Local Fields

Lectures by Rong Zhou

Contents

1 Basic Theory

A motivating question for an algebraic number theorist is 'how can we find solutions to Diophantine equations?' *i.e.* $f(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, d_r],\ f = 0$.

In general, this is very difficult (*e.g.* Fermat's Last Theorem). However, a more approachable problem might be to solve $f(x_1, \ldots, x_r) \equiv 0 \mod p$. From here, we might be able to gain insight into solving $f(x_1, \ldots, x_r) \equiv 0 \mod p^n$ for each $n \in \mathbb{N}$.

Local fields gives us a way to package all of this information together.

1.1 Absolute Values

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

(i) $|x| = 0$ iff $x = 0$

(ii) $|xy| = |x||y|$ for all $x, y \in K$

(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in K$ - this is known as the ***triangle inequality***.

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

Examples:

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

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

  We will ignore this case in this course as it is of no interest to us. However, the *most* interesting example is:

- $K = \mathbb{Q}$, p prime. For $0 \neq x \in \mathbb{Q}$, 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

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

  The intuition behind this is that if you consider, say, just the integers, then the p-adic value of m will be very small if m is highly divisible by p. That is to say it encodes information about how divisible m is by p.

  We check the axioms to be sure this is indeed an absolute value. (i) is clear.

  Write $y = p^m \frac{c}{d}$.

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

  For (iii): wlog. $m \geq n$. Then

$$\begin{aligned} |x + y|_p &= \left| p^n \left(\frac{ad + p^{m-n} bc}{bd} \right) \right|_p \\ &= |p^n|_p \left| \frac{ad + p^{m-n} bc}{bd} \right|_p \end{aligned}$$

In this second term, the denominator is not divisible by p, so the absolute value of the term on the rate is ≤ 1. Hence

$$|x+y|_p \leq p^{-n} = \max(|x|_p, |y|_p)$$

We remark that the above is known as the ***ultrametric inequality***, which is stronger than the triangle inequality.

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

Exercise: prove that $+, \cdot$ are continuous with respect to this topology.

Definition 1.2: (Equivalent Absolute Values) Let $|\cdot|, |\cdot|'$ be absolute values on a field K. We say $|\cdot|, |\cdot|'$ are ***equivalent*** if they induce the same topology.

We will see that if two absolute values are equivalent, then they determine each other and give us the same theory. Accordingly, equivalence of absolute values is indeed an equivalence relation; such an equivalence class is called a ***place***.

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

(i) $|\cdot|, \cdot|'$ are equivalent

(ii) $|x| < 1$ iff $|x|' < 1$ for all $x \in K$

(iii) $\exists c \in \mathbb{R}_{>0}$ such that $|x|^c = |x|'$ for all $x \in K$

Proof. $(i) \implies (ii)$:

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

$(ii) \implies (iii)$: Let $a \in K^\times$ such that $|a| < 1$ (this exsts since $|\cdot|$ is non-trivial). We need to show that

$$\forall x \in K^\times : \ \frac{\log|x|}{\log|a|} = \frac{\log|x|'}{\log|a|'}$$

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

then we have that $n\log|x| < m\log|a|$, but also that $n\log|x|' > m\log|a|'$. Hence $|x^n/a^m| < 1$ and $|x^n/a^m|' > 1$ $\perp$.

Similarly for the case with the inequality reversed.

$(iii) \implies (i)$ is in fact clear, because if (iii) holds then any open ball with respect to one topology will also be an open ball in the other topology. Hence the topology generated by these absolute values is the same. $\square$

So it suffices to work only with equivalence classes of absolute values. In this course, we are mainly interested in the following types of absolute values:

Definition 1.4: (Non-Archimedean AV) An absolute value 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.

For example:

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

It turns out that non-archimedean absolute values give rise to some rather interesting properties:

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

Proof. **Fact**: $|1| = |-1| = 1$, and $|-y| = |y|$. These results are left as an exercise.

Observe that $|x-y| \leq \max(|x|,|y|) = |y|$, and moreover $|y| \leq \max(|x|,|x-y|)$, so by assumption $|y| \leq |x-y|$. Hence we have equality. □

While this property is unusual and might appear to make some things more difficult to reason about, there are in fact some properties of this topology that make our lives easier - for example, convergence.

Proposition 1.6: Let $(K, |\cdot|)$ be non-archimedean and $(x_n)_{n=1}^\infty$ 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 $\varepsilon > 0$, choose N such that $|x_n - x_{n+1}| < \varepsilon$ for all $n > N$. Then for $N < n < m$:

$$\begin{aligned} |x_n - x_m| &= |(x_n - x_{n+1}) + (x_{n+1} - x_{n+2}) + \cdots + (x_{m-1} - x_m)| \\ &< \varepsilon \end{aligned}$$

So $(x_n)_{n=1}^\infty$ is Cauchy. □

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

(i) $x_n^2 + 1 \equiv 0 \mod 5^n$

(ii) $x_n \equiv x_{n+1} \mod 5^n$

as follows.

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

$$\begin{aligned} x_{n+1}^2 + 1 &= x_n^2 + 2b \cdot 5^n + b^2 \cdot 5^{2n} + 1 \\ &= a5^n + 2b5^n + b^2 5^{2n} \end{aligned}$$

We remark that the final term is already $\equiv 0 \mod 5^{n+1}$ as $n > 1$, hence we need only choose b such that $a + 2b \equiv 0 \mod 5$, which is always possible since 2 is a unit $\mod 5$. Then $x_{n+1}^2 + 1 \equiv 0 \mod 5^{n+1}$ as desired.

So we have constructed a sequence satisfying these two properties. The second property tells us that the 5-adic values of the differences between successive terms tends to zero as $n \to \infty$. Hence $(x_n)_{n=1}^{\infty}$ is Cauchy. Does the limit exist?

Suppose $x_n \to \ell \in \mathbb{Q}$. Then $x_n^2 \to \ell^2$. But (i) tells us that $x_n^2 \to -1$, so $\ell^2 = -1$ $\perp$.

Thus $(\mathbb{Q}, |\cdot|_5)$ is *not* complete.

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

This gives us analogy with $\mathbb{R}$; $\mathbb{R}$ is the completion of $\mathbb{Q}$ under $|\cdot|_\infty$, whereas $\mathbb{Q}_p$ is the completion under $|\cdot|_p$.

The p-adic numbers are the prototypical example of a local field. They also have a field structure (*c.f.* sheet 1), and as we have seen are strictly larger than the rationals. The completion for the reals is much more geometric, whereas the completion for the p-adics contains more interesting *arithmetic* information.