Z}_p$ is clopen.*

Proof. Follows from Lemma 3.12. □

Theorem 4.10. *$\mathbb{Z}_p$ is compact.*

Proof. Take $(a^n) \in \mathbb{Z}_p$. We can write $a^n = \sum_{k=0} a_k^n p^n$. Find $b_0 \in \{0, \ldots, p-1\}$ such that there are infinitely many $n \in \mathbb{N}$ with $a_0^n = b_0$. Let (a^{1n}) be the subsequence of (a^n) where each $a_0^{1n} = b_0$. Find $b_1 \in \{0, \ldots, p-1\}$ such that there are infinitely many $n \in \mathbb{N}$ with $a_1^{1n} = b_1$. Let (a^{2n}) be the subsequence of (a^{1n}) where each $a_1^{2n} = b_1$.

Repeat to construct $(a^{kn}), b_k$ for each $k \in \mathbb{N}$. Now, take the subsequence (a^{nn}) of (a^n) – that is, the first element is a^{11}, the second a^{22}, etc. We have $(a^{nn}) \to \sum_{k=0}^{\infty} b_k p^k$. □

Corollary 4.11. *$\mathbb{Q}_p$ is locally compact.*

Proof. $\forall x \in \mathbb{Q}_p$, take the neighborhood $x + \mathbb{Z}_p$. □

I will end this section by commenting that $\mathbb{Q}_p$ in fact has some very intriguing "geometric" properties. For example, one can show that any three points in $\mathbb{Q}_p$ form an isosceles triangle. Moreover, if this isosceles triangle is not equilateral, then its base (i.e. the side with a different length from the others) is the shortest side. For proof and more results, see [7].

5. Complete Valued Fields

Where $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$, we saw in the previous section that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. There are in fact many more properties of $\mathbb{Q}_p$ or – more generally – complete valued fields that are worthy of interest.

5.1. Hensel's Lemma.

Let us recall an important definition from ring theory.

Definition 5.1. Let R be a ring. The polynomial ring $R[x]$ is the set of polynomials with coefficients in R. More formally, $\forall f(x) \in R[x]$, we have

$$f(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_n \cdot x^n$$

In addition, for this $f(x)$ we define its "formal derivative" $f'(x)$ as

$$f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$$

Lemma 5.2. *(Hensel's Lemma) Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(x) \in O_K[x]$ and assume $\exists a \in O_K$ such that $|f(a)| < |f'(a)|^2$. Then $\exists$ unique $t \in O_K$ such that $f(t) = 0$ and $|t - a| < |f'(a)|$.*

Proof. (Existence) $\exists$ uniformizer $\pi \in O_K[x]$. Let $r = v(f'(a))$. We will use this to construct a Cauchy sequence that convergers to our desired t. Specifically, we construct a sequence (t_n) in O_K such that (i) $f(t_n) \equiv 0 \pmod{\pi^{n+2r}}$ and (ii) $t_n \equiv t_{n+1} \pmod{\pi^{r+n}}$. Property (ii) will be used to show that the sequence is Cauchy. Property (i) will be needed to ensure that, at the limit t, we have $f(t) = 0$ and $|t - a| < |f'(a)|$. The following exposition recounts the specifics.

We proceed by induction. Take $t_1 = a$. Observe that $f'(a) = \pi^r u$. By assumption, we have

$$|f(a)| < |f'(a)|^2 \implies v(f(a)) > 2v(f'(a)) = 2r$$

In particular, $v(f(a)) \geq 2r + 1$. It follows that $f(t_1) = f(a) \equiv 0 \pmod{\pi^{1+2r}}$, proving (i).

Suppose we have $t_1, \ldots, t_n$ satisfying (i) and (ii). Define

$$t_{n+1} = t_n - \frac{f(t_n)}{f'(t_n)}$$

We now check that t_{n+1} satisfies (i) and (ii). By (ii), $t_n \equiv t_1 \pmod{\pi^{r+1}}$. Observe that the equivalence is preserved under applying f'. That is, $f'(t_n) \equiv f'(t_1) \pmod{\pi^{r+1}}$. In particular, we know that $v(f'(t_1)) = r$ so

$$v(f'(t_n)) = r \iff f'(t_n) = \pi^r \cdot u \text{ for some } u \in O_K^\times$$

Moreover, $f(t_n) \equiv 0 \pmod{\pi^{n+2r}}$ by (ii) $\implies f(t_n) = \pi^k \cdot v$ for some $k \geq n + 2r$ and $v \in O_K^\times$. Then,

$$\frac{f(t_n)}{f'(t_n)} = \pi^{k-r} \cdot \frac{v}{u}$$

Since $k - r \geq n + r$ and $\frac{v}{u} \in O_K^\times$, this means that $\frac{f(t_n)}{f'(t_n)} \equiv 0 \pmod{\pi^{n+r}}$. In other words, modulo π^{n+r}, adding or subtracting $\frac{f(t_n)}{f'(t_n)}$ does not a make a difference. Hence,

$$t_{n+1} = t_n - \frac{f(t_n)}{f'(t_n)} \equiv t_n \pmod{\pi^{n+r}}$$

proving that t_{n+1} satisfies (i).

We will now show (ii). Note that for any polynomial $f(x)$ and any $c \in \mathbb{R}$ we can write

$$\begin{aligned} f(x + c) &= a_0 + a_1(x + c) + a_2(x + c)^2 + \ldots + a_n(x + c)^n \\ &= a_0 + a_1 x + \ldots + a_n x^n \\ &+ c\left(a_1 + 2a_2 x + 3a_3 x^2 + \ldots + n a_n x^{n-1}\right) \\ &+ c^2 g(x) \\ &= f(x) + f'(x) \cdot c + g(x) \cdot c^2 \end{aligned}$$

for some polynomial $g(x)$. Therefore,

$$f(t_{n+1}) = f(t_n + c) = f'(t_n) \cdot c + g(t_n) \cdot c^2$$

where $c = -\frac{f(t_n)}{f'(t_n)}$. Since $\frac{f(t_n)}{f'(t_n)} \equiv 0 \pmod{\pi^{n+r}}$, we have $c^2 \equiv 0 \pmod{\pi^{2n+2r}}$. For $n \geq 1$, this translates to $c^2 \equiv 0 \pmod{\pi^{n+2r+1}}$. Moreover, observe that by definition

$$f(t_n) + f'(t_n) \cdot c = 0$$

It follows that $f(t_{n+1}) \equiv 0 \pmod{\pi^{n+2r+1}}$ proving (ii).

(ii) $\implies$ (t_n) Cauchy. Let $t \in O_K$ such that $t_n \to t$. By (i), $f(t) = \lim_{n\to} f(t_n) = 0$ (polynomials are cts). (ii) also implies that

$$a \equiv t_n \pmod{\pi^{r+1}}$$

for all n so $a \equiv t \pmod{\pi^{r+1}}$ at the limit. In particular, this means that $v(t-a) \geq r+1 > v(f'(a))$ and hence

$$|t - a| < |f'(a)|$$

This concludes the proof of the existence of t.

(Uniqueness) Suppose t' also satisfies $f(t') = 0$ and $|t' - a| < |f'(a)|$. Let $\delta = t' - t$. Then $|\delta| = |t' - t| < |f'(a)|$. Also,

$$\begin{aligned} 0 = f(t') = f(t+\delta) &= f(t) + f'(t)\cdot\delta + g(t)\cdot\delta^2 \\ \implies |f'(t)\cdot\delta| = |-f'(t)\cdot\delta| &= |g(t)\cdot\delta^2| \leq |\delta|^2 \end{aligned}$$

where the last inequality follows from the fact that $g(x) \in O_K$. But $a \equiv x \pmod{\pi^{1+r}} \implies f(a) \equiv f(x) \not\equiv 0 \pmod{\pi^{1+r}} \implies |f'(x)| = |f'(a)|$. Thus, if $\delta \neq 0$ then $|f'(a)| \leq |\delta|$ which is a contradiction. □

Hensel's Lemma tells us that whenever we have a "close enough" solution to a polynomial, we can lift it into a unique solution "nearby". The following corollary demonstrates an application of Hensel's Lemma.

Corollary 5.3.

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p > 2 \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p = 2 \end{cases}$$

Proof. Every non-zero p-adic number $x \in \mathbb{Q}_p^\times$ can be uniquely written as

$$x = p^n \cdot u \text{ with } n \in \mathbb{Z}, u \in \mathbb{Z}_p^\times$$

$$\implies \mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}$$

Consequently, $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}_p^\times \times \mathbb{Z})/(\mathbb{Z}_p^\times \times \mathbb{Z})^2 \cong \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \times (\mathbb{Z}/2\mathbb{Z})$. Thus, it suffices to consider $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$.

Case 1: $p > 2$
Consider $b \in \mathbb{Z}_p^\times$ and $\bar{b} \equiv b \pmod{p} \in \mathbb{F}_p^\times$. I claim that $b \in (\mathbb{Z}_p^\times)^2$ iff $\bar{b} \in (\mathbb{F}_p^\times)^2$.

($\Rightarrow$) Suppose $\bar{b} \notin (\mathbb{F}_p^\times)^2$. Then $x^2 - \bar{b}$ has no roots in $\mathbb{F}_p^\times$. Suppose for the sake of contradiction that $\exists y \in \mathbb{Z}_p^\times$ such that $y^2 = b$. Then $y^2 \equiv b \pmod{p}$ or $\bar{y}^2 = \bar{b} \pmod{p}$ which is a contradiction.

($\Leftarrow$) Suppose $\bar{b} \in (\mathbb{F}_p^\times)^2$. Then, $\exists y \in \mathbb{F}_p^\times$ such that $y^2 \equiv \bar{b} \pmod{p} \implies |y^2 - \bar{b}| \leq \frac{1}{p}$.

Let $f(x) = 2x - b$. We have $|f'(y)| = |2y| = 1$ so we can apply Hensel's Lemma to find a s.t. $a^2 = b$. Then

$$|b| = 1 \implies |a| = 1 \implies a \in \mathbb{Z}_p^\times \implies b \in (\mathbb{Z}_p^\times)^2$$

With this, observe that $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ (homomorphism with a trivial kernel). Moreover, observe that $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$ (hint: $(\mathbb{F}_p)^2 = \langle g^2 \rangle$ has degree $\frac{p-1}{2}$). It follows that

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^2$$

Case 2: $p = 2$
Let $b \in \mathbb{Z}_p^\times$ and $f(x) = x^2 - b$. Let $b \equiv 1 \pmod 8$. $|f(1)|_2 \leq 2^{-3} < 2^{-2} = |f'(1)|^2 \implies f$ has a unique root a with $a \equiv b \pmod 4$ by Hensel's Lemma. Moreover, let $b \in (\mathbb{Z}_p^\times)^2$ and suppose there exists $a \in \mathbb{Z}_p^\times$ such that $a^2 = b$. It follows that $a \equiv 1 \pmod 2$, or $a = 1 + 2x$ for some $x \in \mathbb{Z}_p$. Then,

$$b \equiv 1 + 4x + 4x^2 \pmod 8$$

But for all $x \in \mathbb{Z}_p$, we know that $4(x)(x+1) \equiv 0 \pmod 8$ and so $b \equiv 1 \pmod 8$. It follows that $b \in (\mathbb{Z}_p^\times)^2$ iff $b \equiv 1 \pmod 8$. Therefore,

$$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2$$

which implies $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \equiv (\mathbb{Z}/2\mathbb{Z})^3$. □

This corollary shows that there are a finite number of quadratic extensions of $\mathbb{Q}_p$ (in fact, a very small number).

Lemma 5.4. *(Hensel's Lemma Version 2) Let $(K, |\cdot|)$ be a complete discretely valued field and let $f \in O_K[x]$. Let $\bar{f} = f \pmod m$. If there is a factorization $\bar{f} = \bar{g}\bar{h}$ with $\bar{g}, \bar{h} \in k[x]$ coprime, then there is a factorization $f(x) = g(x)h(x)$ with $g, h \in O_K[x]$, $g = \bar{g} \pmod m, h = \bar{h} \pmod m$ and $\deg g = \deg \bar{g}$.*

Proof. The idea of the proof is to inductively construct g_n, h_n so that

$$f = g_n h_n + \pi^n r \quad r \in O_K[x]$$

Start off by taking arbitrary lifts g_1, h_1 of $\bar{g}, \bar{h}$ with $\deg \bar{g} = \deg g, \deg \bar{h} = \deg h$. Since $\bar{g}, \bar{h}$ are coprime, find $a, b \in O_K[x]$ such that $ag_1 + bh_1 \equiv 1 \pmod m$. Note that we have

$$f = g_1 h_1 + \pi r_1$$

Moreover, $ag_1 + bh_1 = 1 - \pi r$ so in fact

$$f = g_1 h_1 + \pi r_1(ag_1 + bh_1) + \pi^2 r_1 r$$

Suppose that $\deg r_1 b \leq \deg \bar{g}$. Observe now that we can factorize to get

$$f = (g_1 + \pi r_1 b)(h_1 + \pi r_1 a) + \pi^2(r_1 r - r_1^2 ab)$$

Letting $g_2 = g_1 + \pi r_1 b, h_2 = h_1 + \pi r_1 a, r_2 = r_1 r - r_1^2 ab$, we have $f = g_2 h_2 + \pi^2 r_2$ where $g_2 \equiv g_1 \pmod \pi, h_2 \equiv h_1 \pmod \pi$ and $\deg g_2 = \deg \bar{g}$.

Now, in the case of $\deg r_1 b > \deg \bar{g}$, we cannot factorize since then $\deg g_2 > \deg \bar{g}$. To handle this case, write

$$r_1 b = q g_0 + p \implies f = g_1 h_1 + \pi((r_1 a + q h_1)g_1 + p_1) = g_1 h_1 + \pi(a' g_1 + b' h_1)$$

Now, we have $\deg b' < \deg \bar{g}$ and so we can proceed as above. Now, given

$$f = g_2 h_2 + \pi^2 r_2$$

observe that g_2, h_2 are still coprime $\pmod{\pi}$. It follows that we can repeat inductively to construct a sequence g_n, h_n with

$$f \equiv g_n h_n \pmod{\pi^n}$$
$$g_{n+1} \equiv g_n \pmod{\pi^n}$$
$$h_{n+1} \equiv h_n \pmod{\pi^n}$$

and $\deg g_n = \deg \bar{g}$. Moreover, observe that the bound $\deg h_n \leq \deg f - \deg g_n$ holds (after dropping out terms in h_n with coefficients in $\pi^n O_K$). It follows that $(g_n), (h_n)$ converge, let

$$g = \lim_{n\to\infty} g_n, h = \lim_{n\to\infty} h_n$$

and we obtain the functions that satisfy the statement of the Lemma. □

This version of Hensel's Lemma tells us that if we can factorize a polynomial with coefficients in k, the residue field, then we can also factorize any corresponding polynomial with coefficients in O_K, the valuation ring.

Example 5.5. Is $x^2 + 19x + 11$ irreducible (in $O_{\mathbb{Q}_7}[x]$)? No. We know $k_7 = \mathbb{F}_7$ and therefore,

$$x^2 + 19x + 11 \equiv x^2 + 5x + 4 \pmod{\mathbb{F}_7}$$

Since $x^2 + 5x + 4 = (x + 4)(x + 1)$, by Version 2 of Hensel's Lemma, this implies that $x^2 + 19x + 11$ is factorizable.

Hensel's Lemma Version 2 gives us a very useful corollary.

Corollary 5.6. *Let $f(x) = a_n x^n + \ldots + a_0 \in K[x]$ where K is a discretely valued field with $a_0, a_n \neq 0$. If f is irreducible, then $|a_i| \leq \max\{|a_0|, |a_n|\}$ for all i.*

Proof. Rescale so that $\max_i |a_i| = 1 \implies f(x) \in O_K[x]$. We want to show that either $|a_0| = 1$ or $|a_n| = 1$. Suppose not. Let r be minimal such that $|a_r| = 1$. Then,

$$f(x) \equiv x^r(a_r + \ldots + a_n x^{n-r}) \pmod{\pi}$$

By Hensel's Lemma Version 2, we can lift this factorization to a non-trivial factorization over O_K, contradicting irreducibility. □

5.2. **Teichmüller Lifts.**

Definition 5.7. Let R be a ring. The characteristic of R, char$R$, is the smallest positive n such that $na = 0\ \forall a \in R$. If such an n does not exist, then we say char$R = 0$.

Definition 5.8. A ring of characteristic $p > 0$ is called perfect if the Frobenius map $x \mapsto x^p$ is a bijection.

Whereas Hensel's Lemma allows us to lift a "close enough" solution to an actual one, the Teichmüller Lift allow us to lift an element of the residue field $k = O_K/m$ uniquely to a element in the ring O_K. Formally,

Theorem 5.9. *(Teichmüller Lift Theorem) Let $(K, |\cdot|)$ be a complete discretely valued field such that $k = O_K/m$ is a perfect field of characteristic p. Then there exists a unique map $[\cdot] : k \to O_K$ such that*

(i) $a = [a] \pmod{m}$
(ii) $[ab] = [a][b]$

Moreover, if charK = p then this lifting $[\cdot]$ *is a ring homomorphism. The element* $[a] \in O_K$ *is the Teichmüller lift of* a*.*

Before proving this Theorem, we first need the following Lemma.

Lemma 5.10. *Let* $(K, |\cdot|)$ *have the same properties as Theorem 5.9. Let* $\pi \in O_K$ *be a uniformizer and let* $x, y \in O_K$ *be such that* $x \equiv y \pmod{\pi^k}$ *for some* $k \geq 1$*. Then*

$$x^p \equiv y^p \pmod{\pi^{k+1}}$$

Proof. Let $x = y + u\pi^k$ with $u \in O_K$. Then,

$$x^p = \sum_{i=0}^{p} \binom{p}{i} y^{p-i}(ux^k)^i = y^p + p\pi^k + u^p\pi^{pk}$$

Since $p\pi^k = 0$ and $p > 1 \implies pk > k+1$ it follows that $x^p \equiv y^p \pmod{\pi^{k+1}}$ as desired. □

Proof. (of Teichmüller Lift Theorem)
Let $a \in k$. For each $i \geq 0$, choose a lift $y_i \in O_K$ of $a^{\frac{1}{p^i}}$ and define $x_i = y_i^{(p^i)}$. We claim that (x_i) is a Cauchy sequence and its limit x is independent of our choice of y_i.

By construction, $y_i \equiv a^{\frac{1}{p^i}} \equiv \left(a^{\frac{1}{p^{i+1}}}\right)^p \equiv y_{i+1}^p \pmod{\pi}$. By Lemma 5.10, we have $y_i^p \equiv y_{i+1}^{p^2} \pmod{\pi^2}$. By induction, $y_i^{p^r} \equiv y_i^{p^{r+1}} \pmod{\pi^{r+1}} \implies x_i \equiv x_{i+1} \pmod{\pi^{i+1}}$. Then, (x_i) is Cauchy. Suppose $(x_i) \to x \in O_K$.

Now, suppose we have another (x_i'), generated with a different choice of y_i'. Then $(x_i') \to x' \in O_K$. Define

$$x_i'' = \begin{cases} x_i & \text{for } i \text{ even} \\ x_i' & \text{for } i \text{ odd} \end{cases}$$

It follows that (x_i'') is Cauchy $\implies (x_i'') \to x, (x_i'') \to x' \implies x = x'$. This proves that x is independent of choice of y_i.

Define $[a] = x$. Then $x_i = y_i^{p^i} \equiv (a^{\frac{1}{p^i}})^{p^i} \equiv a \pmod{\pi}$. This holds for all i and so $x \equiv a \pmod{\pi}$, proving (i).

Let $b \in k$ and choose $u_i \in O_K$ a lift of $b^{\frac{1}{p^i}}$. let $z_i = u_i^{p^i}$. Then $\lim_{i\to\infty} z_i = [b]$. Now, $y_i u_i$ is a lift of $(ab)^{\frac{1}{p^i}}$. Hence,

$$[ab] = \lim_{i\to\infty} x_i z_i = \lim_{i\to\infty} x_i \lim_{i\to\infty} z_i = [a][b]$$

This shows (ii).

To verify that $|\cdot|$ is a ring homomorphism, it suffices to check $[a+b] = [a] + [b]$.

We know that $u_i + y_i$ is a lift of $a^{\frac{1}{p^i}} + b^{\frac{1}{p^i}} = (a+b)^{\frac{1}{p^i}}$ $(\text{char}K = p)$. Therefore,

$$\begin{aligned}[a+b] = \lim_{i\to\infty}(u_i + y_i)^{p^i} &= \lim_{i\to\infty} u_i^{p^i} + y_i^{p^i} \\ &= \lim_{i\to\infty} u_i^{p^i} + \lim_{i\to\infty} y_i^{p^i} \\ &= [a] + [b]\end{aligned}$$

as desired.

Finally, let us show that $[\cdot]$ is unique. Let $\phi : k \to O_K$ be another map. Then $\forall a \in K, \phi\left(a^{\frac{1}{p^i}}\right)$ lifts $a^{\frac{1}{p^i}}$. Therefore,

$$[a] = \lim_{i\to\infty} \phi\left(a^{\frac{1}{p^i}}\right)^{p^i} = \phi(a)$$

□

Example 5.11. Consider the example $K = \mathbb{Q}_p$, $[\cdot] : \mathbb{F}_p \to \mathbb{Z}_p$. Now, take any $a \in \mathbb{F}_p^\times, [a]^{p-1} = [a^{p-1}] = [1] = 1$. Hence, $[a]$ is a $(p-1)^{th}$ root of unity. This is perhaps another way of verifying the fact that $a^{p-1} \equiv 1 \pmod p$ (Fermat's Little Theorem).

There is a corollary that demonstrates the usefulness of the Teichmüller Lift Theorem. Before stating and proving it, however, we first need a definition.

Definition 5.12. Let K be an arbitrary field. Then

$$K((t)) = \left\{ \sum_{n=n_0}^{\infty} k_n t^n \mid k_n \in K, n_0 \in \mathbb{Z} \right\}$$

$K((t))$ is called the formal Laurent series with coefficients in K. We can moreover define,

$$K[[t]] = \left\{ \sum_{n=n_0}^{\infty} k_n t^n \mid k_n \in K, n_0 \in \mathbb{Z}, n_0 \geq 0 \right\}$$

the formal power series with coefficients in K.

Observe that $K((t))$ is the field of fractions of $K[[t]]$. Moreover, for any $f(x) = \sum_{n=n_0}^{\infty} k_n t^n \in K[[t]]$, we can set $v(f) = n_0$. It is left as an exercise to the reader to check that v is in fact a valuation.

Corollary 5.13. *Let $(K, |\cdot|)$ be a complete discretely valued field with charK = $p > 0$. Assume $k = O_k/m$ is perfect. Then $K \cong k((t))$.*

Proof. It suffices to show that $O_K \cong k[[t]]$ (since extending to their field of fractions preserves the isomorphism). Fix $\pi \in O_K$ a uniformizer, let $[\cdot] : k \to O_K$ be the Teichmüller lift. Define $\phi : k[[t]] \to O_K$ by

$$\phi\left(\sum_{i=0}^{\infty} a_i t^i\right) = \sum_{i=0}^{\infty} [a_i]\pi^i$$

Then, ϕ is a ring homomorphism since $[\cdot]$ is. It is a bijection since the kernel is trivial. That is, we must have

$$[a_i] = 0 \ \forall i \implies a_i = 0 \implies \sum_{i=0}^{\infty} a_i t^i = 0$$

□

5.3. **Extensions.** Let K/F be a field extension. Then K can be viewed as a vector space of F. Then $[K : F] = \dim_F(K)$ (the dimension of K as a vector space over F). Some fairly crucial properties should be noted regarding extensions of complete valued fields.

Definition 5.14. Let L/K be a field extension. For any $x \in K$, define the linear transformation $m_x(y) = xy$. Then, we define

$$N_{L/K}(x) := \det(m_x)$$

Example 5.15. Consider the field extension $\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$. Let $x = a + b\sqrt{2}$. Then,

$$m_x(y) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$$

and so $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}} = a^2 - 2ab$.

Theorem 5.16. *Let $(K, |\cdot|)$ be a complete non-archimedean discrete valued field and L/K a field extension of degree n. Then*

(i) $|\cdot|$ extends uniquely to an absolute value $|\cdot|_L$ on L defined by

$$|y|_L = |N_{L/K}(y)|^{\frac{1}{n}}$$

(ii) L is complete w.r.t. $|\cdot|_L$

Aiming to prove this Theorem, we need to first show some preliminary results.

Theorem 5.17. *Let $(K, |\cdot|)$ be a complete non-archimedean valued field and V a finite dimensional vector space over K. Then any two norms on V are equivalent. In particular, V is complete with respect to any norm.*

Proof. V is complete with respect to $||\cdot||_{\sup}$ (since $\mathbb{R}$ is complete). Therefore, it suffices to show $||\cdot||$ is equivalent to $||\cdot||_{\sup}$. Let $e_1, \ldots, e_n$ be a basis. Set $D := \max_i ||e_i||$. Then $||x|| \leq D\,||x||_{\sup}$. To find the lower bound, perform induction.

For $n = 1$, clear. Let $n > 1$, set $V_i = \langle e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n\rangle$. By inductive hypothesis, V_i is complete (and hence closed). Then $e_i + V_i$ is also closed $\forall i$ so $S = \bigcup_{i=1}^{n}(e_i + V_i)$ is closed. S does not contain 0, so there exist $c > 0$ s.t. $B(0, c) \cap S = \emptyset$. Let $0 \neq x = \sum_{i=1}^{n} x_i e_i$ and suppose $|x_i| = ||x||_{\sup}$. Then $\frac{1}{x_i}x \in S$ so $\left|\left|\frac{1}{x_i}x\right|\right| \geq c$. That is, $||x|| \geq c\,||x||_{\sup}$. □

Definition 5.18. Let K be a field. An element $x \in K$ is integral over R if it satisfies a monic polynomial with coefficients in R:

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0 \quad (a_i \in R)$$

R is integrally closed if it contains all elements in K that are integral over R.

Lemma 5.19. *Let $(K, |\cdot|)$ be a valued field. Then O_K is integrally closed in K.*

Proof. Take $x \in O_K$. Suppose $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. We want to show that $|x| \leq 1$. Suppose not. We know $|a_{n-1}x^{n-1} + \ldots + a_0| \leq \max |a_i x^i| \leq |x|^i < |x|^n$ which is a contradiction. □

Now we are ready to prove Theorem 5.16.

Proof. We first show that $|\cdot|_L = |N_{L/K}(\cdot)|^{\frac{1}{n}}$ defines an absolute value on L. Property (i) comes from the fact that we are working in a field $\implies$ m_x is invertible iff $x \neq 0$. Property (ii) comes from $det(AB) = det(A) \cdot det(B)$. Therefore, it suffices to show $|x + y|_L \leq \max\{|x|_L, |y|_L\}$. Let $O_L = \{y \in L \mid |y|_L \leq 1\}$. We claim that O_L is the integral closure of O_K in L.

Suppose $y \in L$ is integral over O_K. Let $f(x) = x^m + a_{m-1}x^{m-1} \ldots + a_0 \in K[x]$ be its minimal polynomial. Moreover, the coefficients are sums and products of conjugates of y and so a_i is integral over O_K. In particular, $a_i \in O_K$ so $f(x) \in O_K[x]$. Then, $|N_{L/K}(y)| = |\pm a_0^k| \leq 1$ (see [3], pg. 10) which implies $y \in O_L$.

Conversely, suppose $y \in O_L$ and let $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0 \in K[x]$ be its minimal polynomial over K. By Corollary 5.6, we have $|a_{m-1}|, \ldots, |a_1| \leq \max 1, |a_0| = 1$ (once again, conjugates) so $f \in O_K[x]$ and thus y is integral over K.

This proves the claim. In particular, we now know that O_L is a subring. Now, to prove the ultrametric inequality. WLOG assume $|x|_L \leq |y|_L$. Then $\left|\frac{x}{y}\right|_L \leq 1$ so $\frac{x}{y} \in O_L$. But $\frac{x}{y} + 1 \in O_L$ so $|x + y|_L \leq |y|_L$.

This shows that $|\cdot|_L$ is an absolute value. It is trivial to check that it extends the absolute on K. If $|\cdot|_L, |\cdot|'_L$ are norms on L then by Theorem 5.17 they are equivalent. Thus, $|\cdot|_L = |\cdot|_L^c$. But both agree on K so $c = 1$. Moreover, L is complete with respect to $|\cdot|_L$ also by Theorem 5.17. □

Corollary 5.20. *Let L/K be a finite extension.*

(i) L is discretely valued with respect to $|\cdot|_L$
(ii) O_L is the integral closure of O_K in L

Proof. (ii) is the claim in the proof of Theorem 5.16. For (i), let v be the valuation on K and v_L its extension to L. Then $v_L(y) = \frac{1}{n}v(N_{L/K}(y))$ so $v_L(L^\times) \subset \frac{1}{n}v(K^\times)$ is also discrete. □

6. Local Fields

6.1. **Properties of Local Fields.** We start off, of course, with the definition of local fields.

Definition 6.1. Let $(K, |\cdot|)$ be a valued field. K is a local field if it is complete and locally compact.

A local field that we are already very familiar with is $\mathbb{Q}_p$ (Corollary 4.11).

Proposition 6.2. *Let $(K, |\cdot|)$ be a non-archimedean complete valued field. The following are equivalent:*

(i) K is locally compact
(ii) O_K is compact
(iii) v is discrete and $k = O_K/m$ is finite

Proof. $(i) \implies (ii)$ Let U be a compact neighborhood of 0. Then $\exists 0 \neq x \in O_K$ such that $xO_K \subseteq U$. Since xO_K is closed $\implies$ compact. It follows that O_K is compact (since $O_K \to xO_K$ is a homeomorphism).
$(ii) \implies (i)$ Obvious.

$(ii) \implies (iii)$ Let $x \in m$ and $A_x \subset O_K$ be a set of coset representatives for O_K/xO_K. Then $O_K = \bigcup_{y \in A_x} y + xO_K$ is a disjoint open cover. As O_K is compact, A_x is finite and so O_K/xO_K is finite $\implies O_K/m$ is finite.

Suppose v is not discrete. Let there be $x = x_1, x_2, \ldots$ such that $v(x_1) > v(x_2) > \ldots > 0$. Then $x_1O_K \subset x_2O_K \subset x_3O_K \subset \ldots \subset O_K$. This then implies $O_K/x_1O_K \supset O_K/x_2O_K \supset O_K/x_3O_K \supset \ldots$ which is not possible since O_K/x_1O_K is finite.

$(iii) \implies (ii)$ Let (x_n) be a sequence in O_K and fix a uniformizer $\pi \in O_K$. Since $\pi^i O_K/\pi^{i+1}O_K \cong K$, we have $O_K/\pi^i O_K$ is finite for all i.
$O_K/\pi O_K$ is finite, so there exists $a \in O_K/\pi O_K$ and a subsequence $(x_{1n})_{n=1}^{\infty}$ such that $x_{1n} \equiv a \pmod{\pi}$ for all n. Since $O_K/\pi^2 O_K$ is finite, $\exists a_2$ and a subsequence (x_{2n}) of (x_{1n}) such that $x_{2n} \equiv a_2 \pmod{\pi^2}$. Repeat to obtain $(x_{in})_n$ for $i = 1, 2, \ldots$ such that

(1) $(x_{(i+1)n})$ is a subsequence of (x_{in})
(2) For any $i, \exists a_i \in O_K/\pi^i O_K$ such that $x_{in} \equiv a_i \pmod{\pi^i}O_K$.

Moreover, we have $a_i \equiv a_{i+1} \pmod{\pi^i}$. Now, let $y_i = x_{ii}$. (y_i) is Cauchy and so converges. □

What does the topology of the local field look like? To answer this question, let us first make a definition (that I really could have introduced ages ago).

Definition 6.3. Let $(A_n)_{n=1}^{\infty}$ be a sequence of rings together with homomorphisms $\phi_n : A_{n+1} \to A_n$. The inverse limit of the system (A_n, ϕ_n) is

$$A := \lim_{\leftarrow n} A_n = \{(a_n) \in \Pi_{n=1}^{\infty} A_n \mid \phi_n(a_{n+1}) = a_n \ \forall n \in \mathbb{N}\}$$

The profinite or inverse limit topology is the infinite product topology on the inverse limit. That is, the basic open set is of the form

$$\left\{x \in \lim_{\leftarrow n} A_n \mid x_i = a_i \text{ for } 1 \leq i \leq n\right\}$$

where we specify the first $n \in \mathbb{N}$ coordinates.

In a non-archimedean field $(K, |\cdot|)$, we in fact have

$$O_K \cong \lim_{\leftarrow n} O_K/\pi^n O_K$$

under the map $O_K \to \lim_{\leftarrow n} O_K/\pi^n O_K$ defined by

$$x \mapsto (x \bmod \pi, x \bmod \pi^2, x \bmod \pi^3 \ldots)$$

It will be left to the reader to verify that this is indeed a homomorphism.

Proposition 6.4. *Let K be a non-archimedean local field. Under the isomorphism $O_K \cong \lim_{\leftarrow n} O_K/\pi^n O_K$ the topology on O_K coincides with the profinite topology.*

Proof. The usual topology on O_K has basic open sets of the form $a+\pi^n O_K$. Check that this corresponds to the basic open sets of the profinite topology. □

Lemma 6.5. *Let K be a non-archimedean local field and L/K a field extension. Then L is a local field.*

Proof. From Theorem 5.16 and Corollary 5.20, we know that L is complete and discretely valued. By Proposition 6.2, it suffices to show $k_L = O_L/m_L$ is finite. Let $e_1, \dots, e_n$ be a basis for L as a K-vector space. Then by Theorem 5.17, $||\cdot||_{\text{sup}}$ is equivalent to $|\cdot|_L$. So there exists $r > 0$ such that

$$O_L \subseteq \left\{ x \in L \mid ||x||_{\text{sup}} < r \right\}$$

Take $a \in K$ such that $|a| \geq r$. Then,

$$O_L \subseteq \oplus_{i=1}^n a e_i O_K$$

From Proposition 3.17, we know that O_K is Noetherian. Therefore, every submodule of a finitely generated O_K–module is finitely generated $\implies O_L$ is finitely generated. Suppose $O_L = (a_1, \dots, a_n)$. Then $k_L = (a_1 \pmod{m_L}, \dots, a_n \pmod{m_L})$ is finitely generated over O_K (and in fact over k – check this). But k is finite by Proposition 6.2 and a finite dimensional vector space over a finite field is finite $\implies k_L$ is finite. □

Although quite technical, this Lemma is powerful in that it tells us that extending a local field retains the "local" property.

6.2. **Classification of Local Fields.** The next few theorems will attempt to classify local fields. Let us start with a definition.

Definition 6.6. A non-archimedean valued field $(K, |\cdot|)$ has equal characteristic if $\text{char}K = \text{char}k$. Otherwise, it is called mixed characteristic.

Theorem 6.7. *Let K be a non-archimedean local field of equal characteristic $p > 0$. Then $K \cong \mathbb{F}_{p^n}((t))$.*

Proof. The statement of this Theorem shouts – Teichmüller lift! In particular, we want to apply Corollary 5.13. Therefore, we need to show that k is perfect.

WLOG, let $k = \mathbb{F}_{p^n}$ (recall from Algebra that all finite fields are of this form). Recall the definition of the Frobenius map

$$Frob_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, x \mapsto x^p$$

and that it satisfies the following properties.

(i) $Frob_p(x+y) = Frob_p(x) + Frob_p(y)$
(ii) $Frob_p(xy) = Frob_p(x) \cdot Frob_p(y)$
(iii) $Frob_p(1) = 1$

(ii) and (iii) are trivial. (i) becomes obvious once we recall that F has characteristic p. Combined, this implies $Frob_p$ is a ring homomorphism. Observe that $x^p = 0 \implies x = 0$ (properties of field). Thus, $Frob_p$ is injective. $\mathbb{F}_{p^n}$ finite, $\implies Frob_p$ is bijective $\implies \mathbb{F}_{p^n}$ perfect. □

Although the proof is rather simple (immediately obvious in fact if one knows that finite fields are perfect), it tells us that all local fields of equal characteristic have this rather simple and straightforward form! Let us continue our project of classifying local fields.

Theorem 6.8. *(Ostroski's Theorem) Any non-trivial absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$.*

This is quite an impactful theorem that tells us there are actually only 2 "ways" of completing $\mathbb{Q}$. Either we complete via the usual absolute value and get $\mathbb{R}$, or we apply a p–adic absolute value and get $\mathbb{Q}_p$. To prove Theorem 6.8, let us first prove a lemma.

Lemma 6.9. *An absolute value on K is non-archimedean iff it is bounded on $\mathbb{Z}$.*

Proof.
($\Rightarrow$) The following facts imply this.

(i) $|1| = 1, |0| = 0$
(ii) $|n| = |\underbrace{1 + \ldots + 1}_{n \text{ repetitions}}| \leq |1|$
(iii) $|-n| = |n|$

($\Leftarrow$) Suppose $|n| \leq B$ for $n \in \mathbb{Z}$. Let $x, y \in K$ such that $|x| \leq |y|$. Then

$$\begin{aligned} |x+y|^m = \left|\sum_{i=0}^{m} \binom{m}{i} x^i y^{m-i}\right| &\leq \sum_{i=0}^{m} \left|\binom{m}{i} x^i y^{m-i}\right| \\ &\leq (m+1)B|y|^m \end{aligned}$$

Then $|x+y| \leq [(m+1)B]^{\frac{1}{m}}|y|$. This hold for all m, so $|x+y| \leq |y|$. □

Proof. (of Ostrowski's Theorem)
Case 1: $|\cdot|$ is archimedean. We fix an integer $b > 1$ such that $|b| > 1$ by Lemma 6.9. Let $a > 1$ be an integer and write b^n in base a. That is,

$$b^n = c_m a^m + c_{m-1} a^{m-1} + \ldots + c_1 x + c_0$$

where $0 \leq c_i < a$ and $c_m \neq 0$. Let $B = \max_{0 \leq c \leq a} |c|$. Then,

$$|b|^n \leq (m+1) \cdot B \cdot \max\{|a|^m, 1\}$$

Observe that $m \leq n \log_a b$ so $|b| \leq [(n \log_a b + 1)B]^{\frac{1}{n}} \max\left\{|a|^{\log_a b}, 1\right\} \implies |b| \leq \max\left\{|a|^{\log_a b, 1}\right\}$. Then $|a| > 1$ and $|b| \leq |a|^{\log_a b}$. We can then switch the roles of a, b to get $|a| \leq |b|^{\log_b a}$. This gives

$$\frac{\log|a|}{\log a} = \frac{\log|b|}{\log b} := \lambda$$

Then $|a| = a^\lambda \forall a \in \mathbb{Z}_{>1} \implies |x| = |x|_\infty^\lambda \forall x \in \mathbb{Q}$. This is precisely the statement for $|\cdot|, |\cdot|_\infty$ equivalent (Proposition 3.11).

Case 2: $|\cdot|$ is non-archimedean. Then we have $|n| \leq 1$ for all $n \in \mathbb{Z}$ as given by Lemma 6.9. As $|\cdot|$ is non-trivial, there exist $n \in \mathbb{Z}_{>0}$ such that $|n| < 1$. Then there is a prime factor p of n such that $|p| < 1$. Suppose there exists another prime $q \neq p$ with $|q| < 1$. Then

$$vp + sq = 1$$

for some $r, s \in \mathbb{Z}$. Then

$$1 = |1| = |vp + sq| \leq \max |vp|, |sq| < 1$$

by ultrametric inequality. This is a contradiction. Then $\alpha := |p| < 1$ and $|q| = 1$ for all primes $q \neq p$. Then, for any $p^n \frac{a}{b} \in \mathbb{Q}$, we have $\left|p^n \frac{a}{b}\right| = \alpha^{-n}$. In other words, this uniquely determines $|\cdot|$. Moreover,

$$\left|p^n \cdot \frac{a}{b}\right| = \alpha^{-n} = \left(2^{-n}\right)^{\log_\alpha 2} = \left|p^n \cdot \frac{a}{b}\right|_p^{\log_\alpha 2}$$

□

We can now use Ostrowski's Theorem to further classify local fields – in particular, local fields of mixed characteristic.

Theorem 6.10. *Let $(K, |\cdot|)$ be a non-archimedean local field of mixed characteristic. Then K is a finite extension of $\mathbb{Q}_p$ for some p.*

Proof. Suppose $\mathrm{char}K = p, \mathrm{char}k = q$ where $p \neq q$ and $p > 0$. Observe that $\mathrm{char}O_K = \mathrm{char}K = p$. Consider the natural homomorphism

$$\phi : O_K \to k$$

Now, we have $p \cdot 1_K = 0 \implies \pi(p \cdot 1_K) = p \cdot 1_k = 0$. In other words, $\mathrm{char}k$ divides p. Therefore, $\mathrm{char}k = p$ which is a contradiction. It follows that $\mathrm{char}K = 0$.

Then $\mathbb{Q} \subseteq K$. O_k/m is finite, so there must be some $n \in \mathbb{Z}$ such that $n \in m$. Then $|n| < 1 \implies |\cdot|$ is non-trivial. By Theorem 6.8, $|\cdot|$ is equivalent to $|\cdot|_p$ for some p. K complete $\implies \mathbb{Q}_p \subseteq K$. Let $\pi \in O_K$ be a uniformizer, v a normalized valuation on K and set $v(p) = e$. Then we have

$$O_K/pO_K \cong O_K/\pi^e O_K$$

Note that $O_K/\pi^e O_K$ must be finite by Proposition 6.2. Let $x_1, \ldots, x_n$ be a set of coset representatives for a basis of O_K/pO_K as a $\mathbb{F}_p$–vector space. Then

$$\left\{ \sum_{i=0}^{n} a_i x_i \mid a_i \in \{0, \ldots, p-1\} \right\}$$

is a set of coset representatives for O_K/pO_K. Let $y \in O_K$. We then get

$$y = \sum_{i=0}^{\infty} \left(\sum_{j=1}^{n} a_{ij} x_j \right) p^i = \sum_{j=1}^{n} \left(\sum_{i=0}^{\infty} a_{ij} p^i \right) x_j$$

Note that we are able to exchange summations due to the nice property given by Lemma 3.4. Note also that $\sum_{i=0}^{\infty} a_i p^i$ converges in $\mathbb{Z}_p$ so the x_j give a generating set of O_K over $\mathbb{Z}_p$.

Now, we know that $p = v \cdot \pi^e$ for some $v \in O_k, e \geq 1$. Hence, $\pi^{-1} = v \cdot \pi^{e-1} \cdot p^{-1}$ with $e - 1 \geq 0$. Therefore, for any $x \in K$ we have

(i) $x = u\pi^m$ for $m > 0$, in which case $x \in O_k$ and so is generated by the x_j's over $\mathbb{Z}_p$ (and hence $\mathbb{Q}_p$).

(ii) $x = u\pi^{-m}$ for $m > 0$. Then, $x = u(v \cdot \pi^{e-1} \cdot p^{-1})^m = uv^m \pi^{m(e-1)} p^{-m}$. Now, $uv^m \pi^{m(e-1)} \in O_k$ so $x = \sum_{i=0}^{n} \frac{a_i}{p^m} x_i \implies x$ is generated by the x_j's over $\mathbb{Q}_p$.

This proves K is finite over $\mathbb{Q}_p$. □

We end with the classification of archimedean local fields, which is surprisingly simple.

Theorem 6.11. *Let $(K, |\cdot|)$ be an archimedean local field. Then $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$.*

Proof. Since archimedean, $|\cdot|$ is non-trivial. Apply Ostrowski's Theorem to conclude that $\mathbb{R} \subseteq K$. Suppose $K \neq \mathbb{R}$. K must be a finite extension of $\mathbb{R}$ (since K is locally compact). It is a classic result from Galois Theory that all finite extensions of $\mathbb{R}$ are either $\mathbb{R}$ itself or isomorphic to $\mathbb{C}$ (you do not have irreducible polynomials with degree ≥ 3). □

Acknowledgments

I am deeply grateful to my mentor, Pranjal Warade, for her patient guidance as I learned and explored abstract algebra, algebraic number theory, and local fields. I have required constant help throughout the process and her support and patience have been invaluable. I would also like to thank Professor Peter May for his dedication in administering and organizing the program. This paper would not have been possible without their help.

References

[1] Chua, Dextor. Part III - Local Fields. Based on Lectures of H. C. Johansson. Available at: https://dec41.user.srcf.net/notes/III_M/local_fields_thm_proof.pdf
[2] Conrad, Keith. The p-adic Expansion of Rational Numbers. Available at: https://kconrad.math.uconn.edu/blurbs/gradnumthy/rationalsinQp.pdf
[3] Conrad, Keith. Trace and Norm. Available at: https://kconrad.math.uconn.edu/blurbs/galoistheory/tracenorm.pdf
[4] Dummit, David S. and Foote, Richard M. Abstract Algebra. John Wiley & Sons, Inc. 2004.
[5] Gouvêa, Fernando Q. p-adic Numbers: An Introduction. Springer. 1997.
[6] Lang, Serge. Algebra (Revised Third Edition). Springer-Verlag New York. Inc. 2002.
[7] Pomerantz, Alexa. An Introduction to the p-adic Numbers. The University of Chicago REU 2020. Available at: https://math.uchicago.edu/~may/REU2020/REUPapers/Pomerantz.pdf.
[8] Rojas, J. Maurice. Note on p-adic Expansions in $\mathbb{Q}$. Available at: https://artsci.tamu.edu/mathematics/~rojas/padic.pdf.
[9] Serre, Jean-Pierre. Local Fields. Springer-Verlag New York. Inc. 1979.
[10] Tomczak, Leonard. Local Fields. Based on Lectures of Rong Zhou. Available at: https://math.berkeley.edu/~ltomczak/notes/Mich2022/LF_Notes.pdf.