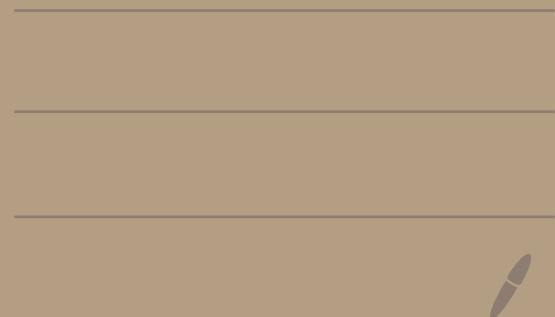


# Algebraic Number Theory

14. 1. 2026



$K/\mathbb{Q}$  number field

$$(0) \neq \varphi \leq 0_K \implies |\varphi|_p \quad \alpha \in K^*, \quad |\alpha|_p = N(\varphi) \xrightarrow{\sim} v_p(\alpha)$$

There are non-archimedean

$$\text{For } \varphi: K \hookrightarrow \mathbb{R} \implies |\alpha|_\varphi := |\varphi(\alpha)|$$
$$\sigma: K \hookrightarrow \mathbb{C} \implies |\alpha|_\sigma := |\sigma(\alpha)|$$

archimedean values

Relation:  $\prod_{\varphi} |\alpha|_\varphi \cdot \prod_{\sigma: K \hookrightarrow \mathbb{C}} |\alpha|_\sigma = 1.$

Completions

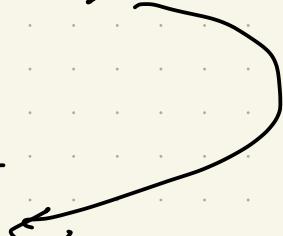
Let  $(K, ||)$  be a valued field.

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

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

Example:

1)



2)  $K$  number field,  $|| = ||_p$

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

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

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

$$|\alpha| := \lim_{n \rightarrow \infty} |\alpha_n|, \text{ where}$$

$$\alpha = (\alpha_n)_{n \in \mathbb{N}} \bmod \mathfrak{m}.$$

Since  $|\alpha_n| - |\alpha_m| \leq |\alpha_n - \alpha_m|$  series tending to 0.

$(|\alpha_n|)_{n \in \mathbb{N}}$  is a Cauchy series in  $\mathbb{R}$ , hence converges.  $\downarrow n \geq m \rightarrow \infty$

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

$$= -\log \lim_{n \rightarrow \infty} |\alpha_n|$$

$$= \lim_{n \rightarrow \infty} (-\log |\alpha_n|) = \lim_{n \rightarrow \infty} v(\alpha_n)$$

$$\alpha = (\alpha_n)_{n \in \mathbb{N}} \bmod \mathfrak{m}.$$

Remark: we have

$$\begin{aligned}\underline{v(a_n)} &= \hat{v}(a_n - \alpha + \alpha) \\ &= \min \{ \hat{v}(a_n - \alpha), \hat{v}(\alpha) \} = \underline{\hat{v}(\alpha)}, \\ &\text{for } n \gg 0.\end{aligned}$$

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

Theorem: Let  $v$  be a discrete, <sup>normalized</sup> valuation on  $K$ .

Let  $\hat{K}$  be the completion and  $\hat{v}$  the extension of  $v$  to  $\hat{K}$ . Let

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

$$\begin{aligned}\hat{\mathcal{O}} &:= \{ x \in \hat{K} \mid \hat{v}(x) \geq 0 \} \supseteq \hat{\mathcal{O}} \\ &= \{ x \in \hat{K} \mid |x| \leq 1 \}\end{aligned}$$

Then:

$$\frac{\mathcal{O}}{\hat{\mathcal{O}}^n} \cong \mathcal{O}/\mathcal{O}^n, \quad n \geq 1.$$

Beweis: Similar as for  $\mathbb{Q}_p \cong \mathbb{Q}$

UI

UI

$\mathbb{Z}_p$

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

■

Theorem: Let  $R \subseteq \mathcal{O}$  be a set of representatives of  $\mathcal{O}/\mathfrak{p}$ ,  $0 \in R$ . Let  $\pi$  be a prime element. Then each  $x \in \hat{\mathcal{O}}^\times$  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

$$u = a_0 + a_1 \pi + \dots + a_{n-1} \pi^{n-1} + \pi^n b_n, \quad b_n \in \hat{\mathcal{O}}$$

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

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

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

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

$$\frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$$

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

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

$$\sum_{r \geq m} a_r \pi^r, \quad v_{\mathfrak{p}}(\pi) = 1$$

$\pi \in K$   
 $m \in \mathbb{Z}$   
 $a_r \in \mathcal{R}$

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

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

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

$$K/\mathfrak{p} \cong \mathbb{Z}/5\mathbb{Z}$$

$$\mathbb{Q} \supseteq \mathbb{Z} \supseteq 5\mathbb{Z} \quad \mathcal{R} = \{0, \dots, 4\}$$

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

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

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

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

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

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

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

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

### Hensel's 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.:  $f \in \mathbb{O}[x]$  is called primitive, if  
 $f \not\equiv 0 \pmod{g}$

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

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

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

Hensel Lemma: Let  $f \in \mathbb{O}[x]$  be primitive.  
If  $f \pmod{g}$  has a decomposition

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

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

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

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

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

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

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

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

$$f(x) = 0, \quad x \equiv a \pmod{p} .$$



Example:  $\mu_{p-1} \subseteq \mathbb{Z}_p$

Pf:  $x^{p-1} - 1 \in \mathbb{Z}_p[x]$  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 Hensel's Lemma.

Corollary: Let  $K$  be complete wrt. the non-archimedean value  $|\cdot|$ . Let

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

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

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

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

↑ the first with value 1.

$$\Rightarrow f(x) \equiv x^r (a_0 + \dots + a_{n-r} x^{n-r}) \pmod{y}$$

If  $0 < r < n$ , we would get a decomposition of  $f$  in  $\mathbb{O}[x]$  by Hensel's Lemma  $\Downarrow$  

SATZ: Let  $K$  be complete with respect to  $|\cdot|$ .

Let  $L/K$  be a field extension with  $n := [L:K]$ .

Then  $|\cdot|$  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  $|\cdot|_L$ .

Example:  $\mathbb{C} \ni \alpha = a+bi$

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

Proof of SATZ: Only for non-archimedean values.

$L \supseteq \mathbb{O}_L$  integral closure of  $\mathbb{O}$  in  $L$ .

$$n \mid 1$$

$$K \supseteq \mathbb{O}$$

$$\underline{\text{Claim}}: \quad \mathbb{O}_L = \{ \alpha \in L \mid N_{L/K}(\alpha) \in \mathbb{O} \} \quad (\star)$$

Pf.:

$$n \in \mathbb{N} \quad \checkmark$$

Let  $f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0 \in K[x]$   
be the minps of  $\alpha$ .

$$\begin{pmatrix} L \\ K(\alpha) \end{pmatrix}^m$$

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

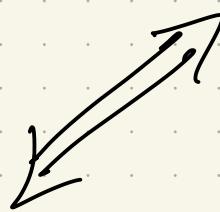
$$\Rightarrow |a_0|^m \leq 1 \Rightarrow |a_0| \leq 1$$

$$\Rightarrow f(x) \in O[x] \Rightarrow \alpha \in O_L. \quad \boxed{}$$

Proof of  $\Delta$ -inequality: We have to show

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

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



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

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

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

$$\stackrel{(*)}{\Rightarrow} \frac{\alpha}{\beta} \in O_L$$

$$\stackrel{(*)}{\Rightarrow} \frac{\alpha}{\beta} + 1 \in O_L$$

$$\stackrel{(*)}{\Rightarrow} N_{L/K} \left( \frac{\alpha}{\beta} + 1 \right) \in O$$

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

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

Remark:  $\mathcal{O}_L$  = integral closure  
 = valuation ring in  $L$  w/  $|\cdot|_L$ .