

# Part III - Local Fields

Lectured by Rong Zhou

Artur Avameri

## Contents

<b>0</b>	<b>Introduction</b>	<b>2</b>
<b>1</b>	<b>Basic Theory</b>	<b>2</b>
1.1	Absolute values . . . . .	2

## 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 Basic Theory

### 1.1 Absolute values

**Definition 1.1.** Let  $K$  be a field. An **absolute value** on  $K$  is a function  $|\cdot| : K \rightarrow \mathbb{R}_{\geq 0}$  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 **value 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):  $|x| < 1 \iff x^n \rightarrow 0$  with respect to  $|\cdot| \iff x^n \rightarrow 0$  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

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

a contradiction. The other inequality is analogous.

(iii)  $\implies$  (i): Clear. □

**Remark.**  $|\cdot|_\infty^2$  on  $\mathbb{C}$  is not an absolute value by our definition (doesn't satisfy the triangle inequality). Some authors replace this by the condition  $|x + y|^\beta \leq |x|^\beta + |y|^\beta$  for some fixed  $\beta \in \mathbb{R}_{>0}$ . The induced topologies 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**

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

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,  $|y| \leq \max(|x|, |x - y|) = |x - y|$ .  $\square$

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  $|x_n - x_{n+1}| \rightarrow 0$ , 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  $N < n < m$ ,

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

so  $(x_n)$  is Cauchy.  $\square$

**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

$$x_{n+1}^2 + 1 = x_n^2 + 2bx_n5^n + b^25^{2n} + 1 = a5^n + 2bx_n5^n + \overset{\equiv 0 \pmod{5^{n+1}}}{b^25^{2n}}.$$

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,  $x_n \rightarrow l \in \mathbb{Q}$ . Then  $x_n^2 \rightarrow l^2 \in \mathbb{Q}$ . But by (i),  $x_n^2 \rightarrow -1$ , 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  $|\cdot|_p$ .