Algebraic Number Theory

14. 1. 2026

$K \mid \mathbb{Q}$ number field

$$(0) \neq \mathfrak{p} \trianglelefteq \mathcal{O}_K \rightsquigarrow |\ |_{\mathfrak{p}}$$

$$\alpha \in K^\times, \quad |\alpha|_{\mathfrak{p}} = N(\mathfrak{p})^{-v_{\mathfrak{p}}(\alpha)}$$

These are non-archimedean

For $\rho : K \hookrightarrow \mathbb{R} \rightsquigarrow |\alpha|_\rho := |\rho(\alpha)|$

$\sigma : K \hookrightarrow \mathbb{C} \rightsquigarrow |\alpha|_\sigma := |\sigma(\alpha)|$

archimedean values

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

Completions

Let $(K, |\ |)$ be a valued field.

$$(\mathbb{Q}, |\ |_p) \overset{\text{completion}}{\rightsquigarrow} (\mathbb{Q}_p, |\ |_p)$$

$$(\mathbb{Q}, |\ |_\infty) \rightsquigarrow (\mathbb{R}, |\ |_\infty)$$

Examples:

1)

2) K number field, $|\ | = |\ |_{\mathfrak{p}}$

$$\rightsquigarrow (K_{\mathfrak{f}}, |\ |_{\mathfrak{f}})$$

$K_{\mathfrak{f}}$ is valued field, complete and we have the strong Δ- inequality.

Let $(K, |\,|)$ be non-archemedean. Let $\hat{K}$ be the completion. Let v the valuation associated with $|\,|$. Define

$$|\alpha| := \lim_{n\to\infty} |a_n| \, , \quad \text{where}$$

$$\alpha = (a_n)_{n\in\mathbb{N}} \bmod \mathcal{M}.$$

series tending to 0.

Since $\big| |a_n| - |a_m| \big| \leq |a_n - a_m|$
$$\downarrow \quad n \geq m \longrightarrow \infty$$
$$0$$

$(|a_n|)_{n\in\mathbb{N}}$ is a Cauchy series in $\mathbb{R}$, hence converges.

Define $\hat{v}(\alpha) := -\log|\alpha|$

$$= -\log \lim_{n\to\infty} |a_n|$$

$$= \lim_{n\to\infty} \left(-\log|a_n|\right) = \lim_{n\to\infty} v(a_n)$$

$$\alpha = (a_n)_{n\in\mathbb{N}} \bmod \mathcal{M}.$$

Remark: We have

$$\underline{\underline{v(a_n)}} = \hat{v}(a_n - \alpha + \alpha)$$

$$= \min\{\hat{v}(a_n - \alpha), \hat{v}(\alpha)\} = \underline{\underline{\hat{v}(\alpha)}},$$

for $n >> 0$.

Corollary: $v(K^\times) = \hat{v}(\widehat{K}^\times)$. In particular, if v is discrete, then also $\hat{v}$ is discrete.

Theorem: Let v be a discrete normalized valuation on K. Let $\widehat{K}$ be the completion and $\hat{v}$ the extension of v to $\widehat{K}$. Let

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

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

$$\widehat{\mathcal{O}} := \{x \in \widehat{K} \mid \hat{v}(x) \geq 0\} \supseteq \widehat{\mathfrak{p}}$$

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

Then:

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n \simeq \mathcal{O}/\mathfrak{p}^n, \quad \forall n \geq 1.$$

Beweis: Similar as for

$$\begin{array}{ccc} \mathbb{Q}_p & \supseteq & \mathbb{Q} \\ \rotatebox{90}{$\subseteq$} & & \rotatebox{90}{$\subseteq$} \\ \mathbb{Z}_p & & \mathbb{Z}_{(p)} \end{array}$$

$\blacksquare$

Theorem: Let $R \subseteq \mathcal{O}$ be a set of representatives of $\mathcal{O}/\mathfrak{p}$, $0 \in R$, let π be a prime element. Then each $x \in \hat{K}^\times$ has a unique representation as a convergent series

$$x = \pi^m (a_0 + a_1 \pi + \dots), \quad a_i \in R$$

$$a_0 \neq 0$$

$$m = v(x) \in \mathbb{Z}.$$

Proof: Let $x = \pi^m u$, $u \in \hat{\mathcal{O}}^\times$. Since

$$\hat{\mathcal{O}}/\hat{\mathfrak{p}} \simeq \mathcal{O}/\mathfrak{p}$$

there exists $a_0 \in R$ with

$$u \equiv a_0 \pmod{\hat{\mathfrak{p}}} \Rightarrow u = a_0 + \pi b_1, \, b_1 \in \hat{\mathcal{O}}$$

Suppose that we found $a_0, \dots, a_{n-1} \in R$ such that

$$u = a_0 + a_1 \pi + \dots + a_{n-1} \pi^{n-1} + \pi^n b_n,$$

$$b_n \in \hat{\mathcal{O}}$$

Write $b_n = a_n + \pi b_{n+1}$, $a_n \in R$

$$\Rightarrow \quad u = a_0 + \dots + a_n \pi^n + \pi^{n+1} b_{n+1} \qquad \blacksquare$$

Example: $K = \mathbb{Q}$, $v = v_p$

$R = \{0, 1, \dots, p-1\}$ is a set of representatives of

$$\mathbb{Z}_{(p)} / p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z}$$

Example: K number field, $\mathfrak{p} \trianglelefteq \mathcal{O}_K$, $\hat{K} = K_{\mathfrak{p}}$

Then we can identify $K_{\mathfrak{p}}$ with formal infinite series

$$\sum_{\nu \geq m} a_\nu \pi^\nu, \qquad v_{\mathfrak{p}}(\pi) = 1$$

$m \in \mathbb{Z}$

$\pi \in K$

$a_\nu \in R$

R is a set of representatives of $\mathcal{O}_K/\mathfrak{p}$; so $|R| < \infty$.

Explicit example: $K = \mathbb{Q}(i)$

$$\mathfrak{p} = (2+i) = \langle 5, 2+i \rangle_{\mathbb{Z}}$$

$$\begin{tikzcd}
K \arrow[d, dash] & & & \mathfrak{p} \arrow[dr, dash] & & \bar{\mathfrak{p}} \arrow[dl, dash] \\
\mathbb{Q} & \supseteq & \mathbb{Z} & \supseteq & 5\mathbb{Z} &
\end{tikzcd}$$

$$\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{Z}/5\mathbb{Z}$$

$$R = \{0, \ldots, 4\}$$

Do the $\mathfrak{p}$-adic expansion of $\alpha = 11$:

$$11 \equiv 1 \pmod{\pi} \qquad \pi = 2+i$$

$$\Rightarrow \quad 11 = 1 + \pi \cdot 2(2-i)$$

$$2(2-i) \equiv 3 \pmod{\pi}$$

$$\Rightarrow \quad 11 = 1 + \pi\left(3 + \pi(-i)\right)$$

$$= 1 + 3\pi + \pi^2(-i)$$

$$-i \equiv -i + (2+i) = 2 \pmod{\pi}$$

$$\Rightarrow \quad 11 = 1 + 3\pi + 2\pi^2 + O(\pi^3)$$

Hensels Lemma

Let K be a field which is complete with respect to a non-archimedean value. Let $\mathcal{O}$ be the valuation ring and $\mathfrak{p}$ the maximal ideal. Let $k := \mathcal{O}/\mathfrak{p}$

Def.: $f \in \mathcal{O}[x]$ is called primitive, if
$f \not\equiv 0 \pmod{\mathfrak{p}}$

Def.: $|f| := \max(|a_0|, \dots, |a_n|)$, where

$$f(x) = a_n X^n + \dots + a_1 X + a_0, \quad a_i \in K$$

Clearly: $f \in \mathcal{O}[x]$ prim. $\Longleftrightarrow$ $|f| = 1$.

Hensel Lemma: Let $f \in \mathcal{O}[x]$ be primitive.
If f mod $\mathfrak{p}$ has a decomposition

$$f(x) \equiv \bar{g}(x)\,\bar{h}(x) \pmod{\mathfrak{p}}$$

with coprime $\bar{g}, \bar{h} \in k[x]$, then

$$f(x) = g(x)\,h(x)$$

with $g, h \in \mathcal{O}[x]$, such that

$$\deg(g) = \deg(\bar{g})$$

$$g(x) \equiv \bar{g}(x) \pmod{\mathfrak{p}}$$

$$h(x) \equiv \bar{h}(x) \pmod{\mathfrak{p}}.$$

Corollary: Let $f \in \mathcal{O}[x]$ is primitive and suppose $(\bar{f}, \bar{f}') = 1$. Let $a \in \mathcal{O}/\mathfrak{p}$ such that $\bar{f}(a) = 0$. Then there exists $\alpha \in \mathcal{O}$ with

$$f(\alpha) = 0 , \quad \alpha \equiv a \pmod{\mathfrak{p}} . \qquad \blacksquare$$

<u>Example:</u> $\mu_{p-1} \subseteq \mathbb{Z}_p$

<u>Pf:</u> $x^{p-1} - 1 \in \mathbb{Z}_p[x]$ is primitive

$x^{p-1} - 1 \in \mathbb{F}_p[x]$ decomposes in linear factors; each $a \in \mathbb{F}_p^{\times}$ is a zero of $x^{p-1} - 1 \in \mathbb{F}_p[x]$.

We can lift by the corollary to Hensels Lemma.

<u>Corollary:</u> Let K be complete wrt. the non-archimedean value $|\ |$. Let

$$f(x) = a_n x^n + \dots + a_0 \in K[x] , \quad a_n a_0 \neq 0$$

be irreducible.

Then: $|f| = \max(|a_n|, |a_0|)$

In particular, if $f \in K[x]$ is normalized with $a_0 \in \mathcal{O}$, then

$$f \in \mathcal{O}[x] .$$

<u>Proof:</u> wlog $f \in \mathcal{O}[x]$ with $|f| = 1$.

Let $a_0, a_1, \dots, a_r, \dots, a_n$

$\uparrow$ the first with value 1.

$$\Rightarrow \quad f(x) \equiv x^{r}\left(a_r + \dots + a_n x^{n-r}\right) \pmod{\mathfrak{p}}$$

If $0 < r < n$, we would get a decomposition of f in $\mathcal{O}[x]$ by Hensels Lemma $\lightning$ $\blacksquare$

<u>SATZ</u>: Let K be complete with respect to $|\ |$. Let L/K be a field extension with $n := [L:K]$. Then $|\ |$ has a unique extension to L given by

$$|\alpha|_L := \sqrt[n]{|N_{L|K}(\alpha)|}, \quad \alpha \in L.$$

In addition, L is complete with respect to $|\ |_L$.

<u>Example:</u>

$$\begin{tikzcd} \mathbb{C} \ni \alpha = a+bi \arrow[d, dash, "2"] \\ \mathbb{R} \end{tikzcd}$$

$$|\alpha|_{\mathbb{C}} = \sqrt{|N_{\mathbb{C}|\mathbb{R}}(\alpha)|} = \sqrt{a^2+b^2}$$

<u>Proof of SATZ:</u> Only for non-archimedean values.

$$\begin{tikzcd} L \supseteq \mathcal{O}_L \arrow[d, dash] \\ K \supseteq \mathcal{O} \end{tikzcd}$$

L over K of degree n; $\mathcal{O}_L$ integral closure of $\mathcal{O}$ in L.

<u>Claim:</u> $\mathcal{O}_L = \{\alpha \in L \mid N_{L|K}(\alpha) \in \mathcal{O}\}$ $(\ast)$

Pf: „$\subseteq$" ✓

„$\supseteq$" Let $f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0 \in K[x]$ be the mipo of α.

$$\begin{tikzcd} L \arrow[d, dash, "m"] \\ K(\alpha) \arrow[d, dash] \\ K \end{tikzcd}$$

$$\Rightarrow N_{L|K}(\alpha) = \pm a_0^m, \quad m = [L : K(\alpha)].$$

$$\Rightarrow |a_0|^m \leq 1. \Rightarrow |a_0| \leq 1$$

$$\Rightarrow f(x) \in \mathcal{O}[x] \Rightarrow \alpha \in \mathcal{O}_L.$$

Proof of Δ-inequality: We have to show

$$|\alpha + \beta|_L \leq \max(|\alpha|_L, |\beta|_L) = |\beta|_L$$

wlog $|\alpha|_L \leq |\beta|_L$

$$\Updownarrow$$

$$\left|\frac{\alpha}{\beta} + 1\right|_L \leq 1$$

$$\left|\frac{\alpha}{\beta}\right|_L \leq 1 \Rightarrow \left|N_{L|K}\left(\frac{\alpha}{\beta}\right)\right| \leq 1$$

$$\Rightarrow N_{L|K}\left(\frac{\alpha}{\beta}\right) \in \mathcal{O}$$

$$\overset{(*)}{\Longrightarrow} \frac{\alpha}{\beta} \in \mathcal{O}_L$$

$$\Rightarrow \frac{\alpha}{\beta} + 1 \in \mathcal{O}_L$$

$$\overset{(*)}{\Longrightarrow} N_{L|K}\left(\frac{\alpha}{\beta} + 1\right) \in \mathcal{O}$$

$$\Rightarrow \sqrt[n]{\left| N_{L|K}\left(\frac{\alpha}{\beta}+1\right)\right|} \leq 1$$

$$\parallel$$

$$\left|\frac{\alpha}{\beta}+1\right|_L .$$

<u>Remark:</u> $\mathcal{O}_L$ = integral closure

= valuation ring in L wrt $|\,|_L$.