Enumerating extensions of p-adic fields with given invariants

Sebastian Pauli

(joint work with Brian Sinclair)

University of North Carolina Greensboro

Notation

K finite extension of $\mathbb{Q}_p$

$\mathcal{O}_K$ valuation ring of K

π uniformizing element in $\mathcal{O}_K$

v_π exponential valuation normalized such that $v(\pi) = 1$

$\underline{K}$ residue class field $\mathcal{O}_K/(\pi)$ of K

For the coefficients of $\varphi(x) = \varphi_n x^n + \varphi_{n-1}x^{n-1} + \cdots + \varphi_0$ we write $\varphi_i = \sum_{j=0}^{\infty} \varphi_{i,j}\pi^j$.

Example ($\mathbb{Q}_p$, deg 9, $e = 9$)

To show the progression of results, we use the following diagram. Each space represents a coefficient in the p-adic expansion of a coefficient of a polynomial.

A monic Eisenstein polynomial of degree 9 over $\mathbb{Q}_p$ looks like this:

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
p^2	*	*	*	*	*	*	*	*	*	0
p^1	$\neq 0$	*	*	*	*	*	*	*	*	0
p^0	0	0	0	0	0	0	0	0	0	1

0 or 1 indicates exactly 0 or 1, $\neq 0$ a non-zero value, and * is free.

Degree and Discriminant

Ore's Conditions

Given $j \in \mathbb{Z}$, let $a, b \in \mathbb{Z}$ be such that $j = an + b$ with $0 \leq b \leq n - 1$. There exist totally ramified extensions $L/\mathbb{Q}_p$ of degree n and discriminant $(p)^{n+j-1}$ if and only if

$$\min\{v_p(b)n, v_p(n)n\} \leq an + b \leq v_p(n)n.$$

This allows us to enumerate all possible discriminants.

Example ($\mathbb{Q}_3$, deg 9, $e = 9$, $v(\text{disc}) = 15$)

Generating polynomials $x^n + \sum \varphi_i x^i$ of totally ramified extensions L of $\mathbb{Q}_3$ of degree 9 with $v(\text{disc}(L)) = 15$.

For the discriminant to be correct, we must have $v(\varphi_7) = 1$ and certain minimum valuations.

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
3^2	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	0
3^1	$\neq 0$	0	0	$*$	0	0	$*$	$\neq 0$	$*$	0
3^0	0	0	0	0	0	0	0	0	0	1

Degree and Discriminant

For an extension of degree n and discriminant $(p)^{n+j-1}$:

If $j = an + b$, let $c \in \mathbb{Z}$ with $c > 1 + 2a + \frac{2b}{n}$.

By Krasner's Lemma, we only need to consider Eisenstein polynomials $x^n + \sum \varphi_i x^i$ with coefficients of the form for a generating polynomial:

$$\varphi_i = (\varphi_{i,0}) + (\varphi_{i,1})p + (\varphi_{i,2})p^2 + \cdots + (\varphi_{i,c-1})p^{c-1} \text{ for } 0 \leq i \leq n-1$$

Thus we have a finite number of possible generating polynomials for extensions of a given degree and discriminant.

Mass given Degree and Discriminant

Theorem (Krasner 1966)

The number of distinct totally ramified extensions of $\mathbb{Q}_p$ of degree n and discriminant p^{n+j-1} is

$$\begin{array}{ll} n\,p^{n+j-1-\sum_{i=1}^{n-1} l(i)} & \text{for } b = 0 \\ n\,(p-1)\,p^{n+j-1-\sum_{i=1}^{n-1} l(i)-1} & \text{for } b > 0 \end{array}$$

where $j = an + b$, with $0 \leq b < n$, satisfies Ore's Conditions.

This yields an algorithm for explicitly enumerating generating polynomials for all extensions of given degree and discriminant (P., Roblot 2001).

Example ($\mathbb{Q}_3$, deg 9, $e = 9$, $v(\text{disc}) = 15$)

As $v(\text{disc}) = 15$ we have $j = 7$.

Thus $7 = 0 \cdot 9 + 7$ and $c > 1 + 2 \cdot 0 + \frac{2\cdot 7}{9} = 1 + \frac{14}{9}$ and we only need to consider 3-adic coefficients below 3^3.

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
3^3	0	0	0	0	0	0	0	0	0	0
3^2	*	*	*	*	*	*	*	*	*	0
3^1	$\neq 0$	0	0	*	0	0	*	$\neq 0$	*	0
3^0	0	0	0	0	0	0	0	0	0	1

$3^{12} \cdot 2^2 = 2\,125\,764$ polynomials to generate 162 extensions.

Ramification Polygons

Let $\varphi(x) = x^n + \varphi_{n-1}x^{n-1} + \cdots + \varphi_0 \in \mathbb{Q}_p[x]$ be Eisenstein with root α and $L = \mathbb{Q}_p(\alpha)$.

Ramification Polynomial and Polygon

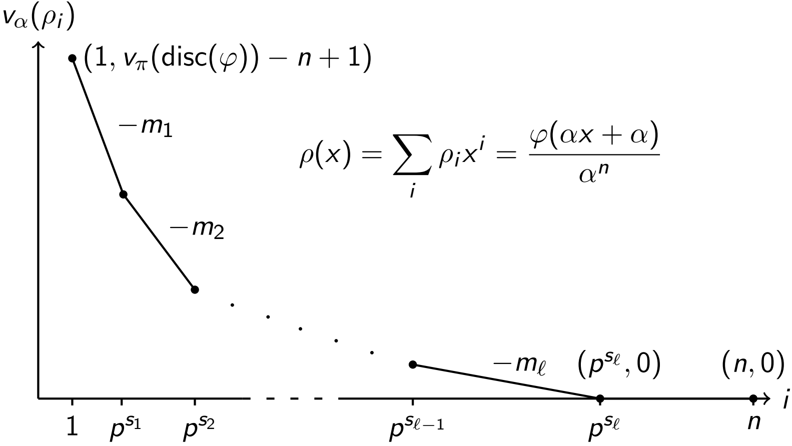
The ramification polygon of φ is the Newton polygon of the ramification polynomial $\rho(x) = \alpha^{-n}\varphi(\alpha x + \alpha)$ of φ.

The ramification polygon is an invariant of $L/\mathbb{Q}_p$,

Relation between coefficients of φ and ρ

$$v_\alpha(\rho_i) = \min_{i\le k\le n}\left\{ v_\alpha\left(\binom{k}{i}\varphi_k\,\alpha^k\right) - n\right\}$$

Ramification Polygons



$$\rho(x) = \sum_i \rho_i x^i = \frac{\varphi(\alpha x + \alpha)}{\alpha^n}$$

We can generate all polygons for a given degree and discriminant.

Mass given Ramification Polygon

Theorem (Sinclair)

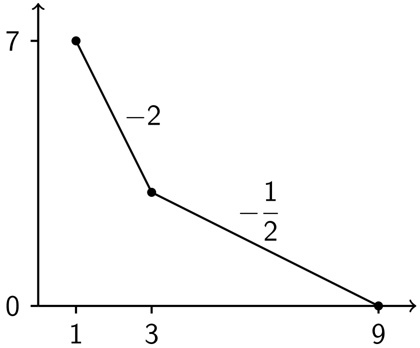
Let $\mathcal{R} = \{(p^s, a_s n + b_s)\}$ be the vertices of a ramification polygon and let $B_R = \{b_s \mid b_s > 0\}$.

The number of distinct totally ramified extensions of $\mathbb{Q}_p$ of degree n, discriminant p^{n+j-1}, and ramification polygon $\mathcal{R}$ is

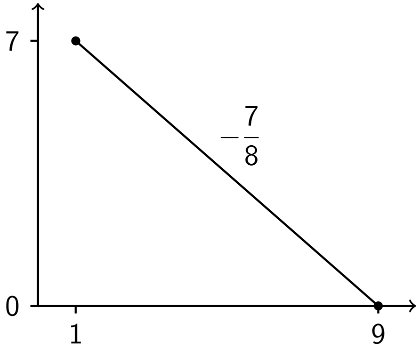
$$n(p-1)^{\# B_{\mathcal{R}}}\, p^{n+j-1-\sum_{i=1}^{n-1} L(i) - \# B_{\mathcal{R}}}$$

Example ($\mathbb{Q}_3$, deg 9, $e = 9$, $v(\text{disc}) = 15$)

In this case, there are two possible polygons:



$\mathcal{R}_1 = \{(1,7),(3,3),(9,0)\}$
108 extensions



$\mathcal{R}_2 = \{(1,7),(9,0)\}$
54 extensions

Let us choose $\mathcal{R}_1$ as a polygon to further investigate.

Example ($\mathbb{Q}_3$, deg 9, $e = 9$, $v(\mathrm{disc}) = 15$, $\mathcal{R}_1$)

The ramification polygon dictates $v(\varphi_3) = 1$, but does not otherwise change our valuation lower bounds.

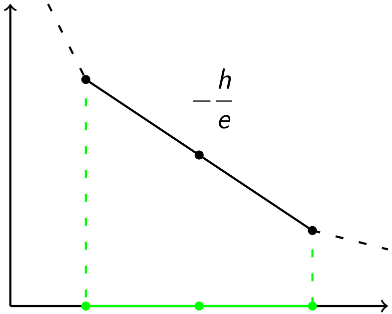
Our updated picture:

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
3^2	*	*	*	*	*	*	*	*	*	0
3^1	$\neq 0$	0	0	$\neq 0$	0	0	*	$\neq 0$	*	0
3^0	0	0	0	0	0	0	0	0	0	1

$3^{11}2^3 = 1\ 417\ 176$ polynomials to generate 108 extensions.

Residual Polynomials of Segments

Residual polynomials were introduced by Ore and are a core component of OM (Ore/Okutsu-MacLane/Montes) algorithms.



For the segment
$(p^s, \nu(\rho_{p^s}))$ to $((p^t, \nu(\rho_{p^t}))$

$$\underline{A}(z) = \sum_{j=0}^{(p^t-p^s)/e} \underline{\rho_{je+p^s} p^{jh-p^s}} z^j$$

Another Invariant: Residual Polynomial Classes

Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein, α a root of φ, and $L = K(\alpha)$. Let $S_1, \ldots, S_r$ be the segments of the ramification polygon with slopes $m_i = h_i/d_i$ and residual polynomials $\underline{A_i}$. Then

$$\mathcal{A} = \left\{ \left(\underline{\delta}^{-h_1 \deg \underline{A_1}} \underline{A_1}(\underline{\delta}^{h_1} z), \ldots, \underline{\delta}^{-h_r \deg \underline{A_r}} \underline{A_r}(\underline{\delta}^{h_r} z) \right) : \underline{\delta} \in \underline{K} \right\}$$

is an invariant of L/K called *residual polynomial clases*.

We also write $\mathcal{A} = \{(A_1, \ldots, A_r)\}$.

Mass given Polygon and Residual Polynomial Classes

Theorem (Sinclair)

Let $\mathcal{R} = \{(p^s, a_s n + b_s)\}$ be the vertices of a ramification polygon and let $B_{\mathcal{R}} = \{b_s \mid b_s > 0\}$.

The number of distinct totally ramified extensions of K of degree n, discriminant $(\pi)^{n+J_0-1}$, ramification polygon $\mathcal{R}$, and residual polynomial classes $\mathcal{A}$ is

$$n\,(\#\mathcal{A})\,p^{n+j-1-\sum_{i=1}^{n-1} L(i) - \#B_{\mathcal{R}}}$$

The Constant Term

Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein of degree n and denote by $\varphi_0 = \sum \varphi_{0,i}\pi^i$ the constant term of φ.

Lemma

Let $\underline{S}_0 : \underline{K} \to \underline{K}, a \mapsto a^n$.

- If and only if $\underline{\delta} \in \underline{S}_0(\underline{K})$, there is $g \in \mathcal{O}_K[x]$ Eisenstein with $g_{0,1} \equiv \delta f_{0,1} \bmod (\pi)$ such that $K[x]/(g) \cong K[x]/(\varphi)$.
- If $n = p^r$ then S_0 is surjective and there is $g \in \mathcal{O}_K[x]$ Eisenstein with $g_{0,1} \equiv 1 \bmod (\pi)$ such that $K[x]/(g) \cong K[x]/(\varphi)$.

Example ($\mathbb{Q}_3$, deg 9, $e = 9$, disc 3^{15}, $\mathcal{R}_1$)

For $\varphi_0 \equiv 3 \bmod 9$ we obtain 4 choices for $\mathcal{A}$:

$$\mathcal{A}_{a,b} = \{(a + bx^2, b + x^3)\} \text{ where } a, b \in \{1, 2\}$$

This yields

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
3^2	*	*	*	*	*	*	*	*	*	0
3^1	1	0	0	$2a$	0	0	*	$2b$	*	0
3^0	0	0	0	0	0	0	0	0	0	1

$3^8 \cdot 2^2 \cdot 3^2 = 708\,588$ polynomials to generate 108 extensions

(27 extensions for each $\mathcal{A}_{a,b} = \{(a + bx^2, b + x^3)\},\ a, b \in \{1, 2\}$)

Residual Polynomials of Components

For $\lambda \in \mathbb{Q}$ the λ-component of $\mathcal{R}$ is

$$\{(k, w) \in \mathcal{R} \mid \lambda k + w = \min\{\lambda l + u \mid (l, u) \in \mathcal{R}\}\}.$$

Definition

Let $C_m = \text{cont}_\alpha \rho(\alpha^m x)$. We call

$$\underline{S}_m(x) = \underline{\alpha^{-C_m} \rho(\alpha^m x)}$$

the residual polynomial of the $(-m)$-component of $\mathcal{R}$.

$C_m = n\phi(m)$ where ϕ is the generalized Hasse-Herbrand function.

$\underline{S}_m$ is an additive polynomial.

Monge (2011) uses the $\underline{S}_m$ to define and find *reduced Eisenstein polynomials* that generate a given extension.

Reduced Eisenstein Polynomials

Let α and β be uniformizers for the same extension, where $\beta = \alpha + \theta\alpha^{m+1} + \cdots$, and let $\varphi(\alpha) = 0$ and $\psi(\beta) = 0$.

$$\underline{(\varphi(\alpha) - \psi(\alpha))\alpha^{-C_m - n}} = \underline{S}_m(\theta)$$

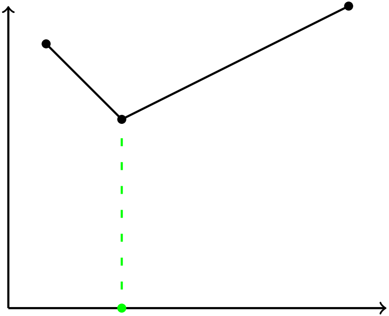
To reduce Eisenstein polynomials one fixes a choice of $\underline{\varphi_0/}$ and considers the images of the $\underline{S}_m$. Write $\varphi_i = \sum_{j\geq 1}^{\infty} \varphi_{i,j}\, p^j$.

If $\underline{S}_m$ is surjective, then we can set $\varphi_{i,j} = 0$ where

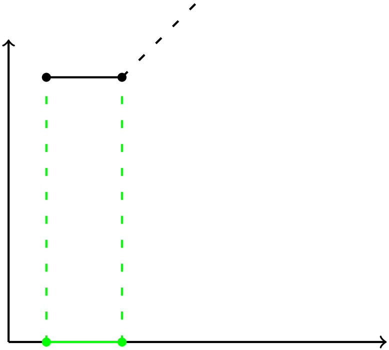
- $i \equiv \mathrm{cont}_\alpha \rho(\alpha^m T) \mod n$, and
- $j = \mathrm{cont}_\alpha \rho(\alpha^m T) - i$.

If $\mathcal{R}$ has a segment of slope $-m$ then $\underline{S}_m = \underline{A}x^k$ where $\underline{A}$ is the residual polynomial of the segment and only then $\underline{S}_m$ can be non-surjective.

Example ($\mathbb{Q}_3$, deg 9, $e = 9$, disc 3^{15}, $\mathcal{R}_1$)



$\underline{S}_1(x) = \underline{\alpha^{-C_1}\rho(\alpha x)} = x^3$
is surjective.



$\underline{S}_2(x) = \underline{\alpha^{-C_2}\rho(\alpha^2 x)}$
$= ax + bx^3.$

Example ($\mathbb{Q}_3$, deg 9, $e = 9$, disc 3^{15}, $\mathcal{R}_1$)

With $\underline{S}_1 = x^3$, $\underline{S}_2 = a(x + x^3)$ surjective, $\underline{S}_m = x$ for $m > 2$ we get

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
3^2	0	0	0	0	0	0	0	0	0	0
3^1	1	0	0	$2a$	0	0	0	$2a$	*	0
3^0	0	0	0	0	0	0	0	0	0	1

With $\underline{S}_1 = x^3$, $\underline{S}_2 = ax - ax^3$ "$=$" 0 , $\underline{S}_m = x$ for $m > 2$ we obtain

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
3^2	*	0	0	0	0	0	0	0	0	0
3^1	1	0	0	$2a$	0	0	0	$-2a$	*	0
3^0	0	0	0	0	0	0	0	0	0	1

$2 \cdot 3 + 2 \cdot 3^2 = 24$ polynomials to generate 108 extensions.

Example ($\mathbb{Q}_3$, deg 9, $e=9$, disc 3^{15}, $\mathcal{R}_1$)

Slopes -2 and $-\frac{1}{2}$, $\mathcal{A}=\{(1+x^2, 1+x^3)\}$

$$x^9+6x^7+6x^3+3$$
$$x^9+3x^8+6x^7+6x^3+3$$
$$x^9+6x^8+6x^7+6x^3+3$$

Slopes -2 and $-\frac{1}{2}$, $\mathcal{A}=\{(2+2x^2, 2+x^3)\}$

$$x^9+3x^7+3x^3+3$$
$$x^9+3x^8+3x^7+3x^3+3$$
$$x^9+6x^8+3x^7+3x^3+3$$

These 6 polynomials each generate 9 extensions.

Example ($\mathbb{Q}_3$, deg 9, $e = 9$, disc 3^{15}, $\mathcal{R}_1$)

Slopes -2 and $-\frac{1}{2}$, $\mathcal{A} = \{(2 + x^2, 1 + x^3)\}$

$x^9 + 6x^7 + 3x^3 + 3$	$x^9 + 3x^8 + 6x^7 + 3x^3 + 3$	$x^9 + 6x^8 + 6x^7 + 3x^3 + 3$
$x^9 + 6x^7 + 3x^3 + 12$	$x^9 + 3x^8 + 6x^7 + 3x^3 + 12$	$x^9 + 6x^8 + 6x^7 + 3x^3 + 12$
$x^9 + 6x^7 + 3x^3 + 21$	$x^9 + 3x^8 + 6x^7 + 3x^3 + 21$	$x^9 + 6x^8 + 6x^7 + 3x^3 + 21$

Slopes -2 and $-\frac{1}{2}$, $\mathcal{A} = \{(1 + 2x^2, 2 + x^3)\}$

$x^9 + 3x^7 + 6x^3 + 3$	$x^9 + 3x^8 + 3x^7 + 6x^3 + 3$	$x^9 + 6x^8 + 3x^7 + 6x^3 + 3$
$x^9 + 3x^7 + 6x^3 + 12$	$x^9 + 3x^8 + 3x^7 + 6x^3 + 12$	$x^9 + 6x^8 + 3x^7 + 6x^3 + 12$
$x^9 + 3x^7 + 6x^3 + 21$	$x^9 + 3x^8 + 3x^7 + 6x^3 + 21$	$x^9 + 6x^8 + 3x^7 + 6x^3 + 21$

These 18 polynomials each generate 3 extensions.

`https://www.uncg.edu/mat/numbertheory/tables/local/counting/q3n27.html`

Galois Group – One segment case

$\varphi(x) = x^{p^m} + \sum_{i=1}^{p^m-1} \varphi_i x^i + \varphi_0 \in \mathcal{O}_K[x]$ Eisenstein polynomial whose ramification polygon has only one side.

Let $\wp$ be the maximal ideal of the splitting field of $\varphi(x)$.

$\Theta_h : G_h/G_{h+1} = G_1 \to \wp^h/\wp^{h+1} : g \mapsto \left(\frac{\pi^g}{\pi} - 1\right) \mod \wp^{h+1}$

$\mathrm{Gal}(\varphi)$ is isomorphic to the group

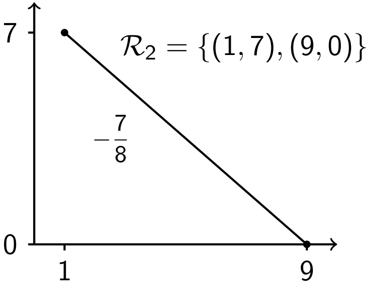
$$\left\{ t_{a,v} : (\mathbb{F}_p)^m \to (\mathbb{F}_p)^m : x \mapsto xa + v \;\middle|\; a \in H' \leq \mathrm{GL}(m,p), v \in (\mathbb{F}_p)^m \right\}$$

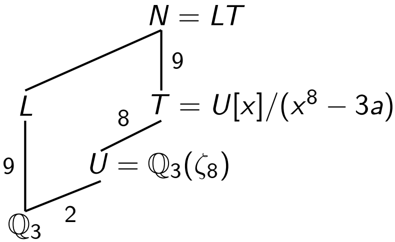
of permutations of the vector space $(\mathbb{F}_p)^m$, where H' describes the action of $\mathrm{Gal}(N/K)$ on $\Theta_h(G_h/G_{h+1}) \leq \wp^h/\wp^{h+1}$.

Corollary

If the ramification polygon of φ consists of one segement we can obtain $\mathrm{Gal}(\varphi)$ from the ramification polygon and the residual polynomial classes.

Example ($\mathbb{Q}_3$, deg 9, $e = 9$, disc 3^{15}, $\mathcal{R}_2$)





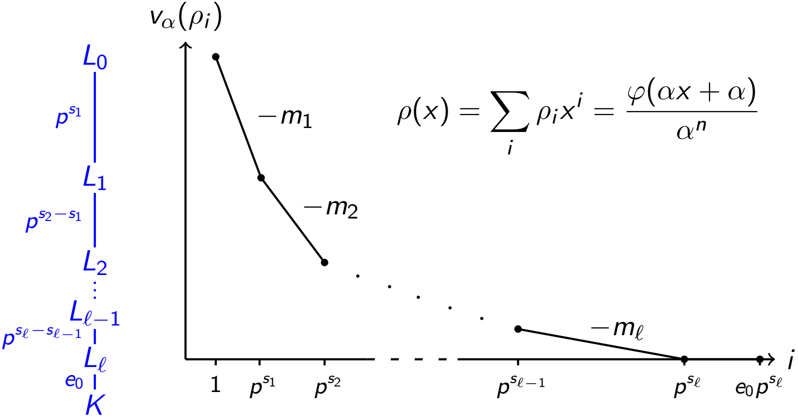
Possible residual polynomial classes $\mathcal{A} = \{(a+x)\}$ where $a \in \{1,2\}$

For $U = \mathbb{Q}_3(\zeta_8)$ we have $[U : \mathbb{Q}_3] = 2$.

If $T = U[x]/(x^8 - 3a)$ then $N = LT$ is the normal closure.

Gal(L) is 9T19 of order $2^4 \cdot 3^2$.

Ramification Polygons and Subfields



Each segment of the ramification polygon of φ corresponds to a subfield of $L_0 = K[x]/(\varphi)$.

Subfields of Splitting Field

Theorem (Greve, P.)

$\varphi \in \mathcal{O}_K[x]$ Eisenstein of degree $n = ep^m$. Ramification polygon $\mathcal{R}$ of φ has $\ell + 1$ segments with slopes $m_i = h_i/e_i$ and residual polynomials $\underline{A}_i$ with root $\underline{\gamma}_i$ and f_i the lcm of the degrees of the irreducible factors of $\underline{A}_i$.

U/K unramified, $[U{:}K] = \operatorname{lcm}(f_1, .., f_{\ell+1}, [K(\zeta_{e_1}){:}K], .., [K(\zeta_{e_\ell}){:}K])$
$T = U\left(\sqrt[e_1]{\gamma_1^n \varphi_0}, \dots, \sqrt[e_\ell]{\gamma_\ell^n \varphi_0}, \sqrt[e]{\varphi_0}\right)$ and N splitting field of φ.

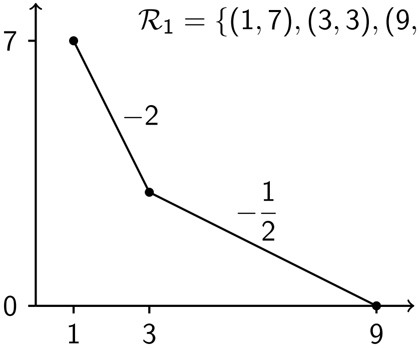
Let α be a root of φ and $K(\alpha) = L_0 \supset L_1 \supset \cdots \supset L_\ell \supset K$ be the tower of subfields corresponding to $\mathcal{R}$. Then:

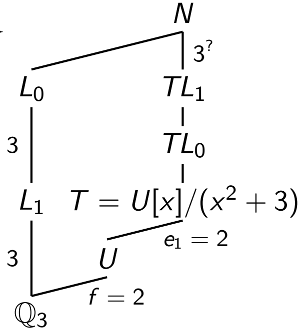
(a) TL_{i-1}/TL_i is elementary abelian.

(b) N/T is a p-extension.

Example ($\mathbb{Q}_3$, deg 9, $e = 9$, disc 3^{15}, $\mathcal{R}_1$)

$$\mathcal{R}_1 = \{(1,7),(3,3),(9,0)\}$$





For $\mathcal{A} = \{(x^2+1, x^3+1)\}$ we obtain the possible Galois groups 9T8, 9T18, and 9T24 from the invariants.

From the generating polynomials we get 9T8 and 9T18.