Vorlesung 7.1.2026

Alg. Number Theory

Valued fields

Def.: A value on a field K is a function

$$|\ | : K \longrightarrow \mathbb{R}$$

s.t. ....

Def.: $|\ |_1 \sim |\ |_2 \iff$ they induce the same topology on K

Theorem: TFAE:

a) $|\ |_1 \sim |\ |_2$

b) $|x|_1 < 1 \implies |x|_2 < 1$

c) $|x|_2 < 1 \implies |x|_1 < 1$

d) $\exists\, s \in \mathbb{R}_{>0}$ s.t. $|x|_1 = |x|_2^s$

Approximation theorem (WAT)

Let $|\ |_1, \dots, |\ |_n$ be pairwise inequivalent values on K. Let $a_1, \dots, a_n \in K$. Let $\varepsilon > 0$. Then there exists $x \in K$ such that

$$|x - a_i|_i < \varepsilon.$$

Pf: **Claim:** $\exists\, z \in K$ with $|z|_1 > 1$ and $|z|_j < 1$, $j = 2, \dots, n$

Proof by induction:

<u>$n=2$:</u> $|\ |_1 \not\sim |\ |_2 \Rightarrow \exists\, \alpha \in K: |\alpha|_1 < 1, |\alpha|_2 \geq 1$

$\exists\, \beta \in K: |\beta|_2 < 1, |\beta|_1 \geq 1$

Then: Take $z := \beta/\alpha$.

<u>$n-1 \longrightarrow n$:</u> Let $z \in K$ with

$|z|_1 > 1, \ |z|_j < 1, \ j = 2, \ldots, n-1$

<u>Case 1:</u> $|z|_n \leq 1$

Let $y \in K$ with $|y|_1 > 1, \ |y|_n < 1$

Then $z^m y$ with $m \gg 0$ does the job.

<u>Case 2:</u> $|z|_n > 1$

$$t_m := \frac{z^m}{1+z^m} \xrightarrow{m \to \infty} 1$$

wrt. $|\ |_1$ and $|\ |_n$ because $|z|_1 > 1, |z|_n > 1$

$$t_m \xrightarrow{m \to \infty} 0$$

wrt. $|\ |_j$, $j = 2, \ldots, n$

because $|z|_j < 1$.

Now take $t_m y$ with $m \gg 0$.

So the claim is proved.

Now look at

$$\frac{z^m}{1+z^m} \xrightarrow{m\to\infty} 1 \quad \text{wrt. } |\ |_1$$

$$\frac{z^m}{1+z^m} \longrightarrow 0 \quad \text{wrt. } |\ |_j, \quad j = 2, \dots, n$$

So for fixed $i \in \{1, \dots, n\}$ we can contruct z_i with

$$|z_i|_j \text{ small}, \ j \neq i, \qquad |z_i - 1|_i \text{ small}$$

<u>Claim:</u> $x = a_1 z_1 + \dots + a_n z_n$ satisfies WAT.

<u>Pf:</u> $$|x - a_i|_i = |a_i(z_i - 1)| + \sum_{j\neq i} |a_j z_j|_i$$

$$\leq |a_i|_i \underbrace{|z_i - 1|_i}_{\text{small}} + \sum_{j \neq i} |a_j|_i \underbrace{|z_j|_i}_{\text{small}}$$

$$< \varepsilon$$ $\blacksquare$

<u>Relation with CRT</u> Let $K = \mathbb{Q}$.

Let $p_1, \dots, p_n$ be pairwise distinct primes.

Let $|\ |_i = |\ |_{p_i}$, i.e.

$$|x|_i = \left(\frac{1}{p_i}\right)^{v_{p_i}(x)}$$

Let $a_1, \dots, a_n \in \mathbb{Z}$. Then

$$|x - a_i|_i < \varepsilon \iff \left(\frac{1}{p_i}\right)^{v_{p_i}(x-a_i)} < \varepsilon.$$

Choose m big enough such that

$$\left(\frac{1}{p_i}\right)^m < \varepsilon, \quad i = 1, \dots, n$$

Solve by CRT

$$x \equiv a_i \pmod{p_i^m}, \quad i = 1, \dots, n.$$

Then x satisfies the WAT.

<u>Def.:</u> $|\,|$ is called <u>non-archimedean</u> or <u>finite</u>, if $|n|$ is bounded for $n \in \mathbb{N}$. Otherwise $|\,|$ is called <u>archimedean.</u>

<u>Theorem:</u> $|\,|$ is finite $\iff |x+y| \leq \max(|x|, |y|)$, $\forall x, y \in K$.

<u>Pf:</u> „$\Leftarrow$" $|n| = |1 + \dots + 1| \leq |1| = 1$

„$\Rightarrow$" Let $|n| \leq N$, $\forall n \in \mathbb{N}$.

$$|x+y|^n \leq \sum_{\nu=0}^{n} \left|\binom{n}{\nu}\right| |x|^\nu |y|^{n-\nu}$$

$$\leq N(n+1)|x|^n \quad , \text{ if } x,y \in K \text{ and } |x| \geq |y|$$

$$\Rightarrow |x+y| \leq N^{1/n}(n+1)^{1/n}|x| \qquad \text{To show: } |x+y| \leq |x|$$

$$\xrightarrow{n\to\infty} |x|$$

∎

<u>Theorem:</u> Each value of $\mathbb{Q}$ is equivalent to $|\ |_p$ or $|\ |_\infty$.

<u>Proof of the non-archimedean case:</u> Let $\|\ \|$ be a finite value on $\mathbb{Q}$. Then

$$\|n\| = \|1+\dots+1\| \leq \|1\| = 1. \qquad \forall n \in \mathbb{N}$$

Since $\|-1\| = \|1\| = 1$ we have

$$\|m\| \leq 1, \quad \forall\, m \in \mathbb{Z}.$$

Let p be a prime with $\|p\| < 1$. (p exists since otherwise $\|\ \|$ would be trivial).

Look at $\mathfrak{a} := \{a \in \mathbb{Z} \mid \|a\| < 1\} \trianglelefteq \mathbb{Z}$

by the strong Δ-inequality.

We have $p\mathbb{Z} \subseteq \mathfrak{a} \underset{1 \notin \mathfrak{a}}{\subsetneq} \mathbb{Z} \Rightarrow p\mathbb{Z} = \mathfrak{a}$.

Let $a \in \mathbb{Z}$, $a = bp^m$, $p \nmid b$.

Then $b \notin \mathfrak{p} \Rightarrow \|b\| = 1$

$$\Rightarrow \|a\| = \|p\|^m = |a|_p^s \quad \text{with} \quad s := -\frac{\log \|p\|}{\log |p|}$$

$$|a|_p^s = p^{-v_p(a)s} = p^{-ms}$$

$\blacksquare$

For the archimedean case look at [Neu, Th. 3.7]

$\blacksquare$

For a finite value $|\,|$ on K we define a valuation by

$$v(x) := -\log |x|, \quad \forall x \in K^*$$

$$v(0) := \infty$$

<u>Then:</u>

$$v(x) = \infty \iff x = 0$$

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

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

$$v_1 \sim v_2 \iff \exists s \in \mathbb{R}_{>0} : v_1 = sv_2$$

<u>Theorem:</u> $\mathcal{O} = \{x \in K \mid v(x) \geq 0\} \subseteq K$

$$= \{x \in K \mid |x| \leq 1\}$$

is an integral domain with unique maximal ideal

$$\mathfrak{m} = \{ x \in K \mid v(x) > 0 \}$$
$$= \{ x \in K \mid |x| < 1 \}$$

Pf: $\mathcal{O}$ is local because:

$$\mathcal{O}^\times = \{ x \in K \mid v(x) = 0 \}$$
$$= \{ x \in K \mid |x| = 1 \}$$

$\mathcal{O} \setminus \mathcal{O}^\times = \mathfrak{m}$ is an ideal. ∎

Remarks 1) Equivalent values (valuations) lead the the same valuation rings.

2) For $x \in K^\times$ we have:
Either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.

Definition: A valuation v on K is called discrete, if v has a minimal positive value s. ($s \in \mathbb{R}_{>0}$)

Then:
$$v(K^\times) = s\mathbb{Z}$$

Pf: Let $\pi \in K$ with $v(\pi) = s$. Then
$$v(\pi^n) = n\, v(\pi) = ns$$

Let $\alpha \in K^\times$. Let $v(\alpha) = st$

To show: $t \in \mathbb{Z}$.

$$v(\pi^n \alpha) = v(\pi^n) + v(\alpha) = s(t+n).$$

If $t \notin \mathbb{Z}$, then there exists $n \in \mathbb{Z}$ s.t. $0 < t+n < 1$. $\lightning$

$\blacksquare$

Def.: v is called normalized, if $s = 1$. Each $\pi \in K$ with $v(\pi) = 1$ is called a prime element or uniformizing element.

Lemma: Let v be a discrete normalized valuation on K. Let $\pi \in K$ with $v(\pi) = 1$. Then each $x \in K^\times$ can be uniquely written in the form

$$x = u\pi^m \quad \text{with } u \in \mathcal{O}^\times,\ m = v(x) \in \mathbb{Z}.$$

Pf: If $v(x) = m$, then

$$x = \pi^m \underbrace{(\pi^{-m} x)}_{\in \mathcal{O}^\times}$$

$\blacksquare$

Example: 1) $K = \mathbb{Q}$, $|\,| = |\,|_p$, p prime

$v = v_p$, $\pi = p$

$$\mathcal{O} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; a, b \in \mathbb{Z},\ (a,b) = 1,\ p \nmid b \right\}$$

$$\mathcal{O}^\times = \left\{ \frac{a}{b} \;\middle|\; (a,b) = 1,\ p \nmid ab \right\}$$

$$\mathfrak{m} = \left\{ \frac{a}{b} \;\middle|\; (a,b) = 1,\ p \mid a,\ p \nmid b \right\}$$

2) K number field, $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ prime ideal

$| \, | = | \, |_\mathfrak{p}$, $v = v_\mathfrak{p}$ defined by

$\alpha \in K$ $\qquad v_\mathfrak{p}(\alpha) = v_\mathfrak{p}(\alpha \mathcal{O}_K)$

Choose $\mathfrak{b} \trianglelefteq \mathcal{O}_K$ such $\mathfrak{p}\mathfrak{b} = \pi \mathcal{O}_K$ with $\mathfrak{p} \nmid \mathfrak{b}$. Then π is a prime element.

$$\mathcal{O} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathcal{O}_K,\ b \in \mathcal{O}_K \setminus \mathfrak{p} \right\}$$

$$\mathcal{O}^\times = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathcal{O}_K,\ a, b \in \mathcal{O}_K \setminus \mathfrak{p} \right\}$$

$$\mathfrak{m} = \left\{ \frac{a}{b} \;\middle|\; a \in \mathfrak{p},\ b \in \mathcal{O}_K \setminus \mathfrak{p} \right\}$$

<u>Theorem:</u> If v is a discrete valuation on K, then

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

is a PID. If v is normalised, then the set of ideals of K is given by

$$(\mathfrak{p}^n =) \ \pi^n \mathcal{O} = \{ x \in K \mid v(x) \geq n \} \quad , n \geq 0$$

Put

$$\mathfrak{p} = \pi \mathcal{O}.$$

Then

$$\mathfrak{p}^n / \mathfrak{p}^{n+1} \simeq \mathcal{O}/\mathfrak{p}.$$

<u>Pf:</u> As with $\mathbb{Z}_p$.

$$\mathfrak{p}^n / \mathfrak{p}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{p}$$

$$a\pi^n + \mathfrak{p}^{n+1} \longmapsto a + \mathfrak{p}. \qquad \blacksquare$$

Let K be a number field. For $\mathfrak{p}$ we have value $v_\mathfrak{p}$. For $\varsigma : K \hookrightarrow \mathbb{C}$ a real embedding we have

$$|\alpha|_\varsigma := |\varsigma(\alpha)|_\mathbb{R}$$

For $\sigma : K \hookrightarrow \mathbb{C}$ a complex embedding we have $|\alpha|_\sigma := |\sigma(\alpha)|_{\mathbb{C}}$.

Clearly, $\bar{\sigma}$ defines the same value.

<u>Th:</u> These are all values on K up to equivalence.

<u>Proposition:</u> For $\alpha \in K^\times$ one has

$$\prod_{\mathfrak{p}} |\alpha|_{\mathfrak{p}} \cdot \prod_{\tau : K \hookrightarrow \mathbb{C}} |\alpha|_\tau = 1.$$

$\blacksquare$