

Lectures 2-5 of Berger's IHP notes

Lecture 2 Hensel's lemma & Newton polygon.

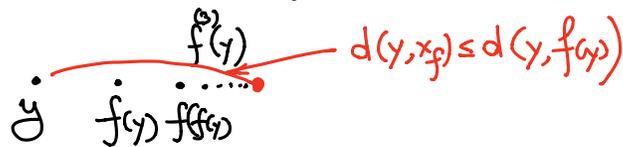
Theorem 2.1 : (Fix point theorem)

Let X be a complete metric space & $f: X \rightarrow X$ satisfies
 $d(f(x), f(y)) \leq \lambda \cdot d(x, y)$ for some $0 \leq \lambda < 1$.

Then f admits a unique fixed pt x_f .

(proof: Start w/ any $x, x, f(x), f(f(x)), \dots$
 if $y \neq x$ $y, f(y), f(f(y)), \dots$ \rightarrow same limit)

Moreover, if the metric is an ultrametric (satisfies strong triangle inequality)
 then for every $x \in X$, $d(y, x_f) = d(y, f(y))$



Theorem 2.2 (Hensel's lemma; Newton method form)

• A domain, complete for a valuation $\text{val}(\cdot)$, which is ≥ 0 on A .

e.g. \mathbb{Z}_p , $\mathbb{Z}_p[x]^\wedge \leftarrow \text{val}(\sum_{n \geq 0} a_n x^n) = \min_n \text{val}(a_n)$

K CDVF with residual field $\mathbb{F}_p(x_1, \dots, x_n)$, $A = (\text{subring of } \mathcal{O}_K)^\wedge$.

• If $P(x) \in A[x]$ & $\alpha_0 \in A$, s.t.

① $P(\alpha_0)/P'(\alpha_0)^2 \in A$

② $\text{val}(P(\alpha_0)/P'(\alpha_0)^2) = \varepsilon > 0$,

e.g. $P(x) \in \mathcal{O}_K[x]$

& $\begin{cases} P(\alpha_0) \bmod \mathfrak{m}_K = 0 \\ P'(\alpha_0) \bmod \mathfrak{m}_K \neq 0 \end{cases}$

Then $\exists \alpha \in A$ s.t. $P(\alpha) = 0$ and $\text{val}(\alpha - \alpha_0) \geq \varepsilon + \text{val}(P'(\alpha_0))$

i.e. if α_0 is so that $P(\alpha_0)$ is small, then α_0 is very close to a zero of $P(x)$

Proof is in Berger's notes, instead, we explain the proof of its generalization

"Improving a factorization $P \approx QR$ to $P = \tilde{Q}\tilde{R}$ " when $A = \mathcal{O}_K$.

• Gauss norm on $K[x]$, $\|a_0 + a_1x + \dots + a_nx^n\|_G := \max |a_i|$

Set $W_d := K[x]^{\deg \leq d-1}$

• If $Q(x)$ & $R(x)$ are polynomials of $\deg \leq m$ & $\leq n$, resp.

consider $\theta_{Q,R}: W_n \times W_m \longrightarrow W_{m+n-1}$

$$(U, V) \longmapsto QU + RV$$

$$\text{res}(Q,R) := \det(\theta_{Q,R})_{\text{basis } 1, x, x^2, \dots}$$

Rmk: When $P(x) = a_0 + a_1x + \dots + a_nx^n$,

$$Q(x) = x - \alpha_0, \rightsquigarrow P(x) = (x - \alpha_0) \cdot R(x) + P(\alpha_0)$$

$$\theta_{Q,R}: K \times W_{n-1} \longrightarrow W_n$$

$$(a, V) \longmapsto a \cdot R(x) + (x - \alpha_0) \cdot V$$

To compute $\det \theta_{Q,R}$, may change variable $x \mapsto x + \alpha_0$,

$$\& \text{ assume } \alpha_0 = 0 \Rightarrow R(x) = a_1 + a_2x + \dots + a_{n-1}x^{n-1}$$

$$\text{res}(\theta_{Q,R}) = \det \begin{pmatrix} a_1 & & & & \\ a_2 & 1 & & & 0 \\ \vdots & & \ddots & & \\ a_{n-1} & 0 & \dots & 1 & \end{pmatrix} = a_1 = \underline{P'(\alpha_0)}$$

Theorem 2.3: (Improve a factorization $P \approx QR$ into $P = \tilde{Q}\tilde{R}$)

* $P, Q, R \in \mathcal{O}_K[x]$ $\deg P = m+n$, $\deg Q = m$, $\deg R = n$

* $0 \leq \lambda < 1$.

Assume • $\deg(P - QR) \leq m+n-1$

• $\|P - QR\|_G \leq \lambda \cdot |\text{res}(Q,R)|^2 \iff \left| \frac{P(\alpha_0)}{P'(\alpha_0)^2} \right| \leq \lambda$

when $Q = x - \alpha_0$, $P = QR + P(\alpha_0)$

Then there exist polynomials \tilde{Q} and \tilde{R} such that

(1) $\deg(\tilde{Q} - Q) \leq m-1$ and $\|Q - \tilde{Q}\|_G \leq \lambda \cdot |\text{res}(Q,R)|$

(2) $\deg(\tilde{R} - R) \leq n-1$ and $\|R - \tilde{R}\|_G \leq \lambda \cdot |\text{res}(Q,R)|$

(3) $P = \tilde{Q}\tilde{R}$.

Proof: If $\text{res}(Q,R) = 0$, we are done as $P = QR$.

Assume $\rho := |\text{res}(Q,R)| \neq 0$ & $\rho < 1$.

Then $\theta_{Q,R}: W_n \times W_m \rightarrow W_{m+n}$ is invertible.

Hope: $P = (Q+V)(R+U)$

$$\Leftrightarrow \underbrace{QU + RV}_{\theta_{Q,R}(U,V)} = QR - P + UV$$

Consider $\varphi: W_n \times W_m \rightarrow W_n \times W_m$

$$(U, V) \mapsto \theta_{Q,R}^{-1}(QR - P + UV)$$

so that $\varphi(U, V) = (U, V)$

$$\Leftrightarrow \theta_{Q,R}(U, V) = QR - P + UV \quad \checkmark$$

Want to use fixed point theorem on

$$\varphi \subset B(0, \lambda\rho) \subseteq W_n \times W_m$$

$$\{ (U, V) \in W_n \times W_m, \|U\|_G \leq \lambda\rho, \|V\| \leq \lambda\rho \}$$

Need to check: ① $\|U\|_G \leq \lambda\rho, \|V\|_G \leq \lambda\rho \Rightarrow \|\varphi(U, V)\|_G \leq \lambda\rho$

$$\|\theta_{Q,R}^{-1}(QR - P + UV)\|_G \leq \rho^{-1} \|QR - P + UV\|_G$$

$$\leq \rho^{-1} \min\{\lambda\rho^2, (\lambda\rho)^2\} \leq \lambda\rho$$

② If $(U, V), (U', V') \in B(0, \lambda\rho)$, then

$$\|\varphi(U, V) - \varphi(U', V')\|_G \leq \lambda \cdot \|(U - U', V - V')\|_G$$

$$\hookrightarrow = \|\theta_{Q,R}^{-1}(UV - U'V')\|_G$$

$$\leq \rho^{-1} \|UV - U'V'\|_G = \rho^{-1} \|U(V - V') + V(U - U')\|_G$$

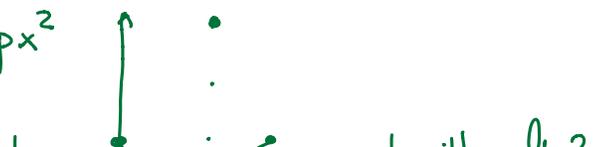
$$\leq \rho^{-1} \cdot \lambda\rho \cdot \|(U - U', V - V')\|_G. \quad \checkmark \quad \square$$

Newton polygon K completely valued field, $v_K(-)$

$$P(x) = a_0 + a_1x + \dots + a_d x^d \in K[x]$$

$NP(P) =$ lower convex hull of $(0, v_K(a_0)), (1, v_K(a_1)), \dots, (d, v_K(a_d))$

E.g. $P(x) = p + x + p^3 x^2 + p x^2$



slope $\frac{1}{2}$ with mult. 2.

Theorem 2.4. If all the slopes of $NP(P)$ are $\lambda_1 < \dots < \lambda_r$ with mult. m_1, \dots, m_r then $P(x)$ has exactly m_i zeros with valuation $-\lambda_i$

Cor: $NP(P \cdot Q) = NP(P) \# NP(Q)$

↑ This is to union all slopes of $NP(P)$ & $NP(Q)$ with multiplicity & then reorder them to redraw a Newton polygon.

(b/c $\{ \text{zeros of } P \cdot Q \} = \{ \text{zeros of } P \} \cup \{ \text{zeros of } Q \})$

Proof: Equivalent to show the inverse statement:

Assume that $P(x)$ has exactly m_i zeros with valuation $-\lambda_i : \alpha_i^{(1)}, \dots, \alpha_i^{(m_i)}$

May assume $P(0) = 1$

Let NP be the ^{convex} polygon starts at $(0,0)$

with slopes λ_i (mult. m_i)

$$\Rightarrow P(x) = \prod_{i,j} (1 - (\alpha_i^{(j)})^{-1} x) = a_0 + a_1 x + \dots + a_n x^n$$

$$a_n = \pm \sum \text{product of } n \text{ numbers in } (\alpha_i^{(j)})^{-1} \text{'s.}$$

$$\Rightarrow v_K(a_n) \geq NP \text{ at } n$$

Equality is achieved precisely at

$$n = m_1 + \dots + m_k$$

b/c in this case, the leading term is

$$\left(\prod_{1 \leq i \leq k} \alpha_i^{(j)} \right)^{-1}$$

□

E.g.

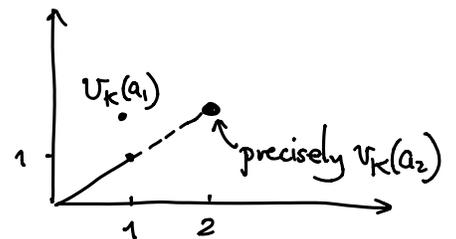
α_1	, β_1	val -1
α_2		val -2
α_3		val -3

$$\Rightarrow -a_1 = \alpha_1^{-1} + \beta_1^{-1} + \alpha_2^{-1} + \alpha_3^{-1}$$

$$\Rightarrow v_K(a_1) \geq 1$$

$$a_2 = \alpha_1^{-1} \beta_1^{-1} + \alpha_1^{-1} \alpha_2^{-1} + \alpha_1^{-1} \alpha_3^{-1} + \beta_1^{-1} \alpha_2^{-1} + \beta_1^{-1} \alpha_3^{-1} + \alpha_2^{-1} \alpha_3^{-1}$$

leading term



Cor: $P(x) = \prod P_i(x)$ with $P_i(x)$ having exactly the zeros with val $-\lambda_i$.

Lecture 3 Holomorphic functions

- $E \subseteq \mathbb{C}_p$ closed subfield.
- $f(x) = \sum_{n \in \mathbb{Z}} a_n x^n$ formal Laurent series
- $I \subset \mathbb{R} \cup \{\infty\}$ interval.

$$\leadsto A(I) := \{z \in \mathbb{C}_p, \text{val}(z) \in I\}$$

Definition: We say $f(x)$ is holomorphic on the annulus $A(I)$ if the following equivalent conditions hold:

(1) $f(x)$ converges at each $z \in A(I)$

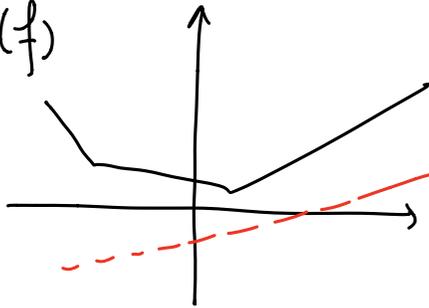
(2) $\text{val}_p(a_n) + n\mu \rightarrow \infty$ as $n \rightarrow \pm\infty$ for every $\mu \in I$.

$\text{val}_p(a_n z^n)$ with $\text{val}_p(z) = \mu$

\rightarrow e.g. $I = [r, s]$ just need $\text{val}_p(a_n) + nr \rightarrow \infty$ as $n \rightarrow +\infty$

& $\text{val}_p(a_n) + ns \rightarrow \infty$ as $n \rightarrow -\infty$

(3) $NP(f)$



\leftarrow consider lines with slope $-\mu$ with $\mu \in I$.

$\forall \mu \in I$, $NP(f)$ lies above a line with slope $-\mu$.

• $\mathcal{H}(I) := \{\text{holomorphic functions on } A(I)\} \leftarrow \forall \mu \in I \text{ valuation}$

\cup

$$V(f; \mu) := \min_{n \in \mathbb{Z}} (\text{val}_p(a_n) + n\mu)$$

• $\mathcal{B}(I) := \{\text{bounded holomorphic functions on } A(I)\}$

\leftarrow meaning $\{V(f; \mu) ; \mu \in I\}$ is bounded below

when $\infty \in I$, only consider power series.

* $\mathcal{H}(I) = \text{Fréchet complete for } (V(\cdot; \mu))_{\mu \in I}$.

i.e. $f_i \rightarrow f$ if $\forall \mu \in I, V(f_i - f; \mu) \rightarrow \infty$

* If I is closed, $\mathcal{H}(I) = \mathcal{B}(I)$.

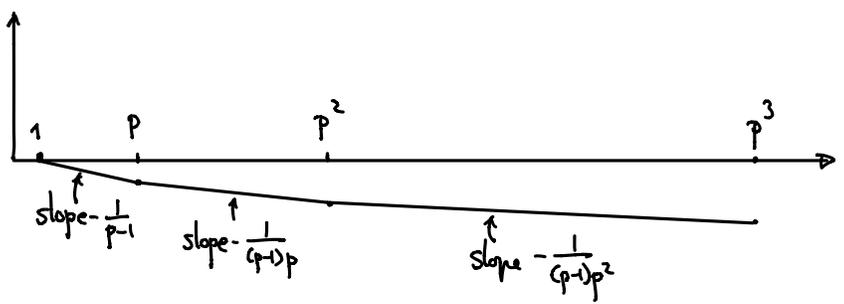
In general, $\mathcal{H}(\bar{I}) \subseteq \mathcal{B}(I) \subseteq \mathcal{H}(I)$

closure of I .

Examples: $I = (0, +\infty]$, i.e. $A(I) = \text{open disk}$.

① $f(x) = \log(1+x) = x - \frac{x^2}{2} + \dots + (-1)^{n-1} \frac{x^n}{n}$

$NP(f) =$



zeros of $\log(1+x)$ are precisely $\sum_{p^n}^j -1$'s. note: $v_p(\sum_{p^n} -1) = \frac{1}{p^{n-2}(p-1)}$.

$f(x) \in \mathcal{H}(I)$ but not bounded.

Remark: $\Phi_n = n^{\text{th}}$ cyclotomic polynomial = $\frac{(1+x)^{p^n} - 1}{(1+x)^{p^{n-1}} - 1}$

Then $\log(1+x) = x \cdot \prod_{n \geq 1} \frac{\Phi_n(x)}{p}$

② $f(x) = 1 + x + x^2 + \dots$ $f(x) \in \mathcal{B}(I)$ is bounded
but $f(x) \notin \mathcal{H}([0, +\infty])$

③ $f(x) = \sum p^n x^{n^2}$, $f(x) \in \mathcal{H}([0, +\infty])$

Theorem 3.2 If $f(x) \in \mathcal{H}(I)$, $s \in I$, then

width of slope $-s$ segment in $NP(f) = \#$ of zeros of $f(x)$ with $\text{val}_p^n s$.

We can factor $f(x) = g_s(x)P(x)$ unique up to scalar multiple

s.t. $g_s(x)$ has all zeros with $\text{val}_p^n s$

$P(x)$ has no zeros with $\text{val}_p^n s$.

Cor. If $f(x) \in \mathcal{H}(I)$, then $f(x)$ has finitely many zeros in $A(I) \Rightarrow f(x) \in \mathcal{B}(I)$.

if K has discrete valuation

Proof: Say $r = \inf(I)$ & $s = \inf(I)$

Then $f(x) \in \mathcal{H}(I)$ is bounded $\Leftrightarrow \text{val}_p(a_n) + nr$ is bounded below when $n \rightarrow +\infty$

• Assume K is CDVF.

A divisor D on $A(I)$ is a formal sum $\sum_{z \in A(I)} n_z \cdot [z]$ $n_z \in \mathbb{Z}$

s.t. for each $J \subseteq I$ closed, $\sum_{z \in A(J)} |n_z|$ is finite

Then each $f(x) \in \mathcal{H}(I) \rightarrow \text{div}(f) = \sum z \text{ zeros of } f$ is a divisor on $\mathcal{H}(I)$.

Theorem 3.7 (Chinese remainder theorem)

Suppose we are given • an effective divisor $D = \sum_{z \in A(I)} n_z \cdot [z]$ on $A(I)$

• polynomials Q_s for each $s \in I$ s.t. $\deg Q_s < \sum_{z \in A(I \setminus \{s\})} n_z$.

Then $\exists f \in \mathcal{H}(I)$ s.t. $f \equiv Q_s \pmod{\prod_{z \in A(I \setminus \{s\})} (x-z)^{n_z}}$

Corollary 3.8. The ring $\mathcal{H}(I)$ is a Bézout domain,

i.e. every finitely generated ideals are principal.

Example: $\mathcal{H}((0, +\infty])$ is not a PID

Recall $\log(1+x) = x \cdot \prod_{n \geq 1} \frac{\Phi_n(x)}{p}$

$$I = \left(\prod_{n \geq n_0} \frac{\Phi_n(x)}{p} \quad ; \text{ for all } n_0 \geq 1 \right)$$

Lecture 5 Ax and Ax-Sen-Tate's theorem

Theorem 5.1. If F is a complete valued field, then \widehat{F}^{alg} is algebraically closed.

Proof: Prove by induction on degree that every polynomial $P(x) \in \widehat{F}^{\text{alg}}[x]$ of degree ≥ 1

• May assume that $P(x) \in \mathcal{O}_{\widehat{F}^{\text{alg}}}[x]$ is monic has a root.

(o/w can use NP(P) to factor it)

Write $P(x) = \lim P_n(x)$ for monic $P_n(x) \in \mathcal{O}_{\widehat{F}^{\text{alg}}}[x]$

Pick one root α_n of P_n so $P(\alpha_n) \rightarrow 0$

* If $P'(\alpha_n) \not\rightarrow 0$, then $\exists n$ s.t. $P(\alpha_n)$ small but $P'(\alpha_n)$ not too small

Hensel's lemma $\Rightarrow \exists \alpha \in \mathcal{O}_{\widehat{F}^{\text{alg}}}$ a zero of P

* If $P'(\alpha_n) \rightarrow 0$, then inductive hypo $\Rightarrow P'(x)$ decomposes

$\Rightarrow \alpha_n \rightarrow$ a zero of $P(x)$, say α
 Then $P(\alpha)$ is the limit of $P(\alpha_n)$, which is also 0. \checkmark

Theorem 5.2 If F is a valued field of char $p > 0$, then F^{sep} is dense in F^{alg} .

Proof: If $y \in F^{\text{alg}}$, then $y^{p^n} = \alpha \in F^{\text{sep}}$ for some n .

WLOG $v(\alpha) \geq 0$.

Take $\pi \in F$ with $v(\pi) > 0$

Let y_i be a root of $y^{p^n} - \pi^i y - \alpha = 0$ $\Rightarrow y_i \in F^{\text{sep}}$ & $v(y_i) \geq 0$

$$\left. \begin{aligned} \Rightarrow y^{p^n} &= \alpha \\ y_i^{p^n} &= \alpha + \pi^i y_i \end{aligned} \right\} \Rightarrow (y - y_i)^{p^n} = \pi^i y_i$$

$\Rightarrow y_i \rightarrow y$ as $i \rightarrow \infty$

Theorem 5.3 (Ax-Sen-Tate)

If F is a complete p -adic field, and if $F \subset K \subset F^{\text{alg}}$ (K a possibly infinite ext'n of F)
 then $(\widehat{F^{\text{alg}}})^{\text{Gal}(F^{\text{alg}}/K)} = \widehat{K}$

Proof: Clearly, $\widehat{K} \subseteq \widehat{F^{\text{alg}}}^{G_K}$

Why do we care?

Answer: Making sure that take completion is okay with Galois theory.

$$\begin{array}{ccccc} \mathbb{Q}_p^{\text{alg}} & F^{\text{alg}} & \rightsquigarrow & \widehat{F^{\text{alg}}} & \\ | & | \text{) } G_K & & | \text{) } "G_K" & \\ \mathbb{Q}_p(\mu_{p^\infty}) & K & \longrightarrow & \widehat{K} & \\ | & | & & | \text{) } "Gal(\widehat{K}/F)" & \\ \text{e.g. } \mathbb{Q}_p & F & & F & \end{array}$$

Now show the opposite inclusion

If $\alpha \in F^{\text{alg}}$, let $\Delta_K(\alpha) := \inf_{g \in G_K} \text{val}_p(g(\alpha) - \alpha)$ $\text{val}_p(p) = 1.$

(so if $\alpha \in K$, then $\Delta_K(\alpha) = \infty$.)

Let $\alpha \in \widehat{F^{\text{alg}}}^{G_K}$. Write $\alpha = \lim \alpha_n$ with $\alpha_n \in F^{\text{alg}}$

Then $\Delta_K(\alpha_n) \geq \text{val}_p(\alpha - \alpha_n) \rightarrow \infty$

Lemma 5.4. If $\alpha \in F^{\text{alg}}$, then $\exists \delta \in K$ s.t.

$$\text{val}_p(\alpha - \delta) \geq \Delta_K(\alpha) - \frac{p}{(p-1)^2}$$

$\Rightarrow \exists \delta_n \in K$ s.t.
 $\text{val}_p(\alpha_n - \delta_n) \rightarrow \infty$
 $\Rightarrow \alpha = \lim \delta_n \checkmark$.

Proof: Induction on $n := [K(\alpha) : K]$ s.t. we can find such a δ

with $\text{val}_p(\alpha - \delta) \geq \Delta_K(\alpha) - \sum_{k=0}^m \frac{1}{p^k(p-1)}$ where $p^{m+1} \leq n < p^{m+2}$

Basically, this says that if $\Delta_K(\alpha)$ is large, can find $\delta \in K$ very close to α .

Write $Q(x) = \text{min poly}(\alpha)$ over K assume this

When $K(\alpha)$ is Galois over K ,

$$Q(x) = \prod_{g \in \text{Gal}(K(\alpha)/K)} (x - g(\alpha)) \approx (x - \alpha)^n \text{ has coeffs in } K.$$

So if $p \nmid n$, $\alpha \approx -\frac{a_{n-1}}{n} \checkmark$

if $n = p^k \cdot r$, then we consider a_{n-p^k} .

Say degree $Q(x) = n$. $Q(x) = x^n + a_{n-1}x^{n-1} + \dots \in K[x]$

Case 1: $p \nmid n$, then $\text{val}_p(a_{n-1} - n\alpha) \geq \Delta_K(\alpha)$

We are done!

$K(\alpha)$ Apply Case 1, $\exists \alpha' \in K_r$

s.t. $\text{val}_p(\alpha - \alpha') \geq \Delta_K(\alpha)$

$\Rightarrow \Delta_K(\alpha') \geq \Delta_K(\alpha)$

Reduces question to α' .

p-power

degree prime-to-p
 K_r

K

Case 2. $n = p^k$.

Reduce α zero of $Q(x)$

to β zero of $Q^{(p^{k-1})}(x)$

) by our earlier philosophy
 $\alpha \approx \beta$.

Need to find a β s.t. $\text{val}_p(\alpha - \beta)$ is "large" $\geq \Delta_K(\alpha) - \frac{1}{p^{k-1}(p-1)}$

Let $P(x) = Q(x + \alpha) \in F^{\text{alg}}[x]$

Known: All zeros of $P(x)$ have $\text{val}_p \geq \Delta_K(\alpha)$

WTS: $P^{(p^{k-1})}(x) = Q^{(p^{k-1})}(x + \alpha)$ has a zero " $\beta - \alpha$ " whose
 $\text{val}_p \geq \Delta_K(\alpha) - \frac{1}{p^{k-1}(p-1)}$

Write $P(x) = x^{p^k} + \dots + a_{p^k}$

$$\Rightarrow \text{val}_p(a_{p^k - p^{k-1}}) \geq (p^k - p^{k-1}) \cdot \Delta_K(\alpha)$$

$$\frac{P^{(p^{k-1})}(x)}{p^k \dots (p^k - p^{k-1} + 1)} = x^{p^k - p^{k-1}} + \dots + \frac{a_{p^k - p^{k-1}}}{\binom{p^k}{p^{k-1}}}$$

so at least one zero of $P^{(p^{k-1})}(x)$ has val_p

$$\geq \frac{1}{p^k - p^{k-1}} \left(\text{val}_p(a_{p^k - p^{k-1}}) - \underbrace{\text{val}_p\left(\frac{p^k}{p^{k-1}}\right)}_{=1} \right)$$

$$\geq \Delta_K(\alpha) - \frac{1}{p^k - p^{k-1}}$$

So question about α
 $[K(\alpha):K] = p^k$

\rightsquigarrow question about β
 $[K(\beta):K] < p^k$

\rightsquigarrow ...
degree p -power part
of $[K(\beta):K]$