Distinguished Defining Polynomials for Extensions of p-adic Fields

Sebastian Pauli

with

Jordi Guardia, John Jones, Kevin Keating, David P. Roberts, David Roe

AIM SQuaRE: improved tabulation of local fields

https://www.lmfdb.org/padicField/

- more fields (1,393,286)
- families with generic defining polynomials
- more invariants, *e.g.* residual polynomial invariant, indices of inseparability
- new diagrams and knowls
- **distinguished (pseudo canonical) defining polynomials**

Distinguished Defining Polynomials

Ingredients

- Krasner-Monge reduction for Eisenstein polynomials
- Øystein polynomials as defining polynomials of general extensions
- Reduction of Øystein polynomials
- Selection of distinguished polynomials among the reduced polynomials

Setup

$$
\begin{tikzcd}
L = K(\pi) \cong K[x]/(\varphi) \arrow[d, dash, "e = p^w\epsilon"'] \\
K = \mathbb{Q}_p(\xi) \cong \mathbb{Q}_p[x]/(\nu) \arrow[d, dash, "f"'] \\
\mathbb{Q}_p
\end{tikzcd}
$$

$\varphi(\pi) = 0$
$\varphi \in \mathcal{O}_K[x]$ Eisenstein

unramified extension
$\nu(\xi) = 0$
$\overline{\nu} \in \mathbb{F}_p[x]$ Conway or JR'06 Polynomial

Krasner Bound

Let $\varphi \in \mathcal{O}_K[x]$ and $\psi \in \mathcal{O}_K[x]$ be Eisenstein of degree e with $v_p(\mathrm{disc}(\varphi)) = v_p(\mathrm{disc}(\psi)) = e + ae + b - 1$ where $b < e$.

If $\varphi \equiv \psi \bmod p^c$ for $c > 1 + 2a + \frac{2b}{e}$ then

$$K[x]/(\varphi) \cong K[x]/(\psi).$$

Slope 0 Reduction of Eisenstein Polynomials

$\varphi(x) = x^e + \sum_{i=1}^{e-1} \varphi_i + \sum \varphi_{0,i}\pi^i \in \mathcal{O}_K[x]$ Eisenstein and $\varphi(\pi) = 0$.

We use transformations of the uniformizer of the form $\varpi = \delta\pi$ to reduce $\varphi_{0,1}$.

1. Find the set D of all $\delta \in \overline{K}^\times$ such that

$$\log_\xi(\varphi_{0,1}\delta^e) \bmod (\#\overline{K} - 1)$$

   is minimal.

2. The set of slope 0 reductions of φ is

$$M_0 = \left\{\psi(x) = \delta^e \varphi\left(\tfrac{1}{\delta}x\right) : \delta \in D\right\}$$

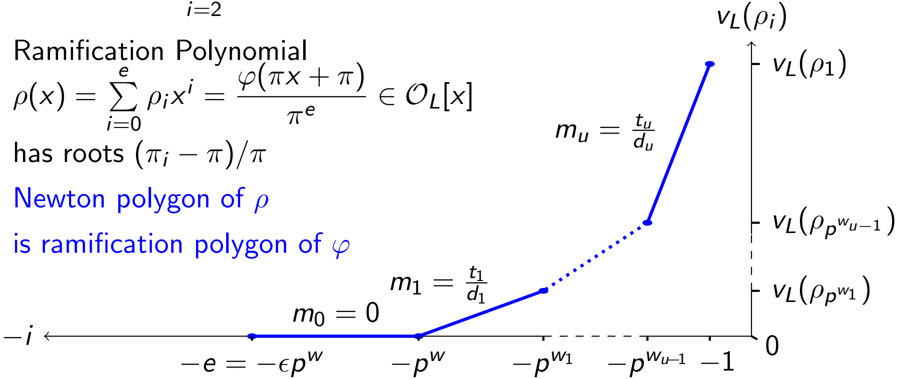
Ramification Polygon of an Eisenstein polynomial

$$\varphi(x) = (x-\pi)\prod_{i=2}^{e}(x-\pi_i) \in \mathcal{O}_K[x] \text{ Eisenstein, } e = p^w\epsilon, \text{ and } L = K(\pi)$$

Ramification Polynomial
$$\rho(x) = \sum_{i=0}^{e} \rho_i x^i = \frac{\varphi(\pi x + \pi)}{\pi^e} \in \mathcal{O}_L[x]$$
has roots $(\pi_i - \pi)/\pi$

Newton polygon of ρ

is ramification polygon of φ



Ramification Polygon of an Eisenstein polynomial

$$\varphi(x) = (x-\pi)\prod_{i=2}^{e}(x-\pi_i) \in \mathcal{O}_K[x] \text{ Eisenstein, } e = p^w\epsilon, \text{ and } L = K(\pi)$$

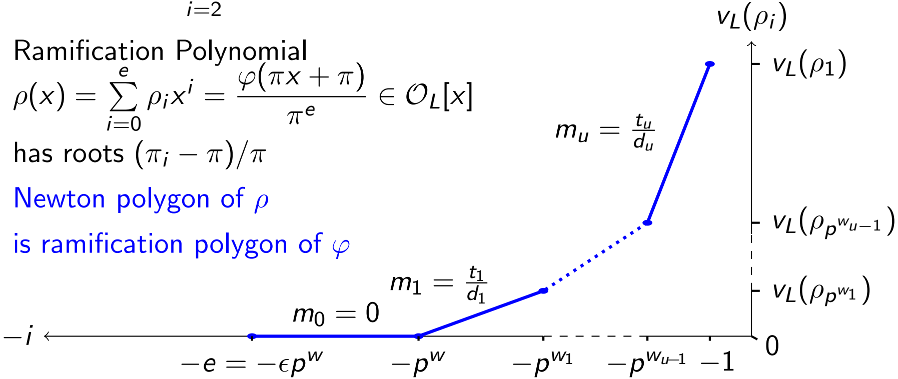
Ramification Polynomial

$$\rho(x) = \sum_{i=0}^{e} \rho_i x^i = \frac{\varphi(\pi x + \pi)}{\pi^e} \in \mathcal{O}_L[x]$$

has roots $(\pi_i - \pi)/\pi$

Newton polygon of ρ

is ramification polygon of φ



The ramification polygon is an invariant of L/K.

$$\varphi(x) = (x-\pi)\prod_{i=2}^{e}(x-\pi_i) \in \mathcal{O}_K[x] \text{ Eisenstein, } e = p^w\epsilon, \text{ and } L = K(\pi)$$

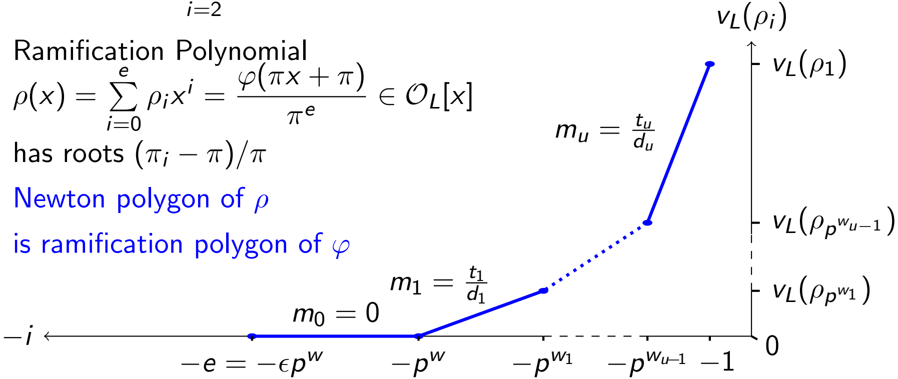
Ramification Polynomial

$$\rho(x) = \sum_{i=0}^{e} \rho_i x^i = \frac{\varphi(\pi x + \pi)}{\pi^e} \in \mathcal{O}_L[x]$$

has roots $(\pi_i - \pi)/\pi$

Newton polygon of ρ

is ramification polygon of φ



The ramification polygon is an invariant of L/K.

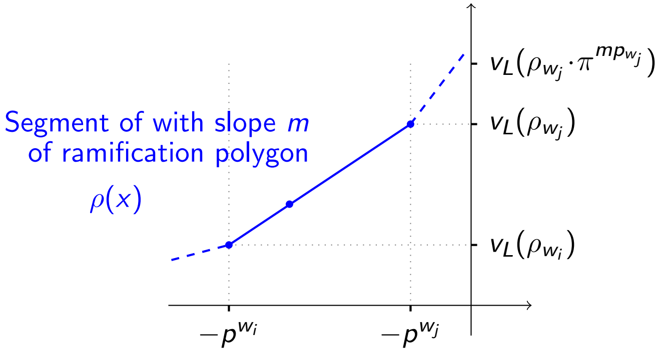
Hasse-Herbrand function of L/K is given by $e\Phi(m) = \min_{1\le i\le e} v_L(\rho_i) + i\cdot m$.

Additive Residual Polynomials of Eisenstein polynomials

$\varphi \in \mathcal{O}_K[x]$ Eisenstein of degree e, $\varphi(\pi) = 0$, $L = K(\pi)$

$\rho(x) = \frac{\varphi(\pi x + \pi)}{\pi^e}$ ramification polynomial of φ

The additive residual polynomial to slope m is $\overline{A}_m^+(x) = \overline{\left(\frac{\rho(\pi^m x)}{\pi^{e\Phi(m)}}\right)}$

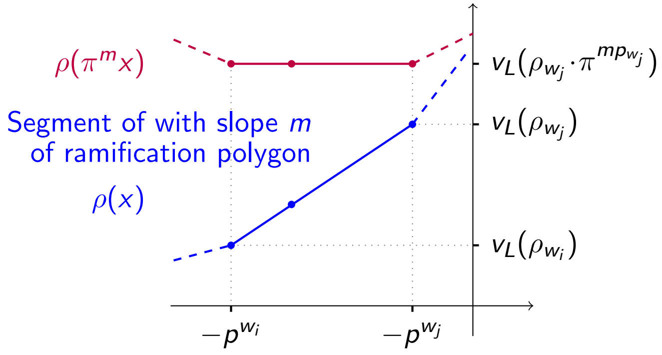


Additive Residual Polynomials of Eisenstein polynomials

$\varphi \in \mathcal{O}_K[x]$ Eisenstein of degree e, $\varphi(\pi) = 0$, $L = K(\pi)$

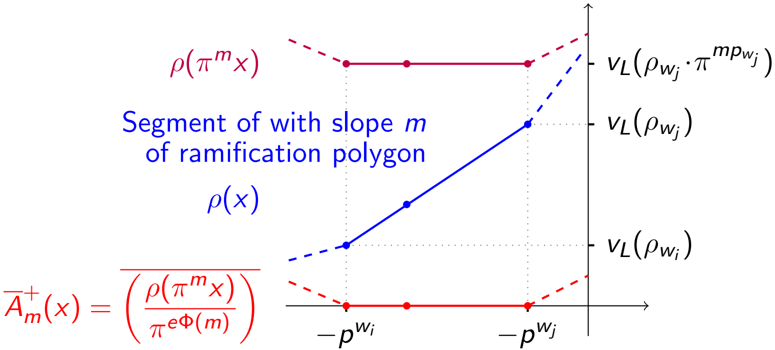
$\rho(x) = \frac{\varphi(\pi x + \pi)}{\pi^e}$ ramification polynomial of φ

The additive residual polynomial to slope m is $\overline{A}_m^+(x) = \overline{\left(\frac{\rho(\pi^m x)}{\pi^{e\Phi(m)}}\right)}$



Additive Residual Polynomials of Eisenstein polynomials

$\varphi \in \mathcal{O}_K[x]$ Eisenstein of degree e, $\varphi(\pi) = 0$, $L = K(\pi)$
$\rho(x) = \frac{\varphi(\pi x + \pi)}{\pi^e}$ ramification polynomial of φ
The additive residual polynomial to slope m is $\overline{A}_m^+(x) = \overline{\left(\frac{\rho(\pi^m x)}{\pi^{e\Phi(m)}}\right)}$

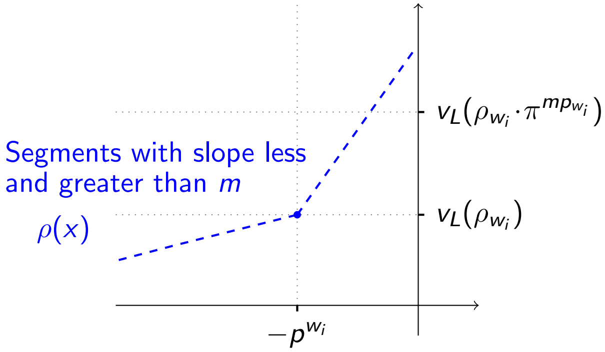


Additive Residual Polynomials of Eisenstein polynomials

$\varphi \in \mathcal{O}_K[x]$ Eisenstein of degree e, $\varphi(\pi) = 0$, $L = K(\pi)$

$\rho(x) = \frac{\varphi(\pi x+\pi)}{\pi^e}$ ramification polynomial of φ

The additive residual polynomial to slope m is $\overline{A}_m^+(x) = \overline{\left(\frac{\rho(\pi^m x)}{\pi^{e\Phi(m)}}\right)}$

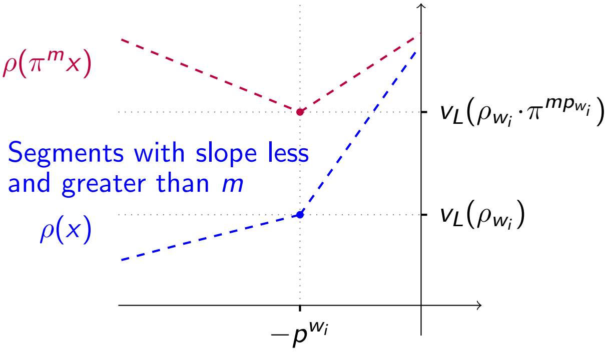


Additive Residual Polynomials of Eisenstein polynomials

$\varphi \in \mathcal{O}_K[x]$ Eisenstein of degree e, $\varphi(\pi) = 0$, $L = K(\pi)$

$\rho(x) = \frac{\varphi(\pi x + \pi)}{\pi^e}$ ramification polynomial of φ

The additive residual polynomial to slope m is $\overline{A}_m^+(x) = \overline{\left(\frac{\rho(\pi^m x)}{\pi^{e\Phi(m)}}\right)}$

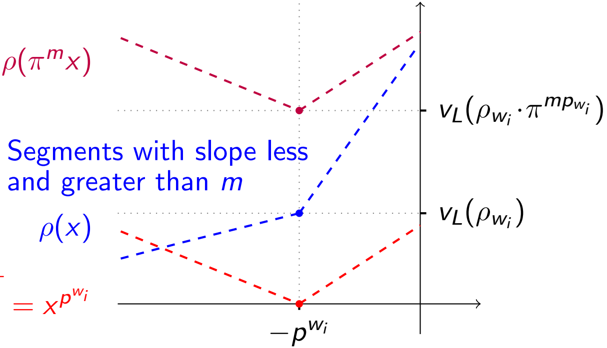


Additive Residual Polynomials of Eisenstein polynomials

$\varphi \in \mathcal{O}_K[x]$ Eisenstein of degree e, $\varphi(\pi) = 0$, $L = K(\pi)$

$\rho(x) = \frac{\varphi(\pi x + \pi)}{\pi^e}$ ramification polynomial of φ

The additive residual polynomial to slope m is $\underline{A}_m^+(x) = \overline{\left(\frac{\rho(\pi^m x)}{\pi^{e\Phi(m)}}\right)}$



$\underline{A}_m^+(x) = \overline{\left(\frac{\rho(\pi^m x)}{\pi^{e\Phi(m)}}\right)} = x^{p^{w_i}}$

Slope m Reduction of Eisenstein Polynomials

Krasner (1937), modernized by Monge (2014)

Proposition

$\varphi = x^e + \sum_{i=0}^{e-1} \varphi_i x^i \in \mathcal{O}_K[x]$ Eisenstein with $\varphi_i = \sum_{j=1}^{\infty} \varphi_{i,j} p^j$ and root π

$\varpi = \pi + \gamma\pi^{m+1}$ where $v_p(\gamma) = 0$ with minimal polynomial $\psi = x^e + \sum_{i=0}^{e-1} \psi_i x^i$

$\overline{A}_m^+(z)$ be the additive residual polynomial of φ for the slope m

- $\varphi_{i,k} = \psi_{i,k}$ for all i, k such that $i + ek < e(\Phi(m) + 1)$.
- If $h = e\Phi(m)$, $i = h \bmod e$, $k = (h \operatorname{div} e) + 1$, and $\eta = p/\pi^e$ then

$$\overline{\psi}_{i,k} = \overline{\varphi}_{i,k} - \overline{A}_m^+(\gamma) \cdot \overline{\eta}^{-k}$$

Slope m Reduction of Eisenstein Polynomials

- $\varphi_{i,k} = \psi_{i,k}$ for all i, k such that $i + ek < e(\Phi(m) + 1)$.
- If $h = e\Phi(m)$, $i = h \bmod e$, $k = (h \operatorname{div} e) + 1$, and $\eta = p/\pi^e$ then

$$\overline{\psi}_{i,k} = \overline{\varphi}_{i,k} - \overline{A}_m^+(\gamma) \cdot \overline{\eta}^{-k}$$

We use transformations of the uniformizer of the form $\varpi = \pi + \gamma\pi^{m+1}$ to reduce $\varphi_{i,k}$:

1. Let $\overline{\delta}$ be the reduction of $\overline{\varphi_{i,k}}$ given by reducing its coordinate vector by the matrix representation of $\overline{A}_m^+$.
2. Let $\Theta = \left\{\theta \in \overline{K} : \overline{\varphi_{i,k}(\alpha)} - \overline{\delta} = \overline{\eta}^{-k} \cdot \overline{A}_m^+(\overline{\theta})\right\}$.
3. The set of slope m reductions of M_m is

$$\left\{\chi_{L/K}(\alpha + \widehat{\theta} \cdot \nu(\alpha)^{m+1}) : \theta \in \Theta\right\}$$

where $\chi_{L/K}(\beta)$ is the minimal polynomial of $\beta \in L$ over K.

If $\overline{A}_m^+$ is surjective then $\psi_{i,j} = 0$ for $\psi \in M_m$.

Reduction Algorithm

Input $\varphi = x^e + \sum_{i=0}^{e-1} \varphi_i x^i \in \mathcal{O}_K[x]$ Eisenstein

Output Set M of reductions of φ

1. find the ramification polynomial ρ and ramification polygon $\mathcal{R}$ of φ.
2. compute the set M_0 of slope 0 reductions of φ
3. for $m \in \{1, \ldots, \lceil \widetilde{m} \rceil\}$ where $\widetilde{m}$ is the steepest slope of $\mathcal{R}$:
   - $M_m \leftarrow \emptyset$
   - for $\psi \in M_{m-1}$:
     - let M_ψ be the set of slope m reductions of ψ.
     - $M_m \leftarrow M_m \cup M_\psi$
4. for $\psi \in M_{\lceil \widetilde{m} \rceil}$ and $m > \widetilde{m}$:
   - $\psi_i \leftarrow 0$ where $i = e\Phi_{L/K}(m) \bmod e$, $k = (e\Phi_{L/K}(m) \operatorname{div} e) + 1$
5. return $M_{\lceil \widetilde{m} \rceil}$.

Øystein Polynomials

Definition

Let $\nu(x) \in \mathbb{Z}_p[x]$ monic and irreducible modulo p.

$$\varphi(x) = \nu(x)^e + \sum_{i=1}^{e-1} \varphi_i^*(x)\nu(x)^i + \varphi_0^*(x)$$

is ν-Øystein when $p \mid \varphi_i^*(x)$ and $\deg \varphi_i^* < \deg \nu$, and $\min_j v_p(\varphi_{0,j}^*) = 1$.

Øystein Polynomials

Definition

Let $\nu(x) \in \mathbb{Z}_p[x]$ monic and irreducible modulo p.

$$\varphi(x) = \nu(x)^e + \sum_{i=1}^{e-1} \varphi_i^*(x)\nu(x)^i + \varphi_0^*(x)$$

is ν-Øystein when $p \mid \varphi_i^*(x)$ and $\deg \varphi_i^* < \deg \nu$, and $\min_j v_p(\varphi_{0,j}^*) = 1$.

- Ore called Øystein polynomials *regular Polynomials*.
- In Ford, P., Roblot the are called *polynomials in Eisenstein form*.

Øystein Polynomials

Definition

Let $\nu(x) \in \mathbb{Z}_p[x]$ monic and irreducible modulo p.

$$\varphi(x) = \nu(x)^e + \sum_{i=1}^{e-1} \varphi_i^*(x)\nu(x)^i + \varphi_0^*(x)$$

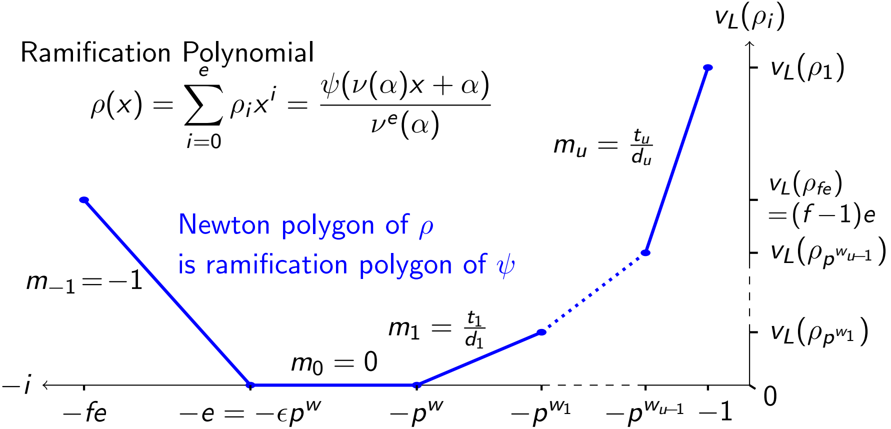
is ν-Øystein when $p \mid \varphi_i^*(x)$ and $\deg \varphi_i^* < \deg \nu$, and $\min_j v_p(\varphi_{0,j}^*) = 1$.

- Ore called Øystein polynomials *regular Polynomials*.
- In Ford, P., Roblot the are called *polynomials in Eisenstein form*.
- Every finite extension of $\mathbb{Z}_p$ can be defined with an Øystein polynomial.
- $\nu(\alpha)$ is a uniformizer of L and $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

$\psi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \psi_i^*(x)\nu(x)^i \in \mathbb{Z}_p[x]$ Øystein polynomial of degree $n = f \cdot e = f \cdot \epsilon p^w$ with $\psi(\alpha) = 0$ and $L = \mathbb{Q}_p(\alpha)$

Ramification Polynomial

$$\rho(x) = \sum_{i=0}^{e} \rho_i x^i = \frac{\psi(\nu(\alpha)x + \alpha)}{\nu^e(\alpha)}$$



Reduction of Øystein Polynomials

$$\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i \text{ with } \varphi_i^*(x) = \sum_{j=0}^{f-1} x^j \sum_{k=1}^{\infty} \varphi_{i,j,k}^* p^k$$

Ramification polynomial

$$\rho(x) = \sum_{i=0}^{e} \rho_i x^i = \frac{\varphi(\nu(\alpha)x + \alpha)}{\nu^e(\alpha)}$$

Additive residual polynomials to the slope m

$$\overline{A}_m^+(x) = \overline{\left(\frac{\rho(\nu(\alpha)^m x)}{\nu(\alpha)^{\Phi(m)}}\right)}$$

Reduction relation

$$\sum_{j=0}^{f-1} \left(\overline{\varphi_{\widetilde{\imath},j,\widetilde{k}}^*} - \overline{\psi_{\widetilde{\imath},j,\widetilde{k}}^*}\right) \overline{\alpha}^j = \overline{\eta}(\overline{\alpha})^{-k} \overline{A}_m^+(\overline{\gamma}(\overline{\alpha})).$$

Distinction

Let $\psi(x) = \nu(x)^e + \sum_{i=1}^{e-1} \psi_i^*(x)\nu(x)^i + \sum_{k=0}^{\infty} \psi_{ik}^*(x)p^k$ be ν-Øystein and $\psi(\alpha) = 0$.

$\psi(x)$ is distinguished when:

1. $\log_{\overline{\alpha}} \overline{\psi}_{0,1}^*(\alpha)$ is minimal.
2. the coefficients of residual polynomial invariants have smallest discrete logarithms
3. ψ is Krasner-Monge reduced.
4. ψ is minimal among the polynomials satisfying the above with respect to a lexicographic ordering.

False Friends

- ξ root of $\nu(x) = x^2 + 2x + 2 \in \mathbb{Z}_p[x]$
- $\varphi_i \in \mathbb{Z}_3(\xi)[y]$ distinguished relative defining Eisenstein polynomials
- $\psi_i \in \mathbb{Z}_3[x]$ distinguished absolute defining Øystein polynomials

such that $\mathbb{Q}_3(\xi)[y]/(\psi_i) \cong \mathbb{Q}_3[x]/(\varphi_i)$

Defining Polynomials	Ramification Polygon
$\varphi_1(y) = y^9 + (6\xi + 6)y^7 + 3\xi y^6 + 3$	$(-9, 0), (-1, 7)$
$\psi_1(x) = \nu(x)^9 + (3x + 3)\nu(x)^7 + 3x\nu(x)^6 + 3$	$(-18, 9), (-9, 0), (-1, 7)$
$\varphi_2(y) = y^9 + (3\xi + 3)y^7 + 3\xi y^6 + 3$	$(-9, 0), (-1, 7)$
$\psi_2(x) = \nu(x)^9 + (6x + 3)\nu(x)^6 + 3$	$(-18, 9), (-9, 0), (-1, 7)$
$\varphi_3(y) = y^9 + (6\xi + 3)y^6 + 3$	$(-9, 0), (-3, 6), (-1, 15)$
$\psi_3(x) = \nu(x)^9 + (9x + 18)\nu(x)^8 + (24x + 15)\nu(x)^7 + 3x\nu(x)^6 + (27x + 27)\nu(x) + 3$	$(-18, 9), (-9, 0), (-3, 6), (-1, 15)$

The polynomials ψ_1 and φ_2 and ψ_2 and φ_3 are 'false friends'. The distinguished polynomial φ_1 is the reduction of the false friend of ψ_3.