Local Fields

October 12, 2020

1 Basic Theory

Suppose we have a diophantine polynomial $f(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, x_r]$. Then we might want to find integer solutions to the equation $f(x_1, \ldots, x_r) = 0$. However, it turns out this can be very difficult to do, for instance showing $x^n + y^n - z^n = 0$ has no solutions for $x, y, z \in \mathbb{Z}$ took hundreds of years and a lot of advanced mathematics.

Instead, we study congruences of the form $f(x_1, \ldots, x_r) \equiv 0 \mod p^n$, for prime p and integer n. This then becomes a finite computation, and hence a much easier problem. Local fields will give us a way to package all this information together.

1.1 Absolute Values

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

1. $|x| = 0 \iff x = 0$
2. $|xy| = |x||y| \ \forall x, y \in K$
3. $|x + y| \leq |x| + |y| \ \forall x, y \in K$

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

Examples:

1. $K = \mathbb{R}$ or $\mathbb{C}$ with $|\cdot|$ the usual absolute value. We write $|\cdot|_\infty$ for this absolute value.
2. K is any field. The ***trivial absolute value*** on K is defined by:

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

   We will ignore this absolute value in this course.

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

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

   We check the axioms.

1. Clear from the definition.

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

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

An absolute value on K induces a metric $d(x,y) = |x-y|$ on K, and hence induces a topology on K. As an exercise, check that $+, \cdot$ are continuous.

Definition 1.2. *Let $|\cdot|, |\cdot|'$ be absolute values on a field K. We say that $|\cdot|, |\cdot|'$ are* **equivalent** *if they induce the same topology on K. An equivalence class of absolute values is called a* **place***.*

Proposition 1.3. *Let $|\cdot|, |\cdot|'$ be non-trivial absolute values on K. The following are equivalent:*

1. *$|\cdot|, |\cdot|'$ are equivalent.*

2. *$|x| < 1 \iff |x|' < 1\ \forall x \in K$.*

3. *$\exists\, c \in \mathbb{R}_{>0}$ s.t. $|x|^c = |x|'\ \forall x \in K$*

Proof.
1. $\Longrightarrow$ 2.

$$\begin{aligned} |x| < 1 &\iff x^n \to 0 \text{ w.r.t. } |\cdot| && (2)\\ &\iff x^n \to 0 \text{ w.r.t. } |\cdot|' && (3)\\ &\iff |x|' < 1 && (4)\end{aligned}$$

2. $\Longrightarrow$ 3. Let $a \in K^\times$ s.t. $|a| < 1$, which exists since $|\cdot|$ is non-trivial. We need to show that, for all $x \in K^\times$, we have:

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

Assume $\frac{\log|x|}{\log|a|} < \frac{\log|x|'}{\log|a|'}$. Then choose $m, n \in \mathbb{Z}$ so that $\frac{\log|x|}{\log|a|} < \frac{m}{n} < \frac{\log|x|'}{\log|a|'}$. Then we have:

$$n\log|x| < m\log|a|$$
$$n\log|x|' > m\log|a|'$$

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

3. $\Longrightarrow$ 1. This is clear, as open balls in one topology will also be open balls in the other, hence the topologies will be the same. $\square$

In this course, we will be mainly interested in the following types of absolute values:

Definition 1.4. *An absolute value $|\cdot|$ on K is said to be* **non-archimedean** *if it satisfies the ultrametric inequality $|x+y| \leq \max(|x|, |y|)$*

If $|\cdot|$ is not non-archimedean, then it is archimedean.
Examples:

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

Lemma 1.5 (All triangles are isosceles)**.** *Let $(K, |\cdot|)$ be a non-archimedean valued field, and $x, y \in K$. If $|x| < |y|$, then $|x-y| = |y|$.*

Proof. Observe that $|1| = |1 \cdot 1| = |1| \cdot |1|$, and so $|1| = 1$ or 0. But $1 \neq 0$, so $|1| = 1$. Similarly, $|-1| = 1$, and so $|-y| = |y|$ for all $y \in K$.

Then if $|x| < |y|$, $|x-y| \leq \max(|x|, |y|) = |y|$.

At the same time $|y| \leq \max(|x|, |x-y|) \implies |y| \leq |x-y|$.

Hence $|y| = |x-y|$. □

Proposition 1.6. *Let $(K, |\cdot|)$ be non-archimedean, and $(x_n)_{n=1}^{\infty}$ be a sequence in K.*

If $|x_n - x_{n+1}| \to 0$, then $(x_n)_{n=1}^{\infty}$ is Cauchy.

In particular, if K is in addition complete, then $(x_n)_{n=1}^{\infty}$ converges.

Proof. For $\epsilon > 0$, choose N such that $|x_n - x_{n+1}| < \epsilon \; \forall n > N$.

Then for $N < n < m$, we have:

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

And so the sequence is Cauchy. □

For example, if $p = 5$, construct the sequence $(x_n)_{n=1}^{\infty}$ such that:

1. $x_n^2 + 1 \equiv 0 \mod 5^n$
2. $x_n \equiv x_{n+1} \mod 5^n$

as follows:

Take $x_1 = 2$. Suppose we have constructed x_n. Let $x_n^2 + 1 = a5^n$, and set $x_{n+1} = x_n + b5^n$. Then $x_{n+1}^2 + 1 = x_n^2 + 2b5^n x_n + b^2 5^{2n} + 1 = a5^n + 2b5^n x_n + b^2 5^{2n}$.

We choose b such that $a + 2bx_n \equiv 0 \mod 5$, i.e. $b \equiv -\frac{a}{2x_n} \mod 5$, and then we have $x_{n+1}^2 + 1 \equiv 0 \mod 5^{n+1}$ as desired.

The second property implies that $|x_{n+1} - x_n|_5 < 5^{-n} \to 0$, and so the sequence is Cauchy. Now suppose that $x_n \to L \in \mathbb{Q}$. Then $x_n^2 \to L^2$. But the first property then gives us that $x_n^2 \to -1 \implies L^2 = -1 \lightning$. So $(\mathbb{Q}, |\cdot|_5)$ is not complete.

Definition 1.7. *The p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.*

We have an analogy with $\mathbb{R}$, in that $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$.

If $(K, |\cdot|)$ is a valued field, for $x \in K, r \in \mathbb{R}_{>0}$, we define:

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

and call these the ***open*** and ***closed balls*** of radius r centred at x, respectively.

Lemma 1.8. *Let $(K, |\cdot|)$ be non-archimedean. Then:*

1. *If $z \in B(x, r)$, then $B(z, r) = B(x, r)$.*

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

3. $B(x,r)$ *is closed.*

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

Proof.

1. Let $y \in B(x,r)$. Then $|x-y| < r \implies |z-y| = |(z-x)+(x-y)| \le \max(|z-x|, |x-y|) < r$.

2. Same as in *1.*, but with $\le$ instead of $<$.

3. Let $y \notin B(x,r)$. We need to show there is an open neighbourhood of y not intersecting $B(x,r)$. If $z \in B(x,r) \cap B(y,r)$, then $B(x,r) = B(z,r) = B(y,r)$. But then $y \in B(x,r)$ $\lightning$. So $B(x,r)$ and $B(y,r)$ are disjoint, and so $B(x,r)$ is closed.

4. If $z \in \overline{B}(x,r)$, then we need to show there is an open neighbourhood of z contained in $\overline{B}(x,r)$. But $B(z,r) \subseteq \overline{B}(z,r) = \overline{B}(x,r)$, and so $\overline{B}(x,r)$ is open.

$\square$

2 Valuation Rings

Definition 2.1. *Let* K *be a field. A* **valuation** *on* K *is a function* $v : K^\times \to \mathbb{R}$ *such that:*

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

2. $v(x+y) \le \min(v(x), v(y))$

Fix $0 < \alpha < 1$. If v is a valuation on K, then $|x| = \begin{cases} \alpha^{v(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$ determines a non-archimedean absolute value. Conversely, a non-archimedean absolute value determines a valuation $v(x) = \log_\alpha |x|$.

We will ignore the trivial valuation $v(x) \equiv 0$, which corresponds to the trivial absolute value.

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

Examples:

- $K = \mathbb{Q}, v_p() = -\log_p |x|_p$ is the p-adic valuation.
- k any field, $K = k(t) = \mathrm{Frac}(k[t])$, the rational function field. $v\left(t^n \frac{f(t)}{g(t)}\right) = n$ where $f, g \in k[t], f(0), g(0) \neq 0$. This is the t-adic valuation.
- $K = k((t)) = \mathrm{Frac}(k[[t]])$, the field of ***formal Laurent series over k***. Then we have $v\left(\sum_i a_i t^i\right) = \min\{i : a_i \neq 0\}$ is the t-adic valuation on K.

Definition 2.2. *Let* $(K, |\cdot|)$ *be a non-archimedean valued field. The* **valuation ring** *of* K *is defined to be:*

$$\begin{aligned} \mathcal{O}_K &= \{x \in K : |x| \le 1\} \quad (= \bar{B}(0,1)) \\ &= \{x \in K^\times : v(x) \ge 0\} \cup \{0\} \end{aligned}$$

Proposition 2.3.

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

Proof.

1. $|1| = 1, |0| = 0$, so $1, 0 \in \mathcal{O}_K$. $|-x| = |x|$, so $x \in \mathcal{O}_K \implies -x \in \mathcal{O}_K$. If $x, y \in \mathcal{O}_K$, then $|x + y| \leq \max(|x|, |y|) \leq 1$, and so $x + y \in \mathcal{O}_K$, and $|xy| = |x||y| \leq 1$, so $xy \in \mathcal{O}_K$. Since $\mathcal{O}_K = \bar{B}(0, 1)$, it is open.
2. The proof of this is the same as *1.*
3. Note that $|x||x^{-1}| = |xx^{-1}| = 1$. So $|x| = 1 \iff |x^{-1}| = 1$. This can happen if and only if $x, x^{-1} \in \mathcal{O}_K$, i.e. $x \in \mathcal{O}_K^\times$.

□

As a point of notation, we will define $m \coloneqq \{x \in \mathcal{O}_K : |x| < 1\}$, a maximal ideal of $\mathcal{O}_K$, and $k \coloneqq \mathcal{O}_K/m$ to be the ***residue field***.

Corollary 2.4. *$\mathcal{O}_K$ is a local ring with a unique maximal ideal m.*

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

Examples:

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

Definition 2.5. *Let $v : K^\times \to \mathbb{R}$ be a valuation. If $v(K^\times) \cong \mathbb{Z}$, we say v is a* **discrete valuation***, and K is said to be a* **discretely valued field**. *An element $\pi \in \mathcal{O}_K$ is a* **uniformizer** *if $v(\pi) = 0$ and $v(\pi)$ generates $v(K^\times)$.*

Remark: If v is a discrete valuation, we can replace it with an equivalent one such that $v(K^\times) = \mathbb{Z} \subseteq \mathbb{R}$. Such v are called ***normalized valuations***, and have $v(\pi) = 1$ for π a uniformizer.

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

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

Proof.
1. $\implies$ *2.* Let $I \subseteq \mathcal{O}_K$ be a non-zero ideal. Let $x \in I$ such that $v(x) = \min\{v(a) : a \in I\}$, which exists since v is discrete. Then $x\mathcal{O}_K = \{a \in O_K : v(a) \geq v(x)\} \subseteq I$, and hence $x\mathcal{O}_K = I$ by definition of x - if $y \in I \setminus (x)$, then $v(y) < v(x)$↯.

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

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

4. $\Longrightarrow$ *1.* Let $m = \pi\mathcal{O}_K$ for some $\pi \in \mathcal{O}_K$, and let $c = v(\pi)$. Then if $v(x) > 0$, $x \in m$ and hence $v(x) \geq c$. Thus $v(K^\times) \cap (0, c) = \emptyset$. Since $v(K^\times)$ is a subgroup of $(\mathbb{R}, +)$, we have $v(K^\times) = c\mathbb{Z}$. □

Lemma 2.7. *Let v be a discrete valuation on K, and $\pi \in \mathcal{O}_K$ a uniformizer. Then for any $x \in K^\times$ there exists $n \in \mathbb{Z}$ and $u \in \mathcal{O}_K^\times$ such that $x = \pi^n u$. In particular, $K = \mathcal{O}_K\left[\frac{1}{x}\right]$ for any $x \in m$ and hence $K = \operatorname{Frac}\mathcal{O}_K$.*

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

Definition 2.8. *A ring R is called a* **discrete valuation ring (DVR)** *if it is a PID with exactly one non-zero prime ideal.*

Lemma 2.9.

1. *Let v be a discrete valuation on K. Then $\mathcal{O}_K$ is a DVR.*
2. *Let R be a DVR. Then there is a valuation v on $K \coloneqq \operatorname{Frac}(R)$ such that $R = \mathcal{O}_K$.*

Proof.

1. $\mathcal{O}_K$ is a PID by **2.6**. Let $0 \neq I \subseteq \mathcal{O}_K$ be an ideal, then $I = (x)$ for some x. If $x = \pi^n u$ for π a uniformizer, then (x) is prime if and only if $n = 1$, and $I = (\pi) = m$.
2. Let R be a DVR with maximal ideal m. Then $m = (\pi)$ for some $\pi \in R$. Since PIDs are UFDs, we may write $x \in R \setminus \{0\}$ uniquely as $\pi^n u, n \geq 0, u \in R^\times$. Then any $y \in K \setminus \{0\}$ can be written uniquely as $\pi^m u, u \in R^\times, m \in \mathbb{Z}$. Then define $v(\pi^m u) = m$, and it is easy to check v is a valuation and $\mathcal{O}_K = R$.

□

Examples:

- $\mathbb{Z}_{(p)}$ is a DVR, the valuation ring of $|\cdot|_p$ on $\mathbb{Q}$.
- $k[[t]]$ is a DVR, the valuation ring of the t-adic valuation on $k((t))$.
- $K = k(t), K' = K\left(t^{\frac{1}{2}}, t^{\frac{1}{4}}, t^{\frac{1}{8}}, \dots\right)$. The t-adic valuation extends to K', but we must have $v(t^{\frac{1}{2^n}}) = \frac{1}{2^n}$, which is not discrete.