Part III - Local Fields

Lectured by Rong Zhou

Artur Avameri

Contents

0 Introduction

This is a first class in graduate algebraic number theory. Something we'd like to do is solve diophantine equations, e.g. $f(x_1, \dots, x_r) \in \mathbb{Z}[x_1, \dots, x_r]$. In general, solving $f(x_1, \dots, x_r) = 0$ is very difficult. A simpler question we might consider is solving $f(x_1, \dots, x_r) \equiv 0 \pmod{p}$, or $\pmod{p^2}$, $\pmod{p^3}$, etc. Local fields package all of this information together.

1 Absolute values

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

(1) $|x| = 0 \iff x = 0$.

(2) $|xy| = |x||y| \ \forall x, y \in K$.

(3) $|x + y| \leq |x| + |y| \ \forall x, y \in K$ (triangle inequality).

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

- Take $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with the usual absolute value $|a + ib| = \sqrt{a^2 + b^2}$. We call this $|\cdot|_\infty$.

- For K any field, we have the trivial absolute value $|x| = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{else.} \end{cases}$

  We will ignore this in this course.

- Take $K = \mathbb{Q}$ and p a prime. For $0 \neq x \in \mathbb{Q}$, write $x = p^n \frac{a}{b}$ where $(a, p) = (b, p) = 1$. Then 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 can check the axioms:

  (1) The first axiom is clear.

  (2)
$$|xy|_p = \left| p^{n+m} \frac{ac}{bd} \right|_p = p^{-(n+m)} = |x|_p |y|_p.$$

  (3) WLOG let $m \geq n$. Then

$$|x + y|_p = \left| p^n \left(\frac{ad + p^{m-n} bc}{bd} \right) \right|_p \leq p^{-n} = \max(|x|_p, |y|_p).$$

Any absolute value $|\cdot|$ on K induces a metric $d(x,y) = |x-y|$ on K, hence induces a topology on K.

Definition 1.2. Suppose we have two absolute values $|\cdot|, |\cdot|'$ on K. We say these absolute values are **equivalent** if they induce the same topology. An equivalence class is called a **place**.

Proposition 1.1. Let $|\cdot|, |\cdot|'$ be (nontrivial) absolute values on K. Then the following are equivalent:

(i) $|\cdot|$ and $|\cdot|'$ are equivalent.

(ii) $|x| < 1 \iff |x|' < 1\ \forall x \in K$.

(iii) $\exists c \in \mathbb{R}_{>0}$ such that $|x|^c = |x'|\ \forall x \in K$.

Proof. (i) $\implies$ (ii): $|x| < 1 \iff x^n \to 0$ with respect to $|\cdot| \iff x^n \to 0$ with respect to $|\cdot|'$ (since the topologies are the same) $\iff |x|' < 1$.

(ii) $\implies$ (iii): Note that $|x|^c = |x|' \iff c\log|x| = \log|x|'$. Take $a \in K^\times$ such that $|a| > 1$. This exists since $|\cdot|$ is nontrivial. We need to show that $\forall x \in K^\times$,

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

Assume $\frac{\log|x|}{\log|a|} < \frac{\log|x|'}{\log|a|'}$. Choose $m, n \in \mathbb{Z}$ such that $\frac{\log|x|}{\log|a|} < \frac{m}{n} < \frac{\log|x|'}{\log|a|'}$. We then have

$$\begin{cases} n\log|x| < m\log|a| \\ n\log|x|' > m\log|a|' \end{cases}$$
$$\implies \left|\frac{x^n}{a^m}\right| < 1, \left|\frac{x^n}{a^m}\right|' > 1,$$

a contradiction. The other inequality is analogous.

(iii) $\implies$ (i): Clear, since they have the same open balls. $\square$

Remark. $|\cdot|_\infty^2$ on $\mathbb{C}$ is not an absolute value by our definition (doesn't satisfy the triangle inequality). Some authors replace the triangle inquality by the condition $|x+y|^\beta \le |x|^\beta + |y|^\beta$ for some fixed $\beta \in \mathbb{R}_{>0}$. The equivalence classes are the same in either case.

In this course, we will mainly be interested in the following:

Definition 1.3. An absolute value $|\cdot|$ on K is said to be **non-archimedean** if it satisfies the **ultrametric inequality**

$$|x+y| \le \max(|x|, |y|).$$

If $|\cdot|$ is not non-archimedean, we say it is **archimedean**.

Example 1.1.
- $|\cdot|_\infty$ on $\mathbb{R}$ is archimedean.
- $|\cdot|_p$ on $\mathbb{Q}$ is non–archimedean.

Lemma 1.2. Let $(K, |\cdot|)$ be non–archimedean and $x, y \in K$. If $|x| < |y|$, then $|x - y| = |y|$.

Proof. On the one hand, $|x-y| \leq \max(|x|, |y|) = |y|$ (using $|x| = |-x|$).

On the other, $|y| \leq \max(|x|, |x-y|) = |x-y|$. □

Convergence is easier in non–archimedean fields:

Proposition 1.3. Let $(K, |\cdot|)$ be non–archimedean and $(x_n)_{n=1}^\infty$ a sequence on K. If $|x_n - x_{n+1}| \to 0$, then $(x_n)_{n=1}^\infty$ is Cauchy. In particular, if K is complete, then the sequence converges.

Proof. For $\epsilon > 0$, choose N such that $|x_n - x_{n+1}| < \epsilon$ for $n \geq N$. Then for $N < n < m$,

$$|x_n - x_m| = |(x_n - x_{n+1}) + (x_{n+1} - x_{n+2}) + \ldots + (x_{m-1} - x_m)| < \epsilon,$$

so (x_n) is Cauchy. □

Example 1.2. For $p = 5$, we can construct a sequence in $\mathbb{Q}$ satisfying:

(i) $x_n^2 + 1 \equiv 0 \pmod{5^n}$,

(ii) $x_n \equiv x_{n+1} \pmod{5^n}$.

We construct it by induction. Take $x_1 = 2$. Now suppose we've constructed x_n and write $x_n^2 + 1 = a \cdot 5^n$ and set $x_{n+1} = x_n + b \cdot 5^n$. We compute

$$x_{n+1}^2 + 1 = x_n^2 + 2bx_n 5^n + b^2 5^{2n} + 1 = a5^n + 2bx_n 5^n + \underbrace{b^2 5^{2n}}_{\equiv 0 \pmod{5^{n+1}}} + 1.$$

Hence we choose b such that $a + 2bx_n \equiv 0 \pmod 5$ and we're done.

Now (ii) tells us that (x_n) is Cauchy, but we claim it doesn't converge. Suppose it does, $x_n \to l \in \mathbb{Q}$. Then $x_n^2 \to l^2 \in \mathbb{Q}$. But by (i), $x_n^2 \to -1$, so $l^2 = -1$, a contradiction.

This tells us that $(\mathbb{Q}, |\cdot|_5)$ is not complete.

Definition 1.4. The p–adic numbers $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

10 Oct 2022, Lecture 2

Let $(K, |\cdot|)$ be a non–archimedean valued field. For $x \in K$ and $r \in \mathbb{R}_{>0}$, we define $B(x, r) = \{y \in K \mid |y - x| < r\}$ and $\overline{B} = \{y \in K \mid |y - x| \leq r\}$ to be the open and closed balls of radius r.

Lemma 1.4. (i) If $z \in B(x,r)$, then $B(z,r) = B(x,r)$, i.e. open balls don't have centers.

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

(iii) $B(x,r)$ is closed.

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

Proof. (i) Let $y \in B(x,r)$. Then $|x-y| < r \implies |z-y| = |(z-x)+(x-y)| \leq \max(|z-x|, |x-y|) < r$, so $B(x,r) \subset B(z,r)$. The reverse inclusion is analogous.

(ii) Analogous to (i) by replacing $<$ with $\leq$.

(iii) Let $y \in K \setminus B(x,r)$. If $z \in B(x,r) \cap B(y,r)$, then $B(x,r) = B(z,r) = B(y,r)$ by (i), so $y \in B(x,r)$, a contradiction. Hence $B(x,r) \cap B(y,r) = \varnothing$. Since y was arbitrary, $K \setminus B(x,r)$ is open, so $B(x,r)$ is closed.

(iv) If $z \in \overline{B}(x,r)$, then $B(z,r) \subset \overline{B}(z,r) \overset{\text{(ii)}}{=} \overline{B}(x,r)$.

□

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

(i) $v(xy) = v(x) + v(y)$.

(ii) $v(x+y) \geq \min(v(x), v(y))$.

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 on K. Conversely, a non–archimedean absolute value on K determines a valuation $v(x) = \log_\alpha |x|$.

Remark. We ignore the trivial evaluation $v(x) = 0 \; \forall x \in K$, which corresponds to the trivial absolute value.

Definition 2.2. We say valuations v_1, v_2 are equivalent if $\exists c \in \mathbb{R}_{>0}$ such that $v_1(x) = cv_2(x) \; \forall x \in K^\times$.

Example 2.1.
- If $K = \mathbb{Q}$, $v_p(x) = -\log_p |x|_p$ is the p–adic valuation.
- Let k be a field. Let $K = k(t) = \mathrm{Frac}(k[t])$ be a rational function field. We let
$$v\left(t^n \frac{f(t)}{g(t)}\right) = n$$
for $f, g \in k[t]$, $f(0) \neq 0, g(0) \neq 0$. This is called a t–adic valuation.

- Let $K = k((t)) = \mathrm{Frac}(k[[t]]) = \{\sum_{i=n}^{\infty} a_i t^i \mid a_i \in k, n \in \mathbb{Z}\}$, the field of formal Laurent series over k. We define
$$v\left(\sum_i a_i t^i\right) = \min\{i \mid a_i \neq 0\},$$
the t–adic valuation on K.

Definition 2.3. Let $(K, |\cdot|)$ be a non–archimedean valued field. The **valuation ring** of K is defined to be

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

(i.e. the closed unit ball, $\mathcal{O}_K = \overline{B}(0,1)$, or $\mathcal{O}_K = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$).

Proposition 2.1. (i) $\mathcal{O}_K$ is an open subring of K.

(ii) The subsets $\{x \in K \mid |x| \leq r\}$ and $\{x \in K \mid |x| < r\}$ for $r \leq 1$ are open ideals in $\mathcal{O}_K$.

(iii) $\mathcal{O}_K^\times = \{x \in K \mid |x| = 1\}$.

Proof. (i) We find:

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

Thus $\mathcal{O}_K$ is a subring, and since $\mathcal{O}_K = \overline{B}(0,1)$, it is open.

(ii) As $r \leq 1$, $\{x \in K \mid |x| \leq r\} = \overline{B}(0,r) \subset \mathcal{O}_K$, so it is open. We find:

- If $x, y \in \overline{B}(0,r)$, then $|x+y| \leq \max(|x|, |y|) \leq r$, so $x + y \in \overline{B}_r$.
- If $x \in \mathcal{O}_K, y \in \overline{B}_r$, then $|xy| = |x||y| \leq 1 \cdot |y| \leq r$, so $xy \in \overline{B}_r$.

Hence this is an open ideal. The proof for $\{x \in K \mid |x| < r\}$ is analogous.

(iii) Note that $|x||x^{-1}| = |xx^{-1}| = 1$. Thus $|x| = 1 \iff |x^{-1}| = 1 \iff x, x^{-1} \in \mathcal{O}_K \iff x \in \mathcal{O}_K^\times$.

$\square$

Notation. Let $\mathfrak{m} = \{x \in \mathcal{O}_K \mid |x| < 1\}$. It turns out this is a maximal ideal in $\mathcal{O}_K$. Also let $\mathfrak{k} = \mathcal{O}_K/\mathfrak{m}$, the residue field.

Corollary 2.2. $\mathcal{O}_K$ is a **local ring** (i.e. a ring with a unique maximal ideal) with unique maximal ideal $\mathfrak{m}$.

Proof. Let $\mathfrak{m}'$ be a maximal ideal. If $\mathfrak{m}' \neq \mathfrak{m}$, then $\exists x \in \mathfrak{m}' \setminus \mathfrak{m}$. Hence $|x| = 1$, so by (iii) above, x is a unit, so $\mathfrak{m}' = \mathcal{O}_K$, a contradiction. $\square$

Example 2.2. $K = \mathbb{Q}$ with $|\cdot|_p$. Then $\mathcal{O}_K = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$. In this case, $\mathfrak{m} = p\mathbb{Z}_{(p)}$ and $\mathfrak{k} = \mathbb{F}_p$.

Definition 2.4. Let $v : K^\times \to \mathbb{R}$ be a valuation. If $v(K^\times) \cong \mathbb{Z}$, then we say v is a **discrete valuation**. In this case, K is said to be a **discretely valued field**.

An element $\pi \in \mathcal{O}_K$ is said to be a **uniformizer** if $v(\pi) > 0$ and $v(\pi)$ generates $v(K^\times)$.

Example 2.3.

- $K = \mathbb{Q}$ with the p–adic valuation and $K = k(t)$ with the t–adic valuation are discretely valued fields.
- $K = k(t)(t^{\frac{1}{2}}, t^{\frac{1}{4}}, t^{\frac{1}{8}}, \ldots)$ with the t–adic valuation is not a discretely valued field.

Remark. If v is a discrete valuation, we can scale v, i.e. replace it with an equivalent valuation such that $v(K^\times) = \mathbb{Z}$. Such v are called **normalized valuations**. Then π is a uniformizer $\iff v(\pi) = 1$.

Lemma 2.3. Let v be a valuation on K. Then the following are equivalent:

(i) v is discrete;

(ii) $\mathcal{O}_K$ is a PID;

(iii) $\mathcal{O}_K$ is Noetherian;

(iv) $\mathfrak{m}$ is principal.

Proof. (i) $\implies$ (ii): $\mathcal{O}_K \subset K$, so $\mathcal{O}_K$ is an integral domain. Let $I \subset \mathcal{O}_K$ be a nonzero ideal and pick $x \in I$ such that $v(x) = \min\{v(a) \mid a \in I, a \neq 0\}$, which exists as v is discrete. Then we claim that $x\mathcal{O}_K = \{a \in \mathcal{O}_K \mid v(a) \geq v(x)\}$ is equal to I. The inclusion $x\mathcal{O}_K \subset I$ is clear, as I is an ideal. For $x\mathcal{O}_K \supset I$, let $y \in I$, then $v(x^{-1}y) = v(y) - v(x) \geq 0 \implies y = x(x^{-1}y) \in x\mathcal{O}_K$.

(ii) $\implies$ (iii): Clear, as being a PID means every ideal is generated by one element, i.e. by finitely many.

(iii) $\implies$ (iv): Write $\mathfrak{m} = x_1\mathcal{O}_K + \ldots + x_n\mathcal{O}_K$ and WLOG assume $v(x_1) \leq v(x_2) \leq \ldots \leq v(x_n)$. Then $x_2, \ldots, x_n \in x_1\mathcal{O}_K$, since $x_1\mathcal{O}_K = \{a \in \mathcal{O}_K \mid v(a) \geq v(x_1)\}$, so $\mathfrak{m} = x_1\mathcal{O}_K$.

(iv) $\implies$ (i): Let $\mathfrak{m} = \pi\mathcal{O}_K$ for some $\pi \in \mathcal{O}_K$ and let $c = v(\pi)$. Then if $v(x) > 0$, i.e. $x \in \mathfrak{m}$, then $v(x) \geq c$. Thus $v(K^\times) \cap (0, c) = \varnothing$. Since $v(K^\times)$ is a subgroup of $(\mathbb{R}, +)$, we have $v(K^\times) = c\mathbb{Z}$. $\square$

Remark. Let v be a discrete valuation on K, $\pi \in \mathcal{O}_K$ a uniformizer. For $x \in K^\times$, let $n \in \mathbb{Z}$ such that $v(x) = nv(\pi)$. Then $u = x\pi^{-n} \in \mathcal{O}_K^\times$ and $x = u\pi^n$. In particular, $K = \mathcal{O}_K\left[\frac{1}{\pi}\right]$ and hence $K = \mathrm{Frac}(\mathcal{O}_K)$. 12 Oct 2022, Lecture 3

Definition 2.5. A ring R is called a **discrete valuation ring** (DVR) if it is a PID with exactly one nonzero prime ideal (which is then necessarily maximal).

Lemma 2.4. (i) Let v be a discrete valuation on K. Then $\mathcal{O}_K$ is a DVR.

(ii) Let R be a DVR. Then there exists a valuation v on $K = \mathrm{Frac}(R)$ such that $R = \mathcal{O}_K$.

Proof. (i) $\mathcal{O}_K$ is a PID by the previous lemma, hence any nonzero prime ideal is maximal. Since $\mathcal{O}_K$ is a local ring, it is a DVR.

(ii) Let R be a DVR with maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} = (\pi)$ for $\pi \in R$. Since PIDs are UFDs, we can write any nonzero $x \in R$ uniquely as $\pi^n u$ for some $n \geq 0$, u a unit (since π is the only prime). Then any $y \in K^\times$ can be written uniquely as $\pi^m u$, $m \in \mathbb{Z}$. Define $v(\pi^m u) = m$. Exercise: check that this is a valuation and $R = \mathcal{O}_K$.

□

Example 2.4. $\mathbb{Z}_{(p)}$, $R[[t]]$ for R a field are DVRs.

3 p–adic numbers

Recall that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. It is an exercise on example sheet 1 to show that $\mathbb{Q}_p$ is a field. Moreover, $|\cdot|_p$ extends to $\mathbb{Q}_p$ and the associated valuation is discrete (example sheet again).

Definition 3.1. The **ring of p–adic integers** $\mathbb{Z}_p$ is the valuation ring

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}.$$

Facts. $\mathbb{Z}_p$ is a DVR and has a principal maximal ideal $p\mathbb{Z}_p$. In $\mathbb{Z}_p$, all nonzero ideals are given by $p^n\mathbb{Z}_p$.

Proposition 3.1. $\mathbb{Z}_p$ 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 $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Note $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Since $\mathbb{Z}_p \subset \mathbb{Q}_p$ is open, $\mathbb{Z}_p \cap \mathbb{Q}$ is dense in $\mathbb{Z}_p$. But

$$\mathbb{Z}_p \cap \mathbb{Q} = \{x \in \mathbb{Q} \mid |x|_p \leq 1\} = \left\{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\right\} = \mathbb{Z}_{(p)}.$$

Thus it suffices to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$. Let $\frac{a}{b} \in \mathbb{Z}_{(p)}$ with $a, b \in \mathbb{Z}$ and $p \nmid b$. For $n \in \mathbb{N}$, choose $y_n \in \mathbb{Z}$ such that $by_n \equiv a \pmod{p^n}$. Then $y_n \to \frac{a}{b}$ as $n \to \infty$.

For the last part, note that $\mathbb{Z}_p$ is complete (as it is a closed subset of a complete space) and $\mathbb{Z} \subset \mathbb{Z}_p$ is dense. □

Inverse limits. Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets/groups/rings together with homomorphisms $\phi_n : A_{n+1} \to A_n$ (called **transition maps**). Then the **inverse limit** of $(A_n)_{n=1}^{\infty}$ is the set/group/ring

$$\varprojlim_n A_n = \left\{ (a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} A_n \mid \phi_n(a_{n+1}) = a_n \ \forall n \right\}.$$

Fact. If A_n is a group/ring, then the inverse limit is also a group/ring. Here the group/ring operations are defined componentwise. Let $\theta_m : \varprojlim_n A_n \to A_m$ denote the natural projection.

The inverse limit satisfies the following universal property:

Proposition 3.2. For any set/group/ring B together with homomorphisms $\psi_n : B \to A_n$ such that the following diagram commutes,

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

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

Proof. Define $\psi : B \to \prod_{n=1}^{\infty} A_n$ by $b \mapsto (\psi_n(b))_{n=1}^{\infty}$. Then $\psi_n = \theta_n \circ \psi_{n+1} \implies \psi(b) \in \varprojlim_n A_n$. This map is clearly unique (determined by $\psi_n = \phi_n \circ \psi_{n+1}$), and is a homomorphism of sets/groups/rings. □

Definition 3.2. Let $I \subset R$ be an ideal (in a ring R). The I–**adic completion of** R is the ring $\hat{R} = \varprojlim_n R/I^n$ where $R/I^{n+1} \to R/I^n$ is the natural projection.

Note that there exists a natural map $i : R \to \hat{R}$ by the universal property (since there exist maps $R \to R/I^n$).

Definition 3.3. We say R is I–**adically complete** if i is an isomorphism.

Fact. $\ker(i : R \to \hat{R}) = \bigcap_{n=1}^{\infty} I^n$ (check!).

Let $(K, |\cdot|)$ be a non–archimedean valued field and $\pi \in \mathcal{O}_K$ such that $|\pi| < 1$.

Proposition 3.3. Assume K is complete with respect to $|\cdot|$. Then:

(i) $\mathcal{O}_K \overset{i}{\cong} \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ (i.e. $\mathcal{O}_K$ is π–adically complete)[1].

(ii) Every $x \in \mathcal{O}_K$ can be written uniquely as $x = \sum_{i=0}^{\infty} a_i \pi^i$ with $a_i \in A$, where $A \subset \mathcal{O}_K$ is a set of coset representatives for $\mathcal{O}_K/\pi\mathcal{O}_K$. Moreover, any such power series converges (in $\mathcal{O}_K$).

Proof. (i) K is complete and $\mathcal{O}_K \subset K$ is closed, so $\mathcal{O}_K$ is complete. If $x \in \bigcap_{n=1}^{\infty} \pi^n\mathcal{O}_K$, then $v(x) \geq nv(\pi)\ \forall n \implies x = 0$, hence the natural map $\mathcal{O}_K \to \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ is injective.

For surjectivity, let $(x_n)_{n=1}^{\infty} \in \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ and for each n, let $y_n \in \mathcal{O}_K$ be a lifting[2] of $x_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$. Then $y_n - y_{n+1} \in \pi^n\mathcal{O}_K$, thus $(y_n)_{n=1}^{\infty}$ is a Cauchy sequence in $\mathcal{O}_K$. Let $y_n \to y \in \mathcal{O}_K$. Then y maps to $(x_n)_{n=1}^{\infty}$ in $\varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$.

(ii) Left as exercise on example sheet 1.

□

Corollary 3.4. (i) $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

(ii) Every element in $\mathbb{Q}_p$ can be written uniquely as $x = \sum_{i=n}^{\infty} a_i p^i$ where we have $a_i \in \{0, 1, \dots, p-1\}$.

14 Oct 2022, Lecture 4

Proof. (i) By the previous proposition, it suffices to show that $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}$. Let $f_n : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ be the natural map. Then $\ker(f_n) = \{x \in \mathbb{Z} \mid |x|_p \leq p^{-n}\} = p^n\mathbb{Z}$, thus the natural map $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ is injective. For surjectivity, take $\overline{z} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ and $c \in \mathbb{Z}_p$ a lift. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, there exists $x \in \mathbb{Z}$ such that $x \in c + p^n\mathbb{Z}_p$ ($p^n\mathbb{Z}_p$ is open in $\mathbb{Z}_p$). Then $f_n(x) = \overline{z}$, so $Z/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ is surjective.

(ii) Follows from the second part of the previous proposition applied to $p^{-n}x \in \mathbb{Z}_p$ for some $n \in \mathbb{Z}$.

□

Example 3.1. We have $\frac{1}{1-p} = 1 + p + p^2 + p^3 + \dots$ in $\mathbb{Q}_p$.

[1] There a bit of abuse of notation here – really, $\mathcal{O}_K$ is (π)–adically complete.

[2] Given a surjective map $G \to G'$, a lift of an element $x \in G'$ is a choice of $y \in G$ such that $y \mapsto x$ under this map.

4 Complete valued fields

4.1 Hensel's lemma

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 $\exists a \in \mathcal{O}_K$ such that $|f(a)| < |f'(a)|^2$ for $f'(a)$ the formal derivative. 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 $r = v(f'(a))$ where v is a normalized valuation, i.e. $v(\pi) = 1$. We inductively construct a sequence (x_n) in $\mathcal{O}_K$ such that

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

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

Take $x_1 = a$, so $f(x_1) \equiv 0 \pmod{\pi^{1+2r}}$. Now suppose we've constructed $x_1, \ldots, x_n$ satisfying the conditions. Then define $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$. Since $x_n \equiv x_1 \pmod{\pi^{r+1}}$, $v(f'(x_n)) = v(f'(x_1)) = r$ and hence $\frac{f(x_n)}{f'(x_n)} \equiv 0 \pmod{\pi^{n+r}}$ by (i). It follows that $x_{n+1} \equiv x_n \pmod{\pi^{n+r}}$, so (ii) holds.

Note that for X, Y indeterminates, we can write $f(X + Y) = f_0(X) + f_1(X)Y + f_2(X)Y^2 + \ldots$, where $f_i \in \mathcal{O}_K[X]$ and $f_0(X) = f(X), f_1(X) = f'(X)$. Thus $f(x_{n+1}) = f(x_n) + f'(x_n)c + f_2(x_n)c^2 + \ldots$ for $c = -\frac{f(x_n)}{f'(x_n)}$. Since $c \equiv 0 \pmod{\pi^{n+r}}$ and $v(f_i(x_n)) \geq 0$, we have $f(x_{n+1}) \equiv f(x_n) + cf'(x_n) \pmod{\pi^{n+2r+1}}$ (since the other terms vanish), but this is $\equiv 0 \pmod{\pi^{n+2r+1}}$, so (i) holds.

This gives the construction of (x_n). Property (ii) implies that (x_n) is Cauchy, so let $x \in \mathcal{O}_K$ be the limit, $x_n \to x$. Then $f(x) = \lim_{n\to\infty} f(x_n) = 0$ by property (i). Moreover, (ii) implies $a = x_1 \equiv x_n \pmod{\pi^{r+1}}$ $\forall n$, so $a \equiv x \pmod{\pi^{r+1}}$, thus $|x - a| < |f'(a)|$.

For uniqueness, suppose x' also satisfies $f(x') = 0$ and $|x' - a| < |f'(a)|$. Set $\delta = x' - x \neq 0$. Then $|x' - a| < |f'(a)|$ and $|x - a| < |f'(a)|$, so the ultrametric inequality implies $|\delta| = |x' - x| < |f'(a)| = |f'(x)|$ (since $a \equiv x \pmod{\pi^{r+1}}$). But

$$0 = f(x') = f(x + \delta) = \underbrace{f(x)}_{=0} + f'(x)\delta + \underbrace{\delta^2 \ldots}_{|\cdot| \leq |\delta|^2}.$$

Hence $|f'(x)\delta| \leq |\delta|^2 \implies |f'(x)| \leq |\delta|$, a contradiction. $\square$

Corollary 4.2. Let $(K, |\cdot|)$ be a complete discretely valued field, let $f(x) \in \mathcal{O}_K[x]$ and let $\overline{c} \in k = \mathcal{O}_K/\mathfrak{m}$ be a simple root of $\overline{f}(x) = f(x) \pmod{\mathfrak{m}} \in k[x]$. Then there exists a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and $x \equiv \overline{c} \pmod{\mathfrak{m}}$.

Proof. Apply Hensel's lemma to a lift $c \in \mathcal{O}_K$ of $\bar{c}$. Then $|f(c)| < 1 = |f'(c)|^2$ since $f'(c)$ is a simple root. $\square$

Example 4.1. Consider $f(x) = x^2 - 2$, which has a simple root mod 7. Thus $\sqrt{2} \in \mathbb{Z}_p \subset \mathbb{Q}_7$.

Corollary 4.3. $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 \text{ if } p > 2. \\ (\mathbb{Z}/2\mathbb{Z})^3 \text{ if } p = 2. \end{cases}$

Proof. First consider $p > 2$. Let $b \in \mathbb{Z}_p^\times$. Applying the previous corollary to $f(x) = x^2 - b$, we find that $b \in (\mathbb{Z}_p^\times)^2$ if and only if $b \in (\mathbb{F}_p^\times)^2$. Thus $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ has kernel $(\mathbb{Z}_p^\times)^2$, so induces an isomorphism $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \to \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})$ (since $\mathbb{F}_p^\times = \mathbb{Z}/(p-1)\mathbb{Z}$).

We have an isomorphism $\mathbb{Z}_p^\times \times \mathbb{Z} \to \mathbb{Q}_p^\times$ given by $(u, n) \mapsto up^n$. Then $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^2$.

If $p = 2$, let $b \in \mathbb{Z}_2^\times$. Consider $f(x) = x^2 - b$, so $f'(x) = 2x \equiv 0 \pmod 2$. Instead now let $b \equiv 1 \pmod 8$. Then $|f(1)|_2 \leq 2^{-3} < 2^{-2} = |f'(1)|_2^2$. Hensel's lemma now implies that $b \in (\mathbb{Z}_2^\times)^2 \iff b \equiv 1 \pmod 8$. Thus $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \cong (\mathbb{Z}/8\mathbb{Z})^\times = (\mathbb{Z}/2\mathbb{Z})^2$. Again using $\mathbb{Q}_2^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}$, we obtain that $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$. $\square$

Remark. The proof of Hensel's lemma uses the iteration $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$. We can think of the proof as the non–archimedean analogue of the Newton-Raphson method.

Theorem 4.4 (Hensel's lemma, version 2)**.** Let $(K, |\cdot|)$ be a complete discretely valued field and $f(x) \in \mathcal{O}_K[x]$. Suppose $\overline{f}(x) = f(x) \pmod{\mathfrak{m}} \in k[x]$ factorizes as $\overline{f}(x) = \overline{g}(x)\overline{h}(x) \in k[x]$ with $\overline{g}(x), \overline{h}(x)$ coprime. Then there is a factorization $f(x) = g(x)h(x)$ in $\mathcal{O}_K[x]$ with $\overline{g}(x) \equiv g(x) \pmod{\mathfrak{m}}$, $\overline{f}(x) \equiv f(x) \pmod{\mathfrak{m}}$ and $\deg(\overline{g}) = \deg(g)$.

Proof. Left as an exercise on example sheet 1. $\square$