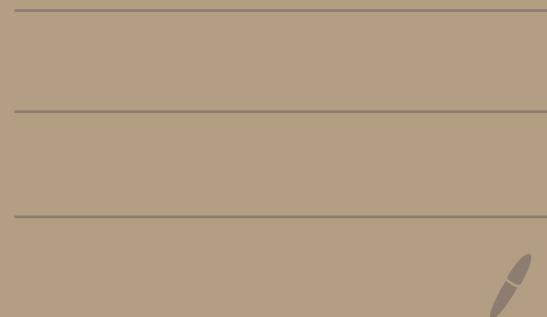


Vorlesung 7.1. 2026

Alg. Number Theory



Valued fields

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

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

s. t. \dots

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

Theorem: TFAE:

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

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

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

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:

$$\underline{n=2:} \quad \| \cdot \|_1 \not\sim \| \cdot \|_2 \Rightarrow \exists \alpha \in K: |\alpha|_1 < 1, |\alpha|_2 \geq 1$$

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

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

$n-1 \rightarrow n$: Let $z \in K$ with

$$|z|_n > 1, \quad |z|_j < 1, \quad j = 2, \dots, n-1$$

Case 1: $|z|_n \leq 1$

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

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

Case 2: $|z|_n > 1$

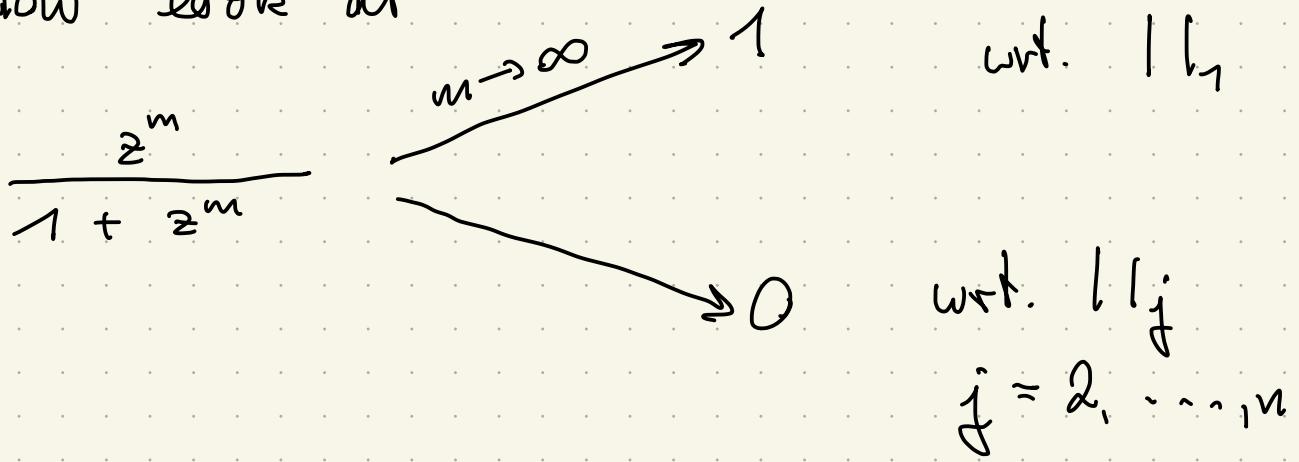
$$t_m := \frac{z^m}{1 + z^m} \xrightarrow{m \rightarrow \infty} 1 \quad \text{wrt. } \| \cdot \|_1 \text{ and} \\ | \cdot |_n \text{ because}$$

$$t_m \xrightarrow{m \rightarrow \infty} 0 \quad \text{wrt. } \| \cdot \|_j, \quad j = 2, \dots, n \\ \text{because } |z|_j < 1.$$

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

So the claim is proved.

Now look at



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

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

Claim: $x = a_1 z_1 + \dots + a_n z_n$ satisfies WAT.

$$\begin{aligned} \text{Pf: } |x - a_i|_i &= |a_i(z_i - 1) + \sum_{j \neq i} a_j z_j|_i \\ &\leq |a_i|_i \underbrace{|z_i - 1|_i}_{\text{small}} + \sum_{j \neq i} |a_j|_i \underbrace{|z_j|_i}_{\text{small}} \\ &< \varepsilon \end{aligned}$$



Relation with CRT 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.

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

Otherwise $||$ is called archimedean.

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

Pf: $\Leftarrow^n |n| = |1 + \dots + 1| \leq |1| = 1$

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

$$|x+y|^n \leq \sum_{r=0}^n |(n)| |x|^r |y|^{n-r}$$

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

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

$$\xrightarrow{n \rightarrow \infty} |x| \quad \blacksquare$$

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

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

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

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 $\|\cdot\|$ would be trivial).

$$\text{Look at } \mathcal{O} := \{a \in \mathbb{Z} \mid \|a\| < 1\} \subseteq \mathbb{Z}$$

by the strong
Δ-inequality.

$$\text{We have } p\mathbb{Z} \subseteq \mathcal{O} \nsubseteq \mathbb{Z} \Rightarrow p\mathbb{Z} = \mathcal{O}.$$

$1 \notin \mathcal{O}$

Let $a \in \mathbb{Z}_1$, $a = bp^m$, $p \neq b$.

Then $b \neq 0 \Rightarrow \|b\| = 1$

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



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



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

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

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

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

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

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

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

Theorem: $O = \{x \in K \mid v(x) \geq 0\} \subseteq K$
 $= \{x \in K \mid |x| \leq 1\}$

is an integral domain with unique maximal

ideal

$$\begin{aligned}m &= \{ x \in K \mid v(x) > 0 \} \\&= \{ x \in K \mid |x| < 1 \}\end{aligned}$$

Pf: \mathcal{O} is local because:

$$\begin{aligned}\mathcal{O}^x &= \{ x \in K \mid v(x) = 0 \} \\&= \{ x \in K \mid |x| = 1 \}\end{aligned}$$

$\mathcal{O} \setminus \mathcal{O}^x = m$ is an ideal.



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

2) For $x \in K^x$ 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 .

Then:

$$v(K^x) = s\mathbb{Z}$$

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

$$v(\pi^n) = nv(\pi) = ns$$

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

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

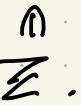
$$v(\pi^n \alpha) = v(\pi^n) + v(\alpha) = s(t+n).$$

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

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

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

 \mathbb{Z} .

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

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


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

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

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

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

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

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

$$|| = \left| \frac{1}{b_{\mathfrak{p}}} \right|, v = v_{\mathfrak{p}} \text{ defined by}$$

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

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

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

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

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

Theorem: 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

$$\left(\frac{f^n}{f^{n+1}} \right) \mathcal{O} = \{ x \in K \mid v(x) \geq n \}, \quad n \geq 0$$

Part

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

Then

$$\frac{\mathcal{O}^n}{\mathcal{O}^{n+1}} \cong \mathcal{O}/\mathcal{O}.$$

Pf: vts with \mathbb{Z}_p .

$$\frac{\mathcal{O}^n}{\mathcal{O}^{n+1}} \rightarrow \mathcal{O}/\mathcal{O}$$

$$a\pi^n + \mathcal{O}^{n+1} \mapsto a + \mathcal{O}.$$



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

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

For $\sigma: K \hookrightarrow \mathbb{C}$ a complex embedding

we have $|\alpha|_F = |\sigma(\alpha)|_F$.

Clearly, σ defines the same value.

Th: These are all values on K
up to equivalence.

Proposition: For $\alpha \in K^\times$ one has

$$\overline{\text{If } T} |\alpha|_F \cdot \overline{\text{If } \iota: K \hookrightarrow \mathbb{C}} |\alpha|_z = 1.$$

III