

# Local Fields

Lectured by Dr Rong Zhou  
Typed by David Kurniadi Angdinata

Michaelmas 2020

**Syllabus**

## Contents

<b>1</b>	<b>Basic theory</b>	<b>3</b>
1.1	Absolute values . . . . .	3
1.2	Valuation rings . . . . .	5
1.3	The $p$ -adic numbers . . . . .	8
<b>2</b>	<b>Complete valued fields</b>	<b>10</b>
2.1	Hensel's lemma . . . . .	10
2.2	Teichmüller lifts . . . . .	11
2.3	Extensions of complete valued fields . . . . .	13
<b>3</b>	<b>Local fields</b>	<b>16</b>
3.1	Local fields . . . . .	16

# 1 Basic theory

Lecture 1  
Friday  
09/10/20

How can we find solutions to Diophantine equations? Let  $f(x_1, \dots, x_r) \in \mathbb{Z}[x_1, \dots, x_r]$  be a polynomial with integer coefficients. What are integer or rational solutions to  $f(x_1, \dots, x_r) = 0$ ? Finding solutions to Diophantine equations in general is a very difficult problem. Consider a related but much simpler problem of solving the congruences

$$f(x_1, \dots, x_r) \equiv 0 \pmod{p}, \quad \dots, \quad f(x_1, \dots, x_r) \equiv 0 \pmod{p^n}, \quad \dots$$

Now this is just a finite computation, since modulo primes there are only finitely many choices for solutions, so this is a much easier problem. Local fields give a way to package all this information together.

## 1.1 Absolute values

**Definition 1.1.1.** Let  $K$  be a field. An **absolute value** on  $K$  is a function  $|\cdot| : K \rightarrow \mathbb{R}_{\geq 0}$  such that,

1.  $|x| = 0$  if and only if  $x = 0$ ,
2.  $|xy| = |x||y|$  for all  $x, y \in K$ , and
3. the triangle inequality  $|x + y| \leq |x| + |y|$  for all  $x, y \in K$ .

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

**Example.**

- Let  $K = \mathbb{R}, \mathbb{C}$  with the usual absolute value. Write  $|\cdot|_{\infty}$  for this absolute value.
- Let  $K$  be any field. The **trivial absolute value** on  $K$  is defined by

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

Ignore this case in this course.

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

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

Axiom 1 is clear. Write  $y = p^m (c/d)$ . Axiom 2 is

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

Without loss of generality  $m \geq n$ . Axiom 3 is

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

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

**Exercise.**  $+$  and  $\cdot$  are continuous.

**Definition 1.1.2.** Let  $|\cdot|$  and  $|\cdot|'$  be absolute values on a field  $K$ . We say  $|\cdot|$  and  $|\cdot|'$  are **equivalent** if they induce the same topology. An equivalence class of absolute values is called a **place**.

**Proposition 1.1.3.** *Let  $|\cdot|$  and  $|\cdot|'$  be non-trivial absolute values on  $K$ . The following are equivalent.*

1.  $|\cdot|$  and  $|\cdot|'$  are equivalent.
2.  $|x| < 1$  if and only if  $|x|' < 1$  for all  $x \in K$ .
3. There exists  $c \in \mathbb{R}_{>0}$  such that  $|x|^c = |x|'$  for all  $x \in K$ .

*Proof.*

- 1  $\implies$  2.  $|x| < 1$  if and only if  $x^n \rightarrow 0$  with respect to  $|\cdot|$ , if and only if  $x^n \rightarrow 0$  with respect to  $|\cdot|'$ , if and only if  $|x|' < 1$ .
- 2  $\implies$  3. Let  $a \in K^\times$  such that  $|a| < 1$ , which exists since  $|\cdot|$  is non-trivial. We need to show that

$$\frac{\log|x|}{\log|a|} = \frac{\log|x|'}{\log|a|'}, \quad x \in K^\times.$$

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

$$\frac{\log|x|}{\log|a|} < \frac{m}{n} < \frac{\log|x|'}{\log|a|'}.$$

Then we have  $n \log|x| < m \log|a|$  and  $n \log|x|' > m \log|a|'$ , so  $|x^n/a^m| < 1$  and  $|x^n/a^m|' > 1$ , a contradiction. Similarly for  $\log|x| / \log|a| > \log|x|' / \log|a|'$ .

- 3  $\implies$  1. Clear. □

This course is mainly interested in the following types of absolute values.

**Definition 1.1.4.** 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**.

**Example.**

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

**Lemma 1.1.5** (All triangles are isosceles). *Let  $(K, |\cdot|)$  be a non-archimedean valued field and  $x, y \in K$ . If  $|x| < |y|$ , then  $|x - y| = |y|$ .*

**Fact.**

- $|1| = |-1| = 1$ .
- $|-y| = |y|$ .

*Proof.*  $|x - y| \leq \max(|x|, |y|) = |y|$ , and  $|y| \leq \max(|x|, |x - y|)$ , so  $|y| \leq |x - y|$ . □

Convergence is easier for non-archimedean  $|\cdot|$ .

**Proposition 1.1.6.** *Let  $(K, |\cdot|)$  be non-archimedean and  $(x_n)_{n=1}^\infty$  a sequence in  $K$ . If  $|x_n - x_{n+1}| \rightarrow 0$ , 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  $|x_n - x_{n+1}| < \epsilon$  for all  $n > N$ . Then for  $N < n < m$ ,

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

so  $(x_n)_{n=1}^\infty$  is Cauchy. □

**Example.** Let  $p = 5$ . Construct a sequence  $(x_n)_{n=1}^{\infty}$  such that

1.  $x_n^2 + 1 \equiv 0 \pmod{5^n}$ , and
2.  $x_n \equiv x_{n+1} \pmod{5^n}$ ,

as follows. Take  $x_1 = 2$ . Suppose have constructed  $x_n$ . Let  $x_n^2 + 1 = a5^n$  and set  $x_{n+1} = x_n + b5^n$ . Then

$$x_{n+1}^2 + 1 = x_n^2 + 2bx_n5^n + b^25^{2n} + 1 = a5^n + 2x_nb5^n + b^25^{2n} \equiv (a + 2x_nb)5^n \pmod{5^{n+1}}.$$

We choose  $b$  such that  $a + 2x_nb \equiv 0 \pmod{5}$ . Then we have  $x_{n+1}^2 + 1 \equiv 0 \pmod{5^{n+1}}$  as desired. By 2,  $(x_n)_{n=1}^{\infty}$  is Cauchy. Suppose  $x_n \rightarrow L \in \mathbb{Q}$ . Then  $x_n^2 \rightarrow L^2$ . But by 1,  $x_n^2 \rightarrow -1$ , so  $L^2 = -1$ , a contradiction. Thus  $(\mathbb{Q}, |\cdot|_5)$  is not complete.

**Definition 1.1.7.** The  $p$ -**adic numbers**  $\mathbb{Q}_p$  is the completion of  $\mathbb{Q}$  with respect to  $|\cdot|_p$ .

**Remark.** By analogy,  $\mathbb{R}$  is the completion of  $\mathbb{Q}$  with respect to  $|\cdot|_{\infty}$ .

Let  $K$  be a non-archimedean valued field. For  $x \in K$  and  $r \in \mathbb{R}_{>0}$ , define

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

**Lemma 1.1.8.** Let  $(K, |\cdot|)$  be non-archimedean.

1. If  $z \in B(x, r)$ , then  $B(z, r) = B(x, r)$ , so open balls do not have centres.
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  $|x - y| < r$ , so  $|z - y| = |(z - x) + (x - y)| \leq \max(|z - x|, |x - y|) < r$ . Thus  $B(x, r) \subseteq B(z, r)$ . The reverse inclusion follows by symmetry.
2. Same as 1.
3. Let  $y \notin B(x, r)$ . If  $z \in B(x, r) \cap B(y, r)$ , then  $B(x, r) = B(z, r) = B(y, r)$ , so  $y \in B(x, r)$ , a contradiction. Thus  $B(x, r) \cap B(y, r) = \emptyset$ .
4. If  $z \in \overline{B}(x, r)$ , then  $B(z, r) \subseteq \overline{B}(z, r) = \overline{B}(x, r)$ , by 2.

□

## 1.2 Valuation rings

**Definition 1.2.1.** Let  $K$  be a field. A **valuation** on  $K$  is a function  $v : K^{\times} \rightarrow \mathbb{R}$  such that

- $v(xy) = v(x) + v(y)$ , and
- $v(x + y) \geq \min(v(x), v(y))$ .

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  $v(x) = \log_{\alpha}|x|$ .

**Remark.**

- We ignore the trivial valuation  $v(x) = 0$  for all  $x \in K^{\times}$ , which corresponds to the trivial absolute value.
- Say  $v_1$  and  $v_2$  are **equivalent** if there exists  $c \in \mathbb{R}_{>0}$  such that  $v_1(x) = cv_2(x)$  for all  $x \in K^{\times}$ .

**Example.**

- Let  $K = \mathbb{Q}$ . Then  $v_p(x) = -\log_p |x|_p$  is the  **$p$ -adic valuation**.
- Let  $k$  be a field, and let  $K = k(t) = \text{Frac } k[t]$  be the **rational function field**. Then

$$v\left(t^n \frac{f(t)}{g(t)}\right) = n, \quad f, g \in k[t], \quad f(0), g(0) \neq 0$$

is the  **$t$ -adic valuation**.

- Let  $K = k((t)) = \text{Frac } k[[t]] = \{\sum_{i=n}^{\infty} a_i t^i \mid a_i \in k, n \in \mathbb{Z}\}$  be the **field of formal Laurent series** over  $k$ . Then

$$v\left(\sum_i a_i t^i\right) = \min\{i \mid a_i \neq 0\}$$

is the  $t$ -adic valuation on  $K$ .

**Definition 1.2.2.** Let  $(K, |\cdot|)$  be a non-archimedean valued field. The **valuation ring** of  $K$  is defined to be

$$\mathcal{O}_K = \overline{B}(0, 1) = \{x \in K \mid |x| \leq 1\} = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}.$$

**Proposition 1.2.3.**

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

*Proof.*

1. By last lecture,  $|1| = 1$ , so  $1 \in \mathcal{O}_K$ . Since  $|0| = 0$ ,  $0 \in \mathcal{O}_K$ . Since  $|-1| = 1$ ,  $|-x| = |x|$ . Thus if  $x \in \mathcal{O}_K$ , then  $-x \in \mathcal{O}_K$ . 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 ring. Since  $\mathcal{O}_K = \overline{B}(0, 1)$  it is open.
2. Similar to 1.
3. Note that  $|x||x^{-1}| = |xx^{-1}| = 1$ . Thus  $|x| = 1$  if and only if  $|x^{-1}| = 1$ , if and only if  $x, x^{-1} \in \mathcal{O}_K$ , if and only if  $x \in \mathcal{O}_K^\times$ .

□

**Notation.**

- $\mathfrak{m} = \{x \in \mathcal{O}_K \mid |x| < 1\}$  is a maximal ideal of  $\mathcal{O}_K$ .
- $k = \mathcal{O}_K/\mathfrak{m}$  is the **residue field**.

A ring is **local** if it has a unique maximal ideal.

**Exercise.**  $R$  is local if and only if  $R \setminus R^\times$  is an ideal.

**Corollary 1.2.4.**  $\mathcal{O}_K$  is a local ring with unique maximal ideal  $\mathfrak{m}$ .

**Example.**

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

**Definition 1.2.5.** Let  $v : K^\times \rightarrow \mathbb{R}$  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 **uniformiser** if  $v(\pi) > 0$  and  $v(\pi)$  generates  $v(K^\times)$ .

**Example.**

- $K = \mathbb{Q}$  with the  $p$ -adic valuation.
- $K = k(t)$  with the  $t$ -adic valuation.

**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 **normalised valuations**. Then  $v(\pi) = 1$  for  $\pi$  a uniformiser.

**Lemma 1.2.6.** *Let  $v$  be a valuation on  $K$ . The following are equivalent.*

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

*Proof.*

- 1  $\implies$  2. Let  $I \subseteq \mathcal{O}_K$  be a non-zero ideal. Let  $x \in I$  such that  $v(x) = \min \{v(a) \mid a \in I\}$  which exists since  $v$  is discrete. Then  $x\mathcal{O}_K = \{a \in \mathcal{O}_K \mid v(a) \geq v(x)\} \subseteq I$ , and hence  $x\mathcal{O}_K = I$  by definition of  $x$ .
- 2  $\implies$  3. Clear.
- 3  $\implies$  4. Write  $\mathfrak{m} = \mathcal{O}_K x_1 + \cdots + \mathcal{O}_K x_n$ . Without loss of generality  $v(x_1) \leq \cdots \leq v(x_n)$ . Then  $\mathfrak{m} = \mathcal{O}_K x_1$ .
- 4  $\implies$  1. Let  $\mathfrak{m} = \mathcal{O}_K \pi$  for some  $\pi \in \mathcal{O}_K$  and let  $c = v(\pi)$ . Then if  $v(x) > 0$ ,  $x \in \mathfrak{m}$  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 1.2.7.** *Let  $v$  be a discrete valuation on  $K$  and  $\pi \in \mathcal{O}_K$  a uniformiser. For all  $x \in K^\times$ , there exist  $n \in \mathbb{Z}$  and  $u \in \mathcal{O}_K^\times$  such that  $x = \pi^n u$ . In particular  $K = \mathcal{O}_K[1/\pi]$  for any  $x \in \mathfrak{m}$  and hence  $K = \text{Frac } \mathcal{O}_K$ .*

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

**Definition 1.2.8.** A ring  $R$  is called a **discrete valuation ring (DVR)** if it is a PID with exactly one non-zero prime ideal, necessarily maximal.

**Lemma 1.2.9.**

1. Let  $v$  be a discrete valuation on  $K$ . Then  $\mathcal{O}_K$  is a DVR.
2. Let  $R$  be a DVR. Then there exists a valuation  $v$  on  $K = \text{Frac } R$  such that  $R = \mathcal{O}_K$ .

*Proof.*

1.  $\mathcal{O}_K$  is a PID by Lemma 1.2.6. Let  $0 \neq I \subseteq \mathcal{O}_K$  be an ideal, then  $I = \langle x \rangle$ . If  $x = \pi^n u$  for  $\pi$  a uniformiser, then  $\langle x \rangle$  is prime if and only if  $n = 1$  and  $I = \langle \pi \rangle = \mathfrak{m}$ .
2. Let  $R$  be a DVR with maximal ideal  $\mathfrak{m}$ . Then  $\mathfrak{m} = \langle \pi \rangle$  for some  $\pi \in R$ . By unique factorisation of PIDs, we may write any  $x \in R \setminus \{0\}$  uniquely as  $\pi^n u$  for  $n \geq 0$  and  $u \in R^\times$ . Then any  $y \in K \setminus \{0\}$  can be written uniquely as  $\pi^m u$  for  $u \in R^\times$  and  $m \in \mathbb{Z}$ . Define  $v(\pi^m u) = m$ . It is easy to check  $v$  is a valuation and  $\mathcal{O}_K = R$ .

□

**Example.**

- $\mathbb{Z}_{(p)}$  is a DVR, the valuation ring of  $|\cdot|_p$  on  $\mathbb{Q}$ .
- The ring of formal power series  $k[[t]] = \left\{ \sum_{n \geq 0} a_n t^n \mid a_n \in k \right\}$  is a DVR, the valuation ring for the  $t$ -adic absolute value on  $k((t))$ .
- Non-example. Let  $K = k(t)$  be the rational function field, and let  $K' = K(t^{1/2}, t^{1/4}, \dots)$ . Then the  $t$ -adic valuation extends to  $K'$ , and  $v(t^{1/2^n}) = 1/2^n$  is not discrete.

### 1.3 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  $|\cdot|_p$ . By example sheet 1,  $\mathbb{Q}_p$  is a field,  $|\cdot|_p$  extends to  $\mathbb{Q}_p$ , and the associated valuation is discrete, so  $\mathbb{Q}_p$  is a discretely valued field.

Lecture 3  
Wednesday  
14/10/20

**Definition 1.3.1.** The ring of  $p$ -adic integers  $\mathbb{Z}_p$  is the valuation ring

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

**Fact.**

- $\mathbb{Z}_p$  is a DVR with maximal ideal  $p\mathbb{Z}_p$ .
- The non-zero ideals in  $\mathbb{Z}_p$  are  $p^n\mathbb{Z}_p$  for  $n \in \mathbb{N}$ .

**Proposition 1.3.2.**  $\mathbb{Z}_p$  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.* Need to show  $\mathbb{Z}$  is dense in  $\mathbb{Z}_p$ . Since  $\mathbb{Q}$  is dense in  $\mathbb{Q}_p$  and  $\mathbb{Z}_p \subseteq \mathbb{Q}_p$  is open,  $\mathbb{Z}_p \cap \mathbb{Q}$  is dense in  $\mathbb{Z}_p$ . Then

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

the localisation at  $\langle p \rangle$ . Thus it suffices to show  $\mathbb{Z}$  is dense in  $\mathbb{Z}_{(p)}$ . Let  $a/b \in \mathbb{Z}_{(p)}$  for  $a, b \in \mathbb{Z}$  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  $y_n \rightarrow a/b$  as  $n \rightarrow \infty$ . In particular,  $\mathbb{Z}$  is dense in  $\mathbb{Z}_p$ , which is complete.  $\square$

Let  $(A_n)_{n=1}^\infty$  be a sequence of sets or groups or rings together with homomorphisms  $\phi_n : A_{n+1} \rightarrow A_n$ , the **transition maps**. The **inverse limit** of  $(A_n)_{n=1}^\infty$  is the set or group or ring

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

so

$$\begin{array}{ccccc} A_{n+1} & \xrightarrow{\phi_n} & A_n & \xrightarrow{\phi_{n-1}} & A_{n-1} \\ a_{n+1} & \mapsto & a_n & \mapsto & a_{n-1} \end{array}.$$

**Fact.** If  $A_n$  is a group or ring, then  $\varprojlim_n A_n$  is a group or ring.

Let  $\theta_m : \varprojlim_n A_n \rightarrow A_m$  denote the natural projection. The inverse limit satisfies the following universal property.

**Proposition 1.3.3.** Let  $((A_n)_{n=1}^\infty, (\phi_n)_{n=1}^\infty)$  as above. Then for any set or group or ring  $B$  together with homomorphisms  $\psi_n : B \rightarrow A_n$  such that

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

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

*Proof.* Define

$$\begin{array}{ccc} \psi & : & B \longrightarrow \prod_{n=1}^\infty A_n \\ b & \longmapsto & \prod_{n=1}^\infty \psi_n(b) \end{array}.$$

Then  $\psi_n = \phi_n \circ \psi_{n+1}$  implies that  $\psi(b) \in \varprojlim_n A_n$ . The map is clearly unique, determined by  $\psi_n = \phi_n \circ \psi_{n+1}$ , and is a homomorphism of rings.  $\square$



**Definition 1.3.4.** 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  $\phi_n : R/I^{n+1} \rightarrow R/I^n$  is the natural projection. Note there is a natural map  $\iota : R \rightarrow \widehat{R}$  by the universal property. We say that  $R$  is  $I$ -adically complete if  $\iota$  is an isomorphism.

**Fact.**  $\ker(\iota : R \rightarrow \widehat{R}) = \bigcap_{n=1}^{\infty} I^n$ .

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

**Proposition 1.3.5.** Assume  $K$  is complete.

1. Then  $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n \mathcal{O}_K$ , so  $\mathcal{O}_K$  is  $\pi$ -adically complete.
2. If in addition  $K$  is discretely valued and  $\pi$  is a uniformiser, then every  $x \in \mathcal{O}_K$  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  $k = \mathcal{O}_K/\pi \mathcal{O}_K$ . Moreover, any series  $\sum_{i=0}^{\infty} a_i \pi^i$  converges to an element in  $\mathcal{O}_K$ .

*Proof.*

1. Let  $\iota : \mathcal{O}_K \rightarrow \varprojlim_n \mathcal{O}_K/\pi^n \mathcal{O}_K$ . Since  $\bigcap_{n=1}^{\infty} \pi^n \mathcal{O}_K = \{0\}$ ,  $\iota$  is injective. 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  $v(y_n - y_{n+1}) \geq n$ , since  $y_n - y_{n+1} \in \pi^n \mathcal{O}_K$ , so  $(y_n)_{n=1}^{\infty}$  is a Cauchy sequence in  $\mathcal{O}_K$ . But  $\mathcal{O}_K$  is complete, since  $\mathcal{O}_K \subseteq K$  is closed, so  $y_n \rightarrow y$ , and  $y$  maps to  $(x_n)_{n=1}^{\infty}$ . Thus  $\iota$  is surjective.
2. Let  $x \in \mathcal{O}_K$ . Choose  $a_i$  inductively. Choose  $a_0 \in A$  such that  $a_0 \equiv x \pmod{\pi}$ . Suppose have chosen  $a_0, \dots, a_k$  such that  $\sum_{i=0}^k a_i \pi^i \equiv x \pmod{\pi^{k+1}}$ . Then  $\sum_{i=0}^k a_i \pi^i - x = c\pi^{k+1}$  for  $c \in \mathcal{O}_K$ . Choose  $a_{k+1} \equiv -c \pmod{\pi}$ . Then  $\sum_{i=0}^{k+1} a_i \pi^i \equiv x \pmod{\pi^{k+2}}$ , so  $\sum_{i=0}^{\infty} a_i \pi^i = x$ . For uniqueness, assume  $\sum_{i=0}^{\infty} a_i \pi^i = \sum_{i=0}^{\infty} b_i \pi^i \in \mathcal{O}_K$ . Then let  $n$  be minimal such that  $a_n \neq b_n$ . Then  $\sum_{i=0}^{\infty} a_i \pi^i \not\equiv \sum_{i=0}^{\infty} b_i \pi^i \pmod{\pi^{n+1}}$ , a contradiction. □

A warning is if  $(K, |\cdot|)$  is not discretely valued,  $\mathcal{O}_K$  is not necessarily  $\mathfrak{m}$ -adically complete.

**Corollary 1.3.6.** If  $K$  is as in Proposition 1.3.5.2, then every  $x \in K$  can be written uniquely as  $\sum_{i=n}^{\infty} a_i \pi^i$  for  $a_i \in A$ . Conversely any such expression defines an element of  $K$ .

*Proof.* Use  $K = \mathcal{O}_K[1/\pi]$ . □

**Corollary 1.3.7.**

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  $\sum_{i=n}^{\infty} a_i p^i$  for  $a_i \in \{0, \dots, p-1\}$ .

*Proof.*

1. By Proposition 1.3.5, it suffices to show that  $\mathbb{Z}_p/p^n \mathbb{Z}_p \cong \mathbb{Z}/p^n \mathbb{Z}$ . Let  $f_n : \mathbb{Z} \rightarrow \mathbb{Z}_p/p^n \mathbb{Z}_p$  be the natural map. We have  $\ker f_n = \{x \in \mathbb{Z} \mid |x|_p \leq p^{-n}\} = p^n \mathbb{Z}$ , so  $\mathbb{Z}/p^n \mathbb{Z} \rightarrow \mathbb{Z}_p/p^n \mathbb{Z}_p$  is injective. 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  $\mathbb{Z}_p$ , can choose  $x \in \mathbb{Z}$  such that  $x \in c + p^n \mathbb{Z}_p$ , which is open in  $\mathbb{Z}_p$ , so  $f_n(x) = \bar{c}$ . Thus  $\mathbb{Z}/p^n \mathbb{Z} \rightarrow \mathbb{Z}_p/p^n \mathbb{Z}_p$  is surjective.
2. Follows from Corollary 1.3.6 noting that  $\mathbb{Z}_p/p \mathbb{Z}_p \cong \mathbb{F}_p$ . □

**Example.**

- $1/(1-p) = 1 + p + \dots \in \mathbb{Q}_p$ .
- Let  $K = k((t))$  with the  $t$ -adic valuation. Then  $\mathcal{O}_K = k[[t]] = \varprojlim_n k[[t]]/\langle t^n \rangle$ . Moreover  $\mathcal{O}_K$  is the  $t$ -adic completion of  $k[t]$ .

## 2 Complete valued fields

### 2.1 Hensel's lemma

Lecture 4  
Friday  
16/10/20

For complete valued fields, there is a nice way to produce solutions in  $\mathcal{O}_K$  to certain equations from solutions modulo  $\mathfrak{m}$ .

**Theorem 2.1.1** (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  $|f(a)| < |f'(a)|^2$ , where  $f'(a)$  is the **formal derivative** such that if  $f(X) = X^n$  then  $f'(X) = nX^{n-1}$ . 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 uniformiser and let  $r = v(f'(a))$ . We construct a sequence  $(x_n)_{n=1}^\infty$  in  $\mathcal{O}_K$  such that

1.  $f(x_n) \equiv 0 \pmod{\pi^{n+2r}}$ , and
2.  $x_{n+1} \equiv x_n \pmod{\pi^{n+r}}$ .

Take  $x_1 = a$ , then  $f(x_1) \equiv 0 \pmod{\pi^{1+2r}}$ . Suppose we have constructed  $x_1, \dots, x_n$  satisfying 1 and 2. Define

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

2. Since  $x_n \equiv x_1 \pmod{\pi^{1+r}}$ ,  $v(f'(x_n)) = r$  and hence  $f(x_n)/f'(x_n) \equiv 0 \pmod{\pi^{n+r}}$  by 1. It follows that  $x_{n+1} \equiv x_n \pmod{\pi^{n+r}}$  so 2 holds.
1. Note that for  $X$  and  $Y$  indeterminates,

$$f(X+Y) = f_0(X) + f_1(X)Y + \dots, \quad f_i(X) \in \mathcal{O}_K[X], \quad f_0(X) = f(X), \quad f_1(X) = f'(X).$$

Thus

$$f(x_{n+1}) = f(x_n) + f'(x_n)c + \dots, \quad c = -\frac{f(x_n)}{f'(x_n)}.$$

Since  $c \equiv 0 \pmod{\pi^{n+r}}$  and  $v(f'(x_n)) \geq 0$ , we have  $f(x_{n+1}) \equiv f(x_n) + f'(x_n)c \equiv 0 \pmod{\pi^{n+2r+1}}$ , so 1 holds.

This gives the construction of  $(x_n)_{n=1}^\infty$ .

- By property 2,  $(x_n)_{n=1}^\infty$  is Cauchy, so let  $x \in \mathcal{O}_K$  such that  $x_n \rightarrow x$ . Then  $f(x) = \lim_{n \rightarrow \infty} f(x_n) = 0$  by 1. Moreover 2 implies  $a = x_1 \equiv x_n \pmod{\pi^{1+r}}$  for all  $n$ , so  $a \equiv x \pmod{\pi^{1+r}}$ , so  $|x - a| < |f'(a)|$ . This proves existence.
- For uniqueness, suppose  $x'$  also satisfies  $f(x') = 0$  and  $|x' - a| < |f'(a)|$ . Set  $\delta = x' - x \neq 0$ . Then  $|x' - a| < |f'(a)|$ ,  $|x - a| < |f'(a)|$ , and the ultrametric inequality implies  $|\delta| = |x - x'| < |f'(a)| = |f'(x)|$ . But

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

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

**Corollary 2.1.2.** *Let  $(K, |\cdot|)$  be a complete discretely valued field. Let  $f(X) \in \mathcal{O}_K[X]$  and  $\bar{c} \in k = \mathcal{O}_K/\mathfrak{m}$  a simple root of  $\bar{f}(X) = f(X) \pmod{\mathfrak{m}} \in k[X]$ . Then there exists a unique  $x \in \mathcal{O}_K$  such that  $f(x) = 0$  and  $x \equiv \bar{c} \pmod{\mathfrak{m}}$ .*

*Proof.* Apply Theorem 2.1.1 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 modulo seven. Thus  $\sqrt{2} \in \mathbb{Z}_7 \subseteq \mathbb{Q}_7$ .

**Corollary 2.1.3.**

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

*Proof.*

$p > 2$ . Let  $b \in \mathbb{Z}_p^\times$ . Applying Corollary 2.1.2 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  $\mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$  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  $(u, n) \mapsto up^n$ . 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  $f'(X) = 2X \equiv 0 \pmod{2}$ . Let  $b \equiv 1 \pmod{8}$ . Then  $|f(1)|_2 \leq 2^{-3} < |f'(1)|_2^2 = 2^{-2}$ . By Hensel's lemma,  $f(X)$  has a root in  $\mathbb{Z}_2$ , so  $b \in (\mathbb{Z}_2^\times)^2$  if and only if  $b \equiv 1 \pmod{8}$ . Thus  $\mathbb{Z}_2^\times / (\mathbb{Z}_2^\times)^2 \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2$ . Again using  $\mathbb{Q}_2^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}$ , we find that  $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$ . □

**Remark.** The proof of Hensel's lemma uses the iteration  $x_{n+1} = x_n - f(x_n)/f'(x_n)$ , the non-archimedean analogue of the Newton-Raphson method.

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

**Theorem 2.1.4** (Hensel's lemma version 2). *Let  $(K, |\cdot|)$  be a complete discretely valued field and  $f(X) \in \mathcal{O}_K[X]$ . Suppose  $\bar{f}(X) = f(X) \pmod{\mathfrak{m}} \in k[X]$  factorises as  $\bar{f}(X) = \bar{g}(X)\bar{h}(X)$  in  $k[X]$ , with  $\bar{g}(X)$  and  $\bar{h}(X)$  coprime. Then there is a factorisation  $f(X) = g(X)h(X)$  in  $\mathcal{O}_K[X]$ , with  $\bar{g}(X) = g(X) \pmod{\mathfrak{m}}$ ,  $\bar{h}(X) = h(X) \pmod{\mathfrak{m}}$ , and  $\deg \bar{g} = \deg g$ .*

*Proof.* Example sheet 1. □

**Corollary 2.1.5.** *Let  $f(X) = a_n X^n + \cdots + a_0 \in K[X]$  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  $\max(|a_0|, |a_n|) = 1$ . If not, let  $r$  be minimal such that  $|a_r| = 1$ , then  $0 < r < n$ . Thus we have  $\bar{f}(X) = X^r(a_r + \cdots + a_n X^{n-r}) \pmod{\mathfrak{m}}$ . Then Theorem 2.1.4 implies  $f(X) = g(X)h(X)$  and  $0 < \deg g < n$ . □

## 2.2 Teichmüller lifts

Recall that in lecture 3 every element of  $x \in \mathbb{Q}_p$  can be written as  $x = \sum_{i=n}^{\infty} a_i p^i$  for  $a_i \in A = \{0, \dots, p-1\}$ , but  $\mathbb{F}_p \rightarrow A \subseteq \mathbb{Z}_p$  does not respect any algebraic structure. It turns out there is a natural choice of coset representatives in many cases which does respect some algebraic structure.

Lecture 5  
Monday  
19/10/20

**Definition 2.2.1.** A ring  $R$  of characteristic  $p$  is a **perfect ring** if the Frobenius  $x \mapsto x^p$  is an automorphism of  $R$ . A field of characteristic  $p$  is a **perfect field** if it is perfect as a ring.

**Remark.** Since  $\text{ch } R = p$ ,  $(x+y)^p = x^p + y^p$ , so Frobenius is a ring homomorphism.

**Example.**

- $\mathbb{F}_{p^n}$  and  $\overline{\mathbb{F}_p}$  are perfect fields.
- $\mathbb{F}_p[t]$  is not perfect, since  $t$  is not in the image of Frobenius.
- $\mathbb{F}_p(t^{1/p^\infty}) = \mathbb{F}_p(t, t^{1/p}, \dots)$  is a perfect field, 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 a **perfectoid field**.

**Fact.** A field  $k$  is perfect if and only if any finite extension of  $k$  is separable.

**Theorem 2.2.2.** *Let  $(K, |\cdot|)$  be a complete discretely valued field such that  $k = \mathcal{O}_K/\mathfrak{m}$  is a perfect field of characteristic  $p$ . Then there exists a unique map  $[\cdot] : k \rightarrow \mathcal{O}_K$  such that*

1.  $a \equiv [a] \pmod{\mathfrak{m}}$  for all  $a \in k$ , and
2.  $[ab] \equiv [a][b] \pmod{\mathfrak{m}}$  for all  $a, b \in k$ .

Moreover if  $\text{ch } \mathcal{O}_K = p$ ,  $[\cdot]$  is a ring homomorphism.

**Definition 2.2.3.** The element  $[a] \in \mathcal{O}_K$  constructed in Theorem 2.2.2 is called the **Teichmüller lift** of  $a$ .

The following is the idea of the proof. Let  $\alpha \in \mathcal{O}_K$  be any lift of  $a \in k$ . Then  $\alpha$  is well-defined up to  $\pi \mathcal{O}_K$ . Let  $\beta \in \mathcal{O}_K$  be a lift of  $a^{1/p}$ . We claim that  $\beta$  is a better lift. Why? Let  $\beta' \in \mathcal{O}_K$  be another lift of  $a^{1/p}$ , then  $\beta = \beta' + \pi u$  for  $u \in \mathcal{O}_K$ , so

$$\beta^p = (\beta' + \pi u)^p = \beta'^p + \underbrace{\sum_{i=1}^p \binom{p}{i} \beta'^{p-i} (\pi u)^i}_{\in \pi^2 \mathcal{O}_K},$$

by using  $p \in \langle \pi \rangle$ , so  $\beta^p$  is well-defined up to  $\pi^2 \mathcal{O}_K$ . Repeat this process to get better and better lifts.

**Lemma 2.2.4.** *Let  $(K, |\cdot|)$  be as in Theorem 2.2.2, and fix  $\pi \in \mathcal{O}_K$  a uniformiser. Let  $x, y \in \mathcal{O}_K$  such that  $x \equiv y \pmod{\pi^k}$  for  $k \geq 1$ . Then  $x^p \equiv y^p \pmod{\pi^{k+1}}$ .*

*Proof.* Let  $x = y + u\pi^k$  for  $u \in \mathcal{O}_K$ . Then

$$x^p = \sum_{i=0}^p \binom{p}{i} (u\pi^k)^i y^{p-i} = y^p + pu\pi^k y^{p-1} + \sum_{i=2}^p \binom{p}{i} (u\pi^k)^i y^{p-i}.$$

Since  $\mathcal{O}_K/\pi \mathcal{O}_K$  has characteristic  $p$ , we have  $p \in \langle \pi \rangle$ . Thus  $pu\pi^k y^{p-1} \in \pi^{k+1} \mathcal{O}_K$ . For  $i \geq 2$ ,  $(u\pi^k)^i \in \pi^{k+1} \mathcal{O}_K$ , so  $x^p \equiv y^p \pmod{\pi^{k+1}}$ .  $\square$

*Proof of Theorem 2.2.2.* Let  $a \in k$ . For each  $i \geq 0$  we choose a lift  $y_i \in \mathcal{O}_K$  of  $a^{1/p^i}$ , and we define

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

Then  $x_i \equiv y_i^{p^i} \equiv (a^{1/p^i})^{p^i} \equiv a \pmod{\pi}$ . We claim that  $(x_i)_{i=1}^\infty$  is a Cauchy sequence, and its limit  $x_i \rightarrow x$  is independent of the choice of  $y_i$ .

- By construction  $y_i \equiv y_{i+1}^{p^i} \pmod{\pi}$ . By Lemma 2.2.4 and induction on  $k$ , we have  $y_i^{p^k} \equiv y_{i+1}^{p^{k+1}} \pmod{\pi^{k+1}}$ , and hence  $x_i \equiv x_{i+1} \pmod{\pi^{i+1}}$ , by taking  $k = i$ , so  $|x_i - x_{i+1}| \rightarrow 0$ . Then  $(x_i)_{i=1}^\infty$  is Cauchy, so  $x_i \rightarrow x \in \mathcal{O}_K$ .
- Suppose  $(x'_i)_{i=1}^\infty$  arises from another choice of  $y'_i$  lifting  $a^{1/p^i}$ . Then  $x'_i$  is Cauchy, and  $x'_i \rightarrow x' \in \mathcal{O}_K$ . Let

$$x''_i = \begin{cases} x_i & i \text{ even} \\ x'_i & i \text{ odd} \end{cases}.$$

Then  $x''_i$  arises from lifting

$$y''_i = \begin{cases} y_i & i \text{ even} \\ y'_i & i \text{ odd} \end{cases}.$$

Then  $(x''_i)_{i=1}^\infty$  is Cauchy and  $x''_i \rightarrow x$  and  $x''_i \rightarrow x'$ , so  $x = x'$ , hence  $x$  is independent of  $y_i$ .

We define  $[a] = x$ .

1.  $x \equiv a \pmod{\pi}$ , so 1 is satisfied.
2. We let  $b \in k$  and we choose  $u_i \in \mathcal{O}_K$  a lift of  $b^{1/p^i}$ , and let  $z_i = u_i^{p^i}$ . Then  $\lim_{i \rightarrow \infty} z_i = [b]$ . Now  $u_i y_i$  is a lift of  $(ab)^{1/p^i}$ , hence

$$[ab] = \lim_{i \rightarrow \infty} x_i z_i = \lim_{i \rightarrow \infty} x_i \lim_{i \rightarrow \infty} z_i = [a][b],$$

so 2 is satisfied.

If  $\text{ch } \mathcal{O}_K = p$ ,  $y_i + u_i$  is a lift of  $a^{1/p^i} + b^{1/p^i} = (a + b)^{1/p^i}$ . Then

$$[a + b] = \lim_{i \rightarrow \infty} (y_i + u_i)^{p^i} = \lim_{i \rightarrow \infty} (y_i^{p^i} + u_i^{p^i}) = \lim_{i \rightarrow \infty} (x_i + z_i) = [a] + [b].$$

It is easy to check that  $[0] = 0$  and  $[1] = 1$ , so  $[\cdot]$  is a ring homomorphism. For uniqueness, let  $\phi : k \rightarrow \mathcal{O}_K$  be another such map. Then for  $a \in k$ ,  $\phi(a^{1/p^i})$  is a lift of  $a^{1/p^i}$ , it follows that

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

□

**Example 2.2.5.** Let  $K = \mathbb{Q}_p$ , and let  $[\cdot] : \mathbb{F}_p \rightarrow \mathbb{Z}_p$ . If  $a \in \mathbb{F}_p^\times$ , then  $[a]^{p-1} = [a^{p-1}] = [1] = 1$ , so  $[a]$  is a  $(p-1)$ -th root of unity.

More generally is the following.

**Lemma 2.2.6.** Let  $(K, |\cdot|)$  be a complete discretely valued field. If  $k = \mathcal{O}_K/\mathfrak{m} \subseteq \overline{\mathbb{F}_p}$ ,  $[a] \in \mathcal{O}_K^\times$  is a root of unity.

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

**Theorem 2.2.7.** Let  $(K, |\cdot|)$  be a complete discretely valued field such that  $k$  is perfect with  $\text{ch } k = p > 0$ . Then  $K \cong k((t))$ .

*Proof.* Since  $K = \text{Frac } \mathcal{O}_K$ , it suffices to show  $\mathcal{O}_K \cong k[[t]]$ . Fix  $\pi \in \mathcal{O}_K$  a uniformiser, let  $[\cdot] : k \rightarrow \mathcal{O}_K$  be the Teichmüller map, and define

$$\begin{aligned} \phi : k[[t]] &\longrightarrow \mathcal{O}_K \\ \sum_{i=0}^{\infty} a_i t^i &\longmapsto \sum_{i=0}^{\infty} [a_i] \pi^i. \end{aligned}$$

Then  $\phi$  is a ring homomorphism since  $[\cdot]$  is a ring homomorphism and it is a bijection by Proposition 1.3.5.2. □

### 2.3 Extensions of complete valued fields

**Theorem 2.3.1.** Let  $(K, |\cdot|)$  be a complete non-archimedean discretely valued field and  $L/K$  a finite extension of degree  $n$ .

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

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

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

Recall that if  $L/K$  is finite,

$$\begin{aligned} N_{L/K} : L &\longrightarrow K \\ y &\longmapsto \det_K(\cdot y), \end{aligned}$$

where  $\cdot y : L \rightarrow L$  is the  $K$ -linear map induced by multiplication by  $y$ .

**Fact.**

- $N_{L/K}(xy) = N_{L/K}(x) N_{L/K}(y)$ .
- Let  $X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$  be the minimal polynomial of  $y \in L$ . Then  $N_{L/K}(y) = \pm a_0^m$  for  $m \geq 1$ .

Lecture 6  
Wednesday  
21/10/20

**Definition 2.3.2.** Let  $(K, |\cdot|)$  be a non-archimedean valued field and  $V$  a vector space over  $K$ . A **norm** on  $V$  is a function  $\|\cdot\| : V \rightarrow \mathbb{R}_{\geq 0}$  satisfying

- $\|x\| = 0$  if and only if  $x = 0$ ,
- $\|\lambda x\| = |\lambda| \|x\|$  for all  $\lambda \in K$  and  $x \in V$ , and
- $\|x + y\| \leq \max(\|x\|, \|y\|)$  for all  $x, y \in V$ .

**Example.** If  $V$  is finite dimensional and  $e_1, \dots, e_n$  is a basis of  $V$ , the **sup norm** on  $V$  is defined by

$$\|x\|_{\sup} = \max_i |x_i|, \quad x = \sum_{i=1}^n x_i e_i.$$

**Exercise.**  $\|\cdot\|_{\sup}$  is a norm.

**Definition 2.3.3.** Two norms  $\|\cdot\|_1$  and  $\|\cdot\|_2$  on  $V$  are **equivalent** if there exists  $C, D > 0$  such that

$$C\|x\|_1 \leq \|x\|_2 \leq D\|x\|_1, \quad x \in V.$$

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

**Proposition 2.3.4.** Let  $(K, |\cdot|)$  be complete non-archimedean and  $V$  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  $e_1, \dots, e_n$  a basis for  $V$ . Write  $v_i = \sum_{j=1}^n x_j^i e_j$ . Then  $(x_j^i)_{i=1}^{\infty}$  is a Cauchy sequence in  $K$ . Let  $x_j^i \rightarrow x_j \in K$ , then  $v_i \rightarrow v = \sum_{j=1}^n x_j e_j$ .  $\square$

**Theorem 2.3.5.** Let  $(K, |\cdot|)$  be complete 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 the set of norms, it suffices to show any norm  $\|\cdot\|$  is equivalent to  $\|\cdot\|_{\sup}$ . Let  $e_1, \dots, e_n$  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

$$\|x\| \leq \max_i \|x_i e_i\| = \max_i |x_i| \|e_i\| \leq D \max_i |x_i| = D\|x\|_{\sup}.$$

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

$n = 1$ .  $\|x\| = \|x_1 e_1\| = |x_1| \|e_1\|$  so take  $C = \|e_1\|$ , since  $|x_1| = \|x\|_{\sup}$ .

$n > 1$ . Set  $V_i = \langle e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n \rangle$ . By induction,  $V_i$  is complete with respect to  $\|\cdot\|$ , hence closed.

Then  $e_i + V_i$  is closed for all  $i$ , and hence  $S = \bigcup_{i=1}^n (e_i + V_i)$  is a closed subset not containing zero. Thus there exists  $C > 0$  such that  $B(0, C) \cap S = \emptyset$  where  $B(0, C) = \{x \in V \mid \|x\| < C\}$ .

Let  $x = \sum_{i=1}^n x_i e_i$  and suppose  $|x_j| = \max_i |x_i|$ . Then  $\|x\|_{\sup} = |x_j|$ , and  $(1/x_j)x \in S$ . Thus  $\|(1/x_j)x\| \geq C$ , so  $\|x\| \geq C|x_j| = C\|x\|_{\sup}$ .

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

**Definition 2.3.6.** 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**  $R^{\text{Int } S}$  of  $R$  inside  $S$  is defined to be

$$R^{\text{Int } S} = \{s \in S \mid s \text{ is integral over } R\}.$$

- We say  $R$  is **integrally closed** in  $S$  if  $R^{\text{Int } S} = R$ .

**Proposition 2.3.7.**  $R^{\text{Int } S}$  is a subring of  $S$ . Moreover  $R^{\text{Int } S}$  is integrally closed in  $S$ .

*Proof.* Example sheet 2.  $\square$

**Lemma 2.3.8.** Let  $(K, |\cdot|)$  be a non-archimedean valued field. Then  $\mathcal{O}_K$  is integrally closed in  $K$ .

*Proof.* Let  $x \in K$  be integral over  $\mathcal{O}_K$ , and without loss of generality  $x \neq 0$ . Let  $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathcal{O}_K[X]$  such that  $f(x) = 0$ . Then  $x = -a_{n-1} - \dots - a_0/x^{n-1}$ . If  $|x| > 1$ , we have  $|-a_{n-1} - \dots - a_0/x^{n-1}| \leq 1$ , a contradiction. Thus  $|x| \leq 1$ , so  $x \in \mathcal{O}_K$ .  $\square$

*Proof of Theorem 2.3.1.*

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

1.  $|y|_L = 0$  if and only if  $|N_{L/K}(y)| = 0$ , if and only if  $N_{L/K}(y) = 0$ , if and only if  $y = 0$ , by property of  $N_{L/K}$ .
2.  $|y_1 y_2|_L = |N_{L/K}(y_1 y_2)| = |N_{L/K}(y_1) N_{L/K}(y_2)| = |N_{L/K}(y_1)| |N_{L/K}(y_2)| = |y_1|_L |y_2|_L$ .
3. Set  $\mathcal{O}_L = \{y \in L \mid |y|_L \leq 1\}$ . Claim that  $\mathcal{O}_L$  is the integral closure of  $\mathcal{O}_K$  inside  $L$ .
  - Let  $0 \neq y \in \mathcal{O}_L$  and let  $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$  be the minimal polynomial of  $y$ . By property of  $N_{L/K}$ , there exists  $m \geq 1$  such that  $N_{L/K}(y) = \pm a_0^m$ . By Corollary 2.1.5, we have  $|a_i| \leq \max(|N_{L/K}(y)|^{1/m}, 1) = 1$ , since  $|N_{L/K}(y)| \leq 1$ . Thus  $a_i \in \mathcal{O}_K$  for all  $i$ , so  $f \in \mathcal{O}_K[X]$ , so  $y$  is integral over  $\mathcal{O}_K$ .
  - Conversely let  $y \in L$  be integral over  $\mathcal{O}_K$ . Again by property of  $N_{L/K}$ , we have

$$N_{L/K}(y) = \left( \prod_{\sigma: L \rightarrow \bar{K}} \sigma(y) \right)^d, \quad d \geq 1,$$

where  $\bar{K}$  is an algebraic closure of  $K$  and  $\sigma$  runs over  $K$ -algebra homomorphisms. For all such  $\sigma: L \rightarrow \bar{K}$ ,  $\sigma(y)$  is integral over  $\mathcal{O}_K$ . Thus  $N_{L/K}(y) \in K$  is integral over  $\mathcal{O}_K$ . By Lemma 2.3.8,  $N_{L/K}(y) \in \mathcal{O}_K$ , so  $|N_{L/K}(y)| \leq 1$ , so  $y \in \mathcal{O}_L$ .

Thus  $\mathcal{O}_K^{\text{Int } L} = \mathcal{O}_L$  and proves the claim. Now we prove 3. Let  $x, y \in L$ . Without loss of generality assume  $|x|_L \leq |y|_L$ , then  $|x/y|_L \leq 1$ , so  $x/y \in \mathcal{O}_L$ . Since  $1 \in \mathcal{O}_L = \mathcal{O}_K^{\text{Int } L}$ , we have  $1 + x/y \in \mathcal{O}_L$  and hence  $|1 + x/y|_L \leq 1$ , so  $|x + y|_L \leq |y|_L = \max(|y|_L, |x|_L)$ . Thus 3 is satisfied. If  $|\cdot|'_L$  is another absolute value on  $L$  extending  $|\cdot|$ , then note that  $|\cdot|_L$  and  $|\cdot|'_L$  are norms on  $L$ . By Theorem 2.3.5,  $|\cdot|'_L$  and  $|\cdot|_L$  induce the same topology on  $L$ , so  $|\cdot|'_L = |\cdot|_L^c$  for some  $c > 0$ . Since  $|\cdot|'_L$  extends  $|\cdot|$ , we have  $c = 1$ .

2. Since  $|\cdot|_L$  defines a norm on  $K$ , Theorem 2.3.5 implies  $L$  is complete with respect to  $|\cdot|_L$ .

□

**Corollary 2.3.9.** *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  $|\cdot|_L$ , and
2.  $\mathcal{O}_L$  is the integral closure of  $\mathcal{O}_K$  in  $L$ .

*Proof.*

1. Let  $v$  be a valuation on  $K$ , and let  $v_L$  be a valuation on  $L$  such that  $v_L$  extends  $v$ . If  $y \in L^\times$ , then  $|y|_L = |N_{L/K}(y)|^{1/n}$  for  $n = [L : K]$ , so  $v_L(y) = (1/n)v(N_{L/K}(y))$ . Thus  $v_L(L^\times) \subseteq (1/n)v(K^\times)$ , so  $v_L$  is discrete.
2. Proved in the last lecture.

□

**Corollary 2.3.10.** *Let  $(K, |\cdot|)$  be a complete non-archimedean discretely valued field and  $\bar{K}/K$  an algebraic closure. Then  $|\cdot|$  extends to a unique absolute value  $|\cdot|_{\bar{K}}$  on  $\bar{K}$ .*

*Proof.* If  $x \in \bar{K}$ , then  $x \in L$  for some  $L/K$  finite. Define  $|x|_{\bar{K}} = |x|_L$ . Well-defined, that is independent of  $L$ , by the uniqueness in Theorem 2.3.1. The axioms for  $|\cdot|_{\bar{K}}$  to be an absolute value can be checked over finite extensions. Uniqueness is clear. □

**Remark.**  $|\cdot|_{\bar{K}}$  on  $\bar{K}$  is never discrete. For example, if  $K = \mathbb{Q}_p$ , then  $\sqrt[n]{p} \in \bar{\mathbb{Q}}_p$  for all  $n \in \mathbb{N}_{>0}$ , so  $v_p(\sqrt[n]{p}) = (1/n)v_p(p) = 1/n$ . Then  $\bar{\mathbb{Q}}_p$  is not complete with respect to  $|\cdot|_{\bar{\mathbb{Q}}_p}$ . By example sheet 2, if  $\mathbb{C}_p$  is the completion of  $\bar{\mathbb{Q}}_p$  with respect to  $|\cdot|_{\bar{\mathbb{Q}}_p}$ , then  $\mathbb{C}_p$  is algebraically closed.

### 3 Local fields

#### 3.1 Local fields

**Definition 3.1.1.** Let  $(K, |\cdot|)$  be a valued field. Then  $K$  is a **local field** if it is complete and locally compact.

**Example.**  $\mathbb{R}$  and  $\mathbb{C}$  are local fields.

**Proposition 3.1.2.** Let  $(K, |\cdot|)$  be a non-archimedean complete valued field. The following are equivalent.

1.  $K$  is locally compact.
2.  $\mathcal{O}_K$  is compact.
3.  $v$  is discrete and  $k = \mathcal{O}_K/\mathfrak{m}$  is finite.

*Proof.*

- 1  $\implies$  2. Let  $U \ni 0$  be a compact neighbourhood of zero. Then there exists  $x \in \mathcal{O}_K$  such that  $x\mathcal{O}_K \subseteq U$ . Since  $x\mathcal{O}_K$  is closed,  $x\mathcal{O}_K$  is compact, so  $\mathcal{O}_K$  is compact, since  $x^{-1} : x\mathcal{O}_K \rightarrow \mathcal{O}_K$  is homeomorphism.
- 2  $\implies$  1. If  $\mathcal{O}_K$  is compact, then  $a + \mathcal{O}_K$  compact for all  $a \in K$ , so  $K$  is locally compact.
- 2  $\implies$  3. Let  $x \in \mathfrak{m}$ , and  $A_x \subseteq \mathcal{O}_K$  be a set of coset representatives for  $\mathcal{O}_K/x\mathcal{O}_K$ . Then

$$\mathcal{O}_K = \bigcup_{y \in A_x} (y + x\mathcal{O}_K)$$

is a disjoint open cover, so  $A_x$  is finite by compactness of  $\mathcal{O}_K$ , so  $\mathcal{O}_K/x\mathcal{O}_K$  is finite, so  $\mathcal{O}_K/\mathfrak{m}$  is finite. Suppose  $v$  is not discrete. Let  $x = x_1, x_2, \dots$  such that  $v(x_1) > v(x_2) > \dots > 0$ . Then  $x_1\mathcal{O}_K \subsetneq x_2\mathcal{O}_K \subsetneq \dots \subsetneq \mathcal{O}_K$ . But  $\mathcal{O}_K/x\mathcal{O}_K$  is finite so can only have finitely many subgroups, a contradiction.

- 3  $\implies$  2. Since  $\mathcal{O}_K$  is a metric space, it suffices to show  $\mathcal{O}_K$  is sequentially compact. Let  $(x_n)_{n=1}^\infty$  be a sequence in  $\mathcal{O}_K$  and fix  $\pi \in \mathcal{O}_K$  a uniformiser in  $\mathcal{O}_K$ . Since  $\pi^i\mathcal{O}_K/\pi^{i+1}\mathcal{O}_K \cong k$ ,  $\mathcal{O}_K/\pi^i\mathcal{O}_K$  is finite for all  $i$ , since  $\mathcal{O}_K \supseteq \dots \supseteq \pi^i\mathcal{O}_K$ . Since  $\mathcal{O}_K/\pi\mathcal{O}_K$  is finite, there exists  $a_1 \in \mathcal{O}_K/\pi\mathcal{O}_K$  and a subsequence  $(x_{1,n})_{n=1}^\infty$  such that  $x_{1,n} \equiv a_1 \pmod{\pi}$ . We define  $y_1 = x_{1,1}$ . Since  $\mathcal{O}_K/\pi^2\mathcal{O}_K$  is finite, there exists  $a_2 \in \mathcal{O}_K/\pi^2\mathcal{O}_K$  and a subsequence  $(x_{2,n})_{n=1}^\infty$  of  $(x_{1,n})_{n=1}^\infty$  such that  $x_{2,n} \equiv a_2 \pmod{\pi^2}$ . Define  $y_2 = x_{2,2}$ . Continuing in this fashion, we obtain sequences  $(x_{i,n})_{n=1}^\infty$  for  $i = 1, 2, \dots$  such that

- $(x_{i+1,n})_{n=1}^\infty$  is a subsequence of  $(x_{i,n})_{n=1}^\infty$ , and
- for any  $i$ , there exists  $a_i \in \mathcal{O}_K/\pi^i\mathcal{O}_K$  such that  $x_{i,n} \equiv a_i \pmod{\pi^i}$  for all  $n$ .

Then necessarily  $a_i \equiv a_{i+1} \pmod{\pi^i}$  for all  $i$ . Now choose  $y_i = x_{ii}$ . This defines a subsequence  $(y_n)_{n=1}^\infty$ . Moreover  $y_i \equiv a_i \equiv a_{i+1} \equiv y_{i+1} \pmod{\pi^i}$ . Thus  $y_i$  is Cauchy, hence converges by completeness. □

**Example.**

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

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

**Definition 3.1.3.** Assume  $A_n$  is finite. The **profinite topology** on  $A = \varprojlim_n A_n$  is the weakest topology on  $A$  such that  $A \rightarrow A_n$  is continuous for all  $n$ , where  $A_n$  are equipped with the discrete topology.

**Fact.**  $A = \varprojlim_n A_n$  with profinite topology is compact, totally disconnected, and Hausdorff.



**Proposition 3.1.4.** *Let  $K$  be a local field. Under the isomorphism  $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n \mathcal{O}_K$  for  $\pi \in \mathcal{O}_K$  a uniformiser, the topology on  $\mathcal{O}_K$  coincides with the profinite topology.*

*Proof.* One checks that the sets

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

where  $A_{\pi^n}$  is a set of coset representatives for  $\mathcal{O}_K/\pi^n \mathcal{O}_K$ , is a basis of open sets in both topologies. For  $|\cdot|$ , this is clear. For the profinite topology,  $\mathcal{O}_K \rightarrow \mathcal{O}_K/\pi^n \mathcal{O}_K$  is continuous if and only if  $a + \pi^n \mathcal{O}_K$  is open for all  $a \in A_{\pi^n}$ . Thus  $B$  is a basis for the profinite topology.  $\square$

**Remark.** This gives another proof that  $\mathcal{O}_K$  is compact.