PAWS 2024: Local Fields

Catherine Hsu

Introduction

Many questions in number theory are motivated by studying the solutions of polynomial equations with integer or rational coefficients. For example, consider the equation

$$x^2 - 2y^2 = 5z^2. \tag{1}$$

By inspection, we can see that there are many real solutions—for example, $(\sqrt{5}, 0, 1)$—but we might ask for solutions in which x, y, z are rational. It turns out that

$$x = y = z = 0$$

is the only rational solution, as we can see by studying this equation modulo 5. Indeed, suppose that we have a rational solution $(x, y, z) \neq (0, 0, 0)$ to (1). Then, we can rescale x, y, z by a common factor to obtain another solution, and thus, up to rescaling, we can assume that x, y, z are integers with $5 \nmid \gcd(x, y, z)$. Moreover, we may assume that $5 \nmid y$ since if this were not the case, we would also have $5 \mid x$, which implies $5^2 \mid (x^2 - 2y^2)$, so that $5 \mid z$ as well. Thus, since we may assume the residue class of y is invertible mod 5, any rational solution (x, y, z) to (1) yields a non-zero solution (x, y) to the equation

$$x^2 y^{-2} \equiv 2 \pmod 5.$$

However, such a solution is impossible since 2 is not a quadratic residue modulo 5!

Now, we can rephrase what we've just shown as proving that (1) does not have any non-zero solutions over the *field of* 5*-adic numbers,* denoted $\mathbb{Q}_5$. The field $\mathbb{Q}_5$ is an example of a *local field,* and these types of fields are the focus of this mini-course. One key feature of $\mathbb{Q}_5$ is that studying solutions of polynomial equations in $\mathbb{Q}_5$ can often be reduced to the solving congruence relations modulo 5^n for every integer $n \geqslant 1$, and so, determining the existence of solutions over a local field can be as straightforward as solving the equation over a finite field. In contrast, over a so-called *global field* (such as the rational numbers), questions about solutions to polynomial equations can run very deep. Local and global fields are related by the *local-to-global principle*, which states, roughly speaking, that if a solution to an equation exists "everywhere locally," then it exists "globally." In the example we considered above, this would mean that if (1) has a solution over $\mathbb{Q}_p$, for every prime p, as well as over the real numbers $\mathbb{R}$, then (1) has a solution over $\mathbb{Q}$. Unfortunately, the local-to-global principle only holds for a special class of degree 2 equations, and this result is known as the *Hasse–Minkowski Theorem.* Nevertheless, the study of local solutions to polynomial equation is often a key tool to the study of global solutions. In this course, we will start by introducing the theory of local fields and their algebraic properties.

Acknowledgements. In writing these notes, I drew from many excellent texts on local fields; the main references I used are [2, Ch. 1-4], [5, Ch. 7], [5, Ch. 7], [6, Ch. 9], and [7, Ch. 1-2]. I thank Alice Pozzi for many insightful conversations during the process of writing these lecture notes, and I thank Greg Knapp, Chathumini Kondasinghe, Jaclyn Lang, Sean O'Donnell, Nick Rome, Aniruddha Sudarshan, and Ian Whitehead for helpful feedback on earlier versions of my notes and lectures.

Draft last updated: September 28, 2024

Lecture 1

One of the many useful properties of the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ is that we have a notion of size for elements in $\mathbb{R}$ or $\mathbb{C}$. Specifically, for any real number $x \in \mathbb{R}$, we can define the (real) absolute value of x by

$$|x|_{\mathbb{R}} = \begin{cases} x & \text{if } x \geqslant 0, \\ -x & \text{if } x < 0, \end{cases} \tag{1.1}$$

and for any complex number $x = a + bi$, $a, b \in \mathbb{R}$, we can define the (complex) absolute value of x by

$$|x|_{\mathbb{C}} = \sqrt{a^2 + b^2}.$$

In particular, you might notice that the restriction of $|\cdot|_{\mathbb{C}}$ to $\mathbb{R}$ agrees with $|\cdot|_{\mathbb{R}}$. It turns out that this notion of the size of an element, or more precisely, the notion of an *absolute value* on $\mathbb{R}$ or $\mathbb{C}$, is one of the key ideas that has allowed mathematicians to develop a robust analytic theory for $\mathbb{R}$ and $\mathbb{C}$. In this lecture, we explore how to generalize the notion of an absolute value and construct fields that share some important properties with $\mathbb{R}$ or $\mathbb{C}$ but also have several different features.

1.1 Absolute values

We start with the following definition of an absolute value on a field K:

Definition 1.1.1. An *absolute value* (or *multiplicative valuation*) on a field K is a function

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

such that

(i) $|x| \geqslant 0$, and $|x| = 0$ if and only if $x = 0$,

(ii) $|xy| = |x||y|$,

(iii) $|x + y| \leqslant |x| + |y|$ (the triangle inequality).

If, in addition, we have

(iv) $|x + y| \leqslant \max\{|x|, |y|\}$ (the strong triangle inequality),

the absolute value $|\cdot|$ is called *non-archimedean*. Otherwise, $|\cdot|$ is called *archimedean*.

When a field K is equipped with an absolute value, we call it a *valued field*. We start with several examples of absolute values on the following fields:

- the field of rational numbers, $\mathbb{Q} = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$,
- the field of rational functions over a finite field, $\mathbb{F}_q(t) = \left\{ \frac{g(t)}{h(t)} \,\middle|\, g(t), h(t) \in \mathbb{F}_q[t] \text{ and } h(t) \neq 0 \right\}$,
- the field of Gaussian numbers, $\mathbb{Q}(i) = \{a + bi \,|\, a, b \in \mathbb{Q}\}$.

Recall that the rings $\mathbb{Z}$, $\mathbb{F}_q[t]$, and $\mathbb{Z}[i]$ are all unique factorization domains, meaning that in each of these rings, we have a well-defined notion of unique factorization into irreducible elements. We also recall that in a unique factorization domain, an element is irreducible if and only if it is prime. These properties plays an important role when defining non-archimedean absolute values.

Example 1.1.2. For any field K, the *trivial absolute value* is defined by

$$|x| = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \neq 0. \end{cases}$$

Note that we largely omit this absolute value from our discussion.

Example 1.1.3. We give two types of absolute values on $\mathbb{Q}$:

(1) The *standard absolute value*, denoted $|\cdot|_\infty$, is defined by (1.1) restricted to $\mathbb{Q}$.

(2) For a prime p, the *p-adic absolute value* is defined by

$$|x|_p = \begin{cases} 0 & \text{if } x = 0, \\ \frac{1}{p^m} & \text{if } x \neq 0, \end{cases}$$

where we have expressed $x \in \mathbb{Q}^\times$ as $x = p^m \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $p \nmid ab$.

Example 1.1.4. We give two types of absolute values on $\mathbb{F}_q(t)$:

(1) The *degree absolute value* on $\mathbb{F}_q(t)$ is defined by

$$|f|_\infty = \begin{cases} 0 & \text{if } f = 0, \\ q^{\deg h - \deg g} & \text{if } f \neq 0, \end{cases}$$

where we have expressed $f(t) \in \mathbb{F}_q(t)^\times$ as $f = \frac{g}{h}$, for some $g, h \in k[t]$, with $h \neq 0$,

(2) For a monic irreducible polynomial $p(t)$ of degree d, the *$p(t)$-adic absolute value* is defined by

$$|f|_{p(t)} = \begin{cases} 0 & \text{if } f = 0, \\ \frac{1}{q^{dm}} & \text{if } f \neq 0, \end{cases}$$

where we have expressed $f(t) \in \mathbb{F}_q(t)^\times$ as

$$f(t) = p(t)^m \frac{g(t)}{h(t)},$$

for some $g(t), h(t) \in \mathbb{F}_q[t]$ with $p(t) \nmid g(t)h(t)$.

Example 1.1.5. If $(K, |\cdot|)$ is a valued field, then $(K, |\cdot|^s)$ is a valued field for any $s \in \mathbb{R}_{>0}$.

Example 1.1.6. Let K be a field equipped with a non-archimedean absolute value $|\cdot|$. We can extend the absolute value $|\cdot|$ to the function field $K(t)$ in a natural way by defining

$$\| f \| = \max\{|a_0|, \ldots, |a_n|\}$$

for a polynomial $f(t) = a_0 + a_1 t + \cdots + a_n t^n$.

($\star$) Example 1.1.7. We can check that 3 is a prime element in $\mathbb{Z}[i]$, which allows us to write an element $a \in \mathbb{Q}(i)^\times$ as $a = 3^m \cdot \frac{b'}{c'}$ for some elements $b', c' \in \mathbb{Z}[i]$ with $3 \nmid b'c'$. Then we can define an absolute value on $\mathbb{Q}(i)$ by

$$|x| = \begin{cases} 0 & \text{if } x = 0, \\ \frac{1}{3^m} & \text{if } x \neq 0, \end{cases}$$

and this absolute value agrees with $|\cdot|_3$ when restricted to $\mathbb{Q}$.

(⋆) **Example 1.1.8.** If we instead consider 5 as an element in $\mathbb{Q}(i)$, we see that it factors as $5 = (2+i)(2-i)$, and neither of the factors $(2 \pm i)$ is a unit in $\mathbb{Z}[i]$. As such, we cannot adapt the absolute value defined in Example 1.1.7 by replacing 3 with 5. (**Exercise 1.1.9:** Why not?)

However, we find that $(2 \pm i) \in \mathbb{Z}[i]$ are both prime elements, and there is no unit $u \in \mathbb{Z}[i]^\times$ with $(2+i) = u(2-i)$. So, for each choice of $\pi = (2 \pm i)$, we can write an element $a \in \mathbb{Q}(i)^\times$ as $a = \pi^m \cdot \frac{b}{c}$ for some elements $b, c \in \mathbb{Z}[i]$ with $\pi \nmid bc$. Then, we can define an absolute value on $\mathbb{Q}(i)$ by

$$|x|_\pi = \begin{cases} 0 & \text{if } x = 0, \\ \frac{1}{5^m} & \text{if } x \neq 0. \end{cases}$$

We want to show that both of these choices of an absolute value on $\mathbb{Q}(i)$ agree with the 5-adic absolute value when restricted to the rationals—that is, if $x \in \mathbb{Q}$, we have $|x|_5 = |x|_{2\pm i}$. Let

$$x = 5^m \frac{b}{c} = (2+i)^m (2-i)^m \frac{b}{c}$$

with integers b, c such that $5 \nmid bc$ in $\mathbb{Z}$. It suffices to show that $(2 \pm i) \nmid bc$ in $\mathbb{Z}[i]$. Suppose for the sake of a contradiction that $(2 \pm i) \cdot d = bc$ for $d \in \mathbb{Z}[i]$. Then, taking the complex absolute value squared of both sides, we obtain an equality of integers

$$5 \cdot |d|_{\mathbb{C}}^2 = |(2 \pm i)|_{\mathbb{C}}^2 |d|_{\mathbb{C}}^2 = |bc|_{\mathbb{C}}^2 = (bc)^2$$

which implies that 5 divides bc since 5 is prime when considered as an integer.

Remark 1.1.10. For a general number field, we typically define valuations attached to a prime ideal in its ring of integers rather than a prime element; we can conflate these notions in Examples 1.1.7 and 1.1.8 without confusion because of the fact that $\mathbb{Z}[i]$ is a principal ideal domain.

Exercise 1.1.11. Which of the absolute values in the examples above are non-archimedean?

Now, given a valued field $(K, |\cdot|)$, we define the distance between two points $x, y \in K$ by

$$d(x, y) = |x - y|,$$

which makes K into a metric space. In particular, the family of open balls defined by

$$B(a, r) := \{x \in K \mid |x - a| < r\}$$

forms a base of neighborhoods for a uniquely determined topology on K. We call two absolute values on K *equivalent* if they define the same topology on K. The following proposition gives concrete conditions for two absolute values on K to be equivalent:

Proposition 1.1.12. Let $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on K. The following are equivalent:

(i) $|\cdot|_1$ and $|\cdot|_2$ are equivalent.

(ii) There exists a real number $s > 0$ such that $|x|_1 = |x|_2^s$ for all $x \in K$.

(iii) For any $x \in K$, $|x|_1 < 1$ implies $|x|_2 < 1$.

Proof. We prove (ii) $\Rightarrow$ (i) $\Rightarrow$ (iii) $\Rightarrow$ (ii).

(ii) $\Rightarrow$ (i): If there exists a real number $s > 0$ such that $|x|_1 = |x|_2^s$ for all $x \in K$, the subsets

$$B_1(a, r) = \{x \in K \mid |x - a|_1 < r\} \text{ and } B_2(a, r^{1/s}) = \{x \in K \mid |x - a|_2 < r^{1/s}\}$$

coincide. Thus, the topologies induced by $|\cdot|_1$ and $|\cdot|_2$ are the same.

(i) ⇒ (iii): This implication follows from the fact that for any absolute value $|\cdot|$ on K, the inequality $|x| < 1$ is equivalent to having

$$\lim_{n\to\infty} x^n = 0$$

with respect to the topology induced by $|\cdot|$.

(iii) ⇒ (ii): Assume (iii), and fix an element $y \in K$ such that $|y|_1 > 1$. To prove (ii), it suffices to show that for any non-zero element $x \in K$, we have

$$\frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{\log|y|_2} > 0.$$

Equivalent, we show that if $|x|_1 = |y|_1^\alpha$ for some $\alpha \in \mathbb{R}$, then $|x|_2 = |y|_2^\alpha$. Indeed, let $x \in K$ with $x \neq 0$. Since $|y|_1 > 1$, there exists some $\alpha \in \mathbb{R}$ such that $|x|_1 = |y|_1^\alpha$. To prove that $|x|_2 \leqslant |y|_2^\alpha$, we construct a sequence of rational numbers $(a_n/b_n)_{n\in\mathbb{N}}$ that converges to α from above. Then, since

$$|x|_1 = |y|_1^\alpha < |y|_1^{a_n/b_n} \Longrightarrow \left|\frac{x^{b_n}}{y^{a_n}}\right|_1 < 1,$$

condition (iii) implies that

$$\left|\frac{x^{b_n}}{y^{a_n}}\right|_2 < 1 \Longrightarrow |x|_2 \leqslant |y|_2^{a_n/b_n}.$$

Thus, we have $|x|_2 \leqslant |y|_2^\alpha$, and a similar argument establishes the reverse inequality.

□

Example 1.1.13. On $\mathbb{Q}$, the norms $|\cdot|_p$ and $|\cdot|_q$ are not equivalent if $p \neq q$.

Example 1.1.14. On $\mathbb{Q}(i)$, the norms $|\cdot|_{(2\pm i)}$ defined in Example 1.1.8 are not equivalent. To see this, we note that the sequence $(2+i)^n$ converges to 0 with respect to $|\cdot|_{(2+i)}$, but $|(2+i)^n|_{(2-i)} = 1$.

We state without proof a classification of absolute values on $\mathbb{Q}$, which is due to Ostrowski:

Proposition 1.1.15 ([6, Ch.2, Proposition 3.7])**.** Every absolute value on $\mathbb{Q}$ is equivalent to either a p-adic valuation $|\cdot|_p$ or the standard absolute value $|\cdot|_\infty$.

Exercise 1.1.16. Prove the *product formula*: for every rational number $a \neq 0$, we have

$$\prod_p |a|_p = 1,$$

where p varies over all prime numbers as well as the symbol ∞.

1.2 Additive valuations

For field K equipped with a non-archimedean absolute value $|\cdot|$, we can define a function

$$v : K \to \mathbb{R} \cup \{\infty\}$$

by

$$v(x) = -\log|x| \text{ for } x \neq 0 \text{ and } v(0) = \infty,$$

where $\log : \mathbb{R}_{>0} \to \mathbb{R}$ is the natural logarithm function. In particular, the properties of a non-archimedean absolute value listed in Definition 1.1.1 translate to analogous properties of v, which we now summarize in the following definition:

Definition 1.2.1. An *additive valuation* on a field K is a function

$$v : K \to \mathbb{R} \cup \{\infty\}$$

such that

(i) $v(x) = \infty$ if and only if $x = 0$,

(ii) $v(xy) = v(x) + v(y)$,

(iii) $v(x + y) \geqslant \min\{v(x), v(y)\}$, with equality if $v(x) \neq v(y)$.

If, in addition, $v(K^\times)$ has a smallest positive value, we call the valuation v *discrete*.

We have just seen that a non-archimedean absolute value gives rise to an additive valuation on K. Conversely, for an additive valuation v on K, we obtain an absolute value by setting

$$|x| = q^{-v(x)},$$

for some fixed real number $q > 1$. As Proposition 1.1.12 might suggest, two additive valuations v_1 and v_2 on K are equivalent if $v_1 = sv_2$ for some real number $s > 0$. Throughout these notes, we switch freely between the language of multiplicative and additive valuations depending on the context. For instance, we frequently use both the "p-adic absolute value" $|\cdot|_p$ and the "p-adic valuation" v_p in discussions of $\mathbb{Q}$.

Now, given an additive valuation on a field K, we introduce the following terminology:

- The *valuation group* of K is $v(K^\times) \subseteq \mathbb{R}$. If v is discrete, then $v(K^\times) = s\mathbb{Z}$, where $s \in v(K^\times)$ is the smallest positive value; it is called *normalized* if $s = 1$.
- The *valuation ring* of K is the subset

  $$\mathcal{O} = \{x \in K \mid v(x) \geqslant 0\} = \{x \in K \mid |x| \leqslant 1\}.$$

  We see immediately from Definition 1.2.1 that $\mathcal{O}$ is a ring. More precisely, one can show that $\mathcal{O}$ an integral domain with field of fractions K that satisfies the additional property that for every $x \in K$, we have either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. (In a general context, this type of domain is referred to as a valuation ring, which is the reason for calling $\mathcal{O}$ the valuation ring of K.)
- The *unit group* of $\mathcal{O}$ is $\mathcal{O}^\times = \{x \in K \mid v(x) = 0\} = \{x \in K \mid |x| = 1\}$.
- Since $\mathcal{O}$ is a valuation ring, the subset $\mathcal{O} \smallsetminus \mathcal{O}^\times$ forms an ideal of $\mathcal{O}$. In fact, this is the unique *maximal ideal* of $\mathcal{O}$, and we denote it by

  $$\mathfrak{p} = \{x \in K \mid v(x) > 0\} = \{x \in K \mid |x| < 1\} = \{x \in \mathcal{O} \mid x^{-1} \notin \mathcal{O}\}.$$
- The *residue field* of $\mathcal{O}$ is $\kappa = \mathcal{O}/\mathfrak{p}$. If K has the same characteristic as κ, we say K is of *equal characteristic*; if not, we say K is of *mixed characteristic*. When $\kappa < \infty$, we set $q = \#\kappa$.
- When v is discrete, a *prime* (or *uniformizing*) *element* of $\mathcal{O}$ is any element $\pi \in \mathcal{O}$ such that $v(\pi)$ is the smallest positive value in the valuation group $v(K^\times)$. One can check that $\mathfrak{p} = \pi\mathcal{O}$.

Conventions. Throughout these notes, we fix the notation $\mathcal{O}, \mathfrak{p}, \kappa$ as above for a field K equipped with a non-archimedean valuation v. If in addition, v is discrete, we assume that v is normalized since we can always replace a discrete valuation with an equivalent normalized discrete valuation.

To denote a correspondence between an additive and a multiplicative valuation, we use matching subscripts but often suppress this subscript when the correspondence is implied. If a discrete valuation v gives rise to an absolute value $|\cdot|$, we write $|\cdot| = q^{-v(x)}$ for some real number $q > 1$. In particular, if the residue field κ has finite order, we take $q = \#\kappa$ unless otherwise specified.

Example 1.2.2. Let p be a prime, and equip the field $\mathbb{Q}$ with the p-adic valuation v_p. Then,

- The valuation group $v(\mathbb{Q}^\times)$ is $\mathbb{Z}$.
- The valuation ring is $\mathcal{O} = \left\{ \frac{r}{s} \in \mathbb{Q} \,\middle|\, (r,s) = 1,\, p \nmid s \right\}$.
- The unique maximal ideal of $\mathcal{O}$ is $\mathfrak{p} = \left\{ \frac{r}{s} \in \mathcal{O} \,\middle|\, p \mid r \right\}$.
- The residue field of $\mathcal{O}$ is $\kappa = \mathbb{F}_p$ via the map $\frac{r}{s} \mapsto rs^{-1} \pmod{p}$.
- We can take $\pi = p$ to be a prime element in $\mathcal{O}$.

Example 1.2.3. Equip the field $\mathbb{F}_q(t)$ with the t-adic valuation. Then,

- The valuation group $v(\mathbb{F}_q(t)^\times)$ is $\mathbb{Z}$.
- The valuation ring is $\mathcal{O} = \left\{ f(t) = \frac{g(t)}{h(t)} \in \mathbb{F}_q(t) \,\middle|\, g, h \in \mathbb{Q}[t] \text{ and } h(0) \neq 0 \right\}$.
- The unique maximal ideal of $\mathcal{O}$ is $\mathfrak{p} = \{ f(t) \in \mathcal{O} \mid f(0) = 0 \}$.
- The residue field of $\mathcal{O}$ is $\kappa = \mathcal{O}/\mathfrak{p}$ is isomorphic to $\mathbb{F}_q$ via the map $f \mapsto f(0)$.
- We can take $\pi = t$ to be a prime element in $\mathcal{O}$.

We conclude this section with the following proposition that establishes that $\mathcal{O}$ is always a principal ideal domain when v is a discrete valuation:

Proposition 1.2.4. Let v be a discrete valuation on K. The nonzero ideals of $\mathcal{O}$ are given by

$$\mathfrak{p}^n = \pi^n \mathcal{O} = \{ x \in K \mid v(x) \geqslant n \}, \quad n \geqslant 0,$$

where π is a prime element, i.e., $v(\pi) = 1$, and we have

$$\mathfrak{p}^n / \mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}. \tag{1.2}$$

Proof. Recall that by convention, we assume any discrete valuation has been normalized, so we can fix a prime element $\pi \in \mathcal{O}$ with $v(\pi) = 1$. Let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{O}$, and let $x \in \mathfrak{a}$ be an element with smallest possible value $v(x) = n < \infty$. We can write $x = u\pi^n$ for some unit $u \in \mathcal{O}^\times$, and thus $\pi^n \mathcal{O} \subseteq \mathfrak{a}$. For the reverse inclusion, if $y = u'\pi^m \in \mathfrak{a}$ is an arbitrary element with $u' \in \mathcal{O}^\times$, then $m = v(y) \geqslant n$, and hence, we have $y = (u'\pi^{m-n})\pi^n \in \pi^n \mathcal{O}$.

The isomorphism in (1.2) arises from the map $a\pi^n \mapsto a \pmod{\mathfrak{p}}$. □

Remark 1.2.5. While we have only seen examples of discrete valuations thus far, non-discrete valuations do exist—we construct an example of such a valuation in Lecture 5.

1.3 Completions

We now shift to studying how the notion of *convergence* interacts with non-archimedean absolute values; as we see below, the strong triangle inequality has many implications on the behavior of sequences in K. We start by recalling the definition of a special type of sequence:

Definition 1.3.1. A sequence $(a_n)_{n\in\mathbb{N}}$ is called *Cauchy* if, for every $\varepsilon > 0$, there exists an $N \in \mathbb{N}$ such that

$$|a_n - a_m| < \varepsilon \quad \text{for all} \quad n, m \geqslant N.$$

It is very useful to note that the characterization of Cauchy sequences simplifies considerably when the absolute value is non-archimedean. For instance, if $|\cdot|$ is non-archimedean, then a sequence $(x_n)_{n\in\mathbb{N}}$ is Cauchy if and only if

$$\lim_{n\to\infty} |x_{n+1} - x_n| = 0.$$

Moreover, if $\lim_{n\to\infty} x_n = x \neq y$ with respect to a non-archimedean absolute value $|\cdot|$, then we have

$$|x_n - y| = |x - y|$$

for sufficiently large $n \in \mathbb{N}$.

Exercise 1.3.2. Prove these claims about sequences that are Cauchy with respect to a non-archimedean absolute value and show that they need not hold for an archimedean absolute value.

Definition 1.3.3. A valued field $(K, |\cdot|)$ is called *complete* if every Cauchy sequence $(a_n)_{n\in\mathbb{N}}$ in K converges to an element $a \in K$, i.e., there exists an element $a \in K$ such that

$$\lim_{n\to\infty} |a_n - a| = 0.$$

Example 1.3.4. The field $\mathbb{R}$ is complete with respect to the real absolute value $|\cdot|_{\mathbb{R}}$.

Example 1.3.5. The field $\mathbb{Q}$ is not complete with respect to the 5-adic absolute value. To prove this, it suffices to show that there is a sequence $(x_n)_{n\in\mathbb{N}}$ of integers such that $(x_n)_{n\in\mathbb{N}}$ is Cauchy with respect to the 5-adic absolute value and such that $x := \lim_{n\to\infty} x_n$ satisfies

$$|x^2 + 1|_5 = \lim_{n\to\infty} |x_n^2 + 1|_5 = 0.$$

Indeed, if $x \in \mathbb{Q}$, this would imply that a rational number satisfies the equation $x^2 + 1 = 0$, which is impossible since all rational squares are positive. To exhibit the sequence x_n, we can start by choosing an integer x_1 such that $x_1^2 + 1 = 0 \pmod 5$. For example, take $x_1 = 2$. Then, we can construct the sequence $(x_n)_{n\in\mathbb{N}}$ iteratively such that at each step, we have

- $x_n^2 + 1 = b_n 5^n$, for some $b_n \in \mathbb{Z}$, and
- $x_{n+1} \equiv x_n \pmod{5^n}$.

More specifically, given x_n and b_n as above, we define x_{n+1} as follows. Writing

$$x_{n+1} = x_n + a_n 5^n$$

for an unknown variable $a_n \in \mathbb{Z}$, we impose the condition

$$x_{n+1}^2 + 1 = x_n^2 + 2a_n x_n 5^n + 5^{2n} + 1 = 5^n(b_n + 2a_n x_n) \equiv 0 \pmod{5^{n+1}}.$$

Thus, it suffices to solve for a_n in the congruence relation

$$b_n + 2x_n a_n \equiv b_n + 2 \cdot 2a_n \equiv 0 \pmod 5.$$

But 4 is invertible in $\mathbb{Z}/5\mathbb{Z}$, so a solution for a_n always exists.

Exercise 1.3.6. In the above example, explain how we implicitly used the fact that the polynomial $x^2 + 1$ has distinct roots mod 5.

Exercise 1.3.7. For an odd prime p, show that $\mathbb{Q}$ is not complete with respect to the p-adic absolute value by exhibiting a Cauchy sequence of rationals whose square converges p-adically to a squarefree integer. Try to adapt the method to $p = 2$—what goes wrong?

Given any valued field $(K, |\cdot|)$, the process of *completion* yields a complete valued field $(\widehat{K}, |\cdot|)$. To describe this process, we construct a field $\widehat{K}$ and show how to extend the absolute value $|\cdot|$ to $\widehat{K}$. We leave it as **Exercise 1.3.8** to prove that $(\widehat{K}, |\cdot|)$ is both complete and unique. Indeed, to construct $\widehat{K}$, we take R be the ring of all Cauchy sequences of $(K, |\cdot|)$ under term-by-term addition and multiplication, and define $\mathfrak{m}$ to be the ideal of all nullsequences with respect to $|\cdot|$, i.e.,

$$\mathfrak{m} := \left\{ \text{sequences } (x_n)_{n\in\mathbb{N}} \text{ in } K \;\middle|\; \lim_{n\to\infty} |x_n| = 0 \right\}.$$

One can show that $\mathfrak{m}$ is in fact a maximal ideal in R, so we can define a field

$$\widehat{K} := R/\mathfrak{m}.$$

We embed K into $\widehat{K}$ by mapping every $a \in K$ to the class of the constant Cauchy sequence $(a, a, a, \dots)$, and we extend the valuation $|\cdot|$ to $\widehat{K}$ by setting

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

where $a \in \widehat{K}$ is represented by the Cauchy sequence $(a_n)_{n\in\mathbb{N}}$.

Exercise 1.3.9. Why does this limit exist?

Now, the most well-known examples of complete fields are probably the fields $\mathbb{R}$ or $\mathbb{C}$, both of which are complete with respect to the standard (archimedean) absolute value. A famous theorem of Ostrowski proves that for any valued field $(K, |\cdot|)$ that is complete with respect to an archimedean valuation, there is an isomorphism σ from K onto $\mathbb{R}$ or $\mathbb{C}$ satisfying

$$|a| = |\sigma a|^s \quad \text{for all} \quad a \in K,$$

for some fixed $s \in (0, 1]$. In light of this result, henceforth, we will focus nearly all of our attention on non-archimedean absolute values. The following example of a non-archimedean absolute value on $\mathbb{Q}$ highlights many of the ideas that are to come in the next lecture:

Example 1.3.10. Let p be a prime. The *field of p-adic numbers*, denoted $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ with respect to the p-adic absolute. We now describe $\mathbb{Q}_p$ more explicitly. Following the completion process outlined above, we define

$$\mathbb{Q}_p := R/\mathfrak{m},$$

where R (resp. $\mathfrak{m}$) is the ring (resp. maximal ideal) of Cauchy sequences (resp. nullsequences) with respect to the p-adic absolute value. Consider the formal series

$$\sum_{v=m}^{\infty} a_v p^v, \tag{1.3}$$

where a_v is an integer satisfying $0 \leqslant a_v < p$ and $m \in \mathbb{Z}$. We can write down an associated sequence of partial sums

$$x_k = \sum_{v=m}^{m+k} a_v p^v.$$

In particular, the sequence $(x_k)_{k\in\mathbb{N}}$ is Cauchy since we have

$$\lim_{k\to\infty} |x_{k+1} - x_k|_p = \lim_{k\to\infty} \left|a_{k+1}p^{k+1}\right|_p \leqslant \lim_{k\to\infty} \frac{1}{p^{k+1}} = 0.$$

Thus, any formal series of the form in (1.3) is an element of $\mathbb{Q}_p$, and we prove in the next lecture that any element of $\mathbb{Q}_p$ can be expressed as such a formal series.

Lecture 2

Let K be a field that is equipped with a discrete non-archimedean valuation v. In the previous lecture, we described a process for constructing the completion $\widehat{K}$ of K with respect to v; we review a few key points of this construction using the language of additive valuations. Indeed, supposing we have constructed $\widehat{K}$, we can canonically extend v to a valuation $\widehat{v}$ on the completion $\widehat{K}$ by taking

$$\widehat{v}(a) = \lim_{n\to\infty} v(a_n),$$

where $a_n \in K$ and $a = \lim_{n\to\infty} a_n \in \widehat{K}$. Since v satisfies the strong triangle inequality, if $a \neq 0$, then the sequence $v(a_n)$ must eventually become constant. In other words, for sufficiently large n, we have an equality $v(a_n) = v(a)$, and thus, an equality of valuation groups $v(K^\times) = \widehat{v}(\widehat{K}^\times)$. This means that the extended valuation $\widehat{v}$ is also discrete and normalized.

Throughout this section, we keep the conventions set in Lecture 1. Specifically, we'll take $\mathcal{O} \subseteq K$ (resp. $\widehat{\mathcal{O}} \subseteq \widehat{K}$) to be the valuation ring of v (resp. $\widehat{v}$), and let $\mathfrak{p}$ (resp. $\widehat{\mathfrak{p}}$) be its maximal ideal.

2.1 More on completions

Continuing from the end of Lecture 1, we start with the following proposition:

Proposition 2.1.1. For $n \geqslant 1$, we have an isomorphism

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n.$$

Proof. Consider the homomorphism $\mathcal{O} \to \widehat{O}/\widehat{\mathfrak{p}}^n$ defined by

$$a \mapsto a \pmod{\widehat{\mathfrak{p}}^n}.$$

By inspection, the kernel of this map is $\mathfrak{p}^n$. To see it is surjective, we note that by the construction of $\widehat{K}$, for every $x \in \widehat{O}$, there is an element $a \in \mathcal{O}$ such that $v(x-a) \geqslant n$, i.e., $a \equiv x \pmod{\widehat{\mathfrak{p}}^n}$. □

Now, Proposition 2.1.1 implies that the residue fields of $\widehat{K}$ and K are equal; we can use this fact to characterize elements of $\widehat{K}$ using formal Laurent series:

Proposition 2.1.2. Let $R \subseteq \mathcal{O}$ be a system of representatives for $\kappa = \mathcal{O}/\mathfrak{p}$ such that $0 \in R$, and let $\pi \in \mathcal{O}$ be a prime element. Then, every $x \neq 0$ in $\widehat{K}$ admits a unique representation as a convergent series

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots),$$

where $a_i \in R$, $a_0 \neq 0$, and $m \in \mathbb{Z}$.

Proof. Let $x = \pi^m u$ for some $u \in \widehat{\mathcal{O}}^\times$ and $m \in \mathbb{Z}$. By Proposition 2.1.1, the residue class $u \pmod{\widehat{\mathfrak{p}}}$ has a unique representative $a_0 \in R$ with $a_0 \neq 0$, which means we can write $u = a_0 + \pi b_1$ for some $b_1 \in \widehat{\mathcal{O}}$. Repeating this process iteratively, for each $n \geqslant 1$, we can obtain an expression

$$u = a_0 + a_1\pi + a_2\pi^2 + \cdots + a_n\pi^n + \pi^{n+1}b_{n+1},$$

where the a_i are uniquely determined by previous equations and each $b_i \in \widehat{\mathcal{O}}$ is some element. This process yields a uniquely determined infinite series

$$\sum_{\nu=0}^{\infty} a_\nu \pi^\nu.$$

In particular, this infinite series converges to $u \in \widehat{\mathcal{O}}^\times$ since

$$\lim_{n\to\infty} |u - s_n| \leqslant \lim_{n\to\infty} |\pi^{n+1} b_{n+1}| = 0,$$

where $(s_n)_{n\in\mathbb{N}}$ is the associated sequence of partial sums. □

Example 2.1.3. Recall that in Example 1.3.10, we constructed the field of p-adic numbers, $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the p-adic valuation $|\cdot|_p$. Its valuation ring, denoted $\mathbb{Z}_p$, is called the ring of *p-adic integers* and its residue field is $\mathbb{F}_p$, the finite field with p elements. Using Proposition 2.1.2, we can now define $\mathbb{Z}_p$ as the set of formal sums

$$a_0 + a_1 p + a_2 p^2 + \cdots, \tag{2.1}$$

where a_k is an integer satisfying $0 \leqslant a_k < p$, and addition and multiplication in $\mathbb{Z}_p$ is defined via the usual carry-over rules for digits. Below are some examples of p-adic expansions of elements of $\mathbb{Z}_p$:

(a) $-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots \in \mathbb{Z}_p$,

(b) $\dfrac{1}{p-1} = 1 + p + p^2 + p^3 + \cdots \in \mathbb{Z}_p$,

(c) Example 1.3.5 give a 5-adic expansion for $i \in \mathbb{Z}_5$.

(d) **(Exercise)** Show that $x \in \mathbb{Q}_p$ is rational if and only if its p-adic expansion is periodic.

Example 2.1.4. Consider the field of rational functions $\mathbb{F}_q(t)$ equipped with the t-adic valuation v_t. We show that the completion of $\mathbb{F}_q(t)$ with respect to v_t is the *field of formal Laurent series over* $\mathbb{F}_q$, which we denote by $\mathbb{F}_q(\!(t)\!)$. Indeed, in Example 1.2.3, we computed that $\mathbb{F}_q$ is the residue of $\mathbb{F}_q(t)$ with respect to v_t. Thus, by Proposition 2.1.2, elements in the completion of $\mathbb{F}_q(t)$ with respect to v_t can be written as formal Laurent series of the form

$$f(t) = t^m(a_0 + a_1 t + a_2 t^2 + \cdots),$$

where a_i is an integer satisfying $0 \leqslant a_i < q$ and $m \in \mathbb{Z}$. The valuation ring of $\mathbb{F}_q(\!(t)\!)$ is the *ring of formal power series*, denoted $\mathbb{F}_q[\![t]\!]$.

(⋆) Example 2.1.5. We complete the field $\mathbb{Q}(i)$ with respect to the (non-archimedean) absolute value $|\cdot|_3$ defined in Example 1.1.7. Since $\mathbb{Q} \subseteq \mathbb{Q}(i)$, we have

$$\mathbb{Q}_3(i) \subseteq \widehat{\mathbb{Q}(i)}.$$

Using Proposition 2.1.2, we show that this is in fact an equality. Indeed, we first note that

$$\kappa = \mathbb{Z}[i]/(3) \cong \mathbb{Z}[x]/(3, x^2+1) \cong \mathbb{F}_3[x]/(x^2+1),$$

and since $x^2 + 1$ does not have a root in $\mathbb{F}_3$,

$$\mathbb{F}_3[x]/(x^2+1) \cong \mathbb{F}_{3^2} \ncong \mathbb{F}_3.$$

Fix a system $R \subseteq \mathbb{Z}[i]$ of representatives for κ such that each $a \in R$ is of the form $c + id$ for integers $0 \leqslant c, d < 3$, and let $x \in \widehat{\mathbb{Q}(i)}$. By Proposition 2.1.2, we can express x uniquely as a formal sum

$$x = \sum_{k \geqslant m} a_k 3^k,$$

where $a_i \in R$ and $m \in \mathbb{Z}$. Since a_k is of the form $a_k = c_k + id_k,\ 0 \leqslant c_k, d_k < 3$, for each k, we can rewrite the formal sum expression for x as

$$\begin{aligned} x &= \sum_{k \geqslant m} (c_k + id_k)3^k \\ &= \sum_{k \geqslant m} c_k 3^k + i \sum_{k \geqslant m} d_k 3^k, \end{aligned}$$

which is an element of $\mathbb{Q}_3(i)$, as desired.

(⋆) **Example 2.1.6.** We complete the field $\mathbb{Q}(i)$ with respect to the (non-archimedean) absolute value $|\cdot|_\pi$ defined in Example 1.1.8. Our approach follows the previous example identically, with the exception of two key differences: first, since $\pi = 2 \pm i$, we have

$$\mathbb{Z}[i]/(\pi) \cong \mathbb{Z}/5\mathbb{Z} \cong \mathbb{F}_5.$$

Second, we showed $|5|_\pi = |5|_5 = |\pi|_\pi$, and so, we can take $5 \in \mathbb{Z}(i)$ as a uniformizing element with respect to $|\cdot|_\pi$. Thus, by Proposition 2.1.2, we can express any $x \in \widehat{\mathbb{Q}(i)}$ uniquely as a formal sum

$$\sum_{k \geqslant m} a_k 5^k,$$

where $a_k \in \mathbb{Z}$ with $0 \leqslant a_k < 5$ and $m \in \mathbb{Z}$. We conclude that $\widehat{\mathbb{Q}(i)} = \mathbb{Q}_5$.

2.2 Locally compact fields

Henceforth, we assume $|\cdot|$ is a discrete non-archimedan absolute value and that $(K, |\cdot|)$ is a complete valued field. We denote the valuation corresponding to $|\cdot|$ by v and write $|\cdot| = q^{-v(x)}$. Let $\mathcal{O}$ denote the valuation ring of K, and let $\mathfrak{p}$ and $\kappa = \mathcal{O}/\mathfrak{p}$ denote the maximal ideal and residue field of $\mathcal{O}$, respectively. Additionally, we fix a uniformizing element $\pi \in \mathcal{O}$.

We explore some topological properties of K arising from the fact that $\mathcal{O}$ is a discrete valuation ring. Indeed, recall that the absolute value $|\cdot|$ induces a topology on K whose base of neighborhoods is given by the family of open balls

$$B(a, r) := \{x \in K \,|\, |x, a| < r\}.$$

To start, the following proposition shows that K is *totally disconnected*:

Proposition 2.2.1. The following properties hold in any field that is equipped with a non-archimedean absolute value:

(1) Any point of an open ball is a center of the ball.

(2) Two open balls are either disjoint, or one is contained in the other.

(3) Every ball is both open and closed, and all balls are homeomorphic.

Proof. We leave the proofs of (1) and (2) as **Exercise 2.2.2**. For (3), let $r > 0$, and let

$$B_c(a, r) := \{x \in K \,|\, |x, a| < r.\}$$

denote the closed ball of radius r centered at $a \in K$. Then, if $q^{-(n+1)} < r \leqslant q^{-n}$, we have

$$B(a, r) = B_c(a, q^{-(n+1)}),$$

and if $q^{-(n+1)} < r \leqslant q^{-n}$, we have

$$B_c(a, r) = B(a, q^{-n}).$$

To see that all open balls are homeomorphic, we note that the map given by

$$x \mapsto \frac{x - a}{r}$$

maps the open ball of radius r centered at a onto the open unit ball centered at 0. In particular, its inverse is given by

$$x \mapsto a + rx.$$

□

Remark 2.2.3. It will be useful in later lectures to remember that the valuation ring $\mathcal{O}$ is both open and closed in K since it coincides exactly with the closed unit ball $B_c(0, 1)$.

Exercise 2.2.4. Use Proposition 2.2.1 to give an alternative proof to Proposition 2.1.1.

Example 2.2.5. We write an explicit basis of neighborhoods in K of the zero element as the chain

$$\mathcal{O} \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \mathfrak{p}^3 \supseteq \cdots$$

of ideals in the valuation ring $\mathcal{O}$. Indeed, we have

$$\mathfrak{p}^n = \left\{ x \in K \,\middle|\, |x| < \frac{1}{q^{n-1}} \right\} = B\left(0, \frac{1}{q^{n-1}}\right).$$

While we originally defined the notion of completing a field analytically, we now give a more algebraic characterization of $\mathcal{O}$; as we see below, this new perspective on $\mathcal{O}$ is actually closely related to the language of power series we used in Proposition 2.1.2 but has some important advantages.

For $n \geqslant 1$, there are canonical homomorphisms

$$\mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p}^n$$

and

$$\mathcal{O}/\mathfrak{p} \xleftarrow{\lambda_1} \mathcal{O}/\mathfrak{p}^2 \xleftarrow{\lambda_2} \mathcal{O}/\mathfrak{p}^3 \xleftarrow{\lambda_3} \cdots.$$

This collection of maps allows us to construct a homomorphism

$$\mathcal{O} \longrightarrow \varprojlim_n \mathcal{O}/\mathfrak{p}^n$$

into the projective limit

$$\varprojlim_n \mathcal{O}/\mathfrak{p}^n = \left\{ (x_n) \in \prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n \,\middle|\, \lambda_n(x_{n+1}) = x_n,\ \forall n \geqslant 1 \right\}.$$

In particular, viewing the rings $\mathcal{O}/\mathfrak{p}^n$ as topological rings with the discrete topology, we can equip $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$ with the *product topology*, and $\varprojlim_n \mathcal{O}/\mathfrak{p}^n$ becomes a topological ring in the natural way.

We have the following characterization of $\mathcal{O}$:

Proposition 2.2.6. The canonical map

$$\mathcal{O} \longrightarrow \varprojlim_n \mathcal{O}/\mathfrak{p}^n$$

is an isomorphism (of rings) as well as a homeomorphisms (of topological spaces).

Proof. As a homomorphism of rings, this map is injective since its kernel is

$$\bigcap_{n=1}^{\infty} \mathfrak{p}^n = (0).$$

For surjectivity, let $\mathfrak{p} = \pi\mathcal{O}$, and fix a system of representatives $R \subseteq \mathcal{O}$ of $\mathcal{O}/\mathfrak{p}$ such that $0 \in R$. As we saw in the proof of Proposition 2.1.2, elements $a \pmod{\mathfrak{p}^n} \in \mathcal{O}/\mathfrak{p}^n$ can be written uniquely as

$$a \equiv a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \pmod{\mathfrak{p}^n},$$

where $a_i \in R$. In particular, this means each element $s \in \varprojlim_n \mathcal{O}/\mathfrak{p}^n$ is given by a sequence of sums

$$s_n = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}, \quad \text{for } n \geqslant 1,$$

where the $a_i \in R$ are fixed coefficients. Thus, s is the image of the element

$$x = \lim_{n\to\infty} s_n = \sum_{\nu=0}^{\infty} a_\nu \pi^\nu \in \mathcal{O}.$$

To show this map is in fact a homeomorphism, we note that it maps the basis of neighborhoods of zero in $\mathcal{O}$ given in Example 2.2.5 onto a basis of neighborhoods of zero in $\varprojlim_n \mathcal{O}/\mathfrak{p}^n$. □

Example 2.2.7. We exhibit the isomorphism in Proposition 2.2.6 for $K = \mathbb{Q}_p$. In this case, we have $\mathcal{O} = \mathbb{Z}_p$, and recall that we have been viewing a p-adic integer

$$x = \sum_{k=0}^{\infty} a_k p^k \in \mathbb{Z}_p$$

as a sequence of partial sums of integers. To translate to viewing $\mathbb{Z}_p$ as a projective limit, we instead consider x to be a sequence of residue classes

$$x_n = \sum_{k=0}^{n-1} a_k p^k \pmod{p^n} \in \mathbb{Z}/p^n\mathbb{Z},$$

so that by construction, the sequence $(x_n)_{n\in\mathbb{N}}$ satisfies the property that

$$\lambda_n(x_{n+1}) = x_n,$$

where $\lambda_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is the canonical projection. In other words, we have shown that

$$x \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_n) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \,\middle|\, \lambda_n(x_{n+1}) = x_n,\ \forall n \geqslant 1 \right\}.$$

While this might seem like a subtle change in how we view $\mathbb{Z}_p$, it has quite an impact on how we do arithmetic in $\mathbb{Z}_p$. Specifically, we replace the carry-over arithmetic used in in Example 2.1.3 with component-wise operations in the projective limit. It can be surprising that the projective limit of the finite rings $\mathbb{Z}/p^n\mathbb{Z}$ is of characteristic 0.

Now, the projective limit presentation of the valuation ring $\mathcal{O}$ not only gives a more natural ring structure but also provides new tools for studying topological properties of $\mathcal{O}$. Specifically, when the residue field $\kappa = \mathcal{O}/\mathfrak{p}$ is finite, (1.2) implies that $\mathcal{O}/\mathfrak{p}^n$ is a finite ring for every $n \geqslant 1$. So, in this case, Proposition 2.2.6 expresses $\mathcal{O}$ as the projective limit of finite rings, and thus, $\mathcal{O}$ is *compact*. This fact, combined with Proposition 2.2.1, implies that if K has finite residue field, it is *locally compact*, i.e., every point $x \in K$ has a compact neighborhood. This class of fields is very important, and so we have the following definition:

Definition 2.2.8. A *non-archimedean local field* is a field that is complete with respect to a discrete valuation and has a finite residue field.

It immediately follows from our discussion above that a non-archimedean local field $(K, |\cdot|)$ is locally compact and that its valuation ring $\mathcal{O}$ is compact.

Example 2.2.9. Here are some non-archimedean local fields that we've encountered so far:

- $(\mathbb{Q}_p, |\cdot|_p)$
- $(\mathbb{F}_q((t)), |\cdot|_t)$
- $(\mathbb{Q}_3(i), |\cdot|_3)$
- $(\mathbb{Q}_5(i) \cong \mathbb{Q}_5, |\cdot|_{(2\pm i)})$

Example 2.2.10. We give an example of a field that is complete with respect to a discrete non-archimedean absolute value but has an infinite residue field. Indeed, let $F = \mathbb{Q}(t)$ be the field of rational functions of the rational numbers, and equip F with the t-adic valuation defined in Example 1.1.4(2). As shown in Example 1.2.3, this valuation is discrete and non-archimedean, but its residue field is isomorphic to $\mathbb{Q}$ via the map $f \mapsto f(0)$.

Lecture 3

Throughout this lecture, we take $(K, |\cdot|)$ to be a non-archimedean local field and let $\mathcal{O}$ denote the valuation ring of K, and let $\mathfrak{p}$ and $\kappa = \mathcal{O}/\mathfrak{p}$ denote its maximal ideal and residue field, respectively. We also fix a choice of uniformizing element $\pi \in \mathcal{O}$.

3.1 Hensel's Lemma

Let $f(x) \in \mathcal{O}[x]$ be a polynomial, and let $\overline{f}(x) \in \kappa[x]$ denote its reduction modulo π. When f has a root in $\mathcal{O}$, then $\overline{f}$ necessarily has a root in κ. It turns out that the converse is often true in non-archimedean local fields: in this case, we say that a root of $\overline{f}$ in κ can be *lifted* to a root of f in $\mathcal{O}$. In fact, we already saw an instance of this idea in Example 1.3.5 when we constructed a root of $x^2 + 1$ in $\mathbb{Q}_5$ starting from a root in $\mathbb{F}_5$. We start with the following proposition, which is a version of Hensel's Lemma stated for roots of polynomials:

Proposition 3.1.1 (Hensel's Lemma for roots)**.** Let $f(x) \in \mathcal{O}[x]$ be a monic polynomial and suppose that there exists an element $a \in \mathcal{O}$ such that:

- $f(a) \equiv 0 \pmod{\pi}$,
- $f'(a) \not\equiv 0 \pmod{\pi}$.

Then there exists a unique $\tilde{a} \in \mathcal{O}$ such that $f(a) = 0$ and $\tilde{a} \equiv a \pmod{\pi}$.

Now, Proposition 3.1.1 is an immediate corollary of the following more general statement of Hensel's lemma. To state this general result, we recall from Example 1.1.6 that we can extend the absolute value $|\cdot|$ to the function field $K(t)$ in a natural way by defining

$$\| f \| = \max\{|a_0|, \ldots, |a_n|\}$$

for a polynomial $f(t) = a_0 + a_1 t + \cdots + a_n t^n$. We call a polynomial $f(x) \in \mathcal{O}[x]$ *primitive* if $\| f \| = 1$.

Theorem 3.1.2 (Hensel's Lemma)**.** If a primitive polynomial $f(x) \in \mathcal{O}[x]$ admits a factorization

$$f(x) \equiv \overline{g}(x)\overline{h}(x) \pmod{\mathfrak{p}}$$

into relatively prime polynomials $\overline{g}$, $\overline{h} \in \kappa[x]$, then $f(x)$ admits a factorization

$$f(x) = g(x)h(x)$$

into polynomials g, $h \in \mathcal{O}[x]$ such that $\deg(g) = \deg(\overline{g})$ and

$$g(x) \equiv \overline{g}(x) \pmod{\mathfrak{p}} \quad \text{and} \quad h(x) \equiv \overline{h}(x) \pmod{\mathfrak{p}}.$$

Proof. Our approach to this proof is similar to the iterative method that we used in Example 1.3.5 to show that there is a factorization

$$x^2 + 1 = (x - \alpha)(x - \beta)$$

over $\mathbb{Q}_5$. However, in this setting, we must be a bit careful about the degrees of the polynomials in each step of our construction. Let $d = \deg(f)$ and $m = \deg(\overline{g})$ so that $\deg(\overline{h}) \leqslant d - m$. Additionally, let g_0, $h_0 \in \mathcal{O}[x]$ be polynomials such that

- $g_0 \equiv \overline{g} \pmod{\mathfrak{p}}$,
- $h_0 \equiv \overline{h} \pmod{\mathfrak{p}}$,
- $\deg(g_0) = m$ and $\deg(h_0) \leqslant d - m$.

Since $(\overline{g}, \overline{h}) = 1$, there exist polynomials a, $b \in \mathcal{O}[x]$ such that $ag_0 + bh_0 \equiv 1 \pmod{\mathfrak{p}}$. So, we fix a choice of $\tau \in \mathfrak{p}$ such that

$$|\tau| = \max\{\| f - g_0 h_0 \|, \| ag_0 + bh_0 - 1 \|\}.$$

We now iteratively construct polynomials g_n, $h_n \in \mathcal{O}[x]$ of the form

$$g_n = g_0 + p_1\tau + \cdots + p_n\tau^n,$$
$$h_n = h_0 + q_1\tau + \cdots + q_n\tau^n,$$

where $p_i, q_i \in \mathcal{O}[x]$ are polynomials of deg $< m$ and $\leqslant d - m$, respectively, and such that for $n \geqslant 0$,

$$f \equiv g_n h_n \pmod{\tau^{n+1}}. \tag{3.1}$$

Then, taking the limit as $n \to \infty$ will give the desired $g, h \in \mathcal{O}[x]$. Indeed, (3.1) is satisfied for $n = 0$ by our choice of τ. So, assuming we have polynomials $g_n, h_n \in \mathcal{O}[x]$ satisfying (3.1), we show how to construct the desired $g_{n+1}, h_{n+1} \in \mathcal{O}[x]$. Let

$$f_{n+1} = \tau^{-(n+1)}(f - g_n h_n) \in \mathcal{O}[x].$$

Then, one can show that (3.1) holding for $n + 1$ reduces to the equivalence

$$g_0 q_{n+1} + h_0 p_{n+1} \equiv f_{n+1} \pmod{\tau}.$$

Since $g_0 a + h_0 b \equiv 1 \pmod{\tau}$ for some $a, b, \in \mathcal{O}[x]$, we can write

$$g_0 a f_{n+1} + h_0 b f_{n+1} \equiv f_{n+1} \pmod{\tau}, \tag{3.2}$$

and so we might naively take $q_{n+1} = af_{n+1}$ and $p_{n+1} = bf_{n+1}$. However, since the degrees of these choices for q_n, p_n might be too large, we instead write

$$b(x) f_{n+1}(x) = q(x) g_0(x) + p_{n+1}(x),$$

where $\deg(p_{n+1}) < \deg(g_0) = m$. Then, since the leading coefficient of g_0 is a unit, we have $q(x) \in \mathcal{O}[x]$, and thus, by plugging this expression for bf_{n+1} into (3.2), we obtain the congruence

$$g_0(af_{n+1} + h_0 q) + h_0 p_{n+1} \equiv f_{n+1} \pmod{\tau}.$$

We leave it as **Exercise 3.1.3** to show that we can take $q_{n+1} \in \mathcal{O}[x]$ to be the polynomial $af_{n+1} + h_0 q$ with all coefficients divisible by τ omitted. □

Hensel's lemma is a very powerful tool for studying complete valued fields—in fact, many of the results we prove for such fields can be proved from Hensel's lemma directly without the full strength of completeness. The remainder of this lecture gives several applications of Hensel's lemma within the context of non-archimedean local fields; the upcoming problem set explores more general properties of *Henselian fields*, i.e., fields that are equipped with a non-archimedean valuation whose valuation rings satisfies Hensel's lemma. To aid in the applications discussed below, we state without proof a stronger version of Hensel's lemma:

Theorem 3.1.4 (Hensel's Lemma, stronger version, [3, Ch. II.2, Proposition 2])**.** Let $f(x) \in \mathcal{O}[x]$ and suppose that there exists $a \in \mathcal{O}$ such that

$$|f(a)| < |f'(a)|^2.$$

Then, there exists a unique $a' \in \mathcal{O}$ such that $f(a') = 0$ and $|a' - a| < |f'(a)|$.

3.2 Squares in $\mathbb{Q}_p$

Our first application of Hensel's lemma is an explicit description of elements that are squares in $\mathbb{Q}_p$:

Proposition 3.2.1. Let p be a prime. An element $a \in \mathbb{Q}_p^\times$ is a square if and only if $a = p^{2n}u$ for some $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$ with

- $u \pmod p$ is a square in $\mathbb{F}_p$ if p is odd;
- $u \equiv 1 \pmod 8$ if $p = 2$.

Proof. Let $a \in \mathbb{Q}_p^\times$. First, we note that if $a = b^2$, for some $b \in \mathbb{Q}_p^\times$, then $v(a)$ is even, so up to rescaling by a power of p, we can assume that $a \in \mathbb{Z}_p^\times$. Suppose that $a \in \mathbb{Z}_p^\times$ is a square. If p is odd, the mod p reduction of a must be a quadratic residue. If $p = 2$, then a must be a non-zero square mod 8, and hence, $a \equiv 1 \pmod 8$.

Conversely, consider the polynomial $f(x) = x^2 - a \in \mathcal{O}[x]$. Then $f'(x) = 2x$.

- If p is odd and there exists $b \in \mathbb{Z}$ with $b^2 \equiv a \pmod p$, it follows that
$$|f(b)|_p < 1 = |f'(b)|_p^2,$$
so by Theorem 3.1.4, there exists a unique lift $\tilde{b} \in \mathbb{Z}_p$ with $\tilde{b} \equiv b \pmod p$ and $f(\tilde{b}) = 0$.
- If $p = 2$ and $a \equiv 1 \pmod 8$, we have
$$|f(1)|_2 = |1^2 - a|_2 \leqslant \frac{1}{8} < \frac{1}{4} = |2 \cdot 1|_2^2,$$
so by Theorem 3.1.4, there exists a unique $b \in \mathbb{Z}_2$ such that $|b - 1|_2 < \frac{1}{2}$ and $f(b) = 0$.

□

As we'll discuss in Lectures 5, Proposition 3.2.1 allows us to classify quadratic extensions of $\mathbb{Q}_p$.

3.3 Roots of unity in non-archimedean local fields

We next use Hensel's lemma to study roots of unity in non-archimedean local fields. For any field K, we denote the groups of n-th roots of unity and roots of unity in $K^\times$ by

$$\mu_n(K) = \{x \in K \mid x^n = 1\} \quad \text{and} \quad \mu_\infty(K) = \bigcup_{n>0} \mu_n(K),$$

respectively. Then, since any finite subgroup of the multiplicative group of a field is cyclic, $\mu_n(K)$ is cyclic of order dividing n. The group $\mu_\infty(K)$ is torsion—that is, every element has finite order—but it need not be finite. For example, $\mu_\infty(\mathbb{C})$ is infinite.

For a non-archimedean local field K, it turns out that $\mu_\infty(K)$ is always finite. To prove this fact, we start by studying the groups $\mu_n(K)$ for $p \nmid n$ via Hensel's Lemma.

Proposition 3.3.1. Let K be a non-archimedean local field with residue field $\kappa \cong \mathbb{F}_q$ of characteristic p. If $n \in \mathbb{Z}_{>0}$ is coprime to p, then $\mu_n(K)$ is cyclic of order $\gcd(n, q-1)$.

Proof. Let $a \in \mu_n(K)$ be an n-th root of unity, so that $a^n = 1$ for some $n \in \mathbb{Z}_{>0}$. Then $|a|_p^n = |1|_p$, so $a \in \mathcal{O}$. Thus, it suffices to determine the roots of $f(x) = x^n - 1$ in $\mathcal{O}$. Indeed, the polynomial $f(x) = x^n - 1 \in \mathcal{O}[x]$ has derivative $f'(x) = nx^{n-1}$. In particular, since $p \nmid n$, we see that the mod π reductions $(\bar{f}, \bar{f}')$ are coprime. Thus, since any element $a \in \mathcal{O}$ with $a^n = 1$ reduces to a non-zero element in κ, we can apply Proposition 3.1.1 to see that the roots of f are in bijection with the solutions of $\bar{f}$ in $\kappa^\times$. Since any finite subgroup of the units of a field is cyclic, we deduce that $\kappa^\times$ is a cyclic group of order $(q-1)$, and hence, the number of solutions of $\bar{f}$ in κ is equal to $\gcd(n, q-1)$. □

Now, Proposition 3.3.1 shows that $\mu_\infty(K)$ contains a cyclic subgroup of order $(q-1)$, and so we might wonder whether $\mu_\infty(K) = \mu_{q-1}(K)$. Indeed, since we have determined all the elements of $\mu_\infty(K)$ of order prime to p, to answer this question, it suffices to study the roots of unity of p-power order. However, Hensel's Lemma does not help in this respect, since

$$(x^{p^n} - 1) = (x-1)^{p^n} \in \kappa[x],$$

so that all p^n-th roots of unity reduce to 1 in κ. Instead, to study the structure of $\mu_{p^n}(K)$, we require properties of the p-adic exponential and logarithm functions. After we develop these tools in the next lecture, we prove that $\mu_{p^n}(K)$ is in fact finite; for now, however, we study this question by hand in two concrete cases.

Example 3.3.2. If K has finite characteristic, then $\mu_\infty(K) = \mu_{q-1}(K)$. This is immediate, since

$$(x^{p^n} - 1) = (x-1)^{p^n} \in K[x].$$

Example 3.3.3. Let $K = \mathbb{Q}_p$ for an odd prime p. We will show that the only p-th root of unity in $\mathbb{Q}_p$ is 1, so that $\mu_\infty(\mathbb{Q}_p) = \mu_{p-1}(\mathbb{Q}_p)$ is cyclic of order $p-1$. By contradiction, suppose that $\zeta \neq 1$ is a p-th root of 1 in $\mathbb{Q}_p$; then $\zeta = 1 + px$ for some $x \in \mathbb{Z}_p$. Then

$$\begin{aligned} 0 &= \frac{\zeta^p - 1}{\zeta - 1} = \zeta^{p-1} + \zeta^{p-2} + \cdots + \zeta + 1 \\ &= \sum_{i=0}^{p-1} (1+xp)^i. \end{aligned}$$

By noting that $(1+xp)^p = 1 + ipx \pmod{p^2}$, we obtain

$$0 = \sum_{i=0}^{p-1} (1+ipx) = p + \frac{p^2(p-1)x}{2} = p \pmod{p^2},$$

a contradiction.

Exercise 3.3.4. Show that $\mu_\infty(\mathbb{Q}_2) = \mu_2(\mathbb{Q}_2) = \{\pm 1\}$.
Hint: Show that the only 4-th roots of unity in $\mathbb{Q}_2$ are ± 1.

We continue to study fields that contain roots of unity through the remainder of this mini-course. Specifically, in Lectures 4 & 5, we consider fields of the form $\mathbb{Q}_p(\zeta_m)$, where $\zeta_m \in \overline{\mathbb{Q}}_p$ is a primitive m-th root of unity for $m \in \mathbb{Z}_{>0}$. Such a field is called a *cyclotomic field*—we will see that these types of fields are again non-archimedean local fields and that they provide an interesting class of examples for studying local fields.

3.4 The Teichmuller map

We conclude our exploration of applications related to Hensel's lemma by revisiting Proposition 2.1.2, which gave a description of the elements of a complete local field as power series with respect to a fixed prime element. As we saw in its proof, this result relies on a choice of a system of representatives in $\mathcal{O}$ for the residue field κ. For example, in $\mathbb{Z}_p$, we often choose the set of representatives, $R = \{0, 1 \dots, p-1\}$. While this choice is natural in many ways, R is not closed under multiplication, which can complicate arithmetic. As it turns out, a canonical choice of representatives can be chosen using the *Teichmuller map* that we now describe. To summarize, the non-zero representatives in this canonical choice are precisely the roots of unity in κ of order prime to p.

Theorem 3.4.1. Let K be a non-archimedean local field with residue field κ of characteristic p. There is a uniquely defined map $\omega\colon \kappa \to \mathcal{O}$, called the *Teichmuller map*, that satisfies

$$\omega(ab) = \omega(a)\omega(b).$$

Moreover, if K also has characteristic p, ω is a ring homomorphism.

To prove Theorem 3.4.1, we require the following lemma:

Lemma 3.4.2. Let $a, b \in \mathcal{O}$ such that $a \equiv b \pmod{\pi^n}$. Then $a^p \equiv b^p \pmod{\pi^{n+1}}$.

Proof. This statement is clear if $p = 2$. So, suppose p is odd and write $a = b + x\pi^n$ for some $x \in \mathcal{O}$. Then, we have

$$a^p = (b + x\pi^n)^p = \sum_{i=0}^{p} \binom{p}{i} b^i = b^p + p \cdot \pi^n y + \pi^{np} z$$

for some $y, z \in \mathcal{O}$. The result follows since the element p is in the ideal (π) if κ has characteristic p. □

Proof of Theorem 3.4.1. We construct the Teichmuller map as follows. For every element $a \in \kappa$, choose a lift of $\widetilde{a} \in \mathcal{O}$. For an element $a \in \kappa$, define the sequence

$$a_0 = a, \qquad a_{n+1} = (a_n)^{\frac{1}{p}} \text{ for } n \geqslant 0.$$

We leave it as **Exercise 3.4.3** to show that this construction makes sense because the map $x \mapsto x^p$ is a field automorphism on κ. Consider the sequence of elements of $\mathcal{O}$ given by $(\widetilde{a_n}^{p^n})_{n \geqslant 0}$. It follows from Lemma 3.4.2 that this sequence is Cauchy; moreover, its limit is independent of the choice of representatives of elements of κ in $\mathcal{O}$, again by Lemma 3.4.2. For $a \in \kappa$, we denote

$$\omega(a) := \lim_{n \to \infty} \widetilde{a_n}^{p^n}.$$

It remains to show that ω is compatible with multiplication. Given $a, b \in \kappa$, by definition

$$\omega(ab) = \lim_{n \to \infty} \widetilde{a_n b_n}^{p^n} \quad \text{and} \quad \omega(a)\omega(b) = \lim_{n \to \infty} (\widetilde{a_n} \cdot \widetilde{b_n})^{p^n}.$$

But, from Lemma 3.4.2,

$$\lim_{n \to \infty} |\widetilde{a_n b_n}^{p^n} - (\widetilde{a_n} \cdot \widetilde{b_n})^{p^n}| = 0.$$

Hence ω respects multiplication. In addition, if K has characteristic p (so $\widetilde{a_n}^{p^n} + \widetilde{b_n}^{p^n} = (\widetilde{a_n} + \widetilde{b_n})^{p^n}$), a similar argument shows that ω is compatible with addition as well. In the latter case, one can easily check that $\omega(1) = 1$, so that ω is a ring homomorphism. □

For $a \in \kappa$, we call $\omega(a) \in \mathcal{O}$ the *Teichmuller lift* of a. It is an immediate consequence of Theorem 3.4.1 that the Teichmuller map can be used to describe the roots of unity in K of order prime to p:

Corollary 3.4.4. If $\#\kappa = q$, the Teichmuller map defines a group isomorphism

$$\omega \colon \kappa^\times \to \mu_{q-1}(K).$$

In fact, using Theorem 3.4.1, we can classify non-archimedean local fields of equal characteristic, up to isomorphism:

Theorem 3.4.5. Let $(K, |\cdot|)$ be a non-archimedean local field of equal characteristic p, and let κ be the residue field of K. Then, K is isomorphic to $\kappa(\!(T)\!)$.

Proof. Let π be a prime element for K. Since K is the fraction field of $\mathcal{O}$, it suffices to show that $\mathcal{O} \cong \kappa[[T]]$. Consider the map

$$\begin{aligned} \phi \colon \kappa[[T]] &\to \mathcal{O} \\ \sum_{n \geqslant 0} a_n T^n &\mapsto \sum_{n \geqslant 0} \omega(a_n)\pi^n \end{aligned}$$

where ω is the Teichmuller map. Then, ϕ is a ring homomorphism because ω is a ring homomorphism, and it is bijective by Prop. 2.1.2. The conclusion follows. □

In the next lecture, we complete the classification of non-archimedean local fields by treating the mixed characteristic case.

Lecture 4

Throughout this section, we take $(K, |\cdot|)$ to be a non-archimedean local field. As usual, let $\mathcal{O}$ denote the valuation ring of K, and let $\mathfrak{p}$ and $\kappa = \mathcal{O}/\mathfrak{p}$ denote its maximal ideal and residue field, respectively. The goal of this lecture is to combine some of the tools we acquired in Lectures 2 & 3 to classify non-archimedean local fields and then study the multiplicative structure of $K^\times$.

4.1 Review of some field theory

Before we return to the classification of non-archimedean local fields, we recall some important facts from field theory, starting from the following definition:

Definition 4.1.1. If $K \subset L$ are fields, we say that L is a *(field) extension* of K and denote it by L/K. We say that L/K is *finite* if L is finite-dimensional as a K-vector space; in this case, the *degree* of L/K, denoted $[L : K]$ is equal to the dimension of L as a K-vector space.

Example 4.1.2. Here are some examples of finite field extensions that we have encountered so far:

(1) $\mathbb{C}/\mathbb{R}$ is a field extension of degree 2.

(2) $\mathbb{Q}(i)/\mathbb{Q}$ is a field extension of degree 2.

(3) $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$, where ζ_m is a primitive m-th root of unity, is a cyclotomic field extension. We will study this type of field extension in detail in the next lecture.

(4) $\mathbb{F}_{p^r}/\mathbb{F}_p$ is a field extension of degree r.

We frequently require the fact that if L/K is a finite extension, then every element $\alpha \in L$ is *algebraic* over K—that is, α is the root of a polynomial $g(x) \in K[x]$ of positive degree. To see this, consider the map

$$\varphi : K[x] \to L, \quad g \mapsto g(\alpha)$$

If this map were injective, the subring generated by α in L, denoted by $K[\alpha]$, would be infinite dimensional over K, which would prevent L from being finite dimensional over K. Moreover, the map is non-zero because constants are mapped to non-zero elements of L. Thus, the kernel of φ is an ideal $0 \subsetneq I \subsetneq K[x]$, and so since $K[x]$ is a principal ideal domain, we can write $\ker(\varphi) = (f(x))$ for some monic polynomial of positive degree. The polynomial $f(x) \in K[x]$ is called the *minimal polynomial* of α over K and is necessarily irreducible in $K[x]$. If, in addition, α is the root of a monic polynomial in $\mathcal{O}[x]$, we say that α is *integral* over $\mathcal{O}$, and the subring of elements in L that are integral over $\mathcal{O}$ is called the *integral closure* of $\mathcal{O}$ in L.

4.2 Classification of non-archimedean local fields

Our goal is to prove the following classification of non-archimedean local fields:

Proposition 4.2.1. Any non-archimedean local fields is either isomorphic to a finite extension of $\mathbb{Q}_p$ for a prime p or isomorphic to $\mathbb{F}_q((t))$ for a prime power q.

Before we can prove Proposition 4.2.1, we need to understand how to extend an absolute value on K to an absolute value on a finite extension L/K. Indeed, let L/K be a finite extension of degree n. We start by defining the *norm map* $N_{L/K} : L \to K$ as follows: for an element $\alpha \in L$, the *norm* of α, denoted $N_{L/K}(\alpha)$, is the determinant of the K-linear map on L defined by multiplication by α. From this definition, we obtain the following properties of the norm map:

- $N_{L/K}(0) = 0$,
- $N_{L/K}(\alpha) = \alpha^n$ for any $\alpha \in K$,
- $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$ for any $\alpha, \beta \in L$.

Exercise 4.2.2. Prove that these properties of the norm map hold.

Now, in Theorem 4.2.4 below, we use the norm map to give an explicit formula for extending the absolute value on K to an absolute value on L. The existence and uniqueness of this absolute value on L relies crucially on the following lemma, which makes use of Hensel's Lemma to characterize integrality of elements of L purely in terms of the norm map.

Lemma 4.2.3. Let $(K, |\cdot|)$ be a non-archimedean local field, and let L/K be a finite extension of degree n. Also, let $\mathcal{A} \subseteq L$ be the integral closure of $\mathcal{O}$ in L. Then, we have

$$\mathcal{A} = \left\{\alpha \in L \,\middle|\, N_{L/K}(\alpha) \in \mathcal{O}\right\}.$$

Proof. Let $\alpha \in L^\times$, and let

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$$

be the minimal polynomial of α over K. It is a (non-trivial) fact that $N_{L/K}(\alpha) = \pm a_0^m$; for a complete proof, cf. [6, Ch. 1.2]. Suppose that α is a root of the polynomial $g(x) \in \mathcal{O}[x]$. Then $f(x)$ divides $g(x)$ as a polynomial in $K[x]$; then it follows that $f(x)$ itself is in $\mathcal{O}[x]$ by Gauss's Lemma, cf. [1, Ch. 9.3 Proposition 5]. Given this, we have $\alpha \in \mathcal{A} \Rightarrow f(x) \in \mathcal{O}[x] \Rightarrow N_{L/K}(\alpha) \in \mathcal{O}$.

For the reverse implication, we use Hensel's lemma to show for any irreducible polynomial

$$g(x) = b_0 + b_1 x + \cdots + b_n x^n \in K[x]$$

such that $b_0 b_n \neq 0$, we have

$$|b_i| \leqslant \max\{|b_0|, |b_n|\} \quad \text{for} \quad 0 < i < n. \tag{4.1}$$

We then apply this to $f(x)$ to conclude that $N_{L/K}(\alpha) \in \mathcal{O} \Rightarrow a_0 \in \mathcal{O} \Rightarrow f(x) \in \mathcal{O}[x] \Rightarrow \alpha \in \mathcal{A}$. Indeed, let $g(x)$ be as above. After multiplying g by a suitable element of K, we can assume that $g \in \mathcal{O}[x]$ with $1 = \max\{|b_0|, \ldots, |b_n|\}$. Suppose for the sake of a contradiction that (4.1) does not hold, and let b_r to be the first coefficient with $|b_r| = 1 > \max\{|b_0|, |b_n|\}$. Then, we have

$$\max\{|b_0|, \cdots, |b_{r-1}|\} < 1,$$

meaning there is a modulo $\mathfrak{p}$ factorization of $g(x)$ of the form

$$g(x) \equiv x^r(b_r + b_{r+1}x + \cdots + b_n x^{n-r}) \pmod{\mathfrak{p}}.$$

However, this contradicts Hensel's lemma since $g(x)$ is assumed to be irreducible. □

We are finally ready to prove how to extend absolute values for finite extensions of non-archimedean local fields, which then allows us to prove Proposition 4.2.1:

Theorem 4.2.4. Let $(K, |\cdot|_K)$ be a non-archimedean local field, and let L/K be a finite extension of degree n. We can extend $|\cdot|_K$ in a unique way to a valuation $|\cdot|_L$ of L via the formula

$$|\alpha|_L = \left|N_{L/K}(\alpha)\right|_K^{1/n}.$$

In this case, L is also complete with respect to the extended valuation.

Proof. For $\alpha \in L$, we show that the function defined by

$$|\alpha|_L = \left|N_{L/K}(\alpha)\right|_K^{1/n} \tag{4.2}$$

is a non-archimedean absolute value on L, and by inspection, it agrees with $|\cdot|_K$ on its restriction to K. Conditions (i) and (ii) in Definition 1.1.1 follow immediately from (4.2), so we verify that the strong triangle inequality holds. Indeed, we leave it as **Exercise 4.2.5** to use Lemma 4.2.3 to prove

$$|\gamma|_L \leqslant 1 \Longleftrightarrow \gamma \in \mathcal{A} \quad \text{for all } \gamma \in L,$$

i.e., $\mathcal{A} = \mathcal{O}_L$. Once this has been established, the fact that $\mathcal{O}_L \subseteq L$ is a subring implies

$$|\gamma|_L \leqslant 1 \Rightarrow |\gamma + 1|_L \leqslant 1, \quad \text{for all } \gamma \in L,$$

which is equivalent to the strong triangle inequality.

To show that this extension of $|\cdot|_K$ to L is unique, let $|\cdot|'_L$ be another extension of $|\cdot|_K$ to L. By Proposition 1.1.12(iii), it suffices to show that for all $\alpha \in L$

$$|\alpha|_L < 1 \Rightarrow |\alpha|'_L < 1.$$

Suppose that this does not hold, i.e., there is some $\alpha \in L$ such that $|\alpha|_L < 1$ but $|\alpha|'_L > 1$. Then, if

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathcal{O}[x]$$

is the minimal polynomial of α over K, we can rearrange the equation $f(\alpha) = 0$ to obtain

$$|1|'_L = \left|-a_{d-1}\alpha^{-1} - \cdots - a_0(\alpha^{-1})^d\right|'_L \leqslant \max\{\left|a_{d-1}\alpha^{-1}\right|'_L, \ldots, \left|a_0(\alpha^{-1})^d\right|'_L\}. \tag{4.3}$$

However, since each $a_i \in \mathcal{O}$ and $|\alpha^{-1}|'_L < 1$, (4.3) yields the inequality $1 < 1$, a contradiction.

Lastly, the fact that L is complete with respect to the extended valuation follows from viewing L as a normed n-dimensional vector space over K, cf. [6, Ch. 2, Proposition 4.9]. □

Remark 4.2.6. For a non-archimedean local fields $(K, |\cdot|_K)$ of equal characteristic p, we have showed that $K \cong \mathbb{F}_q(\!(T)\!)$ for some $q = p^f$. On the other hand, we have showed that every finite extension of a local field is itself a local field. This is not a contradiction. For example, let $K = \mathbb{F}_p(\!(T)\!)$ and let $f(x) = x^2 - T$, which is irreducible over K. Denoting $L = K[x]/(f(x))$ the extension L/K is quadratic, and one can see that $L = \mathbb{F}_p(\!(x)\!)$, so that K and L are isomorphic as fields. However, the natural map

$$K = \mathbb{F}_p(\!(T)\!) \to L = \mathbb{F}_p(\!(x)\!), \qquad T \mapsto x^2$$

is not an isomorphism!

Remark 4.2.7. Theorem 4.2.4 actually holds for any complete valued field $(K, |\cdot|)$. However, if $(K, |\cdot|)$ is not complete, the uniqueness of the extension of a valuation does not hold. For example, on 5-adic valuation on $\mathbb{Q}$ extends to the non-equivalent absolute values $|\cdot|_{(2\pm i)}$ over $\mathbb{Q}(i)$.

Conventions warning. In Theorem 4.2.4, let v_K be the additive valuation associated to $|\cdot|_K$ so that v_K extends uniquely to an additive valuation v_L of L via the formula

$$v_L(\alpha) = \frac{1}{n} v_K\left(N_{L/K}(\alpha)\right).$$

While the valuation v_L is discrete, it is not necessarily normalized since by our conventions, we assume that v_K is normalized. When we need to distinguish between the valuation v_L that extends v_K and the normalized valuation on L, we use $v_{\mathfrak{p}_L}$ to denote the latter.

Proof of Proposition 4.2.1. First, let L be a finite extension of degree n of $K = \mathbb{Q}_p$ or $K = \mathbb{F}_p(\!(t)\!)$. By Theorem 4.2.4, we conclude that L is complete with respect to the (discrete non-archimedean) extended absolute value. To see that L also has a finite reside field, we note that its residue field ν is an extension of $\mathbb{F}_p$ of maximal degree n. Indeed, this follows from the fact that if $\overline{x}_1, \ldots, \overline{x}_n \in \nu$ are linearly independent over $\mathbb{F}_p$, then any choice of preimages $x_1, \ldots, x_n \in L$ are linearly independent over K.

Now, let L be a non-archimedean local field, v its discrete valuation, and p the characteristic of its residue class field. Theorem 3.4.5 already addressed the case where L has characteristic p, so we assume that L has characteristic 0. In this case, since $v(p) > 0$, the restriction of v to $\mathbb{Q}$ must be equivalent to the p-adic valuation v_p. Since K is complete, it must contain $\mathbb{Q}_p$, i.e., K is an extension of $\mathbb{Q}_p$. The finiteness of the extension $K/\mathbb{Q}_p$ follows from the local compactness of the topological vector space K. □

This classification of non-archimedean local fields leads to the following definition:

Definition 4.2.8. We call non-archimedean local fields of mixed characteristic *p-adic number fields* and non-archimedean local fields of equal characteristic *power series fields*.

4.3 Multiplicative structure of $K^\times$

We begin our study of the multiplicative structure of $K^\times$ by defining the following subsets of $K^\times$:

$$U^{(n)} = 1 + \mathfrak{p}^n = \left\{ x \in K \,\middle|\, |x| < \frac{1}{q^{n-1}} \right\}.$$

Similarly to the basis of neighborhoods of $0 \in K$ given in Example 2.2.5, the subsets $U^{(n)}$ form a basis of neighborhoods of $1 \in K^\times$. Moreover, one can check that each $U^{(n)} \subseteq \mathcal{O}^\times$ is actually a subgroup, giving a descending chain

$$\mathcal{O}^\times = U^{(0)} \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \cdots.$$

We call $U^{(n)}$ the *n-th higher unit group* and $U^{(1)}$ the *group of principal units*.

Exercise 4.3.1. Prove that for $n \geqslant 1$, there are isomorphisms

$$\mathcal{O}^\times/U^{(n)} \cong (\mathcal{O}/\mathfrak{p}^n)^\times \quad \text{and} \quad U^{(n)}/U^{(n+1)} \cong \mathcal{O}/\mathfrak{p}.$$

The next proposition uses Hensel's lemma to give an initial decomposition of $K^\times$:

Proposition 4.3.2. The multiplicative group of a non-archimedean local field K admits the decomposition

$$K^\times \cong (\pi) \times \mu_{q-1}(K) \times U^{(1)},$$

where $\pi \in \mathcal{O}$ is a uniformizing element, $(\pi) = \{\pi^k \mid k \in \mathbb{Z}\} \subseteq \mathcal{O}$, and $q = \#\kappa$.

Proof. Given the choice of a uniformizing element $\pi \in \mathcal{O}$, we can write every element $a \in K$ as $a = \pi^v \cdot u$ for $u \in \mathcal{O}^\times$. Let $\bar{u}$ the image of $u \in \kappa$. Then by Corollary 3.4.4, we have

$$u = \omega(\bar{u}) \cdot \frac{u}{\omega(\bar{u})}$$

where $\omega(\bar{u}) \in \mu_{q-1}(K)$ and $\frac{u}{\omega(\bar{u})} \in U^{(1)}$. □

Now, Proposition 4.3.2 reduces understanding the multiplicative structure of $K^\times$ to understanding the multiplicative structure of $U^{(1)}$. While it is possible to give a precise module structure of $U^{(1)}$ for any non-archimedean local field K, we restrict our attention to p-adic number fields for the remainder of this section. In this case, we can construct both an exponential function and a logarithm function, and these functions are quite useful tools. However, there's a key difference between the usual exponential and logarithm functions defined on $\mathbb{R}$ or $\mathbb{C}$: the p-adic exponential function is not defined on all of K, while the p-adic logarithm function is defined on all of $K^\times$.

To construct a p-adic logarithm function on $K^\times$, we show that there is a uniquely determined continuous homomorphism

$$\log : K^\times \to K$$

such that $\log p = 0$ and such that for principal units $(1+x) \in U^{(1)}$, we have

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots . \tag{4.4}$$

Our strategy for accomplishing this is to do the following:

(i) Show that the logarithm series defined in (4.4) converges for $(1+x) \in U^{(1)}$.

(ii) Show that the logarithm series defined in (4.4) is a homomorphism for elements in $U^{(1)}$.

(iii) Use Proposition 4.3.2 to extend the logarithm function on $U^{(1)}$ to all of $K^\times$.

Indeed, let v_p denote the valuation on K extending the usual p-adic valuation on $\mathbb{Q}_p$, and, let $(1+x) \in U^{(1)}$. For (i), we leave it as **Exercise 4.3.3** to show that if $v_p(x) > 0$, then

$$\lim_{n\to\infty} \left| \frac{x^n}{n} \right| = 0.$$

For (ii), the logarithm series in (4.4) defines a homomorphism since we have an equality

$$\log\left((1+x)(1+y)\right) = \log(1+x) + \log(1+y)$$

as formal power series, and all series in the above equation converge for $(1+x), (1+y) \in U^{(1)}$.

It remains to extend our logarithm function to all of $K^\times$. To this end, let $v_\mathfrak{p}$ be the normalized valuation on K so that $v_\mathfrak{p} = e v_p$, where $p\mathcal{O} = \mathfrak{p}^e$, and fix a choice of uniformizing element $\pi \in \mathcal{O}$. Then, for every $\alpha \in K^\times$, writing $\alpha = \pi^{v_\mathfrak{p}(\alpha)} \cdot u_\alpha$, Proposition 4.3.2 gives a unique representation

$$\alpha = \pi^{v_\mathfrak{p}(\alpha)} \omega(\bar{u}_\alpha) \frac{u_\alpha}{\omega(\bar{u}_\alpha)},$$

where $\bar{u}_\alpha$ the image of $u_\alpha \in \kappa$, $\omega(\bar{u}_\alpha) \in \mu_{q-1}(K)$, and $\frac{u_\alpha}{\omega(\bar{u}_\alpha)} \in U^{(1)}$. Defining

$$\log \pi = -\frac{1}{e} \log\left(\frac{u_p}{\omega(\bar{u}_p)} \right),$$

we obtain the desired homomorphism $\log : K^\times \to K$ by setting

$$\log \alpha = v_\mathfrak{p}(\alpha) \log \pi + \log\left(\frac{u_\alpha}{\omega(\bar{u}_\alpha)} \right).$$

By inspection, this map is continuous and satisfies the property that $\log p = 0$.

Exercise 4.3.4. Show this construction is independent of the choice of uniformizing element $\pi \in \mathcal{O}$.

We next use the p-adic logarithm to give an isomorphism $U^{(n)} \cong \mathfrak{p}^n$ for sufficiently large n:

Proposition 4.3.5. Let $K/\mathbb{Q}_p$ be a p-adic number field with valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{p}$, and let $p\mathcal{O} = \mathfrak{p}^e$. Then, for $n > \frac{e}{p-1}$, the power series

$$\log(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \cdots \quad \text{and} \quad \exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

give two mutually inverse isomorphisms (and homeomorphisms)

$$U^{(n)} \underset{\exp}{\overset{\log}{\rightleftarrows}} \mathfrak{p}^n.$$

Proof. This proof requires a careful analysis of the p-adic valuation of the terms that appear in the power series expansions of log and exp. We outline the main steps of the proof below, but leave the details as **Exercise 4.3.6**. Throughout the proof, v_p is the usual p-adic valuation on $\mathbb{Q}_p$, and we assume it has been extended (uniquely) to $K/\mathbb{Q}_p$; the normalized valuation of K is $v_\mathfrak{p} = ev_p$.

To start, let $n \in \mathbb{N}$ be a natural number with $n = \sum_{i=0}^{r} a_i p^i, 0 \leqslant a_i < p$. One can show that

(i) $\dfrac{v_p(n)}{n-1} \leqslant \dfrac{1}{p-1}$;

(ii) $v_p(n!) = \dfrac{1}{p-1} \displaystyle\sum_{i=0}^{r} a_i(p^i - 1)$.

Next, we use (i) to show that for $z \neq 0$ with $v_\mathfrak{p}(z) > \frac{e}{p-1}$, we have

$$v_p\left(\frac{z^n}{n}\right) \geqslant v_p(z) \Rightarrow v_\mathfrak{p}(\log(1+z)) = v_\mathfrak{p}(z),$$

and thus, log maps $U^{(n)}$ into $\mathfrak{p}^n$ for $n > \frac{e}{p-1}$. For the reverse map in Proposition 4.3.5, we use (ii) to show that $\exp(x)$ converges for $v_\mathfrak{p}(x) > \frac{e}{p-1}$ and that if, in addition $x \neq 0$ and $n > 1$, we have

$$v_p\left(\frac{x^n}{n!}\right) \geqslant v_p(x) \Rightarrow v_\mathfrak{p}(\exp(x) - 1) = v_\mathfrak{p}(x).$$

Thus, exp maps $\mathfrak{p}^n$ into $U^{(n)}$ for $n > \frac{e}{p-1}$. Lastly, for $v_\mathfrak{p}(x), v_\mathfrak{p}(z) > \frac{e}{p-1}$, we have

$$\exp\log(1+z) = 1 + z \quad \text{and} \quad \log\exp(x) = x,$$

by the usual identities of these formal power series. □

We finally have the tools to give a more explicit description of the structure of $K^\times$. Note that the proof of this result uses some more advanced commutative algebra techniques; the main idea is to use the isomorphism in Proposition 4.3.5 to show that we can write $U^{(1)}$ as the direct product of some number of copies of $\mathbb{Z}_p$ and a finite order subgroup, which turns out to be given by the p-power roots of unity in $K^\times$.

Proposition 4.3.7. Let K be a p-adic number field, and let $q = \#\mathcal{O}/\mathfrak{p}$. Then, we have

$$K^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^{[K:\mathbb{Q}_p]},$$

for some $a \in \mathbb{Z}_{>0}$, where this isomorphism holds both algebraically and topologically.

Proof. By Proposition 4.3.2, it suffices to describe the structure of $U^{(1)}$ an abelian group. We prove this in two cases. First, if $\frac{e}{p-1} < 1$, Proposition 4.3.5 immediately implies that $U^{(1)} \cong \mathfrak{p} = \pi\mathcal{O} \cong \mathcal{O}$, so it suffices to describe the latter as an abelian group. Here K is a finite extension of $\mathbb{Q}_p$, so that $\mathcal{O}$ can be viewed as a $\mathbb{Z}_p$-module. It is also finitely generated, cf. [2, Proposition 2.36], so it must be isomorphic to $\mathcal{O} \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ as a $\mathbb{Z}_p$-module by the structure theorem for finitely generated modules over PIDs. This concludes the argument in case $\frac{e}{p-1} < 1$.

On the other hand, if $\frac{e}{p-1} > 1$, we pick some $n > \frac{e}{p-1}$, and note that $U^{(n)} \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$. In addition, $U^{(1)}$ itself has a canonical structure of $\mathbb{Z}_p$-module: for $a \in \mathbb{Z}_p$, we choose a sequence of $a_n \in \mathbb{Z}_{>0}$ with $a_n \to a$ in $\mathbb{Z}_p$ and for $x \in \mathfrak{p}$, define

$$(1+x)^a := \lim_{n\to\infty} (1+x)^{a_n} \tag{4.5}$$

We leave it as **Exercise 4.3.8** to show that (4.5) gives a well-defined $\mathbb{Z}_p$-module structure on $U^{(1)}$.

Now, we have the following commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U^{(n)} & \longrightarrow & \mathcal{O}^\times & \longrightarrow & (\mathcal{O}/\mathfrak{p}^n)^\times & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & U^{(1)} & \longrightarrow & \mathcal{O}^\times & \longrightarrow & (\mathcal{O}/\mathfrak{p})^\times & \longrightarrow & 1 \end{array}$$

where the rows are exact. In particular, the Snake Lemma, cf. [4, Ch. III.9, Lemma 9.1], implies that

$$U^{(1)}/U^{(n)} \cong \ker\left((\mathcal{O}/\mathfrak{p}^n)^\times \to (\mathcal{O}/\mathfrak{p})^\times\right).$$

Moreover, the map

$$\mathcal{O}/\pi^{n-1} \to U^{(1)}/U^{(n)}, \qquad a \mapsto 1 + \pi a$$

is a bijection (though not a group homomorphism!), so the target has order q^{n-1}. Thus, we have an exact sequence of $\mathbb{Z}_p$-modules,

$$1 \to U^{(n)} \to U^{(1)} \to U^{(n)}/U^{(1)} \to 1$$

where $U^{(n)}$ is free of rank $[K:\mathbb{Q}_p]$ and the quotient $U^{(n)}/U^{(1)}$ is finite of order q^{n-1}. From the structure theorem for finitely generated modules over PIDs, cf. [1, Ch. 12.1, Theorem 5], we have

$$U^{(1)} \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times C,$$

for C a finite group of order dividing q^{n-1}. But C is a finite subgroup of the multiplicative group of a field, so it has to be cyclic of p-power order. This concludes the general case. □

Remark 4.3.9. We have the following analogous statement for when K is a power series field:

$$K^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}_p^{\mathbb{N}}.$$

As in the above proof, we need to determine the $\mathbb{Z}_p$-module structure of $U^{(1)}$, but this setting requires a much more involved argument; see [6, Ch. 2, Proposition 5.7] for a complete proof.

Lecture 5

Throughout this section, we take $(K, |\cdot|_K)$ to be a non-archimedean local field and let v_K be the additive valuation associated to $|\cdot|_K$. Recall from Theorem 4.2.4 that if L/K is a finite extension of degree n, then v_K extends uniquely to an additive valuation v_L of L via the formula

$$v_L(\alpha) = \frac{1}{n} v_K\left(N_{L/K}(\alpha)\right). \tag{5.1}$$

Following our usual conventions, we denote the valuation ring of K by $\mathcal{O}_K$ and its maximal ideal and residue field by $\mathfrak{p}_K$ and κ_K, respectively. The corresponding invariants for the finite extension L/K are denoted by $\mathcal{O}_L, \mathfrak{p}_L$, and κ_L. From (5.1), we observe that

$$v_K(K^\times) \subseteq v_L(L^\times) \quad \text{and} \quad \kappa_K \subseteq \kappa_L.$$

Our goal in this lecture is to study how valuation groups and residue fields behave in extensions of non-archimedean local fields, which is a first step towards classifying p-adic fields.

5.1 Quadratic extensions of $\mathbb{Q}_p$

We begin by using Propositions 3.2.1 and 4.3.7 to classify quadratic extensions of $\mathbb{Q}_p$. Indeed, let $L/\mathbb{Q}_p$ be a quadratic extension of K so that we have $L = \mathbb{Q}_p(\alpha)$, where α is the root of an irreducible quadratic polynomial $f(x) = ax^2 + bx + c \in \mathbb{Q}_p[x]$. By the quadratic formula, we can write

$$\alpha = \frac{-b + \sqrt{b^2 - 4ac}}{2c},$$

and so for $\Delta = b^2 - 4ac$, we have $L = \mathbb{Q}_p(\sqrt{\Delta})$. Thus, to classify the possible quadratic extensions of $\mathbb{Q}_p$, it suffices to determine the structure of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. To this end, Proposition 4.3.7 gives

$$\mathbb{Q}_p^\times \cong (p) \times \langle \omega(a) \rangle \times U^{(1)},$$

where $\omega(a)$ is the Teichmuller lift of a generator $a \in \mathbb{F}_p^\times$, i.e., $\langle \omega(a) \rangle \cong \mu_{p-1}(\mathbb{Q}_p)$. Now, when p is an odd prime, Proposition 3.2.1 implies that we have

$$(\mathbb{Q}_p^\times)^2 \cong (p^2) \times \langle \omega(a)^2 \rangle \times U^{(1)},$$

and thus,

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

To summarize, we have shown the following classification of quadratic extension of $\mathbb{Q}_p$:

Proposition 5.1.1. When p is odd, there are 3 quadratic extensions of $\mathbb{Q}_p$, up to isomorphism.

Exercise 5.1.2. Determine, up to isomorphism, the number of quadratic extensions of $\mathbb{Q}_2$.

We exhibit these extensions of $\mathbb{Q}_p$ explicitly in the example below, which allows us to compare and contrast the behavior of the valuation group and residue field in each extension.

Example 5.1.3. Let p be an odd prime and fix a choice of integer $0 < a \leqslant p-1$ such that a is not a square modulo p. We define the following quadratic extensions of $K = \mathbb{Q}_p$:

- $L_1 = \mathbb{Q}_p(\sqrt{p})$
- $L_2 = \mathbb{Q}_p(\sqrt{ap})$

- $L_3 = \mathbb{Q}_p(\sqrt{a})$

By our above discussion, L_1, L_2, and L_3 are the three non-isomorphic quadratic extensions of $\mathbb{Q}_p$, so let's compare the valuation groups of these extensions. Indeed, for ease of notation, we shorten the subscript "L_i" to "i" on the invariants associated to L_i. For example, v_i denotes the additive valuation on L_i extending the p-adic valuation on $\mathbb{Q}_p$. We first note that $v_p(\mathbb{Q}_p^\times) = v_3(L_3^\times) = \mathbb{Z}$ since $a = (\sqrt{a})^2$ implies

$$v_3(a) = 2v_3(\sqrt{a}) \Rightarrow v_3(\sqrt{a}) = 0.$$

On the other hand, since $p = (\sqrt{p})^2$, we have

$$v_1(p) = 2v_1(\sqrt{p}) \Rightarrow v_1(\sqrt{p}) = \frac{1}{2},$$

which means $v_p(\mathbb{Q}_p^\times) \subsetneq v_1(L_1^\times) \subseteq \frac{1}{2}\mathbb{Z}$. A similar argument shows $v_p(\mathbb{Q}_p^\times) \subsetneq v_2(L_2^\times) \subseteq \frac{1}{2}\mathbb{Z}$.

Exercise 5.1.4. Prove that $\kappa_1 = \kappa_2 = \mathbb{F}_p$ but $\mathbb{F}_p \subsetneq \kappa_3$.

5.2 Ramification index and inertia degree

As Example 5.1.3 illustrated, the relative behavior of valuation groups and residue fields is useful in characterizing extensions of non-archimedean local fields, which leads us to the following definition:

Definition 5.2.1. We define the *ramification index* of the extension L/K to be the index

$$e = e(L/K) = \left(v_L(L^\times) : v_K(K^\times)\right),$$

and we define the *inertia degree* of the extension L/K to be the degree

$$f = f(L/K) = [\kappa_L : \kappa_K].$$

Exercise 5.2.2. Prove that if $K \subseteq L \subseteq M$ is a tower of non-archimedean local fields, then

$$e(M/K) = e(M/L)e(L/K) \quad \text{and} \quad f(M/K) = f(M/L)f(L/K).$$

Now, we've already seen that $n \geqslant f$ in the proof of Proposition 4.2.1, and we can observe that $n \geqslant e$ by (5.1). In fact, we have a much more precise relationship between the degree of the field extension L/K and its ramification index and inertia degree:

Proposition 5.2.3. If L/K is a finite extension of non-archimedean local fields, then

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

Proof. We first prove the inequality $ef \leqslant [L : K]$. Let $w_1, \ldots, w_f \in \mathcal{O}_L$ be representatives of a basis of κ_L/κ_K, and let $\pi_L \in \mathcal{O}_L$ be a prime element in $\mathcal{O}_L$ so that $1, \pi_L, \ldots, \pi_L^{e-1} \in L^\times$ represent the cosets in $v_L(L^\times)/v_K(K^\times)$. We show that the elements

$$\left\{w_j\pi_L^i \,\middle|\, 1 \leqslant j \leqslant f \text{ and } 0 \leqslant i \leqslant e-1\right\} \tag{5.2}$$

are linearly independent over K. Suppose that

$$\sum_{i=0}^{e-1}\left(\sum_{j=1}^{f} a_{ij}w_j\right)\pi_L^i = \sum_{i=0}^{e-1} s_i\pi_L^i = 0, \tag{5.3}$$

where $a_{ij} \in K$ with some $a_{ij} \neq 0$. Without loss of generality, assume that for each $0 \leqslant i \leqslant e-1$, if $s_i \neq 0$, then $v_K(a_{i1})$ is minimal among the coefficients of s_i. We first show that if $s_i \neq 0$, then $v_L(s_i) \in v_K(K^\times)$. Indeed, since the set $\{w_j\}$ form a set of representatives of a basis of κ_L/κ_K, if $s_i \neq 0$, then we have a linear combination

$$\frac{s_i}{a_{i1}} \equiv w_1 + b_{i2}w_2 + \cdots + b_{if}w_f \not\equiv 0 \pmod{\mathfrak{p}_L}, \tag{5.4}$$

which implies $v_L(\frac{s_i}{a_{i1}}) < 1$. However, the b_{ij} in (5.4) are all in $\mathcal{O}_K$ so that $v_L(\frac{s_i}{a_{i1}}) \geqslant 0$. Thus,

$$v_L\left(\frac{s_i}{a_{i1}}\right) = 0 \Longrightarrow v_L(s_i) = v_K(a_{i1}) \in v_K(K^\times).$$

Returning to (5.3), we can combine our assumption that there is some $a_{ij} \neq 0$ with the strong triangle inequality to conclude that there must be some $\ell \neq i$ with

$$v_L(s_i\pi_L^i) = v_L(s_\ell\pi_L^\ell) \neq 0.$$

However, this gives a contradiction since it would imply that

$$v_L(\pi_L^i) = v_L(\pi_L^\ell) + v_L(s_\ell) - v_L(s_i) \equiv v_L(\pi_L^\ell) \pmod{v_K(K^\times)}.$$

The reverse inequality $ef \geqslant [L:K]$ follows from the fact that the set in (5.2) gives an integral basis of $\mathcal{O}_L$ over $\mathcal{O}_K$. To see this, consider the $\mathcal{O}_K$-module

$$M = \sum_{i=0}^{e-1}\sum_{j=1}^{f} \mathcal{O}_K w_j \pi_L^i.$$

We leave is as **Exercise 5.2.4** to first show that for each $n \geqslant 1$, we have

$$\mathcal{O}_L = M + \mathfrak{p}_K^n \mathcal{O}_L,$$

and then use this fact to conclude $M = \mathcal{O}_L$, as desired. □

The equality $[L:K] = ef$ is often called the *fundamental identity*. As we see in the next section, this relationship between the ramification index and inertia degree plays an important role in the study of extensions of non-archimedean local fields, starting from the following definition:

Definition 5.2.5. Let L/K be a finite extension of non-archimedean local fields of degree n, and let $e = e(L/K)$ and $f = f(L/K)$ be the ramification index and inertia degree of L/K, respectively.

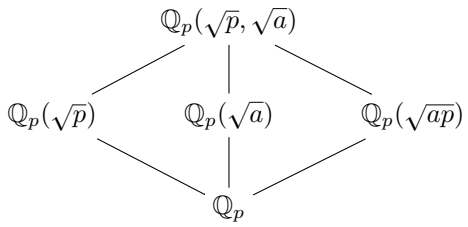
(a) If $e = 1$ (and $f = n$), we call the extension L/K *unramified*.

(b) If $e = n$ (and $f = 1$), we call the extension L/K *totally ramified*.

It can be useful to keep in mind the following characterization of unramified and totally ramified extensions: an extension L/K in unramified when π_K is a generator for the maximal ideal $\mathfrak{p}_L \subseteq \mathcal{O}_L$ and is totally ramified when the residue field does not grow, i.e., $\kappa_L = \kappa_K$.

Example 5.2.6. Continuing Example 5.1.3, we've shown that $\mathbb{Q}_p$ has two totally ramified quadratic extensions and one unramified quadratic extension. Consider the quartic extension $\mathbb{Q}_p(\sqrt{p}, \sqrt{a})/\mathbb{Q}_p$. It is the composite of two totally ramified quadratic extensions of $\mathbb{Q}_p$ but is not itself totally ramified. Rather, as we see in the field diagram below, $\mathbb{Q}_p(\sqrt{p}, \sqrt{a})/\mathbb{Q}_p$ contains an unramified subextension

$\mathbb{Q}_p(\sqrt{a})$, and so since ramification indices and inertia degrees are multiplicative in field extensions, we conclude that $\mathbb{Q}_p(\sqrt{p}, \sqrt{a})/\mathbb{Q}_p$ has both ramification index and inertia degree equal to 2.



Example 5.2.7. While we do not prove it in this mini-course, it turns out there are only finitely many extensions of a non-archimedean local field of a fixed degree. For $p < 200$, the LMFDB database [8] classifies (up to isomorphism) all p-adic fields of degree < 16 and provides interesting information about each p-adic field, including its ramification index and inertia degree over $\mathbb{Q}_p$.

5.3 Decomposing extensions of non-archimedean local fields

We now shift our focus to decomposing an extension of non-archimedean local fields into subextensions that have specific ramification behavior. The key idea that allows such a decomposition is that every finite extension L/K contains a (unique) maximal unramified subextension whose residue field is equal to κ_L. This follows from the next proposition, which characterizes unramified subextensions of a non-archimedean local field:

Proposition 5.3.1. Let L/K be a finite extension of non-archimedean local fields. The map $K' \mapsto \kappa'$ sending an unramified extension K' of K contained in L to its residue field κ' is a one-to-one correspondence between the sets

$$\{K \subseteq K' \subseteq L,\ K'/K \text{ unramified }\} \longleftrightarrow \{\kappa \subseteq \kappa' \subseteq \kappa_L\}.$$

Moreover, the bijection is compatible with inclusion.

Proof. We start by showing surjectivity: let κ' be a field with $\kappa \subseteq \kappa' \subseteq \kappa_L$, and write $\kappa' = \kappa(\alpha)$ for some $\alpha \in \kappa_L$. Also, let $f(x) \in \kappa[x]$ be the minimal polynomial of α over κ. Then, over κ', we have

$$f(x) = (x - \alpha)g(x), \tag{5.5}$$

and since any irreducible polynomial in $\kappa[x]$ is coprime to its derivative, cf. [1, Chapter 13.5, Proposition 37], the factors $g(x)$ and $(x - \alpha)$ are coprime. Take any monic lift $\tilde{f}(x) \in \mathcal{O}_K[x]$ of degree $\deg f = n$; by Proposition 3.1.1, there is a factorization

$$\tilde{f} = (x - \tilde{\alpha})\tilde{g}(x),$$

for $\tilde{\alpha} \in \mathcal{O}_L$ and $\tilde{g} \in \mathcal{O}_L[x]$. Since f is irreducible over κ, $\tilde{f}$ must be irreducible over K, so that $\tilde{f}$ is the minimal polynomial of $\tilde{\alpha}$ over K. Let $K' := K[\tilde{\alpha}]$. Its residue field contains κ', so that $f(K'/K) \geqslant [\kappa' : \kappa] = n$. On the other hand, by the fundamental identity, we have

$$n = [K' : K] = e(K'/K)f(K'/K)$$

which forces $e(K'/K) = 1$ and $f(K'/K) = n$. Thus, K'/K is unramified with residue field κ'.

To show injectivity, and compatibility with inclusion, we proceed as follows. Let $K_1, K_2 \subseteq L$ be two unramified extensions of K with residue fields

$$\kappa \subseteq \kappa_1 \subseteq \kappa_2 \subseteq \kappa_L.$$

As above, write $\kappa_1 = \kappa(\alpha)$, let f be the minimal polynomial of α over κ, and take $\tilde{f} \in \mathcal{O}_K[x]$ to be any monic lift of f of degree $n = \deg f$. By the uniqueness in Proposition 3.1.1, we deduce that there is a unique root $\tilde{\alpha} \in \mathcal{O}_L$ of $\tilde{f}$ reducing to $\alpha \in \kappa_L$. Moreover, since $\alpha \in \kappa_1 \subseteq \kappa_2$, $\tilde{\alpha}$ is contained in both K_1 and K_2. However, since K_1 is unramified, comparing degrees as above gives $K_1 = K(\tilde{\alpha})$, and we conclude $K_1 \subseteq K_2$. □

Remark 5.3.2. In the proof of Proposition 5.3.1, we took $\tilde{f}(x) \in \mathcal{O}[x]$ to be a lift of the minimal polynomial $f(x) \in \kappa[x]$ of *any* generator of the field extension κ'/κ_K. Thus, if $\#\kappa' = p^f$, we can assume that $f(x)$ divides $x^{p^f-1} - 1 \in \kappa[x]$, cf. [1, Ch. 14.2, Proposition 15].

As an immediate consequence of Proposition 5.3.1, we see that if L/K is a finite extension of non-archimedean local fields, then there is a unique maximal intermediate extension

$$K \subseteq K_{\mathrm{ur}} \subseteq L$$

that is unramified over K and has degree $f(L/K)$. Thus, by Proposition 5.2.3, we have

$$e(L/K)f(L/K) = [L : K] = [L : K_{\mathrm{ur}}][K_{\mathrm{ur}} : K] = [L : K_{\mathrm{ur}}] \cdot f(L/K).$$

We can therefore express L/K as a totally ramified extension of an unramified extension:

$$\begin{array}{c} L \\ \Big| \text{ totally ramified, degree } e(L/K) \\ K_{\mathrm{ur}} \\ \Big| \text{ maximal unramified, degree } f(L/K) \\ K \end{array} \tag{5.6}$$

This type of field diagram is especially useful because we can give explicit descriptions of unramified and totally ramified extensions of non-archimedean local fields.

Now, to illustrate this decomposition idea more concretely, we revisit an important example that appeared in Lecture 3: cyclotomic extensions of $\mathbb{Q}_p$, i.e., $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$, where $\zeta \in \overline{\mathbb{Q}}_p$ is a primitive m-th root of unity. The following two examples demonstrate that ramification in the extension $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ behaves completely differently depending on whether p dividies m. By understanding the two cases $(m, p) = 1$ and $m = p^s$, we can describe ramification in a general cyclotomic extension of $\mathbb{Q}_p$.

Example 5.3.3. Let $\zeta \in \overline{\mathbb{Q}}_p$ be an m-th root unity, where $(m, p) = 1$, and let $L = \mathbb{Q}_p(\zeta)$. We use the same approach as in the proof of Proposition 5.3.1 to show $L/\mathbb{Q}_p$ is an unramified extension of degree f, where f is the smallest natural number such that $p^f \equiv 1 \pmod{m}$. Indeed, let $\phi(x) \in \mathbb{Z}_p[x]$ be the minimal polynomial of ζ over $\mathbb{Q}_p$. Since $\phi(x) \mid x^m - 1$, we can apply Hensel's lemma as in the proof of Proposition 3.3.1 to see that the modulo $\mathfrak{p}_L$ reduction $\overline{\phi}(x) \in \mathbb{F}_p[x]$ is the minimal polynomial of $\overline{\zeta} = \zeta \pmod{\mathfrak{p}_L}$ over κ_L. Thus, since $\phi(x)$ and $\overline{\phi}(x)$ have equal degrees, we have shown

$$[L : \mathbb{Q}_p] = [\mathbb{F}_p(\overline{\zeta}) : \mathbb{F}_p] \leqslant [\kappa_L : \mathbb{F}_p] \leqslant [L : \mathbb{Q}_p],$$

i.e., $L/\mathbb{Q}_p$ is unramified. Now, let $f = [\kappa_L : \mathbb{F}_p]$ so that $\#\kappa_L = p^f$. To see that f is the smallest number such that $n \mid p^f - 1$, we note that $\kappa_L^\times$ contains a cyclic subgroup of order m generated by $\overline{\zeta}$. Thus, $m \mid p^f - 1$, and the minimality of f follows since $\kappa_L = \mathbb{F}_p(\overline{\zeta})$.

Example 5.3.4. Let $\zeta \in \overline{\mathbb{Q}}_p$ be a p^s-th root unity, and let $L = \mathbb{Q}_p(\zeta)$. We show that $L/\mathbb{Q}_p$ is a totally ramified extension of degree $(p-1)p^{m-1}$ and that $1-\zeta \in \mathcal{O}_L$ is a prime element. We consider the two cases $s = 1$ and $s \geqslant 2$:

(i) Let $s = 1$, and recall from Example 3.3.3 that ζ is a root of the polynomial

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

One can show that $\Phi_p(x)$ is the minimal polynomial of ζ over $\mathbb{Q}_p$, meaning $[L : \mathbb{Q}_p] = p - 1$. Moreover, we can factor $\Phi_p(x)$ over $\mathcal{O}_L$ as $\Phi_p(x) = \prod_{i=1}^{p-1}(x - \zeta^i)$, which yields the equality

$$\Phi_p(1) = p = \prod_{i=1}^{p-1}(1 - \zeta^i).$$

We leave it as **Exercise 5.3.5** to use the identity

$$1 - \zeta^i = (1 - \zeta)(1 + \zeta + \cdots + \zeta^{i-1})$$

to show that $v_L(1 - \zeta) = v_L(1 - \zeta^i)$ for $1 \leqslant i \leqslant p - 1$, from which it follows that

$$v_L(p) = (p - 1)v_L(1 - \zeta) \Rightarrow v_L(1 - \zeta) = \frac{1}{p - 1}.$$

Thus, by Proposition 5.2.3, we have $v_L(L^\times) = \frac{1}{p-1}\mathbb{Z}$, and our conclusion follows.

(ii) Let $s = t + 1 \geqslant 2$. Since ζ^{p^t} is a p-th root of unity, case (i) shows that

$$v_L(\zeta^{p^t} - 1) = \frac{1}{p - 1}.$$

Now, write $\zeta = 1 + \eta$ for some $\eta \in \mathcal{O}_L$ with $v_L(\eta) > 0$ so that we have

$$\zeta^{p^t} - 1 = (1 + \eta)^{p^t} - 1 = \eta^{p^t} + p\eta y, \tag{5.7}$$

for some $y \in \mathcal{O}_L$. By rearranging (5.7) and using that $v_L(p\eta y) > v_L(p) \geqslant \frac{1}{p-1} = v_L(\zeta^{p^t} - 1)$, we obtain

$$v_L(\eta^{p^t}) = \frac{1}{p - 1} \Rightarrow v_L(\eta) = v_L(\zeta - 1) = \frac{1}{(p - 1)p^t}.$$

To conclude that $v_L(L^\times) = \frac{1}{(p-1)p^t}$, we note that ζ is a root of the polynomial $\Phi_p(x^{p^t})$, meaning

$$[L : \mathbb{Q}_p] \leqslant (p - 1)p^t.$$

We now combine Examples 5.3.3 and 5.3.4 to determine the behavior of ramification in a general cyclotomic extension of $\mathbb{Q}_p$. Let ζ_m be a primitive m-th root of unity and write $m = m'p^s$, with $(m', p) = 1$. We can decompose the extension $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ into a tower of subextensions as follows:

$$\begin{array}{c} L = \mathbb{Q}_p(\zeta_m) \\ \Big| \text{ totally ramified, degree } p^{s-1} \\ K_{\mathrm{ur}}(\zeta_p) \\ \Big| \text{ totally ramified, degree } p - 1 \\ K_{\mathrm{ur}} = \mathbb{Q}_p(\zeta_{m'}) \\ \Big| \text{ maximal unramified, degree } f \text{ as in Ex. 5.3.3} \\ K = \mathbb{Q}_p \end{array}$$

We conclude that the extension $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ is neither unramified nor totally ramified. Instead, it has ramification index $(p - 1)p^{s-1}$ and its residue field is of degree f over $\mathbb{F}_p$.

Remark 5.3.6. As promised in Remark 1.2.5, we construct a field that is equipped with a non-discrete valuation. Let $K = \mathbb{Q}_p(\zeta_p)$, and for each $n \geqslant 1$, let $K_n = \mathbb{Q}_p(\zeta_{p^{n+1}})$. Then, we have the following infinite tower of non-archimedean local fields:

$$\mathbb{Q}_p \subset K \subset K_1 \subset \cdots \subset K_n \subset \cdots$$

At each step in this construction, we can extend the p-adic valuation v_p on $\mathbb{Q}_p$ to a discrete valuation on K_n. However, if we define $K_\infty = \bigcup_{n \geqslant 1} K_n$, then Example 5.3.4 shows that v_p extends to a non-discrete valuation on K_∞. This type of construction plays an important role in *Iwasawa theory*.

For a general extension L/K of non-archimedean local fields, the process of decomposing L/K into a diagram of the form (5.6) is of course a bit more complicated than in the cyclotomic case. However, we can still describe it in a surprisingly explicit way. Indeed, the maximal unramified subextension $K \subseteq K_{\mathrm{ur}} \subseteq L$ is obtained by adjoining all roots of unity contained in L whose order is prime to the characteristic of κ_K; this follows exactly as in Example 5.3.3 but replacing $\mathbb{Q}_p$ with K. As for the totally ramified extension L/K_{ur}, the following proposition characterizes totally ramified extensions of non-archimedean local fields:

Proposition 5.3.7. Let L/K be a finite extension of non-archimedean local fields. Then, L/K is totally ramified if and only if $L = K(\alpha)$, where α is a root of a polynomial

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$$

with

$$v(a_0) = 0,\ v(a_i) > 0 \text{ for } i = 1, \ldots, n-1, \text{ and } v(a_n) = 1.$$

Such a polynomial is called an *Eisenstein* polynomial.

Proof. We leave the proof of this proposition for your future explorations of local fields, but if you want a proof now, see [5, Proposition 7.55]. □

Thus, Propositions 5.3.1 and 5.3.7 show that we can characterize unramified and totally extensions of $\mathbb{Q}_p$ using roots of cyclotomic and Eisenstein polynomials, respectively. While the construction of the totally ramified extensions $\mathbb{Q}_p(\zeta_{p^s})/\mathbb{Q}_p$ in Example 5.3.4 might seem unrelated to Proposition 5.3.7, the two are actually related in an interesting way: since

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

we see that the shifted polynomial

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \cdots + \frac{p(p-1)}{2}x + p$$

has $\zeta_p - 1$ as a root and is an Eisenstein polynomial in $\mathbb{Q}_p[x]$. Similarly, we can show that $\zeta_{p^s} - 1$ is a root of the Eisenstein polynomial $\Phi_p((x+1)^{p^{s-1}})$, and thus, the totally ramified cyclotomic extensions $\mathbb{Q}(\zeta_{p^s})/\mathbb{Q}_p$ are generated by roots of Eisenstein polynomials.

Bibliography

[1] D.S. Dummitt and R.M. Foote. *Abstract Algebra*. 3rd Edition, John Wiley & Sons, Inc., 2004.

[2] Pierre Guillot. *A gentle course in local class field theory*. Cambridge University Press, Cambridge, 2018. Local number fields, Brauer groups, Galois cohomology.

[3] S Lang. *Algebraic Number Theory*. Springer-Verlag, 1994.

[4] Serge Lang. *Algebra*, volume 211. Springer Science & Business Media, 2012.

[5] James S Milne. *Algebraic number theory*. https://www.jmilne.org/math/CourseNotes/ANT.pdf.

[6] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[7] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[8] The LMFDB Collaboration. *The L-functions and modular forms database*. https://www.lmfdb.org, 2024.