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

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

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

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

$(ii) \implies (iii)$: 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. $\qquad \square$

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

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 $|x - y| \le \max(|x|, |y|) = |y|$, and moreover $|y| \le \max(|x|, |x - y|)$, so by assumption $|y| \le |x - y|$. Hence we have equality. $\qquad \square$

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 $N < n < m$:

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

So $(x_n)_{n=1}^\infty$ is Cauchy. $\qquad \square$

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

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

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 $a + 2bx_n \equiv 0 \mod 5$, which is always possible since both 2 and x_n are units $\mod 5$. 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 $x_n^2 \vec{\to} \ell^2$. 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.

Lecture 2

Let $(K, | \cdot |)$ be a non-archimedean valued field.

For $x \in K$ and $r \in \mathbb{R}_{>0}$, define the ***open/closed balls***:

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

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

(i) If $z \in B(x, r)$, then $B(z, r) = B(x, r)$. In other words, open balls don't have centres.

(ii) If $z \in \overline{B}(x, r)$, then $\overline{B}(z, r) = \overline{B}(x, r)$ - ditto for closed balls.

(iii) $B(x, r)$ is closed

(iv) $\overline{B}(x, r)$ is open

These statements are unusual from someone who has an archimedean perspective, since they are obviously not true in *e.g.* the reals. This suggests that we will make heavy use of the ultrametric inequality in the proof.

Proof. (i) Let $y \in B(x, r)$. Then

$$|x - y| < r \implies |z - y| = |(z - x) + (x - y)|$$
$$\leq \max(|z - x|, |x - y|)$$
$$< r$$

6

Thus $B(x, r) \subset B(z, r)$, and the reverse inclusion follows by symmetry.

(ii) Follows in the same way as (i), just with $\leq$ instead of $<$.

(iii) We show that for any point not in the ball, there exists a ball around it that does not intersect with $B(x, r)$.

Let $y \notin B(x, r)$. If $z \in B(x, r) \cap B(y, r)$, then $B(x, r) = B(z, r) = B(y, r)$. But then $y \in B(x, r) \perp$. Hence $B(x, r) \cap B(y, r) = \emptyset$, and so $B(y, r)$ is the ball we desire.

(iv) again follows similarly. We show that every point inside $\cap B(x, r)$, there is an open neighbourhood contained within that contains it.

If $z \in \overline{B}(x, r)$, then $B(z, r) \subset \overline{B}(z, r) = \overline{B}(x, r)$. $\qquad \square$

2   Valuation Rings

Definition 2.1: (Valuation)   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) $v(x + y) \leq \min(v(x), v(y))$

What's the point of this definition? Well, this valuation actually determines a non-archimedean absolute value.

Fix $0 < \alpha < 1$. If v is a valuation on K, then

$$|x| = \left\{ \begin{array}{ll} \alpha^{v(x)} & x \neq 0 \\ 0 & x = 0 \end{array} \right.$$

determines a non-archimedean absolute value.

Conversely, a non-archimedean absolute value determines a valuation $v(x) = \log_\alpha |x|$.

So these determine each other; what is the point of a valuation then? Well, it turns out that thinking about valuations is in some cases a little bit more useful. We will use the concept of a valuation to define something called a discrete valuation, and this will make our lives easier. Moreover, the concept of a valuation is more amenable to generalisation than an absolute value.

We can in fact define a more general version of a valuation, whereby we replace the reals in the definition with a totally ordered group. Using this we can define geometric objects called ***adic spaces***. These are super useful nowadays due to some recent work from Peter Schultzer. He invented ***perfectoid spaces***, but this is getting a little beyond the course now.

Remarks: • We ignore the trivial valuation $v(x) = 0$ for all $x \in K^\times$. This corresponds with the trivial absolute value in the above way.

   • We say v_1, v_2 are ***equivalent*** if $\exists c \in \mathbb{R}_{>0}$ such that $v_1(x) = c v_2(x) \ \forall x \in K^\times$. This notion of equivalence of course corresponds with the notion of equivalence of absolute values - so again we can reduce to considering just equivalence classes of valuations.

Examples: • Let $K = \mathbb{Q}$, $v_p(x) = -\log_p |x|_p$ is the p-adic valuation. This is obtained in the above way by taking $\alpha = 1/p$. So the valuation of x is just the power of p appearing in its prime factorisation.

- Let k be a field, and define $K = k(t) = \text{Frac}(k[t])$ its rational function field. We can then define a valuation $v\left(t^n f(t)/g(t)\right) = n$, where $f, g \in k[t]$, $f(0), g(0) \neq 0$ (note that we can always write any rational function in this way). This is known as the *t-adic valuation*

  There is an important analogy here with K and the rational numbers. $\mathbb{Q}$ and K are the prototypical examples of a *global field*. A lot of modern number theory in fact leverages this analogy to derive results about $\mathbb{Q}$ by studying K.

- $K = k((t)) = \text{Frac}(k[[t]]) = \{\sum_{i=n}^{\infty} a_i t^i : a_i \in k, n \in \mathbb{Z}\}$ is the field of formal Laurent series over k. We then have the valuation $v\left(\sum_i a_i t^i\right) = \min\{i : a_i \neq 0\}$. This is also known as the t-adic valuation on k.

  The reason for this is that example three is in fact the completion of example two under the topology induced in two.

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

$$\mathcal{O}_K = \{x \in K : |x| \leq 1\}$$
$$(= \overline{B}(0, 1))$$
$$(= x \in K^\times : v(x) \geq 0 \cup \{0\})$$

Proposition 2.3: Let $(K, |\cdot|)$ be as usual.

(i) $\mathcal{O}_K$ is an open subring of K - this is a very special, non-archimedean property.

(ii) The subsets $\{x \in K : |x| \leq r\}$ and $\{x \in K : |x| < r\}$ for ≤ 1 are open ideals in $\mathcal{O}_K$

(iii) $\mathcal{O}_K^\times = \{x \in K : |x| = 1\}$

Proof. Last lecture, we say $|1| = 1$, so $1 \in \mathcal{O}_K$, and $|0| = 0$ so $0 \in \mathcal{O}_K$. Moreover, $|-1| = |1| \implies |-x| = |x|$, so if $x \in \mathcal{O}_K$ then $-x \in \mathcal{O}_K$.

If $x, y \in \mathcal{O}_K$, then $|x + y| \leq \max(|x|, |y|) \leq 1$, which implies $x + y \in \mathcal{O}_K$ also.

If $x, y \in \mathcal{O}_K$, then $|xy| = |x||y| \leq 1$, so again $xy \in \mathcal{O}_K$.

Thus $\mathcal{O}_K$ is a ring. Then since $\mathcal{O}_K = \overline{B}(0, 1)$, it is open.

(ii) Is very similar to (i) (exercise).

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

The point here is that there some very nice algebraic structure going on here.

Notation:
- $m := \{x \in \mathcal{O}_K : |x| < 1\}$ - this is a maximal ideal of $\mathcal{O}_K$

- $k := \mathcal{O}_K/m$ is the *residue field*

Corollary 2.4: $\mathcal{O}_K$ is a local ring with a unique maximal ideal, and this ideal is m.

Recall that a ring with a maximal ideal is a local ring iff everything outside the maximal ideal is a unit. From Prop 2.3 we see that if an element of $\mathcal{O}_K$ doesn't lie in the maximal ideal m, then it has to have absolute value 1, and is hence a unit.

Examples: We exhibit some example of valuation rings:

- $K = k((t))$. Then $\mathcal{O}_K = k[[t]]$, $m = (t)$. The residue field is just k.

- $K = \mathbb{Q}$ with $|\cdot|_p$. Then $\mathcal{O}_K = \mathbb{Z}_{(p)}$, $m = p\mathbb{Z}_{(p)}$, $k = \mathbb{F}_p$

We have arrived at an important definition:

Definition 2.5: (Discrete Valuation) Let $v : K^\times \to \mathbb{R}$ be a valuation. If $v(K^\times) \simeq \mathbb{Z}$, 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 $v(K^\times)$ - *i.e.* an element with minimal positive valuation. These of course only exist when the valuation is discrete.

Examples: In this course we are mainly going to be focused on the cases when the valuation is discrete - such fields turn out to have some very nice properties. The valuations we have met so far indeed happen to be discrete.

- $K = \mathbb{Q}$, the p-adic valuation

- $K = k(t)$, the t-adic valuation

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

Lemma 2.6: Let v be a valuation on K. TFAE:

(i) v is discrete

(ii) $\mathcal{O}_K$ is a PID

(iii) $\mathcal{O}_K$ is Noetherian

(iv) m is principal

(ii) is the strongest condition, clearly implying (iii) and (iv). However, the equivalence of all the statements is quite cool, because it tells us that if our valuation is discrete then $\mathcal{O}_K$ satisfies some very nice properties.

Proof. (i) $\implies$ (ii) We need to show every non-zero ideal is principal. Let $I \subset \mathcal{O}_K$ be a non-zero ideal. Let $x \in I$ scuh that $v(d) = \min\{v(a) : a \in I\}$ which exists since v is discrete. Then $x\emptyset_K = \{a \in \mathcal{O}_K : v(a) \geq v(x)\} \subset I$, and hence $x\mathcal{O}_K = I$ by the definition of x. If we have some $y \in I \backslash x\mathcal{O}_K$, then $v(y) < v(x)$.

(ii) $\implies$ (iii) is clear, since all PIDs are finitely generated (by one element).

(iii) $\implies$ (iv): Write $m = x_1\mathcal{O}_K + \cdots + x_n\mathcal{O}_K$, and wlog. $v(x_1) \leq v(x_2) \leq \cdots \leq v(x_n)$. Then by a similar argument to (i) $\implies$ (ii) we have that $m = x_1\mathcal{O}_K$.

(iv) $\implies$ (i): 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 $(\mathbb{R}, +)$, this can only happen if $v(K^\times) = c\mathbb{Z}$. $\square$

Lemma 2.7: Let v be a discrete valuation on K and $\pi \in \mathcal{O}_K$ a uniformizer. $\forall x \in K^\times$, $\exists n \in \mathbb{Z}$ and $\exists u \in \mathcal{O}_K^\times$ such that $x = \pi^n u$. In particular, $K = \mathcal{O}_K[1/x]$, for any $x \in m$ and hence $k = \mathrm{Frac}(\mathcal{O}_K)$.

This says that the arithmetic of the field is determined by the arithmetic of the valuation field.

Proof. For $x \in K^\times$, let n be s.t. $v(x) = v(\pi^n) = nv(\pi)$. Then $v(x\pi^{-n}) = 0$, so $u = x\pi^{-n} \in \mathcal{O}_K^\times$.

Then if you invert any element of the maximal ideal, you also have to invert the uniformizer. $\qquad \square$

Definition 2.8: (Discrete Valuation Ring) A rgint R is called a ***discrete valuation ring*** (DVR) if it is a PID with exactly one non-zero prime ideal (that is necessarily maximal).

Note that while this name contains the term 'valuation', despite its definition lacking any explicit reference. This is now cleared up:

Lemma 2.9:

(i) Let v be a discrete valuation on K. Then $\mathcal{O}_K$ is a DVR.

(ii) Let R be a DVR. Then there exists a valuation v on $K := \operatorname{Frac}(R)$ such that $R = \mathcal{O}_K$.

Proof. (i) $\mathcal{O}_K$ is a PID by Lemma 2.6.

Let $0 \neq I \subset \mathcal{O}_K$ be an ideal, so $I = (x)$. If we write $x = \pi^n u$ for π a uniformizer, then (x) is prime iff $n = 1$, and so $I = (\pi) = m$. This is because if $n > 1$ we can break up x into a product of two elements, each containing a power of the uniformizer. So (x) is the product of two ideals and is not prime. So we must have $n = 1$, and this is clearly sufficient.

(ii) Let R be a DVR with maximal ideal m. Then $m = (\pi)$ for some $\pi \in R$. By unique factorisation of PIDs, we may write any $x \in R\backslash\{0\}$ uniquely as $\pi^n u$, with $n \geq 0$ and $u \in R^\times$. Then any $y \in K^\times$ can be written uniquely as $\pi^m u$, $u \in R^\times$, $m \in \mathbb{Z}$.

We then define $v(\pi^m u) = m$; it is easy to check that this is a well-defined valuation and $\mathcal{O}_K = R$. $\quad \square$

Examples: We revisit our previous examples.

- $\mathbb{Z}_{(p)}$ is a DVR, which is the valuation ring of $|\cdot|_p$ on $\mathbb{Q}$.

- $k[[t]]$, the ring of formal power series is a DVR, the valuation ring for the t-adic absolute value on $k((t))$.

- We also have a *non*-example. Let $K = k(t)$ be the rational function field, and define $K' = K(t^{1/2}, t^{1/4}, t^{1/8}, \dots)$. It can be shown that the t-adic valuation in fact extends to this larger field, and then that $v(t^{1/2^n}) = 1/2^n$, so the valuation cannot be discrete. The idea here is that we've found an infinite sequence of elements with positive valuation tending to zero.