Local Fields

October 16, 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.

$$|x| < 1 \iff x^n \to 0 \text{ w.r.t. } |\cdot| \tag{2}$$
$$\iff x^n \to 0 \text{ w.r.t. } |\cdot|' \tag{3}$$
$$\iff |x|' < 1 \tag{4}$$

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

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 $x_n^2 \to -1 \implies L^2 = -1 \not\downarrow$. 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 $x, x^{-1} \in \mathcal{O}_K$, i.e. $x \in \mathcal{O}_K^\times$.

□

As a point of notation, we will define $m \coloneqq \{x \in \mathcal{O}_K : |x| < 1\}$, a maximal ideal of $\mathcal{O}_K$, and $k \coloneqq \mathcal{O}_K/m$ 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. *$\mathcal{O}_K$ is a local ring with a unique maximal ideal m.*

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

Examples:

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

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 $\pi \in \mathcal{O}_K$ 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 π a uniformizer.

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

1. *v is discrete.*
2. *$\mathcal{O}_K$ is a PID.*
3. *$\mathcal{O}_K$ is noetherian.*
4. *m is principal.*

Proof.
1. $\implies$ 2. Let $I \subseteq \mathcal{O}_K$ 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 $x\mathcal{O}_K = \{a \in O_K : v(a) \geq v(x)\} \subseteq I$, and hence $x\mathcal{O}_K = I$ by definition of x - if $y \in I \setminus (x)$, then $v(y) < v(x)$↯.

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

3. $\implies$ 4. Write $m = x_1\mathcal{O}_K + \ldots + x_n\mathcal{O}_K$. WLOG, $v(x_1) \leq v(x_2) \leq \ldots \leq v(x_n)$. Then $m = x_1\mathcal{O}_K$.

4. $\implies$ 1. Let $m = \pi\mathcal{O}_K$ for some $\pi \in \mathcal{O}_K$, 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 $\pi \in \mathcal{O}_K$ a uniformizer. Then for any $x \in K^\times$ there exists $n \in \mathbb{Z}$ and $u \in \mathcal{O}_K^\times$ such that $x = \pi^n u$. In particular, $K = \mathcal{O}_K\left[\frac{1}{x}\right]$ for any $x \in m$ and hence $K = \operatorname{Frac} \mathcal{O}_K$.*

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

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 $K \coloneqq \mathrm{Frac}(R)$ 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 π 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 $\mathcal{O}_K = R$.

□

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 $a_{n+1} \overset{\varphi_n}{\longmapsto} a_n \overset{\varphi_{n-1}}{\longmapsto} a_{n-1}$. 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*

$$\begin{array}{ccc} B & \xrightarrow{\psi_{n+1}} & A_{n+1} \\ & \searrow^{\psi_n} & \downarrow{\scriptstyle \varphi_n} \\ & & A_n \end{array}$$

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 $\widehat{R} \coloneqq \varprojlim_n R/I^n$, 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 $\pi \in \mathcal{O}_K$ such that $|\pi| < 1$.

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

1. *$\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$, i.e. $\mathcal{O}_K$ is π-adically complete.*

2. *If in addition K is discretely valued and π is a uniformizer, then every element $x \in \mathcal{O}_K$ 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 $k \coloneqq \mathcal{O}_K/\pi\mathcal{O}_K$.*

   Moreover, any series $\sum_{i=0}^{\infty} a_i \pi^i$ converges in $\mathcal{O}_K$.

Proof.

1. There is a natural map $i : \mathcal{O}_K \to \varprojlim_n \mathcal{O}_K/\pi\mathcal{O}_K$. Since $\bigcap_{n=1}^{\infty} \pi^n \mathcal{O}_K = \{0\}$, i is injective.

   Now let $(x_n)_{n=1}^{\infty} \in \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$, and for each n choose $y_n \in \mathcal{O}_K$ a lift of $x_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$.

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

   So $(y_n)_{n=1}^{\infty}$ is a Cauchy sequence in $\mathcal{O}_K$, but $\mathcal{O}_K$ is complete as $\mathcal{O}_K \subseteq K$ 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 $x \in \mathcal{O}_K$. Choose a_i inductively as follows:

   Choose $a_0 \in A$ such that $a_0 \equiv x \mod \pi\mathcal{O}_K$. 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 $c \in \mathcal{O}_K$. Then choose $a_{k+1} \equiv c \mod \pi\mathcal{O}_K$.

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

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

   For the moreover part, any series of this form defines a Cauchy sequence, which as in *1* converges in $\mathcal{O}_K$.

□

Warning: if $(K, |\cdot|)$ is not discretely valued, then $\mathcal{O}_K$ 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 $K = \mathcal{O}_K\left[\frac{1}{\pi}\right]$. □

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 $f_n : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$, 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, $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ 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.*

□

Examples:

- $\frac{1}{1-p} = 1 + p + p^2 + p^3 + \ldots \in \mathbb{Q}_p$.
- Let $K = k((t))$ with the t-adic valuation. Then $\mathcal{O}_K = k[[t]] = \varprojlim_n k[[t]]/(t^n)$. Moreover, $\mathcal{O}_K$ 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 $\mathcal{O}_K$ 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 $f(x) \in \mathcal{O}_K[x]$, and assume there exists $a \in \mathcal{O}_K$ such that $|f(a)| < |f'(a)|^2$.*

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

Proof. Let $\pi \in \mathcal{O}_K$ be a uniformizer, and let $r = v(f'(a))$. We construct a sequence $(x_n)_{n=1}^{\infty}$ in $\mathcal{O}_K$ 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 $x_{n+1} \coloneqq x_n - \frac{f(x_n)}{f'(x_n)}$. 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 $f_i(x) \in \mathcal{O}_K[x]$, 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 $x \in \mathcal{O}_K$. 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 $f(x) \in \mathcal{O}_K[x]$, and $\bar{c} \in k \coloneqq \mathcal{O}_K/m$ a simple root of $\bar{f}(x) \coloneqq f(x) \mod m \in k[x]$ (i.e. not a root of $\bar{f}'(x)$).*

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

Proof. Apply **4.1** to a lift $c \in \mathcal{O}_K$ 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 $\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}$, given by $(u, p) \mapsto up^n$

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

$p = 2$: Let $b \in \mathbb{Z}_2^\times$. Consider $f(x) = x^2 - b$. Then $f'(x) = 2x \cong 0 \mod 2$, 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 fine 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 $\bar{f}(x) \coloneqq f(x) \mod m \in k[x]$ 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. □