Local Fields

October 9, 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. $\implies$ 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. $\implies$ 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. $\implies$ 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 $|y| = |x - y|$. $\square$

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. $\square$

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 $|\cdot|_\infty$.