$\boxed{\text{LOCAL FIELDS}}$

register → graduate.studies@maths.ox.ac.uk

Assessment : weekly homework on the course webpage

→ tcclocalfields@gmail.com

§ Absolute values

Def An absolute value on a field K is a function

$$|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0} \quad \text{s.t.}$$

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

(ii) $|xy| = |x| \cdot |y|$

(iii) $|x+y| \leq |x| + |y|$.

If in addition $\forall x, y \in K$

(iii)' $|x+y| \leq \max(|x|, |y|)$

it is called <u>ultrametric</u> or non-Archimedean, otherwise Archimedean

<u>Immediate consequences</u> :

$|x^n| = |x|^n \quad n \in \mathbb{Z}$

$|1/x| = 1/|x|$ generally $|u| = 1$ for

$|1| = 1, \ |-1| = 1,$ every root of unity.

Ex $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$|\cdot| = |\cdot|_\infty$ usual absolute value (Archimedean)

Ex K any

$$|x| = \begin{cases} 1 & x \in K^\times \\ 0 & x = 0 \end{cases}$$ trivial absolute value

Ex K finite $(\mathbb{F}_p, \mathbb{F}_q)$, or $K = \overline{\mathbb{F}_p}$

All $x \neq 0$ are roots of unity $\Rightarrow$ every $|\cdot|$ is trivial.

Main examples:

<u>Ex</u> (p-adic absolute value) $K = \mathbb{Q}$, p prime,

pick real $\alpha \in (0,1)$

$$|\cdot| : \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$$

$$0 \longmapsto 0$$

$$p^n \frac{a}{b} \longmapsto \alpha^n$$

$(p \nmid a,b,\ n \in \mathbb{Z})$

Check $\longleftarrow$

(i) ✓

(ii) ✓

(iii)' $\left|p^n \frac{a}{b} + p^m \frac{u}{v}\right| =$

$$= \Big| p^{\min(m,n)} \underbrace{(\dots)}_{\text{no } p \text{ in denominator}} \Big| \leq \left|p^{\min(m,n)}\right|$$

$$= \alpha^{\min(m,n)} = \max(\alpha^n, \alpha^m).$$

✓

Ex (Order of vanishing at a)

$$K = \mathbb{C}(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f, g \in \mathbb{C}[x],\ g \neq 0 \right\}$$

function field in one variable ; fix $0<\alpha<1$.

Pick $a \in \mathbb{C}$, let

$$|\cdot|_a : K^\times \longrightarrow \mathbb{R}_{>0}$$

$$(x-a)^n \frac{f(x)}{g(x)} \longrightarrow \alpha^n$$

$f(a) \neq 0,\ g(a) \neq 0$

$$|\cdot|_\infty : \frac{f(x)}{g(x)} \longmapsto \alpha^{\deg g - \deg f}$$

§ Equivalence & Ostrowski's Thm

From now on all abs.values are non-trivial.

Def Two abs.values $|\cdot|_1$ and $|\cdot|_2$ are <u>equivalent</u> if $\exists c \in \mathbb{R}_{>0}$ s.t. $|x|_2 = |x|_1^c \quad \forall x \in K$.

Ex Different α's in examples above $\Rightarrow$ equivalent absolute values.

Def <u>Normalised</u> p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ is one with $\alpha = \frac{1}{p}$. $\quad \left|p^n \frac{a}{b}\right|_p = \frac{1}{p^n}$

<u>Ex</u> $|2^{10}3^2|_2 = 2^{-10}$

$|2^{10}3^2|_3 = 3^{-2}$

$|2^{10}3^2|_p = \underline{1}$ all $p \neq 2, 3$.

$|2^{10}3^2|_\infty = 2^{10}3^2$

So "$x, y \in \mathbb{Q}$ close to each other w.r.to $|\cdot|_p$"

$\iff$ $x \equiv y$ modulo high power of p."

<u>Thm</u> (Ostrowski) Every abs. value $|\cdot|$ on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some p.

<u>Proof</u> <u>Step 1</u> For $a, b \in \mathbb{Z}$, $a, b > 1$

$$|b| \leq \max\left(|a|^{\log_a b}, 1 \right) \quad (*)$$

Indeed, write b^n in base a,

$$b^n = c_m a^m + \ldots + c_1 a + c_0, \quad c_i \in \{0, \ldots, a-1\}$$

$$|b^n| \leq |c_m| \cdot |a|^m + \dots + |c_0|$$

$$\leq (m+1) \cdot M \cdot \max(|a|^m, \dots, |a|, |1|)$$

$\max(|1|, \dots, |a-1|)$

$$\leq (n \log_a b + 1) \cdot M \cdot \max(|a|^{n \log_a b}, 1)$$

Take n^{th} root, let $n \to \infty$ $\Rightarrow$ $(*)$

Step 2 Suppose $|\cdot|$ unbounded on $\mathbb{Z}$.

So $|b| > 1$ for some $b \in \mathbb{N}$.

For any $a > 1$,

$$1 < |b| \overset{(*)}{<} \max\left(|a|^{\log_a b}, 1 \right) \implies$$

- $|a| > 1$ for all $a > 1$.
- $|b| \leq |a|^{\log_a b} = |a|^{\frac{\log b}{\log a}}$

and (swap $a \leftrightarrow b$)

$$|a| \leq |b|^{\log_b a} = |b|^{\frac{\log a}{\log b}}$$

So
$$|b|^{\frac{1}{\log b}} \leqslant |a|^{\frac{1}{\log a}} \leqslant |b|^{\frac{1}{\log b}}$$

$\Rightarrow$ all equal to some constant $\Rightarrow$

$|a| = a^c$ some $c \in \mathbb{R}_{>0}$

$\Rightarrow |\cdot| \sim |\cdot|_\infty.$

Suppose

Step 3 $|\cdot|$ is bounded on $\mathbb{Z}$.

So $|a| \leqslant 1$ all $a \in \mathbb{N}$

If all $|a| = 1 \Rightarrow$ trivial abs. value

If some $|a| < 1$ write $a = p_1^{n_1} \cdots p_k^{n_k}$, get

$|p| < 1$, some prime $p \in \{p_1, \dots, p_k\}$

Enough to show $|q| = 1$ all primes $q \neq p$

$(\Rightarrow |\cdot| \sim |\cdot|_p)$.

Suppose not, so

$$|p| < 1, \ |q| < 1 \qquad p \neq q$$

Take n large, so

$$|p^n| < \tfrac{1}{2}, \ |q^n| < \tfrac{1}{2}$$

Write $1 = ap^n + bq^n \qquad a, b \in \mathbb{Z}$

$$1 = |1| \leq \underbrace{|a|}_{\leq 1} \cdot \underbrace{|p^n|}_{< \frac{1}{2}} + \underbrace{|b|}_{\leq 1} \cdot \underbrace{|q^n|}_{< \frac{1}{2}} < 1 \quad ↯$$

∎

<u>Note</u> For $x \in \mathbb{Q}^\times$ we have a product formula

$$\prod |x| = 1$$

all normalised abs. values on $\mathbb{Q}$

$|\cdot| = |\cdot|_\infty, |\cdot|_2, |\cdot|_3, \dots$

[$\leftarrow$ $x = \pm p_1^{a_1} \cdots p_k^{a_k}$

$|x|_\infty = p_1^{a_1} \cdots p_k^{a_k}$

$|x|_{p_i} = p_i^{-a_i}$

$|x|_q = 1 \quad q \neq p_i$

& take the product].

Analogues

K number field Every abs. value on K is either

$\sim |\cdot|_{\mathfrak{p}}$ $\quad \mathfrak{p} \subseteq \mathcal{O}_K$ prime ideal $\leftarrow$ non.-Arch

$\sim |\cdot|_{\sigma}$ $\quad \sigma : K \hookrightarrow \mathbb{C}$ embedding $\leftarrow$ Arch.

An equivalence class of abs. values on K is called a *place* ("real", "complex", "finite").

$\underline{K = \mathbb{C}(t)}$ Every abs. value on K which is trivial on $\mathbb{C}$ is either

$\sim |\cdot|_a \quad a \in \mathbb{C} \qquad \left[\ |(x-a)^n \frac{f}{g}|_a = \alpha^n\ \right]$

$\sim |\cdot|_\infty \qquad \left[\ |f|_\infty = \alpha^{-\deg f}\ \right]$

Generally $\underline{K = k(C)}$, C nonsing. proj. curve $/k = \overline{k}$

Every abs. value on K, trivial on k, is

$\sim |\cdot|_P \quad P \in C(k)$ point.

§ Independence

Lemma $|\cdot|_1, |\cdot|_2$ (non-trivial) abs. values on K. Then

(1) $|\cdot|_1 \sim |\cdot|_2 \iff$ (2) $|x|_1 < 1 \Rightarrow |x|_2 < 1$

Pf (1) $\Rightarrow$ (2) clear

(2) $\Rightarrow$ (1) Exc*.

More generally,

<u>Thm</u> $|\cdot|_1, \dots, |\cdot|_n$ inequivalent abs. values on K.

Then $\exists a \in K$ s.t. $|a|_1 > 1$ but $|a|_2 < 1, \dots, |a|_n < 1$.

<u>Pf</u> By induction on n.

$n = 2$ Lemma.

$n > 2$ Take $b, c \in K$ s.t

$|b|_1 > 1$, $|b|_2, \dots, |b|_{n-1} < 1$

$|c|_1 > 1$, $|c|_n < 1$.

If $|b|_n < 1$ $\quad a := b$

If $|b|_n = 1$ $\quad a := cb^r$ $\quad r$ large

If $|b|_n > 1$ $\quad a := \dfrac{cb^r}{1+b^r}$ $\quad r$ large ∎

<u>Cor</u> $\exists\, a \in K$ s.t. a is arb. close to 1 in $|\cdot|_1$ & arb. close to 0 in $|\cdot|_2, \dots, |\cdot|_n$.

<u>Pf</u> Pick b s.t. $|b|_1 > 1$, but $|b|_2 < 1, \dots, |b|_n < 1$ and let $a := \dfrac{b^r}{1+b^r}$ $\quad r$ large. ∎.

<u>Cor</u> (Weak Approximation)

$|\cdot|_1, \ldots, |\cdot|_n$ inequivalent abs. values on K

$a_1, \ldots, a_n \in K$, $\varepsilon > 0$.

Then $\exists a \in K$ s.t. all $|a - a_i|_i < \varepsilon$.

<u>Pf</u> Take b_i close to 1 in $|\cdot|_i$, to 0 in all others,

and let $a := a_1 b_1 + \ldots + a_n b_n$. ∎

<u>Note</u> For $K=\mathbb{Q}$ this is basically Chinese Remainder Theorem: $\exists a \in \mathbb{Q}$ s.t. $a \equiv a_i \mod p_i^{k_i}$

(plus real condition, e.g. $a<0$ or $1<a<1.01$)

<u>Note</u> Consequently, no relations between fin. many abs. values like

$$\prod |x|_i = 1 \quad \forall x \in K^\times$$

for finitely many abs. values.

§ Archimedean abs. values

<u>Thm</u> (Ostrowski II) If $|\cdot|$ Archimedean abs. value on K, there exists $i : K \hookrightarrow \mathbb{C}$ s.t. $|\cdot| \sim$ usual abs. value on $\mathbb{C}$ restricted to K.

§ Non-Archimedean abs. values & valuations

1.1 non-Archimedean abs. value on K, $\alpha \in (0,1)$

$\Rightarrow$ $v(x) = \log_\alpha |x|$ is a <u>valuation</u>

(and conversely $v \Rightarrow |x| := \alpha^{v(x)}$).

<u>Def</u> A <u>valuation</u> is a function $K^\times \xrightarrow{v} \mathbb{R}$ s.t.

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

(2) $v(x+y) \geq \min(v(x), v(y))$

- We extend v to K by letting $v(0) = \infty$.
- We call v and cv ($c \in \mathbb{R}_{>0}$ constant) equivalent
- v is a group hom. $K^\times \longrightarrow \mathbb{R}$, so its image is a subgroup of $\mathbb{R}$, called the <u>value group</u> of v. If it is discrete (i.e. $= c\mathbb{Z}$) we call v a <u>discrete valuation</u> <u>and normalised</u> if $v(K^\times) = \mathbb{Z}$.

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

$$v_p\left(p^n \frac{a}{b}\right) := n$$

p-adic valuation (normalised discrete).

Ex $K = \mathbb{C}(x)$, $a \in \mathbb{C}$

$$v_a\left((x-a)^n \frac{f}{g}\right) = n$$

order of vanishing at a (— " —)

$$v_\infty\left(\frac{f}{g}\right) = \deg g - \deg f$$

order of vanishing at ∞ (— " —)

Algebraic properties

$v : K^\times \longrightarrow \mathbb{R}$ valuation ($\leftrightarrow$ abs. value $|\cdot|$)

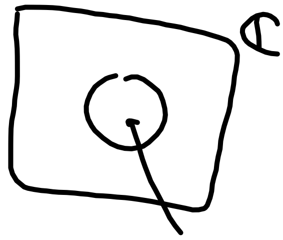
$\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$ is a ring. $(= \{x \in K \mid |x| \leq 1\}$ closed unit ball).

$\Big[\, v(x) \geq 0, v(y) \geq 0 \Rightarrow v(xy) = v(x) + v(y) \geq 0$

$v(x \pm y) \geq \min(v(x), v(y)) \geq 0. \,\Big]$.

This ring $\mathcal{O} = \mathcal{O}_v$ is called the <u>valuation ring</u> of v (or <u>ring of integers</u>).

<u>Note</u> Uses non-Archimedean, e.g.



$\mathcal{O} = \{x \in \mathbb{C} \mid |x| \leq 1\}$

Units

$$\mathcal{O}^\times = \{x \in K \mid v(x) = 0\}$$

not a ring.

($\leftrightarrow |x| = 1$ unit sphere).

and

$$\mathfrak{m} = \{x \in K \mid v(x) > 0\}$$ is an ideal in $\mathcal{O}$.

($\leftrightarrow |x| < 1$ open unit ball).

In particular $\mathfrak{m}$ is a maximal ideal, and the unique maximal ideal of $\mathcal{O}$.

So $\mathcal{O}$ is a local ring.

$k = \mathcal{O}/\mathfrak{m}$ is the residue field of v.

<u>Ex</u> $v_p : \mathbb{Q}^\times \twoheadrightarrow \mathbb{Z}$

$$p^n \frac{a}{b} \longrightarrow n \qquad (p \nmid a, b).$$

$K = \mathbb{Q}$

$\mathcal{O} = \mathcal{O}_v = \{ p^n \frac{a}{b} \mid n \geq 0 \} \cup \{0\}.$

numbers with no p's in the denominator; ring

$\mathcal{O}^\times = \{ \frac{a}{b} \mid p \nmid a, b \}$ units

$\mathfrak{m} = \{ p^n \frac{a}{b} \mid n > 0 \} \cup \{0\}$ max. ideal

$$\mathcal{O}/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$$

$$\frac{m}{n} \xmapsto[\text{reduce mod } p]{} \frac{\overline{m}}{\overline{n}} \in \mathbb{Z}/p\mathbb{Z}$$