

I Basic Theory

Lecture 1

Eg. $f(x_1, \dots, x_r) \in \mathbb{Z}[x_1, \dots, x_r]$, $f(x_1, \dots, x_r) = 0$?

$$\begin{array}{ccc} f(x_1, \dots, x_r) \equiv 0 & \text{mod } p \\ \text{"} & \text{"} & \text{mod } p^2 \\ \vdots & \vdots & \vdots \\ \text{"} & \text{"} & \text{mod } p^n \end{array}$$

Local fields packages all this information together.

§1 Absolute values

Definition 1.1: Let K be a field. An

absolute value on K is a function $|\cdot|: K \rightarrow \mathbb{R}_{\geq 0}$ such that:

- (i) $|x| = 0$ iff $x = 0$
- (ii) $|xy| = |x||y| \quad \forall x, y \in K$
- (iii) $|x+y| \leq |x| + |y| \quad \forall x, y \in K$
(triangle inequality)

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

Eg. • $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with usual abs. val. $|a+ib|$
 $= \sqrt{a^2+b^2}$. Write $|\cdot|_\infty$ for this abs. val.

• K any field. Trivial absolute value

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

- $K = \mathbb{Q}$, p prime

For $0 \neq x \in \mathbb{Q}$, write $x = p^n \frac{a}{b}$,

where $(a, p) = 1$, $(b, p) = 1$

The *p-adic absolute value* is defined to be

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

Axioms: (i) clear

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

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

(iii) wlog. $m \geq n$

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

3

An abs. val $|\cdot|$ on K induces a metric $d(x, y) = |x - y|$ on K , hence induces a topology on K .

Defn 1.2: Let $|\cdot|, |\cdot|'$ be absolute values on a field K . We say $|\cdot|, |\cdot|'$ are

equivalent if they induce the same topology. An equiv. class of abs. values is called a *place*.
Proposition 1.3: Let $|\cdot|, |\cdot|'$ be *(non-trivial)* abs. values

properties: ...

on K . The following are equivalent (TFAE)

(i) $|\cdot|$ and $|\cdot|'$ are equivalent.

(ii) $|x| < 1 \Leftrightarrow |x|' < 1 \quad \forall x \in K$.

(iii) $\exists c \in \mathbb{R}_{>0}$ s.t. $|x|^c = |x|' \quad \forall x \in K$.

Proof: (i) \Rightarrow (ii)

$$|x| < 1 \Leftrightarrow x^n \rightarrow 0 \text{ w.r.t. } |\cdot|$$

$$\stackrel{(i)}{\Leftrightarrow} x^n \rightarrow 0 \text{ w.r.t. } |\cdot|'$$

$$\Leftrightarrow |x|' < 1$$

9

(ii) \Rightarrow (iii)

$$|x|^c = |x|'$$

$$\Leftrightarrow c \log |x| = \log |x|'$$

$$\Leftrightarrow c = \frac{\log |x|'}{\log |x|} \text{ if } |x| \neq 1$$

Let $a \in K^\times$ s.t. $|a| < 1$ (exists since $|\cdot|$ non-trivial)

We need to show that

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

$$\text{Assume } \frac{\log |x|}{\log |a|} < \frac{\log |x|'}{\log |a|'}$$

$$\text{Choose } m, n \in \mathbb{Z} \text{ s.t. } \frac{\log |x|}{\log |a|} < \frac{m}{n} < \frac{\log |x|'}{\log |a|'}$$

$$\text{Then we have } n \log |x| < m \log |a|$$

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

$$\Rightarrow \left| \frac{x^n}{a^m} \right| < 1 \quad \text{and} \quad \left| \frac{x^n}{a^m} \right|' > 1$$

$$\therefore \log \left| \frac{x^n}{a^m} \right| < \log \left| \frac{x^n}{a^m} \right|'$$

converging for $\frac{\log |a|}{\log |a|} = \frac{\log |a|}{\log |a|}$ \square

(iii) \Rightarrow (i)

Remark: $|\cdot|_\infty$ on \mathbb{C} is not an abs. val. by our defn. Some authors replace Δ ineq. with

$$|x+y|^p \leq |x|^p + |y|^p \text{ for some fixed } p \in \mathbb{R}_{>0}$$

5 This course: Mainly interested in.

Defn 1.4: An absolute value $|\cdot|$ on K is said to be **non-archimedean** if it satisfies the **ultrametric inequality**:

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

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

Ex. $|\cdot|_\infty$ on \mathbb{R} is archimedean.

$|\cdot|_p$ is a non-archimedean abs. val. on \mathbb{Q} .

Lemma 1.5: Let $(K, |\cdot|)$ non-arch. $x, y \in K$.

If $|x| < |y|$, then $|x-y| = |y|$.

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

$$|y| \leq \max(|x|, |x-y|)$$

$$\Rightarrow |y| \leq |x-y|. \quad \square$$

Convergence is easier for non-arch. $|\cdot|$.

Proposition 1.6: Let $(K, |\cdot|)$ non-arch. and $(x_n)_{n=1}^{\infty}$ a sequence in K . If $|x_n - x_{n+1}| \rightarrow 0$, 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 s.t. $|x_n - x_{n+1}| < \varepsilon$ for $n > N$.

$$\begin{aligned} \text{Then for } N < n < m, |x_n - x_m| &= |(x_n - x_{n+1}) + (x_{n+1} - x_{n+2}) + \\ &\quad \dots + (x_{m-1} - x_m)| \\ &\leq \varepsilon \end{aligned}$$

$\Rightarrow (x_n)_{n=1}^{\infty}$ Cauchy.

In particular part: clear. \square

Eg. $p=5$. Construct sequence $(x_n)_{n=1}^{\infty}$ in \mathbb{Q} s.t.

$$(i) \quad x_n^2 + 1 \equiv 0 \pmod{5^n}$$

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

as follows.

Take $x_1 = 2$. Suppose have constructed x_n .

Let $x_n^2 + 1 = a5^n$ and set $x_{n+1} = x_n + b5^n$

$$\begin{aligned} \text{Then } x_{n+1}^2 + 1 &= x_n^2 + 2b5^n + b^25^{2n} + 1 \\ &= a5^n + 2b5^n + \underline{b^25^{2n}} \equiv 0 \pmod{5^n} \end{aligned}$$

We choose b s.t. $a + 2b \equiv 0 \pmod{5}$;

then we have $x_{n+1} + 1 \equiv 0 \pmod{5^{n+1}}$ as desired.

Now (ii) $\Rightarrow (x_n)_{n=1}^{\infty}$ is Cauchy.

Suppose $x_n \rightarrow l \in \mathbb{Q}$

Then $x_n^2 \rightarrow l^2$

But i) $\Rightarrow x_n^2 \rightarrow -1 \Rightarrow l^2 = -1 \nexists$.

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

Defn 1.7: The p -adic numbers \mathbb{Q}_p is the completion of \mathbb{Q} w.r.t $|\cdot|_p$.

Analogy with \mathbb{R}

$$\begin{array}{ccc} & & \mathbb{R} \\ & \nearrow^{|\cdot|_{\infty}} & \\ \mathbb{Q} & & \\ & \searrow_{|\cdot|_p} & \\ & & \mathbb{Q}_p \end{array}$$

For $x \in K$ and $r \in \mathbb{R}_{>0}$, define

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

$$\bar{B}(x, r) = \{ y \in K \mid |x - y| \leq r \}$$

Lemma 1.5: Let $(K, |\cdot|)$ be non-archimedean.

- (i) If $z \in B(x, r)$, then $B(z, r) = B(x, r)$
- (ii) If $z \in \bar{B}(x, r)$, then $\bar{B}(z, r) = \bar{B}(x, r)$
- (iii) $B(x, r)$ is closed
- (iv) $\bar{B}(x, r)$ is open

$$\begin{aligned} \text{Proof: (i) } |x - y| \leq r &\Rightarrow |z - y| = |(z - x) + (x - y)| \\ &\leq \max(|z - x|, |x - y|) \\ &= r \end{aligned}$$

$$\text{Thus } B(x, r) \subseteq B(z, r)$$

Reverse inclusion follows by symmetry.

(ii) same as i)

(iii) If $u \notin B(x, r)$. Then $B(x, r) \cap B(u, r) = \emptyset$

... $\cup B(x, r) \cup B(y, r) \cup \dots$

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

□

r