SINCLAIR, BRIAN, Ph.D. Algorithms for Enumerating Invariants and Extensions of Local Fields. (2015)
Directed by Dr. Sebastian Pauli. 106 pp.

There are many computationally difficult problems in the study of p-adic fields, among them the classification of field extensions and the decomposition of global ideals. The main goal of this work is present efficient algorithms, leveraging the Newton polygons and residual polynomials, to solve many of these problems faster and more efficiently than currently available methods. Considering additional invariants, we extend Krasner's mass formula, dramatically improve general extension enumeration using the *reduced Eisenstein polynomials* of Monge, and provide a detailed account of algorithms that compute Okutsu invariants, which have many uses, through the lens of partitioning zeros.

ALGORITHMS FOR ENUMERATING INVARIANTS AND EXTENSIONS OF LOCAL FIELDS

by

Brian Sinclair

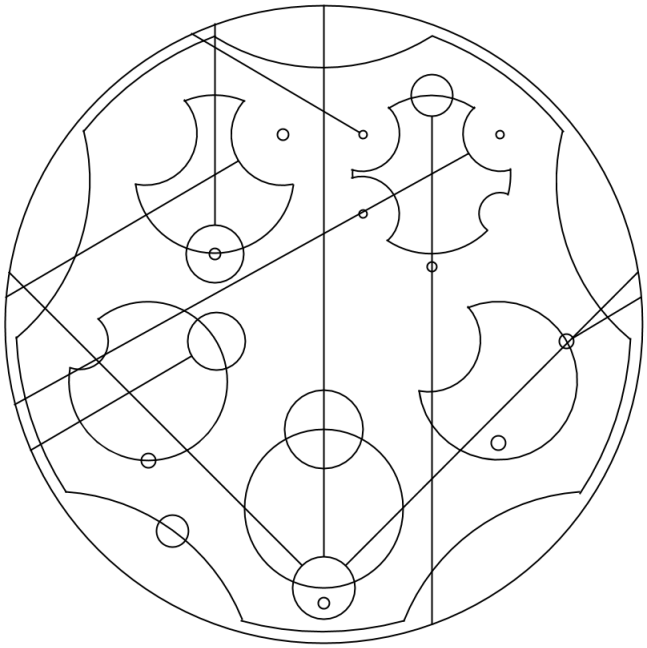
A Dissertation Submitted to
the Faculty of the Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Greensboro
2015

Approved by

_____
Committee Chair

To my wife, Maura,



APPROVAL PAGE

This dissertation written by Brian Sinclair has been approved by the following committee of the Faculty of The Graduate School at The University of North Carolina at Greensboro.

Committee Chair _____
Sebastian Pauli

Committee Members _____
David Ford

_____
Paul Duvall

_____
Brett Tangedal

_____
Dan Yasaki

_____
Date of Acceptance by Committee

_____
Date of Final Oral Examination

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Page

LIST OF ALGORITHMS

CHAPTER I

INTRODUCTION

There are many computationally difficult problems in the study of p-adic fields, among them the classification of field extensions and the decomposition of global ideals. The main goal of this work is to present efficient algorithms, leveraging the Newton polygons and residual polynomials, to solve many of these problems faster and more efficiently than present methods. Considering additional invariants, we extend Krasner's mass formula [Kra66], dramatically improve general extension enumeration [PR01] using the *reduced Eisenstein polynomials* of Monge [Mon14], and provide a detailed account of algorithms that compute Okutsu invariants [Oku82], which have many uses, through the lens of partitioning zeros.

In the following we give an account of the history of p-adic fields followed by an overview over this thesis.

1.1 Early History of the p-Adics

The p-adic numbers were created by an analogy. As a student of Kronecker, Kurt Hensel was working on extending Kronecker's work on the factoring of prime ideals in number fields when he made a keen observation. He observed that the prime ideals of $\mathbb{C}[x]$, namely the functions $(x-a)$, have an role analogous to the role of the prime ideals of $\mathbb{Q}$, namely the prime numbers. Hensel concluded that methods from complex analysis where one can consider the global properties of a function by expanding functions locally, should be translatable to number theory. Analogously to the Laurent series expansion of a complex function $f \in \mathbb{C}(x)$ about a point $a \in \mathbb{C}$

$$f(x) = \sum_{i=N}^{\infty} a_i (x-a)^i$$

he considered the Laurent series expansion of a rational number $r \in \mathbb{Q}$ in terms of powers of a prime number p,

$$r = \sum_{i=N}^{\infty} r_i p^i.$$

Hensel called this series the *p-adic expansion* of r. With respect to a prime number $p \in \mathbb{Z}$, any rational number can be expressed p-adically in this way. These p-adic expansions yield local information about r near p, analogous to how the Laurent series expansion yield local information about $f(x)$ near a.

Hensel showed that the set of all such series for a given prime p form a field, the field of *p-adic numbers*, which he denoted by $K(p)$, but in modern notation is written $\mathbb{Q}_p$. Though a field by modern standards, $\mathbb{Q}_p$ failed to meet the requirement of Dedekind's definition of field that it be a subfield of the complex numbers, which motivated Steinitz's work on abstract field theory [Ste10]. The introduction of p-adic fields led to the definition of what we now call local fields. Hensel introduced the p-adic numbers in a short paper [Hen97] and expounded on the subject in further papers and books. In particular, he found that one could factor the ideal generated by p in a number field if you can factor the generating polynomial of that number field over $\mathbb{Q}_p$.

In his development of the p-adics, Hensel introduced a topological viewpoint by defining the p-adic absolute value of $r \in \mathbb{Q}$

$$\|\cdot\|_p : \mathbb{Q} \to \mathbb{R}, \quad r \mapsto \|r\|_p = p^{-v_p(r)},$$

where $r = p^{v_p(r)} \dfrac{a}{b}$ with a, b, and p pairwise coprime and by convention $v_p(0) = \infty$, so that $\|0\|_p = 0$. Inspired by Hensel, specifically his book on algebraic numbers [Hen08], Josef Kürschák set out to provide a solid foundation of the p-adic numbers, in a manner similar to that of Cantor for the real and complex numbers. His result, announced at the Cambridge International Congress of Mathematicians in 1912 [Kür12], stated the first abstract structure theorems on valued fields. Kürschák's paper on the subject [Kür13] provided a general theory of valuations (of which Hensel's v_p are examples) and laid the groundwork for valuation theory as a separate, axomitized field of study. This presentation and paper was, however, his only contribution to the subject.

After Kürschák began the study of valuations, Alexander Ostrowski provided much of its early development. Ostrowski left Kiev in 1911 to study with Hensel in Marburg. In his first paper

there [Ost13], he answered a standing question of Kürschák by showing that a separable algebraic extension of a complete valued field is again complete if and only if it is a finite extension of that field. When revisiting and reproving the results from that paper in [Ost17], he proved that the extension of a valuation to its algebraic closure is unique. Finally, Ostrowski determined all possible valuations on on $\mathbb{Q}$:

Theorem 1.1 (Ostrowski [Ost18]). *An absolute value on $\mathbb{Q}$ either coincides with $(\|\cdot\|_p)^r$ for some prime p and some $r \in [0,1]$, or with $(\|\cdot\|_\infty)^r$ for some $r \in \mathbb{R}$ where $\|\cdot\|_\infty$ is the traditional absolute value.*

In 1921, the connection between the rational numbers and p-adic numbers was solidified by a student of Hensel's, Helmut Hasse. For his thesis, he classified quadratic forms with rational coefficients in terms of the simpler classification of quadratic forms over real and p-adic numbers. This result was the first of many to be referred to as a Local-Global Principle. In the years to follow, Hasse published several other important papers in quick succession, elaborating upon this and further demonstrating how number theoretic problems could be solved by local methods. His development of Local-Global Principles required working with norm symbols which would lead to his foundational work on local class field theory in 1930 [Has30]. Local class field theory describes the Galois group of the maximal abelian extension of a local field and through a reciprocity map, the means to study finite abelian extensions of local fields. With the aim of defining this without the use of its global equivalent, Hasse, in 1931, determines the structure of the Brauer group, which could be translated to provide local class field theory. An explicit construction can be seen in papers of Hasse [Has33] and Chevalley [Che33a, Che33b]. The global theory then follows through the use of Local-Global Principles, as proved jointly by Brauer, Hasse and Noether [BHN32]. Thus, the p-adic numbers, and in general, local fields, developed into a crucial part of algebraic number theory.

1.2 Classification of Extensions

For a finite extension K of the field of p-adic numbers $\mathbb{Q}_p$, the description of all extensions of K in a fixed algebraic closure is an important problem. Restricted to 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 [Pau06]. Recently Monge [Mon14] 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 [Ama71].

Krasner worked on building a non-abelian local class field theory. In [Kra66], he gave a formula for the number of totally ramified extensions, using his famous lemma as a main tool.

Theorem 1.2 (Krasner's Lemma)**.** *Let K be a local field complete with respect to non-archimedian absolute value $\|\cdot\|$ and let $\overline{K}$ be a separable closure of K. Let $\alpha \in \overline{K}$ with conjugates $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$. If $\beta \in \overline{K}$ is such that*

$$\|\alpha - \beta\| < \|\alpha - \alpha^{(i)}\| \text{ for } 2 \leq i \leq n,$$

then $K(\alpha) \subseteq K(\beta)$.

It follows from Krasner's Lemma that a local field has only finitely many extensions of a given degree and discriminant. Following his approach, Pauli and Roblot [PR01] presented the first general 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 [Pan95] to obtain one generating polynomial for each extension. This algorithm of Pauli and Roblot has been used extensively by Jones and Roberts [JR06, JR07, JR08] and Awtrey [AS13, AS15] for computing tables of extensions of p-adic fields and their invariants.

A new approach for determining whether two polynomials generate the same extension was recently presented by Monge [Mon14]. He introduces *reduced polynomials* that yield a canonical set of generating polynomials for each totally ramified extension of a local field 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.

1.3 Decomposition of Ideals

Ideal decomposition is the foundational problem of the p-adic numbers, and deeply related to the computation of polynomial factorizations and integral bases. To factor prime ideals in algebraic extensions of the rational numbers, Hensel would factor polynomials over p-adic fields. For *unramified* primes, those that do not divide the discriminant of the extension, this method suffices.

In 1907, Bauer adapted the techniques of Newton polygons, which had traditionally been used to study singularities of plane curves, to study arithmetical questions [Bau07]. By drawing the lower convex hull of the points $(i, v_p(a_i))$ where a_i are the coefficients of the generating polynomial of a number field, one can detect a factorization if there is more than one segment. In the 1920s, Ore greatly expanded on Bauer's methods by introducing a more general concept of the polygon and attaching to each segment a residual polynomial over a finite field [Ore24, Ore28]. Newton polygons and residual polynomials are at the center of many algorithms for computations in local fields, including those presented in this work.

Ore's methods worked defining polynomials satisfying a condition of *p-regularity*, but he wondered if, by constructing further generalizations of Newton polygons and residual polynomials, a method for the general case existed. Saunders MacLane answered this question in 1936 [ML36a, ML36b] with more general results. For any discrete valuation v on a field K, MacLane classified all extensions of v to $K[x]$. These valuations are described by a sequence of *augmented valuations*, where a specific polynomial of a certain type is assigned a valuation. These augmentations provide the needed generalization of Ore's methods to factor ideals in general.

The task of factoring ideals in number fields is closely related to the computation of integral bases of local and global fields. The Round Four algorithm of Zassenhaus [FL94, For87] was originally conceived as an algorithm for the computation of integral bases of algebraic number fields, and since its introduction, has seen many improvements [CG00, FPR02, PR01] and has implementations in `Maple` [FL94], `Pari` [PG14], and `Magma` [BCP97]. These algorithms work to find successively better approximations to the input polynomial's irreducible factors until gaining sufficient precision to apply Hensel lifting. However, they suffer from precision loss in computing characteristic polynomials and in approximating greatest common divisors, both of which are used in the core part of the algorithm as well as in the lifting of the factorization.

As an alternative to Round Four, the Montes algorithm [GMN11, GMN12, Mon99, MN92] avoids the computation of characteristic polynomials by exploiting Newton polygons of higher order. Here the most expensive operations are division with remainder and polynomial factorization over finite fields. The algorithm is based on Ore's suggestion of "higher-order" Newton Polygons [Ore26]. In 2006, Guardia, Montes, and Nart [GMN12] revisited Montes' work, and this has led to a wealth of improvements and to a better understanding of the algorithm, including complexity analyses [BNS13, FoVe10, Ver09].

Many of the intermediate values computed in the process of the Round Four and Montes algorithms are Okutsu invariants. In a series of papers [Oku82], Okutsu defined sequences of invariants of a polynomial whose construction can build an integral basis. Algorithms that compute these, which we will call *OM algorithms*, are the subject of Chapter VI.

1.4 Overview

In Chapter II, we present the necessary theory of local fields and their extensions from a modern viewpoint. We begin with the basic definitions of the p-adic numbers, their absolute value, and valuation, culminating in the general definition of a local field. The terminology and basic facts regarding local field extensions follow, with some discussion of Hensel lifting and Newton polygons. Ramification groups, their filtration, and the Hasse-Herbrand function close the chapter.

In the third chapter, we consider three extension invariants: the discriminant, the ramification polygon, and the class of residual polynomials of ramification polygon segments. Each of these is dependent on the prior, effectively partitioning extensions into finer sets. The discussion of the discriminant recalls results of Ore and Krasner on what discriminants are possible and how a choice of discriminant limits the possible generating polynomials for an extension. We begin considering ramification polygons from a lemma of Scherk [Sch03] and develop a necessary and sufficient set of conditions for a convex polygon to be a ramification polygon. Given these, we can compute all possible ramification polygons for extensions of a given degree and discriminant. Much as in the case of the discriminant, we can use the choice of ramification polygon to give conditions on generating polynomials. Our final invariant, based upon the residual polynomials of the segments of a ramification polygon, is new. Such polynomials were used by Greve and Pauli in [GP12] to determine the subfields of splitting fields of Eisenstein polynomials and the splitting field itself in

the case when the ramification polygon consists of one segment. As with the ramification polygon, we find conditions suitable for enumerating all possibilities, and the effects of a choice of invariant on the generators of extensions.

In the fourth chapter, a set of mass formulas are developed, one for each invariant, generalizing the work of Krasner [Kra66]. These results also appear in [Sin15]. The principal argument is developed by generalizing Krasner's original method. We present his metric on Eisenstein polynomials, whose relation to the metric on the field is essential. Next we construct a finite set of Eisenstein polynomials generating all extensions with given invariants, based upon discs in this polynomial metric. Through the relation of the two metrics, we can relate the number of these polynomials to the number of extensions.

Equipped with detailed descriptions of these invariants and their effects on generating polynomials, the fifth chapter presents an algorithm to enumerate all extensions of a p-adic field given these invariants. This algorithm, and the results leading to it, first appear in [PS14]. The premise of this algorithm is similar to that of Pauli and Roblot [PR01], who used Krasner's constructive description of a finite set of Eisenstein polynomials capable of generating all extensions of given degree and discriminant. In addition to a finer classification of extensions, the algorithm is far faster than current methods, due to results of Monge [Mon14], who used residual polynomials of components to obtain his reduced set of Eisenstein polynomials. By constructing only reduced polynomials, we greatly reduce and frequently eliminate the need to check our set of generating polynomials for isomorphisms.

In the sixth chapter, a general description of OM algorithms is given in the context of partitioning the the set of zeros of a polynomial. This approach is similar to the one used in [MPS15], which describes an OM algorithm for computing splitting fields. OM Algorithms are a versatile family of algorithms with numerous applications in algebraic number theory. Data computed by OM algorithms can be used to compute integral bases (both local and global), to factor polynomials over local fields, to determine valuations in extensions, and to solve the defining problem of p-adic numbers, the decomposition of ideals in global fields.

1.5 Implementations

All algorithms presented in this work have been implemented in computer algebra systems. We have implemented the new algorithms for enumerating invariants (Algorithms 1 and 2), counting extensions (Mass formulas from Chapter IV), and enumerating extensions (Algorithms 3, 4, and 5) described in this thesis in Magma [BCP97]. Additionally implemented is an aggregation of extension counting which produces a number of extensions for over all possibilities for invariants, see Table 2 and `http://www.uncg.edu/mat/numbertheory/tables/local/counting/`. There are several existing implementations of OM Algorithms. In Pari [PG14], they are used for polynomial factorization over $\mathbb{Z}_p$ and the computation of maximal orders of number fields. In Magma [BCP97], the power computing maximal orders, general local field polynomial factorization [Pau10], and an entire package for working with ideals [GMN10a]. We have added OM functionality to SAGE [S$^+$14], allowing polynomial factorization over $\mathbb{Z}_p$ and the construction of polynomials with given Okutsu invariants.

1.6 Future Work

While the algorithms for enumerating extensions in this work greatly improve upon current methods, there is more that can be done. The polynomials returned by Algorithm 3 do not necessarily generate distinct extensions, and the cost of filtering that list is more expensive than finding it. Using Monge's reduction methods [Mon14] instead of Panayi's root finding [Pan95] is helpful, but ideally, neither would be needed. In certain cases, we know our polynomials generate distinct extensions (see Theorem 5.9). As we see in Example 5.8, generalization of residual polynomials of segments could provide additional cases where we can avoid filtering or possibly a method to avoid it in all cases.

The formulas and algorithms of this paper are all developed over p-adic fields, not local fields in general. To work in local fields, they would need to be formulated for characteristic p local fields. As many of the results required here, in particular the work of Krasner, have seen generalization to characteristic p local fields, the generalization of this work should be possible as well.

CHAPTER II

LOCAL FIELDS AND THEIR EXTENSIONS

In this chapter, we provide an introduction to fundamental concepts in the theory of local fields. The material here is ordered in the manner of a modern instructional treatment as opposed to its historical development. For a more detailed introduction to the theory see [Ser79] or [FeVo02].

2.1 Local Fields

Definition 2.1. A map $\|\cdot\|$ from a field K to the non-negative real numbers is said to be an *ultrametric* or *non-archimedian absolute value* on K if the following hold:

$$\|x\| > 0 \text{ if } x \neq 0, \text{ with } \|0\| = 0,$$
$$\|xy\| = \|x\| \cdot \|y\|$$
$$\|x + y\| \leq \max\{\|x\|, \|y\|\}$$

The third property (the *ultrametric inequality*) distinguishes this class from general absolute values that are only bound by the weaker triangle inequality: $\|x + y\| \leq \|x\| + \|y\|$. Absolute values satisfying the triangle inequality, but not the ultrametric inequality are called *archimedian absolute values*.

Remark. Notice that if $\|x\| < \|y\|$, then

$$\|x + y\| \leq \max\{\|x\|, \|y\|\} = \|y\| = \|x + y - x\| \leq \max\{\|x + y\|, \|x\|\} = \|x + y\|,$$

which shows that $\|x + y\| = \|y\|$. Thus, if $\|x\| \neq \|y\|$, then $\|x + y\| = \max\{\|x\|, \|y\|\}$.

Definition 2.2. An *(exponential) valuation* on the field K is a map $v : K \to \mathbb{Q} \cup \{\infty\}$ such that for $a, b \in K$,

$$v(a) = \infty \iff a = 0$$
$$v(ab) = v(a) + v(b)$$
$$v(a + b) \geq \min\{v(a), v(b)\}$$

A valuation is *discrete* if $v(K^*)$ is isomorphic to $\mathbb{Z}$.

Remark. Similar to the previous remark, notice that if $v(a) > v(b)$, then

$$v(a + b) \geq \min\{v(a), v(b)\} = v(b) = v(a + b - a) \geq \min\{v(a + b), v(a)\} = v(a + b).$$

Thus, $v(a + b) = v(b)$. In general, if $v(a) \neq v(b)$, then $v(a + b) = \min\{v(a), v(b)\}$.

Example 2.3. Let p be a prime number and r be a rational number. There is a unique expression of r by $r = p^k(a/b)$ where $(a, b) = 1$ and p divides neither a or b. We can define the following:

- The map $\|r\|_p = p^{-k}$ is a non-archimedian absolute value on $\mathbb{Q}$ called the *p-adic absolute value.*
- The map $v_p(r) = k$ is a discrete valuation on $\mathbb{Q}$ called the *p-adic valuation.*

Example 2.4. The absolute value $\|\cdot\|_\infty$, defined by

$$\|a\|_\infty = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

is an archimedian absolute value on $\mathbb{Q}$.

Theorem 2.5 (Ostrowski [Ost18])**.** *An absolute value on $\mathbb{Q}$ either coincides with $(\|\cdot\|_\infty)^r$ for some $r \in \mathbb{R}$, or with $(\|\cdot\|_p)^r$ for some prime p and some $r \in [0, 1]$.*

Example 2.6. Let q be a power of a prime number p. Consider the field of formal Laurent series $\mathbb{F}_q(t)$ over the finite field $\mathbb{F}_q$. Let $\alpha \in \mathbb{F}_q(t)$ with $\alpha = \sum_{i=m}^{\infty} a_i t^i$ where a_m is a non-zero coefficient. The map $v(\alpha) = m$ is a discrete valuation on $\mathbb{F}_q(t)$.

Definition 2.7. A *local field* is a field complete with respect to a discrete non-archimedian absolute value.

Let K be a local field, complete with respect to $\|\cdot\|$. The *valuation ring* of K is

$$\mathcal{O}_K = \{\alpha \in K : \|\alpha\| \leq 1\}.$$

$\mathcal{O}_K$ is a local ring with principal, maximal ideal

$$\mathfrak{p} = \{\alpha \in K : \|\alpha\| < 1\}.$$

A generator of $\mathfrak{p}$ is called a *prime element* or *uniformizer* of K and denoted π_K. The corresponding valuation, normalized so that the valuation of π is 1, is denoted by v_π or v_K.

The *residue class field* of K is

$$\underline{K} = \mathcal{O}_K/\mathfrak{p},$$

and for $\alpha \in \mathcal{O}_K$, we write $\underline{\alpha}$ to denote the class $\alpha + \mathfrak{p}$ in $\underline{K}$. We will also represent 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 $\underline{0} \in \underline{K}$.

We may write any element of $\alpha \in K$ as a π_K*-adic expansion*

$$\alpha = \sum_{i=v_K(\alpha)}^{\infty} a_i \pi_K^i \text{ where } a_i \in \underline{K}.$$

Most of the time we are mainly interested in the first nonzero term in the π-adic expansion of an element.

Example 2.8. Let p be a prime number. The completion of $\mathbb{Q}$ with respect to $\|\cdot\|_p$ is a local field denoted $\mathbb{Q}_p$. An element $\alpha \in \mathbb{Q}_p$ can be written uniquely as the sum $\sum_{i=m}^{\infty} a_i p^i$, where $a_i \in \mathbb{F}_p$ and a_m is non-zero ($m \in \mathbb{Z}$ need not be positive). We have the non-archimedian absolute value $\|\alpha\|_p = p^{-m}$ and the valuation $v_p(\alpha) = m$. The valuation ring of $\mathbb{Q}_p$ is the ring of *p-adic integers*,

denoted by $\mathbb{Z}_p$, consisting of those elements of $\mathbb{Q}_p$ for which $m \geq 0$. The principal, maximal ideal of $\mathbb{Z}_p$ is (p) and so p is a uniformizer of $\mathbb{Q}_p$. The residue class field of $\mathbb{Q}_p$ is $\mathbb{Z}_p/(p) = \mathbb{F}_p$.

Example 2.9. Let q be a power of a prime number p. The field of formal Laurent series $\mathbb{F}_q(t)$ over the finite field $\mathbb{F}_q$ is a local field. The valuation ring of $\mathbb{F}_q(t)$ is the ring of formal power series $\mathbb{F}_q[t]$ over $\mathbb{F}_q$ with principal, maximal ideal (f), generated by any irreducible polynomial f. The residue class field of $\mathbb{F}_q(t)$ is $\mathbb{F}_q[t]/(t) = \mathbb{F}_q$.

2.2 Extensions of Valuations and Local Fields

Let K be a local field and let $\varphi \in K[x]$ be a separable, monic, and irreducible polynomial with $\deg \varphi = n$. By adjoining a root α of φ to K, we construct an algebraic extension L of K. So we have that $L = K(\alpha)$ and L is isomorphic to $K[x]/(\varphi)$. The degree of the extension L/K is $[L : K] = \deg \varphi = n$.

Definition 2.10. Let $\overline{K}$ be an algebraic closure of K. Denote the roots of φ in $\overline{K}$ by $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ where $\alpha^{(1)} = \alpha$. We say that $\alpha^{(i)}$ is the *i-th conjugate* of α.

The extension L is a vector space over K of dimension n with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$. For an element $\gamma \in L$, there is a unique representation with respect to the basis:

$$\gamma = \sum_{i=0}^{n} g_i \alpha^i \text{ with } g_i \in K \text{ for } 0 \leq i \leq n-1.$$

The conjugates of γ are $\gamma^{(i)} = \sum_{i=0}^{n-1} g_i \left(\alpha^{(i)}\right)^i$ and we define the *norm* of γ to be $\mathrm{N}_{L/K}(\gamma) = \prod_{i=0}^{n} \gamma^{(i)}$ and the *trace* of γ to be $\mathrm{tr}_{L/K}(\gamma) = \sum_{i=0}^{n} \gamma^{(i)}$.

Theorem 2.11. *Let K be a local field with valuation v_K and L/K a finite algebraic extension of degree n. Then there exists a unique extension of the valuation v_K to a valuation $v_L : L \to \mathbb{Q} \cup \{\infty\}$ with the restriction of v_L to K coinciding with v_K. The local field L is complete with respect to v_L, which is defined by $v_L(\gamma) = v_K(\mathrm{N}_{L/K}(\gamma))/n$ for $\gamma \in L$.*

Given the uniqueness of this extension, we will commonly denote both the valuation of a local field K and its extension to an algebraic closure $\overline{K}$ of K (or to any intermediate field) by v when its meaning is clear. We introduce an equivalence relation on the elements of $\overline{K}$ which reflects this.

Definition 2.12. For $\gamma \in \overline{K}^*$ and $\delta \in \overline{K}^*$ we write $\gamma \sim \delta$ if

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

and make the supplementary assumption $0 \sim 0$. For $\varphi(x) = \sum_{i=0}^{n} c_i x^i$ and $\psi(x) = \sum_{i=0}^{n} b_i x^i$ in $\overline{K}[x]$ we write $\varphi \sim \psi$ if

$$\min_{0 \le i \le n} v(c_i - e_i) \; > \; \min_{0 \le i \le n} v(c_i).$$

It follows immediately that the relation $\sim$ is symmetric, transitive, and reflexive. Let L be a finite extension of K with uniformizing element π_L. Two elements $\gamma = \gamma_0 {\pi_L}^u \in L$ and $\delta = \delta_0 {\pi_L}^w \in L$ with $v(\gamma_0) = v(\delta_0) = 0$ are equivalent with respect to $\sim$ if and only if $u = w$ and $\gamma_0 \equiv \delta_0 \bmod (\pi_L)$.

Definition 2.13. A local field that is a finite extension of $\mathbb{Q}_p$ is called a *p-adic field*.

Definition 2.14. Let L/K be an algebraic extension. Let $\mathrm{Aut}(L/K)$ be the group of automorphisms of L that fix K point-wise. If $\#\mathrm{Aut}(L/K) = [L : K]$ then we say that the extension L/K is *Galois* and that $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$ is the *Galois group of* L/K. If L is the splitting field of a non-constant polynomial $\varphi \in K[x]$, then we call $\mathrm{Gal}(\varphi) = \mathrm{Gal}(L/K)$ the *Galois group* of φ.

Definition 2.15. If L/K is an algebraic extension of degree n, then $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of degree n, and we say that a basis for $\mathcal{O}_L$ over $\mathcal{O}_K$ is an *integral basis* of L/K.

Definition 2.16. Let $\varphi \in K[x]$ be a monic polynomial of degree n with such that $\varphi(x) = \prod_{i=1}^{n}(x - \alpha^{(i)})$ in $\overline{K}$. We definite the *discriminant* of φ to be

$$\mathrm{disc}\,(\varphi) = \prod_{i<j} \left(\alpha^{(i)} - \alpha^{(j)}\right)^2 = \prod_{i \ne j} (-1)^{(n^2-n)/2} \left(\alpha^{(i)} - \alpha^{(j)}\right)$$

If φ is an irreducible polynomial and α a root of φ, then $\mathrm{disc}\,(\varphi) = \mathrm{N}_{\overline{K}/K}(\varphi'(\alpha))$.

Definition 2.17. Let L/K be an algebraic extension of degree n with integral basis $(\delta_1, \ldots, \delta_n)$. Then we define the *discriminant* of L/K to be $\mathrm{disc}\,(L/K) = \left(\det(\delta_j^{(i)})\right)^2$.

Definition 2.18. Let L be an algebraic extension of K. If $[L : K] = [\underline{L} : \underline{K}]$, then L/K is *unramified*. If $[\underline{L} : \underline{K}] = 1$, then L/K is *totally ramified*.

There exists a unique unramified extension for any positive integer degree. In fact, given any irreducible polynomial $\varphi_m \in \underline{K}[x]$ of degree m, any monic lift of φ_m to $K[x]$ defines the unramified extension of K of degree m. If L/K is an unramified extension of degree m defined by φ_m, then the uniformizer of L is the same as that of K (that is, $\pi_L = \pi_K$), $\mathrm{Gal}(L/K) = \mathrm{Gal}(\underline{L}/\underline{K})$, and $v_K(\mathrm{disc}\,(\varphi_m)) = v_K(\mathrm{disc}\,(L/K)) = 0$.

Given an extension L/K, we can construct the unique intermediate extension L^{ur}, which is unramified and of degree $[\underline{L} : \underline{K}]$. This provides a decomposition of the extension L into the tower $L/L^{ur}/K$ where L/L^{ur} is totally ramified and L^{ur}/K is unramified.

Definition 2.19. Let L be a finite algebraic extension of K. We say that the *inertia degree* of L/K is $f_{L/K} = [\underline{L} : \underline{K}]$ and that the *ramification index* of L/K is $e_{L/K} = [L : L^{ur}]$. The degree of the extension L/K is $n = e_{L/K} \cdot f_{L/K}$.

2.3 Totally Ramified Extensions and Eisenstein Polynomials

Definition 2.20. We call a monic polynomial $\varphi \in \mathcal{O}_K[x]$ with $\varphi(x) = \sum \varphi_i x^i$ an *Eisenstein polynomial* if $v_K(\varphi_0) = 1$ and $v_K(\varphi_i) \geq 1$ for $1 \leq i \leq n-1$.

Eisenstein polynomials are irreducible and define totally ramified extensions. The valuation of the discriminant of an extension defined by an Eisenstein polynomial is precisely the valuation of the discriminant of the polynomial itself. Furthermore, any prime element of a totally ramified extension of finite degree is the root of an Eisenstein polynomial and is a generating element for the extension.

Let the residue class field $\underline{K}$ have characteristic p. We say that an extension L/K is *tamely ramified* if $p \nmid e_{L/K}$ and *wildly ramified* otherwise. Given a totally ramified extension L/K, we can construct an intermediate extension L^{tame}, so that our extension splits into the tower $L/L^{tame}/K$, where L/L^{tame} is wildly ramified and L^{tame}/K is tamely ramified.

Theorem 2.21 ([GP12, Proposition 2.1])**.** *Let $n = e_0 p^m$ with $p \nmid e_0$ and let*

$$\varphi(x) = x^n + \sum_{i=1}^{n-1} \varphi_i x^i + \varphi_0 \in \mathcal{O}_K[x]$$

be a polynomial whose Newton polygon is a line of slope $-h/n$, where $\gcd(h,n)=1$. *Let α be a root of φ. The maximum tamely ramified subextension L^{tame} of $L=K(\alpha)$ of degree e_0 can be generated by the Eisenstein polynomial $x^{e_0}+\psi_0^b\pi^{e_0 a}$ with $\psi_0 \equiv \varphi_0 \mod(\pi^{h+1})$ and where a and b are integers such that $ae_0+bh=1$.*

In examples we will frequently use a table to represent sets of polynomials. 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 $\varphi_i=\sum_{j=0}^{\infty}\varphi_{i,j}\pi_K^j$ where $\varphi_{i,j} \in R_{\underline{K}}$. If φ is Eisenstein, then $\varphi_n=1$, $\varphi_{0,1} \neq 0$ and $\varphi_{i,0}>0$ for $1 \le i < n$. In our table, each cell contains a set from which the corresponding coefficient $\varphi_{i,j}$ of the π_K-adic expansion of the coefficient $\varphi_i=\sum_{j=0}^{\infty}\varphi_{i,j}\pi_K^j$ of the polynomial $\varphi(x)=\varphi_n x^n+\varphi_{n-1}x^{n-1}+\cdots+\varphi_0$ can be chosen.

Example 2.22. 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_K^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_K^1	$\{0\}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$\cdots$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}^{\times}$
π_K^0	$\{1\}$	$\{0\}$	$\{0\}$	$\cdots$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$

2.4 Hensel Lifting and Newton Polygons

Hensel lifting yields a factorization of polynomials over local fields in certain cases and Newton polygons give useful information about the roots of polynomials. We show how these two tools can be used to obtain proper factorizations in more general cases.

Theorem 2.23 (Hensel's Lemma)**.** *Let $\Phi \in \mathcal{O}_K[x]$ be monic. If $\Phi \equiv \varphi_1\varphi_2 \mod(\pi)$ where φ_1 and φ_2 are coprime modulo π, then there is a factorization $\Phi=\Phi_1\Phi_2$ with $\Phi_1 \equiv \varphi_1 \mod(\pi)$ and $\Phi_2 \equiv \varphi_2 \mod(\pi)$.*

For an example of an efficient Hensel lifting algorithm that lifts a factorization modulo (π) to a factorization modulo $(\pi)^s$ for any given s, see [Zas69]. We can also obtain an approximation to

a factorization of Φ if Hensel lifting can be applied to the characteristic polynomial of an element $\varphi + (\Phi)$ in $\mathcal{O}_K[x]/(\Phi)$.

Definition 2.24. Let $\Phi(x) = \prod_{j=1}^{N}(x - \theta_j) \in \mathcal{O}_K[x]$. For $\varphi \in K[x]$ we define

$$\chi_\varphi(y) := \prod_{i=1}^{N}(y - \varphi(\theta_i)) = \mathrm{res}_x(\Phi(x), y - \varphi(x)) \in L[y].$$

Proposition 2.25. *Let $\gamma \in K[x]$ with $\chi_\gamma \in \mathcal{O}_K[y]$. If $\underline{\chi}_\gamma$ has at least two distinct irreducible factors then Φ is reducible in $\mathcal{O}_K[x]$.*

Proof. Suppose $\underline{\chi}_\gamma$ has at least two irreducible factors. Then, Hensel's lemma gives relatively prime monic polynomials $\chi_1 \in \mathcal{O}_K[y]$ and $\chi_2 \in \mathcal{O}_K[y]$ with $\chi_1\chi_2 = \chi_\gamma$. Reordering the roots $\theta_1, \ldots, \theta_N$ of Φ if necessary, we may write

$$\chi_1(y) = (y - \gamma(\theta_1)) \cdots (y - \gamma(\theta_r)) \text{ and } \chi_2(y) = (y - \gamma(\theta_{r+1})) \cdots (y - \gamma(\theta_N)),$$

where $1 \leq r < N$. It follows that

$$\Phi = \gcd(\Phi, \chi_1(\gamma)) \cdot \gcd(\Phi, \chi_2(\gamma))$$

is a proper factorization of Φ. □

Definition 2.26 (Newton Polygon)**.** Let $\Phi(x) = \sum_{i=0}^{N} c_i x^i$. The lower convex hull of $\{(i, v(c_i)) \mid 0 \leq i \leq N\}$ is the Newton polygon of Φ.

The negatives of the slopes of the segments of the Newton polygon of Φ are the valuations of the roots of Φ. The length of the segment (in x-direction) is the number of roots with this valuation. The negatives of the slopes of the Newton polygon of the characteristic polynomial χ_φ of $\varphi + (\Phi)$ are the valuations $v(\varphi(\theta))$ for the roots θ of Φ. Proposition 2.25 yields a constructive method for finding a factorization of Φ if χ_φ has more than one segment:

Corollary 2.27. *Let $\varphi \in K[x]$ with $\chi_\varphi \in \mathcal{O}_K[y]$. If there are roots θ and θ' of Φ such that $v(\varphi(\theta)) \neq v(\varphi(\theta'))$ then we can find two proper factors of Φ over $\mathcal{O}_K[x]$.*

Proof. Let Θ be the set of roots of Φ and let $h/e = \min\{v(\varphi(\theta)) \mid \theta \in \Theta\}$. Setting $\gamma := \varphi^e/\pi^h$ we get

$$\max\{v(\gamma(\theta)) \mid \theta \in \Theta \text{ and } \gamma(\theta) = 0\} > \min\{v(\gamma(\theta)) \mid \theta \in \Theta \text{ and } \gamma(\theta) = 0\} = 0.$$

Thus Proposition 2.25 yields a factorization of Φ. □

Remark. Repeated application of Corollary 2.27 yields one factor of Φ for each segment of the Newton polygon of χ_γ.

2.5 Ramification Groups

The ramification groups define a sequence of decreasing normal subgroups which are eventually trivial and which give structural information about the Galois group of a $\mathfrak{p}$-adic field. Throughout this section, let L/K be a Galois extension with Galois group G. We first define a function on the Galois group of L/K, $i_{L/K} : G \to \mathbb{Q} \cap \{\infty\}$ by $i_{L/K}(\sigma) = \inf_{x \in \mathcal{O}_L} v_L(\sigma(x) - x)$. Notice that if α is such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, then $i_{L/K}(\sigma) = v_L(\sigma(\alpha) - \alpha)$. For any real number x, we define the following subsets of the Galois group

$$G_x = \{\sigma \in G : i_{L/K}(\sigma) \geq x + 1\}.$$

For non-integers x, we have that $G_x = G_{\lfloor x \rfloor}$. If we restrict our consideration to integers, we define the *ramification groups* of G.

Definition 2.28. For an integer $i \geq -1$, we define the *i-th ramification group* of G to be

$$G_i = \{\sigma \in G : i_{L/K}(\sigma) \geq i + 1\}.$$

The group G_0 is called the *inertia group*, the group G_1 is called the *ramification group*, and the groups G_i, $i > 1$, are called the *higher ramification groups* of L over K. Each G_i is a normal subgroup of G, and G_i is trivial for large enough i.

Proposition 2.29. *Let L/K be a Galois extension with Galois group G.*

(a) $G_{-1} = G$.

(b) G_0 *is trivial if and only if* L/K *is unramified.*

(c) G_1 *is trivial if and only if* L/K *is tamely ramified.*

Now let us consider the ramification filtration of a subextension fixed by a subgroup of G, and see how this allows us to restrict the study the higher ramification groups to the case of totally ramified extensions. Let H be a subgroup of G, and K' be the subextension of L fixed by H.

Proposition 2.30. $\mathrm{Gal}(L/K') = H$, $H_i = G_i \cap H$, *and for every* $\sigma \in G$, $i_{L/K'}(\sigma) = i_{L/K}(\sigma)$

Corollary 2.31. *Let L^{ur} be the maximum unramified subextension of L/K. Then L/L^{ur} has the same ramification groups of index ≥ 0 as L/K.*

Suppose additionally that the subgroup H is normal. Then we can consider the extension K'/K and its ramification groups.

Proposition 2.32. $\mathrm{Gal}(K'/K) = G/H$, *and for every* $\sigma \in G/H$,

$$i_{K'/K}(\sigma) = \frac{1}{e_{L/K}} \sum_{s \to \sigma} i_{L/K}(s).$$

Corollary 2.33. *If $H = G_j$ for some integer $j \geq 0$, then $(G/H)_i = G_i/H$ for $i \leq j$ and $(G/H)_i = \{1\}$ for $i \geq j$.*

In addition to the sequence of decreasing groups, we can consider the particular indices at which the sets become strictly smaller and how they are related to one another.

Definition 2.34. Integers i such that $G_i \neq G_{i+1}$ are called the *(lower) ramification breaks* of L/K.

Proposition 2.35. *If G is abelian, then every ramification break must be divisible by the order of G_0/G_1.*

Proposition 2.36. *Let p be the characteristic of $\underline{L}$ and i and j be any two ramification breaks of L/K. Then $i \equiv j \mod p$.*

2.6 The Hasse-Herbrand Function

Let L/K be a Galois extension with Galois group G. We define the *Hasse-Herbrand function* on L/K by

$$\phi_{L/K}(u) = \int_0^u \frac{dt}{[G_0 : G_t]}.$$

We can make the definition of ϕ more explicit by observing that our ramification breaks occur at integers, that is, $G_t = G_{\lfloor t \rfloor}$. Let $m \in \mathbb{Z}^{>0}$ and $u \in \mathbb{R}$ with $m \leq u \leq m+1$. Then

$$\phi_{L/K}(u) = \frac{1}{\#G_0}\left(\#G_1 + \ldots \#G_m + (u-m)\#G_{m+1}\right)$$

and in particular for integers,

$$\phi_{L/K}(m) + 1 = \frac{1}{\#G_0}\sum_{i=0}^{m} \#G_i$$

Proposition 2.37. *The function $\phi_{L/K}$ has the following properties.*

(a) *The function $\phi_{L/K}$ is continuous, piecewise linear, increasing, and concave.*

(b) $\phi_{L/K}(0) = 0$.

(c) *Let $\partial_+\phi_{L/K}$ and $\partial_-\phi_{L/K}$ denote the right and left derivatives of $\phi_{L/K}$, then $\partial_-\phi_{L/K}(u) = [G_0 : G_u]^{-1}$ and*

$$\partial_+\phi_{L/K}(u) = \begin{cases} \partial_-\phi_{L/K}(u) = [G_0 : G_u]^{-1} & \text{if } u \text{ is not an integer} \\ [G_0 : G_{u+1}]^{-1} & \text{if } u \text{ is an integer} \end{cases}.$$

Let $\psi_{L/K}$ be the inverse of ϕ.

Proposition 2.38. *The function $\psi_{L/K}$ has the following properties.*

(a) *The function $\psi_{L/K}$ is continuous, piecewise linear, increasing, and convex.*

(b) $\psi_{L/K}(0) = 0$.

(c) *If* $v = \phi_{L/K}(u)$, *then* $\partial_- \psi_{L/K}(v) = \left(\partial_- \phi_{L/K}(u)\right)^{-1}$ *and* $\partial_+ \psi_{L/K}(v) = \left(\partial_+ \phi_{L/K}(u)\right)^{-1}$. *In particular,* $\partial_- \psi_{L/K}$ *and* $\partial_+ \psi_{L/K}$ *are integers.*

(d) *If* v *is an integer, then so is* $u = \psi_{L/K}(v)$.

These functions allow us to define the *upper numbering* of ramification groups. While the lower numbering is well suited for the consideration of subgroups, the upper number is adapted to quotients.

Definition 2.39. The upper number of ramification groups is

$$G^v = G_{\psi_{L/K}(v)} \text{ or, equivalently, } G^{\phi_{L/K}(u)} = G_u.$$

Any number v such that $G^v \neq G^{v+\epsilon}$ is an *upper ramification break* of L/K.

Proposition 2.40. *If* H *is a normal subgroup of* G, *then* $(G/H)^v = G^v H/H$.

Theorem 2.41 (Herbrand)**.** *If* $v = \phi_{L/K}(u)$, *then* $G_u H/H = (G/H)_v$ *for all* v.

The upper numbering is particularly interesting in the abelian case.

Theorem 2.42 (Hasse-Arf)**.** *If* G *is an abelian group and if* v *is an upper ramification break, then* v *is an integer.*

CHAPTER III

INVARIANTS OF LOCAL FIELD EXTENSIONS

In this chapter, we develop the properties of three invariants of local fields, the discriminant, the ramification polygon, and residual polynomials of segments. For each, we will develop conditions for the invariant to take a certain value, conditions on generating polynomials, and describe and enumerate the permissible values.

3.1 Discriminant

We recall some of the results Krasner used to obtain his formula for the number of extensions of a p-adic field [Kra66]. These can also be found in [PR01].

The possible discriminants of finite extensions are given by Ore's conditions [Ore26]:

Proposition 3.1 (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 3.2. *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 [Kra66].

Lemma 3.3. *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 3.2 and Lemma 3.3 we obtain a finite set of polynomials that generate all extensions of a given degree and discriminant. In [PR01] this set in conjunction with Krasner's mass formula [Kra66] and Panayi's root finding algorithm is used to obtain a generating polynomial for each extension of a given degree and discriminant.

Example 3.4. 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 3.2 with $J_0 = 10$, $a_0 = 1$, and $b_0 = 1$ we get $v_\pi(\varphi_1) = 2$ and $v_\pi(\varphi_i) = 2 - v_\pi(i)$ for $1 < i < n$. Furthermore by Lemma 3.3 $\varphi_{i,j} = 0$ for $0 \leq i \leq 9$ and $j > 3$. 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}	**{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}**	{0,1,2}	**{0}**	**{0}**	{1,2}
3^0	{1}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}

3.2 Ramification Polygons

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

Definition 3.5. 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 [GP12, 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 [Sch03], compute splitting fields and Galois groups [GP12], describe maximal abelian extensions [Lub81], and answer questions of commutativity in p-adic dynamical systems [Li97].

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

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

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

$$v_\alpha(\rho_i) = \min_{i \le k \le n} \left\{ v_\alpha\left(\binom{k}{i} \varphi_k \, \alpha^k \right) - n \right\} = \min_{i \le k \le n} \left\{ n \left[v_\pi\left(\binom{k}{i} \varphi_k \right) - 1 \right] + k \right\}. \tag{3.1}$$

Lemma 3.6 ([Sch03, 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. 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 3.4.

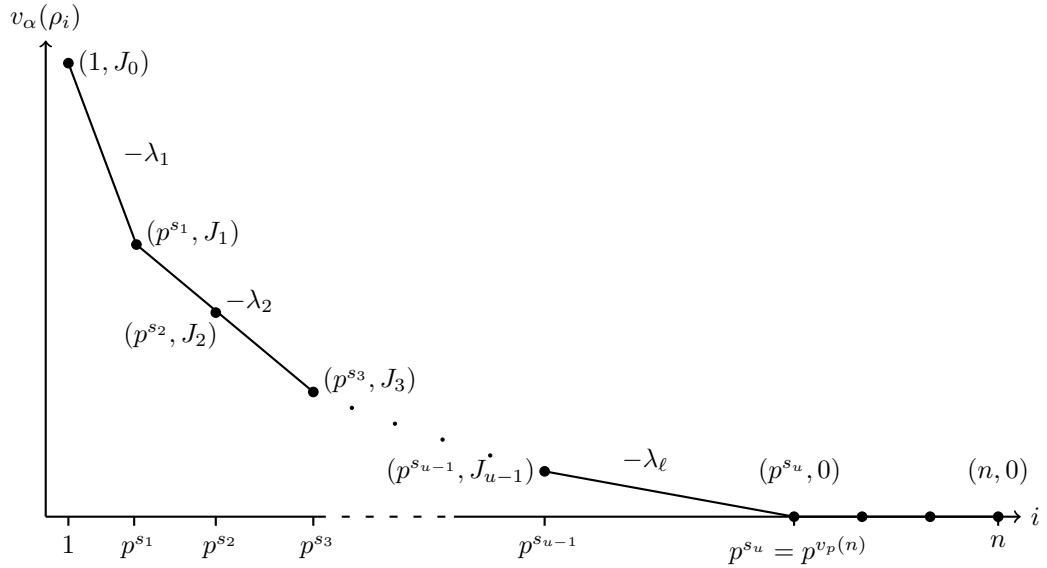


Figure 1. Ramification polygon of an Eisenstein polynomial φ of degree n and discriminant $(\pi)^{n+J_0-1}$ with $\ell+1$ segments and $u-1$ points on the polygon with ordinate above 0.

We now investigate the points on a ramification polygon further.

Lemma 3.7. *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 $v_\alpha(\rho_i) = 0$ and $\rho_i \equiv \binom{n}{i} \bmod (\alpha)$ if and only if $v_\alpha\binom{n}{i} = 0$.*

(b) *For $0 \le i \le u$ we have*

$$\rho_{p^{s_i}} \sim \varphi_{b_i} \binom{b_i}{p^{s_i}} \alpha^{b_i - n}.$$

It follows from (a) 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 3.8. *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 $0 \leq b_i \leq n-1$. Then for $0 \leq t \leq u$, we have*

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

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

Proof. By Equation (3.1), for all k with $s_t \leq k \leq n$,

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

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,

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

Now if we consider a point $(p^{s_t}, a_t n + b_t)$ with $b_t \neq 0$, then by Equation (3.1) we have

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

and as $0 < b_t < n$, 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 3.1) 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 3.9. *Let $\mathcal{R}_\varphi$ be the ramification polygon of φ as in Lemma 3.8. Then for each point (p^{s_i}, J_i) where $J_i = a_i n + b_i$ with $0 \le b_i \le n-1$,*

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

Proof. The $k = n$ term of Equation (3.1) is

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

If $b_i \neq 0$, then by Lemma 3.8, $v_\pi(\varphi_{b_i}) = a_i + 1 - v_\pi\binom{b_i}{p^{s_i}}$. 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 $v_\pi(\varphi_{b_i}) \ge 1$, hence $nv_\pi(\varphi_{b_i}) - n \ge 0$. This combined with $b_i > 0$ gives us that

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

If $b_i = 0$, then the minimum term of Equation (3.1) 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 3.10. *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 (3.1), 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 3.8 and 3.10 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 3.11. 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

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

Lemma 3.12. *Let $\mathcal{R}_\varphi$ be the ramification polygon of φ with points*

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

where $J_i = a_i n + b_i$ with $0 \leq b_i \leq n-1$. Then $p^{s_i} \mid J_i$ for $0 \leq i \leq u$.

Proof. As J_0 is an integer, $p^0 = 1$ divides J_0, and as $J_u = 0$, clearly $p^{s_u} | J_u$.

Suppose that for some $1 \leq i < u$ we have $v_p(J_i) = t < s_i$. If $\mathcal{R}$ is the ramification polygon of φ with ramification polynomial ρ and contains (p^{s_i}, J_i), then $t < s_i$ must imply that $J_i < v_\alpha(\rho_{p^t})$, which is bounded above by the $k = b_i$ term of Equation (3.1). By Lemma 3.8, we have that $v_\pi(\varphi_{b_i}) = a_i + 1 - v_\pi\binom{b_i}{p^{s_i}}$. If we substitute this value of $v_\pi(\varphi_{b_i})$ into Equation (3.1), then

$$v_\alpha(\rho_{p^t}) \leq n\left[v_\pi\binom{b_i}{p^t} + v_\pi(\varphi_{b_i}) - 1\right] + b_i = n\left[v_\pi\binom{b_i}{p^t} + a_i - v_\pi\binom{b_i}{p^{s_i}}\right] + b_i$$

As $p^t || b_i$, the p^t-term of the base p expansion of b_i is non-zero, so $v_p\binom{b_i}{p^t} = 0$ and consequently $v_\pi\binom{b_i}{p^t} = 0$. Thus, $v_\alpha(\rho_{p^t}) \leq n\left[a_i - v_\pi\binom{b_i}{p^i}\right] + b_i \leq a_i n + b_i = J_i$. This implies that $\mathcal{R}$ cannot have the point (p^{s_i}, J_i), and by contradiction, our claim is shown. □

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 3.13. *Let*

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

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

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

(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*

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

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 Corollary 3.9. If $b_i = b_k$, then by Lemma 3.8

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

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 3.8, we have that for all other points (p^{s_t}, J_t),

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

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 3.10, for each point $(p^{s_i}, a_i n + b_i)$ of $\mathcal{P}$ with $b_i > p^i$,

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

from which we have assumption (d). Assumption (e) is given by Lemma 3.7. 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 (3.1) 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 $v_\alpha(\rho_{p^{s_i}})$.

$$v_\alpha(\rho_{p^{s_i}}) = \min\left\{\min_{\{(p^{s_k}, J_k) \in \mathcal{P} : b_k \geq p^{s_i}\}}\left\{n\left[a_k - v_\pi\binom{b_k}{p^{s_k}} + v_\pi\binom{b_k}{p^{s_i}}\right] + b_k\right\}, n v_\pi\binom{n}{p^{s_i}}\right\}. \tag{3.2}$$

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 (3.2) 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 (3.2) 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 (3.2), 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 our assumption

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

and substitute it into Equation (3.2). After simplifying we get

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

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 3.7, $\mathcal{R}_\psi$ has points satisfying Assumption (e). Thus $\mathcal{R}_\psi = \mathcal{P}$. □

Proposition 3.14. *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 3.11.

Proof. If φ has ramification polygon $\mathcal{R}$, then this is the result of Lemmas 3.8 and 3.10.

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 (3.1) 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 3.13 (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 3.13 (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 $\mathcal{R}_\varphi = \mathcal{R}$. □

Definition 3.15. 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 3.13 a *ramification polygon*. We call the function $\phi_{\mathcal{R}} : \mathbb{R}^{>0} \to \mathbb{R}^{>0}$, $\lambda \mapsto \min_{0 \leq i \leq u}\{\frac{1}{n}(J_i + \lambda p^{s_i})\}$ the *Hasse-Herbrand function* of $\mathcal{R}$.

Remark. The function $\phi_{\mathcal{R}}$ in Definition 3.15 agrees with the connections between the ramification polygon and the Hasse-Herbrand transition function as observed in [Lub81, Li97]. 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 [Ser79, FeVo02]. For non-Galois extensions, our function agrees with the transition function for ramification sets defined by Helou in [Hel90].

Example 3.16 (Example 3.4 continued)**.** There are three possible ramification polygons for extensions L of $\mathbb{Q}_3$ of degree 9 with $v_3(\mathrm{disc}\,(L)) = 18$. These polygons are $\mathcal{R}_1 = \{(1,10),(9,0)\}$, $\mathcal{R}_2 = \{(1,10),(3,3),(9,0)\}$, and $\mathcal{R}_3 = \{(1,10),(3,6),(9,0)\}$ and are illustrated in Figure 2.

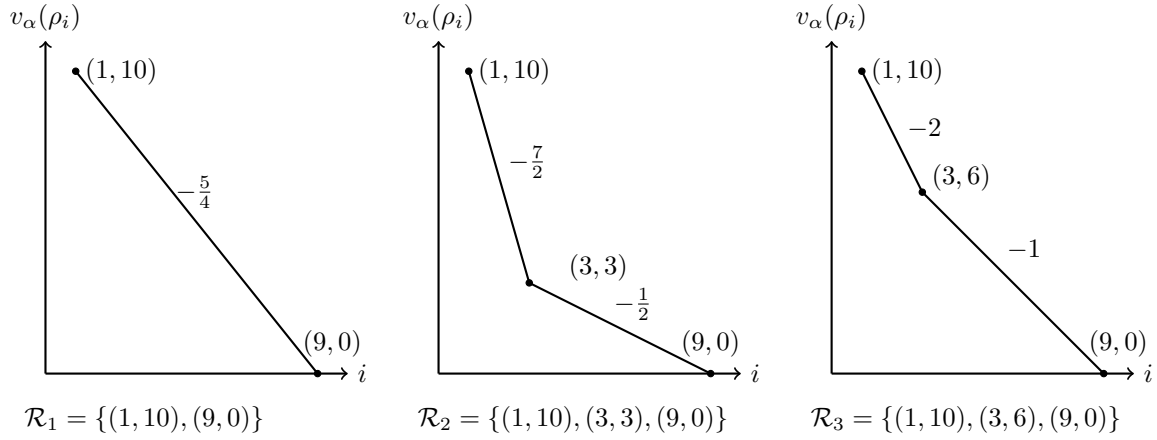


Figure 2. Possible ramification polygons of extensions L of $\mathbb{Q}_3$ of degree 9 with $v_3(\mathrm{disc}\,(L)) = 18$.

Since by Lemma 3.8 we have $v(\varphi_3) = 1$, 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}

3.3 Enumerating Ramification Polygons

In order to use later counting and enumerating results, we need a method of computing all of the possible ramification polygons for a given base field, degree, and discriminant. A naive method exists: Ramification polygons only depend on the valuations of the coefficients of an Eisenstein polynomial, and by Krasner's bound (Lemma 3.3), those are bounded above, so we can simply try all sequences of valuations. However, no matter how fast finding a ramification polygon by Equation (3.1) may be, this still requires at least $(c-1)^{n-2}$ such computations. Proposition 3.13 provides a

necessary and sufficient set of conditions for a set of points to be a ramification polygon, which gives rise to a far more efficient enumeration method.

Given a degree $n = e_0 p^r$ and discriminant valuation $n - J_0 + 1$, we know that $(1, J_0)$ must be on our polygon, and that we have a segment from $(p^r, 0)$ to $(n, 0)$. This gives us a partial ramification polygon $\mathcal{P}$ to start from, after which we can consider what points may be above p^{r-1} and then continue from right to left, considering each abscissa. Our algorithm proceeds recursively, considering the next abscissa from a partial polygon $\mathcal{P}$.

Assume we have a partial polygon $\mathcal{P}$ and the minimum valuations of φ_i required for the points of $\mathcal{P}$ and wish to find all points above p^s that we can attach. Let (p^t, J_t) be the next point in $\mathcal{P}$ to the right of p^s. Geometrically, the ordinate above p^s must be between the continuation of the segment ending at p^t and the segment from (p^t, J_t) and $(1, J_0)$. This can be seen in Figure 3. Algebraically, using Lemma 3.8, we can use our minimum values of φ_i and Equation (3.1) to find a minimum for $v(\rho_{p^s})$ and the valuations fixed by the points of the polygon to find a maximum. In this allowable range, we only have to consider multiples of p^s, by Lemma 3.12. In order to add a point, we simply have to verify that the valuation fixed by the new point is not below our existing minimum valuations and that the change to our minimum valuations from adding the point (Lemma 3.8) and any absence of points for all p^k with $p^s < p^k < p^t$ (Lemma 3.10) do not increase existing $v(\varphi_i)$ fixed by the points $\mathcal{P}$.

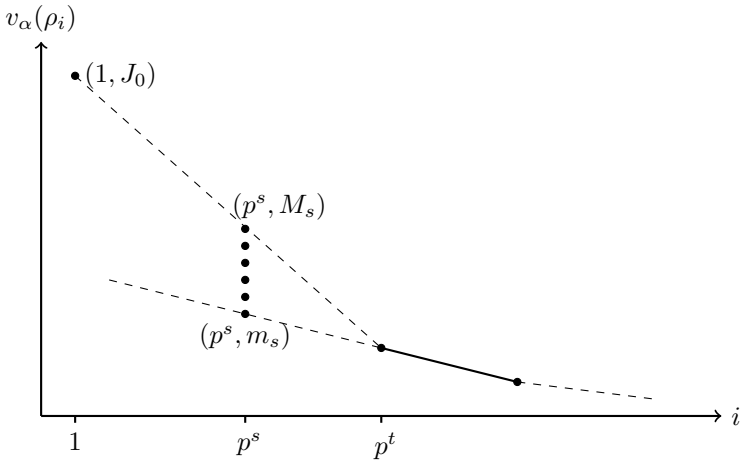


Figure 3. Possible points on a ramification polygon above p^s based on existing points.

Algorithm `AllRamificationPolygons`

Input: A π-adic field K, partial ramification polygon $\mathcal{P}$, exponent s of the abscissa to consider, and $V(i)$, minimum valuations for φ_i based on $\mathcal{P}$.

Output: All ramification polygons that may differ from $\mathcal{P}$ by points above p to p^s.

(a) Let (p^t, J_t) be the point of $\mathcal{P}$ with minimal t given $t > s$.

(b) If $s = 0$, then

  (i) For $k \in \{t-1, t-2, \ldots, 1\}$ do

  - $M_v \leftarrow v(\rho_{p^k})$ assuming $v(\varphi_i) = V(i)$ for $i \in \{y \mod n | (x,y) \in \mathcal{P}\} \cup \{n\}$
  - If $M_v < \left(\dfrac{J_0 - J_t}{1 - p^t}\right)(p^k - 1) + J_0$ then return $\emptyset$.
  - $V(i) \leftarrow \max\{V(i), l(i,k)\}$ with l computed for no point above p^k.

  (ii) Return $\{\mathcal{P}\}$.

(c) $m_v \leftarrow v(\rho_{p^k})$ assuming $v(\varphi_i) = V(i)$.

(d) $m_s \leftarrow \max\{p^s, \lambda(p^s - p^t) + J_t\}$ where λ is the slope of the segment with p^t as left vertex.

(e) $M_v \leftarrow v(\rho_{p^k})$ assuming $v(\varphi_i) = V(i)$ for $i \in \{y \mod n | (x,y) \in \mathcal{P}\} \cup \{n\}$.

(f) $M_s \leftarrow \left(\dfrac{J_0 - J_t}{1 - p^t}\right)(p^s - 1)$

(g) $m \leftarrow \max\{m_v, m_s\}$ and $M \leftarrow \min\{M_v, M_s\}$.

(h) If $m > M$, then return `AllRamificationPolygons`$(K, \mathcal{P}, s-1, V)$.

(i) $R \leftarrow \{\mathcal{P}\}$.

(j) For $y \in \{y \in \mathbb{Z} \mid m \le y \le M \text{ and } y \mod p^s \equiv 0\}$ do

  (i) $b \leftarrow y \mod n$.

  (ii) If $b > 0$ and $V(s) > l(b,s)$ (using the point (p^s, y)), then **next** y.

  (iii) $V_y(i) \leftarrow \max\{V(i), l(i,s)\}$ with $l(i,s)$ computed for point (p^s, y).

  (iv) For $k \in \{t-1, t-2, \ldots, s+1\}$ do

  - $M_v \leftarrow v(\rho_{p^k})$ assuming $v(\varphi_i) = V(i)$ for $i \in \{y \mod n | (x,y) \in \mathcal{P}\} \cup \{n\}$.
  - If $M_v < \left(\dfrac{y - J_t}{p^s - p^t}\right)(p^k - p^s) + y$ then **next** y.
  - $V_k(i) \leftarrow l(i,k)$ computed for no point above p^k.
  - If $V(i) < V_k(i)$ for any $i \in \{y \mod n | (x,y) \in \mathcal{P}\} \cup \{b\}$ then **next** y.
  - $V_y(i) \leftarrow \max\{V_y(i), V_k(i)\}$.

  (v) If $\min_{p^s \le i \le n} \left\{ n \left[v_\pi\binom{i}{p^s} + V_y(i) - 1 \right] + i \right\} \neq y$ then **next** y.

  (vi) Append $\mathcal{P} \cup \{(p^s, y)\}$ to R.

(k) Return $\bigcup_{r \in R}$ `AllRamificationPolygons`$(K, r, s-1, V_y)$.

Algorithm 1. `AllRamificationPolygons`

The algorithm `AllRamificationPolygons` (Algorithm 1) does what we have described and can be used to find all ramification polygons for a given degree $n = e_0 p^r$ and discriminant valuation $n + J_0 - 1$, by initializing $\mathcal{P} = \{(1, J_0), (n, 0), (p^r, 0)\} \cup \{(i, 0) \mid p^r < i < n \text{ and } v_p\binom{n}{i} = 0\}$ and $V(i) = l(i, 0)$ (Definition 3.11).

Example 3.17. In Table 1, we consider all ramification polygons for extensions of $\mathbb{Q}_3$ with discriminants given by the following values of J_0: 1, 11, 33, and 81. For all of these except 11, there is only one ramification polygon actually possible.

Table 1. Construction of all ramification polygons for degree 27 extensions over $\mathbb{Q}_3$ with discriminant $(3)^{27+J_0-1}$ for $J_0 \in \{1, 11, 33, 81\}$.

J_0	Initial $\mathcal{P}$	Above 9	Above 3	Notes
1	$\{(1,1),(27,0)\}$	*none* (step h)	*none* (step h)	Only polygon for $J_0 = 1$
11	$\{(1,11),(27,0)\}$	*none* (step h)	*none*	Valid polygon
			(3,3)	Valid polygon
			(3,6)	Valid polygon
			(3,9)	Fails in step (j)(v)
33	$\{(1,33),(27,0)\}$	*none*	*none*	Fails in step (b)(i)(2) $(k = 1)$
			(3,6)	Only polygon for $J_0 = 33$
		(9,9)	*none*	Fails in step (b)(i)(2) $(k = 1)$
		(9,18)	–	Fails in step (j)(v)
81	$\{(1,81),(27,0)\}$	*none*	*none*	Fails in step (b)(i)(2) $(k = 1)$
			(3,54)	Fails in step (j)(iv)(2) $(k = 2)$
		(9,27)	*none*	Fails in step (b)(i)(2) $(k = 1)$
			(3,54)	Only polygon for $J_0 = 81$

The table shows, from left to right, the recursions of the algorithm. We first begin with our initial polygon $\mathcal{P}$. There are three stages in this example, considering possible points above 9 and 3, and then verifying our polygon if it has no point above 3 (and possibly 9 as well). It should be noted that the absence of a point is not checked until another point is added, or we reach $s = 0$. For instance, we know that we cannot have the polygon $\{(1, 81), (27, 0)\}$ because of the check performed at the $s = 0$ stage, whereas we learn that we cannot have $\{(1, 81), (3, 54), (27, 0)\}$ when we attempt to add $(3, 54)$. Except for waiting to check the validity of a missing point, the algorithm discards a

branch as soon as it is clear that no valid polygons will come from it. This is what happens when we attempt to add $(9, 18)$ to $\{(1, 33), (27, 0)\}$.

3.4 Residual Polynomials of Segments

Residual (or associated) polynomials were introduced by Ore [Ore28]. 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 [GMN13, Mon99, MN92] and the closely related problem of polynomial factorization over local fields [GNP12, Pau10].

Definition 3.18 (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. 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 [GP12, Theorem 9.1].

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

Lemma 3.19. *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 $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ and let $\underline{A}_1, \ldots, \underline{A}_\ell$ 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 3.7 we obtain:

Proposition 3.20. *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 $(p^{s_k}, J_k), \ldots, (p^{s_l}, J_l)$ 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 immediately get:

Corollary 3.21. *Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein and $\mathcal{R}_\varphi$ its ramification polygon.*

(a) *The residual polynomial of the rightmost segment of $\mathcal{R}_\varphi$ is monic.*

(b) *Let (p^{s_l}, J_l) be the right end point of the i-th segment of $\mathcal{R}_\varphi$ and $\underline{A}_i = \sum_{j=0}^{m_i} \underline{A}_{i,j}$ its residual polynomial and let (p^{s_k}, J_k) be the left end point of the $(i+1)$-st segment of $\mathcal{R}_\varphi$ and $\underline{A}_{i+1} = \sum_{j=0}^{m_{i+1}} \underline{A}_{i+1,j}$ its residual polynomial. Then $\underline{A}_{i,m_i} = \underline{A}_{i+1,0}$.*

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

Proposition 3.22. *Let $n = p^r e_0$ with $\gcd(p, e_0) = 1$ and let $\mathcal{R}$ be a polygon with points*

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

satisfying Proposition 3.13. Write $J_k = a_k n + b_k$ with $0 \leq b_k \leq n$. Let $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ be the segments of $\mathcal{R}$ with endpoints (p^{k_i}, J_{k_i}) and (p^{l_i}, J_{l_i}) and slopes $-h_i/e_i$ $(1 \leq i < \ell)$. For $1 \leq i < \ell$ 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 $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ with residual polynomials $\underline{A}_1, \ldots, \underline{A}_\ell \in \underline{K}[x]$ if and only if

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

(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 3.19 (b) and property (b) is given by Proposition 3.20 (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 3.20, 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 ψ be a

polynomial in $\mathcal{O}_K[x]$ with $\psi_{e_0 p^r} = 1$, $v_\pi(\psi_0) = 1$ and

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

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

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

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 $1 \le t, q \le u$, we have $b_t = b_q$, with $s_{k_i} \le s_t \le s_{l_i}$ and $s_{k_j} \le s_q \le s_{l_j}$, then let $b = b_t = b_q$ and we have

$$\begin{aligned}\underline{\psi}_{b, 1+a_t - v_\pi\binom{b}{p^{s_t}}} &= \underline{A}_{i,(p^{s_t} - p^{s_{k_i}})/e_i} \underline{\binom{b}{p^{s_t}}^{-1} (-\psi_{0,1})^{a_t+1} \pi^{v_\pi\binom{b}{p^{s_t}}}} \\ \underline{\psi}_{b, 1+a_q - v_\pi\binom{b}{p^{s_q}}} &= \underline{A}_{j,(p^{s_q} - p^{s_{k_j}})/e_j} \underline{\binom{b}{p^{s_q}}^{-1} (-\psi_{0,1})^{a_q+1} \pi^{v_\pi\binom{b}{p^{s_q}}}}.\end{aligned}$$

As $\mathcal{R}$ is a ramification polygon, by Proposition 3.13 (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 3.13, 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 3.20, 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,

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

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

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

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

3.4.1 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 [GP12, Proposition 4.4] we obtain:

Lemma 3.23. *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 3.22 we obtain:

Theorem 3.24. *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 $\underline{A}_i(x) = \sum_{j=0}^{m_i}$ its residual*

polynomial. Then

$$\mathcal{A} = \left\{ \left(\gamma_{\delta,1} \underline{A}_1(\underline{\delta}^{h_1} x), \ldots, \gamma_{\delta,\ell} \underline{A}_\ell(\underline{\delta}^{h_\ell} x) \right) : \underline{\delta} \in \underline{K}^\times \right\} \tag{3.3}$$

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* $1 \le i \le \ell - 1$ *is an invariant of the extension* $K[x]/(\varphi)$.

Example 3.25. 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 $\mathcal{A} = \{(1 + 2x, 2 + x^3), (1 + x, 1 + x^3)\}$.

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 3.26. *Let* $\varphi \in \mathcal{O}_K[x]$ *be Eisenstein of degree* n. *Let* $\mathcal{S}$ *be a segment of 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*

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

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

Proof. By Lemma 3.8, $v_\pi(\varphi_{b_i}) = j$ and by Proposition 3.20

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

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

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

As by Lemma 3.7 $v_\alpha(\varphi_{b_i}) = v_\alpha(\rho_{p^{s_i}}) - v_\alpha\binom{b_i}{p^{s_i}} - b_i + n = a_i n + b_i - v_\alpha\binom{b_i}{p^{s_i}} - b_i + n = n(a_i+1) - v_\alpha\binom{b_i}{p^{s_i}}$ we have $\varphi_{b_i} \sim \varphi_{b_i,j}\pi^{a_i+1-v_\pi\binom{b_i}{p^{s_i}}}$. Therefore

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

A change of the uniformizer α of $L = K(\alpha)$ to $\delta\alpha$ with $v(\delta) = 0$ that determines the representative $(\underline{A}_1, \dots, \underline{A}_\ell) \in \mathcal{A}$ also effects the constant coefficient of the generating polynomial. Namely if the Eisenstein polynomial $\varphi = x^n + \sum_{i=0}^{n-1}\varphi_i x^i \in \mathcal{O}_K[x]$ is the minimal polynomial of α then $\psi(x) = \delta^n\varphi\left(\frac{x}{\delta}\right)$ with $\psi_{0,1} = \delta^n\varphi_{0,1}$ is the minimal polynomial of $\delta\alpha$.

Lemma 3.27. *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 [Mon14, 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

$$\mathcal{A}^* = \left\{\left(\gamma_{\delta,1}\underline{A}_1(\underline{\delta}^{h_1}x), \dots, \gamma_{\delta,\ell}\underline{A}_\ell(\underline{\delta}^{h_\ell}x)\right) : \underline{\delta} \in \underline{K}^\times, \underline{\delta}^n = 1\right\} \tag{3.4}$$

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. Let a ramification polygon $\mathcal{R}$ and $\underline{A}_1, \dots, \underline{A}_\ell \in \underline{K}[x]$ satisfying Proposition 3.22. Let $\mathcal{A}$ as in Theorem 3.24 and $\mathcal{A} = \mathcal{A}^{*1} \cup \dots \cup \mathcal{A}^{*k}$ be the partition of $\mathcal{A}$ into sets as in Equation (3.4). 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 3.28. *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 3.20, 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

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

Thus, the residual polynomials of $\varphi(x)$ are $(\underline{A}_1, \ldots, \underline{A}_\ell)$ and $K[x]/(\psi) \cong K[x]/(\varphi)$. □

Example 3.29 (Example 3.16 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 3.25) and $\mathcal{A}_{2,2} = \{(2+2x, 2+x^3), (2+x, 1+x^3)\}$.

By Lemma 3.27 all extensions of $\mathbb{Q}_3$ with ramification polygon $\mathcal{R}$ can be generated by polynomials $\varphi \in \mathbb{Z}_3[x]$ with $\varphi_0 \equiv 3 \bmod 9$. 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 3.26 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 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 3.4.2 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 $\mathcal{A}$.

3.5 Enumerating Residual Polynomials of Segments

To compute all possible $(\underline{A}_1, \ldots, \underline{A}_\ell)$ for a given ramification polygon $\mathcal{R}$, we can create sequence of residues, with one assigned to each point of $\mathcal{R}$, insuring that the requirements of Proposition 3.22

hold, and directly construct the polynomials. By making the assignment to points, the matching of the leading term of one polynomial to the constant term of the next is handled by construction. The principle problem, then, is to make sure that coefficients linked to each other as in Proposition 3.22 (c) are correctly computed. This requires us to choose the constant coefficient of our Eisenstein polynomial, effectively choosing a tamely ramified subextension.

Our algorithm `AllResidualPolynomials` (Algorithm 2) does just this. It does not, however, directly compute all possibilities for the invariant $\mathcal{A}$. Instead it finds all representatives of possible $\mathcal{A}^*$ given the fixed choice of $\underline{\varphi_{0,1}}$. By Remark 3.4.2, if n is a power of p, then each $(\underline{A}_1, \ldots, \underline{A}_\ell)$ in the output belongs to a disjoint $\mathcal{A}^*$. On the other hand, if n is not a power of p, then the output may contain more than one representative of each $\mathcal{A}^*$. In order to compute the possible $\mathcal{A}^*$, one would need to construct the set from Equation (3.4) for each $(\underline{A}_1, \ldots, \underline{A}_\ell)$ in the output and check their intersections to partition them into the distinct $\mathcal{A}^*$.

At any degree, multiple elements of the output may belong to the same invariant $\mathcal{A}$. Similar to partitioning into distinct $\mathcal{A}^*$, we can compute the possible $\mathcal{A}$ by constructing the sets from Equation (3.3) for each $(\underline{A}_1, \ldots, \underline{A}_\ell)$ in the output and comparing to partition them into the distinct $\mathcal{A}$.

Algorithm `AllResidualPolynomials`

Input: A π-adic field K, ramification polygon $\mathcal{R}$, and residue of constant coefficient $\underline{\varphi_{0,1}}$

Output: All $(\underline{A}_1, \ldots, \underline{A}_\ell)$ satisfying the conditions of Proposition 3.22.

(a) If $b_0 = 0$ then $L \leftarrow \{(n(-\varphi_{0,1})^{-a_0})\}$, else $L \leftarrow \{(\delta) : \delta \in \underline{K}^\times\}$

(b) While $\min_{A \in L}\{len(A)\} < \#\mathcal{R}$ do

  (i) Remove A from the front of L and let $s \leftarrow len(A) + 1$.
  Let $(x_s, a_s n + b_s)$ be the s^{th} point of $\mathcal{R}$.

  (ii) If $b_s = 0$ then

  - If $x_s = n$ then append $\underline{1}$ to A, else append $\underline{\binom{n}{x_s}(-\varphi_{0,1})^{-a_s}}$ to A.
  - Append A to the end of L.

  (iii) Else if $b_s = b_q$ for some $q < s$ then append $\underline{\binom{b_s}{x_s}\binom{b_s}{x_q}^{-1}(-\varphi_{0,1})^{a_q - a_s}}$ to A, and append A to the end of L.

  (iv) Else for $\delta \in \underline{K}^\times$, let A' be A with δ appended and append A' to L.

(c) $R \leftarrow \{\}$.

(d) For A in L do

  (i) $P \leftarrow \{\}$.

  (ii) For each segment $\mathcal{S}$ of $\mathcal{R}$ do

  - Let (x_k, J_k) be the left endpoint and $\frac{-h}{e}$ be the slope of $\mathcal{S}$.
  - Append $\displaystyle\sum_{(x_s, J_s) \in \mathcal{S}} A_s z^{(x_s - x_k)/e}$ to P

  (iii) Append P to R.

(e) Return R.

Algorithm 2. `AllResidualPolynomials`

CHAPTER IV

COUNTING EXTENSIONS WITH GIVEN INVARIANTS

In [Kra66], Krasner gave a formula for the number of totally ramified extensions of a $\mathfrak{p}$-adic field, using his famous lemma as a main tool. In addition to the choice of degree, his formula depended on the choice of discriminant. This choice allows the construction of a finite set of Eisenstein polynomials which generate all totally ramified extensions of given discriminant. A metric on polynomials provides us one of the needed bounds for this set and relates the number of these polynomials to the number of extensions. In this chapter, we generalize these methods to compute the number of totally ramified extensions with the additional choice of ramification polygon and residual polynomials of segments.

4.1 An Ultrametric Distance of Polynomials

For two irreducible polynomials $f, g \in K[x]$ of degree n, we define an ultrametric distance that we will later relate to the distance of the roots of these two polynomials.

Proposition 4.1. *Let $f, g \in K[x]$ be two irreducible polynomials of degree n. If α is any root of f and β is any root of g, then $d(f,g) = |f(\beta)| = |g(\alpha)|$ defines an ultrametric distance over the set of irreducible polynomials of degree n in $K[x]$. Additionally, if $\alpha = \alpha_1, \ldots, \alpha_n$ are the roots of f, and β is one of the roots of g which is closest to α, then*

$$d(f,g) = \prod_{i=1}^{n} \{|\beta - \alpha|, |\alpha - \alpha_i|\}.$$

Proof. The proof closely follows that of Proposition 4.1 in [PR01].

To begin, let $d(f,g) = |f(\beta)|$. It is clear that $d(f,g) = 0$ if and only if $f = g$.

First we show that $d(f,g) = |f(\beta)|$ does not depend on the choice of β. Let β' of g be any root of g and σ be in the Galois group of g over K such that $\sigma(\beta) = \beta'$. As σ is isometric, we have $|f(\beta)| = |\sigma(f(\beta))| = |f(\sigma(\beta))| = |f(\beta')|$, and $d(f,g)$ does not depend on the choice of root of β.

Next we show that $|f(\beta)| = |g(\alpha)|$. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the roots of f and $\beta = \beta_1, \ldots, \beta_n$ be the roots of g, and notice that

$$|f(\beta)|^n = \prod_i |f(\beta_i)| = \prod_{i,j} |\beta_i - \alpha_j|$$

As the last formula is symmetric with respect to f and g, and $|f(\alpha)|, |f(\beta)| \in \mathbb{R}^+$, this gives us that $|f(\beta)| = |g(\alpha)|$. Thus, $|f(\beta)| = |g(\alpha)|$ and $d(f,g) = d(g,f)$.

Now let us fix a root α of f and choose β from the roots of g such that $|\beta - \alpha|$ is minimal. Notice that this distance does not depend on our choice of α. If $|\beta - \alpha_i| \neq |\beta - \alpha|$, then from our choice of β, we have $|\beta - \alpha_i| > |\beta - \alpha|$. Thus, $|\alpha - \alpha_i| = |(\alpha - \beta) + (\beta - \alpha_i)| = |\beta - \alpha_i|$. This gives us our desired formula,

$$d(f,g) = \prod_{i=1}^{n} \{|\beta - \alpha|, |\alpha - \alpha_i|\}.$$

Finally, we show that $d(f,g)$ satisfies the ultrametric inequality. Let $h \in K[x]$ be irreducible and of degree n and assume that γ and γ' are roots of h such that $|\beta - \gamma|$ and $|\alpha - \gamma'|$ are minimal. Then

$$\begin{aligned} d(f,h) &= \prod_{i=1}^{n} \max\{|\alpha - \gamma'|, |\alpha - \alpha_i|\} \leq \prod_{i=1}^{n} \max\{|\alpha - \gamma|, |\alpha - \alpha_i|\} \\ &\leq \prod_{i=1}^{n} \max\{\max\{|\alpha - \beta|, |\beta - \gamma|\}, |\alpha - \alpha_i|\} \\ &\leq \prod_{i=1}^{n} \max\{\max\{|\alpha - \beta|, |\alpha - \alpha_i|\}, \max\{|\beta - \gamma|, |\alpha - \alpha_i|\}\} \\ &\leq \max\{d(f,g), d(g,f)\}. \end{aligned}$$

Thus, $d(f,g)$ is an ultrametric distance with the desired properties. □

We can calculate the distance $d(f,g)$ easily using the following lemma.

Lemma 4.2 ([PR01],Lemma 4.2)**.** *Using the same notation as Proposition* 4.1*, write* $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_0$ *and* $g(x) = x^n + g_{n-1}x^{n-1} + \cdots + g_0$*, and set*

$$w = \min_{0 \le i \le n-1} \left\{ v_\pi(g_i - f_i) + \frac{i}{n} \right\}.$$

Then $d(f, g) = |\pi|^w$*.*

Proof. Notice that

$$g(\alpha) = g(\alpha) - f(\alpha) = \sum_{i=0}^{n} (g_i - f_i)\alpha^i,$$

and since α is a prime element $v_\pi(\alpha) = 1/n$. All of the terms in this sum must then have different valuations, of which $g(\alpha)$ is the minimum. □

4.2 Bounded Sets of Eisenstein Polynomials with Given Invariants

In this section, we will use the various restrictions to generating polynomials provided by choices of invariants to construct finite sets of Eisenstein polynomials.

Throughout this section, we will use the following notation to refer to elements in local field K with π-adic coefficients bounded above and below. Let l, m be two integers with $1 \le l \le m$, let $R_{l,m}$ be a fixed set of representatives of the quotient $(\pi)^l/(\pi)^m$, and let $R_{l,m}^\times$ be the subset of $R_{l,m}$ whose elements have π-adic valuation of exactly l.

4.2.1 Eisenstein Polynomials with a Given Discriminant

Using Lemma 3.2 as a lower bound for coefficient valuations and a bound over which the π-adic coefficients of a generating polynomial are chosen to be 0, we construct a finite set of Eisenstein polynomials. Krasner's bound (Lemma 3.3) gives a specific bound over which the π-adic coefficients of a generating polynomial can be chosen to be 0, while still generating the same extensions, but its proof will be shown as a consequence of Theorem 4.9.

First we define $l(i)$, which gives the minimum valuation for the coefficients of the generating polynomials of extensions with given discriminant, and claim that polynomials satisfying this have a given discriminant. These are effectively a restatement of Lemma 3.2.

Definition 4.3. Let $J_0 = a_0 n + b_0$ satisfy Ore's conditions. For $1 \leq i \leq n-1$ Let

$$l(i) = \begin{cases} \max\{2 + a_0 - v_\pi(i), 1\} & \text{if } i < b_0, \\ \max\{1 + a_0 - v_\pi(i), 1\} & \text{if } i \geq b_0. \end{cases}$$

Lemma 4.4. *An Eisenstein polynomial $\varphi \in \mathcal{O}_K[x]$ has 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 $v_\pi(\varphi_i) \geq l(i)$ and, if $b_0 \neq 0$, $v_\pi(\varphi_{b_0}) = l(b_0)$.*

Next we construct our set of polynomials using $l(i)$ as a lower bound.

Definition 4.5. Let l, m be two integers with $1 \leq l \leq m$, let $R_{l,m}$ be a fixed set of representatives of the quotient $(\pi)^l/(\pi)^m$, and let $R^\times_{l,m}$ be the subset whose elements have π-adic valuation of exactly l. Let $J_0 = a_0 n + b_0$, $c > 1 + 2a_0 + \frac{2b_0}{n}$, and let $\Psi_{n,J_0}(c)$ be the set of all polynomials $\psi(x) = x^n + \sum \psi_i x^i \in \mathcal{O}_K[x]$ with

$$\psi_i \in \begin{cases} R^\times_{1,c} & \text{if } i = 0 \\ R^\times_{l(i),c} & \text{if } i = b_0 \neq 0 \\ R_{l(i),c} & \text{if } 1 \leq i \leq n-1 \text{ and } i \neq b_0 \end{cases}$$

These polynomials satisfy Lemma 4.4 by construction.

Proposition 4.6. *The polynomials in $\Psi_{n,J_0}(c)$ are Eisenstein polynomials of discriminant $(\pi)^{n+J_0-1}$.*

4.2.2 Eisenstein Polynomials with a Given Ramification Polygon

Now let us construct a similar set of Eisenstein polygons given a ramification polygon. Similar to the case of discriminants, we have an analogous function $L_{\mathcal{R}}(i)$ for the lower bounds of the valuation of our coefficients (Definition 3.11). The following is true as a consequence of Proposition 3.14.

Proposition 4.7. *Let l, m be two integers with $1 \leq l \leq m$, let $R_{l,m}$ be a fixed set of representatives of the quotient $(\pi)^l/(\pi)^m$, and let $R^\times_{l,m}$ be the subset whose elements have π-adic valuation of exactly l. For a ramification polygon $\mathcal{R}$ with points $(p^0, J_0), (p^{s_1}, J_1), \ldots, (p^{s_\ell}, J_\ell)$, where $J_i = a_i n + b_i$, let $B_{\mathcal{R}}$ be the set of non-zero b_i. Let $c > 1 + 2a_0 + \frac{2b_0}{n}$, and let $\Psi_{n,J_0,\mathcal{R}}(c)$ be the set of all polynomials*

$\psi(x) = x^n + \sum \psi_i x^i \in \mathcal{O}_K[x]$ *with*

$$\psi_i \in \begin{cases} R_{1,c}^{\times} & \text{if } i = 0 \\ R_{L_{\mathcal{R}}(i),c}^{\times} & \text{if } i \in B_{\mathcal{R}} \\ R_{L_{\mathcal{R}}(i),c} & \text{if } 1 \leq i \leq n-1 \text{ and } i \notin B_{\mathcal{R}} \end{cases}$$

The polynomials in $\Psi_{n,J_0,\mathcal{R}}(c)$ *generate totally ramified extensions of* K *of degree* n*, discriminant* $(\pi)^{n+J_0-1}$*, and ramification polygon* $\mathcal{R}$*.*

4.2.3 Eisenstein Polynomials with Given Residual Polynomials

Finally, we construct a set of Eisenstein generating polynomials for extensions with given degree, discriminant, ramification polygon, and invariant $\mathcal{A}$. This set $\Psi_{n,J_0,\mathcal{R},\mathcal{A}}(c)$ is a subset of $\Psi_{n,J_0,\mathcal{R}}(c)$, so its members have the desired discriminant and ramification polygon, and setting certain residues will give us residual polynomials $(\underline{A}_1, \ldots, \underline{A}_\ell) \in \mathcal{A}$ by construction.

Proposition 4.8. *Let* l, m *be two integers with* $1 \leq l \leq m$*, let* $R_{l,m}$ *be a fixed set of representatives of the quotient* $(\pi)^l/(\pi)^m$*, and let* $R_{l,m}^{\times}$ *be the subset whose elements have* π*-adic valuation of exactly* l*. For a ramification polygon* $\mathcal{R}$ *with points* $(p^0, J_0), (p^{s_1}, J_1), \ldots, (p^{s_\ell}, J_\ell)$*, where* $J_i = a_i n + b_i$*, let* $B_{\mathcal{R}}$ *be the set of non-zero* b_i*. Let* $c > 1 + 2a_0 + \frac{2b_0}{n}$*, and let* $\Psi_{n,J_0,\mathcal{R},\mathcal{A}}(c)$ *be the set of all polynomials* $\psi(x) = x^n + \sum \psi_i x^i \in \mathcal{O}_K[x]$ *with*

$$\psi_i \in \begin{cases} R_{1,c}^{\times} & \text{if } i = 0 \\ R_{L_{\mathcal{R}}(i),c}^{\times} & \text{if } i \in B_{\mathcal{R}} \\ R_{L_{\mathcal{R}}(i),c} & \text{if } 1 \leq i \leq n-1 \text{ and } i \notin B_{\mathcal{R}} \end{cases}$$

and where all $\underline{\varphi}_{i,L_{\mathcal{R}}(i)}$ *for* $i \in B_{\mathcal{R}}$ *are set by the same choice of* $(\underline{A}_1, \ldots, \underline{A}_\ell) \in \mathcal{A}$ *according to Lemma* 3.26*. The polynomials in* $\Psi_{n,J_0,\mathcal{R},\mathcal{A}}(c)$ *generate totally ramified extensions of* K *of degree* n*, discriminant* $(\pi)^{n+J_0-1}$*, ramification polygon* $\mathcal{R}$*, and invariant* $\mathcal{A}$*.*

4.3 A Generalization of Krasner's Mass Formula

Now we extend Krasner's results to the cases where we have chosen additional invariants. In order to do this generically, let X be a set of invariants of a totally ramified extension over K minimally containing a degree n and discriminant $(\pi)^{n+J_0-1}$.

Let $\mathbf{K}_X$ denote the set of totally ramified extensions over K with invariants X and $\mathbf{E}_X$ denote the set of Eisenstein polynomials in $K[x]$ generating extensions with invariants X. The roots of the polynomials in $\mathbf{E}_X$ generate all extensions in $\mathbf{K}_X$. Let $c > 1 + (2J_0)/n$ and $\Psi_X(c)$ be the set of all Eisenstein polynomials with coefficients in $R_{1,c}$ whose roots generate totally ramified extensions with invariants X.

Theorem 4.9 (Krasner)**.** *The set $\mathbf{E}_{n,J_0}$ of Eisenstein polynomials of degree n and discriminant $(\pi)^{n+J_0-1}$ over K is the disjoint union of the closed discs $D_{\mathbf{E}_{n,J_0}}(\psi, r)$ with centers $\psi \in \Psi_{n,J_0}(c)$ and radius $r = |\mathfrak{p}^c|$.*

Proof. In Proposition 4.6, we showed that polynomials $\psi \in \Psi_{n,J_0}(c)$ are, in fact, elements of $\mathbf{E}_{n,J_0}$. Let $\psi = \sum_{i=0}^{n} \psi_i x^i$ and $\psi' = \sum_{i=0}^{n} \psi'_i x^i$ be distinct elements of $\Psi_{n,J_0}(c)$, and i be such that $\psi_i \neq \psi'_i$.

$$v_\pi(\psi_i - \psi'_i) + \frac{i}{n} < c - 1 + \frac{i}{n} < c$$

and by Lemma 4.2, $d(\psi, \psi') > r$. Therefore, by the ultrametric property of d, we have that the discs D_ψ and $D_{\psi'}$ are disjoint.

Next, let $f \in \mathbf{E}_{n,J_0}$ with $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_0$. Let $J_0 = a_0 n + b_0$. As f is Eisenstein, $v_\pi(f_0) = 1$ and there exists $\psi_0 \in R^\times_{1,c}$ such that $f_0 \equiv \psi_0 \mod \mathfrak{p}^c$. If $b_0 \neq 0$, then we have that $v_\pi(f_{b_0}) = l(b_0)$, so there is $\psi_{b_0} \in R^\times_{l(b_0),c}$ such that $f_{b_0} \equiv \psi_{b_0} \mod \mathfrak{p}^c$. For all $1 \leq i \leq n-1$ with $i \neq b_0$, $v_\pi(f_i) \geq l(i)$, so there is $\psi_i \in R_{l(i),c}$ such that $f_i \equiv \psi_i \mod \mathfrak{p}^c$. We claim that $f \in D_{\mathbf{E}_{n,J_0}}(\psi, r)$ with $\psi = \sum \psi_i x^i$ and $r = |\mathfrak{p}^c|$. By our choices of ψ_i, we have that $v_\pi(f_i - \psi_i) \geq c$ for $i = 0, \ldots, n-1$. Therefore, for all i,

$$v_\pi(f_i - \psi_i) + \frac{i}{n} \geq c$$

which, by Lemma 4.2, proves our claim. □

Krasner's bound (Lemma 3.3) is a direct consequence of the following corollary.

Corollary 4.10. *Let f be an Eisenstein polynomial of degree n and discriminant $\mathfrak{p}^{n+J_0-1}$ over K and write $f(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_0$. Let $g(x) = x^n + g_{n-1}x^{n-1} + \cdots + g_0$ be a polynomial such that $g_i \equiv f_i \mod \mathfrak{p}^c$. Let α be a root of f and β a root of g such that $|\beta - \alpha|$ is minimal. Then $\alpha \in K(\beta)$.*

Proof. First we observe that $v_\pi(g_i) = v_\pi(f_i)$ and so by Lemma 3.8, g is also an Eisenstein polynomial with discriminant $\mathfrak{p}^{n+J_0-1}$.

Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ denote the roots of f and let Δf be the minimal distance between α and any other root of f. Then, since the α_i are prime elements,

$$|f'(\alpha)| = \prod_{i=2}^{n} |\alpha - \alpha_i| \leq \Delta f \cdot |\mathfrak{p}^{(n-2)/n}|.$$

However, $|f'(\alpha)| = |\mathfrak{p}^{(n+J_0-1)/n}|$, and so $\Delta f \geq |\mathfrak{p}^{(J_0+1)/n}|$.

Now, by Theorem 4.9, we have that $d(f,g) \leq r = |\mathfrak{p}^c|$. We claim that $|\beta - \alpha| < \Delta f$, as otherwise

$$\begin{aligned} d(f,g) &= \prod_{i=1}^{n} \max\{|\beta - \alpha|, |\alpha - \alpha_i|\} \geq \prod_{i=1}^{n} \max\{\Delta f, |\alpha - \alpha_i|\} \\ &\geq \Delta f \prod_{i=2}^{n} |\alpha - \alpha_i| = \Delta f |f'(\alpha)| \geq |\mathfrak{p}^{(n+2J_0)/n}|, \end{aligned}$$

which contradicts $d(f,g) \leq r = |\mathfrak{p}^c|$, by the particular choice of c. Thus, $|\beta - \alpha| < \Delta f$, and by Krasner's Lemma (Theorem 1.2) we have that $\alpha \in K(\beta)$. □

The following is simply a result of the fact that $\mathbf{E}_X \subseteq \mathbf{E}_{n,J_0}$ and $D_{\mathbf{E}_X}(r) \subseteq D_{\mathbf{E}_{n,J_0}}(r)$.

Corollary 4.11. *The set $\mathbf{E}_X$ is the disjoint union of the closed discs $D_{\mathbf{E}_X}(\psi, r)$ with centers $\psi \in \Psi_X(c)$ and radius $r = |\mathfrak{p}^c|$.*

Lemma 4.12. *Let X be a set of invariants of a totally ramified extension over K containing degree n and discriminant $(\pi)^{n+J_0-1}$. Let $c > 1 + 2a_0 + \frac{2b_0}{n}$ and let $\#D_{\mathbf{E}_X}(r)$ denote the number of disjoint*

closed discs of radius $r = |\pi^c|$ *in* $\mathbf{E}_X$. *Then the number of elements in* $\mathbf{K}_X$ *is*

$$\#\mathbf{K}_X = \#D_{\mathbf{E}_X}(r)\frac{n}{(q-1)q^{nc-(n+J_0-1)-2}}$$

Proof. Let Π_X denote the set of all prime elements of members of $\mathbf{K}_X$. Π_X can be differently defined as the union of sets $\mathfrak{p}_L \setminus \mathfrak{p}_L^2$ where $\mathfrak{p}_L$ is the prime ideal of some member L of $\mathbf{K}_X$. Let χ be the map that sends a prime element in Π_X to its minimal polynomial in $\mathbf{E}_X$.

Let $t > J_0 + 1$ be an integer and let $s = |\pi^{(n+j_0-1+t)/n}|$. Let $u = |\pi^t|^{1/n}$, and let $\alpha, \beta \in \Pi_X$ such that $|\alpha - \beta| \leq u$. By Krasner's Lemma, α and β generate the same field. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ denote the roots of $\chi(\alpha)$. Then

$$\begin{aligned} d(\chi(\alpha), \chi(\beta)) &= \prod_{i=1}^{n} \max\{|\beta - \alpha|, |\alpha - \alpha_i|\} \\ &\leq u \prod_{i=2}^{n} |\alpha - \alpha_i| = u|(\chi(\alpha))'(\alpha)| = u|\pi^{(n+j-1)/n}| = s \end{aligned}$$

Let $D_\Pi(\alpha, u)$ denote the closed disc of center α and radius u in Π_X. As $d(\chi(\alpha), \chi(\beta)) \leq s$, we have $\chi(D_\Pi(\alpha, u)) \subset D_{\mathbf{E}_X}(\chi(\alpha), s)$. Conversely, let $f, g \in \mathbf{E}_X$ such that $d(f, g) \leq s$. Let α be a root of f so $f = \chi(\alpha)$ and β be the root of g such that $|\beta - \alpha|$ is minimal. We claim that $|\beta - \alpha| < u$, as otherwise

$$\begin{aligned} d(f, g) &= \prod_{i=1}^{n} \max\{|\beta - \alpha|, |\alpha - \alpha_i|\} \geq \prod_{i=1}^{n} \max\{u, |\alpha - \alpha_i|\} \\ &\geq u \prod_{i=1}^{n} |\alpha - \alpha_i| = u|f'(\alpha)| = u|\pi^{(n+j-1)/n}| = s, \end{aligned}$$

which contradicts the assumption that $d(f, g) < s$. As $|\beta - \alpha| < u$, we have $D_{\mathbf{E}_X}(\chi(\alpha), s) \subset \chi(D_\Pi(\alpha, u))$. So, for all $\alpha \in \Pi_X$,

$$D_{\mathbf{E}_X}(\chi(\alpha), s) = \chi(D_\Pi(\alpha, u)).$$

It is clear that the map χ is n-to-one and surjective. Now, the inverse image of $\chi(\alpha)$ is the set of conjugates of α over K. As $t > j+1$, the closed discs of radius u centered at these conjugates are all disjoint. Thus, the inverse image of any closed disc of radius s in $\mathbf{E}_X$ is the disjoint union of n closed discs of radius u in Π_X. However, by the earlier remark, any such disc is contained in $\mathfrak{p}_L \setminus \mathfrak{p}_L^2$ for some $L \in \mathbf{K}_X$. Therefore, the number of disjoint closed discs of radius u in Π_X is equal to $\#\mathbf{K}_X$ times the number of disjoint closed discs in $\mathfrak{p}_L \setminus \mathfrak{p}_L^2$, which does not depend on L and is $q^{t-1} - q^{t-2}$. Thus,

$$\#\mathbf{K}_X \; q^{t-2}(q-1) = n \; \#D_{\mathbf{E}_X}(s),$$

and choosing $t = nc - (n + J_0 - 1)$ gives us our result. □

4.4 Mass Formula Given a Discriminant (Krasner)

Proposition 4.13. *Let Ψ_{n,J_0} be the set of polynomials over K with degree n and discriminant $(\pi)^{n+J_0-1}$ whose coefficients are in $R_{1,c}$. The number of polynomials in Ψ_{n,J_0} is*

$$\#\mathbf{D}_{E_{n,J_0}}(c) = \begin{cases} (q-1)\, q^{c-2+(n-1)c-\sum_{i=1}^{n-1} l(i)} & \text{for } b = 0 \\ (q-1)^2\, q^{c-2+(n-1)c-\sum_{i=1}^{n-1} l(i)-1} & \text{for } b > 0 \end{cases}$$

Proposition 4.14. *The number of distinct totally ramified extensions of K of degree n and discriminant $(\pi)^{n+J_0-1}$ is*

$$\#\mathbf{K}_{n,J_0} = \begin{cases} n\, q^{n+J_0-1-\sum_{i=1}^{n-1} l(i)} & \text{for } b = 0 \\ n\,(q-1)\, q^{n+J_0-1-\sum_{i=1}^{n-1} l(i)-1} & \text{for } b > 0 \end{cases}$$

Example 4.15. As an example, let us count all totally ramified extensions of $\mathbb{Q}_3$ with degree 9 and discriminant $(3)^{9+7-1}$. From this discriminant, we have $J_0 = 7$. We find minima for the $v_\pi(\varphi_i)$ if φ

is to be an Eisenstein polynomial of this discriminant. By Lemma 3.2,

$$l(i) = v_\pi(\varphi_i) \geq \begin{cases} 2 & \text{for } i \in \{1,2,4,5\} \\ 1 & \text{for } i \in \{3,6,7,8\} \end{cases}$$

So, $\sum l(i) = 12$, and from the formula, we find that there are $9 \cdot 2 \cdot 3^{9+7-1-12-1} = 162$ degree 9 extensions of $\mathbb{Q}_3$ with discriminant $(3)^{9+7-1}$.

4.5 Mass Formula Given a Ramification Polygon

Proposition 4.16. *Let $\Psi_{n,J_0,\mathcal{R}}(c)$ be the set of Eisenstein polynomials with degree n, discriminant $(\pi)^{n+J_0-1}$, and ramification polygon $\mathcal{R}$ with coefficients whose coefficients above c are zero (see Lemma 3.3). Then*

$$\#\Psi_{n,J_0,\mathcal{R}}(c) = (q-1)^{\#B_\mathcal{R}+1}\, q^{c-2+(n-1)c-\sum_{i=1}^{n-1} L(i)-\#B_\mathcal{R}}$$

Proof. The number of elements in $R^*_{1,c}$ is $(q-1)\,q^{c-2}$. For each $i \notin B_\mathcal{R}$, the number of elements in $R_{L_\mathcal{R}(i),c}$ is $q^{c-L(i)}$, and for $i \in B_\mathcal{R}$ the number in $R^*_{L_\mathcal{R}(i),c}$ is $(q-1)q^{c-L(i)-1}$. The product of these is our result. □

Proposition 4.17. *The number of distinct totally ramified extensions of K of degree n, discriminant $(\pi)^{n+J_0-1}$, and ramification polygon $\mathcal{R}$ is*

$$n(q-1)^{\#B_\mathcal{R}}\, q^{n+J_0-1-\sum_{i=1}^{n-1} L(i)-\#B_\mathcal{R}}$$

Proof.

$$\frac{n\,\#\mathbf{D}_{E_{n,J_0,\mathcal{R}}}(c)}{(q-1)q^{nc-(n+J_0-1)-2}} = n(q-1)^{\#B_\mathcal{R}}\, q^{n+J_0-1-\sum_{i=0}^{n-1} L(i)-\#B_\mathcal{R}}$$ □

Example 4.18 (Example 4.15 continued)**.** Now let us count all totally ramified extensions of $\mathbb{Q}_3$ with degree 9 and discriminant $(3)^{9+7-1}$ where we make a choice of ramification polygon. Again,

we have $J_0 = 7$ and

$$l_{\mathcal{R}}(i,0) = l(i) = \begin{cases} 2 & \text{for } i \in \{1,2,4,5\} \\ 1 & \text{for } i \in \{3,6,7,8\} \end{cases}$$

There are two possible ramification polygons for this degree and discriminant: $\mathcal{R}_1$ with vertices $\{(1,7),(9,0)\}$ and $\mathcal{R}_2$ with vertices $\{(1,7),(3,3),(9,0)\}$. We have already considered the conditions on the polynomial dictated by the vertex $(1,7)$, so it only remains to consider the effect of a vertex (or lack thereof) above 3.

For $\mathcal{R}_1$, no vertex above 3 means $l_{\mathcal{R}_1}(3,1) = 2$ and $l_{\mathcal{R}_1}(6,1) = 1$. For an Eisenstein polynomial to have ramification polynomial $\mathcal{R}_1$, the minimum valuations of the coefficients would have to be

$$L_{\mathcal{R}_1}(i) = \max_s\{l_{\mathcal{R}_1}(i,s)\} = \begin{cases} 2 & \text{for } i \in \{1,2,3,4,5\} \\ 1 & \text{for } i \in \{6,7,8\} \end{cases}.$$

So, $\sum L_{\mathcal{R}_1}(i) = 13$. Next we consider the set of fixed valuations of an Eisenstein polynomial generating such an extension and find that

$$B_{\mathcal{R}_1} = \{J_i \bmod n : 0 \le i \le s_\ell \text{ and } J_i \bmod n \neq 0\} = \{7\}$$

The number of fixed valuations is$\#B_{\mathcal{R}_1} = 1$. Thus, by applying the formula, we find that there are $9 \cdot 2^1 \cdot 3^{9+7-1-13-1} = 54$ degree 9 extensions of $\mathbb{Q}_3$ with ramification polygon $\mathcal{R}_1$.

For $\mathcal{R}_2$, the vertex $(3,3)$ gives us that $l_{\mathcal{R}_2}(3,1) = 1$ and $l_{\mathcal{R}_2}(6,1) = 1$. For an Eisenstein polynomial to have ramification polynomial $\mathcal{R}_2$, the minimum valuations of the coefficients would have to be

$$L_{\mathcal{R}_2}(i) = \max_s\{l_{\mathcal{R}_2}(i,s)\} = \begin{cases} 2 & \text{for } i \in \{1,2,4,5\} \\ 1 & \text{for } i \in \{3,6,7,8\} \end{cases}.$$

So, $\sum L_{\mathcal{R}_2}(i) = 12$. Next we consider the set of fixed valuations of an Eisenstein polynomial generating such an extension and find that

$$B_{\mathcal{R}_2} = \{J_i \bmod n : 0 \le i \le s_\ell \text{ and } J_i \bmod n \neq 0\} = \{3, 7\}$$

The number of fixed valuations is $\#B_{\mathcal{R}_2} = 2$. Thus, by applying the formula, we find that there are $9 \cdot 2^2 \cdot 3^{9+7-1-12-2} = 108$ degree 9 extensions of $\mathbb{Q}_3$ with ramification polygon $\mathcal{R}_2$.

Krasner's mass formula states that there are 162 totally ramified extensions of $\mathbb{Q}_3$ with degree 9, which we have partitioned by the two possible ramification polygons.

4.6 Mass Formula Given Residual Polynomials

Proposition 4.19. *The number of Eisenstein polynomials of degree n, with given discriminant $(\pi)^{n+J_0-1}$, ramification polygon $\mathcal{R}$, and invariant $\mathcal{A}$ with coefficients whose coefficients above c are zero (see Lemma 3.3) is*

$$(\#\mathcal{A})\,(q-1)\,q^{c-2+(n-1)c-\sum_{i=1}^{n-1} L_{\mathcal{R}}(i)-\#B_{\mathcal{R}}}$$

Proof. The choice of $\mathcal{A}$ does not change the constant term, so for that coefficient we have the number of elements in $R^*_{1,c}$, which is $(q-1)\,q^{c-2}$. For each $i \notin B_{\mathcal{R}}$, we have the number of elements in $R_{L_{\mathcal{R}}(i),c}$, which is $q^{c-L(i)}$. For $i \in B_{\mathcal{R}}$, the choice of $(\underline{A}_1, \ldots, \underline{A}_\ell) \in \mathcal{A}$, fixes the first non-zero coefficient of our coefficients. The number of elements in $R^*_{L_{\mathcal{R}}(i),c}$ with a fixed first non-zero coefficient is $q^{c-L(i)-1}$. We have $\#\mathcal{A}$ ways to fix those coefficients, and the product of these is our result. □

Proposition 4.20. *The number of distinct totally ramified extensions of K of degree n, discriminant $(\pi)^{n+J_0-1}$, ramification polygon $\mathcal{R}$, and invariant $\mathcal{A}$ is*

$$n\,(\#\mathcal{A})\,q^{n+J_0-1-\sum_{i=1}^{n-1} L_{\mathcal{R}}(i)-\#B_{\mathcal{R}}}$$

Example 4.21 (Example 4.18 continued)**.** As an example, let us count all totally ramified extensions of $\mathbb{Q}_3$ with degree 9, discriminant $(3)^{9+7-1}$, and ramification polygon $\mathcal{R}_2 = \{(1,7),(3,3),(9,0)\}$

As before, for an Eisenstein polynomial to have ramification polynomial $\mathcal{R}_2$, the minimum valuations of the coefficients would have to be

$$L_{\mathcal{R}_2}(i) = \max_s\{l_{\mathcal{R}_2}(i,s)\} = \begin{cases} 2 & \text{for } i \in \{1,2,4,5\} \\ 1 & \text{for } i \in \{3,6,7,8\} \end{cases}.$$

So, $\sum L_{\mathcal{R}_2}(i) = 12$ and the number of fixed valuations is $\#B_{\mathcal{R}_2} = 2$.

There are four possible sets of residual polynomials of segments $(\underline{A}_1, \underline{A}_2)$ for extensions with ramification polygon $\mathcal{R}_2$, belonging to two invariants $\mathcal{A}$:

$$\mathcal{A}_1 = \{(x^2+1, x^3+1), (2x^2+2, x^3+2)\} \text{ and } \mathcal{A}_2 = \{(x^2+2, x^3+1), (2x^2+1, x^3+2)\}.$$

Each of these invariants contain two polynomials, so by applying the formula, we find that there are $9 \cdot 2 \cdot 3^{9+7-1-12-2} = 54$ degree 9 extensions of $\mathbb{Q}_3$ with ramification polygon $\mathcal{R}_2$ and a choice of $\mathcal{A}$. This partitions the 108 extensions of degree 9 with $\mathcal{R}_2$.

4.7 Examples

In Table 2, we show the number of extensions of degree 9 over $\mathbb{Q}_3$ with given invariants. For discriminants $(3)^{9+J_0-1}$ with $J_0 \leq 12$, we list all possible ramification polygons, as generated by Algorithm 1, all residual polynomials, as generated by Algorithm 2, and how many extensions exist with each set of invariants.

Additional examples for different base fields and degrees with all possible discriminants can be found at

`http://www.uncg.edu/mat/numbertheory/tables/local/counting/`.

Table 2. Number of extensions of degree 9 for all possible ramification polygons and residual polynomials over $\mathbb{Q}_3$ with discriminant $(3)^{9+J_0-1}$ for $J_0 \leq 12$.

J_0	Ramification Polygon	Representative of $\mathcal{A}$	$\#\mathcal{A}$	Extensions		
1	$\{(1,1),(9,0)\}$	$(z+1)$	2	18	18	18
2	$\{(1,2),(9,0)\}$	(z^2+1)	1	9	18	18
		(z^2+2)	1	9		
4	$\{(1,4),(9,0)\}$	(z^4+1)	1	9	18	54
		(z^4+2)	1	9		
	$\{(1,4),(3,3),(9,0)\}$	(z^4+z+1)	2	18	36	
		(z^4+z+2)	2	18		
5	$\{(1,5),(9,0)\}$	$(z+1)$	2	18	18	54
	$\{(1,5),(3,3),(9,0)\}$	(z^2+1,z^3+1)	2	18	36	
		$(2z^2+1,z^3+2)$	2	18		
7	$\{(1,7),(9,0)\}$	$(z+1)$	2	54	54	162
	$\{(1,7),(3,3),(9,0)\}$	(z^2+1,z^3+1)	2	54	108	
		$(2z^2+1,z^3+2)$	2	54		
8	$\{(1,8),(9,0)\}$	(z^8+1)	1	9	18	162
		(z^8+2)	1	9		
	$\{(1,8),(3,3),(9,0)\}$	$(z+1,z^3+1)$	2	54	108	
		$(z+2,z^3+1)$	2	54		
	$\{(1,8),(3,6),(9,0)\}$	(z^8+z^2+1)	1	9	36	
		(z^8+2z^2+1)	1	9		
		(z^8+z^2+2)	1	9		
		(z^8+2z^2+2)	1	9		
10	$\{(1,10),(9,0)\}$	(z^2+1)	1	27	54	486
		(z^2+2)	1	27		
	$\{(1,10),(3,3),(9,0)\}$	$(z+1,z^3+1)$	2	162	324	
		$(z+2,z^3+1)$	2	162		
	$\{(1,10),(3,6),(9,0)\}$	(z^2+1,z^6+1)	1	27	108	
		$(2z^2+1,z^6+2)$	1	27		
		(z^2+2,z^6+1)	1	27		
		$(2z^2+2,z^6+2)$	1	27		
11	$\{(1,11),(9,0)\}$	$(z+1)$	2	54	54	486
	$\{(1,11),(3,3),(9,0)\}$	(z^2+1,z^3+1)	2	162	324	
		$(2z^2+1,z^3+2)$	2	162		
	$\{(1,11),(3,6),(9,0)\}$	$(z+1,z^6+1)$	2	54	108	
		$(2z+1,z^6+2)$	2	54		
12	$\{(1,12),(3,3),(9,0)\}$	$(2z+1,z^3+2)$	1	243	486	486
		$(z+2,z^3+1)$	1	243		

CHAPTER V

ENUMERATING EXTENSIONS WITH GIVEN INVARIANTS

As we have seen, Krasner's method of counting extensions [Kra66] and our generalization in Chapter IV construct a finite set of Eisenstein polynomials which generate all totally ramified extensions with given invariants. Pauli and Roblot [PR01] presented an algorithm that returned a set of generating polynomials for all extensions of a given degree and discriminant, following Krasner's approach. They used the root-finding algorithm described by Panayi [Pan95] to obtain one generating polynomial for each extension. A recent paper by Monge [Mon14] provides a new method for determining whether two polynomials generate the same extension and introduces *reduced polynomials* that yield a canonical set of generators for totally ramified extensions of K. Monge's methods 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.

In this chapter, 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.

While our algorithm only generates totally ramified extensions, it can be used to enumerate in the general case. As any finite extension L/K can be uniquely split into a tower $L/L^{ur}/K$ where L/L^{ur} is totally ramified and L^{ur}/K is unramified, general enumeration can be achieved by enumerating over suitable unramified extensions. More details can be found in [PR01, Section 2].

5.1 Residual Polynomials of Components

We now apply some results of Monge [Mon14] 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 $\lambda \in \mathbb{Q}$, the λ-component of $\mathcal{N}$ is

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

Remark. 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 5.2. 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 $\operatorname{cont}_\alpha\big(\rho(\alpha^\lambda z)\big)$ denotes the highest power of α dividing all coefficients of $\rho(\alpha^\lambda z)$.

The quantity $\operatorname{cont}_\alpha(\rho(\alpha^m z))$ 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

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

for the Hasse-Herbrand function $\phi_{\mathcal{R}}$ of $\mathcal{R}$ (Definition 3.15). Thus [Mon14, Proposition 1] yields

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

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 3.6 (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 3.15.

Lemma 5.3. *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 5.1 the component $\mathcal{R}_{(-m)}$ contains $\mathcal{S}$ and by Remark 3.19((a)) $\underline{S}_m(x) = x^k \underline{A}(x)$.

(b) As mentioned in Remark 5.1 $\mathcal{N}_{(-m)}$ and $\mathcal{R}$ only have one point in common. By Lemma 3.6 this point is of the form $(p^s, v(\rho_{p^s}))$. It follows from Lemma 3.6 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 3.6 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 [Mon14, Lemma 3]).

Proposition 5.4. *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 $\varphi_j - \psi_j = \alpha^n \rho(\gamma\alpha^m)$*

(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 3.5 we have

$$\sum_{i=0}^{n-1}(\varphi_i - \psi_i)\beta^i = \varphi(\beta) - \psi(\beta) = \varphi(\beta) = \alpha^n\rho(\beta/\alpha - 1) = \alpha^n\rho(\gamma\alpha^m). \tag{5.1}$$

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 $\varphi_j - \psi_j = \alpha^n\rho(\gamma\alpha^m)$.

(b) Dividing Equation (5.1) by $\alpha^n \operatorname{cont}_\alpha(\rho(\alpha^m x))$ yields

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

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. □

5.1.1 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 5.5. *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 5.5.

Lemma 5.6. *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 5.7 (Example 3.29 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 $\varphi_{6,1} = 0$, $\varphi_{0,2} = 0$, and $\varphi_{3,2} = 0$. Furthermore $\underline{S}_m = x$ for with $9\phi(m) = 10 + m$ for $m \geq 4$. Thus by Lemma 5.6 we can set $\varphi_{k,j} = 0$ 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 $\mathcal{A}_{2,1}^{*1}$.

5.2 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 `AllExtensionsSub`

Input: A π-adic field K, a convex polygon $\mathcal{R}$ with points $(1, a_0n + b_0)$, $(p^{s_1}, a_1n + b_1)$,...,$(p^{s_u}, a_un + b_u) = (p^{s_u}, 0)$,...,$(n, 0)$ satisfying Proposition 3.13 where $0 \le b_i < n$ for $1 \le i \le u = v_p(n)$, $\mathcal{S}_1, \dots, \mathcal{S}_\ell$ the segments of $\mathcal{R}$, a representative $\underline{\delta}_0$ of a class in $\underline{K}^\times/(\underline{K}^\times)^n$, and $\underline{A}_1, \dots, \underline{A}_\ell \in \underline{K}[x]$ satisfying Proposition 3.22.

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 $\underline{A}_1, \dots, \underline{A}_\ell$.

(a) $c \leftarrow \left\lceil 1 + 2a_0 + \frac{2b_0}{n} \right\rceil - 1$ [Lemma 3.3]

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

(c) For $0 \le i \le n-1$ and $L_{\mathcal{R}}(i) \le j \le c$: [Definition 3.11]

- 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 $1 \le m \le \left\lfloor \frac{(a_1n+b1)-(a_0n+b_0)}{p^{s_1}-1} \right\rfloor$:

- $i \leftarrow n\phi_{\mathcal{R}}(m) \bmod n$, $j \leftarrow \frac{n-i+n\phi_{\mathcal{R}}(m)}{n}$
- $\tau_{i,j} \leftarrow R$ where R is a set of representatives of $\underline{K}/\underline{S}_m(\underline{K})$. [Lemma 5.6]

(e) For $1 \le i \le u$:

- Find a segment $\mathcal{S}_t$ of $\mathcal{R}$ such that $(p^{s_i}, a_in + b_i)$ is on $\mathcal{S}_t$.
- $j \leftarrow a_i + 1 - v_\pi\binom{b_i}{p^{s_i}}$
- $\tau_{b_i,j} \leftarrow \left\{ \underline{A}_{t,(p^{s_i}-p^{s_k})/e}(-\underline{\delta}_0)^{a_i+1}\binom{b_i}{p^{s_i}}^{-1}\pi^{v_\pi\binom{b_i}{p^{s_i}}} \right\}$. [Lemma 3.26]
  where $(p^{s_k}, a_kn + b_k)$ 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 3.27]

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

Algorithm 3. `AllExtensionsSub`

As is evident from the following example Algorithm 3 may return more than one generating polynomial for some extensions.

Example 5.8. 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 $m \ge 3$ 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 $\varphi_{3,2} = 0$. As $\underline{S}_m$ for $m \ge 3$ we can set $\varphi_{k,j} = 0$

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 $\varphi_{0,2}$. Thus Algorithm 3 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	$\{0\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$
3^3	$\{0\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$
3^2	$\{0\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{\mathbf{0}\}$	$\{0\}$	$\{\mathbf{0}\}$	$\{0,1,2\}$	$\{\mathbf{2}\}$	$\{\mathbf{0},\mathbf{1},\mathbf{2}\}$
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 $\varphi_{c,d} = x^9+6x^6+9c\cdot x^2+18x+3+9d$ $(c,d \in \{1,2\})$ 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 5.4 (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 $\varphi_d = x^9 + 6x^6 + 18x + 3 + 9d$ where $(d \in \{1,2\})$.

Theorem 5.9. *Let F be the set of polynomials returned by Algorithm 3 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 3 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 3.14, φ has ramification polygon $\mathcal{R}$. By Lemma 3.26, 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 5.6. 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 5.4, 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 3 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 5.6. 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) computing all reduced generating polynomials using [Mon14, Algorithm 3] and comparing these or

(b) using a root finding algorithm (compare [PR01]).

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

([Mon14, Theorem 1]). Alternatively the number extensions generated by each polynomial can be computed using root finding.

5.2.1 Enumerating Extensions of Given Ramification Polygon and Invariant $\mathcal{A}$

Now we present an algorithm to enumerate all extensions with a given invariants. It may require multiple calls to Algorithm 3 `AllExtensionsSub` depending the structure of $\mathcal{A}$ and the number of tame subextensions.

Algorithm `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 (3.4).

  (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. 3]
  - Unless avoidable by Theorem 5.9, filter F' so that no two polynomials generate the same extension using method of choice.
  - $F \leftarrow F \cup F'$.

(c) Return F.

Algorithm 4. `AllExtensions`

Theorem 5.10. *Let F be the set of polynomials returned by Algorithm 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 3.28, 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 5.9, 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 3 generate the same extension. Let φ and ψ be in two such polynomials. By Lemma 3.27, 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 3.4.2, 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 3 with different inputs of δ or residual polynomials returned by Algorithm 4, they cannot generate the same extension. □

5.2.2 Enumerating Extensions of Given Degree and Discriminant

We generalize our enumeration process with an algorithm to enumerate all extensions with a given degree and discriminant, which calls all of our previous enumeration algorithms.

Algorithm `AllExtensionsDisc`

Input: A π-adic field K, a degree $n = e_0 p^r$, and J_0 satisfying Ore's Conditions

Output: A set F that contains one generating Eisenstein polynomial for each totally ramified extension of K of degree n and discriminant of valuation $n + J_0 - 1$.

(a) $S_0 \leftarrow$ a set of representatives of $\underline{K}^\times/(\underline{K}^\times)^n$.

(b) $F \leftarrow \{\}$

(c) $\mathcal{P} \leftarrow \{(1, J_0), (n, 0), (p^r, 0)\} \cup \{(i, 0) \mid p^r < i < n \text{ and } v_p\binom{n}{i} = 0\}$.

(d) $V(i) \leftarrow l(i, 0)$ for $1 \leq i \leq n$.

(e) For $\mathcal{R}$ in `AllRamificationPolygons`$(K, \mathcal{P}, r-1, V(i))$ do [Alg. 1]

- For $\delta \in S_0$ do
  - (i) $P \leftarrow$ `AllResidualPolynomials`$(K, \mathcal{R}, \delta)$. [Alg. 2]
  - (ii) Partition P into disjoint sets $\mathcal{A}^{*1}, \ldots, \mathcal{A}^{*k}$ by Equation (3.4).
  - (iii) 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. 3]
    - Unless avoidable by Theorem 5.9, filter F' so that no two polynomials generate the same extension using method of choice.
    - $F \leftarrow F \cup F'$.

(f) Return F.

Algorithm 5. `AllExtensionsDisc`

Theorem 5.11. *Let K be a π-adic field, $n = e_0 p^r \in \mathbb{Z}^{>0}$ and J_0 satisfying Ore's Conditions. Let F be the set of polynomials returned by Algorithm 5. For each extension L/K of discriminant $(\pi)^{n+J_0-1}$ the set F contains exactly one generating polynomial.*

Proof. Let L/K be a totally ramified extension of degree $n = e_0 p^r \in \mathbb{Z}^{>0}$ and discriminant $(\pi)^{n+J_0-1}$. Let $\psi \in \mathcal{O}_K[x]$ be an Eisenstein polynomial generating L with $\psi_{0,1} \in S_0$. We know such a polynomial exists by Lemma 3.27. The ramification polygon of L/K must satisfy the conditions of Proposition 3.13, so $\mathcal{R}_\psi$ is generated by Algorithm 1. Let $A^{(\psi)}$ be the residual polynomials of segments of $\mathcal{R}_\psi$. As $A^{(\psi)}$ satisfies the conditions of Proposition 3.22, it must be generated by Algorithm 2. $A^{(\psi)}$ belongs to some $\mathcal{A}^*$ in our partition of P. If A is our choice of representative of $\mathcal{A}^*$, then by Lemma 3.28, 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 $\mathcal{R}_\psi$, residual polynomials A, and $\varphi_{0,1} = \psi_{0,1}$, and by Theorem 5.9, 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 3 generate the same extension. Let φ and ψ be in two such polynomials. If $\mathcal{R}_\varphi \neq \mathcal{R}_\psi$, then they cannot generate the same extension. So suppose $\mathcal{R}_\varphi = \mathcal{R}_\psi$. By Lemma 3.27, 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 $\varphi_{0,1} = \psi_{0,1}$ and that $K[x]/(\psi)$ and $K[x]/(\varphi)$ have the same invariant $\mathcal{A}$. By Remark 3.4.2, 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 3 with different input of ramification polygon, δ, or residual polynomials in the process of Algorithm 5, they cannot generate the same extension. □

5.3 Examples

In Figure 4 we compare the implementation of the algorithm from [PR01] in Magma [BCP97] (`AllExtensions`) and Pari [PG14] (`padicfields`) with our implementation of Algorithm 5 in Magma using root finding to filter the set of polynomials to obtain a minimal set. In the implementation of the method from [PR01] Magma we replaced the deterministic enumeration of polynomials by random choices, which yields a considerable performance improvement. In our implementation of

Algorithm 5 the filtering out of redundant polynomials can accelerated by using reduction [Mon14] instead of root finding.

K	n	$v(\mathrm{disc})$	$\#F$	Magma [PR01]	Pari [PR01]	Magma (Alg. 5)
$\mathbb{Q}_3$	9	9	2	10 ms	37 ms	10 ms
$\mathbb{Q}_3$	9	22	96	67 s	11 s	30 ms + 5.77 s†
$\mathbb{Q}_3$	9	26	81	16.61 s	3.64 s	0.05 s
$\mathbb{Q}_3$	27	27	2	30 ms	56 h	10 ms
$\mathbb{Q}_3$	27	107	1,594,323	>5 days	—	17 min

Figure 4. Time needed to compute a minimal set F of generating polynomials of all extensions of K of degree n with discriminant exponent $v(\mathrm{disc})$. All timings were obtained on a computer with a Intel Core 2 Quad CPU at 2.83GHz and 8Gb RAM running Ubuntu Linux 14.04 LTS. († time required to filter output of Alg. 3)

We now present generating polynomials for totally ramified extensions of degree 15 over $\mathbb{Q}_5$ (Example 5.12), totally ramified extensions of degree 8 over an unramified extension of degree 2 over $\mathbb{Q}_2$ (Example 5.13), totally ramified extensions of degree 9 over a ramified extension of $\mathbb{Q}_3$ of degree 3 (Example 5.14), 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 5.15).

Example 5.12. We find generating polynomials for all totally ramified extensions L of $\mathbb{Q}_5$ of degree 15 with $v_5(\mathrm{disc}(L)) = 29$, the highest possible valuation by Proposition 3.1. 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 3.27 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 3.14 only gives us restrictions on φ based on $L_{\mathcal{R}}$ and no coefficients are set by Lemma 3.26. 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 5.6, 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 5.9 (b), no two of these 125 polynomials generate isomorphic extensions of $\mathbb{Q}_5$.

Example 5.13. 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 3.14, 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 3.26, 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 3.27 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	$\{0\}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$R_{\underline{K}}$	$\{\gamma\}$	$R_{\underline{K}}$
2^1	$\{0\}$	$\{0\}$	$\{\gamma\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{1\}$
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 5.3, $\underline{S}_1(z) = z^2\underline{A}_2 = z^2(z^6+\gamma)$ 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 5.6 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	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0,1\}$	$R_{\underline{K}}$	$\{0\}$	$\{\gamma\}$	$\{0\}$
2^1	$\{0\}$	$\{0\}$	$\{\gamma\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{1\}$
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 5.9 (c) that no two of these 8 polynomials generate the same extension.

Example 5.14. Let $K = \mathbb{Q}_3[x]/(x^2-3)$ and let π be a uniformizer of the valuation ring of K. As in Example 3.16, 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 3.8 we have $v_\pi(\varphi_3) = 1$ and by Lemma 3.27 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 3.26 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 5.6 we can set $\varphi_{k,j} = 0$ for $k + 9(j-1) \geq 14$.

Proceeding as in Examples 3.16, 3.29, and 5.7 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 $\mathcal{A}_{2,1}$.

While our choice of residual polynomials relate to the size of the automorphism group of the extensions generated by our polynomials, the polynomials generated by Algorithm 5 (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 5.15. 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.

CHAPTER VI

OM ALGORITHMS

An OM[1] algorithm is an algorithm that computes the Okutsu invariants of a polynomial Φ over a local field. The Okutsu invariants include, among other data, the ramification index and inertia degree of the irreducible factors of Φ. The data returned by an OM algorithm can be used to obtain a factorization of Φ, to find local and global integral bases, and the decomposition of ideals in global fields. Examples of OM-algorithms are the Montes algorithm [Mon99, GMN12] and its variations [Pau10] and the Round Four algorithm [For87, FL94, FPR02] and its variations [CG00, Pau01].

We give an OM algorithm and related results with emphasis on a complete and comprehensive presentation that can serve as a guide for implementing the algorithm. In part our presentation follows the approach of [Pau10] which combines the Montes algorithm with techniques from more recent versions of the Round Four algorithm [FPR02, Pau01]. In the theoretical considerations we view the process of approximating the factors of a polynomials as a process of partitioning the set of its roots (section 6.1). This is followed by detailed, constructive descriptions of the first (section 6.2) and general (section 6.3) iterations and a presentation of algorithm 6.4 as a variation of the Montes [Mon99] algorithm.

In the description, we will frequently make use of a particular representation of polynomials similar to the π-adic expansion of an element.

Definition 6.1. Let $\Phi \in \mathcal{O}_K[x]$ of degree N and $\varphi \in \mathcal{O}_K[x]$ of degree n be monic polynomials. We call

$$\Phi = \sum_{i=0}^{\lceil N/n \rceil} a_i \varphi^i$$

with $\deg(a_i) < n$ the *φ-expansion* of Φ.

Also, by convention, fractions denoted h/e or h_i/e_i are always taken to be in lowest terms.

[1] By convention OM stands for the regular expression (Ore+Okutsu)(MacLane+Montes) [BNS13].

6.1 Partitions of Zeros and Types

Let $\Phi(x) = x^N + \sum_{i=0}^{N-1} c_i x^i \in \mathcal{O}_K[x]$ be squarefree and let $\Theta_0 = \{\theta_1, \ldots, \theta_N\}$ be the set of zeros of Φ in $\overline{K}$. The process of approximating the irreducible factors of Φ can be regarded as a process of partitioning the set of its zeros. We obtain a tree with root node Θ_0 whose leafs are the sets of zeros of the irreducible factors of Φ. In our description of the algorithm, we focus on one path from the root node Θ_0 to a leaf. We indicate where branching would be needed to investigate all irreducible factors, thus describing the construction of all root paths in the tree. The nodes of such a root path are subsets of Θ_0, with each non-root node being a subset of its parent.

As part of this process, we will need to be able to construct polynomials of bounded degree with a particular valuation when evaluated at a root.

Lemma 6.2. *Let $\theta \in \overline{K}$, $(\varphi_i)_{1\le i\le u}$ with $\varphi_i \in \mathcal{O}_K[x]$ and $\varphi_i(\theta) = \frac{h_i}{e_i}$ in lowest terms. Let $E_i = \operatorname{lcm}(e_1, \ldots, e_i) = \operatorname{lcm}(E_{i-1}, e_i)$ and $e_i^+ = E_i/E_{i-1}$. Assume $\deg \varphi_i \ge e_{i-1}^+ \deg \varphi_{i-1}$. If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^{>0}$ with $b \mid E_u$, then there exists $\psi \in K[x]$ with $\deg \psi < e_u^+ \deg \varphi_u$ and $v(\psi(\theta)) = a/b$.*

Proof. We prove the Lemma by induction on u.

- $u = 1$: If $b = 1$ then $\psi = \pi^{s_\pi}$ with $s_\pi = a$ has the property $v(\psi(\theta)) = a = \frac{a}{b}$.

  Otherwise let $1 \le s_1 < e_1^+$ such that $s_1 h_1 \equiv \frac{a}{b} e_1^+ \bmod e_1^+$ such that

  $$\frac{a}{b} - v\left(\varphi_1^{s_1}(\theta)\right) = \frac{a}{b} - s_1 \frac{h_1}{e_1^+} = \frac{a}{b} - \frac{a}{be_1^+} e_1^+ + Be_1^+ = Be_1^+ \in \mathbb{Z}$$

  for some $B \in \mathbb{Z}^{>0}$. Let $s_\pi = Be_1^+ \in \mathbb{Z}$ and $\psi = \pi^{s_\pi} \varphi_1^{s_1}$. Now $v(\psi(\theta)) = \frac{a}{b}$ and $\deg \psi = s_1 \deg \varphi_1 < e_1^+ \deg \varphi_1$.

- $u > 1$: Assume for $a' \in \mathbb{Z}$ and $b' \in \mathbb{Z}^{>0} \setminus \{0\}$ with $b' \mid E_{u-1}$ we can find $\psi' \in K[x]$ with $v(\psi'(\theta)) = \frac{b'}{a'}$ and $\deg \psi' < e_{u-1}^+ \deg \varphi_{u-1}$.

  If $b \mid E_{u-1}$ then we can find ψ by our assumption.

  Otherwise we find $s_u \in \mathbb{Z}$, $0 \le s_u < e_u^+$ such that $s_u h_u \frac{E_u}{e_u} \equiv \frac{a}{b} E_u \bmod e_u^+$. Now $s_u h_u \frac{E_u}{e_u} = \frac{a}{b} E_u + Be_u^+$ for some $B \in \mathbb{Z}$ and thus $s_u \frac{h_u}{e_u} = \frac{a}{b} + \frac{B}{E_{u-1}}$. We get

  $$\frac{a}{b} - v\left(\varphi_u^{s_u}(\theta)\right) = \frac{a}{b} - s_u \frac{h_u}{e_u} = \frac{a}{b} - \frac{a}{b} + \frac{B}{E_{u-1}} = \frac{B}{E_{u-1}} \in \frac{1}{E_{u-1}}\mathbb{Z}.$$

By our assumption there exists $\psi' \in K[x]$ with $v(\psi'(\theta)) = \frac{B}{E_{u-1}}$ and $\deg \psi' < e_{u-1}^{+} \deg \varphi_{u-1}$. Thus for $\psi = \varphi_u^{s_u} \psi'$ we have $v(\psi(\theta)) = \frac{a}{b}$ and

$$\begin{aligned} \deg \psi &= s_u \deg \varphi_u + \deg \psi' < s_u \deg \varphi_u + e_{u-1}^{+} \deg \varphi_{u-1} \\ &\leq s_u \deg \varphi_u + \deg \varphi_u \leq e_u^{+} \deg \varphi_u. \end{aligned}$$

□

We start the first iteration with a linear monic polynomial $\varphi_1 = x + \beta \in \mathcal{O}_K[x]$. The negatives of the slopes of the segments of the Newton polygon of $\Phi(x - \beta)$ are the valuations of the roots of Φ. So the set

$$L_1 = \{v(\varphi_1(\theta)) \mid \theta \in \Theta_0\}$$

contains the negatives of the slopes of the segments of the Newton polygon of $\Phi(x-\beta)$, which yields a partition of Θ_0 into the sets $\{\theta \in \Theta_0 \mid v(\theta) = \lambda\}$ for $\lambda \in L_1$. By Corollary 2.27 each of these sets corresponds to a proper factor of Φ. For some $\lambda_1 \in L_1$ we set

$$\Theta_1^* = \{\theta \in \Theta_0 \mid v(\varphi_1(\theta)) = \lambda_1\}. \tag{6.1}$$

Without computing Θ_1^* explicitly we investigate the factor $\prod_{\theta \in \Theta_1^*}(x - \theta)$ of Φ further.

Let $\lambda_1 = h_1/e_1$ in lowest terms. Then $v(\varphi_1^{e_1}(\theta)/\pi^{h_1}) = 0$ for all $\theta \in \Theta_1^*$. We set

$$R_1 = \left\{ \underline{\rho} \in \underline{K}[z] \;\middle|\; \underline{\rho} \text{ irreducible and } \underline{\rho}\left(\underline{\varphi^{e_1}(\theta)/\pi^{h_1}}\right) = \underline{0} \text{ for some } \theta \in \Theta_1^* \right\}.$$

If R_1 contains more than one polynomial then $\underline{\chi}_{\underline{\varphi_1^{e_1}(\theta)/\pi^{h_1}}} \in \underline{K}[z]$ (see Definition 2.24) has at least two coprime factors and Proposition 2.25 yields a proper factor of Φ for each $\underline{\rho} \in R_1$. We obtain a parition of Θ_1^* into the sets $\left\{\theta \in \Theta_1^* \;\middle|\; \underline{\rho}_1\left(\underline{\varphi_1^{e_1}(\theta)/\pi^{h_1}}\right) = \underline{0}\right\}$. For some $\underline{\rho}_1 \in R_1$ we set

$$\Theta_1 = \left\{\theta \in \Theta_1^* \;\middle|\; \underline{\rho}_1\left(\underline{\theta^{e_1}/\pi^{h_1}}\right) = \underline{0}\right\}. \tag{6.2}$$

Without computing Θ_1 explicitly, we investigate the factor $\prod_{\theta \in \Theta_1}(x - \theta)$ of Φ further.

All information obtained in the considerations above can be derived from the tuple

$$(\varphi_1, \lambda_1, \psi_1, \underline{\rho}_1) = (x, \lambda_1, \pi^{h_1}, \underline{\rho}_1) \in \mathcal{O}_K[x] \times \mathbb{Q} \times K[x] \times \underline{K}[z] \quad (\text{ in fact } \psi_1 = \pi^{h_1} \in K),$$

which is the base for the recursive construction of a sequence of consecutively better approximations to an irreducible factor of Φ. Given $(\varphi_1, \lambda_1, \underline{\rho}_1)$ equations (6.1) and (6.2) yield the subsets of roots Θ_1^* and Θ_1.

For all $\theta \in \Theta_1$, $E_1 = e_1^+ = e_1$ is a divisor of the ramification index and $F_1 = \deg \rho_1$ is a divisor of the inertia degree of $K(\theta)$. Thus $[K(\theta) : K]$ is divisible by $E_1 F_1$ and the degrees of the irreducible factors of Φ with roots in Θ_1 are each divisible by $E_1 F_1$.

The next step is the construction of a monic polynomial $\varphi_2 \in \mathcal{O}_K[x]$ of degree $E_1 \cdot F_1$ with $v(\varphi_2(\theta)) > v(\varphi_1(\theta))$ for all $\theta \in \Theta_1$, which is described in section 6.2.3 below. Assuming we have found such a φ_2 we let $L_2 = \{v(\varphi_2(\theta)) \mid \theta \in \Theta_1\}$. Again each of the slope corresponds to a proper factor of Φ (compare Corollary 2.27). We examine one of these factors further. Let $\lambda_2 = h_2/e_2 \in L_2$ and set $\Theta_2^* = \{\theta \in \Theta_1 \mid v(\varphi_2) = \lambda_2\}$. For each $\theta \in \Theta_2^*$ the ramification index of $K(\theta)$ is divisible by $E_2 = \operatorname{lcm}\{e_1, e_2\}$. By Lemma 6.2, there exists $\psi_2 \in K[x]$ with $\deg \psi_2 < \deg \varphi_2$ and $v(\psi(\theta)) = -e_2^+ \lambda_2 \in \frac{1}{E_1}\mathbb{Z}$ with $e_2^+ = E_2/E_1$. Now

$$R_2 = \left\{ \underline{\rho} \in \underline{K} \;\middle|\; \underline{\rho} \text{ irreducible and } \underline{\rho}\left(\underline{\varphi_2^{e_2^+}/\psi_2}\right) = \underline{0} \text{ for some } \theta \in \Theta_2^* \right\}$$

is the set of irreducible factors of $\underline{\chi}_{\theta^{e_1}\psi} \in \underline{K}[y]$, each of which corresponds to a proper factor of Φ. For some $\underline{\rho}_2 \in R_2$ we set

$$\Theta_2 = \left\{ \theta \in \Theta_2^* \;\middle|\; \underline{\rho}_2\left(\underline{\varphi_2^{e_2^+}/\psi_2}\right) = \underline{0} \right\}.$$

Again the sets Θ_2^* and Θ_2 can be recovered from the information contained in

$$(\varphi_2, \lambda_2, \psi_2, \underline{\rho}_2) \in \mathcal{O}_K[x] \times \mathbb{Q} \times K[x] \times \underline{K}_1[z].$$

We continue this process inductively and keep track of the information computed in a sequence of such tuples.

Definition 6.3. Let $\Phi \in \mathcal{O}_K[x]$. Let $t = (\varphi_i, \lambda_i, \psi_i, \underline{\rho}_i)_{1 \le i \le u}$ where

(a) $\varphi_i \in \mathcal{O}_K[x]$ is monic with $\varphi_1 \in \mathcal{O}_K[x]$ linear,

(b) $\lambda_i = h_i/e_i \in \mathbb{Q}$,

(c) $\psi_i \in K[x]$ with $\deg \psi_i < \deg \varphi_i$, and

(d) $\underline{\rho}_i \in \underline{K}_i$ irreducible with $\underline{K}_i = \underline{K}_{i-1}[z]/(\underline{\rho}_i)$ with $\underline{K}_0 = \underline{K}$.

We call t an *extended type of* Φ if for all θ in some subset Θ of the set of roots of Φ we have:

(e) $v(\varphi_i(\theta)) = \lambda_i$

(f) $v(\psi_i(\theta)) = e_i^+ \lambda_i$ with $e_i^+ = \operatorname{lcm}(e_1, \ldots, e_i)/\operatorname{lcm}(e_1, \ldots, e_{i-1})$,

(g) $\underline{\rho}_i(\underline{\varphi_i^{e_i^+}(\theta)/\psi_i(\theta)}) = \underline{0}$, and

(h) $v(\varphi_i(\theta)) > v(\varphi_{i-1}(\theta))$ and $\deg \varphi_i = e_i^+ \cdot \deg \underline{\rho}_{i-1} \cdot \deg \varphi_{i-1}$ for $2 \le i \le u$.

The sequence $(\varphi_i, \lambda_i, \underline{\rho}_i)_{1 \le i \le u}$ is called a *type of* Φ of order u (see [GMN11, Definitions 1.21, 1.22 and section 2.1]).

A type t describes a root path in a tree of partitions of Θ_0. If $t = (\varphi_i, \lambda_i, \psi_i, \rho_i)_{1 \le i \le u}$ is an extended type with a corresponding subset of roots Θ_u, then $E_u = \operatorname{lcm}(e_1, \ldots, e_u)$ divides the ramification index of $K(\theta)$ for $\theta \in \Theta$ and $F_u = \deg \rho_1 \cdots \deg \rho_u$ divides the inertia degree of $K(\theta)$ for $\theta \in \Theta$. As the degree of the irreducible factors of Φ are minimal polynomials of some $\theta \in \Theta$ is divisible by $E_u F_u$, we construct φ_{u+1} of degree $E_u F_u$. In the following sections we give methods for constructing φ_{u+1}, finding $v(\varphi_{u+1}(\theta))$ for all $\theta \in \Theta_u$, ψ_{u+1}, and ρ_{u+1}. We will see that the sets $\Theta_0 \supset \Theta_1 \supset \cdots \supset \Theta_u$ help in understanding the algorithm, but are not needed in actual computations.

If $\#\Theta_u = E_u F_u$, then φ_u is an approximation to an irreducible factor of Φ of degree $E_u F_u$. Using the information in the type t this approximation can be lifted to give an approximation of any desired precision (see [GNP12]).

Definition 6.4. Let $t = (\varphi_i, \lambda_i, \underline{\rho}_i)_{1\le i\le u}$ be a type, write $\lambda_u = h_u/e_u$ in lowest terms and set $e_u = \operatorname{lcm}(e_1,\dots,e_u)/\operatorname{lcm}(e_1,\dots,e_{u-1})$. Let $\Theta_u^* = \{\theta \in \Theta_0 \mid v(\theta) = \lambda_u\}$ and

$$\Theta_u = \left\{ \theta \in \Theta_u^* \;\middle|\; \underline{\rho}_u\left(\underline{\frac{\varphi^{e_u}}{\psi}(\theta)}\right) = \underline{0} \right\}$$

where $\psi \in K[x]$ with $\deg\psi < \deg\varphi_u$ and $v(\psi(\theta)) = eh_u/e_u$ for $\theta \in \Theta_u^*$. The type t is called *complete* if $E_uF_u = \#\Theta_u$.

If $E_iF_i = 1$ then no new partition of the sets of roots has been found in this step. A type with all these elements omitted is an optimal type:

Definition 6.5. Let $t = (\varphi_i, \lambda_i, \underline{\rho}_i)_{1\le i\le u}$ be a type, write $\lambda_i = h_i/e_i$ in lowest terms and set $E_u = \operatorname{lcm}(e_1,\dots,e_u)$ and $F_u = \deg\underline{\rho}_1 \cdot\cdots\cdot \underline{\rho}_u$. The type t is called *optimal* if $E_iF_i > 1$ for $1 \le i \le u$.

In section 6.6 we will see that if $t = (\varphi_i, \lambda_i, \underline{\rho}_i)_{1\le i\le u}$ is complete and optimal, then the sequence of negated slopes $(\lambda_i)_{1\le i\le u}$ and the sequence $(F_i)_{1\le i\le u}$, where $F_i = \deg\underline{\rho}_1 \cdot\cdots\cdot \underline{\rho}_i$, are invariants of Φ.

6.2 The First Iteration

We start our description of an OM algorithm with the first iteration. We have already gone through these steps in a more conceptual manner in the previous section. As before let $\varphi_1 \in \mathcal{O}_K[x]$ be linear and monic, say $\varphi_1(x) = x + \beta$, and let Θ_0 denote the set of zeros of Φ in $\overline{K}$. Although we use the zeros in Θ_0 in our exposition, they are not needed in any of the computations.

6.2.1 Newton Polygon I

The Newton polygon of $\Phi(y-\beta)$ yields the valuations of the zeros $\theta_1,\dots,\theta_N$ of Φ. We obtain the same polynomial and polygon using the φ_1-expansion of Φ (see Definition 6.1). If $\Phi = \sum a_i\varphi_1^i$ is the φ_1-expansion of Φ, then

$$\chi_1(y) = \sum_{i=0}^{\lceil N/\deg\varphi_1\rceil} a_i y^i = \Phi(y-\beta) \tag{6.3}$$

has the zeros $\varphi_1(\theta)$ where $\theta \in \Theta_0$. The negatives of the slopes of the segments of the Newton polygon of χ_1 are the valuations of $\varphi_1(\theta)$ for $\theta \in \Theta_0$. We obtain a partition of Θ_0 into the sets

$$\{\theta \in \Theta \mid v(\varphi_1(\theta)) = \lambda\}$$

where λ is the negative of the slope of a segment of the Newton polygon of χ_1. To find the splitting field one continues the algorithm for each of the sets in this partition.

6.2.2 Residual Polynomial I

Residual (or associated) polynomials were first introduced by Ore [Ore28, MN92]. They yield information about the unramified part of the extension generated by the zeros of Φ. Let S be a segment of the Newton Polygon of $\chi_1(y) = \sum_{i=1}^{N} a_i y^i$ (see (6.3)), let m_1 be the (horizontal) length of S, $(k, v(a_k))$ and $(k + m_1, v(a_{k+m_1}))$ its endpoints, and $\lambda_1 = \frac{v(a_k)-v(a_{k+n})}{m_1} = \frac{h_1}{e_1}$ the negative of its slope. If

$$\Theta_1^* = \{\theta \in \Theta_0 \mid v(\varphi_1(\theta)) = \lambda_1\},$$

then $|\Theta_1^*| = m_1$. We evaluate χ_1 at $\varphi_1(\theta)y$ and obtain a polynomial whose Newton polygon has a horizontal segment of length m_1. For $\theta \in \Theta_1^*$ we consider $\chi_1(\varphi_1(\theta)y)$. Using the equivalence relation from Definition 2.12 we obtain

$$\chi_1(\varphi_1(\theta)y) = \sum_{i=0}^{N} a_i(\varphi_1(\theta)y)^i \sim \sum_{i=k}^{k+m_1} a_i\varphi_1^i(\theta)y^i \sim \sum_{j=0}^{m_1/e_1} a_{je_1+k}\varphi_1^{je_1+k}(\theta)y^{je_1+k}$$

The last equivalence holds, because the x-coordinates of the points on the segment of the Newton polygon are of the form $k + je_1$ with $0 \leq j \leq m_1/e_1$. Furthermore for $0 \leq j \leq m_1/e_1$ we have $v(a_{je_1+k}\varphi_1^{je_1+k}(\theta)) \geq v(a_k\varphi_1^k(\theta))$ and the polynomial is divisible by y^k. Dividing $\chi_1(\varphi_1(\theta)y)$ by $\pi^{v(a_k)}\varphi_1^k(\theta)y^k$ we obtain a polynomial of degree m_1/e_1 that is equivalent to a polynomial whose

leading coefficient and constant coefficient have valuation zero:

$$\frac{\chi_1(\varphi_1(\theta)y)}{\pi^{v(a_k)}\varphi_1^k(\theta)y^k} \equiv \sum_{j=0}^{m_1/e_1} \frac{a_{je_1+k}\varphi_1^{je_1}(\theta)y^{je_1}}{\pi^{v(a_k)}} \bmod (\pi).$$

For $\epsilon = \varphi_1^{e_1}/\pi^{h_1}$ we have $v(\epsilon(\theta)) = v(\varphi_1^{e_1}(\theta)/\pi^{h_1}) = 0$. Substitution of $\epsilon\pi^{h_1}$ for $\varphi_1^{e_1}$ yields

$$\frac{\chi_1(\varphi_1(\theta)y)}{\pi^{v(a_k)}\varphi_1^k(\theta)y^k} \equiv \sum_{j=0}^{m_1/e_1} \frac{a_{je_1+k}\pi^{jh_1}\epsilon^j y^{je_1}}{\pi^{v(a_k)}} \bmod (\pi).$$

Replacing ϵy^{e_1} by z and considering the resulting polynomial over $\underline{K}$ yields the residual polynomial of S:

$$\underline{A}_1(z) := \sum_{j=0}^{m_1/e_1} \underline{a_{je_1+k}\pi^{jh_1-v(a_k)}} z^j \in \underline{K}[z].$$

For $\theta \in \Theta_1^*$ we have that $\underline{\varphi_1^{e_1}(\theta)/\pi^{h_1}} \in \overline{\underline{K}}$ is a zero of $\underline{A}_1$.

6.2.3 The Next Approximation I

Let $\underline{\rho}_1$ be one of the irreducible factors of $\underline{A}_1$, let $\Theta_1 = \{\theta \in \Theta_1^* \mid \underline{\rho}_1\left(\theta^{e_1}/\pi^{h_1}\right) = 0\}$, and denote by $\rho_1 \in \mathcal{O}_K[x]$ a monic lift of $\underline{\rho}_1$.

We now know that for all $\theta \in \Theta_1$ the ramification index of $K(\theta)$ is divisible by $E_1 = e_1$ and that $F_1 = \deg \rho_1$ is a divisor of its inertia degree. We set

$$\varphi_2 = \pi^{f_1 h_1}\rho_1(\varphi_1^{e_1}/\pi^{h_1}).$$

The polynomial $\varphi_2 \in \mathcal{O}_K[x]$ is monic and has degree $e_1 \cdot f_1$.

Lemma 6.6. *$\varphi_2 \in \mathcal{O}_K[x]$ is irreducible.*

Proof. For $\theta \in \Theta_1$ we have

$$v(\varphi_2(\theta)) = v(\pi^{f_1 h_1}\rho_1(\varphi_1^{e_1}(\theta)/\pi^{h_1})) > f_1 h_1 \geq v(\theta) = \frac{h_1}{e_1}.$$

The Newton polygon of φ_2 consists of one segment of slope $-\lambda_1 = -\frac{h_1}{e_1}$ and for each root α of φ_2 we have $\underline{\rho}_1\left(\underline{\frac{\alpha^{e_1}}{\pi^{h_1}}(\alpha)}\right) = \underline{0}$. So $K(\alpha) \cong K[x]/(\varphi_2)$ is an extension with inertia degree f_1 and ramification index e_1. Thus, as $\deg \varphi_2 = e_1 f_1$, the polynomial φ_2 is irreducible. □

6.2.4 Valuations I

Let $a \in K[x]$ with $\deg a < \deg \varphi_2 = E_1 F_1$. We show how the data computed in the first iteration can be used to find $v(a(\theta))$. Let $a = \sum_{j=0}^{E_1 F_1 - 1} a_j \varphi_1^j$ be the φ_1-expansion of a. (Note that since $\deg \varphi_1 = 1$, each a_j lies in K.) Because the values

$$v(\varphi_1(\theta)) = \frac{h_1}{E_1}, \ldots, v(\varphi_1^{E_1 - 1}(\theta)) = \frac{(E_1 - 1)h_1}{E_1}$$

are distinct and

$$\underline{1}, \underline{\frac{\varphi_1(\theta)^{E_1}}{\pi^{h_1}}}, \ldots, \left(\underline{\frac{\varphi_1(\theta)^{E_1}}{\pi^{h_1}}}\right)^{F_1 - 1}$$

are linearly independent over $\underline{K}$, we have

$$v(a(\theta)) = \min_{0 \le j \le E_1 F_1 - 1} v(a_j \varphi_1^j) = \min_{0 \le j \le E_1 F_1 - 1} v(a_j) + j(h_1/E_1).$$

Furthermore, if we omit all terms with valuation greater than $v(a(\theta))$ we obtain a polynomial b that at θ is equivalent to a. That is, for $J = \{j \mid v(a_j) + j(h_1/e_1) = v(a(\theta))\}$ and $b = \sum_{j \in J} a_j \varphi_1^j$, we have $a(\theta) \sim b(\theta)$ for $\theta \in \Theta_1$.

6.2.5 Arithmetic I

We consider the arithmetic of polynomials of degree less than $E_1 F_1$. Clearly addition and subtraction of two such polynomials again yield polynomials of degree less than $E_1 F_1$.

Let $a(x) = \sum_{i=0}^{E_1 F_1 - 1} a_i x^i$ and $\tau(x) = x^{s_1} \pi^{s_\pi}$ with $s_1, s_\pi \in \mathbb{Z}$. Multiplication gives $a(x)\tau(x) = \sum_{i=0} E_1 F_1 - 1 a_i \pi^{s_\pi} x^{i - s_1}$ which in general is a rational function or a polynomial of degree greater

than $E_1F_1 - 1$. We have $v(\rho_1(\theta^{E_1}/\pi^{h_1})) = 0$. Let $\tau(x) = \rho_1(x) - x^{F_1}$ this gives the relation

$$\theta^{E_1F_1} \sim \pi^{e_1F_1}\tau(\theta).$$

So by repeatedly substituting $\varphi_1^{E_1F_1}$ by $\pi^{h_1F_1}\tau$ we obtain a polynomial $b \in K[x]$ with $\deg b < E_1F_1$ such that $b(\theta) \sim a(\theta)\psi(\theta)$.

6.2.6 Representatives I

Let $\Gamma \in K[x]$ with $v(\Gamma(\theta)) = 0$ be reduced as described in the end of 6.2.4. As $v(\Gamma(\theta)) = 0$ it must be of the form $\Gamma = \sum_{i=0}^{F_1} g_i x^{iE_1}$ with $v(g_i) = ih_1$. So $\underline{\Gamma}(\theta) \sim \sum_{i=0}^{F_1} \underline{g_i/\pi^{ih_1}}\underline{\gamma}_1$.

Each $\underline{b} \in \underline{K}_1$ can be written as $\underline{b} = \sum_{i=0}^{F_1-1} \underline{b}_i\underline{\gamma}_1^i$ with $\underline{b}_i \in \underline{K}$ Let b_i be a representative of $\underline{b}_i$ in $\mathcal{O}_K$. Clearly for $a(x) = \sum_{i=0}^{F_1-1} b_i \frac{x^{iE_1}}{\pi^{h_1}}$ we have $\underline{a(\theta)} = \underline{b}$.

6.3 The *u*-th Iteration

We describe a general iteration of the algorithm. Let $t = (\varphi_i, \lambda_i, \psi_i, \underline{\rho}_i)_{1\le i\le u-1}$ be an extended type of Φ that is not complete. We write $\lambda_i = h_i/e_i$ with $\gcd(h_i, e_i) = 1$ and set $E_i = \operatorname{lcm}\{e_1, \ldots, e_i\}$ and $e_i^+ = E_i/E_{i-1}$. Assume we have found the next approximation $\varphi_u \in \mathcal{O}_K[x]$ to an irreducible factor of Φ with $\deg\varphi_u = E_{u-1}F_{u-1}$ and $v(\varphi_u(\theta)) > v(\varphi_{u-1}(\theta))$ for all $\theta \in \Theta_{u-1}$.

We assume we have the following methods, which rely on the data computed in the previous steps. For each method the base case is described in section 6.2 and the general case in this section. Because of the recursive nature of the algorithm we use forward references in our representation.

`Valuation` given $a \in K[x]$ with $\deg a < \deg\varphi = E_{u-1}$, finds $v(a(\theta))$ for $\theta \in \Theta_{u-1}$ (see sections 6.2.4, 6.3.4 and Algorithm 6).

`PolynomialWithValuation` given $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^{>0}$ with $b \mid E_u$, finds $\psi \in K_u[x]$ with $\deg\psi < \deg\varphi_u = E_{u-1}$ such that $v(\psi(\theta)) = \frac{a}{b}$ for all $\theta \in \Theta_{u-1}$ (see Lemma 6.2).

Furthermore we assume we have methods for arithmetic and reduction of polynomials of degree less than E_u in their representations as sums of power products (see sections 6.2.5, 6.3.5 and Algorithm 9 (`reduce`).

In the u-th iteration of the algorithm we investigate the properties of φ_u and construct the next approximation φ_{u+1} to an irreducible factor of Φ.

6.3.1 Newton Polygon II

We use the φ_u-expansion of Φ to find the valuations $v(\varphi_u(\theta))$ for $\theta \in \Theta_{u-1}$. Let $l_u = \lceil N/\deg \varphi_u \rceil$ and $\Phi = \sum_{i=0}^{l_u} a_i \varphi_u^i$ be the φ_u-expansion of Φ. For each root $\theta \in \Theta_{u-1}$ we have

$$\Phi(\theta) = \sum_{i=0}^{l_u} a_i(\theta)\varphi_u^i(\theta) = 0.$$

Hence

$$\chi_u = \sum_{i=0}^{l_u} a_i(\theta) y^i \in \overline{K}[y]$$

has the zeros $\varphi_u(\theta)$ for $\theta \in \Theta_{u-1}$.

The method `Valuation` returns the valuations of the coefficients $a_i(\theta)$ of χ_u and with these the Newton polygon of χ_u yields the valuations of $\varphi_u(\theta)$ for $\theta \in \Theta_{u-1}$. We obtain a partition of Θ_{u-1} into the subsets $\{\theta \in \Theta_{u-1} \mid v(\varphi(\theta)) = \lambda\}$ where λ is the negative of the slope of a segment of the Newton polygon of χ_u. By Corollary 2.27 each segment of the Newton polygon of χ_u, and thus each set in the partition, corresponds to a factor of Φ.

Definition 6.7. The Newton polygon of χ_u is called the Newton polygon of Φ with respect to φ_u. It is also called a *Newton polygon of higher order* [Mon99, GMN12].

6.3.2 Residual Polynomial II

Let S be a segment of the Newton Polygon of χ_u of length m_u with endpoints $(k, v(a_k(\theta)))$ and $(k + m_u, v(a_{k+m_u}(\theta)))$ for $\theta \in \Theta_{u-1}$. Let

$$\lambda_u = \frac{v(a_k(\theta)) - v(a_{k+m_u}(\theta))}{m_u} = \frac{h_u}{e_u},$$

where $\gcd(h_u, e_u) = 1$ and let $\Theta_u^* = \{\theta \in \Theta_{u-1} \mid v(\varphi_u(\theta)) = \lambda_u\}$. We have $|\Theta_u^*| = m_u \deg \varphi_u$. Set $E_u = \operatorname{lcm}\{e_1, \ldots, e_u\}$ and $e_u^+ = E_u/E_{u-1}$.

The method `PolynomialWithValuation` gives $\psi_u \in K_{u-1}[x]$ with

$$v(\psi_u(\theta)) = v\left(\varphi_u^{e_u^+}\right) = e_u^+ \lambda_u = \frac{h_u}{e_u/e_u^+}$$

for $\theta \in \Theta_u^*$. We have

$$\chi_u(\varphi_u(\theta)) \sim \sum_{i=k}^{k+m_u} a_i(\theta)\varphi_u^i(\theta)x^i \sim \sum_{j=0}^{m_u/(e_u^+)} a_{je_u^++k}(\theta)\varphi_u^{je_u^++k}(\theta)x^{je_u^++k}$$

The last equivalence holds, because the x-coordinates of the points on the segment of the Newton polygon are of the form $k + je_u^+$ $(0 \le j \le m/(e_u^+))$. Division by $\varphi_u^k y^k$ yields

$$\frac{\chi_u(\varphi_u(\theta))}{\varphi_u^k(\theta)y^k} \sim \sum_{j=0}^{m_u/(e_u^+)} a_{je_u^++k}(\theta)\varphi_u^{je_u^+}(\theta)y^{je_u^+}.$$

For $\gamma = \varphi_u(\theta)^{e_u^+}/\psi_u(\theta)$ we have $v(\gamma) = v(\varphi_u^{e_u^+}(\theta)/\psi_u(\theta)) = 0$. By substituting $\gamma\psi_u(\theta)$ for $\varphi_u^{e_u^+}(\theta)$ we get

$$\frac{\chi(\varphi_u(\theta)y)}{\varphi_u^k(\theta)y^k} \sim \sum_{j=0}^{m_u/(e_u^+)} a_{je_u^++k}(\theta)(\gamma\psi_u^j(\theta))y^{je_u^+}$$

The method `PolynomialWithValuation` gives a polynomial $\tau \in K_{u-1}[x]$ with $v(\tau(\theta)) = v(a_k(\theta))$ for $\theta \in \Theta_{u-1}$. Replacing $\gamma y^{e_u^+}$ by y and division by $\tau(\theta)$ yields

$$A(y) = \sum_{j=0}^{m_u/(e_u^+)} \frac{a_{je_u^++k}(\theta)\psi_u^j(\theta)}{\tau(\theta)} y^j.$$

By construction, $v\left(\dfrac{a_{je_u^+ +k}(\theta)\psi_u^j(\theta)}{\tau(\theta)}\right) \geq 0$, and in particular,

$$v\left(\frac{a_k(\theta)\psi_u(\theta)}{\tau(\theta)}\right) = 0 \quad \text{and} \quad v\left(\frac{a_{k+m_u}(\theta)\psi_u^{m_u/(e_u^+)}(\theta)}{\tau(\theta)}\right) = 0.$$

So the polynomial $\underline{A}(z) \in \underline{K}_{u-1}[z]$, called the *residual polynomial* of S, has degree $m_u/(e_u^+)$.

6.3.3 The Next Approximation II

We construct $\varphi_{u+1} \in \mathcal{O}_K[x]$ with

$$v(\varphi_{u+1}(\theta)) > v(\varphi_u(\theta)) \quad \text{and} \quad \deg \varphi_{u+1} = E_u F_u.$$

Let $\underline{\rho}(z) = \sum_{i=0}^{f_u} \underline{r}_i y^i \in \underline{K}_{u-1}$ be one of the irreducible factors of $\underline{A}_u(z)$. We set $R_{f_u} = 1$ and using methods from 6.3.6 and 6.2.6 we obtain polynomials $R_i \in K[x]$ with $\underline{R_i(\theta)} = \underline{r}_i$ for $0 \leq i < f_u$. Now for

$$\varphi_{u+1}^* = \psi^{f_u}\rho\left(\frac{\varphi_u^{e_u}}{\psi}\right) = \sum_{i=0}^{f_u} R_i \psi^{f_u - i}\varphi_u^{ie_u}$$

by construction

$$\varphi_{u+1}^*(\theta) = \psi^{f_u}(\theta)\rho\left(\frac{\varphi_u^{e_u^+}}{\psi}(\theta)\right) > f_u e_u^+ \lambda_u \geq \lambda_u = \varphi_u(\theta).$$

As, in general, $\deg \varphi_{u+1}^* > E_u F_u$ we reduce the degree of this polynomial. It is sufficient to find polynomials $b_i \in K[x]$ with $\deg b < E_u F_u$ $(0 \leq i < f_u)$ such that $b_i(\theta) \sim R_i(\theta)\psi^{f_u - i}(\theta)$. We obtain the b_i by using the methods from 6.3.5 and 6.2.5 for degree reduction and set

$$\varphi_{u+1} = \varphi_u^{e_u f_u} + \sum_{i=0}^{F_u - 1} b_i \varphi_u^{ie_u}.$$

6.3.4 *Valuations II*

For $b \in K_{u-1}[x]$ with $\deg b < E_{u-1}F_{u-1}$ the method `Valuation` yields $v(a(\theta))$ for $\theta \in \Theta_u \subset \Theta_{u-1}$.

Let $a \in K_u[x]$ with $\deg a < E_uF_u$ and $m = \lceil \deg a / \deg \varphi_u \rceil$. Let $a = \sum_{j=0}^{m} a_j \varphi_u^j$ with $\deg a_j < \deg \varphi_u = E_{u-1}$ be the φ_u-expansion of a. As the valuations

$$v(\varphi_u(\theta)) = \frac{h_1}{e_u}, \ldots, v(\varphi_u^{e_u^+ - 1}(\theta)) = \frac{(e_u^+ - 1)h_u}{e_u}$$

are distinct (and not in $\frac{1}{E_{u-1}}\mathbb{Z}$) and

$$\underline{1}, \frac{\underline{\varphi_u^{e_u^+}(\theta)}}{\underline{\pi^{h_u}}}, \ldots, \left(\frac{\underline{\varphi_u^{e_u^+}(\theta)}}{\underline{\pi^{h_u}}}\right)^{f_u - 1}$$

are linearly independent over $\underline{K}_u$, for $\theta \in \Theta_u$ we have

$$v(a(\theta)) = \min_{0 \le j \le m} v\left(a_j(\theta)\varphi_u^j(\theta)\right) = \min_{0 \le j \le m} v(a_j(\theta) + j(h_1/E_1).$$

If we only consider the terms with valuation $v(a(\theta))$ we obtain a polynomial that at θ is equivalent to a, that is, for $J = \{j \mid v(a_j) + jh_u/e_u = v(a(\theta))\}$ and $b = \sum_{j \in J} a_j \varphi_u^j$ we have $a(\theta) \sim b(\theta)$ for $\theta \in \Theta_u$. This also shows we only need the type $((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le n}$ to compute the valuation $v(a(\theta))$ but not θ.

6.3.5 *Arithmetic II*

We consider the arithmetic of polynomials of degree less than E_uF_u. Clearly addition and subtraction of two such polynomials again yield polynomials of degree less than E_uF_u. We assume methods for handling polynomials of degree less than $E_{u-1}F_{u-1}$ are available. That is, given $a \in K_{u-1}[x]$ and $b \in K_{u-1}[x]$ we can find a polynomial $c \in K_{u-1}[x]$ with $\deg c < E_{u-1}F_{u-1}$ such that $c(\theta) \sim a(\theta)b(\theta)$ for $\theta \in \Theta_u \subseteq \Theta_{u-1}$.

Let $a = \sum_{i=0}^{E_1F_1 - 1} a_i \varphi_u^i$ and $b = \varphi_u^{s_u} b'$ with $s_u \in \mathbb{Z}$ and $\psi \in K[x]$ of degree less than $E_{u-1}F_{u-1}$. Multiplication gives $ab = \sum_{i=0} E_1F_1 - 1 a_i b' \varphi^{i - s_u}$ which in general is a rational function or a poly-

nomial of degree greater than $E_uF_u - 1$. By our assumption we can find polynomials $c_i \in K[x]$ with $\deg c_i < E_{u-1}F_{u-1}$ such that $c_i(\theta) \sim a_i(\theta)b'(\theta)$ for $\theta \in \Theta_u \subseteq \Theta_{u-1}$. We have $v(\rho_u(\varphi_u^{e_u}(\theta)/\psi(\theta))) = 0$. Let $\tau = \rho_1 - x^{F_1}$ this gives the relation

$$\theta^{E_1F_1} \sim \pi^{h_1F_1}\tau(\theta).$$

So by repeatedly substituting $\varphi_u^{e_uf_u}$ by $\psi_u^{f_u}\tau(\varphi_u/\psi_u)$ we obtain a polynomial $b \in K[x]$ with $\deg b < e_uf_u$ such that $b(\theta) \sim a(\theta)\psi(\theta)$.

Proposition 6.8. *Let $t = ((\varphi_i, \lambda_i, \underline{\rho}_i))_{1\le i\le u}$ be a type of Φ and Θ_u the corresponding subset of zeros. Let $a, b \in K[x]$ with $\deg a < \deg \varphi_u$ and $\deg b < \deg \varphi_u$ then there exists $c \in K[x]$ with $\deg c < \deg \varphi_u$ such that $c(\theta) \sim a(\theta)b(\theta)$.*

6.3.6 Representatives II

Let $\Gamma \in K[x]$ with $v(\Gamma(\theta)) = 0$ be reduced as described in the end of 6.3.4. As $v(\Gamma(\theta)) = 0$ it must be of the form $\Gamma = \sum_{i=0}^{F_1} g_i x^{iE_1}$ with $v(g_i) = ih_1$. So $\underline{\Gamma}(\theta) \sim \sum_{i=0}^{F_1} \underline{g_i/\pi^{ih_1}}\underline{\gamma}_1$.

Each $\underline{b} \in \underline{K}_{u-1}$ can be written as $\underline{b} = \sum_{i=0}^{F_1-1} \underline{b}_i\underline{\gamma}_1^i$ with $\underline{b}_i \in \underline{K}$ Let b_i be a representative of $\underline{b}_i$ in $\mathcal{O}_K$. Clearly for

$$a = \sum_{i=0}^{F_1-1} b_i \frac{x^{iE_1}}{\pi^{h_1}}$$

we have $\underline{a(\theta)} = \underline{b}$.

6.4 The Algorithm

Let $t = ((\varphi_i, \lambda_i, \underline{\rho}_i))_{1\le i\le u}$ be a type of Φ and let Θ_u be the corresponding subset of the roots of Φ.

First we have to compute the φ_u-expansion of Φ and (recursively) the φ_i-expansions of the coefficients (see 6.3.1). The following step, that is, the computation of the residual polynomial (6.2.2 and 6.3.2), can be conducted in the representation of the polynomials as nested φ_i-expansions, as computed in the first step. This includes the computation of ψ and τ, which only need to be

represented as a sequence of exponents. We need to return to a presentation as polynomials only when constructing the next approximation (6.2.3 and 6.3.3).

In an implementation of the algorithm the methods described below operate on representations of polynomials as nested φ_i-expansions. To avoid having to write down these somewhat involved data structures, we use polynomials to formulate the input and the output of the methods.

Sections 6.2.5 and 6.3.5 yield these methods:

`div`(t, a, b) given $a \in K[x]$ of degree less than $E_u F_u$ and $b = \varphi_u^{s_u} \dots \varphi_1^{s_1} \pi^{s_\pi}$, where $s_i < e_i f_i$, we find $C \in K[x]$ with $\deg c < \deg \varphi_u$ such that $a(\theta)/b(\theta) \sim c(\theta)$ for all $\theta \in \Theta_u$;

`mult`(t, a, b) given $a, b \in K[x]$ of degree less than $E_u F_u$, we find $c \in K[x]$ with $\deg c < \deg \varphi_u$ such that $a(\theta)b(\theta) \sim c(\theta)$ for all $\theta \in \Theta_u$;

`pow`(t, a, n) given $a \in K[x]$ of degree less than $E_u F_u$, we find $c \in K[x]$ with $\deg c < \deg \varphi_u$ such that $a(\theta)^n \sim c(\theta)$ for all $\theta \in \Theta_u$.

Sections 6.2.6 and 6.3.6 yield the methods:

`residue`(t, a) given $a \in K[x]$ with $\deg a < E_u F_u$ and $v(a(\theta)) = 0$ we find $\underline{\gamma} \in \underline{K}_u$ such that $\underline{a(\theta)} = \underline{\gamma}$;

`representative`(t, γ) given $\underline{\gamma} \in \underline{K}_u$, we find with $a \in K[x]$ with $\deg a < E_u F_u$ such that $\underline{a(\theta)} = \underline{\gamma}$;

We give auxiliary algorithms for the computation of $v_t(a) = v(a(\theta))$ for $\theta \in \Theta_u$, the Newton polygon of Φ with respect to φ, polynomials with given valuations, the reduction of elements represented as power products of polynomials, and the computation of residues and residual polynomials.

We use Algorithm 6 (`Valuation`) to compute $v_L(a(\theta))$ for $\theta \in \Theta_u$. It follows from the discussions in sections 6.2.4 and 6.3.4 that to find $v_L(a(\theta))$ for $\theta \in \Theta_u$ we only need the type $t = ((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le u}$ and not θ. We thus obtain one of the valuations of polynomial rings as classified by MacLane in [ML36a]. We write $v_t(a)$ for the valuation computed by the algorithm and have $v_t(a) = v_{K_u}(a(\theta))$

Algorithm `Valuation`

Input: A local field L, type $((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le u}$ over L, and $a(x) \in L[x]$.

Output: Valuation $v_t(a)$.

- If $a \in L$: Return $v_L(a)$.
- Find the φ_{u-1}-expansion of $a(x) = \sum_{j=0}^{\lceil \deg a / \deg \varphi_u \rceil} a_j(x) \varphi_u^j(x)$.
- Return $\min \left\{ \texttt{Valuation}\left(L, ((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le u-1}, a_j\right) + j\lambda_{u-1} \;\middle|\; 1 \le i \le \lceil \frac{\deg a}{\deg \varphi_{u-1}} \rceil \right\}$

Algorithm 6. `Valuation`

Given a type t and $\frac{c}{d} \in \mathbb{Q}$ with $d | E_u$, Algorithm 7 (`PolynomialWithValuation`) returns a polynomial ψ such that $v_t(\psi) = \frac{c}{d}$ as described in the proof of Lemma 6.2 (also see [Pau10, Algorithm 14] or [GNP12, Section 4]).

Algorithm `PolynomialWithValuation`

Input: A type $((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le u}$ and $\frac{c}{d} \in \mathbb{Q}$ with $d | E_u$.

Output: $\psi(x) \in K[x]$ with $\deg \psi < \deg \varphi_u$ and $v_t(\psi(\theta)) = \frac{c}{d}$.

- If $d = 1$: Return π^c.
- If $d | E_{u-1}$: Return $\texttt{PolynomialWithValuation}\left(((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le u-1}, \frac{c}{d}\right)$.
- Find $0 \le s < e_u^+$ such that $sh_u \equiv \frac{c}{d} E_u \bmod e_u^+$.
- If $u = 1$: Return $\pi^{\frac{c}{d} - s\lambda_1} \varphi_1^s(x)$
- Return $\varphi_u^s(x) \cdot \texttt{PolynomialWithValuation}\left(((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le u-1}, \frac{c}{d} - s\lambda_u\right)$.

Algorithm 7. `PolynomialWithValuation`

Algorithm 8 (`NewtonPolygonSegments`) returns the set of segments of the Newton polygon of Φ with respect to φ as described in section 6.2.1 and 6.3.1.

Algorithm `NewtonPolygonSegments`

Input: A local field L, $\Phi \in L[x]$, a type $t = ((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le u}$ over L, and $\varphi \in \mathcal{O}_L[x]$

Output: Set of Segments S of the Newton polygon of Φ with respect to φ.

- Find the φ-expansion $\Phi = \sum_{i=0}^{m} a_i \varphi^i$ where $m = \lceil \deg \Phi / \deg \varphi \rceil$.
- Find $v_i = \texttt{Valuation}(L, t, a_i)$ for $0 \le i \le m$.
- Construct the lower convex hull of the set of points $\{(i, v_i) \mid 1 \le i \le m\}$.
- Return the set S of segments of this broken line.

Algorithm 8. `NewtonPolygonSegments`

In sections 6.2.5 and 6.3.5 we have described how a product $\prod_{i=1}^{u} \phi_i^{s_i}(x)$ can be reduced such that $s_i < e_i^+$ for $1 \le i \le u$. Algorithm 9 (`reduce`) conducts this reduction recursively. Because, for $1 \le i \le u$ the valuations of $\phi_i^{s_i}$ with $s_i < e_i^+$ are linearly independent, there is only one reduced representation of each class of some $a \in L[x]$ with respect to the equivalence relation from Definition 2.12. Thus if $v_t(a) = 0$ then $\texttt{reduce}(a) \in L$. In the course of our algorithm, we find γ_u be such that $\varphi_u^{e_u^+} \sim \gamma_u \psi_u$.

Algorithm `reduce`

Input: An extended type $((\varphi_i, \lambda_i, \psi_i, \underline{\rho}_i))_{1 \le i \le u}$ and $a(x) = \varphi_u^{r_u} \cdot \prod_{i=1}^{u-1} \varphi_i^{r_i} \cdot \delta \in L[x]$ with $\delta \in K$.

Output: $b(x) = \varphi_u^{s_u} c(x) \in L[x]$ with $\deg c < \deg \varphi_u$, $0 \le s_u < e_u^+$, and $a(\theta) \sim b(\theta)$ for $\theta \in \Theta_u$.

- If $a \in L$: Return a.
- $s, d \leftarrow \texttt{divmod}(r_u, e_u^+)$
- $\gamma_u \leftarrow \texttt{representation}(t, \underline{\gamma})$ where $\underline{\gamma}$ is a root of $\underline{\rho}_u$.
- Return $\varphi_u^s \cdot \texttt{reduce}\left(((\varphi_i, \lambda_i, \psi_i, \underline{\rho}_i))_{1 \le i \le u-1}, \gamma_u^d \cdot \psi_u^d \cdot \prod_{i=1}^{u-1} \varphi_i^{r_i} \cdot \delta\right)$.

Algorithm 9. `reduce`

The residual polynomial of a segment of a Newton polygon of higher order is computed in Algorithm 10 (`ResidualPolynomial`).

Algorithm `ResidualPolynomial`

Input: A type $((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le u}$, a segment S of the Newton polygon of Φ with respect to φ, and ψ with $v_t(\psi) = e^+ v_t(\varphi)$ where $e^+ = \operatorname{lcm}\{E_u, e\}/E_u$ and $-h/e$ is the slope of S.

Output: The residual polynomial $\underline{A}$ of S.

- Let $\Phi = \sum_{i=0}^{\lceil N/\deg \varphi_u \rceil} a_i \varphi^i$ be the φ-expansion of $\Phi(x)$.
- Let m be the length of S.
- $\tau \leftarrow$ `PolynomialWithValuation`(t, ν) where ν is the y-coordinate of the first point of S.
- $\underline{A}(z) \leftarrow \sum_{j=0}^{m/e^+}$ `residue`$(t,$ `mult`$(t, a_{k+je^+}(x),$ `div`$(t,$ `pow`$(t, \psi(x), j), \tau(x))))z^j$.
- Return $\underline{A}$.

Algorithm 10. `ResidualPolynomial`

We use Algorithm 11 (`NextApproximation`) to construct the next approximation to an irreducible factor of Φ, following the logic of sections 6.2.3 and 6.3.3. Because we have defined the methods `mult` and `pow` so that they return polynomials that have been reduced to appropriately bounded degrees, we do not directly call `reduce`.

Algorithm `NextApproximation`

Input: An extended type $t = ((\varphi_i, \lambda_i, \psi_i, \underline{\rho}_i))_{1 \le i \le u}$, where $\underline{\rho}_u = \sum_{i=0}^{f_u} \underline{r}_i z^i$

Output: $\varphi \in \mathcal{O}_K[x]$ with $v(\varphi(\theta)) > v(\varphi_u(\theta))$ and $\deg \varphi = E_u F_u$

- $b_i \leftarrow$ `mult` $(t,$ `representative`$(t, \underline{r}_i),$ `pow`$(t, \psi_u, f_u - i))$ for $0 \le i < f_u$.
- Return $\varphi_u^{e_u f_u} + \sum_{i=0}^{F_u - 1} b_i \varphi_u^{i e_u}$.

Algorithm 11. `NextApproximation`

6.4.1 OM Tree

The main algorithm computes a complete and optimal type for every irreducible factor of Φ. In our algorithm we use the empty type t_0, which is the sequence of length zero, as the root of the tree of approximations. In the pseudocode below t_0 is the empty type, which corresponds to the set Θ of all roots of Φ, L is the list of complete, optimal types, and T is the stack of types to process.

Algorithm `OMTree`

Input: $\Phi \in \mathcal{O}_K[x]$ monic and square-free.

Output: Set of all complete optimal types L of Φ.

- Initialize $L \leftarrow \{\ \}$ and $T \leftarrow \{t_0\}$
- While T is non-empty:
  - Choose t from T and remove t from T.
  - $\varphi \leftarrow$ `NextApproximation` (t)
  - For $S \in$ `NewtonPolygonSegments` $(\Phi, t, \varphi))$:
    - Let $\lambda = -h/e$ be the slope of S.
    - $e^+ \leftarrow \operatorname{lcm}\{E_u, e\}/E_u$.
    - $\psi \leftarrow$ `PolynomialWithValuation`$(t, e^+ v_t(\varphi))$.
    - For each factor $\underline{\rho}(z)$ of `ResidualPolynomial` (t, S, ψ):
      - If the length of S is one: [t is complete and optimal]
        - Insert t into L.
      - Else if $e_u f_u = 1$: [this is an improvement step]
        - Insert t with its last member replaced by $(\varphi, \lambda, \psi, \underline{\rho}(z))$ into T.
      - Else: [this is a Montes step]
        - Insert t with $(\varphi, \lambda, \psi, \underline{\rho}(z))$ appended into T.
- Return L.

Algorithm 12. `OMTree`

The termination of the algorithm is assured by the following theorem.

Theorem 6.9 ([Pau01, Proposition 4.1])**.** *Let $\Phi \in \mathcal{O}_K[x]$ be square-free and let Θ_0 be the set of zeros of Φ in $\overline{K}$. Let $\varphi \in K[x]$ such that the degree of any irreducible factor of Φ is greater than or equal to $\deg \varphi$. If $(\deg \Phi) \cdot v(\varphi(\theta)) > 2v(\operatorname{disc} \Phi)$ for all $\theta \in \Theta_0$ then $\deg \varphi = \deg \Phi$ and Φ is irreducible over K.*

By Theorem 6.9 the polynomial Φ is irreducible if we find a monic $\varphi \in \mathcal{O}_K[x]$ such that $(\deg \Phi)v(\varphi_u) > 2v(\operatorname{disc} \Phi)$ for some $u \in \mathbb{Z}^{>0}$. In every iteration of the algorithm the increase from $v(\varphi_u)$ to $v(\varphi_{u+1})$ is at least $1/(\deg \Phi)$. Thus the algorithm terminates after at most $v(\operatorname{disc} \Phi)$ iterations.

6.5 Polynomial Factorization Example

We have implemented an OM algorithm for polynomial factorization as described in [Pau10] along with the single factor lifting method from [GNP12] in the computer algebra system Sage [S$^+$14]. We now describe in the flow of Algorithm 12 the process of factoring $\Phi = x^6+3x^4+6x^3+9x+9 \in \mathbb{Z}_3[x]$.

We begin with an empty type. Our first approximation is $\varphi_1 = x$. The φ_1-expansion of Φ is $\Phi = \sum_{i=0}^{6} a_i x^i$. The valuations of the coefficients are $v(a_0) = 2, v(a_1) = 2, v(a_3) = 1, v(a_4) = 1, v(a_5) = \infty$, and $v(a_6) = 0$. This gives us a Newton polygon with one segment of slope $-\frac{1}{3}$ (see Figure 5). We now have that $e_1^+ = 3$ and $v_t(\varphi_1) = \lambda_1 = \frac{1}{3}$. Next, we find a polynomial ψ_1 with valuation $e_1^+ v_t(\varphi_1) = 1$. So $\psi_1 = 3$. The residual polynomial of our one segment is $z^2 + 2z + 1 = (z+1)^2$, so $\underline{\rho}_1 = z + 1$. We proceed with one extended type in our set $(x, \frac{1}{3}, 3, z+1)$.

The next approximation we find is $\varphi_2 = x^3 - 6$. The φ_2-expansion of Φ is $\Phi = \varphi_2^2 + (3x+18)\varphi_2 + (27x+81)$. The valuations of the coefficients are $v(a_0) = \min\{3+\frac{1}{3}, 4\} = \frac{10}{3}, v(a_1) = \min\{1+\frac{1}{3}, 2\} = \frac{4}{3}$, and $v(a_2) = 0$. This gives us a higher order Newton polygon with two segments (Figure 5), one of slope -2 and one of slope $-\frac{4}{3}$.

Let S be the segment of slope -2. We set $\lambda_2 = 2$. As the denominator of the slope is 1 and $E_1 = 3$, we get $e_2^+ = 1$. We find ψ_2 with valuation $e_2^+ v_t(\varphi_2) = 2$, which gives us $\psi_1 = 3^2$. The residual polynomial is just $z + 1$, so $\underline{\rho}_2 = z + 1$. This segment has length 1, so we add $(x^3 - 6, 2, 3^2, z + 1)$ to our list of complete extended types to return.

Let S be the segment of slope $-\frac{4}{3}$. We set $\lambda_2 = \frac{4}{3}$. As the denominator of the slope is 3 and $E_1 = 3$, we get $e_2^+ = 1$. We find ψ_2 with valuation $e_2^+ v_t(\varphi_2) = \frac{4}{3}$, which gives us $\psi_1 = 3\varphi_1 = 3x$. The residual polynomial is just $z + 1$, so $\underline{\rho}_2 = z + 1$. This segment has length 1, so we add $(x^3 - 6, \frac{4}{3}, 3x, z + 1)$ to our list of complete extended types to return.

To create a factorization, we call `NextApproximation` on each of the returned types, and lift those to factors [GNP12]. The next approximations of our type where $\lambda_2 = 2$ is $x^3 - 24$, which lifts to $x^3 + 3$, For the type with $\lambda_2 = \frac{4}{3}$, we get $x^3 - 6x - 6$, which lifts to $x^3 + 3x + 3$. So, $\Phi = (x^3 + 3)(x^3 + 3x + 3)$.

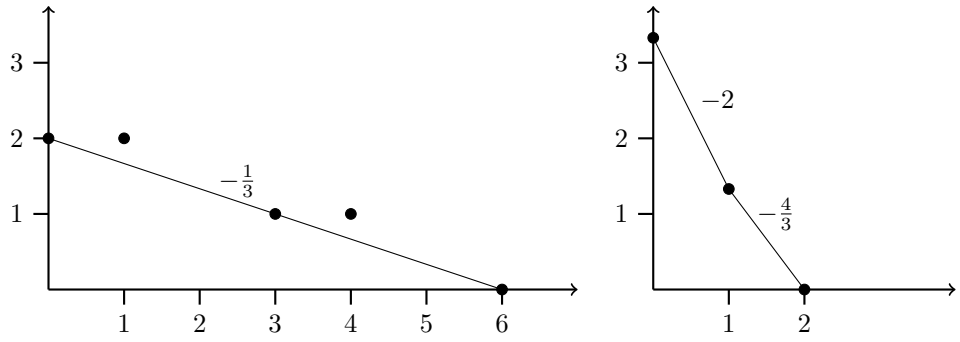


Figure 5. Newton Polygons of $\Phi(x) = x^6 + 3x^4 + 6x^3 + 9x + 9 \in \mathbb{Z}_3[x]$.

6.6 Okutsu Invariants

We now describe the polynomial invariants of Okutsu [Oku82] and how they relate to the values found in an OM algorithm. The connection between the algorithm and these invariants was first explored in [GMN10b] and in many papers since.

Definition 6.10 ([Oku82, II, Definitions 1 and 2])**.** Let $\Phi \in \mathcal{O}_K[x]$ be irreducible and θ be a root of Φ. We recursively define

$$m_0 = \deg \Phi, \tag{6.4}$$

$$\mu_u = \max\{v(\theta - \beta) \mid \beta \in \overline{K} \text{ such that } [K(\beta) : K] < m_{u-1}\}, \tag{6.5}$$

$$m_u = \min\{[K(\alpha) : K] \mid \alpha \in \overline{K} \text{ such that } v(\theta - \alpha) = \mu_u.\} \tag{6.6}$$

The minimal polynomial $\chi_u \in \mathcal{O}_K[x]$ of α with $v(\theta - \alpha) = \mu_u$ is called an u-th primitive divisor polynomial of Φ.

These divisor polynomials are not invariant, but properties of the extensions they generate are. We state a reformulation of Corollary 2.8 from [GMN10b].

Theorem 6.11. *Let $(\varphi_1, \ldots, \varphi_r)$ be a sequence of primitive divisor polynomials of a monic, irreducible, and separable $\Phi \in \mathcal{O}_K[x]$. Let θ be a root of Φ, $L = K(\theta)$, and $K_i = K(\alpha_i)$ where α_i is a root of φ_i. Then $E_i = e(K_i/K)$, $F_i = f(K_i/K)$, and $\lambda_i = v(\varphi_i(\theta))$ do not depend on the choice of frame. Furthermore, $E_r \mid \cdots \mid E_1 \mid e(L/K)$ and $F_r \mid \cdots \mid F_1 \mid f(L/K)$.*

Definition 6.12. An *Okutsu invariant* of Φ is any rational number that depends only on $E_1, \ldots, E_r$ and $F_1, \ldots, F_r$ and $\lambda_1, \ldots, \lambda_r$. An *OM algorithm* is an algorithm that computes the Okutsu invariants of a polynomial.

There are several useful examples of Okutsu invariants. As we have shown, the ramification index and residual degree of $L = K[x]/(\Phi)$ are given by these values. Additionally, the index [GNP12, Proposition 3.5], the exponent [GMN13, Theorem 5.2], and the the conductor [Nar14, Corollary 1.9] of Φ are all Okutsu invariants. Although the different and discriminant are not Okutsu invariants, the different ideal and thus the valuation of the discriminant can be computing using OM methods [Nar14].

In [GMN10b], Guardia, Montes, and Nart show that a sequence of primitive divisor polynomials and a sequence of polynomials $(\varphi_i)_i$ from a type are equivalent. In their formulation, they define an *Okutsu frame* which reorganizes the sequence into increasing degree order to agree with the progression of approximations in a type.

Proposition 6.13. *Let $t = ((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le u}$ be a Φ-complete and optimal type, as returned by Algorithm 12, then φ_i is a $(u-i)$-th primitive divisor polynomial of Φ.*

6.7 Polynomials with Given Okutsu Invariants

An OM algorithm typically computes the Okutsu invariants of a polynomial, but here we present an algorithm that computes a polynomial given a sequence of Okutsu invariants. Our algorithm uses the same methods previously used to describe an OM algorithm. We need one result, originally shown as a consequence of the construction presented in [GMN13].

Theorem 6.14. *Let $t = ((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le u}$ be an optimal type of Φ and Θ_u the corresponding subset of the roots of Φ and $\varphi_{u+1} = \texttt{NextApproximation}(t)$ the next approximation to an irreducible factor of Φ. Then t is a complete optimal type of φ_{u+1}.*

One consequence of this theorem is that each φ_i in a type $((\varphi_i, \lambda_i, \underline{\rho}_i))_{1 \le i \le u}$ is irreducible. Another is that if we have valid data for the other information in a type, we can construct polynomials having that type. With this in mind, our algorithm takes as input a sequence of valuations for approximations $(\lambda_i)_{1 \le i \le u}$ and a sequence of irreducible polynomials $(\underline{\rho}_i)_{1 \le i \le u}$ over $\underline{K}$, which encode

the Okutsu invariants, constructs a type $((\varphi_i, \lambda_i, \underline{\rho}_i))_{1\le i\le u}$ having these values, and concludes by generating φ_{u+1}.

Algorithm `PolynomialWithInvariants`

Input: A sequence of rational numbers $(\lambda_i)_{1\le i\le u}$, where $\lambda_i = h_i/e_i$ and a sequence of irreducible polynomials $(\underline{\rho}_i)_{1\le i\le u}$ in $\underline{K}[x]$ where $f_i = \deg \underline{\rho}_i$. Additionally, we require $\lambda_i \ge e_i f_i \lambda_{i-1}$.

Output: A polynomial Φ having the given Okutsu invariants $E_i = \operatorname{lcm}\{e_1, \dots, e_i\}$, $F_i = \deg \underline{\rho}_1 \cdots \underline{\rho}_i$, and λ_i for $1 \le i \le u$.

- $t \leftarrow (x, \lambda_1, \underline{\rho}_1)$.
- Make t an extended type by including $\psi_1 = \pi^{h_1}$.
- For $2 \le i \le u$:
  - Append $(\texttt{NextApproximation}(t), \lambda_i, \underline{\rho}_i)$ to t.
  - $e^+ \leftarrow \operatorname{lcm}\{e_1, \dots, e_i\}/\operatorname{lcm}\{e_1, \dots, e_{i-1}\}$.
  - $\psi_i \leftarrow \texttt{PolynomialWithValuation}(t, e^+\lambda_i)$.
  - Make t an extended type by including ψ_i.
- Return $\texttt{NextApproximation}(t)$.

Algorithm 13. `PolynomialWithInvariants`

Example 6.15. Let us find a polynomial $\Phi \in \mathbb{Z}_3[x]$ having $(\lambda_i) = (\frac{1}{4}, \frac{5}{4}, \frac{27}{8})$ and $(\underline{\rho}_i) = (x+1, x^2+1, x+1)$. We begin with $\varphi_1 = x$ and $\psi_1 = 3^1$ and start the main loop.

- $i = 2$
  - `NextApproximation` gives us $\varphi_2 = x^4 - 6$.
  - $e^+ = 4$.
  - $\psi_2 = 3^1 x^1$.
- $i = 3$
  - `NextApproximation` gives us $\varphi_3 = x^8 - 12x^4 + 9x^2 + 36$.
  - $e^+ = 1$.
  - $\psi_3 = 3^6 x^3$.

Finally, $\Phi(x) = x^{16} - 24x^{12} + 18x^{10} + 216x^8 - 216x^6 - 783x^4 + 729x^3 + 658x^2 + 1296$. This polynomial has the given Okutsu invariants and generates an extension over $\mathbb{Q}_3$ with inertia degree 2 and ramification index 8.

REFERENCES

[Ama71] Shigeru Amano, *Eisenstein equations of degree p in a* $\mathfrak{p}$*-adic field*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **18** (1971), 1–21. MR 0308086 (46 #7201)

[AS13] Chad Awtrey and Christopher R. Shill, *Galois groups of 2-adic fields of degree 12 with automorphism group of order 6 and 12*, Topics from the 8th Annual UNCG Regional Mathematics and Statistics Conference, Springer Proceedings in Mathematics & Statistics **64** (2013), 55–65.

[AS15] Chad Awtrey and Erin Strosnider, *A linear resolvent for degree 14 polynomials*, Topics from the 9th Annual UNCG Regional Mathematics and Statistics Conference, Springer Proceedings in Mathematics & Statistics **109** (2015), 43–50.

[Bau07] Mihály Bauer, *Zur allgemeinen Theorie der algebraischen Grössen*, Journal für die reine und angewandte Mathematik **132** (1907), 21–32.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

[BHN32] Richard Brauer, Helmut Hasse, and Emmy Noether, *Beweis eines Hauptsatzes in der Theorie der Algebren*, J . Reine Angew. Math. **167** (1932), 399–404.

[BNS13] Jens-Dietrich Bauch, Enric Nart, and Hayden D. Stainsby, *Complexity of OM factorizations of polynomials over local fields*, LMS J. Comput. Math. **16** (2013), 139–171. MR 3081769

[CG00] David G. Cantor and Daniel M. Gordon, *Factoring polynomials over p-adic fields*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 185–208. MR 1850606 (2002f:11175)

[Che33a] Claude Chevalley, *La thórie du symbole de restes normiques*, J. Reine Angew. Math. **169** (1933), 140–157, C. Chevalley, La the'one du symbole de restes normzques. J. Reine Angew. Math., 169 (1933), 140-157.

[Che33b] ———, *Sur la théorie du corps des classes dans les corps finis et les corps locaux*, J. Fac. Sci. Univ. Tokyo Sect. I **2** (1933), 365–476, C. Chevalley, Sur la the'one du corps des classes dans les corps finzs et les corps locaux. J. Fac. Sci. Univ. Tokyo, Sect.1 vo1.2 (1933), 365-476.

[FL94] David Ford and Pascal Letard, *Implementing the round four maximal order algorithm*, J. Théor. Nombres Bordeaux **6** (1994), no. 1, 39–80. MR 1305287 (96d:11141)

[For87] David J. Ford, *The construction of maximal orders over a Dedekind domain*, J. Symbolic Comput. **4** (1987), no. 1, 69–75. MR 908413 (89a:11121)

[FPR02] David Ford, Sebastian Pauli, and Xavier-François Roblot, *A fast algorithm for polynomial factorization over* $\mathbb{Q}_p$, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 151–169. MR 1925995 (2003g:11134)

[FeVo02] Ivan B. Fesenko and Sergey V. Vostokov, *Local fields and their extensions*, 2nd ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, 2002.

[FoVe10] David J. Ford and Olga Veres, *On the complexity of the Montes ideal factorization algorithm*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 174–185. MR 2721420 (2011m:11249)

[GMN10a] Jordi Guárdia, Jesús Montes, , and Enric Nart, *Arithmetic in big number fields: the '+ideals' package*, ArXiv e-prints (2010), arXiv:1005.4596 [math.NT].

[GMN10b] Jordi Guàrdia, Jesús Montes, and Enric Nart, *Okutsu invariants and newton polygons*, Acta Arithmetica **145** (2010), 83–108.

[GMN11] _____, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, J. Théor. Nombres Bordeaux **23** (2011), no. 3, 667–696. MR 2861080

[GMN12] _____, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416. MR 2833586 (2012k:11185)

[GMN13] _____, *A new computational approach to ideal theory in number fields*, Found. Comput. Math. **13** (2013), no. 5, 729–762. MR 3105943

[GNP12] Jordi Guàrdia, Enric Nart, and Sebastian Pauli, *Single-factor lifting and factorization of polynomials over local fields*, J. Symbolic Comput. **47** (2012), no. 11, 1318–1346. MR 2927133

[GP12] Christian Greve and Sebastian Pauli, *Ramification polygons, splitting fields, and Galois groups of Eisenstein polynomials*, International Journal of Number Theory **8** (2012), no. 6, 1401–1424. MR 2965757

[Has30] Helmut Hasse, *Die Normenresttheorie relativ-abelscher Zahlkörper als Klassenkörpertheorie im Kleinen*, Journal für die reine und angewandte Mathematik **162** (1930), 145–154.

[Has33] _____, *Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper. Insbesondere Begründung des Normenrestsymbols und die Herleitung des Reziprozitätsgesetzes mit nichtkommutativen Hilfsmitteln*, Math. Annalen. **107** (1933), 731–760.

[Hel90] Charles Helou, *Non-Galois ramification theory of local fields*, Algebra Berichte [Algebra Reports], vol. 64, Verlag Reinhard Fischer, Munich, 1990. MR 1076620 (91j:11103)

[Hen97] Kurt Hensel, *Über eine neue Begründung der Theorie der algebraischen Zahlen*, Jahresbericht der Deutschen Mathematiker-Vereinigung **6** (1897), 83–88.

[Hen08] _____, *Theorie der Algebraischen Zahlen*, B. G. Teubner, Leipzig, Berlin, 1908.

[JR06] John W. Jones and David P. Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. MR 2194887 (2006k:11230)

[JR07] _____, *Galois number fields with small root discriminant*, J. Number Theory **122** (2007), no. 2, 379–407. MR 2292261 (2008e:11140)

[JR08] ———, *Octic 2-adic fields*, J. Number Theory **128** (2008), no. 6, 1410–1429. MR 2419170 (2009d:11163)

[Kra66] Marc Krasner, *Nombre des extensions d'un degré donné d'un corps* $\mathfrak{p}$*-adique*, Les Tendances Géom. en Algèbre et Théorie des Nombres, Editions du Centre National de la Recherche Scientifique, Paris, 1966, pp. 143–169. MR 0225756 (37 #1349)

[Kür12] József Kürschák, *Über Limesbildung und allgemeine Körpertheorie*, Proceedings of the 5th International Congress of Mathematicians Cambridge 1912 **1** (1912), 285–289.

[Kür13] ———, *Über Limesbildung und allgemeine Körpertheorie*, Journal für die reine und angewandte Mathematik **142** (1913), 211–263.

[Li97] Hua-Chieh Li, *p-adic power series which commute under composition*, Transactions of the American Mathematical Society **349** (1997), no. 4, 1437–1446.

[Lub81] Jonathan D. Lubin, *The local Kronecker-Weber theorem*, Transactions of the American Mathematical Society **267** (1981), no. 1, 133–138.

[ML36a] Saunders Mac Lane, *A construction for absolute values in polynomial rings*, Transactions of the American Mathematical Society **40** (1936), no. 3, 363–395.

[ML36b] ———, *A construction for prime ideals as absolute values of an algebraic field*, Duke Mathematcial Journal **2** (1936), 492–510.

[MN92] Jesús Montes and Enric Nart, *On a theorem of Ore*, J. Algebra **146** (1992), no. 2, 318–334. MR 1152908 (93f:11077)

[Mon99] Jesús Montes, *Poligonos de Newton de orden superior y aplicaciones aritmeticas*, 1999, Thesis (Ph.D.)–Universitat de Barcelona.

[Mon14] Maurizio Monge, *A family of Eisenstein polynomials generating totally ramified extensions, identification of extensions and construction of class fields*, Int. J. Number Theory **10** (2014), no. 7, 1699–1727. MR 3256847

[MPS15] Jonathan Milstead, Sebastian Pauli, and Brian Sinclair, *Constructing splitting fields of polynomials over local fields*, Topics from the 9th Annual UNCG Regional Mathematics and Statistics Conference, Springer Proceedings in Mathematics & Statistics **109** (2015), 101–124.

[Nar14] Enric Nart, *Local computation of differents and discriminants*, Math. Comp. **83** (2014), 1513–1534.

[Oku82] Kousaku Okutsu, *Construction of integral basis, I-IV*, Proc. Jpn. Acad. Ser. A **58** (1982), 47–49, 87–89, 117–119, 167–169.

[Ore24] Öystein Ore, *Zur Theorie der algebraischen Körper*, Acta Mathematica **44** (1924), 219–314.

[Ore26] ———, *Bemerkungen zur Theorie der Differente*, Math. Z. **25** (1926), no. 1, 1–8. MR 1544795

[Ore28] ———, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), no. 1, 84–117 (German). MR 1512440

[Ost13] Alexander Ostrowski, *Über einige Fragen der allgemeinen Körpertheorie*, Journal für die reine und angewandte Mathematik **143** (1913), 211–253.

[Ost17] ———, *Über sogenannte perfekte Körper*, Journal für die reine und angewandte Mathematik **147** (1917), 191–204.

[Ost18] ———, *Über einige Lösungen der Funktionalgleichung* $\psi(x)\psi(y) = \psi(xy)$, Acta Mathematica **41** (1918), no. 1, 271–284.

[Pan95] Peter Panayi, *Computation of Leopoldt's p-adic regulator*, 1995, Thesis (Ph.D.)–University of East Anglia.

[Pau01] Sebastian Pauli, *Factoring polynomials over local fields*, J. Symbolic Comput. **32** (2001), no. 5, 533–547. MR 1858009 (2002h:13038)

[Pau06] ———, *Constructing class fields over local fields*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 627–652. MR 2330432 (2008f:11135)

[Pau10] ———, *Factoring polynomials over local fields II*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 301–315. MR 2721428 (2012c:12002)

[PG14] The Pari Group, *Pari/GP version* `2.7.0`, Bordeaux, 2014, available from `http://pari.math.u-bordeaux.fr/`.

[PR01] Sebastian Pauli and Xavier-François Roblot, *On the computation of all extensions of a p-adic field of a given degree*, Math. Comp. **70** (2001), no. 236, 1641–1659 (electronic). MR 1836924 (2002e:11166)

[PS14] Sebastian Pauli and Brian Sinclair, *Enumerating extensions of* (π)*-adic fields with given invariants*, (preprint) (2014).

[S+14] William A. Stein et al., *Sage Mathematics Software (Version 6.4.1)*, The Sage Development Team, 2014, `http://www.sagemath.org`.

[Sch03] John Scherk, *The ramification polygon for curves over a finite field*, Canad. Math. Bull. **46** (2003), no. 1, 149–156. MR 1955622 (2004c:11220)

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 (82e:12016)

[Sin15] Brian Sinclair, *Counting extensions of* (π)*-adic fields with given invariants*, (preprint) (2015).

[Ste10] Ernst Steinitz, *Algebraische Theorie der Körper*, J. Reine Angew. Math. **137** (1910), 167–309.

[Ver09] Olga Erzsebet Veres, *On the complexity of polynomial factorization over p-adic fields*, ProQuest LLC, Ann Arbor, MI, 2009, Thesis (Ph.D.)–Concordia University (Canada). MR 2941451

[Zas69] Hans Zassenhaus, *On Hensel factorization I*, J. Number Theory **1** (1969), 291–311.