ENUMERATING EXTENSIONS OF (π)-ADIC FIELDS WITH GIVEN INVARIANTS

SEBASTIAN PAULI AND BRIAN SINCLAIR

Abstract. We give an algorithm that constructs a minimal set of polynomials defining all extension of a (π)-adic field with given, inertia degree, ramification index, discriminant, ramification polygon, and residual polynomials of the segments of the ramification polygon.

1. Introduction

It follows from Krasner's Lemma that a local field has only finitely many extensions of a given degree and discriminant. Thus it is natural to ask whether one can generate a list of polynomials such that each extension is generated by exactly one of the polynomials.

For abelian extensions local class field theory, gives a one-to-one correspondence between the abelian extensions of K and the open subgroups of the unit group $K^\times$ of K. An algorithm that constructs the wildly ramified part of the class field as towers of extensions of degree p was given in [17]. Recently Monge [11] has published an algorithm that, given a subgroup of $K^\times$ of finite index, directly constructs the generating polynomial of the corresponding totally ramified extension.

In the non-abelian case, such a complete description is not yet known. However, a description of all tamely ramified extensions is well known and all extensions of degree p have been described completely by Amano [1]. Krasner [8] gave a formula for the number of totally ramified extensions, using his famous lemma as a main tool. Following his approach Pauli and Roblot [19] presented an algorithm that returned a set of generating polynomials for all extensions of a given degree and discriminant. They used the root-finding algorithm described by Panayi [16] to obtain one generating polynomial for each extension. A new approach for determining whether two polynomials generate the same extension was recently presented by Monge [11]. He introduces *reduced polynomials* that yield a canonical set of generators for totally ramified extensions of K.

Monge's methods also considerably reduce the number of generating polynomials that need to be considered when computing a set of polynomials defining all totally ramified extensions of K. We present an algorithm that for each extension with given invariants constructs a considerably smaller set of defining polynomials than the set obtained with Krasner's bound. In many cases this eliminates the need to check whether two polynomials generate the same extension. The polynomials constructed are reduced in Monge's sense.

Overview. In the first three sections of the paper, we examine extension invariants and how specifying each invariant reduces the number of polynomials φ to be considered. We recall some of Krasner's results [8] that are based on degree and discriminant (Section 2) and then add the ramification polygon as an additional invariant (Section 3). Krasner's results allow us to set coefficients high enough in the π-adic expansion of the coefficients of φ to 0 and the ramification polygon determines or gives a lower bound for the valuations of

coefficients of the φ. In Section 4 we introduce an invariant based on the residual polynomials of the ramification polygon, a set containing tuples which consist of a polynomial over the residue class field for each segment of the ramification polygon. This invariant determines the leading coefficients of the π-adic expansion of the coefficients of the φ. The residual polynomials together with ideas of Monge [11] yield conditions on the coefficients of two polynomials that determine whether the polynomials generate isomorphic fields (Section 5). These conditions allow us to set further coefficients in the π-adic expansion of the coefficients of the polynomials φ. Thus reducing the number of polynomials to be considered considerably. In Section 6 we give an algorithm that uses the results of the previous sections to return a set of polynomials that generate all extensions with given invariants. In many cases this set contains exactly one polynomial for each extension. Section 7 contains examples and comparisons with the implementations of the algorithm by Pauli and Roblot [19].

Notation. By convention fractions denoted h/e or h_i/e_i are always taken to be in lowest terms. We denote by $\mathbb{Q}_p$ the field of p-adic numbers and by v_p the (exponential) valuation normalized such that $v_p(p) = 1$. By K we denote a finite extension of $\mathbb{Q}_p$, by $\mathcal{O}_K$ the valuation ring of K, and by π a uniformizer of $\mathcal{O}_K$.

We write v_π for the valuation of K that is normalized such that $v_\pi(\pi) = 1$ and also denote the unique extension of v_π to an algebraic closure $\overline{K}$ of K (or to any intermediate field) by v_π. For $\gamma \in \overline{K}^\times$ and $\delta \in \overline{K}^\times$ we write $\gamma \sim \delta$ if

$$v(\gamma - \delta) > v(\gamma)$$

and make the supplementary assumption $0 \sim 0$.

For $\gamma \in \mathcal{O}_K$ we denote by $\underline{\gamma}$ the class $\gamma + (\pi)$ in $\underline{K} = \mathcal{O}_K/(\pi)$, by $R_{\underline{K}}$ a fixed set of representatives of $\underline{K}$ in $\mathcal{O}_K$, and by $R_{\underline{K}}^\times$ the set $R_{\underline{K}}$ without the representative for $\underline{0} \in \underline{K}$. For a polynomial $\varphi \in \mathcal{O}_K[x]$ of degree n we denote its coefficients by φ_i $(0 \le i \le n)$ such that $\varphi(x) = \varphi_n x^n + \varphi_{n-1}x^{n-1} + \cdots + \varphi_0$ and write $\varphi_i = \sum_{j=0}^{\infty} \varphi_{i,j}\pi^j$. where $\varphi_{i,j} \in R_{\underline{K}}$.

In examples we use a table to represent sets of polynomials. Each cell contains a set from which the corresponding coefficient $\varphi_{i,j}$ of the π-adic expansion of the coefficient $\varphi_i = \sum_{j=0}^{\infty} \varphi_{i,j}\pi^j$ of the polynomial $\varphi(x) = \varphi_n x^n + \varphi_{n-1}x^{n-1} + \cdots + \varphi_0$ can be chosen. We use *, †, and ‡ to indicate which conditions determine which coefficient in the π-adic expansion.

Example 1.1. If $\varphi \in \mathcal{O}_K[x]$ is Eisenstein then $\boldsymbol{\varphi_n = 1^*}$, $\boldsymbol{\varphi_{i,0} = 0}$ for $\boldsymbol{0 \le i < n^\dagger}$, and $\boldsymbol{\varphi_{0,1} \ne 0^\ddagger}$. The Eisenstein polynomials of degree n over $\mathcal{O}_K$ are represented by the template:

	x^n	x^{n-1}	x^{n-2}	$\cdots$	x^4	x^3	x^2	x^1	x^0
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
π^2	$\{0\}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$\cdots$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$
π^1	$\{0\}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$\cdots$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$\boldsymbol{R_{\underline{K}}^{\times\ddagger}}$
π^0	$\boldsymbol{\{1\}^*}$	$\boldsymbol{\{0\}^\dagger}$	$\boldsymbol{\{0\}^\dagger}$	$\cdots$	$\boldsymbol{\{0\}^\dagger}$	$\boldsymbol{\{0\}^\dagger}$	$\boldsymbol{\{0\}^\dagger}$	$\boldsymbol{\{0\}^\dagger}$	$\boldsymbol{\{0\}^\dagger}$

2. Discriminant

We recall some of the results Krasner used to obtain his formula for the number of extensions of a p-adic field [8]. These can also be found in [19]. The possible discriminants of finite extensions are given by Ore's conditions [14]:

Proposition 2.1 (Ore's conditions)**.** *Let K be a finite extension of $\mathbb{Q}_p$, $\mathcal{O}_K$ its valuation ring with maximal ideal (π). Given $J_0 \in \mathbb{Z}$ let $a_0, b_0 \in \mathbb{Z}$ be such that $J_0 = a_0 n + b_0$ and $0 \leq b_0 < n$. Then there exist totally ramified extensions L/K of degree n and discriminant $(\pi)^{n+J_0-1}$ if and only if*

$$\min\{v_\pi(b_0)n, v_\pi(n)n\} \leq J_0 \leq v_\pi(n)n.$$

The proof of Ore's conditions yields a certain form for the generating polynomials of extensions with given discriminant.

Lemma 2.2. *An Eisenstein polynomial $\varphi \in \mathcal{O}_K[x]$ with discriminant $(\pi)^{n+J_0-1}$ where $J_0 = a_0 n + b_0$ with $0 \leq b_0 < n$ fulfills Ore's conditions if and only if*

$$\begin{aligned} v_\pi(\varphi_i) &\geq \max\{2 + a_0 - v_\pi(i), 1\} \text{ for } 0 < i < b_0, \\ v_\pi(\varphi_{b_0}) &= \max\{1 + a_0 - v_\pi(b_0), 1\}, \\ v_\pi(\varphi_i) &\geq \max\{1 + a_0 - v_\pi(i), 1\} \text{ for } b_0 < i < n. \end{aligned}$$

Krasner's Lemma yields a bound over which the coefficients of the π-adic expansion of the coefficients of a generating polynomial can be chosen to be 0 [8].

Lemma 2.3. *Each totally ramified extension of degree n with discriminant $(\pi)^{n+J_0-1}$ where $J_0 = a_0 n + b_0$ with $0 \leq b_0 < n$ can be generated by an Eisenstein polynomial $\varphi \in \mathcal{O}_K[x]$ with $\varphi_{i,j} = 0$ for $0 \leq i < n$ and $j > 1 + 2a_0 + \frac{2b_0}{n}$.*

With Lemma 2.2 and Lemma 2.3 we obtain a finite set of polynomials that generate all extensions of a given degree and discriminant. In [19] this set in conjunction with Krasner's mass formula [8] and Panayi's root finding algorithm is used to obtain a generating polynomial for each extension of a given degree and discriminant.

Example 2.4. We want to find generating polynomials for all totally ramified extensions L of $\mathbb{Q}_3$ of degree 9 with $v_3(\mathrm{disc}\,(L)) = 18$. Denote by $\varphi = \sum_{i=0}^{9} \varphi_i x^i$ an Eisenstein polynomial generating such a field L. By Lemma 2.2 with $J_0 = 10$, $a_0 = 1$, and $b_0 = 1$ we get $\boldsymbol{v_\pi(\varphi_1) = 2^\dagger}$ and $\boldsymbol{v_\pi(\varphi_i) = 2 - v_\pi(i)}$ for $\boldsymbol{1 < i < n^*}$. Furthermore by Lemma 2.3 $\boldsymbol{\varphi_{i,j} = 0}$ for $\boldsymbol{0 \leq i \leq 9}$ and $\boldsymbol{j > 3^\ddagger}$. Thus the template for the polynomials φ is:

	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
3^4	$\{0\}$	$\mathbf{\{0\}^\ddagger}$	$\mathbf{\{0\}^\ddagger}$	$\mathbf{\{0\}^\ddagger}$	$\mathbf{\{0\}^\ddagger}$	$\mathbf{\{0\}^\ddagger}$	$\mathbf{\{0\}^\ddagger}$	$\mathbf{\{0\}^\ddagger}$	$\mathbf{\{0\}^\ddagger}$	$\mathbf{\{0\}^\ddagger}$
3^3	$\{0\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$
3^2	$\{0\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\mathbf{\{1,2\}^\dagger}$	$\{0,1,2\}$
3^1	$\{0\}$	$\mathbf{\{0\}^*}$	$\mathbf{\{0\}^*}$	$\{0,1,2\}$	$\mathbf{\{0\}^*}$	$\mathbf{\{0\}^*}$	$\{0,1,2\}$	$\mathbf{\{0\}^*}$	$\mathbf{\{0\}^\dagger}$	$\{1,2\}$
3^0	$\{1\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$

3. Ramification Polygons

To distinguish totally ramified extensions further we use an additional invariant, namely the ramification polygon.

Definition 3.1. Assume that the Eisenstein polynomial φ defines L/K. The *ramification polygon* $\mathcal{R}_\varphi$ of φ is the Newton polygon $\mathcal{N}$ of the *ramification polynomial* $\rho(x) = \varphi(\alpha x + \alpha)/(\alpha^n) \in K(\alpha)[x]$ of φ, where α is a root of φ.

The ramification polygon $\mathcal{R}_\varphi$ of φ is an invariant of L/K (see [4, Proposition 4.4] for example) called the ramification polygon of L/K denoted by $\mathcal{R}_{L/K}$. Ramification polygons have been used to study ramification groups and reciprocity [20], compute splitting fields and Galois groups [4], describe maximal abelian extensions [10], and answer questions of commutativity in p-adic dynamical systems [9].

Let $\varphi(x) = \sum_{i=0}^{n} \varphi_i x^i \in K[x]$ be an Eisenstein polynomial, denote by α a root of φ, and set $L = K(\alpha)$. Let $\rho(x) = \sum_{i=0}^{n} \rho_i x^i \in L[x]$ be the ramification polynomial of φ. Then the coefficients of ρ are

$$\rho_i = \sum_{k=i}^{n} \binom{k}{i} \varphi_k \, \alpha^{k-n} \tag{1}$$

As $v_\alpha(\alpha) = 1$ and $v_\alpha(\varphi_i) \in n\mathbb{Z}$ we obtain

$$v_\alpha(\rho_i) = \min_{i \le k \le n} \left\{ v_\alpha\left(\binom{k}{i} \varphi_k \, \alpha^k \right) - n \right\} = \min_{i \le k \le n} \left\{ n \left[v_\pi\left(\binom{k}{i} \varphi_k \right) - 1 \right] + k \right\}. \tag{2}$$

Lemma 3.2 ([20, Lemma 1])**.** *Let $\varphi(x) = \sum_{i=0}^{n} \varphi_i x^i \in K[x]$ be an Eisenstein polynomial and $n = e_0 p^m$ with $p \nmid e_0$. Denote by α a root of φ and set $L = K(\alpha)$. Then the following hold for the coefficients of the ramification polynomial $\rho(x) = \sum_{i=0}^{n} \rho_i x^i = \varphi(\alpha x + \alpha)/\alpha^n \in \mathcal{O}_L[x]$ of φ:*

(a) *$v_\alpha(\rho_i) \ge 0$ for all i;*
(b) *$v_\alpha(\rho_{p^m}) = v_\alpha(\rho_n) = 0$;*
(c) *$v_\alpha(\rho_i) \ge v_\alpha(\rho_{p^s})$ for $p^s \le i < p^{s+1}$ and $s < m$.*

This gives the typical shape of the ramification polygon (see Figure 1).

Remark 3.3. Throughout this paper we describe ramification polygons by the set of points $\mathcal{P} = \{(1, J_0), (p^{s_1}, J_1), \ldots, (p^{s_{u-1}}, J_{u-1}), (p^{s_u}, 0), \ldots, (n, 0)\}$ where not all points in $\mathcal{P}$ have to be vertices of the polygon $\mathcal{R}$. We write $\mathcal{R} = \mathcal{P}$. This gives a finer distinction between fields by their ramification polygons and also allows for an easier description of the invariant based on the residual polynomials of the segments of the ramification polygon, see Section 4.

We now investigate the points on a ramification polygon further.

Lemma 3.4. *Let $\rho = \sum_{i=1}^{n} \rho_i x^i$ be the ramification polynomial of an Eisenstein polynomial $\varphi(x) = \sum_{i=0}^{n} \varphi_i x^i \in \mathcal{O}_K[x]$. Denote by*

$$\{(1, J_0), (p^{s_1}, J_1), \ldots, (p^{s_{u-1}}, J_{u-1}), (p^{s_u}, 0), \ldots, (n, 0)\} \subseteq \{(i, v_\alpha(\rho_i)) : 1 \le i \le n\}$$

the points on the ramification polygon of φ and write $J_i = a_i n + b_i$ with $0 \le b_i < n$.

(a) *For $p^{s_u} \le i \le n$ we have $v_\alpha(\rho_i) = 0$ if and only if $v_\alpha\binom{n}{i} = 0$.*
(b) *If $v_\alpha(\rho_i = 0)$ for some $p^{s_u} \le i \le n$ then $\rho_i \equiv \binom{n}{i} \bmod (\alpha)$.*
(c) *For $0 \le i \le u$ we have*

$$\rho_{p^{s_i}} \sim \begin{cases} \varphi_{b_i} \binom{b_i}{p^{s_i}} \alpha^{b_i - n} & \text{if } b_i \neq 0 \\ \varphi_n \binom{n}{p^{s_i}} & \text{if } b_i = 0. \end{cases}$$

Proof. (a) Suppose $v_\alpha(\rho_i) = 0$ for some $p^{s_u} \le i \le n$. By Equation (2) there is a unique $i \le k \le n$ such that

$$0 = n\left[v_\pi\left(\binom{k}{i}\,\varphi_k\right) - 1\right] + k.$$

Thus $n \mid k$ and since $k \le n$ we have $k = n$. As $v(\varphi_n) = 0$ we must have $v_\alpha\binom{n}{i} = 0$.

Suppose $v_\alpha\binom{n}{i} = 0$ for some $p^{s_u} \le i \le n$. By Equation (2)

$$v_\alpha(\rho_i) = \min_{i\le k\le n}\left\{v_\alpha\left(\binom{k}{i}\,\varphi_k\,\alpha^k\right) - n\right\} \le v_\alpha\left(\binom{n}{i}\varphi_n\alpha^n\right) - n = 0.$$

So $v_\alpha(\rho_i) \le 0$, and, by Lemma 3.2(a), $v_\alpha(\rho_i) \ge 0$. Thus, $v_\alpha(\rho_i) = 0$.

(b) With (a), Equation (1), and $\phi_n = 1$, we obtain $\rho_i \equiv \binom{n}{i} \bmod (\alpha)$.

(c) For a point $(p^{s_i}, a_i n + b_i)$ where $0 < b_i < n$, we have by Equation (2),

$$a_i n + b_i = \min_{p^{s_i}\le k\le n}\left\{n\left[v_\pi\left(\binom{k}{p^{s_i}}\,\varphi_k\right) - 1\right] + k\right\}.$$

in which the minimum must be obtained at $k = b_i$. Thus,

$$v_\alpha(\rho_{p^{s_i}}) = v_\alpha\left(\binom{b_i}{p^{s_i}}\,\varphi_{b_i}\,\alpha^{b_i}\right) - n = v_\alpha\left(\binom{b_i}{p^{s_i}}\,\varphi_{b_i}\,\alpha^{b_i-n}\right).$$

For a point $(p^{s_i}, a_i n)$, that is where $b_i = 0$, we have by Equation (2),

$$a_i n = \min_{p^{s_i}\le k\le n}\left\{n\left[v_\pi\left(\binom{k}{p^{s_i}}\,\varphi_k\right) - 1\right] + k\right\},$$

in which we have $n \mid k$, so $k = n$. Thus,

$$v_\alpha(\rho_{p^{s_i}}) = v_\alpha\left(\binom{n}{p^{s_i}}\,\varphi_n\,\alpha^n\right) - n = v_\alpha\left(\binom{n}{p^{s_i}}\,\varphi_n\right).$$

□

It follows from Lemma 3.4(b) that, modulo (α), the coefficients of the ramification polynomial that correspond to the horizontal segment of its Newton polygon only depend on the degree of φ.

Lemma 3.5. *If the ramification polygon of an Eisenstein polynomial $\varphi \in \mathcal{O}_K[x]$ has the points $\{(1, J_0), (p^{s_1}, J_1), \ldots, (p^{s_{u-1}}, J_{u-1}), (p^{s_u}, 0), \ldots, (n, 0)\}$ where $J_i = a_i n + b_i$ with $0 \le b_i \le n-1$. Then for $0 \le t \le u$, we have*

$$v_\pi(\varphi_i) \ge \begin{cases} 2 + a_t - v_\pi\binom{i}{p^{s_t}} \text{ for } p^{s_t} \le i < b_t \\ 1 + a_t - v_\pi\binom{i}{p^{s_t}} \text{ for } b_t \le i \le n-1 \end{cases}$$

and $v_\pi(\varphi_{b_t}) = a_t + 1 - v_\pi\binom{b_t}{p^{s_t}}$ if $b_t \ne 0$.

Proof. By Equation (2), for all k with $p^{s_t} \le k \le n$,

$$J_t = a_t n + b_t \le n\left[v_\pi\left(\binom{k}{p^{s_t}}\,\varphi_k\right) - 1\right] + k,$$

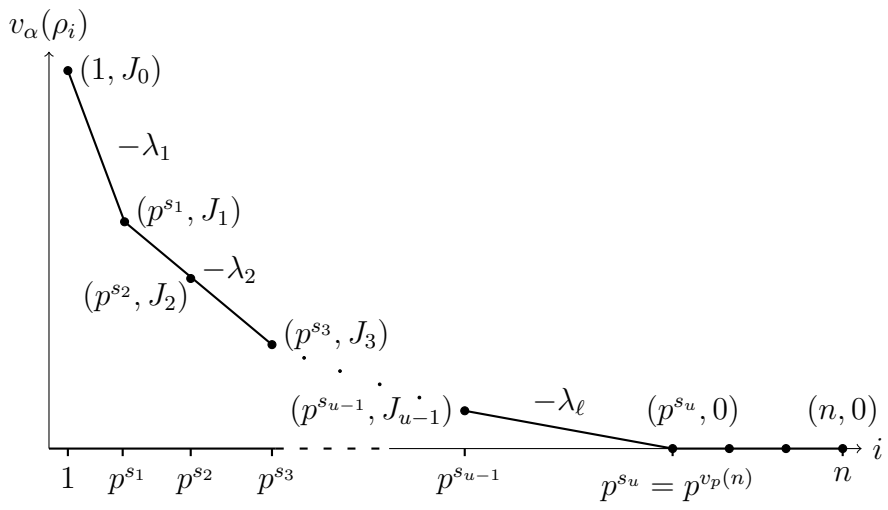

FIGURE 1. Ramification polygon of an Eisenstein polynomial φ of degree n and discriminant $(\pi)^{n+J_0-1}$ with $\ell+1$ segments and $u-1$ points on the polygon with ordinate above 0.

which solved for $v_\pi(\varphi_k)$ gives

$$1 + a_t - v_\pi\binom{k}{p^{s_t}} + \frac{b_t - k}{n} \leq v_\pi(\varphi_k) \text{ for } s_t \leq k \leq n.$$

As $v_\pi(\varphi_k)$ is an integer, we may take the ceiling of the fraction. As $0 \leq b_t \leq n-1$ and $p^{s_t} \leq k \leq n$, if $k < b_t$, then $\left\lceil \frac{b_t - k}{n} \right\rceil = 1$, and if $k \geq b_t$, then $\left\lceil \frac{b_t - k}{n} \right\rceil = 0$. Therefore,

$$v_\pi(\varphi_i) \geq \begin{cases} 2 + a_t - v_\pi\binom{i}{p^{s_t}} \text{ for } p^{s_t} \leq i < b_t \\ 1 + a_t - v_\pi\binom{i}{p^{s_t}} \text{ for } b_t \leq i \leq n-1 \end{cases}.$$

For a point $(p^{s_t}, a_t n + b_t)$ with $0 < b_t < n$ by Equation (2) we have

$$a_t n + b_t = \min_{p^{s_t} \leq k \leq n} \left\{ n \left[v_\pi\left(\binom{k}{p^{s_t}} \varphi_k \right) - 1 \right] + k \right\},$$

where the minimum is attained at $k = b_t$. Hence $a_t = \left[v_\pi\left(\binom{b_t}{p^{s_t}} \varphi_{b_t} \right) - 1 \right]$ and $v_\pi(\varphi_{b_t}) = a_t + 1 - v_\pi\binom{b_t}{p^{s_t}}$. □

From this, we can generalize Ore's conditions (Proposition 2.1) from a statement about the exponent of the discriminant, which is related to the ordinate of the point above 1, to the ordinates of all points.

Lemma 3.6. *Let $\mathcal{R}_\varphi$ be the ramification polygon of φ as in Lemma 3.5. Then for each point (p^{s_i}, J_i) where $J_i = a_i n + b_i$ with $0 \leq b_i \leq n-1$,*

$$\min\left\{ v_\pi\binom{b_i}{p^{s_i}} n, v_\pi\binom{n}{p^{s_i}} n \right\} \leq J_i \leq v_\pi\binom{n}{p^{s_i}} n.$$

Proof. The $k = n$ term of Equation (2) is

$$J_i \leq n\left[v_\pi\left(\binom{n}{p^{s_i}}\varphi_n\right) - 1\right] + n = v_\pi\binom{n}{p^{s_i}}n.$$

If $b_i \neq 0$, then by Lemma 3.5, $v_\pi(\varphi_{b_i}) = a_i+1-v_\pi\binom{b_i}{p^{s_i}}$. So $nv_\pi(\varphi_{b_i})+b_i = na_i+n-nv_\pi\binom{b_i}{p^{s_i}}+b_i$ and $nv_\pi(\varphi_{b_i}) + b_i - n + nv_\pi\binom{b_i}{p^{s_i}} = na_i + b_i = J_i$. As φ is Eisenstein we have $v_\pi(\varphi_{b_i}) \geq 1$, hence $nv_\pi(\varphi_{b_i}) - n \geq 0$. This combined with $b_i > 0$ gives us that

$$J_i = nv_\pi(\varphi_{b_i}) + b_i - n + nv_\pi\binom{b_i}{p^{s_i}} \geq b_i + nv_\pi\binom{b_i}{p^{s_i}} \geq nv_\pi\binom{b_i}{p^{s_i}}.$$

If $b_i = 0$, then the minimum term of Equation (2) defining J_i must be such that $k|n$, which only occurs in the $k = n$ term, so $J_i = v_\pi\binom{n}{p^{s_i}}n$, which is less than $v_\pi\binom{0}{p^{s_i}}n = \infty$. □

Lemma 3.7. *Let $\mathcal{R}_\varphi$ be the ramification polygon of an Eisenstein polynomial $\varphi \in \mathcal{O}_K[x]$ with points*

$$\mathcal{R}_\varphi = \{(1, J_0), (p^{s_1}, J_1), \ldots, (p^{s_{u-1}}, J_{u-1}), (p^{s_u}, 0), \ldots, (n, 0)\},$$

but no point with abscissa p^i, where $s_t < i < s_{t+1}$ for some $1 \leq t \leq u$. Then for k such that $p^i \leq k \leq n$,

$$v_\pi(\varphi_k) > \frac{1}{n}\left[\frac{J_{t+1} - J_t}{p^{s_{t+1}} - p^{s_t}}(p^i - p^{s_t}) + J_t - k\right] + 1 - v_\pi\binom{k}{p^i}$$

Proof. If there is no point on $\mathcal{R}_\varphi$ with abscissa p^i, then the point $(p^i, v_\alpha(\rho_{p^i}))$ must be above the segment from (p^{s_t}, J_t) to $(p^{s_{t+1}}, J_{t+1})$. Thus, $\frac{J_{t+1}-J_t}{p^{s_{t+1}}-p^{s_t}}(p^i - p^{s_t}) + J_t < v_\alpha(\rho_{p^i})$, and so by Equation (2), for k in $p^i \leq k \leq n$,

$$\frac{J_{t+1} - J_t}{p^{s_{t+1}} - p^{s_t}}(p^i - p^{s_t}) + J_t < n\left[v_\pi\left(\binom{k}{p^i}\varphi_k\right) - 1\right] + k.$$

Solving for $v_\pi(\varphi_k)$ provides the result of the lemma. □

We collect the results of Lemmas 3.5 and 3.7 to define functions $l_{\mathcal{R}_\varphi}(i, s)$ for $1 \leq s \leq s_u$ and $p^s \leq i \leq n$ that give the minimum valuation of φ_i due to a point (or lack thereof) above p^s on the ramification polygon $\mathcal{R}_\varphi$ of φ. By taking the maximum of these over all s, we define $L_{\mathcal{R}_\varphi}(i)$ so that $v_\pi(\varphi_i) \geq L_{\mathcal{R}_\varphi}(i)$ for $1 \leq i \leq n-1$.

Definition 3.8. Let $\mathcal{R}_\varphi$ be the ramification polygon of φ with points

$$\mathcal{R}_\varphi = \{(1, J_0), (p^{s_1}, J_1), \ldots, (p^{s_{u-1}}, J_{u-1}), (p^{s_u}, 0), \ldots, (n, 0)\},$$

and where $J_i = a_i n + b_i$ with $0 \leq b_i \leq n-1$. For $0 \leq t \leq u$, let

$$l_{\mathcal{R}_\varphi}(i, s_t) = \begin{cases} \max\{2 + a_t - v_\pi\binom{i}{p^{s_t}}, 1\} & \text{if } p^{s_t} \leq i < b_t, \\ \max\{1 + a_t - v_\pi\binom{i}{p^{s_t}}, 1\} & \text{if } i \geq b_t. \end{cases}$$

If there is no point above p^w with $s_t < w < s_{t+1}$, then for $p^w \leq i \leq n-1$, let

$$l_{\mathcal{R}_\varphi}(i, w) = \max\left\{\left\lceil\frac{1}{n}\left[\frac{J_{t+1} - J_t}{p^{s_{t+1}} - p^{s_t}}(p^w - p^{s_t}) + J_t - k\right] + 1 - v_\pi\binom{k}{p^w}\right\rceil, 1\right\}$$

Finally, set

$$L_{\mathcal{R}_\varphi}(i) = \begin{cases} 1 & \text{if } i = 0 \\ \max\{l_{\mathcal{R}_\varphi}(i,t) : p^t \le i\} & \text{if } 1 \le i \le n-1 \\ 0 & \text{if } i = n \end{cases}.$$

So far we have described many necessary conditions for ramification polygons. We now propose a necessary and sufficient description of a ramification polygon of an extension.

Proposition 3.9. *Let $\mathcal{P}$ be a convex polygon with points*

$$\mathcal{P} = \{(1, J_0), (p^{s_1}, J_1), \ldots, (p^{s_{u-1}}, J_{u-1}), (p^{s_u}, 0), \ldots, (n, 0)\},$$

where $J_i = a_i n + b_i$ with $0 \le b_i \le n-1$. There is an extension L/K with ramification polygon $\mathcal{P}$, if and only if

(a) *For each J_i, $\min\left\{v_\pi\binom{b_i}{p^{s_i}}n, v_\pi\binom{n}{p^{s_i}}n\right\} \le J_i \le v_\pi\binom{n}{p^{s_i}}n$.*

(b) *If $b_i = b_k$, then $a_i = a_k - v_\pi\binom{b}{p^{s_k}} + v_\pi\binom{b}{p^{s_i}}$ where $b_i = b_k$.*

(c) *For each point $(p^{s_i}, a_i n + b_i)$, we have that*

$$a_i \ge \begin{cases} 1 + a_t - v_\pi\binom{b_i}{p^{s_t}} + \binom{b_i}{p^{s_i}} & \text{if } p^{s_t} \le b_i < b_t \\ a_t - v_\pi\binom{b_i}{p^{s_t}} + \binom{b_i}{p^{s_i}} & \text{if } b_i \ge b_t \end{cases}$$

for all other points (p^{s_t}, J_t) with $J_t = a_t n + b_t \neq 0$.

(d) *If there is no point of $\mathcal{P}$ above p^i, with $s_t < i < s_{t+1}$, then for each point $(p^{s_k}, a_k n + b_k)$ of $\mathcal{P}$ with $b_k > p^i$,*

$$a_k > \frac{1}{n}\left[\frac{J_{t+1} - J_t}{p^{s_{t+1}} - p^{s_t}}(p^i - p^{s_t}) + J_t - b_k\right] - v_\pi\binom{b_k}{p^i} + v_\pi\binom{b_k}{p^{s_k}}.$$

(e) *The points with abscissa greater than p^{s_u} are $(i, 0)$ where $v_\pi\binom{n}{i} = 0$.*

Proof. Suppose $\mathcal{P}$ is the ramification polygon for L/K with generating Eisenstein polynomial φ. Assumption (a) follows from Lemma 3.6. If $b_i = b_k$, then by Lemma 3.5

$$v_\pi(\varphi_{b_i}) = a_i + 1 - v_\pi\binom{b_i}{p^{s_i}} = a_k + 1 - v_\pi\binom{b_i}{p^{s_k}}.$$

Thus $a_i = a_k - v_\pi\binom{b_i}{p^{s_k}} + v_\pi\binom{b_i}{p^{s_i}}$, giving us assumption (b). Let $(p^{s_i}, a_i n + b_i)$ be a point of $\mathcal{P}$, then by Lemma 3.5, we have that for all other points (p^{s_t}, J_t),

$$v_\pi(\varphi_{b_i}) = a_i + 1 - v_\pi\binom{b_i}{p^{s_i}} \ge \begin{cases} 2 + a_t - v_\pi\binom{b_i}{p^{s_t}} \text{ for } p^{s_t} \le b_i < b_t \\ 1 + a_t - v_\pi\binom{b_i}{p^{s_t}} \text{ for } b_i \ge b_t \end{cases},$$

from which we see assumption (c). If there no point of $\mathcal{P}$ above p^i, with $s_t < i < s_{t+1}$, then by Lemma 3.7, for each point $(p^{s_i}, a_i n + b_i)$ of $\mathcal{P}$ with $b_i > p^i$,

$$v_\pi(\varphi_{b_i}) = a_i + 1 - v_\pi\binom{b_i}{p^{s_i}} \ge \frac{1}{n}\left[\frac{J_{t+1} - J_t}{p^{s_{t+1}} - p^{s_t}}(p^i - p^{s_t}) + J_t - b_i\right] + 1 - v_\pi\binom{b_i}{p^i},$$

from which we have assumption (d). Assumption (e) is given by Lemma 3.4. Thus, if $\mathcal{P}$ is a ramification polygon of an extension L/K, then these properties are necessary.

Next we will show sufficiency by constructing a polynomial $\psi(x) = \sum \psi_i x^i \in \mathcal{O}_K[x]$ such that $\mathcal{R}_\psi = \mathcal{P}$. First, we let $\psi_n = 1$ and ψ_0 be an element of valuation 1 in $\mathcal{O}_K$. For each point

$(p^{s_i}, a_i n + b_i)$ in $\mathcal{P}$, with $b_i \neq 0$, let ψ_{b_i} be an element of $\mathcal{O}_K$ with valuation $1 + a_i - v_\pi\binom{b_i}{p^{s_i}}$. By assumption (b), ψ_{b_i} is well defined even if it is given by multiple points as those definitions coincide, and by assumption (a) we have that $v_\pi(\psi_{b_i}) \geq 1$. If ψ_j in $0 < j < n$ is not assigned by some b_i, we set $\psi_j = 0$. We now have an Eisenstein polynomial ψ, and we proceed by computing $\mathcal{R}_\psi$.

Let $\mathcal{R}_\psi$ be the ramification polygon of ψ, the Newton polygon $\mathcal{N}$ of the ramification polynomial $\rho(x) = \psi(\alpha x + \alpha)/(\alpha^n) \in K(\alpha)[x]$, where α is a root of ψ. Let $\rho(x) = \sum \rho_i x^i$. Let B be the set of nonzero b_i in the points of $\mathcal{P}$. For all $0 < i < n$ with $i \notin B$, $v_\pi(\psi_i) = \infty$, so we can simplify Equation (2) by only needing to consider terms $k \in B \cup \{n\}$ to

$$v_\alpha(\rho_i) = \min\left\{ \min_{k \in B, k \geq i} \left\{ n\left[v_\pi\left(\binom{k}{i}\psi_k\right) - 1\right] + k \right\}, n v_\pi\binom{k}{i} \right\}.$$

Substitution of our values for $v_\pi(\psi_{b_t})$ gives

$$v_\alpha(\rho_i) = \min\left\{ \min_{\{(p^{s_k}, J_k) \in \mathcal{P} : b_k \geq i\}} \left\{ n\left[a_k - v_\pi\binom{b_k}{p^{s_k}} + v_\pi\binom{b_k}{i}\right] + b_k \right\}, n v_\pi\binom{n}{i} \right\}.$$

Consider $(p^{s_i}, a_i n + b_i) \in \mathcal{P}$ and let us find $v_\alpha(\rho_{p^{s_i}})$. For $\mathcal{B} = \{(p^{s_k}, J_k) \in \mathcal{P} : b_k \geq p^{s_i}\}$ we have

$$v_\alpha(\rho_{p^{s_i}}) = \min\left\{ \min_{\mathcal{B}} \left\{ n\left[a_k - v_\pi\binom{b_k}{p^{s_k}} + v_\pi\binom{b_k}{p^{s_i}}\right] + b_k \right\}, n v_\pi\binom{n}{p^{s_i}} \right\} \tag{3}$$

If $b_i \neq 0$, then the $b_k = b_i$ term in the minimum is $a_i n + b_i$. For $(p^{s_k}, a_k n + b_k) \in \mathcal{P}$ with $p^{s_i} \leq b_k < b_i$, by assumption (c), we have $a_k \geq 1 + a_i - v_\pi\binom{b_k}{p^{s_i}} + \binom{b_k}{p^{s_k}}$. Thus, for all of the terms of (3) with $p^{s_i} \leq b_k < b_i$,

$$n\left[a_k - v_\pi\binom{b_k}{p^{s_k}} + v_\pi\binom{b_k}{p^{s_i}}\right] + b_k \geq n\left[1 + a_i\right] + b_k \geq a_i n + b_i$$

For points $(p^{s_k}, a_k n + b_k)$ on $\mathcal{P}$ with $b_k \geq b_i$, by assumption (c), we have $a_k \geq a_i - v_\pi\binom{b_k}{p^{s_i}} + \binom{b_k}{p^{s_k}}$. Thus, for all of the terms of Equation (3) with $b_k \geq b_i$,

$$n\left[a_k - v_\pi\binom{b_k}{p^{s_k}} + v_\pi\binom{b_k}{p^{s_i}}\right] + b_k \geq a_i n + b_k \geq a_i n + b_i$$

Thus $v_\alpha(\rho_{p^{s_i}}) = \min\left\{a_i n + b_i, n v_\pi\binom{n}{p^{s_i}}\right\}$, which is $a_i n + b_i$ by assumption (a). On the other hand, if $b_i = 0$, then $a_i = v_\pi\binom{n}{p^{s_i}}$, and for all of the terms of the inside minimum of Equation (3), as $a_k \geq a_i - v_\pi\binom{b_k}{p^{s_i}} + \binom{b_k}{p^{s_k}}$, we have

$$n\left[a_k - v_\pi\binom{b_k}{p^{s_k}} + v_\pi\binom{b_k}{p^{s_i}}\right] + b_k \geq a_i n + b_k \geq a_i n = n v_\pi\binom{n}{p^{s_i}}$$

So, $v_\alpha(\rho_{p^{s_i}}) = a_i n$, and all of the points of $\mathcal{P}$ are points of $\mathcal{R}_\psi$.

Suppose there is no point on $\mathcal{P}$ with abscissa p^i for some i with $s_t < i < s_{t+1}$. We take assumption (d)

$$a_k > \frac{1}{n}\left[\frac{J_{t+1} - J_t}{p^{s_{t+1}} - p^{s_t}}(p^i - p^{s_t}) + J_t - b_k\right] - v_\pi\binom{b_k}{p^i} + v_\pi\binom{b_k}{p^{s_k}},$$

and substitute it into Equation (3). After simplifying we get

$$v_\alpha(\rho_{p^i}) > \min\left\{\min_{\{(p^{s_k},J_k)\in\mathcal{P}:b_k\geq p^{s_i}\}}\left\{\frac{J_{t+1}-J_t}{p^{s_{t+1}}-p^{s_t}}(p^i-p^{s_t})+J_t\right\}, nv_\pi\binom{n}{p^{s_i}}\right\}.$$

As the $v_\alpha(\rho_{p^i})$ must be greater than the ordinate above p^i on the line segment between (p^{s_t}, J_t) and $(p^{s_{t+1}}, J_{t+1})$, there is no point on $\mathcal{R}_\psi$ with abscissa p^i. Finally, by Lemma 3.4, $\mathcal{R}_\psi$ has points satisfying assumption (e). Thus $\mathcal{R}_\psi = \mathcal{P}$. □

Using the conditions of Proposition 3.9, we can enumerate all possible ramification polygons for extensions over a p-adic field with given degree and discriminant. Such an algorithm is described in [22].

Proposition 3.10. *An Eisenstein polynomial φ has ramification polygon $\mathcal{R}$ with points*

$$\mathcal{R} = \{(1, J_0), (p^{s_1}, J_1), \ldots, (p^{s_{u-1}}, J_{u-1}), (p^{s_u}, 0), \ldots, (n, 0)\},$$

where $J_i = a_i n + b_i$ with $0 \leq b_i \leq n-1$, if and only if

(a) $v_\pi(\varphi_i) \geq L_\mathcal{R}(i)$
(b) *For $0 \leq t \leq u$, $v_\pi(\varphi_{b_t}) = L_\mathcal{R}(b_t)$ if $b_t \neq 0$.*

where $L_\mathcal{R}$ is as defined in Definition 3.8.

Proof. If φ has ramification polygon $\mathcal{R}$, then this is the result of Lemmas 3.5 and 3.7.

Suppose φ satisfies these assumptions and ρ is the ramification polynomial of φ. If $(p^{s_t}, J_t = a_t n + b_t)$ is a point of $\mathcal{R}$, then substitution of $l_\mathcal{R}(k, s_t)$ for $v_\pi(\varphi_k)$ into Equation (2) gives us

$$v_\alpha(\rho_{p^{s_t}}) = \min\left\{\min_{p^{s_t}\leq k<b_t}\{na_t+n+k\}, \min_{b_t\leq k<n}\{na_t+k\}, nv_\pi\binom{n}{p^{s_t}}\right\}$$

If $b_t = 0$, then this reduces to

$$v_\alpha(\rho_{p^{s_t}}) = \min\left\{na_t+n+p^{s_t}, nv_\pi\binom{n}{p^{s_t}}\right\} = nv_\pi\binom{n}{p^{s_t}} = J_t.$$

as $na_t + n + p^{s_t} \geq J_t = nv_\pi\binom{n}{p^{s_t}}$, by Proposition 3.9 (a). If $b_t \neq 0$, then this reduces to

$$v_\alpha(\rho_{p^{s_t}}) = \min\left\{na_t+b_t, nv_\pi\binom{n}{p^{s_t}}\right\} = na_t+b_t = J_t$$

as $J_t \leq nv_\pi\binom{n}{p^{s_t}}$, by Proposition 3.9 (a). So $\mathcal{R}_\varphi$ contains the points of $\mathcal{R}$.

If there is no point on $\mathcal{R}$ with abscissa p^i, with $s_t < i < s_{t+1}$, then for k in $p^i \leq k \leq n$,

$$v_\pi(\varphi_k) \geq l_\mathcal{R}(k,i) > \frac{1}{n}\left[\frac{J_{t+1}-J_t}{p^{s_{t+1}}-p^{s_t}}(p^i-p^{s_t})+J_t-k\right]+1-v_\pi\binom{k}{p^i}.$$

Some algebraic manipulation of this inequality gives us

$$\frac{J_{t+1}-J_t}{p^{s_{t+1}}-p^{s_t}}(p^i-p^{s_t})+J_t < n\left[v_\pi\left(\binom{k}{p^i}\varphi_k\right)-1\right]+k,$$

which shows that $v_\alpha(\rho_{p^i}) = \min_{p^i\leq k\leq n}\left\{n\left[v_\pi\left(\binom{k}{p^i}\varphi_k\right)-1\right]+k\right\}$ is greater than the value above p^i on the segment from (p^{s_t}, J_t) to $(p^{s_{t+1}}, J_{t+1})$. So there is no point on $\mathcal{R}_\varphi$ above p^i, and thus $\mathcal{R}_\varphi = \mathcal{R}$. □

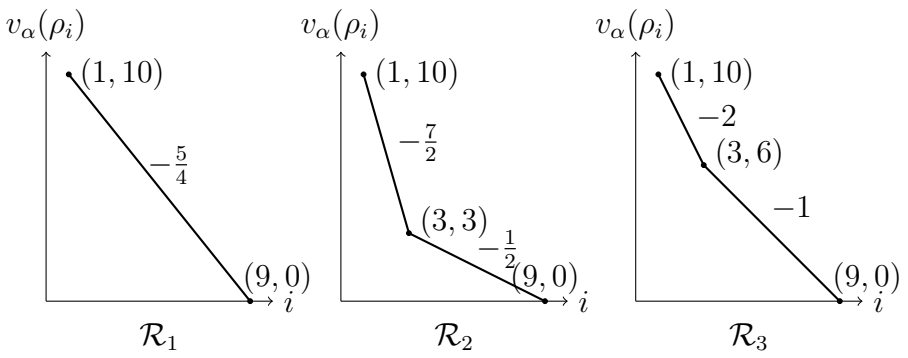

FIGURE 2. Possible ramification polygons of extensions L of $\mathbb{Q}_3$ of degree 9 with $v_3(\mathrm{disc}\,(L)) = 18$: $\mathcal{R}_1 = \{(1,10),(9,0)\}$, $\mathcal{R}_2 = \{(1,10),(3,3),(9,0)\}$, and $\mathcal{R}_3 = \{(1,10),(3,6),(9,0)\}$.

Definition 3.11. We call a polygon $\mathcal{R}$ with points

$$\mathcal{R} = \{(1, J_0), (p^{s_1}, J_1), \ldots, (p^{s_{u-1}}, J_{u-1}), (p^{s_u}, 0), \ldots, (n, 0)\},$$

that fulfills the conditions of Proposition 3.9 a *ramification polygon*. We call the function $\phi_{\mathcal{R}} : \mathbb{R}^{>0} \to \mathbb{R}^{>0}$, $\lambda \mapsto \min_{0\le i\le u}\{\frac{1}{n}(J_i + \lambda p^{s_i})\}$ the *Hasse-Herbrand function* of $\mathcal{R}$.

Remark 3.12. The function $\phi_{\mathcal{R}}$ in Definition 3.11 agrees with the connections between the ramification polygon and the Hasse-Herbrand transition function as observed in [10, 9]. Note that these works define the ramification polygon as the Newton polygon of $\varphi(x+\alpha)$. For normal extensions L/K, our function $\phi_{\mathcal{R}}$ agrees with the classical $\phi_{L/K}$ defined in [21, 3]. For non-Galois extensions, our function agrees with the transition function for ramification sets defined by Helou in [7].

Example 3.13 (Example 2.4 continued)**.** There are three possible ramification polygons for extensions L of $\mathbb{Q}_3$ of degree 9 with $v_3(\mathrm{disc}\,(L)) = 18$, namely $\mathcal{R}_1 = \{(1,10),(9,0)\}$, $\mathcal{R}_2 = \{(1,10),(3,3),(9,0)\}$, and $\mathcal{R}_3 = \{(1,10),(3,6),(9,0)\}$ (see Figure 2).

Since by Lemma 3.5 we have $\boldsymbol{v(\varphi_3) = 1^\dagger}$, the polynomials φ generating extensions with ramification polygon $\mathcal{R}_2$ are given by:

	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
3^4	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}
3^3	{0}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}
3^2	{0}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{1,2}	{0,1,2}
3^1	{0}	{0}	{0}	{0,1,2}	{0}	{0}	**{1,2}†**	{0}	{0}	{1,2}
3^0	{1}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}

4. Residual Polynomials of Segments

Residual (or associated) polynomials were introduced by Ore [15]. They yield information about the unramified part of the extension generated by the factors of a polynomial. This makes them a useful tool in the computation of ideal decompositions and integral bases [5, 12, 13] and the closely related problem of polynomial factorization over local fields [6, 18].

Definition 4.1 (Residual polynomial)**.** Let L be a finite extension of K with uniformizer α. Let $\rho(x) = \sum_i \rho_i x^i \in \mathcal{O}_L[x]$. Let $\mathcal{S}$ be a segment of the Newton polygon of ρ of length l with endpoints $(k, v_\alpha(\rho_k))$ and $(k+l, v_\alpha(\rho_{k+l}))$, and slope $-h/e = (v_\alpha(\rho_{k+l}) - v_\alpha(\rho_k))/l$ then

$$\underline{A}(x) = \sum_{j=0}^{l/e} \underline{\rho_{je+k}\alpha^{jh-v_\alpha(\rho_k)}} x^j \in \underline{K}[x]$$

is called the *residual polynomial* of $\mathcal{S}$.

Remark 4.2. The ramification polygon of a polynomial φ and the residual polynomials of its segments yield a subfield M of the splitting field N of φ, such that N/M is a p-extension [4, Theorem 9.1].

From the definition we obtain some of the properties of residual polynomials.

Lemma 4.3. *Let L be a finite extension of K with uniformizer α. Let $\rho \in \mathcal{O}_L[x]$. Let $\mathcal{N}$ be the Newton polygon of ρ with segments $\mathcal{S}_1, \dots, \mathcal{S}_\ell$ and let $\underline{A}_1, \dots, \underline{A}_\ell$ be the corresponding residual polynomials.*

(a) *If $\mathcal{S}_i$ has integral slope $-h \in \mathbb{Z}$ with endpoints $(k, v_\alpha(\rho_k))$ and $(k+l, v_\alpha(\rho_{k+l}))$ then $\underline{A}_i(x) = \sum_{j=0}^{l} \underline{\rho_{j+k}\alpha^{jh-v_\alpha(\rho_k)}}\, x^j = \underline{\rho(\alpha^h x)\alpha^{-k-v_\alpha(\rho_k)}}\, x^{n-l} \in \underline{K}[x]$.*

(b) *If for $1 \le i \le \ell - 1$ the leading coefficient of $\underline{A}_i$ is denoted by $\underline{A}_{i,\deg \underline{A}_i}$ and $\underline{A}_{i+1,0}$ is the constant coefficient of $\underline{A}_{i+1}$ then $\underline{A}_{i,\deg \underline{A}_i} = \underline{A}_{i+1,0}$.*

(c) *If ρ is monic then $\underline{A}_\ell$ is monic.*

From now on we consider the residual polynomials of the segments of a ramification polygon. From the definition of the residual polynomials and Lemma 3.4 we obtain:

Proposition 4.4. *Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein of degree $n = p^r e_0$ with $\gcd(p, e_0) = 1$, let α be a root of φ, ρ the ramification polynomial, and $\mathcal{R}_\varphi$ the ramification polygon of φ.*

(a) *If $e_0 \neq 1$ then $\mathcal{R}_\varphi$ has a horizontal segment of length $p^r(e_0-1)$ with residual polynomial $\underline{A} = \sum_{i=0}^{n-p^r} \underline{A}_i x^i$ where $\underline{A}_i = \underline{\binom{n}{i}} \neq \underline{0}$ if and only if $v_\alpha \binom{n}{i} = 0$.*

(b) *If $(p^{s_k}, J_k), \dots, (p^{s_l}, J_l)$ are the points on a segment $\mathcal{S}$ of $\mathcal{R}_\varphi$ of slope $-\frac{h}{e}$, then the residual polynomial of $\mathcal{S}$ is*

$$\underline{A}(x) = \sum_{i=k}^{l} \underline{\rho_{p^{s_i}}\alpha^{-J_i}}\, x^{(p^{s_i}-p^{s_k})/e} = \sum_{i=k}^{l} \underline{\varphi_{b_i}\tbinom{b_i}{p^{s_i}}\alpha^{-a_i n - n}}\, x^{(p^{s_i}-p^{s_k})/e}.$$

We now give criteria for the existence of polynomials with given ramification polygon $\mathcal{R}$ and given residual polynomials.

Proposition 4.5. *Let $n = p^r e_0$ with $\gcd(p, e_0) = 1$ and let*

$$\mathcal{R} = \{(1, J_0), (p^{s_1}, J_1), \dots, (p^{s_k}, J_k), \dots, (p^r, 0), \dots, (p^r e_0, 0)\}.$$

be a ramification polygon. Write $J_k = a_k n + b_k$ with $0 \le b_k \le n$. Let $\mathcal{S}_1, \dots, \mathcal{S}_\ell$ be the segments of $\mathcal{R}$ with endpoints (p^{k_i}, J_{k_i}) and (p^{l_i}, J_{l_i}) and slopes $-h_i/e_i$ $(1 \le i < \ell)$. For $1 \le i < \ell$ let $\underline{A}_i(x) = \sum_{j=0}^{(p^{l_i}-p^{k_i})/e_i} \underline{A}_{i,j} x^j \in \underline{K}$.

There is an Eisenstein polynomial of degree $p^r e_0$ with ramification polygon $\mathcal{R}$ and segments $\mathcal{S}_1, \dots, \mathcal{S}_\ell$ with residual polynomials $\underline{A}_1, \dots, \underline{A}_\ell \in \underline{K}[x]$ if and only if

(a) $\underline{A}_{i,\deg \underline{A}_i} = \underline{A}_{i+1,0}$ *for* $1 \le i < \ell$,

(b) $\underline{A}_{i,j} \neq 0$ *if and only if* $j = (q - p^{s_{k_i}})/e_i$ *for some* $q \in \{p^{s_1}, \ldots, p^r\}$ *with* $p^{k_i} \leq q \leq p^{l_i}$,
(c) *if for some* $1 \leq t, q \leq u$ *we have* $b_t = b_q$ *and* $s_{k_i} \leq s_t \leq s_{l_i}$ *and* $s_{k_j} \leq s_q \leq s_{l_j}$ *then*

$$\underline{A}_{i,(p^{s_t} - p^{s_{k_i}})/e_i} = \underline{\binom{b_t}{p^{s_t}}\binom{b_t}{p^{s_q}}^{-1}(-\varphi_0)^{a_q - a_t}}\,\underline{A}_{j,(p^{s_q} - p^{s_{k_j}})/e_j}.$$

Proof. Suppose that φ is an Eisenstein polynomial of degree $p^r e_0$ with ramification polygon $\mathcal{R}$ and segments $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ with residual polynomials $\underline{A}_1, \ldots, \underline{A}_\ell \in \underline{K}[x]$. Property (a) is given by Lemma 4.3 (b) and property (b) is given by Proposition 4.4 (b). To establish property (c), suppose that for some $1 \leq t, q \leq u$ we have $b_t = b_q$ and $s_{k_i} \leq s_t \leq s_{l_i}$ and $s_{k_j} \leq s_q \leq s_{l_j}$. From Proposition 4.4, we have that

$$\underline{A}_{i,(p^{s_t} - p^{s_{k_i}})/e_i} = \varphi_{b_t}\tbinom{b_t}{p^{s_t}}\alpha^{-a_t n - n} \text{ and } \underline{A}_{j,(p^{s_q} - p^{s_{k_j}})/e_j} = \varphi_{b_q}\tbinom{b_q}{p^{s_q}}\alpha^{-a_q n - n}.$$

As $b_t = b_q$, we have that $\varphi_{b_t} = \varphi_{b_q}$. Since

$$\underline{A}_{i,(p^{s_t} - p^{s_{k_i}})/e_i}\tbinom{b_t}{p^{s_t}}^{-1}\alpha^{a_t n + n} = \varphi_{b_t} = \varphi_{b_q} = \underline{A}_{j,(p^{s_q} - p^{s_{k_j}})/e_j}\tbinom{b_t}{p^{s_q}}^{-1}\alpha^{a_q n + n},$$

we have

$$\underline{A}_{i,(p^{s_t} - p^{s_{k_i}})/e_i} = \tbinom{b_t}{p^{s_t}}\tbinom{b_t}{p^{s_q}}^{-1}(-\varphi_0)^{a_q - a_t}\underline{A}_{j,(p^{s_q} - p^{s_{k_j}})/e_j}.$$

Conversely, suppose that $\mathcal{R}$ is a ramification polygon with segments $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ with residual polynomials $\underline{A}_1, \ldots, \underline{A}_\ell \in \underline{K}[x]$ with properties (a), (b), and (c) of the proposition. Let $\psi \in \mathcal{O}_K[x]$ with $\psi_{e_0 p^r} = 1$, $v_\pi(\psi_0) = 1$, and

$$\underline{\psi}_{b_t, 1 + a_t - v_\pi\left(\frac{b_t}{p^{s_t}}\right)} = \underline{A}_{i,(p^{s_t} - p^{s_{k_i}})/e_i}\underline{\binom{b_t}{p^{s_t}}^{-1}(-\psi_{0,1})^{a_t+1}\pi^{v_\pi\left(\frac{b_t}{p^{s_t}}\right)}}$$

for i with $p^{k_i} \leq p^{s_t} \leq p^{l_i}$ for each point $(p^{s_t}, a_t n + b_t)$ in $\mathcal{R}$. For ψ to be well defined, we must check that the same coefficient is not assigned different values. Multiple assignments occur at vertices (when one point contributes to two $\underline{A}_i$) and when multiple points have the same b_t. If $(p^{s_t}, a_t n + b_t)$ is a vertex of $\mathcal{R}$, then we have

$$\begin{aligned}\underline{\psi}_{b_t, 1 + a_t - v_\pi\left(\frac{b_t}{p^{s_t}}\right)} &= \underline{A}_{i,(p^{s_t} - p^{s_{k_i}})/e_i}\underline{\binom{b_t}{p^{s_t}}^{-1}(-\psi_{0,1})^{a_t+1}\pi^{v_\pi\left(\frac{b_t}{p^{s_t}}\right)}} \\ &= \underline{A}_{i+1,(p^{s_t} - p^{s_{k_{i+1}}})/e_{i+1}}\underline{\binom{b_t}{p^{s_t}}^{-1}(-\psi_{0,1})^{a_t+1}\pi^{v_\pi\left(\frac{b_t}{p^{s_t}}\right)}}.\end{aligned}$$

Cancellation gives us $\underline{A}_{i,(p^{s_t} - p^{s_{k_i}})/e_i} = \underline{A}_{i+1,(p^{s_t} - p^{s_{k_{i+1}}})/e_{i+1}}$. As a vertex, p^{s_t} is the abscissa of both the right endpoint of $\mathcal{S}_i$ ($p^{s_{l_i}} = p^{s_t}$) and the left endpoint of $\mathcal{S}_{i+1}$ ($p^{s_{k_{i+1}}} = p^{s_t}$). Thus $(p^{s_t} - p^{s_{k_i}})/e_i = \deg \underline{A}_i$ and $(p^{s_t} - p^{s_{k_{i+1}}})/e_{i+1} = 0$. So, $\underline{A}_{i,\deg \underline{A}_i} = \underline{A}_{i+1,0}$, which is property (a). On the other hand, if for some $1 \leq t, q \leq u$, we have $b_t = b_q$, with $s_{k_i} \leq s_t \leq s_{l_i}$ and $s_{k_j} \leq s_q \leq s_{l_j}$, then let $b = b_t = b_q$ and we have

$$\underline{\psi}_{b, 1 + a_t - v_\pi\left(\frac{b_t}{p^{s_t}}\right)} = \underline{A}_{i,(p^{s_t} - p^{s_{k_i}})/e_i}\underline{\binom{b}{p^{s_t}}^{-1}(-\psi_{0,1})^{a_t+1}\pi^{v_\pi\left(\frac{b}{p^{s_t}}\right)}}$$

$$\underline{\psi}_{b, 1 + a_q - v_\pi\left(\frac{b}{p^{s_q}}\right)} = \underline{A}_{j,(p^{s_q} - p^{s_{k_j}})/e_j}\underline{\binom{b}{p^{s_q}}^{-1}(-\psi_{0,1})^{a_q+1}\pi^{v_\pi\left(\frac{b}{p^{s_q}}\right)}}.$$

As $\mathcal{R}$ is a ramification polygon, by Proposition 3.9 (b), $b_t = b_q$ implies that $a_t = a_q - v_\pi\binom{b}{p^{s_q}} + v_\pi\binom{b}{p^{s_t}}$, so we have that $1 + a_t - v_\pi\binom{b}{p^{s_t}} = 1 + a_q - v_\pi\binom{b}{p^{s_q}}$. These two assignments of coefficients of ψ_b set the same coefficient, and by property (c), they have the same value. Thus, ψ is well-defined, and we have set at most one π-adic coefficient for each polynomial coefficient.

By property (b), none of the assigned coefficients are zero and no others are non-zero. Thus, $v_\pi(\psi_{b_t}) = 1 + a_t - v_\pi\binom{b_t}{p^{s_t}}$, and as per the construction in the proof of Proposition 3.9, ψ is an Eisenstein polynomial with ramification polygon $\mathcal{R}$.

Next we consider the residual polynomials of the segments of $\mathcal{R}$ as given by ψ. Let $\mathcal{S}_i$ be a segment of $\mathcal{R}$ containing points $(p^{s_k}, J_k), \dots, (p^{s_l}, J_l)$ of slope $-h_i/e_i$. Let $\underline{A}_i^*$ be the residual polynomial of $\mathcal{S}_i$. From Proposition 4.4, for each point $(p^{s_t}, a_t n + b_t)$ with $s_k \le s_t \le s_l$, we get

$$\underline{A}^*_{i,(p^{s_t}-p^{s_k})/e} = \underline{\psi_{b_t}\binom{b_t}{p^{s_t}}\alpha^{-a_t n - n}}.$$

We need the right side to reduce to our intended value. By our assignment,

$$\underline{\psi}_{b_t} = \underline{A}_{i,(p^{s_t}-p^{s_{k_i}})/e_i}\underline{\binom{b_t}{p^{s_t}}^{-1}(-\psi_{0,1})^{a_t+1}\pi^{v_\pi\binom{b_t}{p^{s_t}}}\pi^{1+a_t-v_\pi\binom{b_t}{p^{s_t}}}}.$$

With $\alpha^n \sim -\mathrm{N}_{K(\alpha)/K}(\alpha) = -\psi_0 \sim -\psi_{0,1}\pi$ we get

$$\underline{A}^*_{i,(p^{s_t}-p^{s_k})/e} = \underline{\psi_{b_t}\tbinom{b_t}{p^{s_t}}\alpha^{-a_t n - n}} = \underline{A}_{i,(p^{s_t}-p^{s_{k_i}})/e_i}\underline{\tbinom{b_t}{p^{s_t}}^{-1}(-\psi_{0,1})^{a_t+1}\pi^{v_\pi\binom{b_t}{p^{s_t}}}\pi^{1+a_t-v_\pi\binom{b_t}{p^{s_t}}}\tbinom{b_t}{p^{s_t}}(-\psi_{0,1}\pi)^{-a_t-1}}$$

from which cancellation gives us our desired result $\underline{A}^*_{i,(p^{s_t}-p^{s_k})/e} = \underline{A}_{i,(p^{s_t}-p^{s_k})/e}$. □

4.1. **The invariant $\mathcal{A}$ of L/K.** We introduce an invariant of L/K, that is compiled from the residual polynomials of the segments of the ramification polygon of φ. From the proof of [4, Proposition 4.4] we obtain:

Lemma 4.6. *Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein and α a root of φ and $L = K(\alpha)$. Let $\mathcal{S}$ be a segment of the ramification polygon of φ of slope $-h/e$ and let $\underline{A}$ be its residual polynomial. Let $\beta = \delta\alpha$ with $v_\alpha(\delta) = 0$ be another uniformizer of L and ψ its minimal polynomial. If $\underline{\gamma}_1, \dots, \underline{\gamma}_m$ are the (not necessarily distinct) zeros of $\underline{A}$ then $\underline{\gamma}_1/\underline{\delta}^h, \dots, \underline{\gamma}_m/\underline{\delta}^h$ are the zeros of the residual polynomial of the segment of slope $-h/e$ of the ramification polygon of ψ.*

Thus the zeros of the residual polynomials of all segments of the ramification polygon change by powers of the same element $\underline{\delta}$ when transitioning from a uniformizer α to a uniformizer $\delta\alpha$. With Proposition 4.5 we obtain:

Theorem 4.7. *Let $\mathcal{S}_1, \dots, \mathcal{S}_\ell$ be the segments of the ramification polygon $\mathcal{R}$ of an Eisenstein polynomial $\varphi \in \mathcal{O}_K[x]$. For $1 \le i \le \ell$ let $-h_i/e_i$ be the slope of $\mathcal{S}_i$ and $\underline{A}_i$ its residual polynomial. Then*

$$\mathcal{A} = \left\{\left(\gamma_{\delta,1}\underline{A}_1(\underline{\delta}^{h_1}x), \dots, \gamma_{\delta,\ell}\underline{A}_\ell(\underline{\delta}^{h_\ell}x)\right) : \underline{\delta} \in \underline{K}^\times\right\} \tag{4}$$

where $\gamma_{\delta,\ell} = \underline{\delta}^{-h_\ell \deg \underline{A}_\ell}$, and $\gamma_{\delta,i} = \gamma_{\delta,i+1}\underline{\delta}^{-h_i \deg \underline{A}_i}$ for $1 \le i \le \ell - 1$ is an invariant of the extension $K[x]/(\varphi)$.

Example 4.8. Let $\varphi(x) = x^9 + 6x^3 + 9x + 3$. The ramification polygon of φ consists of the two segments with end points $(1, 10), (3, 3)$ and $(3, 3), (9, 0)$ and residual polynomials $1 + 2x$ and $2 + x^3$. We get

$$\mathcal{A} = \{(1 + 2x, 2 + x^3), (1 + x, 1 + x^3)\}.$$

4.2. **Generating Polynomials.** We show how the choice of a representative of the invariant $\mathcal{A}$ determines some of the coefficients of the generating polynomials with this invariant.

Lemma 4.9. *Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein of degree n. Let $\mathcal{S}$ be a segment of the ramification polygon of φ with endpoints $(p^{s_k}, a_k n + b_k)$ and $(p^{s_l}, a_l n + b_l)$ and residual polynomial $\underline{A}(x) = \sum_{j=1}^{p^{s_l}-p^{s_k}} \underline{A}_j x^j \in \underline{K}[x]$. If $(p^{s_i}, a_i n + b_i)$ is a point on $\mathcal{S}$ with $b_i \neq 0$ then the leading coefficient $\varphi_{b_i,j}$ of the π-adic expansion of φ_{b_i} is*

$$\underline{\varphi}_{b_i,j} = \underline{A}_{(p^{s_i}-p^{s_k})/e} \underline{\binom{b_i}{p^{s_i}}^{-1} (-\varphi_{0,1})^{a_i+1} \pi^{v_\pi\left(\binom{b_i}{p^{s_i}}\right)}}$$

where $j = a_i + 1 - v_\pi\binom{b_i}{p^{s_i}}$.

Proof. By Lemma 3.5, $v_\pi(\varphi_{b_i}) = j$ and by Proposition 4.4

$$\underline{A}(x) = \sum_{i=k}^{l} \underline{\varphi_{b_i}\binom{b_i}{p^{s_i}}\alpha^{-a_i n - n}}\, x^{(p^{s_i}-p^{s_k})/e}.$$

Thus $\underline{A}_{(p^{s_i}-p^{s_k})/e} = \underline{\varphi_{b_i}\binom{b_i}{p^{s_i}}\alpha^{-a_i n - n}}$. With $\alpha^n \sim -\mathrm{N}_{K(\alpha)/K}(\alpha) = -\varphi_0 \sim -\varphi_{0,1}\pi$ we get

$$\underline{A}_{(p^{s_i}-p^{s_k})/e} = \underline{\varphi_{b_i}\binom{b_i}{p^{s_i}}(-\varphi_0)^{-a_i-1}}.$$

As by Lemma 3.4 $v_\alpha(\varphi_{b_i}) = v_\alpha(\rho_{p^{s_i}}) - v_\alpha\binom{b_i}{p^{s_i}} - b_i + n = a_i n + b_i - v_\alpha\binom{b_i}{p^{s_i}} - b_i + n = n(a_i + 1) - v_\alpha\binom{b_i}{p^{s_i}}$ we have $\varphi_{b_i} \sim \varphi_{b_i,j}\pi^{a_i+1-v_\pi\binom{b_i}{p^{s_i}}}$. Therefore

$$\begin{aligned}\underline{A}_{(p^{s_i}-p^{s_k})/e} &= \underline{\varphi_{b_i,j}\binom{b_i}{p^{s_i}}(-\varphi_{0,1}\pi)^{-a_i-1}\pi^{a_i+1-v_\pi\binom{b_i}{p^{s_i}}}} \\ &= \underline{\varphi}_{b_i,j}(-\underline{\varphi}_{0,1})^{-a_i-1}\underline{\binom{b_i}{p^{s_i}}\pi^{-v_\pi\binom{b_i}{p^{s_i}}}}.\end{aligned}$$

□

A change of the uniformizer α of $L = K(\alpha)$ to $\delta\alpha$ with $v(\delta) = 0$ that determines the representative $(\underline{A}_1, \ldots, \underline{A}_\ell) \in \mathcal{A}$ also effects the constant coefficient of the generating polynomial. Namely since L/K is totally ramified we can find $\gamma \in K$ such that $\delta \sim \gamma$. Now if the Eisenstein polynomial $\varphi(x) = x^n + \sum_{i=0}^{n-1} \varphi_i x^i \in \mathcal{O}_K[x]$ is the minimal polynomial of α then

$$\psi(x) = \gamma^n \varphi\left(\frac{x}{\gamma}\right) = x^n + \sum_{i=0}^{n-1} \varphi_i \gamma^{n-i} x^i.$$

with $\psi_{0,1} = \gamma^n \varphi_{0,1}$ is the minimal polynomial of $\gamma\alpha$.

Lemma 4.10. *Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein of degree n and $\underline{S}_0 : \underline{K} \to \underline{K}, a \mapsto a^n$.*

(a) *If and only if $\underline{\delta} \in \underline{S}_0(\underline{K})$, there is $\psi \in \mathcal{O}_K[x]$ Eisenstein with $\underline{\psi}_{0,1} = \underline{\delta}\underline{\varphi}_{0,1}$ such that $K[x]/(\psi) \cong K[x]/(\varphi)$.*

(b) *If $n = p^r$ for some $r \in \mathbb{Z}^{>0}$ then $\underline{S}_0$ is surjective and there is $\psi \in \mathcal{O}_K[x]$ Eisenstein with $\underline{\psi}_{0,1} = 1$ such that $K[x]/(\psi) \cong K[x]/(\varphi)$.*

This corresponds to the reduction step 0 in Monge's reduction [11, Algorithm 1]. If $n = p^r e_0$ with $\gcd(p, e_0) = 1$ then $\underline{\varphi}_{0,1}$ determines the tamely ramified subextensions of $K[x]/(\varphi)$, that can be generated by $x^{e_0} + \varphi_{0,1}\pi$.

If we fix $\varphi_{0,1}$ then the set of representatives of $\mathcal{A}$ becomes

$$\mathcal{A}^* = \left\{ \left(\gamma_{\delta,1} \underline{A}_1(\underline{\delta}^{h_1} x), \dots, \gamma_{\delta,\ell} \underline{A}_\ell(\underline{\delta}^{h_\ell} x) \right) : \underline{\delta} \in \underline{K}^\times, \underline{\delta}^n = 1 \right\} \tag{5}$$

where $\gamma_{\delta,\ell} = \delta^{-h_\ell \deg \underline{A}_\ell}$, and $\gamma_{\delta,i} = \gamma_{\delta,i+1} \delta^{-h_i \deg \underline{A}_i}$ for $1 \le i \le \ell - 1$. Thus fixing $\varphi_{0,1}$ yields a partition of $\mathcal{A}$. Also, if n is a power of p then $\mathcal{A}^*$ contains exactly one representative of $\mathcal{A}$.

Remark 4.11. Let $\mathcal{R}$ be a ramification polygon and let $\underline{A}_1, \dots, \underline{A}_\ell \in \underline{K}[x]$ satisfying Proposition 4.5. Let $\mathcal{A}$ as in Theorem 4.7 and $\mathcal{A} = \mathcal{A}^{*1} \cup \dots \cup \mathcal{A}^{*k}$ be the partition of $\mathcal{A}$ into sets as in Equation (5). Let $\underline{\gamma} \in \underline{K}^\times$. Then there is no transformation $\delta\alpha$ of the uniformizer α of an extension with $\mathcal{R}$ and residual polynomials in $\mathcal{A}^{*i}$ for some $1 \le i \le k$ generated by $\varphi \in \mathcal{O}_K[x]$ with $\underline{\varphi}_{0,1} = \underline{\gamma}$ such that the residual polynomials of the segments of $\mathcal{R}_\varphi = \mathcal{R}$ is not in $\mathcal{A}^{*i}$. Thus the construction of generating polynomials for all extensions with $\mathcal{R}$ and $\mathcal{A}$ can be reduced to constructing polynomials with residual polynomials in the sets $\mathcal{A}^{*i}$.

Lemma 4.12. *Let $(\underline{A}_1, \dots, \underline{A}_\ell) \in \mathcal{A}^*$. If $\psi \in \mathcal{O}_K[x]$ is a polynomial with residual polynomials in $\mathcal{A}^*$, then there is a polynomial $\varphi \in \mathcal{O}_K[x]$ with residual polynomials $(\underline{A}_1, \dots, \underline{A}_\ell)$ such that $K[x]/(\psi) \cong K[x]/(\varphi)$.*

Proof. Let $\underline{A}'_1, \dots, \underline{A}'_\ell$ be the residual polynomials of ψ. As $(\underline{A}'_1, \dots, \underline{A}'_\ell) \in \mathcal{A}^*$ there exists a $\underline{\delta} \in \underline{K}^\times$ with $\underline{\delta}^n = 1$ so that

$$(\underline{A}_1, \dots, \underline{A}_\ell) = \left(\gamma_{\delta,1} \underline{A}'_1(\underline{\delta}^{h_1} x), \dots, \gamma_{\delta,\ell} \underline{A}'_\ell(\underline{\delta}^{h_\ell} x) \right).$$

where $\gamma_{\delta,\ell} = \delta^{-h_\ell \deg \underline{A}_\ell}$, and $\gamma_{\delta,i} = \gamma_{\delta,i+1} \delta^{-h_i \deg \underline{A}_i}$ for $1 \le i \le \ell - 1$.

Let α be a root of ψ and $\varphi(x) = \delta^n \psi(\delta^{-1} x)$ be the minimal polynomial of $\delta\alpha$. This gives us that $K[x]/(\psi) \cong K[x]/(\varphi)$.

Let us find the residual polynomials of φ. From Proposition 4.4, we have that the residual polynomial for a segment $\mathcal{S}_i$ of slope h/e with endpoints $(p^{s_{k_i}}, J_{k_i} = a_{k_i} n + b_{k_i})$ and $(p^{s_{l_i}}, J_{l_i} = a_{l_i} n + b_{l_i})$ is

$$\sum_{j=k_i}^{l_i} \underline{\varphi_{b_j} \tbinom{b_j}{p^{s_j}} \alpha^{-a_j n - n}} \, x^{(p^{s_j} - p^{s_{k_i}})/e}.$$

Performing our substitution we have that this polynomial is

$$\sum_{j=k_i}^{l_i} \underline{\delta^{n-b_j} \psi_{b_j} \tbinom{b_j}{p^{s_j}} (\delta\alpha)^{-a_j n - n}} \, x^{(p^{s_j} - p^{s_{k_i}})/e} = \sum_{j=k_i}^{l_i} \underline{\delta^{n-b_j-a_j n-n}} \, \underline{A}'_{i,j} = \sum_{j=k_i}^{l_i} \underline{\delta^{-J_j}} \, \underline{A}'_{i,j}.$$

Next, let us perform the deformation of $\underline{A}'_i$ by δ. First, we consider $\gamma_{\delta,i}$. Notice that for the $\underline{A}'_i$, the residual polynomial of the segment $\mathcal{S}_i$ with endpoints $(p^{s_{k_i}}, J_k)$ and $(p^{s_{l_i}}, J_l)$,

$$\underline{\delta}^{-h_i \deg \underline{A}'_i} = \underline{\delta}^{\lambda_i (p^{s_{l_i}} - p^{s_{k_i}})} = \underline{\delta}^{J_{l_i} - J_{k_i}} = \begin{cases} \underline{\delta}^{J_{l_1} - J_{k_1}} & \text{if } i = 1 \\ \underline{\delta}^{J_{l_i} - J_{l_{i-1}}} & \text{if } 2 \le i < \ell \\ \underline{\delta}^{-J_{l_{\ell-1}}} = \underline{\delta}^{-J_{k_\ell}} & \text{if } i = \ell \end{cases}.$$

This shows us that for $1 \le i \le \ell-1$, $\gamma_{\delta,i} = \gamma_{\delta,i+1}\delta^{-h_i \deg \underline{A}'_i} = \underline{\delta}^{-J_{k_i}}$, and in general, $\gamma_{\delta,i} = \underline{\delta}^{-J_{k_i}}$. So the deformation of $\underline{A}'_i$ by δ is

$$\begin{aligned}\underline{A}_i = \gamma_{\delta,i}\underline{A}'_{i,j}(\delta^{h_i}x) &= \underline{\delta}^{-J_{k_i}} \sum_{j=k_i}^{l_i} \underline{A}'_{i,j}\underline{\delta^{-\lambda_i(p^{s_j}-p^{s_{k_i}})}} \\ &= \underline{\delta}^{-J_{k_i}} \sum_{j=k_i}^{l_i} \underline{A}'_{i,j}\underline{\delta^{-J_j+J_{k_i}}} = \sum_{j=k_i}^{l_i} \underline{\delta^{-J_j}}\ \underline{A}'_{i,j}.\end{aligned}$$

Thus, φ has residual polynomials $(\underline{A}_1, \dots, \underline{A}_\ell)$ and $K[x]/(\psi) \cong K[x]/(\varphi)$. □

Example 4.13 (Example 3.13 continued)**.** Let $\mathcal{R}_2 = \{(1,10),(3,3),(9,0)\}$. There are two choices for the invariant $\mathcal{A}$, namely $\mathcal{A}_{2,1} = \{(1+2x, 2+x^3), (1+x, 1+x^3)\}$ (compare Example 4.8) and $\mathcal{A}_{2,2} = \{(2+2x, 2+x^3), (2+x, 1+x^3)\}$.

By Lemma 4.10 all extensions of $\mathbb{Q}_3$ with ramification polygon $\mathcal{R}$ can be generated by polynomials $\varphi \in \mathbb{Z}_3[x]$ with $\boldsymbol{\varphi_0 \equiv 3 \bmod 9^{\ddagger}}$. Fixing $\varphi_{0,1} = 1$ gives the partition $\mathcal{A}_{2,1} = \mathcal{A}^{*1}_{2,1} \cup \mathcal{A}^{*2}_{2,1}$ with $\mathcal{A}^{*1}_{2,1} = \{(1+2x, 2+x^3)\}$ and $\mathcal{A}^{*2}_{2,1} = \{(1+x, 1+x^3)\}$.

For the generating polynomials of the fields with $\mathcal{A}^{*1}_{2,1}$ by Lemma 4.9 we get, from the point $(1,10) = (3^0, 1\cdot 9+1)$ on $\mathcal{R}_2$ that $\boldsymbol{\varphi_{1,2} = 1^*}$ and from the point $(3,3) = (3^1, 0\cdot 9+3)$ on $\mathcal{R}_2$ that $\boldsymbol{\varphi_{3,1} = 2^{\dagger}}$. The polynomials given by $\mathcal{R}_2$ and $\mathcal{A}^{*1}$ are described by:

	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
3^4	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}
3^3	{0}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}
3^2	{0}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	{0,1,2}	**{1}***	{0,1,2}
3^1	{0}	{0}	{0}	{0,1,2}	{0}	{0}	**{2}†**	{0}	{0}	**{1}‡**
3^0	{1}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}

By Remark 4.11 proceeding as above with $\mathcal{A}^{*2}_{2,1}$ yields a template for generating polynomials for the remaining extensions with ramification polygon $\mathcal{R}$ and invariant $\mathcal{A}$.

5. Residual Polynomials of Components

We now apply some results of Monge [11] to reduce the number of polynomials that we need to consider to generate all extensions with given invariants.

Definition 5.1. Let $\mathcal{N}$ be a Newton polygon. For $\lambda \in \mathbb{Q}$ we call

$$\mathcal{N}_\lambda = \big\{(k,w) \in \mathcal{N} \mid \lambda k + w = \min\{\lambda l + u \mid (l,u) \in \mathcal{N}\}\big\}$$

the λ-component of $\mathcal{N}$.

Remark 5.2. If $\mathcal{N}$ has a segment with slope λ then $\mathcal{N}_\lambda$ contains that segment. Otherwise $\mathcal{N}_\lambda$ consists of only one point.

To each component of integral slope of a ramification polygon we attach a residual polynomial.

Definition 5.3. Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein, α a root of φ, ρ the ramification polynomial of φ, and $\mathcal{R}$ the ramification polygon of φ. For $\lambda \in \mathbb{Z}^{>0}$ the residual polynomial of the $(-\lambda)$-component of $\mathcal{R}$ is

$$\underline{S}_\lambda(x) = \underline{\rho(\alpha^\lambda x)/\operatorname{cont}_\alpha\big(\rho(\alpha^\lambda x)\big)}$$

where $\mathrm{cont}_\alpha\big(\rho(\alpha^\lambda z)\big)$ denotes the highest power of α dividing all coefficients of $\rho(\alpha^\lambda z)$.

The quantity $\mathrm{cont}_\alpha(\rho(\alpha^m z))$ only depends on the ramification polygon. Namely if $\rho(x) = \sum_{i=1}^n \rho_i x^i$ we have $\rho(\alpha^\lambda x) = \sum_{i=0}^n \rho_i(\alpha^\lambda x)^i = \sum_{i=0}^n \rho_i(\alpha^\lambda)^i x^i$ and obtain

$$n\phi_{\mathcal{R}}(\lambda) = \min_{0\le i\le n} v(\rho_i) + i\lambda = \mathrm{cont}_\alpha\big(\rho(\alpha^\lambda x)\big)$$

for the Hasse-Herbrand function $\phi_{\mathcal{R}}$ of $\mathcal{R}$ (Definition 3.11). Thus [11, Proposition 1] yields

$$n\phi_{\mathcal{R}}(\lambda) = \mathrm{cont}_\alpha\big(\rho(\alpha^\lambda x)\big) = n\phi_{L/K}(\lambda).$$

To calculate $n\phi_{\mathcal{R}}(\lambda)$, we only have to take the minimum of the $v(\rho_i) + i\lambda$ for the points $(v(\rho_i), i)$ on the polygon. For $p^s < i < p^{s+1}$, we have $v_\alpha(\rho_{p^s}) \le v_\alpha(\rho_i)$ (Lemma 3.2 (c)) and $p^s < i$, which gives us that $v_\alpha(\rho_{p^s}) + p^s\lambda < v_\alpha(\rho_i) + i\lambda$. This demonstrates the formula for $\phi_{\mathcal{R}}$ from Definition 3.11.

Lemma 5.4. *Let $\mathcal{R}$ be the ramification polygon of φ.*

(a) *If $\mathcal{R}$ has a segment $\mathcal{S}$ of integral slope $-m \in \mathbb{Z}$, with left endpoint (k, w) and residual polynomial $\underline{A}$ then $\underline{S}_m(x) = x^k\underline{A}(x)$.*
(b) *If $\mathcal{R}$ has no segment of slope $-m \in \mathbb{Z}$ then $\underline{S}_m(x) = x^{p^s}$ where $0 \le s \le v_p(n)$ such that $v(\rho_{p^s}) + p^s \cdot m = \min_{0\le r\le v_p(n)} v(\rho_{p^r}) + p^r \cdot m$.*
(c) *For all $m \in \mathbb{Z}^{>0}$ the residual polynomial $\underline{S}_m$ of $\mathcal{R}_{-m}$ is an additive polynomial.*
(d) *$\underline{S}_m : \underline{K} \to \underline{K}$ is $\mathbb{F}_p$-linear.*

Proof. (a) By Remark 5.2 the component $\mathcal{R}_{(-m)}$ contains $\mathcal{S}$ and by Remark 4.3((a)) $\underline{S}_m(x) = x^k\underline{A}(x)$.

(b) As mentioned in Remark 5.2 $\mathcal{N}_{(-m)}$ and $\mathcal{R}$ only have one point in common. By Lemma 3.2 this point is of the form $(p^s, v(\rho_{p^s}))$. It follows from Lemma 3.2 that if the ramification polygon $\mathcal{R}$ of φ has no segment of slope $-m$ then

$$v\left(\mathrm{cont}_\alpha(\rho(\alpha^m x))\right) = \min_{0\le i\le n} v(\rho_i) + i\cdot m = \min_{0\le r\le v_p(n)} v(\rho_{p^r}) + p^r\cdot m$$

and $\underline{S}_m(x) = x^{p^s}$ where $0 \le s \le v_p(n)$ such that $v(\rho_{p^s}) + p^s\cdot m = \min_{0\le r\le v_p(n)} v(\rho_{p^r}) + p^r\cdot m$.

(c) By Lemma 3.2 the abscissa of each point on $\mathcal{R}$ is of the form p^s. Thus the residual polynomial of $\mathcal{R}_{(-m)}$ is the sum of monomials of the form x^{p^s} which implies that $\underline{S}_m$ is additive.

(d) Is a direct consequence of (c).

□

We now investigate the effect of changing the uniformizer α of $K(\alpha)$ on the coefficients of its minimal polynomial (compare [11, Lemma 3]).

Proposition 5.5. *Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein of degree n, let α be a root of φ and let ρ be the ramification polynomial of φ. Let $\beta = \alpha + \gamma\alpha^{m+1}$ where $\gamma \in L = K(\alpha)$ with $v(\gamma) = 0$ be another uniformizer of L and $\psi \in \mathcal{O}_K[x]$ its minimal polynomial.*

(a) *If $0 \le j < n$ and $j \equiv v_\alpha\left(\rho(\gamma\alpha^m)\right) \bmod n$ then $\varphi_j - \psi_j \sim \alpha^n\rho(\gamma\alpha^m)$*
(b) *If $0 \le k < n$ and $k \equiv v_\alpha(\mathrm{cont}_\alpha(\rho(\alpha^m x))) \bmod n$ then*

$$\underline{(\varphi_k - \psi_k)/(\alpha^{n-k}\,\mathrm{cont}_\alpha(\rho(\alpha^m x)))} = \underline{S}_m(\underline{\gamma}).$$

Proof. (a) By Definition 3.1 we have

$$\sum_{i=0}^{n-1}(\varphi_i-\psi_i)\beta^i=\varphi(\beta)-\psi(\beta)=\varphi(\beta)=\alpha^n\rho(\beta/\alpha-1)=\alpha^n\rho(\gamma\alpha^m). \tag{6}$$

Since $v_\pi(\varphi_i)\in\mathbb{Z}$ and $v_\pi(\psi_i)\in\mathbb{Z}$ and $v_\pi(\beta^i)=\frac{i}{n}$ we have

$$v_\pi\left(\sum_{i=0}^{n-1}(\varphi_i-\psi_i)\beta^i\right)=\min_{0\le i<n-1}v_\pi\left((\varphi_i-\psi_i)\beta^i\right).$$

Thus for $0\le j<n$ and $j\equiv v_\pi\left(\rho(\gamma\alpha^m)\right) \bmod n$ we have $\varphi_j-\psi_j\sim\alpha^n\rho(\gamma\alpha^m)$.

(b) Dividing Equation (6) by $\alpha^n\operatorname{cont}_\alpha(\rho(\alpha^m x))$ yields

$$\underline{\left(\frac{\varphi(\beta)-\psi(\beta)}{\alpha^n\operatorname{cont}_\alpha(\rho(\alpha^m x))}\right)}=\underline{\left(\frac{\alpha^n\rho(\gamma\alpha^m)}{\alpha^n\operatorname{cont}_\alpha(\rho(\alpha^m x))}\right)}=\underline{S}_m(\underline{\gamma}).$$

For $0\le k<n$ with $k\equiv v(\operatorname{cont}_\alpha(\rho(\alpha^m x)))\bmod n$ we get

$$\underline{(\varphi_k-\psi_k)\beta^k/(\alpha^n\operatorname{cont}_\alpha(\rho(\alpha^m x)))}=\underline{S}_m(\underline{\gamma}).$$

With $\beta\equiv\alpha \bmod (\alpha^2)$ we obtain the result.

□

5.1. **Generating Polynomials.** Using the results from above we can reduce the set of generating polynomials with given invariants considerably. We show how the coefficients of a generating polynomial can be changed by changing the uniformizer. The coefficients that we can change arbitrarily this way we set to 0, thus reducing the number of polynomials to be considered.

Corollary 5.6. *Let $\varphi\in\mathcal{O}_K[x]$ be Eisenstein of degree n, let α be a root of φ, let $L=K(\alpha)$, and let ρ be the ramification polynomial of φ. Let $m\in\mathbb{Z}^{>0}$, $c=v_\alpha(\operatorname{cont}_\alpha(\rho(\alpha^m x)))$, $0\le k<n$ with $k\equiv c \bmod n$, and $j=\frac{n-k+c}{n}$.*

(a) *If $\underline{\delta}\in\underline{S}_m(\underline{K})$ then for the minimal polynomial $\psi\in\mathcal{O}_K[x]$ of $\beta=\alpha+\gamma\alpha^{m+1}$ where $\underline{\gamma}\in\underline{S}_m^{-1}(\{\underline{\delta}\})$ we have $\underline{\psi}_{k,j}=\underline{\varphi}_{k,j}-\underline{\delta}$.*

(b) *If $\underline{S}_m:\underline{K}\to\underline{K}$ is surjective we can set $\underline{\delta}=\underline{\varphi}_{k,j}$ and obtain $\underline{\psi}_{k,j}=0$.*

(c) *If $\underline{S}_m(\underline{\gamma})=0$ and $d=v_\alpha(\alpha^n\rho(\gamma\alpha^m))$, $0\le l<n$ with $l\equiv d \bmod n$, and $i=\frac{n-l+d}{n}$ then $\underline{\psi}_{l,i}=\underline{\varphi}_{l,i}-\underline{\pi^{-i}\alpha^n\rho(\gamma\alpha^m)}$.*

The next Lemma follows directly from Corollary 5.6.

Lemma 5.7. *Let $\varphi\in\mathcal{O}_K[x]$ be Eisenstein of degree n, $\mathcal{R}$ its ramification polygon. Assume there is $m\in\mathbb{Z}^{>0}$ such that $k\equiv n\phi_{\mathcal{R}}(m) \bmod n$ and $j=\frac{n+n\phi_{\mathcal{R}}(m)-k}{n}$ and let $\underline{S}_m$ be the residual polynomials of $\mathcal{R}_{(-m)}$.*

(a) *If $\underline{S}_m$ is surjective then there is an Eisenstein polynomial $\psi\in\mathcal{O}_K[x]$ with $\psi_{k,j}=0$. such that $K[x]/(\psi)\cong K(\alpha)$.*

(b) *If $\psi\in\mathcal{O}_K[x]$ has the same ramification polygon with the same residual polynomials as φ and $\varphi_{k,j}-\psi_{k,j}\notin\underline{S}_m(\underline{K})$ then $K[x]/(\psi)\ncong K[x]/(\varphi)$.*

Example 5.8 (Example 4.13 continued)**.** The ramification polygon $\mathcal{R}_2 = \{(1,10),(3,3),(9,0)\}$ has no segments with integral slope. We get $\underline{S}_1 = x^3$, $\underline{S}_2 = x^3$, and $\underline{S}_3 = x^3$, with $9\phi(1) = 6$, $9\phi(2) = 9$, and $9\phi(3) = 12$. Thus $\boldsymbol{\varphi_{6,1} = 0^{\dagger}}$, $\boldsymbol{\varphi_{0,2} = 0^{\dagger}}$, and $\boldsymbol{\varphi_{3,2} = 0^{\dagger}}$. Furthermore $\underline{S}_m = x$ with $9\phi(m) = 10 + m$ for $m \geq 4$. Thus by Lemma 5.7 we can set $\boldsymbol{\varphi_{k,j} = 0^{\ddagger}}$ for $k + 9(j-1) \geq 14$.

For the generating polynomials with $\mathcal{A}_{2,1}^{*1}$ we get the template:

	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
3^4	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}
3^3	{0}	**{0}‡**	**{0}‡**	**{0}‡**	**{0}‡**	**{0}‡**	**{0}‡**	**{0}‡**	**{0}‡**	**{0}‡**
3^2	{0}	**{0}‡**	**{0}‡**	**{0}‡**	**{0}‡**	{0,1,2}	**{0}†**	{0,1,2}	{1}	**{0}†**
3^1	{0}	{0}	{0}	**{0}†**	{0}	{0}	{2}	{0}	{0}	{1}
3^0	{1}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}

Since changing the uniformizer cannot change $\varphi_{2,2}$ and $\varphi_{4,2}$ independently from the other coefficients of φ we obtain a unique generating polynomial of each extension with ramification polygon $\mathcal{R}_2$ and $\mathcal{A}_{2,1}^{*1}$.

6. Enumerating Generating Polynomials

We use the results from the previous sections to formulate an algorithm that returns generating polynomials of all extensions with given ramification polynomials and residual polynomials. In certain cases this set will contain exactly one polynomial for each extension.

Algorithm 6.1 (`AllExtensionsSub`)**.**

Input: A π-adic field K, a convex polygon $\mathcal{R}$ with points $(1, a_0 n + b_0)$, $(p^{s_1}, a_1 n + b_1)$,…,$(p^{s_u}, a_u n + b_u) = (p^{s_u}, 0)$,…,$(n, 0)$ satisfying Proposition 3.9 where $0 \leq b_i < n$ for $1 \leq i \leq u = v_p(n)$, $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ the segments of $\mathcal{R}$, a representative $\underline{\delta}_0$ of a class in $\underline{K}^{\times}/(\underline{K}^{\times})^n$, and $\underline{A}_1, \ldots, \underline{A}_\ell \in \underline{K}[x]$ satisfying Proposition 4.5.

Output: A set that contains at least one Eisenstein polynomial for each totally ramified extension of degree n, that can be generated by a polynomial φ with ramification polygon $\mathcal{R}$, $\underline{\varphi}_{0,1} = \underline{\delta}_0$, and residual polynomials $\underline{A}_1, \ldots, \underline{A}_\ell$.

(a) $c \leftarrow \left\lceil 1 + 2a_0 + \frac{2b_0}{n} \right\rceil - 1$ [Lemma 2.3]

(b) Initialize template $(\tau_{i,j})_{0 \leq i \leq n-1, 1 \leq j \leq c}$ with $\tau_{i,j} = \{\underline{0}\} \subset \underline{K}$

(c) For $0 \leq i \leq n-1$ and $L_{\mathcal{R}}(i) \leq j \leq c$: [Definition 3.8]
- If there is no $m \in \mathbb{Z}^{>0}$ with $i \equiv n\phi_{\mathcal{R}}(m) \bmod n$ and $j = \frac{n - i + n\phi_{\mathcal{R}}(m)}{n}$:
  - $\tau_{i,j} \leftarrow \underline{K}$.

(d) For $1 \leq m \leq \left\lfloor \frac{(a_1 n + b1) - (a_0 n + b_0)}{p^{s_1} - 1} \right\rfloor$:
- $i \leftarrow n\phi_{\mathcal{R}}(m)$ `mod` n, $j \leftarrow \frac{n - i + n\phi_{\mathcal{R}}(m)}{n}$
- $\tau_{i,j} \leftarrow R$ where R is a set of representatives of $\underline{K}/\underline{S}_m(\underline{K})$. [Lemma 5.7]

(e) For $1 \leq i \leq u$:
- Find a segment $\mathcal{S}_t$ of $\mathcal{R}$ such that $(p^{s_i}, a_i n + b_i)$ is on $\mathcal{S}_t$.
- $j \leftarrow a_i + 1 - v_\pi \binom{b_i}{p^{s_i}}$
- $\tau_{b_i,j} \leftarrow \left\{ \underline{A}_{t,(p^{s_i} - p^{s_k})/e} (-\underline{\delta}_0)^{a_i+1} \underline{\left(\tbinom{b_i}{p^{s_i}}\right)^{-1} \pi^{v_\pi \binom{b_i}{p^{s_i}}}} \right\}$. [Lemma 4.9]

where $(p^{s_k}, a_k n + b_k)$ is the left end point of $\mathcal{S}_t$ and $-h/e$ is the slope of $\mathcal{S}_t$.

(f) $\tau_{0,1} \leftarrow \{\underline{\delta}_0\}$ [Lemma 4.10]

(g) Return $\left\{x^n + \sum_{i=0}^{n-1}\left(\sum_{j=1}^{c}\varphi_{i,j}\pi^j\right)x^i \in \mathcal{O}_K[x] : \ \varphi_{i,j} \in R_{\underline{K}} \text{ such that } \underline{\varphi}_{i,j} \in \tau_{i,j}\right\}$

As is evident from the following example Algorithm 6.1 may return more than one generating polynomial for some extensions.

Example 6.2. The polygon $\mathcal{R}_3 = \{(1,10),(3,6),(9,0)\}$ has segments with slopes $\frac{10-6}{1-3} = -2$ and $\frac{6-0}{3-9} = -1$. With the choice $\varphi_0 \equiv 3 \bmod 9$ the possible pairs of residual polynomials are $\mathcal{A}_{3,1} = \{(2+x^2, 1+x^6)\}$, $\mathcal{A}_{3,2} = \{(2+2x^2, 2+x^6)\}$, $\mathcal{A}_{3,3} = \{(1+2x^2, 2+x^6)\}$, and $\mathcal{A}_{3,4} = \{(1+x^2, 1+x^6)\}$.

For $\mathcal{A}_{3,2} = \{(2+2x^2, 2+x^6)\}$ we get $\varphi_{1,2} = 2$ and furthermore this choice also gives $\underline{S}_1 = (2+x^6)x^3$, $\underline{S}_2 = (2x^2+2)x = 2(x^3+x)$, and $\underline{S}_m = x$ for $m \geq 3$ with $\underline{S}_1(\mathbb{F}_3) = \{0\}$, $\underline{S}_2(\mathbb{F}_3) = \mathbb{F}_3$, and $\underline{S}_m(\mathbb{F}_3) = \mathbb{F}_3$. As $\underline{S}_2$ is surjective we can set $\boldsymbol{\varphi_{3,2} = 0^{\ddagger}}$. As $\underline{S}_m$ is surjective for $m \geq 3$ we can set $\boldsymbol{\varphi_{k,j} = 0^{\ddagger}}$ for $k + 9(j-1) \geq 14$ where $0 \leq k < 9$. As the image of $\underline{S}_1$ is $\{\underline{0}\}$ changing the uniformizer does not affect $\boldsymbol{\varphi_{0,2}}^{\dagger}$. Thus Algorithm 6.1 generates the template:

	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
3^4	$\{0\}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$
3^3	$\{0\}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$
3^2	$\{0\}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\mathbf{\{0\}^{\ddagger}}$	$\{0\}$	$\mathbf{\{0\}^{\ddagger}}$	$\{0,1,2\}$	$\mathbf{\{2\}^{*}}$	$\mathbf{\{0,1,2\}^{\dagger}}$
3^1	$\{0\}$	$\{0\}$	$\{0\}$	$\mathbf{\{2\}^{*}}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{1\}$
3^0	$\{1\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$

Of the corresponding polynomials $\varphi_{c,d} = x^9 + \mathbf{6}^{*}x^6 + 9c\cdot x^2 + \mathbf{18}^{*}x + 3 + \mathbf{9d}^{\dagger}$ $(c,d \in \{1,2\})$ more than one polynomial generates each extension. Let α be root of $\varphi_{c,d}$ and ρ its ramification polynomial . For $\gamma \in \{\underline{1},\underline{2}\}$ we have $v_\alpha(\rho(\gamma\alpha)) = 11$. If $\psi(x) = \sum_{i=0}^{9}\psi_i x^i$ denotes the minimal polynomial of $\alpha + \gamma\alpha^2$ then by Proposition 5.5 (a) we have $\varphi_2 - \psi_2 = \alpha^9\rho(\gamma\alpha)$. and hence $\psi_{2,2} = \varphi_{2,2} - \rho(\gamma\alpha)/\alpha^9 \not\equiv 0 \bmod \alpha$. As $\gamma + (\alpha) \mapsto \rho(\gamma\alpha)/\alpha^{11} + (\alpha) = 2\gamma + (\alpha)$ is surjective, changing the uniformizer from α to $\alpha + \gamma\alpha$ results in a change of $\varphi_{2,2}$. Thus we can choose γ such that $\varphi_{2,2} = 0$ and get that all extensions with ramification polygon $\mathcal{R}_3$ and residual polynomials $\mathcal{A}_{3,2}$ are generated by exactly one polynomial of the form $\varphi_d = x^9 + \mathbf{6}^{*}x^6 + \mathbf{18}^{*}x + 3 + \mathbf{9d}^{\dagger}$ where $(d \in \{1,2\})$.

Theorem 6.3. *Let F be the set of polynomials returned by Algorithm 6.1 given K and a ramification polygon $\mathcal{R}$, $\underline{\delta}_0 \in \underline{K}$ and polynomials $\underline{A}_1, \ldots, \underline{A}_\ell \in \underline{K}[x]$.*

(a) *F contains at least one Eisenstein polynomial for each totally ramified extension of degree n, that can be generated by a polynomial φ with ramification polygon $\mathcal{R}$, $\underline{\varphi}_{0,1} = \underline{\delta}_0$, and residual polynomials $\underline{A}_1, \ldots, \underline{A}_\ell$.*

(b) *If $\underline{S}_m : \underline{K} \to \underline{K}$ is surjective for all segments with integral slope $-m$, then no two polynomials in F generate isomorphic extensions.*

(c) *If there is exactly one $\underline{S}_m : \underline{K} \to \underline{K}$ that is non-surjective, and for all integers $k > n\phi_{\mathcal{R}}(m)$, there is an $m' \in \mathbb{Z}^{>0}$ such that $n\phi_{\mathcal{R}}(m') = k$, then no two polynomials in F generate isomorphic extensions.*

Proof. (a) Let $\varphi \in F$. In Algorithm 6.1 step (c) we have ensured that $v_\pi(\varphi_i) \geq L_{\mathcal{R}}(i)$ and in step (e) we assign nonzero values to $\varphi_{b_i,j}$ so that $v_\pi(\varphi_{b_i}) = L_{\mathcal{R}}(b_i)$ for points $(p^{s_i}, a_i n + b_i)$ with $b_i \neq 0$. So by Proposition 3.10, φ has ramification polygon

$\mathcal{R}$. By Lemma 4.9, the values assigned in step (e) ensure that $\mathcal{R}_\varphi$ has residual polynomials $(\underline{A}_1, \ldots, \underline{A}_\ell)$. Thus each extension generated by a polynomial with the input invariants is generated by a polynomial in F and all polynomials in F have these invariants.

(b) If $\underline{S}_m : \underline{K} \to \underline{K}$ is surjective for all segments with integral slope $-m$, then all of the nonzero coefficients in our template τ are either fixed by δ_0 or $\mathcal{A}$, or free because they are not set by a choice of element in the image of some $\underline{S}_m$. Any deformation of the uniformizer that might result in two polynomials in F to generate the same extension would have to change one of these free coefficients, but such a change cannot be made independently of the choices we made in order to set coefficients to zero by Lemma 5.7. So no two polynomials in F generate isomorphic extensions.

(c) Suppose there is exactly one $\underline{S}_m : \underline{K} \to \underline{K}$ that is non-surjective, and for all integers $k > n\phi_{\mathcal{R}}(m)$, there is an $m' \in \mathbb{Z}^{>0}$ such that $n\phi_{\mathcal{R}}(m') = k$. As $\underline{S}_m : \underline{K} \to \underline{K}$ is non-surjective, there will be more than one choice for $\varphi_{i,j}$ where $jn + i = n\phi_{\mathcal{R}}(m)$. By Proposition 5.5, the corresponding change of uniformizer (from α to $\alpha + \gamma\alpha^{m+1}$) can change $\varphi_{i',j'}$ where $j'n + i' > jn + i$. Since there exists $m' \in \mathbb{Z}^{>0}$ such that $n\phi_{\mathcal{R}}(m') = j'n + i'$, then Algorithm 6.1 will assign $\varphi_{i',j'}$ based on $\underline{S}_{m'}$. Given that $m \neq m'$, $\underline{S}_{m'}$ is surjective, $\varphi_{i',j'}$ can be set to zero by Lemma 5.7. As all coefficients $\varphi_{i',j'}$ with $j'n + i' \geq jn + i$ are assigned by the residual polynomials of components, no two polynomials generate isomorphic extensions.

□

As in general the algorithm returns more than one polynomial generating each extension with the given invariants, the output needs to be filtered by comparing the generated extensions by

(a) using the set of all reduced polynomials as computed by [11, Algorithm 3] or
(b) a root finding algorithm (compare [19]).

Suppose F is a set of non-isomorphic extensions with the given invariants. For the first method, the set of all reduced polynomials generating each extension in F is computed. Since the polynomials generated by our algorithm are reduced, checking whether a polynomial ϕ generates an extension isomorphic to an extension in F only requires comparing ϕ to the reduced generating polynomials for all extensions in F. Although the computation of the reduced polynomials requires the expensive computation of characteristic polynomials, the efficient comparison makes this method cheaper than the root finding method, where the existence of a root of ϕ is checked over each extension in F. When using either method to compare polynomials, the process can be accelerated by terminating when the number of extensions with the given invariants computed with the mass formulas from [22, 23] is found.

The product $\prod_{m=0}^{\infty} \#\ker \underline{S}_m$ is an upper bound for the number of automorphisms of L/K. This together with the number of reduced polynomials of φ gives the number of automorphisms of L/K ([11, Theorem 1]). Alternatively the number extensions generated by each polynomial can be computed using root finding.

Now we present an algorithm to enumerate all extensions with a given invariants. It may require multiple calls to Algorithm 6.1 `AllExtensionsSub` depending the structure of $\mathcal{A}$ and the number of tamely ramified subextension.

Algorithm 6.4 (`AllExtensions`)**.**

Input: A π-adic field K, a ramification polygon $\mathcal{R}$, and invariant $\mathcal{A}$

Output: A set F that contains one generating Eisenstein polynomial for each totally ramified extension of K with ramification polygon $\mathcal{R}$ and invariant $\mathcal{A}$

(a) $S_0 \leftarrow$ a set of representatives of $\underline{K}^\times/(\underline{K}^\times)^n$.
(b) For $\delta \in S_0$ do
  (i) Partition $\mathcal{A}$ into disjoint sets $\mathcal{A}^{*1}, \ldots, \mathcal{A}^{*k}$ by Equation (5).
  (ii) For $\mathcal{A}^* \in \{\mathcal{A}^{*1}, \ldots, \mathcal{A}^{*k}\}$ do
    - Let A be a representative of $\mathcal{A}^*$.
    - $F' \leftarrow$ `AllExtensionsSub`$(K, \mathcal{R}, A, \delta)$. [Alg. 6.1]
    - Unless avoidable by Theorem 6.3, filter F' so that no two polynomials generate the same extension using method of choice.
    - $F \leftarrow F \cup F'$.
(c) Return F.

Theorem 6.5. *Let F be the set of polynomials returned by Algorithm 6.4. For each extension L/K with ramification polygon $\mathcal{R}$ and invariant $\mathcal{A}$, the set F contains exactly one generating polynomial.*

Proof. Let L/K be a totally ramified extension with ramification polygon $\mathcal{R}$ and invariant $\mathcal{A}$. Let $\psi \in \mathcal{O}_K[x]$ be an Eisenstein polynomial generating L with $\psi_{0,1} \in S_0$. Let $A^{(\psi)}$ be the residual polynomials of segments of $\mathcal{R}$ given ψ. As ψ generates L with invariant $\mathcal{A}$, $A^{(\psi)}$ belongs to some $\mathcal{A}^*$ in our partition of $\mathcal{A}$. If A is our choice of representative of $\mathcal{A}^*$, then by Lemma 4.12, there is a $\varphi \in \mathcal{O}_K[x]$ with residual polynomials A such that $K[x]/(\psi) \cong K[x]/(\varphi)$. Thus, L/K can be generated by an Eisenstein polynomial φ with residual polynomials A, and $\varphi_{0,1} = \psi_{0,1}$, and by Theorem 6.3, there is at least one $\varphi \in F'$ with F' returned by `AllExtensionsSub`$(K, \mathcal{R}_\psi, A, \psi_{0,1})$ generating L/K. The output F contains one generator for every extension that can be generated by any polynomial in any F' produced, and so there is a polynomial in F generating L/K.

To show that no two polynomials in F generate the same extension, it suffices to show that no polynomials produced by different calls to Algorithm 6.1 generate the same extension. Let φ and ψ be in two such polynomials. By Lemma 4.10, if $\varphi_{0,1} \neq \psi_{0,1}$, then as $\varphi_{0,1}, \psi_{0,1} \in \underline{K}^\times/(\underline{K}^\times)^n$, $K[x]/(\psi) \ncong K[x]/(\varphi)$. Now suppose $\varphi_{0,1} = \psi_{0,1}$. By Remark 4.11, if the residual polynomials of φ and ψ are not in the same $\mathcal{A}^*$ then $K[x]/(\psi) \ncong K[x]/(\varphi)$. Thus, if two polynomials are generated by Algorithm 6.1 with different inputs of δ or residual polynomials returned by Algorithm 6.4, they cannot generate the same extension. □

7. Examples

In Figure 3 we compare the implementation of the algorithm from [19] in Magma [2] (`AllExtensions`) with our implementation of Algorithm 6.4 in Magma. In the implementation of the method from [19], we replaced the deterministic enumeration of polynomials by random choices, which yields a considerable performance improvement. Cases are separated into those where filtering was required for Algorithm 6.4 and where it was not. To filter the set of polynomials to obtain a minimal set when required, our implementation of Algorithm 6.4 uses Magma's root finding without the mass formula from [23] as a termination criterion.

Filtering not needed					Filtering needed						
K	n	$v(\text{disc})$	[19]	Alg. 6.4	K	n	$v(\text{disc})$	[19]	#Pol	#Ext	Alg. 6.4
$\mathbb{Q}_2$	8	10	0.016 s	0.015 s	$\mathbb{Q}_2$	8	16	2.079 s	30	128	0.201 s
$\mathbb{Q}_3$	9	16	3.329 s	0.010 s	$\mathbb{Q}_2$	8	17	3.968 s	32	128	0.579 s
$\mathbb{Q}_3$	9	25	69.17 s	0.016 s	$\mathbb{Q}_2$	8	18	3.421 s	28	128	0.141 s
$\mathbb{Q}_3$	27	36	125.70 s	0.031 s	$\mathbb{Q}_2$	8	20	10.36 s	64	256	0.875 s
$\mathbb{Q}_3$	27	43	27.8 hr	0.313 s	$\mathbb{Q}_2$	8	27	121.14 s	512	512	42.92 s
$\mathbb{Q}_5$	25	41	39.4 hr	0.281 s	$\mathbb{Q}_2$	8	30	533.48 s	512	512	177.55 s
$\mathbb{Q}_5$	125	135	8.9 hr	0.219 s	$\mathbb{Q}_2$	16	45	1272.25 s	5120	32768	10.98 s

FIGURE 3. Time needed to compute a minimal set of generating polynomials of all extensions of K of degree n with discriminant exponent $v(\text{disc})$ with the implementation of the algorithm from [19] and Algorithm 6.4in Magma. In the cases where filtering was needed we also give the number of polynomials obtained with our construction and the number of distinct extensions. All timings were obtained on a computer with an Intel Core i5 at 2.6GHz and 4Gb RAM.

We now present generating polynomials for totally ramified extensions of degree 15 over $\mathbb{Q}_5$ (Example 7.1), totally ramified extensions of degree 8 over an unramified extension of degree 2 over $\mathbb{Q}_2$ (Example 7.2), totally ramified extensions of degree 9 over a ramified extension of $\mathbb{Q}_3$ of degree 3 (Example 7.3), and an example over $\mathbb{Q}_3$ that shows that in general not all extensions with the same ramification polygon and invariant $\mathcal{A}$ have the same mass (Example 7.4).

Example 7.1. We find generating polynomials for all totally ramified extensions L of $\mathbb{Q}_5$ of degree 15 with $v_5(\text{disc}(L)) = 29$, the highest possible valuation by Proposition 2.1. There is only one possible ramification polygon $\mathcal{R} = \{(1,15),(5,0),(10,0),(15,0)\}$ and only one possible set of residual polynomials $\mathcal{A} = \{(3z+2, z^{10}+3z^5+3)\}$ for such extensions. Denote by $\varphi(x) = \sum_{i=0}^{15} \varphi_i x^i$ an Eisenstein polynomial generating such a field L.

By Lemma 4.10 all extensions of $\mathbb{Q}_5$ with ramification polygon $\mathcal{R}$ can be generated by polynomials $\varphi \in \mathbb{Z}_5[x]$ with $\varphi_0 \equiv 5 \bmod 25$. As $b_t = 0$ for all points $(p^{s_t}, a_t n + b_t) \in \mathcal{R}$, Proposition 3.10 only gives us restrictions on φ based on $L_{\mathcal{R}}$ and no coefficients are set by Lemma 4.9. This provides the following template for φ:

	x^{15}	x^{14}	x^{13}	x^{12}	x^{11}	x^{10}	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
5^2	$\{0\}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$
5^1	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$R_{\mathbb{F}_5}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$R_{\mathbb{F}_5}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{1\}$
5^0	$\{1\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$

The ramification polygon $\mathcal{R}_2$ has no segments with non-zero integral slope. We get $\underline{S}_1 = x^{15}$, $\underline{S}_2 = x^{15}$, and $\underline{S}_3 = x^{15}$, with $15\phi(1) = 5$, $15\phi(2) = 10$, and $15\phi(3) = 15$. Thus $\varphi_{5,1} = 0$, $\varphi_{10,1} = 0$, and $\varphi_{0,2} = 0$. Further, for $m \geq 4$, $\underline{S}_m = x$. As $15\phi(m) = 15 + m$ for $m \geq 4$, by Lemma 5.7, we can set $\varphi_{k,j} = 0$ for $k + 9(j-1) \geq 19$. Therefore, the generating polynomials φ of the fields over $\mathbb{Q}_5$ with invariants $\mathcal{R}$ and $\mathcal{A}$ follow this template:

	x^{15}	x^{14}	x^{13}	x^{12}	x^{11}	x^{10}	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
5^2	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	$R_{\mathbb{F}_5}$	{0}
5^1	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{1}
5^0	{1}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}

As all of the $\underline{S}_m$ are surjective, by Theorem 6.3 (b), no two of these 125 polynomials generate isomorphic extensions of $\mathbb{Q}_5$.

Example 7.2. Let K be the unramified extension of $\mathbb{Q}_2$ generated by $y^2+y+1 \in \mathbb{Q}_2[y]$. Let γ be a root of y^2+y+1, so $\underline{K} = \mathbb{F}_2(\gamma)$. We want to find generating polynomials for all totally ramified extensions L of K of degree 8 with $v_2(\mathrm{disc}\,(L)) = 16$, ramification polygon with points $\mathcal{R} = \{(1,9),(2,6),(8,0)\}$, and $\mathcal{A}$ containing $(\gamma z+\gamma, z^6+\gamma)$. Denote by $\varphi = \sum_{i=0}^{8} \varphi_i x^i$ an Eisenstein polynomial generating such a field L.

By Proposition 3.10, we have $v(\varphi_1) = 2$ and $v(\varphi_6) = 1$, and that $v(\varphi_i) \geq 2$ for $i \in \{2,3,4,5,7\}$. By Lemma 4.9, the point $(1,9) = (2^0, 1\cdot 8+1)$ on $\mathcal{R}$ gives us that $\varphi_{1,2} = \gamma$ and the point $(2,6) = (2^1, 0\cdot 8+6)$ on $\mathcal{R}$ gives us that $\varphi_{6,1} = \gamma$. We set $\varphi_{0,1} = 1$ by Lemma 4.10 and the template for the polynomials φ is:

	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
2^3	{0}	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$
2^2	{0}	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	{γ}	$R_{\underline{K}}$
2^1	{0}	{0}	{γ}	{0}	{0}	{0}	{0}	{0}	{1}
2^0	{1}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}

It remains to consider the $\underline{S}_m$. Our ramification polygon $\mathcal{R}$ has two segments of integral slope, -3 and -1, respectively. So by Lemma 5.4, $\underline{S}_1(z) = z^2\underline{A}_2 = z^2(z^6+\gamma)$ and $\underline{S}_3(z) = z\underline{A}_1 = z(\gamma z+\gamma)$. As $\underline{S}_1$ is surjective and $n\phi(1) = 8$, we may set $\varphi_{0,2} = 0$. As $\mathcal{R}$ has no segment of slope -2, $\underline{S}_2$ is surjective, so with $n\phi(2) = 10$, we may set $\varphi_{2,2} = 0$. On the other hand, $\underline{S}_3$ is not surjective and has image $\{0,\gamma\}$. By Lemma 5.7 and as $n\phi(3) = 12$, $\varphi_{4,2} \in R_{\underline{K}}/\{0,\gamma\} = \{0,1\}$. For $m \geq 4$, $n\phi(m) = 9+m$, and so we can set $\varphi_{k,j} = 0$ for $k+8(j-1) \geq 13$. This gives us the following template for polynomials φ:

	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
2^3	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}
2^2	{0}	{0}	{0}	{0}	{0,1}	$R_{\underline{K}}$	{0}	{γ}	{0}
2^1	{0}	{0}	{γ}	{0}	{0}	{0}	{0}	{0}	{1}
2^0	{1}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}

As $\underline{S}_3$ is the only non-surjective $\underline{S}_m$, and for all integers k greater than $n\phi(3) = 12$, $n\phi(k-9) = k$, we have by Theorem 6.3 (c) that no two of these 8 polynomials generate the same extension.

Example 7.3. Let $K = \mathbb{Q}_3[x]/(x^2-3)$ and let π be a uniformizer of the valuation ring of K. As in Example 3.13, there are three possible ramification polygons for extensions L of K of degree 9 with $v_3(\mathrm{disc}\,(L)) = 18$, namely $\mathcal{R}_1 = \{(1,10),(9,0)\}$, $\mathcal{R}_2 = \{(1,10),(3,3),(9,0)\}$, and $\mathcal{R}_3 = \{(1,10),(3,6),(9,0)\}$ (compare Figure 2).

Let us again choose to investigate $\mathcal{R}_2$. By Lemma 3.5 we have $v_\pi(\varphi_3) = 1$ and by Lemma 4.10 we can set $\varphi_{0,1} = 1$. As $\underline{K} = \underline{\mathbb{Q}_3}$, we have the same four choices for the invariant $\mathcal{A}$: $\mathcal{A}_{2,1} = \{(1+2x, 2+x^3)\}$, $\mathcal{A}_{2,2} = \{(2+x, 1+2x^3)\}$, $\mathcal{A}_{2,3} = \{(1+x, 1+x^3)\}$, and $\mathcal{A}_{2,4} = \{(2+2x, 2+x^3)\}$.

Let us choose $\mathcal{A}_{2,1}$. By Lemma 4.9 we get from the point $(1,10) = (3^0, 1\cdot 9+1)$ on $\mathcal{R}_2$ that $\varphi_{1,2} = 1$ and from the point $(3,3) = (3^1, 0\cdot 9+3)$ on $\mathcal{R}_2$ that $\varphi_{3,1} = 2$.

The ramification polygon $\mathcal{R}_2$ has no segments with integral slope. We get $\underline{S}_1 = x^3$, $\underline{S}_2 = x^3$, and $\underline{S}_3 = x^3$, with $9\phi(1) = 6$, $9\phi(2) = 9$, and $9\phi(3) = 12$. Thus $\varphi_{6,1} = 0$, $\varphi_{0,2} = 0$, and $\varphi_{3,2} = 0$. Furthermore $\underline{S}_m = x$ for with $9\phi(m) = 10 + m$ for $m \geq 4$. Thus by Lemma 5.7 we can set $\varphi_{k,j} = 0$ for $k + 9(j-1) \geq 14$.

Proceeding as in Examples 3.13, 4.13, and 5.8 we obtain a familiar template for the polynomials generating fields over K with ramification polygon $\mathcal{R}_2$ and invariant $\mathcal{A}_{2,1}$:

	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
π^4	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}
π^3	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}
π^2	{0}	{0}	{0}	{0}	{0}	{0,1,2}	{0}	{0,1,2}	{1}	{0}
π^1	{0}	{0}	{0}	{0}	{0}	{0}	{2}	{0}	{0}	{1}
π^0	{1}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}

As all of the $\underline{S}_m$ are surjective, we obtain a unique generating polynomial of each degree 9 extension of K with $v_3(\mathrm{disc}\,(L)) = 18$, ramification polygon $\mathcal{R}_2$, and invariant $\mathcal{A}_{2,1}$.

As mentioned in the previous section, our choice of residual polynomials relate to the size of the automorphism group of the extensions generated by our polynomials. However, the polynomials generated by Algorithm 6.4 (and in general, those generating extensions of the same degree, discriminant, ramification polygon, and $\mathcal{A}$) do not generate extensions with the same automorphism group size.

Example 7.4. Over $\mathbb{Q}_3[x]$, let $\varphi(x) = x^9 + 6x^6 + 18x^5 + 3$ and $\psi(x) = x^9 + 18x^8 + 9x^7 + 6x^6 + 18x^5 + 3$. Both are Eisenstein polynomials generating degree 9 extensions over $\mathbb{Q}_3$ with ramification polygon $\mathcal{R} = \{(1,14),(3,6),(9,0)\}$ and having residual polynomials $\underline{A}_1 = 2z^2+1$ and $\underline{A}_2 = z^6 + 2$. Using root-finding, we see that over $\mathbb{Q}_3[x]/(\varphi)$, φ has 3 roots, while over $\mathbb{Q}_3[x]/(\psi)$, ψ has 9 roots. Thus ψ generates a normal extension, while φ generates three extensions with automorphism groups of size 3 which shows that not all extension with the same ramification polygon and residual polynomials have the same mass.

8. Acknowledgments

We thank Jonathan Milstead for his careful reading of our manuscript and the anonymous referee for the numerous helpful comments.

References

[1] Shigeru Amano. Eisenstein equations of degree p in a $\mathfrak{p}$-adic field. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 18:1–21, 1971.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Ivan B. Fesenko and Sergey V. Vostokov. *Local Fields and Their Extensions*, volume 121 of *Translations of Mathematical Monographs*. American Mathematical Society, 2nd edition, 2002.

[4] Christian Greve and Sebastian Pauli. Ramification polygons, splitting fields, and Galois groups of Eisenstein polynomials. *International Journal of Number Theory*, 8(6):1401–1424, 2012.

[5] Jordi Guàrdia, Jesús Montes, and Enric Nart. A new computational approach to ideal theory in number fields. *Found. Comput. Math.*, 13(5):729–762, 2013.

[6] Jordi Guàrdia, Enric Nart, and Sebastian Pauli. Single-factor lifting and factorization of polynomials over local fields. *J. Symbolic Comput.*, 47(11):1318–1346, 2012.
[7] Charles Helou. *Non-Galois ramification theory of local fields*, volume 64 of *Algebra Berichte [Algebra Reports]*. Verlag Reinhard Fischer, Munich, 1990.
[8] Marc Krasner. Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique. In *Les Tendances Géom. en Algèbre et Théorie des Nombres*, pages 143–169. Editions du Centre National de la Recherche Scientifique, Paris, 1966.
[9] Hua-Chieh Li. p-adic power series which commute under composition. *Transactions of the American Mathematical Society*, 349(4):1437–1446, 1997.
[10] Jonathan D. Lubin. The local Kronecker-Weber theorem. *Transactions of the American Mathematical Society*, 267(1):133–138, 1981.
[11] Maurizio Monge. A family of Eisenstein polynomials generating totally ramified extensions, identification of extensions and construction of class fields. *Int. J. Number Theory*, 10(7):1699–1727, 2014.
[12] Jesús Montes. *Poligonos de Newton de orden superior y aplicaciones aritmeticas*. PhD thesis, Universitat de Barcelona, 1999.
[13] Jesús Montes and Enric Nart. On a theorem of Ore. *J. Algebra*, 146(2):318–334, 1992.
[14] Öystein Ore. Bemerkungen zur Theorie der Differente. *Math. Z.*, 25(1):1–8, 1926.
[15] Öystein Ore. Newtonsche Polygone in der Theorie der algebraischen Körper. *Math. Ann.*, 99(1):84–117, 1928.
[16] Peter Panayi. *Computation of Leopoldt's p-adic regulator*. PhD thesis, University of East Anglia, 1995.
[17] Sebastian Pauli. Constructing class fields over local fields. *J. Théor. Nombres Bordeaux*, 18(3):627–652, 2006.
[18] Sebastian Pauli. Factoring polynomials over local fields II. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 301–315. Springer, Berlin, 2010.
[19] Sebastian Pauli and Xavier-François Roblot. On the computation of all extensions of a p-adic field of a given degree. *Math. Comp.*, 70(236):1641–1659 (electronic), 2001.
[20] John Scherk. The ramification polygon for curves over a finite field. *Canad. Math. Bull.*, 46(1):149–156, 2003.
[21] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.
[22] Brian Sinclair. *Algorithms for Enumerating Invariants and Extensions of Local Fields*. PhD thesis, University of North Carolina at Greensboro, 2015.
[23] Brian Sinclair. Counting extensions of (π)-adic fields with given invariants. *preprint*, arXiv:1512.06946 [math.NT], 2015.