Non-archimedian abs. values on a number field K

<u>Recall:</u> $\mathfrak{p} \subset \mathcal{O}_K$ prime, then

$v_\mathfrak{p} : K^\times \to \mathbb{Z}$ the $\mathfrak{p}$-adic valuation

($x = u^n y$ for u - uniformizer of $\mathcal{O}_{K,\mathfrak{p}}$, $y \in \mathcal{O}_{K,\mathfrak{p}}^\times$, $n \in \mathbb{Z}$, then $v_\mathfrak{p}(x) = n$)

We define $|x|_\mathfrak{p} = \alpha^{v_\mathfrak{p}(x)}$ for some $0 < \alpha < 1$

<u>Prop 17.5</u> Let $\|\cdot\|$ be a non-trivial non-archimedian abs. value on a number field K. Then $\exists\, \mathfrak{p} \subset \mathcal{O}_K$ prime s.t. $\|x\| = |x|_\mathfrak{p}$ (for some α)

<u>Proof</u> Let $x \in \mathcal{O}_K$. Then $\exists\, a_i \in \mathbb{Z}$

$$x^n + a_1 x^{n-1} + \dots + a_n = 0$$

We know (Lemma 17.1) $\|a_i\| \leq 1$

If $\|x\| > 1$ then $\|x^n\| > \|a_i x^{n-i}\|$ for all $i \geq 1$, then

$$0 = \|x^n + a_1 x^{n-1} + \dots + a_n\| = \|x\|^n \neq 0$$

– contradiction

Hence $\|x\| \leq 1$ for all $x \in \mathcal{O}_K$

$\exists\, 0 \neq x \in \mathcal{O}_K$ s.t. $\|x\| < 1$

(otherwise $\forall\, 0 \neq x, y \in \mathcal{O}_K$ $\|\frac{x}{y}\| = 1$
$\Rightarrow \|\cdot\|$ is trivial)

Consider $\mathfrak{p} = \{x \in \mathcal{O}_K \mid \|x\| < 1\}$

$x \in \mathfrak{p},\ y \in \mathcal{O}_K \Rightarrow \|xy\| = \|x\| \cdot \|y\| < 1$
+ triangle inequal.
$\Rightarrow xy \in \mathfrak{p} \Rightarrow \mathfrak{p}$ is an ideal

$\mathfrak{p}$ is prime (exercise)

Localize at $\mathfrak{p}$: invert all elements
$x \in \mathcal{O}_K \setminus \mathfrak{p}$, i.e. all $x \in \mathcal{O}_K : \|x\| = 1$

$\forall\, x \in \mathcal{O}_{K,\mathfrak{p}}^{\times}$ $\|x\| = 1$

Let u be a uniformizer of $\mathfrak{p} \cdot \mathcal{O}_{K,\mathfrak{p}}$

$\forall\, y \in K$ $\quad y = u^n \cdot x,\quad x \in \mathcal{O}_{K,\mathfrak{p}}^{\times},\ n \in \mathbb{Z}$

Define $\alpha = \|u\|$. Then

$\|y\| = \alpha^n = \alpha^{\nu_\mathfrak{p}(y)} \Rightarrow \|\cdot\| = |\cdot|_\mathfrak{p}$ ☐

<u>Normalized abs. values</u>

$\exists$ a preferred choice of the const. α

One should take $\alpha = \mathrm{Norm}(\mathfrak{p})^{-1}$

so $\quad |x|_p = \mathrm{Norm}(p)^{-\nu_p(x)}$

Then we have the "product formula"

$\forall x \in K$

$$\prod_{p \in \mathrm{Spec}(\mathcal{O}_K)} |x|_p \cdot \prod_{\sigma: K \hookrightarrow \mathbb{C}} |\sigma(x)| = 1$$

<u>Proof</u> $\quad x \cdot \mathcal{O}_K = \prod p_i^{\nu_{p_i}(x)}$

$$\underset{\shortparallel}{\mathrm{Norm}}(x) = |N_{K/\mathbb{Q}}(x)| = \prod_{\sigma: K \hookrightarrow \mathbb{C}} |\sigma(x)|$$

$$\prod_i \mathrm{Norm}(p_i^{\nu_{p_i}(x)})$$

$$\Rightarrow \quad \prod_i \mathrm{Norm}(p_i)^{-\nu_{p_i}(x)} \cdot \prod_\sigma |\sigma(x)| = 1$$

$\square$

<u>18. Complete discrete valuation rings</u>

$\mathcal{O}_{K,p}$ is a DVR $\quad |x|_p = \alpha^{\nu_p(x)}$

$\mathfrak{m} \subset \mathcal{O}_{K,p}$ the max. ideal

take the completion $\rightsquigarrow \hat{\mathcal{O}}_{K,p}$ a complete ring

It can be described as follows:

$$\hat{\mathcal{O}}_{K,p} = \varprojlim_n \mathcal{O}_{K,p}/m^n$$

<u>Recall:</u> If we have a sequence of rings R_n, $n \geq 1$ and ring morphisms $\varphi_{n+1}: R_{n+1} \to R_n$ then

$$\varprojlim_n R_n = \{(r_n)_{n\geq 1} \mid r_n \in R_n,\ \varphi_{n+1}(r_{n+1}) = r_n \ \forall n \geq 1\}$$

There are natural map

$$\begin{aligned} \rho_n : \varprojlim R_n &\longrightarrow R_n \\ (r_n)_{n\geq 1} &\longmapsto r_n \end{aligned}$$

Then is the universal property:

for any ring T with maps $f_n : T \to R_n$, s.t. $\varphi_{n+1} \circ f_{n+1} = f_n$

$\exists$ unique map $f: T \to \varprojlim R_n$

s.t. $f_n = \rho_n \circ f$

For any DVR R consider

$$R_n = R/m^n, \quad \text{natural maps}$$

$$R_{n+1} = R/m^{n+1} \longrightarrow R/m^n = R_n$$

by the univ. prop. we get a map $f: R \longrightarrow \varprojlim R_n = \hat{R}$

Note: $\ker(f) = \bigcap_{n \geq 1} m^n = (0)$

(Lemma 13.5 in lecture 16)

We identify R with its image in $\hat{R}$

We would like to show that $\hat{R}$ is also a DVR.

The ideal $m \cdot \hat{R}$ is exactly the kernel of $\hat{R} \to R/m$

$\Rightarrow \hat{m} = m \cdot \hat{R}$ is a max. ideal in $\hat{R}$

Note: $x \in \hat{R} \setminus \hat{m}$, then the image of x in R/m^n is invertible for all n. $\Rightarrow x \in \hat{R}^\times$

$\Rightarrow \hat{m}$ is unique maximal ideal in $\hat{R}$

If $m = (u)$, then u generates $\hat{m}$ in $\hat{R}$.

If $(0) \neq I \subset \hat{R}$ ideal.

$\exists\ 0 \neq x \in I$ s.t. the image of x in $R/_{m^{k+1}}$ is non-zero for some k

$\Rightarrow x \notin \hat{m}^{k+1}$

Choose k: $I \subset \hat{m}^k$, but $I \not\subset \hat{m}^{k+1}$

$x \in I \setminus \hat{m}^{k+1}$

$x = u^k \cdot v, \quad v \in \hat{R}^\times$

$\Rightarrow I = (u^k) = \hat{m}^k$

Exercise: check that $\hat{R}$ is a domain

Conclusion: $\hat{R}$ is a DVR

Let K be the field of fract. of R and $\hat{K}$ the field of fract. of $\hat{R}$

$\hat{K} = \hat{R}[\frac{1}{u}]$

$\hat{K}$ is complete: if $x_n \in \hat{K}$ is a Cauchy sequence: $\exists n_0\ \forall n, m \geq n_0$

$|x_n - x_m| \leq 1$, i.e. $x_n - x_m \in \hat{R}$

$\Rightarrow \exists N > 0: \quad \forall n \quad u^N \cdot x_n \in \hat{R}$

also $u^N x_n$ is a Cauchy seq. in $\hat{R}$

$\underset{\hat{R} \text{ is complete}}{\Rightarrow} \exists \lim_{n\to\infty} u^N x_n = y \Rightarrow \lim_{n\to\infty} x_n = y/u^N$

$\Rightarrow \hat{K}$ is the completion of K

In the case of number fields $R = \mathcal{O}_{K,p}$; we get a complete DVR $\hat{\mathcal{O}}_{K,p}$ with field of fractions $K_p = \hat{K}$

<u>Lemma 18.1</u> The ring $\hat{\mathcal{O}}_{K,p}$ is compact as a metric space, i.e. every sequence contains convergent subsequence.

<u>Proof</u> $\hat{\mathcal{O}}_{K,p} = \varprojlim_n \mathcal{O}_K/p^n$

$\mathcal{O}_K/p^n$ is finite $\forall n$

($\mathcal{O}_K/p^n$ has a finite filtration by p^m/p^n, with quot. $\simeq \mathbb{F}_q = \mathcal{O}_K/p$)

Assume $(x_i)_{i\geq 1}$ is a sequence in $\hat{\mathcal{O}}_{K,p}$. Choose a subseq.

$(y_i^1)_{i\geq 1}$ s.t. $y_i^1 \equiv y_j^1 \pmod{p}\ \forall i,j$

$(y_i^2)_{i\geq 1}$ s.t. $y_i^2 \equiv y_j^2 \pmod{p^2}\ \forall i,j$.

....

take $z_i = y_i^i \quad i \geq 1$

Then $\forall n \geq 1 \quad z_{n+i} \equiv z_n \pmod{p^n}\ \forall i$

$\Rightarrow |z_{n+i} - z_n|_p < \alpha^n$

$\Rightarrow z_i$ converges in $\hat{\mathcal{O}}_{K,p}$ $\square$

<u>Corollary</u> K_p is a locally compact field (i.e. the closed ball $\{x \in K_p \mid |x|_p \leq 1\}$ is compact)

<u>Proof</u> This closed ball is exactly $\hat{\mathcal{O}}_{K,p}$ $\square$

<u>Remarks</u> 1) If we take the completion of $\mathbb{Z}$ w.r.t. $|\cdot|_\infty$, we get $\mathbb{Z}$.

But for $|\cdot|_p$ $\mathbb{Z} \neq \mathbb{Z}_p$

e.g. consider $x_n = \sum_{i=1}^{n} p^i$

Then $x_{n+1} \equiv x_n \pmod{p^{n+1}}$

$$\Rightarrow \quad x_n \xrightarrow[n \to \infty]{} \underset{\substack{\| \\ \sum_{i=1}^{\infty} p^i}}{x} \quad \text{in } \mathbb{Z}_p$$

More generally any series of the form $\sum_{i=1}^{\infty} a_i p^i$, $a_i \in \mathbb{Z}$ converges in $\mathbb{Z}_p$ (exercise)

2) Geometric intuition: if we consider $\mathbb{C}$ (with the usual topology), then every point has arbitrary small neighborhood – a disc of radius ε

In the arithmetic case we study $\operatorname{Spec} \mathcal{O}_K$, and $\hat{\mathcal{O}}_{K,p}$ may be considered as a ring of functions on a "formal disc" around $p \in \operatorname{Spec} \mathcal{O}_K$

3) Sometimes one can reduce the study of some classes of equations over $\mathbb{Q}$ to the study of the same equations over $\mathbb{Q}_p$ and $\mathbb{R}$.

A non-trivial example:

<u>Thm</u> (Hasse-Minkowski) An equation

$$\sum_{i=1}^{n} a_i X_i^2 = 0 \qquad (*)$$

with $a_i \in \mathbb{Q}$ has a non-zero solution $(x_1, \dots, x_n) \in \mathbb{Q}^n$ if and only if

1) $\forall\, p$ prime $\exists$ a non-zero solution $(y_1, \dots, y_n) \in \mathbb{Q}_p^n$ of $(*)$

2) $\exists$ a non-zero solution $(z_1, \dots, z_n) \in \mathbb{R}^n$ of $(*)$

This holds more generally for degree 2 equations over arbitrary num. field K, but it is <u>not</u> true for equations of deg. ≥ 3