Local Fields Course Notes
Taught by Mark Lau Tin Wai

Bendit Chan

December 2, 2021

Contents

1 Completion of Valued Field 2

1.1 Absolute Values . . . 2

1.2 Completion . . . 4

1.3 Classification of Absolute Values . . . 8

2 Discrete Valuation 11

2.1 Valuation Rings . . . 11

2.2 Investigation: Hensel's Lemma . . . 13

2.3 π-adic expansion and the Teichmüller representative . . . 15

3 Extension of complete fields 17

3.1 Norms . . . 17

3.2 Ramifications . . . 20

4 Ramification Theory 23

1 Completion of Valued Field

In this section, we will start our study on fields equipped with absolute values, and then move on to considering non-archimedean ones. We then pass on to constructing the metric space completion of valued field, which is a valued field as well. At last we will present two important examples that serves as prototypes in later sections.

1.1 Absolute Values

Definition 1.1 (Absolute values)

Let K be a field, then an **absolute value** on K is a function

$$|\cdot|: K \to \mathbb{R}$$

satisfying the following properties,

(K1) We have $|x| \geq 0$ for all $x \in K$, with equality holds if and only if $|x| = 0$;

(K2) We have $|xy| = |x||y|$ for all $x, y \in K$;

(K3) We have the triangle inequality $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

Definition 1.2 (Non-Archimedean, Valued fields)

An absolute value is called **non-archimedean** if the strong triangle inequality holds

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

If $|\cdot|$ defines an non-archimedean absolute value on K, then the pair $(K, |\cdot|)$ is called a **valued field**.

Remark. There are a few arithmetic properties one can notice. Let $x, y \in K$.

1. If $x^n = 1$ then $|x| = 1$. In particular, finite fields have only the trivial absolute value $|\cdot|_0$, defined as

$$|x|_0 = \begin{cases} 0 & \text{for } x = 0 \\ 1 & \text{for } x \neq 0 \end{cases}$$

2. We have $|1| = |-1| = 1$, so $|x| = |-x|$ for all $x \in K$.

3. If K is a valued field and $|x| < |y|$. Then $|x+y| \leq \max\{|x|, |y|\} = |y| = |x+y-x| \leq \max\{|x|, |x+y|\} = |x+y|$. Hence $|x + y| = |y|$ (i.e. every triangle is isosceles).

We shall only put our attention on non-archimedean absolute values. The name of it is emerged from the following lemma. Recall there exist an unique injective homomphism from $\mathbb{Z} \to R$ for any ring R.

Lemma 1.3

Let K be a field with an absolute value $|\cdot|$ on K, then $|\cdot|$ is non-archimedean iff the set $\{|n| : n \in \mathbb{Z}\}$ is bounded.

Proof. ($\Rightarrow$) Since $|n| = |-n|$, we can assume $n \geq 1$. Then $|n| = |1 + 1 + \ldots + 1| \leq |1| = 1$.

($\Leftarrow$) Suppose $|n| \leq B$ for all $n \in \mathbb{Z}$. Let $x, y \in \mathbb{Z}$, then

$$|x+y|^m = \left| \sum_{i=0}^{m} \binom{m}{i} x^i y^{m-i} \right| \leq (m+1)B \max\{|x|, |y|\}^m.$$

Taking roots both sides yields

$$|x+y| \leq (B(m+1))^{1/m} \max\{|x|, |y|\}.$$

Suppose there exist x, y such that the inequality is not true. Notice that the factor $(B(m+1))^{1/m}$ tends to 1 when m tends to infinity. Thus we can choose a sufficiently large m such that we derive a contradiction. Hence $|\cdot|$ is indeed non-archimedean. □

Remark. Lemma 1.3 shows that if $\mathrm{char}(K) > 0$, then all absolute value on K are non-archimedean.

Another distinctive difference between archimedean absolute value and non-archimedean absolute value is that the **valuation ring** only make sense when it is defined in a valued field (i.e. a field with a non-archimedean absolute value), which gives a rich algebraic structure on K. We first need a definition on general valuation rings:

Note

The **characteristic** n of a field F is the smallest number n such that

$$\underbrace{1 + 1 + \ldots + 1}_{n \text{ times}} = 0.$$

If such n does not exist, we say $\mathrm{char}(K) = 0$.

Definition 1.4 (Valuation Ring)

Suppose B is an integral domain and $K = \mathrm{Frac}(B)$. Then B is called a **valuation ring** of K if for any element $x \in K^\times$, we have $x \in B$ or $x^{-1} \in B$.

Proposition 1.5

Given a valued field K, the **valuation ring** (abuse of notation)

$$\mathcal{O}_K := \{x \in K : |x| \leq 1\}$$

is a valuation subring of K. The units in $\mathcal{O}_K$ are exactly $\mathcal{O}_K^\times = \{x \in K : |x| = 1\}$, and the remaining elements form a maximal ideal, i.e.

$$\mathfrak{m}_K = \{x \in K : |x| < 1\}.$$

The quotient $k_K := \mathcal{O}_K / \mathfrak{m}_K$ is then defined as the **residue field**.

Proof. To see that why $K = \mathrm{Frac}(\mathcal{O}_K)$, use Atiyah Corollary 3.2. The rest to prove that $\mathcal{O}_K$ is indeed a valuation ring of K is trivial.

Now if $x \in \mathcal{O}_K$ satisfies $|x| = 1$, then $x^{-1} \in K$. But $|x^{-1}| = 1$ as well, so $x^{-1} \in \mathcal{O}_K$, i.e. x is a unit. This proves the second part. The third part just comes from Atiyah Proposition 1.6. □

Notice that if $|\cdot|$ is archimedean, then $\mathcal{O}_K$ is not even a subring of K (take $\mathbb{R}$ as an example). We quote Atiyah Proposition 5.8 to give some properties of valuation rings:

Proposition 1.6

Let B be a valuation ring of K, then

1. B is a local ring.
2. If B' is a ring such that $B \subseteq B' \subseteq K$, then B' is a valuation ring of K.
3. B is integrally closed in K.

Note

An integral domain B is **integrally closed** in K if it is equal to its integral closure, i.e. the set of all integral elements

$$\{x \in K : \exists n \geq 1, b_i \in B, \\ x^n + b_1 x^{n-1} + \ldots + b_n = 0\}.$$

Proof.

1. Let $\mathfrak{m}$ be the set of non-units of B, so $x \in \mathfrak{m} \Leftrightarrow$ either $x = 0$ or $x^{-1} \notin B$. If $a \in B$ and $x \in \mathfrak{m}$ we have $ax \in \mathfrak{m}$ for if otherwise $(ax)^{-1} \in B \Rightarrow x^{-1} = a \cdot (ax)^{-1} \in B$. Next let x, y be non-zero elements in $\mathfrak{m}$. Then either xy^{-1} or $x^{-1}y \in B$. If $xy^{-1} \in B$ then $x + y = (1 + xy^{-1})y \in B\mathfrak{m} \subseteq \mathfrak{m}$. Similarly for $x^{-1}y \in B$. Hence $\mathfrak{m}$ is an ideal and therefore B is a local ring.
2. It is clear from the definition.
3. Let $x \in K$ be integral over B, then we have
$$x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n = 0$$
with $b_i \in B$. If $x \in B$ then we are done. If $x^{-1} \in B$ then we have $x = -(b_1 + b_2 x^{-1} + \cdots + b_n x^{1-n}) \in B$. □

1.2 Completion

Now we proceed to the construction of completion of K with respect to the absolute value $|\cdot|$. Notice that this construction works for both archimedean absolute value and non-archimedean absolute value. Recall that a field K is **complete** if every Cauchy sequence in K has a limit in K.

Definition 1.7 (Cauchy Sequence)

Let K be a field with absolute value $|\cdot|$. A sequence $(a_n)_{n\geq 0}$ is **Cauchy** if for all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that $\forall n, m > N$, we have
$$|a_n - a_m| < \epsilon.$$

Let $\mathcal{R}$ denote the set of all Cauchy sequences in K. Then $\mathcal{R}$ forms a ring with component-wise addition and multiplication, i.e. $(a_n) + (b_n) := (a_n + b_n)$ and $(a_n) \times (b_n) := (a_n b_n)$.

Furthermore, a Cauchy sequence (a_n) is called a **nilsequence** if

$$\lim_{n\to\infty} |a_n| = 0,$$

(this limit takes place in $\mathbb{R}$) where the set of all nilsequence is denoted as $\mathcal{N}$. We then have the following proposition:

Proposition 1.8

The set of all nilsequence $\mathcal{N}$ forms a maximal ideal of $\mathcal{R}$, and the quotient ring $\widehat{K} := \mathcal{R}/\mathcal{N}$ is a field.

Proof. Let I be an ideal that properly contains $\mathcal{N}$. We want to show that the constant sequence $(1) \in I$ (so $I = \mathcal{R}$).

Claim

Let $(a_n) \in I \setminus \mathcal{N}$. Then it has at most finitely many zeros in the sequence.

Proof. Assume not, then by definition we have:

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n, m > N, |a_m - a_n| < \epsilon,$$

but there are infinitely many zeros in the sequence. Thus we can choose $a_n = 0$ for any $n > N$, so the sequence converges to zero, i.e. it is a nilsequence. Contradiction. □

Now using the same notation, we can add a nilsequence to (a_n) such that it has no non-zero terms, and obtain a new sequence (b_n). But the term-by-term inversion $\left(\frac{1}{b_n}\right)$ is still a Cauchy sequence by basic analysis. Thus $(1) = (b_n)\left(\frac{1}{b_n}\right) \in I$ as required. □

Remark. For any element $k \in K$, notice that the constant sequence $(k)_{n\geq 0}$ is Cauchy and thus induces an injective ring homomorphism $\phi : K \hookrightarrow \mathcal{R}$ given by

$$\phi : k \mapsto (k)_{n\geq 0}.$$

Hence the ring $\mathcal{R}$ contains a copy of K.

At last, we will put an absolute value (induced by $|\cdot|$ on $\widehat{K}$).

Definition 1.9

Define the absolute value[a] on $\widehat{K}$ as

$$|(a_n)|' := \lim_{n\to\infty} |a_n|.$$

[a] Afterwards we will abuse the notation, writing $|-|$ as $|-|'$ to represent the absolute value on $\widehat{K}$.

We have to manually check if this absolute value is well-defined and if it satisfies the three conditions:

Claim

This is a well defined absolute value on $\widehat{K}$.

Proof. Suppose $a_n \sim b_n$ in $\widehat{K}$, i.e. $a_n - b_n \in \mathcal{N}$. We have

$$\lim_{n\to\infty} |b_n| + \lim_{n\to\infty} |a_n - b_n| \geq \lim_{n\to\infty} |a_n|$$

and similarly,

$$\lim_{n\to\infty} |a_n| + \lim_{n\to\infty} |b_n - a_n| \geq \lim_{n\to\infty} |b_n|.$$

Since $a_n - b_n \in \mathcal{N}$, we must have $|(a_n)|' = |(b_n)|'$. □

Claim

This defines an absolute value on $\widehat{K}$.

Proof. (K1) $|(a_n)|' = \lim_{n\to\infty} |a_n| = 0$ if and only if $a_n \in \mathcal{N}$.

(K2) $|(a_n)|'|(b_n)|' = \lim_{n\to\infty} |a_n| \lim_{n\to\infty} |b_n| = \lim_{n\to\infty} |a_n||b_n| = \lim_{n\to\infty} |a_n b_n| = |(a_n b_n)|'$.

(K3) $|(a_n) + (b_n)|' = \lim_{n\to\infty} |a_n + b_n| \leq \lim_{n\to\infty} |a_n| + |b_n| = |(a_n)|' + |(b_n)|'$. □

We also note here that if $|\cdot|$ is non-archimedean, then

$$|(a_n) + (b_n)|' = \lim_{n\to\infty} |a_n + b_n| \leq \lim_{n\to\infty} \max\{|a_n|, |b_n|\} = \max\{|(a_n)|', |(b_n)|'\}$$

as the max function is continuous. Therefore $|\cdot|'$ is also non-archimedean.

Remark. Recall the natural homomorphism ϕ. For $k \in K$, we have $|\phi(k)|' = |k|$.

Now we will prove that the completion of K is indeed complete. We first state a lemma that K is dense in $\widehat{K}$:

Lemma 1.10

Let $(a_n) \in \widehat{K}$, then (a_n) can be approximated arbitrarily close by elements of K.

Note

A set A is **dense** in B if $B = A \cup L$, where L is the set of limit points of A.

Proof. Fix $\epsilon > 0$. As (a_n) is Cauchy, there exist N such that $|a_n - a_m| < \epsilon$ for every $n, m \geq N$. Then we have

$$|(a_n) - \phi(a_N)|' = \lim_{n\to\infty} |a_n - a_N| \leq \epsilon,$$

and so (a_n) converges to (a_N), i.e. K is dense $\widehat{K}$. □

Theorem 1.11

The field $\widehat{K}$ is complete.

Proof. Let (A_n) be a Cauchy sequence in $\widehat{K}$. Then by Lemma 1.10, for all integer n, there exist $a_N \in K$ such that

$$|A_n - \phi(a_N)|' < \frac{1}{n}.$$

Claim

The sequence (a_n) is Cauchy, and thus gives an element $a \in \widehat{K}$.

Proof. We have

$$|a_m - a_n| = |\phi(a_m) - \phi(a_n)|' \leq |\phi(a_m) - A_m|' + |A_m - A_n|' + |A_n - \phi(a_n)| < \frac{1}{m} + \frac{1}{n} + |A_m - A_n|'$$

and therefore (a_n) is Cauchy since (A_n) is a Cauchy sequence. □

To proceed, we further claim that $A_n \to a$ when $n \to \infty$. We have

$$|A_n - a|' \leq |A_n - \phi(a_n)|' + |\phi(a_n) - a|' < \frac{1}{n} + |\phi(a_n) - a|'.$$

When $n \to \infty$, by construction of a we have that $|\phi(a_n) - a|$ is arbitary close to 0 by Lemma 1.10. This proves the assertion. □

Another feature of the completion is that it preserves the residue field:

Proposition 1.12

Let $\hat{K}$ be the completion of the valued field K. Let $\widehat{\mathcal{O}}_K$ and $\widehat{\mathfrak{m}}_K$ be the valuation ring and the maximal ideal of $\hat{K}$ respectively. Then clearly $\mathcal{O}_K = \widehat{\mathcal{O}}_K \cap K$ and $\mathfrak{m}_K = \widehat{\mathfrak{m}}_K \cap K$. Hence there is a natural map

$$\begin{aligned} \theta : \mathcal{O}_K/\mathfrak{m}_K &\to \widehat{\mathcal{O}}_K/\widehat{\mathfrak{m}}_K \\ a + \mathfrak{m}_K &\mapsto \phi(a) + \widehat{\mathfrak{m}}_K \end{aligned}$$

which is an isomorphism.

Proof. It is clearly an injective field homomorphism. For surjectivity, if $\alpha \in \widehat{\mathcal{O}}_K$, then by Lemma 1.10 there exist $a \in K$ such that $|\alpha - \phi(a)| < 1$. Then $a \in \mathcal{O}_K$ and $\alpha - \phi(a) \in \widehat{\mathfrak{m}}_K$. Hence $\theta(a) = \alpha$ as required. □

1.3 Classification of Absolute Values

In the next two examples we will classify all absolute values on some particular fields. Thus it makes sense for us to first define when are two absolute values considered as "same".

Proposition 1.13

Let $|\cdot|_1$ and $|\cdot|_2$ be two non-trivial absolute value on a field K. Then the following are equivalent:

1. $|\cdot|_1$ and $|\cdot|_2$ induce the same topology;
2. $|x|_1 \leq 1$ if and only if $|x|_2 \leq 1$;
3. $|x|_2 = |x|_1^c$ for some constant $c > 0$.

If these conditions holds then we say $|\cdot|_1$ and $|\cdot|_2$ are **equivalent**.

Proof. (1) ⇒ (2). Suppose $|\cdot|_1$ and $|\cdot|_2$ induce the same topology, then any sequence that converges with respect to one absolute value must also converge in the other. Consider the sequence $(x^n)_{n\geq 0}$, this converges to 0 with respect to $|\cdot|$ if and only if $|x| < 1$. This gives (2).

(2) ⇒ (3). Pick $a \in K^\times$ with $|a|_1 < 1$. Let $x \in K^\times$ and $m/n \in \mathbb{Q}$, we have

$$\begin{aligned}\frac{\log|x|_1}{\log|a|_1} > \frac{m}{n} &\iff n\log|x|_1 < m\log|a|_1 \\ &\iff \left|\frac{x^n}{a^m}\right|_1 < 1 \\ &\iff \left|\frac{x^n}{a^m}\right|_2 < 1 \\ &\iff \frac{\log|x|_2}{\log|a|_2} > \frac{m}{n}\end{aligned}$$

Since $m/n \in \mathbb{Q}$ is arbitary, so $\dfrac{\log|x|_1}{\log|a|_1} = \dfrac{\log|x|_2}{\log|a|_2}$, then $\log|x|_2 = c\log|x|_1$ for some $c > 0$, as required.

(3) ⇒ (1). We have

$$|x-a|_1 < r \iff |x-a|_2^c < r \iff |x-a|_2 < r^{1/c},$$

so any open ball with respect to $|\cdot|_1$ is also open with respect to $|\cdot|_2$. □

Example 1.14

Classify all non-trivial absolute values on $\mathbb{Q}$.

Solution. We split into two cases, namely when the absolute value is archimedian and non-archimedian:

Archimedean This first implies that there exist $b \in \mathbb{Z}_{>1}$ such that $|b| > 1$. We shall prove that $|\cdot|$ is equivalent to the usual absolute value, denoted by $|\cdot|_\infty$.

Let $a \in \mathbb{Z}$. Write b^n in base a, i.e. $b^n = c_m a^m + c_{m-1}a^{m-1} + \ldots + c_0$ with $0 \leq c_i < a$ and $m \leq n \log_a b$. Let $B = \max\{|c_i| : 0 \leq c_i \leq a\}$. Then

$$\begin{aligned}|b^n| \leq (m+1)B\max\{|a|^m, 1\} \Rightarrow |b| &\leq \underbrace{(B(m+1))^{1/n}}_{\to 1 \text{ as } n\to\infty} \max\{|a|^{\log_a b}, 1\} \\ &\Rightarrow |b| \leq \max\{|a|^{\log_a b}, 1\}.\end{aligned}$$

This implies that $|a| > 1$ and $|b| \leq |a|^{\log_a b}$. Swap the roles of a and b and we get $|a| \leq |b|^{\log_b a}$. Combining the two results yields

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

and so $|a| = a^\lambda$ for all $a \in \mathbb{Z}_{>1}$. Hence $|\cdot|$ is equivalent to $|\cdot|_\infty$.

Non-archimedean This implies that $|n| \leq 1$ for all $n \in \mathbb{Z}$. As $|\cdot|$ is non-trivial, pick $n \in \mathbb{Z}$ such that $n > 1$ and $|n| < 1$. Write $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}$ with p_i primes. Notice that there exist p_i such that $|p_i| < 1$.

Claim

The prime p_i such that $|p_i| < 1$ is unique.

Proof. Suppose otherwise that $|p| < 1$ and $|q| < 1$ for distinct primes p and q. Write $1 = rp + sq$ for some $r, s \in \mathbb{Z}$ by Bezout's identity. Then $1 = |rp + sq| \leq \max\{|rp|, |sq|\} \leq \max\{|p|, |q|\} < 1$. Contradiction. □

Therefore $|p| = \alpha < 1$ and for all other primes q, we must have $|q| = 1$. Let $v_p(n)$ to be the largest power of p that divides n. Then we have

$$|n|_p = \begin{cases} 0 & \text{for } n = 0 \\ \alpha^{v_p(n)} & \text{for } n \neq 0. \end{cases}$$

This absolute value extends uniquely to $\mathbb{Q}$ by the rule $|p/q| = |p|/|q|$, or by extending the notion v_p to $\mathbb{Q}$ by settubg $v_p(a/b) = v_p(a) - v_p(b)$.

When $\alpha = p^{-1}$, this absolute value is called the **p-adic absolute value** on $\mathbb{Q}$, denoted by $|\cdot|_p$. Notice that other absolute values with different choices of α are equivalent to $|\cdot|_p$. □

We note here that the valuation ring of $\mathbb{Q}$ is actually in the form of

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} : \gcd(a, b) = 1, p \nmid b\right\}.$$

This is actually the localization of $\mathbb{Z}$ at ideal (p) with the residue field $\mathbb{F}_p$, the finite field with p elements. This is not complete. Define the **p-adic numbers** $\mathbb{Q}_p$ to be the completion of $\mathbb{Q}$ with respect to the p-adic absolute value, with $\mathbb{Z}_p$ as the **p-adic integers** which is the valuation ring of $\mathbb{Q}_p$.

Example 1.15

Classify all non-trivial absolute values on $\mathbb{F}_q(T)$.

Solution. Notice that in a finite field, any absolute value is trivial, hence it is non-archimedean. Consider a non-zero polynomial $f(T) = a_0 + a_1 T + \cdots + a_d T^d$ ($a_d \neq 0$). We shall split into two cases:

$|T| > 1$ For each $0 \leq i \leq d$, since $a_i \in \mathbb{F}_q$, we must have $|a_i| = 0$ or 1 and in particular, $|a_d| = 1$. Then $|a_i T^i| < |a_d T^d|$ as $T > 1$. Since "every triangle is isosceles", we have $|f(T)| = |a_d T^d| = |T^d| = |T|^{\deg f}$.

Now let $c = \frac{1}{|T|}$, and so we have $|f(T)| = c^{-\deg f}$. This defines an absolute value on $\mathbb{F}_q[T]$ which extends easily to $\mathbb{F}_q(T)$. This absolute value will be denoted as $|\cdot|_\infty$.

$|T| \leq 1$ Let $\pi(T)$ be a non-constant polynomial with minimal degree such that $|\pi(T)| < 1$.

Claim

$\pi(T)$ is irreducible.

Proof. Suppose the contrary, then $\pi(T) = p(T)q(T)$ with $\deg p, \deg q < \deg \pi$. Therefore $|p|, |q| \geq 1$ by the minimality of the degree. But $|\pi| = |p||q|$, and so $|\pi| \geq 1$. Contradiction. □

WLOG we can assume that $\pi(T)$ is monic by scaling. Now consider $f(T) = \pi(T)^k h(T)$, with $\pi \nmid h$. We will show that $|h(T)| = 1$.

Indeed, write $h(T) = \pi(T)q(T) + r(T)$, by minimality of degree we have $|r(T)| = 1$ (since we already know that for any polynomial, $|f(T)| \leq \max(|a_i T_i|) \leq 1$), and $|\pi(T)q(T)| \leq c < 1$. Hence again by "every triangle is isosceles" we have $|h| = 1$, so $|f(T)| = c^k = c^{-v_\pi(f)}$, where $v_\pi(f)$ is the highest power of π dividing f.

This defines an absolute value on $\mathbb{F}_q[T]$ which extends easily to $\mathbb{F}_q(T)$. We will denote this absolute value as $|\cdot|_\pi$. □

Similar to above, the valuation ring of $\mathbb{F}_q(T)$ with respect to $|\cdot|_\pi$ is the localization of $\mathbb{F}_q(T)$ at ideal (π), with residue field $\mathbb{F}_q$.

For the case $|\cdot|_\infty$, notice that

$$\left|\frac{f(T)}{g(T)}\right|_\infty = \left|\frac{f(1/T)}{g(1/T)}\right|_{1/T} = \deg g - \deg f.$$

This reduces to the case mentioned above. The completion of $\mathbb{F}_q(T)$ with respect to this absolute value is $\mathbb{F}_q((T))$, with the valuation ring $\mathbb{F}_q[[T]]$.

2 Discrete Valuation

In this section, we will consider an equivalent formulation of non-archimedean absolute values, which is named as valuations. We then further specialise into discrete valuations and introduce the notion of local fields, exploring its fruitful properties.

2.1 Valuation Rings

Definition 2.1 (Valuation)

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

1. For all $x, y \in K^\times$, we have $v(xy) = v(x) + v(y)$;
2. For all $x, y \in K^\times$, we have $v(x + y) \geq \min\{v(x), v(y)\}$.

The image $v(K^\times)$ is a subgroup of $(\mathbb{R}, +)$, called the **value group**.

Notice that a valuation is just an alternative way to represent a non-archimedean absolute value. Fix $0 < c < 1$. Then if we have a valuation v, the function

$$|x| = \begin{cases} 0 & \text{for } x = 0 \\ c^{v(x)} & \text{for } x \neq 0 \end{cases}$$

determines a non-archimedean absolute value. Conversely, given an non-archimedean absolute value $|x|$, the function $v(x) = -\log_c |x|$ gives back the induced valuation.

Definition 2.2 (Discretely valued field)

If $v(K^\times) \cong \mathbb{Z}$, then we say that v is a **discrete valuation** (which is **normalised** if $v(K^\times) = \mathbb{Z}$) and K is a **discretely valued field**.
We also call $\pi \in K$ **uniformiser** if $v(\pi)$ generates the value group, so $v(\pi) = 1$ if v is normalised.

Recall from a modified version of Atiyah Chapter 6 in which we have the definition of Noetherian rings:

Definition 2.3

Let A be a ring, A is **Noetherian** if one of the following equivalent conditions holds:

1. Every ideal in A is finitely generated.
2. Every infinite ascending chain of ideals is stationary, i.e. there does not exist $(I)_i$ such that

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

and each of the inclusions are strict.

We then have the following lemma, linking the discrete valuation with Noetherian rings:

Lemma 2.4

Let K be a valued field with valuation v. The following are equivalent:

1. v is a discrete valuation.
2. $\mathcal{O}_K$ is a principal ideal domain.
3. $\mathcal{O}_K$ is a Noetherian ring.
4. $\mathfrak{m}_K$ is principal.

Note

Recall that the valuation ring $\mathcal{O}_K$ is the set

$$\mathcal{O}_K := \{x \in K : |x| \leq 1\},$$

while the non-units form a maximal ideal

$$\mathfrak{m}_K = \{x \in K : |x| < 1\}.$$

Proof. (1) $\Rightarrow$ (2). We shall show that v is an Euclidean function on $\mathcal{O}_K$. $v(a) \leq v(ab)$ is obvious. If $ab^{-1} \in \mathcal{O}_K$, we can write $a = b \cdot ab^{-1} + 0$. Otherwise, we must have $0 > v(ab^{-1}) = v(a) - v(b)$, so $v(a) < v(b)$. Now notice $v(a) = v(b + (a-b)) \geq \min(v(b), v(a-b)) = v(a-b)$. Write $x = 1 \cdot y + (x-y)$ and we are done. (2) $\Rightarrow$ (3) is obvious.

(3) $\Rightarrow$ (4). Write $\mathfrak{m}_K = x_1\mathcal{O}_K + x_2\mathcal{O}_K + \cdots + x_n\mathcal{O}_K$. WLOG we have $|x_1| \geq |x_2| \geq \cdots \geq |x_n|$. Then consider $x\mathcal{O}_K \subseteq y\mathcal{O}_K \Leftrightarrow \frac{x}{y} \in \mathcal{O}_K \Leftrightarrow |x| \leq |y|$. Hence $\mathfrak{m}_K = x_1\mathcal{O}_K$.

(4) $\Rightarrow$ (1). Let $\mathfrak{m}_K = \pi\mathcal{O}_K$. Then for any $x \in K^\times$ with $v(x) > 0$, we have $x \in \mathfrak{m}_K$ so $v(x)$ is generated by $v(\pi)$. □

This leads to the following definition that characterize $\mathcal{O}_K$:

Definition 2.5

A **discrete valuation ring** (DVR) is a principal ideal domain with exactly one non-zero prime ideal (which is also maximal).

It is then clear that if v is discrete, then $\mathcal{O}_K$ is a discrete valuation ring. The converse also holds:

Proposition 2.6

If R is a discrete valuation ring, then there exists a discrete valuation v on $K = \mathrm{Frac}(R)$ such that $R = \mathcal{O}_K$.

Proof. Let R be a DVR with prime element π. Then every non-zero $x \in R$ can be written uniquely by $x = u\pi^r$ where $u \in R^\times$ and $r \geq 0$. Similarly we have every $x \in K^\times$ can be written uniquely by $x = u\pi^r$ where $u \in R^\times$ and $r \in \mathbb{Z}$. Now define $v : K^\times \to \mathbb{R}$ where $u\pi^r \mapsto r \in \mathbb{Z}$. Then we get $R = \mathcal{O}_K$. □

In this set of notes we will be interested in the study of local fields, which is simply a valued field with extra conditions: we will show how the conditions are useful in later sections.

Definition 2.7 (Local Fields)

Let K be a valued field with valuation v. Then K is called a **local field**[a] if it satisfy the following properties.

(L1) v is a discrete valuation;

(L2) K is complete;

(L3) The residue field k_K is finite.

[a] There are literatures that includes $\mathbb{R}$ and $\mathbb{C}$ as archimedean local field. However in this note we focus on non-archimedean ones, so we omit them by definition.

2.2 Investigation: Hensel's Lemma

Normally when we solve diophantine equation in K, we project down to see if the diophantine equation have roots in a residue field k_K. If it has no roots in k then it won't have roots in K.

In here a stronger result is true: If it has a simple root in k, we can lift the root up uniquely in K. This helps us to solve the diophantine equation a lot easier, as illustrated by the following theorem:

Theorem 2.8 (Hensel's Lemma)

Suppose that K be a complete discretely valued field. Let $f(x) \in \mathcal{O}_K[x]$ and there exist $a \in \mathcal{O}_K$ such that

1. $f(a) \equiv 0 \pmod{\pi}$;
2. $f'(a) \not\equiv 0 \pmod{\pi}$.

Then there exist unique $x \in \mathcal{O}_K$ such that

1. $f(x) = 0$;
2. $x \equiv a \pmod{\pi}$.

Proof. We will construct a Cauchy sequence (a_n) of x that satisfies the following properties:

1. $f(a_n) \equiv 0 \pmod{\pi^n}$
2. $a_n \equiv a_{n+1} \pmod{\pi^n}$

And then if we set $a_1 = a$, then we get the desired properties. We will show that such choice of sequence is possible by induction. Let $a_{n+1} = a_n + k\pi^n$ for some $k \in \mathcal{O}_K$. Then consider

$$\begin{aligned} f(a_{n+1}) &= f(a_n) + f'(a_n)k\pi^n + \frac{1}{2}f''(a_n)(k\pi^n)^2 + \cdots \\ &\equiv f(a_n) + f'(a_n)k\pi^n \equiv 0 \pmod{\pi^{n+1}} \end{aligned}$$

where an unique choice of $k \in k_K$ is possible since $f'(a_n) \neq 0$. Furthermore, notice that $f'(a_{n+1}) \neq 0$ in k_K. □

We give an example illustrating this lemma:

Example 2.9

Consider the p-adic number $\mathbb{Q}_p$ with valuation ring $\mathcal{O}_K = \mathbb{Z}_p$ and residue field $k_K = \mathbb{F}_p$. Since $v(p) = 1$ and v is a discrete valuation, we must have the uniformiser $\pi = p$, for the maximal ideal is exactly (p).

Thus the two conditions are actually just $f(a) = 0$ and $f'(a) \neq 0$ in $\mathbb{F}_p$. If both of them are satisfied, then there exist x in $\mathbb{Q}_p$ such that $f(x) = 0$, while $x \equiv a \pmod{p}$ (meaning that we **lifted up** the root from $\mathbb{F}_p$ to $\mathbb{Q}_p$).

To proceed on our study of local fields, we have to first deduce a stronger form of Hensel's Lemma, which requires the notion of primitive polynomials:

Definition 2.10 (Primitive polynomial)

Let $f(x) \in K[x]$ where $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. We say f is **primitive** if the maximum value of a_i (for $1 \leq i \leq n$) is 1.

We are now ready to state the stronger form of Hensel's Lemma as follows:

Theorem 2.11 (Stronger form of Hensel's Lemma)

Let K be a complete discretely valued field and $f \in K[x]$ is a primitive polynomial with $\bar{f} \in k_K[x]$. If there is a factorization

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x)$$

with $\gcd(\bar{g}, \bar{h}) = 1$, then there is a factorization $f(x) = g(x)h(x)$ in $\mathcal{O}_K[x]$ with $\bar{g} \equiv g \pmod{\pi}$ and $\bar{h} \equiv h \pmod{\pi}$ with $\deg g = \deg \bar{g}$.

Proof. Let g_0 and h_0 be arbitrary lifts to $\mathcal{O}_K[x]$ such that $\deg g_0 = \deg \bar{g}$ and $\deg h_0 = \deg \bar{h}$. Then we have $f \equiv g_0 h_0 \pmod{\pi}$ and so $f(x) = g_0 h_0 + \pi r_0$ for some $r_0 \in \mathcal{O}_K$. Since $\bar{g}$ and $\bar{h}$ is coprime there exists a, b such that

$$a g_0 + b h_0 \equiv 1 \pmod{\pi}. \tag{1}$$

Then plugging in (1) into f yields

$$f(x) = g_0 h_0 + \pi r_0 (a g_0 + b h_0) + \pi^2(\ldots) = (g_0 + \pi r_0 b)(h_0 + \pi r_0 a) + \pi^2(\ldots).$$

If $\deg r_0 b < \deg g_0$, then we can set $g_1 = g_0 + \pi r_0 b$ and $h_1 = h_0 + \pi r_0 a$. If not by division algorithm we can write $r_0 b = q g_0 + p$ and rewrite f as

$$f(x) = g_0 h_0 + \pi((r_0 a + q) g_0 + p h_0) + \pi^2(\ldots) = (g_0 + \pi p)(h_0 + r_0 a + q) + \pi^2(\ldots)$$

and proceed as above.

Now we have $f = g_1 h_1 + \pi^2 r_1$, $r_1 \in \mathcal{O}_K[x]$ and $\deg g_1 = \deg \bar{g}$. Inductively do this process to obtain g_k and h_k and set g and h to be the limit of the sequence g_k and h_k respectively. This finishes the proof. □

Remark. We shall morally show that this stronger form implies Theorem 2.8. Indeed, given $a \in \mathcal{O}_K$ such that $f(a) \equiv 0 \pmod{\pi}$ and $f'(a) \not\equiv 0 \pmod{\pi}$, the projection $\bar{f}$ in k_K can in fact factorize in

$$\bar{f}(x) = (x-a)\bar{q}(x)$$

for some $\bar{q}(x)$, while $(x-a, \bar{q}(x)) = 1$ since a is a simple root.

By Theorem 2.11 we can lift up the factorization to $\mathcal{O}_K[x]$ by $f(x) = (x-b)q(x)$ since $\deg g = 1$. But $\bar{g} \equiv g \pmod{\pi}$, so we must have $a \equiv b \pmod{\pi}$, and so the root in $\mathcal{O}_K$ is in fact b.

Corollary 2.12

Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in K[x]$ and $a_0, a_n \neq 0$. If f is irreducible then for all $0 \leq i \leq n$ we have

$$|a_i| \leq \max(|a_0|, |a_n|).$$

Proof. By scaling assume f is primitive, and we shall show that $\max(|a_0|, |a_n|) = 1$. If not let r be minimal such that $|a_r| = 1$. Then the factorization

$$f \equiv x^r(a_r + a_{r+1}x^1 + \ldots + a_nx^{n-r}) \pmod{\pi}$$

lifts up to a factorization of f. Contradiction. □

Hensel's Lemma in fact helps us understand the field extension of local fields. For example, one can show that $\mathbb{Q}_p$ has 3 quadratic extensions only (for $p \neq 2$). We will soon see an application in the following section.

2.3 π-adic expansion and the Teichmüller representative

This following theorem provides us a tool much like the decimal expansion in $\mathbb{R}$, so we don't need to think K as a set of Cauchy sequences anymore. We also have a even better condition that the π-adic expansion is unique.

Theorem 2.13 (π-adic expansion)

Let K be a complete valued field with uniformizer π. Suppose $A \subseteq \mathcal{O}_K$ is a set of coset representatives for $k_K = \mathcal{O}_K/(\pi)$. Then

1. Every series $\displaystyle\sum_{r=0}^{\infty} a_r\pi^r$ (with $a_r \in A$) converges in K.
2. Every $x \in \mathcal{O}_K$ can be written uniquely as $x = \displaystyle\sum_{r=0}^{\infty} a_r\pi^r$ with $a_r \in A$.

Proof.

1. The partial sum S_n is a Cauchy sequence in K, and so it converges due to completeness.
2. Let $x \in \mathcal{O}_K$. Notice that there exist unique $a_0 \in A$ such that $|a_0 - x| < 1$. Then we can write $x = a_0 + \pi y_1$ where $y_1 \in \mathcal{O}_K$. Now we continue inductively. Uniqueness is easy to check by modulo π^r. □

Remark. This shows that if K is complete with respect to a non-trivial absolute value, then K is uncountable.

Let K be a local field with finite residue field k with $|k| = q$. Let $f(x) = x^q - x \in \mathcal{O}_K[x]$. Then for each $\alpha \in k$ which is a simple root of $\bar{f}(x) = x^q - x \in k[x]$, there is a unique $a \in \mathcal{O}_K$ such that (i) $a^q = a$, and (ii) $a \equiv \alpha \pmod{\pi}$ given by Theorem 2.8. This brings us to the following definition:

Definition 2.14 (Teichmüller representative)

Define the unique $a \in \mathcal{O}_K$ satisfying the conditions above (i.e. $a^q = a$ and $a \equiv \alpha \pmod{\pi}$) to be the **Teichmüller representative** for $\alpha \in k$, which is denoted by $a = [\alpha]$.

Theorem 2.15

Let K be a local field with finite residue field k. If $\operatorname{char}(K) = p > 0$ then $K \cong k((T))$.

Proof. Notice that $\operatorname{char}(k) = \operatorname{char}(K) = p$, and so $|k| = q$ is a power of p. We shall show that the **Teichmüller map** $[\cdot] : k \to \mathcal{O}_K$ gives an injective ring homomorphism. It is clear that it is injective by the projection to k.

Claim

This map preserves addition and multiplication.

Proof. Let $\alpha, \beta \in k$. Since p divides $\binom{q}{i}$ for all $0 < i < q$, we have

$$([\alpha] + [\beta])^q = [\alpha]^q + [\beta]^q = [\alpha] + [\beta]$$

as required. Similarly we have $([\alpha][\beta])^q = [\alpha]^q[\beta]^q = [\alpha][\beta]$. □

Then by the definition of $[\alpha\beta]$ we have $[\alpha\beta] = [\alpha][\beta]$. Now we have the isomorphism map $k[[T]] \to \mathcal{O}_K$ defined by

$$\sum_{n=0}^{\infty} a_n T^n \mapsto \sum_{n=0}^{\infty} [a_n] \pi^n$$

Hence their fraction field are isomorphic, proving our assertion. □

3 Extension of complete fields

In this section, we will consider finite extensions of complete fields. What's different from completions of valued field is that it is complicated to put an absolute value on the extensions and thus we shall dedicate the first half of the section to construct it. Afterwards we will continue to a discussion of some properties of the extensions.

3.1 Norms

Given a finite extension L/K, the first task is to put an absolute value on L. However we will first instead treat L as a K-vector space and put a norm on L first, and then we will prove the uniqueness of the norm.

Definition 3.1 (Norm)

Let L be a vector space over a valued field K. A **norm** on L is a function $||\cdot|| : L \to \mathbb{R}$ such that

(N1) We have $||x|| \geq 0$ for all $x \in L$, with equality if and only if $||x|| = 0$;

(N2) We have $||\lambda x|| = |\lambda| ||x||$ for all $\lambda \in K$ and $x \in L$.

(N3) We have the ultrametric inequality for $x, y \in L$:

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

Two norms $||\cdot||_1$ and $||\cdot||_2$ on L are **equivalent** if there exist C, $D \in \mathbb{R}$,

$$C||x||_1 \leq ||x||_2 \leq D||x||_1$$

for all $x \in L$. Notice that equivalent norms induce the same topology.

We will provide an example of norm that is important below.

Example 3.2

Let L be a vector space over K with dimension n. Pick $\{e_i\}$ to be the basis of L over K. Let $v = \sum v_i e_i$. Then the **maximum norm** $||v||_{\max}$ is defined as

$$||v||_{\max} := \max_{0 \leq i \leq n} |v_i|.$$

It is clear that it is a norm. If n is infinite, we can similarly define a norm that take place on the supremum of $\{|v_i|\}$. In this paper, we will just deal with finite extensions so this definition suffices.

Theorem 3.3

Let K be a complete valued field and L be a finite dimensional vector space over K. Then any norm on L are equivalent, and L is complete.

Proof. Let $\{e_1, e_2, \dots, e_n\}$ be the basis of L over K. We shall prove that any norm is equivalent to the maximum norm, i.e. we want to find C and D such that

$$C||x||_{\max} \le ||x|| \le D||x||_{\max}.$$

In here D is easy to find. Just set $D = \sum ||e_i||$ and we have

$$||x|| = \left|\left|\sum_{i=1}^{n} x_i e_i\right|\right| \le \left(\sum_{i=1}^{n} ||e_i||\right) \max |x_i| = D||x||_{\max}.$$

For C, we shall perform induction on n. If $n = 1$, then $||x|| = |x_1| \cdot ||e_1|| = ||e_1|| \cdot ||x||_{\max}$. Hence $C = ||e_1||$ works, and that $L = K$ is complete.

For $n \ge 2$, let $L_i := \operatorname{Span}\{e_1, e_2, \dots, e_{i-1}, e_{i+1}, \dots, e_n\}$. By the induction hypothesis, each L_i is complete with respect to $|| \cdot ||$. In particular L_i is closed in L.

Then the union $\bigcup_{i=1}^{n} e_i + L_i$ is also closed. By construction it doesn't contain 0. Then there exist $C > 0$ such that $||x|| \ge C$. We claim that $C||x||_{\max} \le ||x||$.

Indeed if $x = \sum x_i e_i \in L$ and r such that $|x_r| = \max_i(|x_i|) = ||x||_{\max}$. Then

$$\begin{aligned} ||x||_{\max}^{-1}||x|| &= ||x_r^{-1}x|| \\ &= \left|\left|\frac{x_1}{x_r}e_1 + \frac{x_2}{x_r}e_2 + \cdots + \frac{x_{r-1}}{x_r}e_{r-1} + e_r + \frac{x_{r+1}}{x_r}e_{r+1} + \cdots + \frac{x_n}{x_r}e_n\right|\right| \ge C \end{aligned}$$

since this is an element in $e_r + L_r$.

For completeness, given a Cauchy sequence in L under the max norm, take the limit of each coordinate to get the limit of the sequence, using the fact that K is complete. This completes the proof. □

This proves the uniqueness of norm, thus the uniqueness of absolute value. Now we shall generally move on to proving the existence of absolute values in a extension.

Let K be a local field with $|\cdot|_K$ defined on K, and L/K be a field extension.

Question

Can we extend the valuation $|\cdot|_K$ to $|\cdot|_L$?

Theorem 3.4

Let K be a complete valued field, and L/K be a finite extension. Then the absolute value on K has an unique extension to an absolute value on L, by

$$|\alpha|_L = \sqrt[n]{|N_{L/K}(\alpha)|_K}$$

where $n = [L : K]$. Also L is complete with respect to $|\cdot|_L$.

Note

For a field extension L/K, the **norm** of α is

$$N_{L/K}(\alpha) = \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)^{[L:K(\alpha)]}$$

where $\sigma_i(\alpha)$ are the roots of the minimal polynomial of α over K.

Proof. Uniqueness and completeness are proved in Theorem 3.3. It remains to show that $|\alpha|_L = \sqrt[n]{|N_{L/K}(\alpha)|_K}$ is a valid absolute value. (K1) and (K2) is trivial.

To show the strong triangle inequality, it is equivalent to show that $|\alpha|_L \leq 1$ implies $|\alpha + 1|_L \leq 1$. Consider

$$\mathcal{O}_L = \{\alpha \in L : |\alpha|_L \leq 1\} = \{\alpha \in L : N_{L/K}(\alpha) \in \mathcal{O}_K\}.$$

Claim

$\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$.

Proof. Let $\alpha \in \mathcal{O}_L$, then let the minimal polynomial of α over K to be $f(x) = a_0 + a_1 x + \cdots + x^n \in K[x]$.

We want to show $a_i \in \mathcal{O}_K$. Since f is irreducible, by Corollary 2.12 we have

$$|a_i| \leq \max(|a_0|, 1)$$

but we see that $a_0^d = N_{L/K}(\alpha) \in \mathcal{O}_K$ for some d. Hence α is integral over $\mathcal{O}_K$.

Conversely, suppose α integral over $\mathcal{O}_K$. Let $\bar{K}$ be the splitting field of α over K, notice that

$$N_{L/K}(\alpha) = \Big(\prod_{\sigma : L \to \bar{K}} \sigma(\alpha)\Big)^d$$

since $\sigma(\alpha)$ is integral over $\mathcal{O}_K$ and so is $N_{L/K}(\alpha)$. But $N_{L/K}(\alpha) \in K$ so it is in $\mathcal{O}_K$ since $\mathcal{O}_K$ is integrally closed. □

This claim implies the strong triangle inequality, by Atiyah Corollary 5.3 (i.e. $\mathcal{O}_L$ is a subring of L). □

The following proposition will deal with the discreteness of the valuation:

Proposition 3.5

Let K be a discretely valued field with normalised valuation v_K. Let L/K be a field extension. Then the image of $v_L(L^\times)$ must have the form

$$v_L(L^\times) = \frac{1}{e}\mathbb{Z}$$

where e is a divisor of $[L : K]$, called the **ramification index**.

Proof. Notice that by the identity $v_L(x) = \dfrac{1}{n} v_K(N_{L/K}(x))$ we see that $v_L(L^\times)$ is contained in $\frac{1}{n}\mathbb{Z}$. Let d/e (with d, e relatively prime) be in the image, with the denominator e chosen largest possible. This is possible since e is clearly a divisor of n, so the possible denominators are bounded. Now by Bezout there exist $r, s \in \mathbb{Z}$ such that $rd - se = 1$. Then we have

$$r\frac{d}{e} = \frac{1 + se}{e} = \frac{1}{e} + s \in v(L^\times).$$

Since $s \in \mathbb{Z}$ is clearly in the image, it follows that $1/e \in v_L(L^\times)$. Hence $v_L(L^\times) = \frac{1}{e}\mathbb{Z}$, by the condition of e. □

The ultimate goal of ours is just to show that all finite extensions of local fields are still local fields. It all remains to show that the residue field is finite. This brings us to the following section since this is quite complex.

3.2 Ramifications

We shall develop a set of tools for us to look more closely at the extensions of local fields. It helps us further classify the field extensions into various types, based on their ramification index as described above.

Definition 3.6 (Residue field degree)

Let K be a discretely valued field with residue field k_K. Let L be a field extension of K with residue field k_L. Then k_L is naturally a field extension of k_K. We denote $f = [k_L : k_K]$ to be the **residue field degree**.

Theorem 3.7

Let K be a discretely valued field and L/K be a field extension. Then

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

If $e = 1$, then we say L/K is an **unramified extension**. While if $f = 1$, then we say L/K is a **totally ramified extension**.

Proof. Choose $\alpha_1, \alpha_2, \cdots, \alpha_f \in \mathcal{O}_K^\times$ such that their image $\{\bar{\alpha_i}\}$ is the basis of k_L over k_K. Our major claim is this:

Claim

The set

$$\{\alpha_i \pi_L^j : 1 \le i \le f, 0 \le j \le e-1\}$$

forms the set of basis of L over K.

Proof. It suffices to check the linear independence and the span of the elements in this set:

Linear independence Let $a_{ij} \in K$, not all zero, such that $\sum a_{ij}\alpha_i\pi_L^j = 0$. Put

$$s_j = \sum_{i=1}^{f} a_{ij}\alpha_i.$$

Notice that α_i are linearly independent over K since their reduction are linearly independent over k_K. (Indeed, $\sum a_i\alpha_i = 0$ implies that $\bar{a_i} = 0$ for all i, and so $\pi_L \mid a_i$. This process can continue indefinitely, contradiction.) Hence there exist j such that $s_j \neq 0$.

We claim that if $s_j \neq 0$ then $e \mid v_L(s_j)$. Let k be an index such that $|a_{kj}|$ is maximal. Then

$$a_{kj}^{-1}s_j = \sum_{i=1}^{f} a_{kj}^{-1}a_{ij}\alpha_i.$$

By assumption, $|a_{kj}^{-1}a_{ij}\alpha_i| \le |\alpha_i| = 1$, which attains equality if $i = k$. So we have $a_{kj}^{-1}s_j$

Spanning □

□

Hence the number of basis $e \cdot f$ is the degree of the extension $[L : K]$. □

Theorem 3.8

Let L/K be a finite extension of a local field with degree n. Then L/K is totally ramified if and only if $L = K(\alpha)$ for some $\alpha \in L$, where α is the root of the polynomial of the form

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

where $v_K(a_i) \geq 1$ for all i and $v_K(a_0) = 1$. Such polynomial is called **Eisenstein**.

Proof. ($\Rightarrow$) Let $\alpha = \pi_L$, then $1, \pi_L, \pi_L^2, \ldots, \pi_L^{n-1}$ form a basis over K (by the proof in Theorem 3.7), and hence satisfy the polynomial

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$$

where $a_i \in K$. Considering the absolute value of each term we see that two of the term must have the same absolute value. However notice each term has different absolute value since they belong different coset $v(L^\times)/v(K^\times)$ except the first and last time. Hence $|a_0| = |\pi_K|^n = |\pi_L|$ and other $|a_i| < 1$.

($\Leftarrow$) Assume $L = K(\alpha)$ satisfying the Eisentein polynomial $f(x)$. Then we have $|\alpha|^n < 1 \Longrightarrow |\alpha| < 1$. Hence $|a_0|$ has the largest absolute value in all other terms except possibly the first term. Then we have the first and last term being the same, which implies that $|\alpha|^n = |\pi_K|$. Hence we have $e \geq [L : K]$, which the equality holds, L/K is totally ramified. □

Theorem 3.9

Let L/K be a finite extension of local field with residue field degree f. Let $m = q^f - 1$. Then there exist field $F = K(\zeta_m)$ such that F/K is a unramified extension and L/F is a totally ramified extension.

Before we end our section, we actually have enough tools to classify all possible local fields, which is actually the types we illustrated in Example 1.14 and 1.15:

Proposition 3.10

Local fields can only take hold of the following types:

1. Finite extensions of $\mathbb{Q}_p$;
2. The field of Laurent series $\mathbb{F}_q((t))$ on finite fields.

Proof. If $\text{char}(K) = 0$. Then $\mathbb{Q} \subseteq K$. In Example 1.11 we illustrated the restriction of $|\cdot|$ to $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime p, so we have $\mathbb{Q}_p \subseteq K$, i.e. K is a field extension of $\mathbb{Q}_p$. Since the residue field k is finite, so clearly

$f = [k : \mathbb{F}_p]$ is finite. Similary, as $v(L^\times) = \frac{1}{e}\mathbb{Z} \cong \mathbb{Z}$ we have e also finite. Hence by theorem 3.7 $[L : K] = ef$ is finite, i.e. K is a finite extension of $\mathbb{Q}_p$.

If $\mathrm{char}(K) > 0$. Then by theorem 2.10 we see $K \cong \mathbb{F}_q((t))$. □

4 Ramification Theory

In this section, we will continue the discussion of extension of local fields by decomposing the extension into subfields and study their Galois group.

Definition 4.1

Let L/K be a finite Galois extension of local fields. Then there is a natural surjective group homomorphism

$$\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k_K).$$

Define the **inertia group** I as the kernel of the map $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k_K)$, which has the form

$$I_{L/K} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(x) \equiv x \pmod{\pi_L} \ \forall x \in \mathcal{O}_L\},$$

which has size $e(L/K)$ and is a normal subgroup of $\mathrm{Gal}(L/K)$. We also define the **n^{th} ramification group** as

$$G_n := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(x) \equiv x \pmod{\pi_L^{n+1}} \ \forall x \in \mathcal{O}_L\}.$$

Notice $I = G_0$ and $G = \mathrm{Gal}(L/K) \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots$ forms a chain of normal subgroup.

In fact, looking at π_L is enough to check if $\sigma \in G_n$.

Proposition 4.2

$G_n = \{\sigma \in I_{L/K} : \sigma(\pi_L) \equiv \pi_L \pmod{\pi_L^{n+1}}\}$.

Proof. Consider L/K, by Theorem 3.9 we can split it into a unramified extension F/K and totally ramified extension L/F. Now we have $\mathrm{Gal}(k_L/k_K) \cong \mathrm{Gal}(F/K)$ since $k_F = k_L$ by definition of totally ramified. Now we claim that $I_{L/K}$ is in fact $\mathrm{Gal}(L/F)$. Indeed by Galois Correspondence:

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \cong \mathrm{Gal}(F/K) \cong \mathrm{Gal}(k_L/k_K)$$

Hence $\mathrm{Gal}(L/F)$ is in fact the kernel of the map $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(k_L/k_K)$.

Now we see that L/F is a totally ramified extension, so we have $L = F(\pi_L)$, so if we have $\sigma(\pi_L) \equiv \pi_L \pmod{\pi_L^{n+1}}$, then we have $\sigma(x) \equiv x \pmod{\pi_L^{n+1}} \ \forall x \in \mathcal{O}_L$, since it holds for any polynomials in π_L, proving our claim. □

We shall prove it gives $\mathrm{Gal}(L/K)$ a decomposition series, defined below.

Definition 4.3 (Decomposition series)

Let H be a finite group. A **decomposition series** for H is a chain of normal subgroup

$$H = H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_n = \{e\}$$

such that H_i/H_{i+1} is a cyclic group. If H admits a decomposition series, we call H **solvable**.

Proving this requires a technical lemma.

Lemma 4.4

Let $\sigma, \tau \in G_n$. Then $\tau(\pi_L) = (a_\tau \pi_L^n + 1)\pi_L$ for some $a_\tau \in \mathcal{O}_L$. Also we have the identity

$$\frac{\sigma\tau(\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L}\frac{\tau(\pi_L)}{\pi_L} \pmod{\pi_L^{n+1}}$$

Proof. By definition we have $\tau(\pi_L) \equiv \pi_L \pmod{\pi_L^{n+1}}$, i.e. there exist $a_\tau \in \mathcal{O}_L$ such that $\tau(\pi_L) - \pi_L = a_\tau \pi_L^{n+1}$. Rearranging yield the result. Notice that $u := a_\tau \pi_L^n + 1$ is a unit since it clearly not divisible by π_L. Hence $\tau(\pi_L) = u\pi_L$. Substituting this to the identity yields

$$\begin{aligned} & \frac{\sigma\tau(\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L}\frac{\tau(\pi_L)}{\pi_L} \pmod{\pi_L^{n+1}} \\ \iff & \frac{\sigma(u\pi_L)}{\pi_L} \equiv \frac{\sigma(\pi_L)}{\pi_L}\frac{u\pi_L}{\pi_L} \pmod{\pi_L^{n+1}} \\ \iff & \frac{\sigma(u)\sigma(\pi_L)}{\pi_L} \equiv \frac{u\sigma(\pi_L)}{\pi_L} \pmod{\pi_L^{n+1}} \end{aligned}$$

This is true since $\sigma(u) \equiv u \pmod{\pi_L^{n+1}}$, because $\sigma \in G_n$. □

Proposition 4.5

There is an injective group homomorphism

$$G_0/G_1 \hookrightarrow (k_L^\times, \cdot)$$

Proof. We will prove $G_0 \to (k_L^\times, \cdot)$ is a group homomorphism given by

$$\sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L} \pmod{\pi_L}$$

with kernel G_1. It is indeed a group homomorphism given by Lemma 4.4, now $\frac{\sigma(\pi_L)}{\pi_L} \equiv 1 \pmod{\pi_L}$ if and only if $\sigma(\pi_L) \equiv \pi_L \pmod{\pi_L^2}$, i.e. $\sigma \in G_1$. □

Proposition 4.6

For $n \geq 1$, there is an injective group homomorphism

$$G_n/G_{n+1} \hookrightarrow (k_L, +)$$

Proof. The map $G_n \to (k_L, +)$ is a group homomorphism given by $\sigma \mapsto a_\sigma \pmod{\pi_L}$, with kernel G_{n+1}. □

Remark. This shows that G_n/G_{n+1} is a cyclic group.

Theorem 4.7

Gal(L/K) is solvable.

Proof. Proposition 4.5 and 4.6 gives G_n/G_{n+1} is a cyclic group. It remains to show the chain of normal subgroups G_i terminates at $\{e\}$, i.e. we want to show $\bigcap G_i = \{e\}$.

Let $\sigma \in \bigcap G_i$. Then for all $n \in \mathbb{N}$, we have $\sigma(x) \equiv x \pmod{\pi_l^{n+1}}$, i.e. $v(\sigma(x) - x) \geq n$ for all $n \in \mathbb{N}$. However no real number satisfy the property so $\sigma(x) - x = 0$. The assertion is thus proved. □