# Local Fields

Harry Armitage

October 23, 2020

## Contents

# 1 Basic Theory

Suppose we have a diophantine polynomial $f(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, x_r]$. Then we might want to find integer solutions to the equation $f(x_1, \ldots, x_r) = 0$. However, it turns out this can be very difficult to do, for instance showing $x^n + y^n - z^n = 0$ has no solutions for $x, y, z \in \mathbb{Z}$ took hundreds of years and a lot of advanced mathematics.

Instead, we study congruences of the form $f(x_1, \ldots, x_r) \equiv 0 \mod p^n$, for prime $p$ and integer $n$. This then becomes a finite computation, and hence a much easier problem. Local fields will give us a way to package all this information together.

## 1.1 Absolute Values

**Definition 1.1.** *Let K be a field. An* **absolute value** *on K is a function* $|\cdot| : K \to \mathbb{R}_{\geq 0}$ *such that:*

1. $|x| = 0 \iff x = 0$
2. $|xy| = |x||y| \; \forall x, y \in K$
3. $|x + y| \leq |x| + |y| \; \forall x, y \in K$

*We say that* $(K, |\cdot|)$ *is a valued field.*

Examples:

1. $K = \mathbb{R}$ or $\mathbb{C}$ with $|\cdot|$ the usual absolute value. We write $|\cdot|_\infty$ for this absolute value.
2. $K$ is any field. The ***trivial absolute value*** on $K$ is defined by:

$$|x| = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases} \tag{1}$$

   We will ignore this absolute value in this course.

3. $K = \mathbb{Q}$, $p$ a prime. For $0 \neq x \in \mathbb{Q}$, we can write $x = p^n \frac{a}{b}$, where $a, b \in \mathbb{Z}, (a, p) = 1$, and $(b, p) = 1$. The ***p-adic absolute value*** is defined to be:

$$|x|_p = \begin{cases} 0 & x = 0 \\ p^{-n} & x = p^n \frac{a}{b} \end{cases}$$

   We check the axioms.

   1. Clear from the definition.
   2. $|xy|_p = |p^{m+n} \frac{ac}{bd}|_p = p^{-m-n} = |x|_p |y|_p$
   3. Wlog, $m \geq n$. $|x + y|_p = \left| p^n \left( \frac{ad + p^{m-n} bc}{bd} \right) \right|_p \leq p^{-n} = \max(|x|_p, |y|_p)$

An absolute value on $K$ induces a metric $d(x, y) = |x - y|$ on $K$, and hence induces a topology on $K$. As an exercise, check that $+, \cdot$ are continuous.

**Definition 1.2.** *Let* $|\cdot|, |\cdot|'$ *be absolute values on a field K. We say that* $|\cdot|, |\cdot|'$ *are* **equivalent** *if they induce the same topology on K. An equivalence class of absolute values is called a* **place***.*

**Proposition 1.3.** *Let* $|\cdot|, |\cdot|'$ *be non-trivial absolute values on K. The following are equivalent:*

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

*Proof.*
*1. $\implies$ 2.*

$$\begin{aligned} |x| < 1 &\iff x^n \to 0 \text{ w.r.t. } |\cdot| && (2)\\ &\iff x^n \to 0 \text{ w.r.t. } |\cdot|' && (3)\\ &\iff |x|' < 1 && (4)\end{aligned}$$

*2. $\implies$ 3.* Let $a \in K^\times$ s.t. $|a| < 1$, which exists since $|\cdot|$ is non-trivial. We need to show that, for all $x \in K^\times$, we have:

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

Assume $\frac{\log|x|}{\log|a|} < \frac{\log|x|'}{\log|a|'}$. Then choose $m, n \in \mathbb{Z}$ so that $\frac{\log|x|}{\log|a|} < \frac{m}{n} < \frac{\log|x|'}{\log|a|'}$. Then we have:

$$n \log|x| < m \log|a|$$
$$n \log|x|' > m \log|a|'$$

and hence $|\frac{x^n}{a^m}| < 1, |\frac{x^n}{a^m}|' > 1, \lightning$.

*3. $\implies$ 1.* This is clear, as open balls in one topology will also be open balls in the other, hence the topologies will be the same. □

In this course, we will be mainly interested in the following types of absolute values:

**Definition 1.4.** *An absolute value $|\cdot|$ on $K$ is said to be* **non-archimedean** *if it satisfies the ultrametric inequality $|x + y| \leq \max(|x|, |y|)$*

If $|\cdot|$ is not non-archimedean, then it is archimedean.
Examples:

1. $|\cdot|_\infty$ on $\mathbb{R}$ is archimedean.
2. $|\cdot|_p$ is a non-archimedean absolute value on $\mathbb{Q}$.

**Lemma 1.5** (All triangles are isosceles)**.** *Let $(K, |\cdot|)$ be a non-archimedean valued field, and $x, y \in K$. If $|x| < |y|$, then $|x - y| = |y|$.*

*Proof.* Observe that $|1| = |1 \cdot 1| = |1| \cdot |1|$, and so $|1| = 1$ or $0$. But $1 \neq 0$, so $|1| = 1$. Similarly, $|-1| = 1$, and so $|-y| = |y|$ for all $y \in K$.

Then if $|x| < |y|$, $|x - y| \leq \max(|x|, |y|) = |y|$.

At the same time $|y| \leq \max(|x|, |x - y|) \implies |y| \leq |x - y|$.

Hence $|y| = |x - y|$. □

**Proposition 1.6.** *Let $(K, |\cdot|)$ be non-archimedean, and $(x_n)_{n=1}^{\infty}$ be a sequence in $K$.*

*If $|x_n - x_{n+1}| \to 0$, then $(x_n)_{n=1}^{\infty}$ is Cauchy.*

*In particular, if $K$ is in addition complete, then $(x_n)_{n=1}^{\infty}$ converges.*

*Proof.* For $\epsilon > 0$, choose $N$ such that $|x_n - x_{n+1}| < \epsilon \ \forall n > N$.

Then for $N < n < m$, we have:

$$|x_n - x_m| = |(x_n - x_{n+1}) + (x_{n+1} - x_{n+1}) + \ldots + (x_{m-1} - x_m)| < \epsilon$$

And so the sequence is Cauchy. □

For example, if $p = 5$, construct the sequence $(x_n)_{n=1}^{\infty}$ such that:

1. $x_n^2 + 1 \equiv 0 \mod 5^n$
2. $x_n \equiv x_{n+1} \mod 5^n$

as follows:

Take $x_1 = 2$. Suppose we have constructed $x_n$. Let $x_n^2 + 1 = a5^n$, and set $x_{n+1} = x_n + b5^n$. Then $x_{n+1}^2 + 1 = x_n^2 + 2b5^n x_n + b^2 5^{2n} + 1 = a5^n + 2b5^n x_n + b^2 5^{2n}$.

We choose $b$ such that $a + 2bx_n \equiv 0 \mod 5$, i.e. $b \equiv -\frac{a}{2x_n} \mod 5$, and then we have $x_{n+1}^2 + 1 \equiv 0 \mod 5^{n+1}$ as desired.

The second property implies that $|x_{n+1} - x_n|_5 < 5^{-n} \to 0$, and so the sequence is Cauchy. Now suppose that $x_n \to L \in \mathbb{Q}$. Then $x_n^2 \to L^2$. But the first property then gives us that $x_n^2 \to -1 \implies L^2 = -1 \lightning$. So $(\mathbb{Q}, |\cdot|_5)$ is not complete.

**Definition 1.7.** *The p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.*

We have an analogy with $\mathbb{R}$, in that $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$.

If $(K, |\cdot|)$ is a valued field, for $x \in K, r \in \mathbb{R}_{>0}$, we define:

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

and call these the ***open*** and ***closed balls*** of radius $r$ centred at $x$, respectively.

**Lemma 1.8.** *Let $(K, |\cdot|)$ be non-archimedean. Then:*

1. *If $z \in B(x, r)$, then $B(z, r) = B(x, r)$.*
2. *If $z \in \overline{B}(x, r)$, then $\overline{B}(z, r) = \overline{B}(x, r)$.*
3. *$B(x, r)$ is closed.*
4. *$\overline{B}(x, r)$ is open.*

*Proof.*

1. Let $y \in B(x, r)$. Then $|x - y| < r \implies |z - y| = |(z - x) + (x - y)| \leq \max(|z - x|, |x - y|) < r$.
2. Same as in *1.*, but with $\leq$ instead of $<$.

3. Let $y \notin B(x,r)$. We need to show there is an open neighbourhood of $y$ not intersecting $B(x,r)$. If $z \in B(x,r) \cap B(y,r)$, then $B(x,r) = B(z,r) = B(y,r)$. But then $y \in B(x,r) \lightning$. So $B(x,r)$ and $B(y,r)$ are disjoint, and so $B(x,r)$ is closed.

4. If $z \in \overline{B}(x,r)$, then we need to show there is an open neighbourhood of $z$ contained in $\overline{B}(x,r)$. But $B(z,r) \subseteq \overline{B}(z,r) = \overline{B}(x,r)$, and so $\overline{B}(x,r)$ is open.

□

## 2 Valuation Rings

**Definition 2.1.** *Let $K$ be a field. A* **valuation** *on $K$ is a function $v : K^\times \to \mathbb{R}$ such that:*

1. $v(xy) = v(x) + v(y)$
2. $v(x+y) \geq \min\{v(x), v(y)\}$

Fix $0 < \alpha < 1$. If $v$ is a valuation on $K$, then $|x| = \begin{cases} \alpha^{v(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$ determines a non-archimedean absolute value. Conversely, a non-archimedean absolute value determines a valuation $v(x) = \log_\alpha |x|$.

We will ignore the trivial valuation $v(x) \equiv 0$, which corresponds to the trivial absolute value.

We say $v_1, v_2$ are ***equivalent*** if $\exists\ c \in \mathbb{R}_{>0}$ such that $v_1(x) = cv_2(x)\ \forall x \in K^\times$.

Examples:

- $K = \mathbb{Q}$, $v_p(x) = -\log_p |x|_p$ is the $p$-adic valuation.
- $k$ any field, $K = k(t) = \mathrm{Frac}(k[t])$, the rational function field. $v\left(t^n \frac{f(t)}{g(t)}\right) = n$ where $f, g \in k[t]$, $f(0), g(0) \neq 0$. This is the $t$-adic valuation.
- $K = k((t)) = \mathrm{Frac}(k[[t]])$, the field of ***formal Laurent series over k***. Then we have $v\left(\sum_i a_i t^i\right) = \min\{i : a_i \neq 0\}$ is the $t$-adic valuation on $K$.

**Definition 2.2.** *Let $(K, |\cdot|)$ be a non-archimedean valued field. The* **valuation ring** *of $K$ is defined to be:*

$$\begin{aligned} \mathcal{O}_K &= \{x \in K : |x| \leq 1\} \quad (= \bar{B}(0,1)) \\ &= \{x \in K^\times : v(x) \geq 0\} \cup \{0\} \end{aligned}$$

**Proposition 2.3.**

1. *$\mathcal{O}_K$ is an open subring of $K$.*
2. *The subsets $\{x \in K : |x| \leq r\}$ and $\{x \in K : |x| < r\}$ for $r \leq 1$ are open ideals in $\mathcal{O}_K$.*
3. *$\mathcal{O}_K^\times = \{x \in K : |x| = 1\}$.*

*Proof.*

1. $|1| = 1, |0| = 0$, so $1, 0 \in \mathcal{O}_K$. $|-x| = |x|$, so $x \in \mathcal{O}_K \implies -x \in \mathcal{O}_K$. If $x, y \in \mathcal{O}_K$, then $|x+y| \leq \max(|x|, |y|) \leq 1$, and so $x + y \in \mathcal{O}_K$, and $|xy| = |x||y| \leq 1$, so $xy \in \mathcal{O}_K$. Since $\mathcal{O}_K = \bar{B}(0,1)$, it is open.

2. The proof of this is the same as *1.*
3. Note that $|x||x^{-1}| = |xx^{-1}| = 1$. So $|x| = 1 \iff |x^{-1}| = 1$. This can happen if and only if $x, x^{-1} \in O_K$, i.e. $x \in O_K^\times$.

□

As a point of notation, we will define $m := \{x \in O_K : |x| < 1\}$, a maximal ideal of $O_K$, and $k := O_K/m$ to be the ***residue field***.

We say a ring $R$ is ***local*** if it has a unique maximal ideal. As an exercise, prove that $R$ is local if and only if $R \setminus R^\times$ is an ideal of $R$. We can use this to prove the following:

**Corollary 2.4.** *$O_K$ is a local ring with a unique maximal ideal $m$.*

*Proof.* Suppose $x \in O_K \setminus m$. Then $|x| = 1$, so $x^{-1} \in O_K$, and so any ideal containing $x$ contains $x^{-1}x = 1$, i.e. is all of $O_K$, and hence $m$ is the unique maximal ideal in $O_K$. □

Examples:

- $K = k((t)), O_K = k[[t]], m = (t)$, and the residue field is $k$.
- $K = \mathbb{Q}$ with $|\cdot|_p$. $O_K = \mathbb{Z}_{(p)}, m = p\mathbb{Z}_{(p)}, k = \mathbb{F}_p$.

**Definition 2.5.** *Let $v : K^\times \to \mathbb{R}$ be a valuation. If $v(K^\times) \cong \mathbb{Z}$, we say $v$ is a* **discrete valuation***, and $K$ is said to be a* **discretely valued field***. An element $\pi \in O_K$ is a* **uniformizer** *if $v(\pi) = 0$ and $v(\pi)$ generates $v(K^\times)$.*

Remark: If $v$ is a discrete valuation, we can replace it with an equivalent one such that $v(K^\times) = \mathbb{Z} \subseteq \mathbb{R}$. Such $v$ are called ***normalized valuations***, and have $v(\pi) = 1$ for $\pi$ a uniformizer.

**Lemma 2.6.** *Let $v$ be a valuation on $K$. Then the following are all equivalent:*

1. *$v$ is discrete.*
2. *$O_K$ is a PID.*
3. *$O_K$ is noetherian.*
4. *$m$ is principal.*

*Proof.*
1. $\implies$ 2. Let $I \subsetneq O_K$ be a non-zero ideal. Let $x \in I$ such that $v(x) = \min\{v(a) : a \in I\}$, which exists since $v$ is discrete. Then $xO_K = \{a \in O_K : v(a) \geq v(x)\} \subseteq I$, and hence $xO_K = I$ by definition of $x$ - if $y \in I \setminus (x)$, then $v(y) < v(x)\lightning$.

2. $\implies$ 3. Every PID is noetherian, as all ideals are finitely generated (by a single element).

3. $\implies$ 4. Write $m = x_1O_K + \ldots + x_nO_K$. Wlog, $v(x_1) \leq v(x_2) \leq \ldots \leq v(x_n)$. Then $m = x_1O_K$.

4. $\implies$ 1. Let $m = \pi O_K$ for some $\pi \in O_K$, and let $c = v(\pi)$. Then if $v(x) > 0$, $x \in m$ and hence $v(x) \geq c$. Thus $v(K^\times) \cap (0, c) = \emptyset$. Since $v(K^\times)$ is a subgroup of $(\mathbb{R}, +)$, we have $v(K^\times) = c\mathbb{Z}$. □

**Lemma 2.7.** *Let $v$ be a discrete valuation on $K$, and $\pi \in O_K$ a uniformizer. Then for any $x \in K^\times$ there exists $n \in \mathbb{Z}$ and $u \in O_K^\times$ such that $x = \pi^n u$. In particular, $K = O_K\left[\frac{1}{x}\right]$ for any $x \in m$ and hence* $K = \operatorname{Frac} O_K$.

*Proof.* For any $x \in K^\times$, let $n$ be such that $v(x) = v(\pi^n) = nv(\pi)$, then $v(x\pi^{-n}) = 0 \implies u = x\pi^{-n} \in \mathcal{O}_K^\times$. $\square$

**Definition 2.8.** *A ring $R$ is called a* **discrete valuation ring (DVR)** *if it is a PID with exactly one non-zero prime ideal.*

**Lemma 2.9.**

1. *Let $v$ be a discrete valuation on $K$. Then $\mathcal{O}_K$ is a DVR.*
2. *Let $R$ be a DVR. Then there is a valuation $v$ on $K := \mathrm{Frac}(R)$ such that $R = \mathcal{O}_K$.*

*Proof.*

1. $\mathcal{O}_K$ is a PID by **2.6**. Let $0 \neq I \subseteq \mathcal{O}_K$ be an ideal, then $I = (x)$ for some $x$. If $x = \pi^n u$ for $\pi$ a uniformizer, then $(x)$ is prime if and only if $n = 1$, and $I = (\pi) = m$.
2. Let $R$ be a DVR with maximal ideal $m$. Then $m = (\pi)$ for some $\pi \in R$. Since PIDs are UFDs, we may write $x \in R \setminus \{0\}$ uniquely as $\pi^n u, n \geq 0, u \in R^\times$. Then any $y \in K \setminus \{0\}$ can be written uniquely as $\pi^m u, u \in R^\times, m \in \mathbb{Z}$. Then define $v(\pi^m u) = m$, and it is easy to check $v$ is a valuation and $\mathcal{O}_K = R$.

$\square$

Examples:

- $\mathbb{Z}_{(p)}$ is a DVR, the valuation ring of $|\cdot|_p$ on $\mathbb{Q}$.
- $k[[t]]$ is a DVR, the valuation ring of the $t$-adic valuation on $k((t))$.
- $K = k(t), K' = K\left(t^{\frac{1}{2}}, t^{\frac{1}{4}}, t^{\frac{1}{8}}, \ldots\right)$. The $t$-adic valuation extends to $K'$, but we must have $v(t^{\frac{1}{2^n}}) = \frac{1}{2^n}$, which is not discrete.

# 3 The p-adic Numbers

Recall that $\mathbb{Q}_p$ is defined to be the completion of $\mathbb{Q}$ with respect to the metric induced by $|\cdot|_p$. On example sheet 1, we prove that $\mathbb{Q}_p$ is a field. $|\cdot|_p$ extends from $\mathbb{Q}$ to $\mathbb{Q}_p$, and the associated valuation is discrete, so $\mathbb{Q}_p$ is a discretely valued field.

**Definition 3.1.** *The* **ring of p-adic integers**, *$\mathbb{Z}_p$, is the valuation ring $\{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.*

$\mathbb{Z}_p$ is a discrete valuation ring with maximal ideal $p\mathbb{Z}_p$, and all non-zero ideals in $\mathbb{Z}_p$ are of the form $p^n\mathbb{Z}_p$ for $n \in \mathbb{N}$.

**Proposition 3.2.** *$\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$. In particular, $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to $|\cdot|_p$.*

*Proof.* We need to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. We know that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Since $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ is a closed ball and hence open, $\mathbb{Z}_p \cap \mathbb{Q}$ is dense in $\mathbb{Z}_p$.

$$\begin{aligned}
\mathbb{Z}_p \cap \mathbb{Q} &= \{x \in \mathbb{Q} : |x|_p \leq 1\} \\
&= \left\{\frac{a}{b} \in \mathbb{Q} : p \nmid b\right\} \\
&= \mathbb{Z}_{(p)}
\end{aligned}$$

Thus it suffices to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$.

Let $\frac{a}{b} \in \mathbb{Z}_{(p)}$, so that $a, b \in \mathbb{Z}, p \nmid b$. For $n \in \mathbb{N}$, choose $y_n \in \mathbb{Z}$ such that $by_n \equiv a \mod p^n$. Then $y_n \to \frac{a}{b}$ as $n \to \infty$.

In particular, $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ which is complete. □

## 3.1 Brief Digression on Inverse Limits

Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets/groups/rings together with homomorphisms $\varphi_n : A_{n+1} \to A_n$, called transition maps. The ***inverse limit*** of $(A_n)_{n=1}^{\infty}$ is the set of sequences of elements given by:

$$\varprojlim_n A_n = \left\{(a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} A_n : \varphi_n(a_{n+1}) = a_n\right\}$$

so that $a_{n+1} \xmapsto{\varphi_n} a_n \xmapsto{\varphi_{n-1}} a_{n-1}$. If the $A_n$ are groups/rings, then $\varprojlim_n A_n$ is a group/ring respectively.

Let $\theta_m : \varinjlim_n A_n \to A_m$ denote the natural projection map.

The inverse limit satisfies the following universal property:

**Proposition 3.3.** *Let $((A_n)_{n=1}^{\infty}, (\varphi_n)_{n=1}^{\infty})$ as above. Then for any set/group/ring $B$ together with homomorphisms $\psi_n : B \to A_n$ such that the diagram*

$$\begin{tikzcd}
B \arrow[r, "\psi_{n+1}"] \arrow[dr, "\psi_n"'] & A_{n+1} \arrow[d, "\varphi_n"] \\
& A_n
\end{tikzcd}$$

*commutes for all $n$, there is a unique homomorphism $\psi : B \to \varprojlim_n A_n$ such that $\theta_n \circ \psi = \psi_n$.*

*Proof.* Define $\psi : B \to \prod_{n=1}^{\infty} A_n$ by $b \mapsto \prod_{n=1}^{\infty}\{\psi_n(b)\}$.

Then $\psi_n = \varphi_n \circ \psi_{n+1} \implies \psi(b) \in \varprojlim_n A_n$.

This map is clearly unique, as it is determined by $\psi_n = \varphi_n \circ \psi_{n+1}$, and is a homomorphism of rings. □

**Definition 3.4.** *Let $R$ be a ring and $I \subseteq R$ an ideal. The* **I-adic completion of R** *is the ring $\widehat{R} := \varprojlim_n R/I^n$, where $\varphi_n : R/I^{n+1} \to R/I^n$ is the natural projection.*

Note that there is a natural map $i : R \to \widehat{R}$ by the universal property. We say that $R$ is $I$-adically complete if $i$ is an isomorphism.

As a fact, $\ker(i : R \to \widehat{R}) = \bigcap_{n=1}^{\infty} I^n$.

Let $(K, |\cdot|)$ be a non-archimedean valued field, and $\pi \in O_K$ such that $|\pi| < 1$.

**Proposition 3.5.** *Assume that K is complete. Then:*

1. $O_K \cong \varprojlim_n O_K/\pi^n O_K$*, i.e.* $O_K$ *is* $\pi$*-adically complete.*
2. *If in addition K is discretely valued and* $\pi$ *is a uniformizer, then every element* $x \in O_K$ *can be written uniquely as* $x = \sum_{i=0}^{\infty} a_i \pi^i$ *for* $a_i \in A$ *where A is a set of coset representatives for* $k := O_K/\pi O_K$.

   *Moreover, any series* $\sum_{i=0}^{\infty} a_i \pi^i$ *converges in* $O_K$.

*Proof.*

1. There is a natural map $i : O_K \to \varprojlim_n O_K/\pi O_K$. Since $\bigcap_{n=1}^{\infty} \pi^n O_K = \{0\}$, $i$ is injective. Now let $(x_n)_{n=1}^{\infty} \in \varprojlim_n O_K/\pi^n O_K$, and for each $n$ choose $y_n \in O_K$ a lift of $x_n \in O_K/\pi^n O_K$.

   Let $v$ be the valuation on $K$ normalised such that $v(\pi) = 1$, then $v(y_n - y_{n+1}) \geq n$, as $y_n - y_{n+1} \in \pi^n O_K$.

   So $(y_n)_{n=1}^{\infty}$ is a Cauchy sequence in $O_K$, but $O_K$ is complete as $O_K \subseteq K$ is closed, and we assumed $K$ complete.

   So $y_n \to y$ and $i(y) = (x_n)_{n=1}^{\infty}$, so $i$ is surjective, and hence an isomorphism.
2. Let $x \in O_K$. Choose $a_i$ inductively as follows:

   Choose $a_0 \in A$ such that $a_0 \equiv x \mod \pi O_K$. Suppose we have chosen $a_0, \ldots, a_k$ such that $\sum_{i=0}^{k} a_i \pi^i \equiv x \mod \pi^{k+1}$, Then $a_i \pi^i - x = c\pi^{k+1}$ for some $c \in O_K$. Then choose $a_{k+1} \equiv c \mod \pi O_K$.

   Then $\sum_{i=0}^{k+1} a_i \equiv x \mod \pi^{k+2} O_K$, and so $\sum_{i=0}^{\infty} a_i = x$.

   For uniqueness, assume that $\sum_{i=0}^{\infty} a_i \pi^i = \sum_{i=0}^{\infty} b_i \pi^i \in O_K$. Let $n$ be minimal such that $a_n \neq b_n$. Then $\sum_{i=0}^{\infty} a_i \not\equiv \sum_{i=0}^{\infty} b_i \pi^i \mod \pi^{n+1} \lightning$.

   For the moreover part, any series of this form defines a Cauchy sequence, which as in *1* converges in $O_K$.

□

Warning: if $(K, |\cdot|)$ is not discretely valued, then $O_K$ is not necessarily $m$-adically complete.

**Corollary 3.6.** *If K is as in 2 of* **3.5***, then every* $x \in K$ *can be written uniquely as a series of the form* $\sum_{i=n}^{\infty} a_i \pi^i$, $a_i \in A$*. Conversely, any such expression defines an element of K.*

*Proof.* Use the fact that $K = O_K \left[\frac{1}{\pi}\right]$. □

**Corollary 3.7.**

1. $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

2. *Every element of* $\mathbb{Q}_p$ *can be written uniquely as* $\sum_{i=n}^{\infty} a_i p^i$ *where* $a_i \in \{0, 1, \ldots, p-1\}$.

*Proof.*

1. By **3.5** it is sufficient to show that $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. Note that there is a natural map $f_n : \mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$, since $\mathbb{Z} \subseteq \mathbb{Z}_p$.

   We have that $\ker f_n = \{x \in \mathbb{Z} : |x|_p \leq p^{-n}\} = p^n\mathbb{Z}$.

   Hence, $\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$ is injective.

   For surjectivity, let $\bar{c} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$, and $c \in \mathbb{Z}_p$ a lift. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we can choose $x \in \mathbb{Z}$ such that $x \in c + p^n\mathbb{Z}_p$. This is a closed ball and hence open, so $f_n(x) = \bar{c}$, and the map is surjective.

2. Follows from **3.6**, noting that $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ by *1*.

□

<u>Examples:</u>

- $\frac{1}{1-p} = 1 + p + p^2 + p^3 + \ldots \in \mathbb{Q}_p$.
- Let $K = k((t))$ with the $t$-adic valuation. Then $O_K = k[[t]] = \varprojlim_n k[[t]]/(t^n)$. Moreover, $O_K$ is the $t$-adic completion of $k[t]$.

# 4 Complete Valued Fields

## 4.1 Hensel's Lemma

For complete valued fields, there is a nice way to produce solutions in $O_K$ to certain equations from the solutions mod $m$.

Given $f \in R[x]$ for some ring $R$, we will denote by $f'$ the ***formal derivative*** of $f$, which is the image of $f$ under the linear map taking $x^n \mapsto nx^{n-1}$.

**Theorem 4.1** (Hensel's Lemma, version 1)**.** *Let* $(K, |\cdot|)$ *be a complete discretely valued field. Let* $f(x) \in O_K[x]$*, and assume there exists* $a \in O_K$ *such that* $|f(a)| < |f'(a)|^2$.

*Then there exists a unique* $x \in O_K$ *such that* $f(x) = 0$ *and* $|x - a| < |f'(a)|$.

*Proof.* Let $\pi \in O_K$ be a uniformizer, and let $r = v(f'(a))$. We construct a sequence $(x_n)_{n=1}^{\infty}$ in $O_K$ such that:

(i) $f(x_n) \equiv 0 \mod \pi^{n+2r}$

(ii) $x_{n+1} \equiv x_n \mod \pi^{n+r}$

Take $x_1 = a$; then $f(x_1) \equiv 0 \mod \pi^{1+2r}$.

Suppose we've constructed $x_1, \ldots, x_n$ satisfying (i) and (ii). Define $x_{n+1} := x_n - \frac{f(x_n)}{f'(x_n)}$. Since $x_n \equiv x_1 \mod \pi^{r+1}, v(f'(x_n)) = r$, and hence $\frac{f(x_n)}{f'(x_n)} \equiv 0 \mod \pi^{n+r}$ by (i).

It follows that $x_{n+1} \equiv x_n \mod \pi^{n+r}$, so (ii) holds.

Note that for $x, y$ indeterminates, $f(x+y) = f_0(x) + f_1(x)y + f_2(x)y^2 + \ldots$, where $f_i(x) \in O_K[x]$, and $f_0(x) = f(x)$, $f_1(x) = f'(x)$.

Thus $f(x_{n+1}) = f(x_n) + f'(x_n)c + f_2(x_n)c^2 + \ldots$, where $c = -\frac{f(x_n)}{f'(x_n)} \equiv 0 \mod \pi^{n+r}$. Then since $v(f_i(x_n)) \geq 0$, we have $f(x_{n+1}) \equiv f(x_n) + f'(x_n)c \equiv 0 \mod \pi^{n+2r+1}$, and so (i) holds.

This gives a construction of $(x_n)_{n=1}^{\infty}$. Property (ii) implies our sequence is Cauchy, so by completeness it converges to $x \in O_K$. Then $f(x) = \lim_{n\to\infty} f(x_n) = 0$, which is zero by $(i)$.

Moreover, (ii) implies:

$$\begin{aligned} a = x_1 &\equiv x_n \mod \pi^{r+1}\ \forall n \\ \implies a &\equiv x \mod \pi^{r+1} \\ \implies |x - a| &< |f'(a)| \end{aligned}$$

This proves existence.

For uniqueness, suppose $x'$ also satisfies $f(x') = 0, |x' - a| < |f'(a)|$. Let $\delta = |x' - x| \gneq 0$.

Then $|x' - a| < |f'(a)|, |x - a| < |f'(a)|$, and the ultrametric inequality implies:

$$|\delta| = |x - x'| < |f'(a)| = |f'(x)|$$

But $0 = f(x') = f(x + \delta) = f(x) + f'(x) + \delta + \ldots$, where absolute value of the higher order terms is $\leq |\delta|^2$.

Hence $|f'(x)\delta| \leq |\delta|^2 \implies |f'(x)| \leq |\delta| \lightning$. □

The following corollary is a slightly weaker result, but will often turn out to be more useful for what we want to do.

**Corollary 4.2.** *Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(x) \in O_K[x]$, and $\bar{c} \in k := O_K/m$ a simple root of $\bar{f}(x) := f(x) \mod m \in k[x]$ (i.e. not a root of $\bar{f}'(x)$).*

*Then there is a unique $x \in O_K$ such that $f(x) = 0$ and $x \equiv \bar{c} \mod m$.*

*Proof.* Apply **4.1** to a lift $c \in O_K$ of $\bar{c}$. Then $|f(c)| < |f'(c)|^2 = 1$, since $\bar{c}$ is a simple root. □

Example: $f(x) = x^2 - 2$ has a simple root mod 7. Thus $\sqrt{2} \in \mathbb{Z}_7 \subseteq \mathbb{Q}_7$.

**Corollary 4.3.**

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

*Proof.*

$p > 2$: Let $b \in \mathbb{Z}_p^\times$. By **4.2** applied to $f(x) = x^2 - b$, we have $b \in (\mathbb{Z}_p^\times)^2$ if and only if $b \in (\mathbb{F}_p^\times)^2$.

Thus $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$, since $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

We have an isomorphism $\mathbb{Z}_p^\times \times \mathbb{Z} \cong \mathbb{Q}_p^\times$, given by $(u, n) \mapsto u\pi^n$.

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

$\underline{p = 2}$: Let $b \in \mathbb{Z}_2^\times$. Consider $f(x) = x^2 - b$. Then $f'(x) = 2x \equiv 0 \mod 2$, so we can't use **4.1**.

Let $b \equiv 1 \mod 8$. Then $|f(1)|_2 \leq 2^{-3} < |f'(1)|_2^2 = 2^{-2}$. So by Hensel's lemma, $f(x)$ has a root in $\mathbb{Z}_2$.

Hence $b \in (\mathbb{Z}_p^\times)^2 \iff b \equiv 1 \mod 8$. So $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \equiv (\mathbb{Z}/8\mathbb{Z})^\times \equiv (\mathbb{Z}/2\mathbb{Z})^2$. Again, using $\mathbb{Q}_2^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}$, we find that $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$.

□

The proof of Hensel's lemma uses the iteration $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$, which is the same iteration as used in the Newton-Raphson method for functions on the real numbers. In this case however we can do one better, as Hensel's lemma lets us know when the iteration will converge.

For later applications, we will need the following version of Hensel's lemma:

**Theorem 4.4** (Hensel's Lemma, version 2)**.** *Let $(K, |\cdot|)$ be a complete discretely valued field, and $f(x) \in \mathcal{O}_K[x]$, and suppose that $\bar{f}(x) := f(x) \mod m \in k[x]$ factorises as:*

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

*with $\bar{g}(x), \bar{h}(x)$ coprime.*

*Then there is a factorisation $f(x) = g(x)h(x)$ in $\mathcal{O}_K[x]$, with $g(x) \equiv \bar{g}(x) \mod m, \bar{h}(x) \equiv h(x) \mod m$, and $\deg \bar{g} = \deg g$.*

*Proof.* Example sheet 1. □

**Corollary 4.5.** *Let $f(x) = a_n x^n + \ldots + a_0 \in K[x]$ with $a_0, a_n \neq 0$. If $f(x)$ is irreducible, then $|a_i| \leq \max\{|a_0|, |a_n|\}$ for all $i$.*

*Proof.* Upon scaling, we may assume $f(x) \in \mathcal{O}_K[x]$ with $\max_i\{|a_i|\} = 1$. Thus we need to show that $\max\{|a_0|, |a_1|\} = 1$. If not, let $r$ be minimal such that $|a_r| = 1$, then $0 < r < n$. Thus we have $\bar{f}(x) = x^r(a_r + \ldots a_n x^{n-r}) \mod m$.

Then **4.5** tells us this factorisation lifts to a factorisation in $\mathcal{O}_K[x]$, which is a contradiction. □

# 5 Teichmüller Lifts

Recall that every element of $\mathbb{Q}_p$ can be written as $x = \sum_{i=n}^\infty a_i p^i$, where $a_i \in \{0, \ldots, p-1\} =: A$.

We chose this set $A$ since we found that we needed coset representatives for $\mathbb{F}_p \leq \mathbb{Z}_p$. However, this choice of $A$ doesn't respect any of the algebraic structure on $\mathbb{Z}_p$.

It turns out there is a natural choice of coset representatives in many cases which does respect some algebraic structure.

**Definition 5.1.** *A ring $R$ of characteristic $p$ is* **perfect** *if the Frobenius map* $\mathrm{Frob} : x \mapsto x^p$ *is an automorphism of $R$. A field of characteristic $p$ is perfect if it is perfect as a ring.*

Note that since $\mathrm{char}\, R = p$, $(x+y)^p = x^p + y^p$, so the Frobenius map is a ring homomorphism, so all that is needed is that it is bijective.

<u>Examples:</u>

1. $\mathbb{F}_p$ and $\bar{\mathbb{F}}_p$ are perfect fields.
2. $\mathbb{F}_p[t]$ is not perfect - $t \notin \mathrm{im}(\mathrm{Frob})$.
3. $\mathbb{F}_p\left(t^{1/p^\infty}\right) := \mathbb{F}_p(t, t^{1/p}, t^{1/p^2}, \ldots)$ is a perfect field. This is the smallest perfect field containing $\mathbb{F}_p(t)$, so we call it the ***perfection*** of $\mathbb{F}_p(t)$. The $t$-adic absolute value extends to $\mathbb{F}_p(t^{1/p^\infty})$, and the completion of $\mathbb{F}_p(t^{1/p^\infty})$ is called a ***perfectoid field***. These were the subject of Peter Scholze's PhD thesis.

Fact: a field $k$ is perfect if and only if any finite extension of $k$ is separable.

**Theorem 5.2.** *Let $(K, |\cdot|)$ be a complete discretely valued field such that $k := O_K/m$ is a perfect field of characteristic $p$. Then there is a unique map*

$$[\cdot] : k \to O_K$$

*such that:*

1. *$a \equiv [a] \mod m$ for all $a \in k$.*
2. *$[ab] \equiv [a][b]$ for all $a, b \in k$.*

*Moreover, if* $\mathrm{char}\, O_K = p$*, then $[\cdot]$ is a ring homomorphism.*

**Definition 5.3.** *The element $[a] \in O_K$ constructed in* **5.2** *is called the* **Teichmüller lift** *of $a$.*

The idea of the proof of this theorem is that, if $\alpha \in O_K$ be a lift of $a \in k$. $\alpha$ is well defined then up to the ideal $\pi O_K$ (where $\pi$ is a uniformizer).

Then let $\beta \in O_K$ be a lift of $a^{1/p}$; we claim that $\beta$ is a "better" lift:

Let $\beta' \in O_k$ be another lift of $a^{1/p}$. Then $\beta = \beta' + \pi u, u \in O_K$, and so $\beta^p = \beta'^p + \sum_{i=1}^{\infty} \binom{p}{i} \beta'^i (\pi u))^{p-i}$. Since $p \in \pi$, this sum term lies in $\pi^2 O_K$, and so $\beta$ is well defined up to $\pi^2 O_K$.

The idea is then to repeat this process, getting a sequence of better and better lifts each time, which will converge to a "canonical" lift. To do this rigorously we'll need the following lemma:

**Lemma 5.4.** *Let $(K, |\cdot|)$ be as in* **5.3***, and fix $\pi \in O_K$ a uniformizer. Let $x, y \in O_K$ such that $x \equiv y \mod \pi^k$, for $k \geq 1$. Then $x^p \equiv y^p \mod \pi^{k+1}$.*

*Proof.* Let $x = y + u\pi^k$. Then:

$$\begin{aligned} x^p &= \sum_{i=0}^{p} \binom{p}{i} y^i (u\pi^k)^{p-i} \\ &= y^p + pu\pi^k y^{p-1} + \sum_{i=2}^{p} \binom{p}{i} y^i (u\pi^k)^{p-i} \quad \text{for } p > 2 \end{aligned}$$

Since $O_K/\pi O_K$ is of characteristic $p$, we have $p \in (\pi)$. Thus $pu\pi^k y^{p-1} \in \pi^{k+1} O_K$. Additionally, for $i \geq 2$, $(u\pi^k)^i \in \pi^{k+1} O_K$.

Hence $x^p \equiv y^p \mod \pi^{k+1}$. □

*Proof of* ***Theorem 5.2***. Let $a \in k$. For each $i \geq 0$, we choose a lift $y_i \in O_K$ of $a^{1/p^i}$, and we define:

$$x_i := y_i^{p^i}$$

Then $x_i \equiv y_i^{p^i} \equiv \left(a_i^{1/p^i}\right)^{p^i} \equiv a \mod \pi$.

We then claim that $(x_i)_{i=1}^{\infty}$ is a Cauchy sequence, and that its limit $x_i \to x$ is independent of the choice of $y_i$.

By construction, $y_i \equiv y_{i+1}^p \mod \pi$. By **5.4** and using induction on $k$, we have $y_i^{p^k} \equiv y_{i+1}^{p^{k+1}} \mod \pi^{k+1}$, and hence $x_i \equiv x_{i+1} \mod \pi^{i+1}$, and so the sequence is Cauchy, so converges in $O_K$ to some $x$.

Suppose we had chosen different $y_i$s, getting a different sequence $(x_i')_{i=1}^{\infty}$. Then $x_i' \to x' \in O_K$.

Then let $(x_i'')_{i=1}^{\infty} = \begin{cases} x_i & i \text{ even} \\ x_i' & i \text{ odd} \end{cases}$. Then $(x_i'')$ is also Cauchy, and has convergent subesquences to $x$ and $x'$, so $x = x'$, and our choice of $y_i$ didn't matter.

We then define $[a] = x$.

$x \equiv a \mod \pi$, so the first condition is satisfied.

For the second condition, let $b \in k$, and we choose $u_i \in O_K$ a lift of $b^{1/p^i}$; let $z_i := u_i^{p^i}$. Then $\lim_{i\to\infty} z_i = [b]$.

Now $u_i y_i$ is a lift of $(ab)^{1/p^i}$, hence $[ab] = \lim\limits_{i\to\infty} x_i z_i = \lim\limits_{i\to\infty} x_i \lim\limits_{i\to\infty} z_i = [a][b]$.

If char $O_K = p$, then $y_i + u_i$ is a lift of $a^{1/p^i} + b^{1/p^i} = (a+b)^{1/p^i}$ (raise both sides to $p^i$ and use perfectness $\implies$ bijectivity of Frob). Then we have:

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

It is easy to check that $[0] = 0, [1] = 1$, and so $[\cdot]$ is a ring homomorphism.

For uniqueness, let $\phi : k \to O_K$ be another such map. Then for $a \in k$, $\phi(a^{1/p^i})$ is a lift $a^{1/p^i}$. It follows that:

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

□

Example: $K = \mathbb{Q}_p$, then $[\cdot] : \mathbb{F}_p \to \mathbb{Z}_p$. For $a \in \mathbb{F}_p^\times$, $[a]^{p-1} = [a^{p-1}] = [1] = 1$, and so $[a]$ is a $(p-1)^{\text{th}}$ root of unity. More generally:

**Lemma 5.6.** *Let $(K, |\cdot|)$ be a complete discretely valued field. If $k := O_K/m \subseteq \mathbb{F}_p$, then $[a] \in O_K^\times$ is a root of unity.*

*Proof.* $a \in k \implies a \in \mathbb{F}_{p^n}$ for some $n$, so $[a]^{p^n-1} = [1] = 1$. □

**Theorem 5.7.** *Let $(K, |\cdot|)$ be a complete discretely valued field with* $\operatorname{char} K = p > 0$. *Then $K \cong k((t))$.*

*Proof.* Since $K = \operatorname{Frac}(O_K)$, it suffices to show that $O_K \cong k[[t]]$. Fix $\pi \in O_K$ a uniformizer, and let $[\cdot] : k \to O_K$ be the Teichmüller map, and define:

$$\varphi : k[[t]] \to O_K$$
$$\sum_{i=0}^{\infty} a_i t^i = \sum_{i=0}^{\infty} [a_i]\pi^i$$

Then $\varphi$ is a ring homomorphism since $[\cdot]$ is, and it is a bijection by **3.5**. □

# 6 Extensions of Complete Valued Fields

**Theorem 6.1.** *Let $(K, |\cdot|)$ be a complete non-archimedean discretely valued field, and $L/K$ a finite extension of degree $n$. Then:*

1. *$|\cdot|$ extends uniquely to an absolute value $|\cdot|_L$ on $L$, defined by*

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

2. *$L$ is complete with respect to $|\cdot|_L$.*

Recall that if $L/K$ is finite then $N_{L/K} : L \to K$ is defined by $N_{L/K} = \operatorname{Det}_K(\operatorname{mult}_y)$, where $\operatorname{mult}_y$ is the $K$-linear map induced by multiplication by $y$.

We have also that:

- $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$
- If $x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K[x]$ is the minimal polynomial of $y \in L$, then $N_{L/K}(y) = a_0^m$ for some $m \geq 1$.

Note that the $n^{\text{th}}$ root is not necessary for $|\cdot|_L$ to be an absolute value, but is necessary for it to extend $|\cdot|$, as for $x \in K$, $N_{L/K}(x) = \operatorname{Det}\operatorname{diag}(x, x, \ldots, x) = x^n$.

We will spend this section proving **6.1**.

**Definition 6.2.** *Let $(K, |\cdot|)$ be a non-archimedean valued field, and $V$ a vector space over $K$. A norm on $V$ is a function $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ satisfying:*

1. $\|x\| = 0 \iff x = 0$
2. $\|\lambda x\| = |\lambda|\|x\| \ \forall \lambda \in K, x \in V$
3. $\|x + y\| \leq \max(\|x\|, \|y\|)$

For example, if $V$ is finite dimensional and $e_1, \ldots, e_n$ is a basis of $V$. The sup norm on $V$ is defined by

$$\|x\|_{\sup} = \max_i |x_i|$$

where $x = \sum_{i=1}^{n} x_i e_i$. As an exercise, show $\|\cdot\|_{\sup}$ is a norm.

**Definition 6.3.** *Two norms $\|\cdot\|_1, \|\cdot\|_2$ are equivalent if there are $C, D > 0$ such that*

$$C\|x\|_1 \leq \|x\|_2 \leq D\|x\|_1 \; \forall x \in V$$

A norm defines a metric on $V$, and hence a topology, and equivalent norms induce the same topology.

**Proposition 6.4.** *Let $(K, |\cdot|)$ be complete and non-archimedean, and $V$ be a finite dimensional vector space over $K$. Then $V$ is complete with respect to $\|\cdot\|_{\sup}$.*

*Proof.* Let $(v_i)_{i=1}^{\infty}$ be a Cauchy sequence in $V$, and let $e_1, \ldots, e_n$ be a basis for $V$. Write $v_1 = \sum_{j=1}^{n} x_j^i e_j$; then $(x_j^i)_{i=1}^{\infty}$ is a Cauchy sequence in $K$.

Let $x_j^i \to x_j \in K$, then $v_i \to v = \sum_{i=1}^{n} x_j e_j$. □

**Theorem 6.5.** *Let $(K, |\cdot|)$ be complete and non-archimedean, and $V$ a finite dimensional vector space over $K$. Then any two norms on $V$ are equivalent. In particular, $V$ is complete with respect to any norm.*

*Proof.* Since equivalence defines an equivalence relation on a set of norms, it suffices to show that any norm is equivalent to $\|\cdot\|_{\sup}$.

Let $e_1, \ldots, e_n$ be a basis for $V$, and set $D := \max_i \|e_i\|$.

Then for $x = \sum_{i=1}^{n} x_i e_i$, we have

$$\begin{aligned}
\|x\| &\leq \max_i \|x_i e_i\| \\
&= \max_i |x_i| \|e_i\| \\
&\leq D \max_i |x_i| \\
&= D\|x\|_{\sup}
\end{aligned}$$

To find $C$ such that $C\|\cdot\|_{\sup} \leq \|\cdot\|$, we induct on $n = \dim V$.

If $n = 1$, then $\|x\| = \|x_1 e_1\| = |x_1| \|e_1\|$, so take $C = \|e_1\|$.

Then for $n > 1$, for each $i$, define $V_i := \mathrm{Span}\langle e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n \rangle$.

By induction, $V_i$ is complete with respect to $\|\cdot\|$ and hence closed. Then $e_i + V_i$ is also closed for all $i$, and hence $S := \bigcup_{i=1}^{n} e_i + V_i$ is a closed subset not containing 0.

Thus there is $C > 0$ such that $B(0, C) \cap S = \emptyset$.

Let $x = \sum_{i=1}^{n} x_i e_i$, and suppose $|x_j| = \max_i |x_i|$. Then $\|x\|_{\sup} = |x_j|$, and moreover, $\frac{1}{x_j} x \in S$.

So $\|\frac{1}{x_j} x\| \geq C, so \|x\| \geq C|x_j| = C\|x\|_{\sup}$.

The completeness of $V$ follows since $V$ is complete with respect to $\|\cdot\|_{\sup}$. □

**Definition 6.6.** *Let $R \subseteq S$ be rings. We say $s \in S$ is* **integral** *over $R$ if there exists a monic polynomial $f(x) \in R[x]$ such that $f(s) = 0$. The* **integral closure** *$R^{\mathrm{int}(S)}$ of $R$ inside $S$ is defined to be*

$$R^{\mathrm{int}(S)} = \{s \in S : s \textit{ integral over } R\}$$

*We say $R$ is integrally closed in $S$ if $R^{\mathrm{int}(S)} = R$.*

**Proposition 6.7.** *$R^{\mathrm{int}(S)}$ is a subring of $S$. Moreover, $R^{\mathrm{int}(S)}$ is integrally closed in $S$.*

*Proof.* Example sheet 2. □

**Lemma 6.8.** *Let $(K, |\cdot|)$ be a non-archimedean valued field. Then $O_K$ is integrally closed in $K$.*

*Proof.* Let $x \in K$ be integral over $O_K$, and without loss of generality $x \neq 0$.

Then let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in O_K[x]$ such that $f(x) = 0$. Then:

$$1 = -\frac{1}{x}a_{n-1} - a_{n-2}\frac{1}{x^2} - \ldots - a_0\frac{1}{x^n}$$

If $|x| > 1$, we have $1 = |1| = |-\frac{1}{x}a_{n-1} - \ldots - a_0\frac{1}{x^n}| < 1 \lightning$.

But then $|x| \leq 1$, so $x \in O_K$. □

*Proof of Theorem 6.1.* We show $|\cdot|_L = |N_{L/K}(\cdot)|$ satisfies the three axioms in the definition of absolute values.

1. 
$$\begin{aligned} |y|_L = 0 &\iff |N_{L/K}(y)| = 0 \\ &\iff N_{L/K}(y) = 0 \\ &\iff y = 0 \end{aligned}$$

2. 
$$\begin{aligned} |y_1y_2|_L &= |N_{L/K}(y_1y_2)|^{1/n} \\ &= |N_{L/K}(y_1y_2)|^{1/n} \\ &= |N_{L/K}(y_1)N_{L/K}(y_2)|^{1/n} \\ &= |N_{L/K}(y_1)|^{1/n}|N_{L/K}(y_2)|^{1/n} \\ &= |y_1|_L|y_2|_L \end{aligned}$$

3. Set $O_L = \{y \in L : \|y\|_L \leq 1\}$. We then claim that $O_L$ is the integral closure of $O_K$ inside $L$.

   To see this let $0 \neq y \in O_L$, we want to show that $y$ is integral over $O_K$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K[x]$ be the minimal polynomial of $y$. Then there is $m \geq 1$ with $N_{L/K}(y) = a_0^m$.

   By **4.5**, since $f$ is irreducible, the coefficient with the largest absolute value is either the first or the last in $f$. I.e.:
$$|a_i| \leq \max(|N_{L/K}(y)^{1/m}|, 1) =$$

   Now, since $|N_{L/K}(y)| \leq 1$, we have $|a_i| \leq 1$, i.e. $a_i \in O_K$.

   Hence $f \in O_K[x]$, and $y$ is integral over $O_K$.

Conversely, let $y \in L$ be integral over $\mathcal{O}_K$. Then $N_{L/K}(y) = \left(\prod_{\sigma:L\to\bar{K}} \sigma(y)\right)^d$ for some $d \geq 1$, where $\bar{K}$ is an algebraic closure of $K$ and $\sigma$ runs over all $K$-algebra homomorphisms.

For all such $\sigma : L \longrightarrow \bar{K}$, $\sigma(y)$ satisfies the same monic polynomials as $y$, so is also integral over $\mathcal{O}_K$. Thus $N_{L/K}(y) \in K$ is integral over $\mathcal{O}_K$, and hence $N_{L/K}(y) \in \mathcal{O}_K$.

But then $|N_{L/K}(y)| \leq 1$, and so $y \in \mathcal{O}_L$, so $\mathcal{O}_K^{\mathrm{int}(L)} = \mathcal{O}_L$, and the claim is proved.

Now let $x, y \in L$. Without loss of generality, assume that $|x|_L \leq |y|_L$. Then $|\frac{x}{y}|_L \leq 1$, and so $\frac{x}{y} \in \mathcal{O}_L$.

Since $1 \in \mathcal{O}_L$ and $\mathcal{O}_K^{\mathrm{int}(L)}$, we have $1 + \frac{x}{y} \in \mathcal{O}_L$, and hence $|1 + \frac{x}{y}| \leq 1$, i.e., $|x + y| \leq |y| = \max(|y|_L, |x|_L)$ as required.

For uniqueness, suppose $|\cdot|_L'$ is another absolute value on $L$ extending $|\cdot|$, then note that $|\cdot|_L, |\cdot|_L'$ are norms on $L$, hence induce the same topology on $L$, hence are equivalent, hence $|\cdot|_L' = |\cdot|_L^c$ for some $c > 0$. Since they agree on $K$, $c = 1$.

For the completeness part, since $|\cdot|_L$ defines a norm on $K$, **6.5** implies that $L$ is complete with respect to $|\cdot|_L$. □

**Corollary 6.9.** *Let $(K, |\cdot|)$ be a complete non-archimedean discretely valued field, and L?K a finite extension. Then*

1. *$L$ is discretely valued with respect to $|\cdot|_L$.*
2. *$\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in $L$.*

*Proof.*

1. Let $v$ be the valuation on $K$, $v_L$ the valuation on $L$ such that $v_L v$, and let $n = [L : K]$.

   Then for $y \in L^\times$, $|y|_L = |N_{L/K}(y)|^{1/n}$.

   Hence $v_L(y) = \frac{1}{n}v(N_{L/K}(y))$, and so $v_L(L^\times) \subseteq \frac{1}{n}v(K^\times)$, hence $v_L$ is discrete.
2. Proved in the previous section.

□

**Corollary 6.10.** *Let $(K, |\cdot|)$ be a complete non-archimedean discretely valued field, and $\bar{K}/K$ an algebraic closure of $K$. Then $|\cdot|$ extends to a unique absolute value $|\cdot|_{\bar{K}}$ on $\bar{K}$.*

*Proof.* Let $x \in \bar{K}$. Then $x$ is algebraic over $K$, so $x \in L$ for some $L/K$ finite. Define $|x|_{\bar{K}} = |x|_L$. This is well defined, i.e. is independent of $L$ by the uniqueness proven in **6.1**. The axioms for $|\cdot|_{\bar{K}}$ to be an absolute value can be checked over finite extensions, as can uniqueness. □

N.B.: $|\cdot|_{\bar{K}}$ is *never* discrete. Take $x \in K, |x| = 1$ (e.g. $p \in \mathbb{Q}_p$). Then for all $n \geq 0, v_{\bar{K}}(\sqrt[n]{x}) = \frac{1}{n}$, which can get arbitrarily close to zero as $x$ has all its roots in $\bar{K}$.

# 7 Local Fields

**Definition 7.1.** *Let $(K, |\cdot|)$ be a valued field. Then we say $K$ is a* **local field** *if it is complete and locally compact.*

For example, $\mathbb{R}$ and $\mathbb{C}$ are local fields.

**Proposition 7.2.** *Let $(K, |\cdot|)$ be a non-archimedean complete valued field. Then the following are equivalent:*

1. *$K$ is locally compact.*
2. *$O_K$ is compact.*
3. *$v$ is discrete and $k := O_K/m$ is finite.*

*Proof.*

<u>1. $\implies$ 2.</u> Let $U \ni 0$ be a compact neighbourhood of 0. Then $\exists\ x \in O_K$ such that $xO_K \subseteq U$. Since $xO_K$ is closed, $xO_K$ is compact, and hence $O_K$ is compact, as there is a homeomorphism $xO_K \xrightarrow{x^{-1}} O_K$.

<u>2. $\implies$ 1.</u> $O_K$ is compact, so $a + O_K$ is compact for all $a \in K$, and hence $K$ is locally compact as every $a \in K$ has compact neighbourhood $a + O_K$.

<u>2. $\implies$ 3.</u> Let $x \in m$, and $A_x \subseteq O_K$ be a set of coset representatives for $O_K/xO_K$.

Then $O_K = \bigcup_{y \in A_x} y + xO_K$, which is a disjoint union of open subsets, and hence an irreducible open cover. So by compactness, $A_x$ is finite. So $O_K/m$, which is a quotient of $O_K/xO_K$, is finite.

Now suppose that $v$ is not discrete. Let $x = x_1, x_2, x_3, \ldots$ be a sequence such that

$$v(x_1) > v(x_2) > v(x_3) > \ldots > 0$$

Then we have

$$xO_K \subsetneq x_2O_K \subsetneq x_3O_K \subsetneq \ldots \subsetneq O_K$$

But $O_K/xO_K$ is finite, so can only have finitely many subgroups as an additive group $\lightning$.

Hence $v$ must be discrete.

<u>3. $\implies$ 2.</u> Since $O_K$ is a metric space, it suffices to show $O_K$ is sequentially compact. Let $(x_n)_{n=1}^\infty$ be a sequence in $O_K$ and fix $\pi \in O_K$ a uniformizer.

Then since $\pi^i O_K/\pi^{i+1}O_K \cong k, O_K/\pi^i O_K$ is finite, as $O_K \supseteq \pi O_k \supseteq \ldots \supseteq \pi^i O_K$, and each quotient is finite, hence the total quotient is finite.

Since $O_K/\pi O_K$ is finite, there is some $a \in O_K/\pi O_K$ and a subsequence $(x_{1,n})_{n=1}^\infty$ such that $x_{1,n} \equiv a \mod \pi$.

Define $y_1 = x_{1,1}$.

Since $O_K/\pi^2 O_K$ is finite, there is some $a_2 \in O_K/\pi^2 O_K$ and a subsequence $(x_{2,n})_{n=1}^\infty$ such that $x_{2,n} \equiv a_2 \mod \pi^2 O_K$.

Define $y_2 = x_{2,2}$.

Continuing in this fashion, we get the sequences $(x_{i,n})_{n=1}^{\infty}$ for $i = 1, 2, \ldots$, such that $(x_{i+1,n})_{n=1}^{\infty}$ is a subsequence of $(x_{i,n})_{n=1}^{\infty}$, and, for any $i$, there is some $a_i \in O_K/\pi^i O_K$ with $x_{i,n} \equiv a_i \mod \pi^i$ for all $n$.

Then necessarily $a_i \equiv a_{i+1} \mod \pi^i$ for all $i$. With $y_i = x_{i,i}$, we have $y_i \equiv y_{i+1} \mod \pi^i$, and so $y_i$ is Cauchy, and hence converges by completeness, and hence $O_K$ is sequentially compact.

□

Examples:

1. $\mathbb{Q}_p$ is a local field.
2. $\mathbb{F}_p((t))$ is a local field.

## 7.1 More On Inverse Limits

Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets/groups/rings and $\varphi_n : A_{n+1} \to A_n$ be homomorphisms.

**Definition 7.3.** *Assume $A_n$ is finite for all $n$. Then the* **profinite topology** *on $A := \varprojlim_n A_n$ is the weakest topology on $A$ such that $A \to A_n$ is continuous for all $n$, where $A_n$ are equipped with the discrete topology.*

$A$ with the profinite topology is then compact, totally disconnected, and Hausdorff.

**Proposition 7.4.** *Let $(K, |\cdot|)$ be a local field. Under the isomorphism*

$$O_K \cong \varprojlim_n O_K/\pi^n O_K$$

*where $\pi$ is a uniformizer, the topology on $O_K$ induced via $|\cdot|$ coincides with the profinite topology.*

*Proof.* Just need to check that, if

$$\mathcal{B} := \{a + \pi^n O_K : n \in \mathbb{N}_{\geq 1}, a \in A_{\pi^n}\}$$

where $A_{\pi^n}$ is a set of coset representatives for $O_K/\pi^n O_K$, then $\mathcal{B}$ is a basis of open sets in both topologies.

For $|\cdot|$, this is immediate.

For the profinite topology, $O_K \to O_K/\pi^n O_K$ is continuous if and only if $a + \pi^n O_K$ is open for all $a \in A_{\pi^n}$. Then $\mathcal{B}$ is a basis for the profinite topology. □

This gives another proof that $O_K$ is compact.