Part III - Local Fields

Lectured by Rong Zhou

Artur Avameri

Contents

0 Introduction **2**

1 Basic Theory **2**

1.1 Absolute values 2

1.2 Valuation rings 5

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 $|\cdot| : K \to \mathbb{R}_{\geq 0}$ 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 $|x+y|^\beta \leq |x|^\beta + |y|^\beta$ 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**

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

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

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

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

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

$\square$

1.2 Valuation rings

Definition 1.5. 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 1.6. 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 1.3.

- 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 1.7. 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, $\mathcal{O}_K = \overline{B}(0,1)$).[1]

Proposition 1.5. (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) Similar to (i), left as an exercise.

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

∎

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 1.6. $\mathcal{O}_K$ 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. ∎

[1]Another alternative definition given was $\mathcal{O}_K = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$. Is this equivalent to the above?

Example 1.4. $K = \mathbb{Q}$ 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 1.8. 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 1.5.
- $K = \mathbb{Q}$ 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 1.7. 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 $v(x^{-1}y) \geq 0 \implies y = x(x^{-1}y) \in x\mathcal{O}_K$.

(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 $x_2, \ldots, x_n \in x_1\mathcal{O}_K$, 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 $v(K^\times) = c\mathbb{Z}$. $\square$