MILSTEAD, JONATHAN, Ph.D. Computing Galois Groups of Eisenstein Polynomials Over P-adic Fields. (2017)
Directed by Dr. Sebastian Pauli. 190 pp.

The most efficient algorithms for computing Galois groups of polynomials over global fields are based on Stauduhar's relative resolvent method. These methods are not directly generalizable to the local field case, since they require a field that contains the global field in which all roots of the polynomial can be approximated. We present splitting field-independent methods for computing the Galois group of an Eisenstein polynomial over a p-adic field. Our approach is to combine information from different disciplines. We primarily, make use of the ramification polygon of the polynomial, which is the Newton polygon of a related polynomial. This allows us to quickly calculate several invariants that serve to reduce the number of possible Galois groups. Algorithms by Greve and Pauli very efficiently return the Galois group of polynomials where the ramification polygon consists of one segment as well as information about the subfields of the stem field. Second, we look at the factorization of linear absolute resolvents to further narrow the pool of possible groups.

COMPUTING GALOIS GROUPS OF EISENSTEIN POLYNOMIALS OVER P-ADIC FIELDS

by

Jonathan Milstead

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
2017

Approved by

_____
Committee Chair

APPROVAL PAGE

This dissertation written by Jonathan Milstead 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 _____
Chad Awtrey

_____
Talia Fernos

_____
Dan Yasaki

_____
Date of Acceptance by Committee

_____
Date of Final Oral Examination

ACKNOWLEDGMENTS

I would like to thank my advisor, Dr. Pauli, for his patience, support and guidance. Dr. Pauli has been very committed to my growth as a Mathematician and I will be forever in his debt. I would like to thank my committee, Dr. Awtrey, Dr. Yasaki, and Dr. Fernos for the time and effort they spent assisting me in my studies over the years. Dr. Awtrey has been especially helpful as a source of immense knowledge in many areas vital to my research. I would also like to thank Sandi Rudzinkski for providing some of the proofs for Chapter IV, and Brian Sinclair for creating some examples for Chapter III.

Words alone cannot sufficiently convey how blessed I have been to be a part of the Mathematics Department at UNCG. Thank you.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

CHAPTER I

INTRODUCTION

For a given rational prime p, the field of p-adic numbers $\mathbb{Q}_p$ is a completion of the rational numbers in which two elements are considered "close" if their difference is divisible by a large power of p. This field was introduced in 1897 by Kurt Hensel [41]. Hensel created this number system in an effort to apply some of the tools from complex analysis to solving problems in number theory. Central to his motivation was the keen observation that the expansion of a complex number as a Laurent series is analogous to the p-adic expansion of a rational number, that is the representation of $t \in \mathbb{Q}$ as a linear combination of powers of p. In the years since, p-adic numbers have been applied to numerous disciplines including elliptic curves and Diophantine equations. They, notably, play a role in Andrew Wiles's proof of Fermat's Last Theorem [31].

Much of the current research into p-adic numbers centers around the classification of p-adic fields, finite extensions of $\mathbb{Q}_p$. As the following theorem indicates, this can theoretically be done for all extensions of any finite degree.

Theorem 1.1 ([52, Section 2.5])**.** *Let* K *be a finite extension of* $\mathbb{Q}_p$*, and let* n *be any positive integer. There exist only finitely many extensions of* K *of degree* n*.*

Principally, research on this topic has focused on classifying degree $n > 0$ extensions of a p-adic field by computing a generating polynomial for each extension as well as the polynomial's Galois group. Whereas efficient, general algorithms exist for determining generating polynomials for p-adic extensions of a given degree (see

[67], [68]), the same cannot be said for computing the Galois groups of these generating polynomials. Although explicit methods have been developed for degree n extensions with $p \nmid n$ (see for example [39]) or $n = p$ (see for example [73]), no general algorithms are known for determining Galois groups of polynomials over p-adic fields.

The importance of developing more general algorithms for computing Galois groups in this context can be reinforced by two observations: the sheer difficulty in performing this task and the fact that it will allow others to greatly increase the pool of knowledge of p-adic fields through the classification efforts mentioned above.

Previous algorithms for computing Galois groups of p-adic fields were restricted either to extensions of low degree (up to 15) or to polynomials of special form. Algorithms for degrees up to 11 were given by Jones and Roberts [46][47][45] and were followed by methods for polynomials of degree 12, 14, and 15 by Awtrey and others [3][4][5][6][9]. All of these use a variety of criteria for narrowing down the possible Galois groups, including information about the ramification filtration and absolute resolvents. The algorithms for computing Galois groups of Eisenstein polynomials make use of the information contained in the ramification polygon, that is the Newton polygon of the ramification polynomial, to obtain information about the splitting field of φ. Romano [73] describes $\mathrm{Gal}(\varphi)$ for Eisenstein polynomials φ where the ramification polygon of φ has one segment and the only points on the segment are the endpoints. The algorithm by Greve and Pauli [33] very efficiently returns the Galois group of polynomials where the ramification polygon of φ consists of one segment. In his thesis [32] Greve builds on this approach to give an algorithm for Eisenstein polynomials whose ramification polygon consists of two segments.

We combine ideas from all the above approaches in an algorithm that determines the Galois group $\mathrm{Gal}(\varphi)$ of an Eisenstein polynomial $\varphi \in \mathbb{Z}_p[x]$, where $\mathbb{Z}_p$ denotes the ring of integers of $\mathbb{Q}_p$. For many previously-solved cases such as Greve and Pauli's one-segment method, our algorithm is competitive if not noticeably faster. For Eisenstein polynomials whose ramification polygons consist of two or more segments, our algorithm has been successfully applied to numerous examples with degree as high as 27, a number of which correspond to the three segment case. Recently, our method has been successfully applied to polynomials whose ramification polygons have four segments. This is a clear improvement on previous algorithms that utilized ramification polygons, since those methods didn't deal with ramification polygons that had three or more segments.

Many of the results we utilize are applicable to Eisenstein polynomials over any p-adic field. Because of this, we discuss these results in more general terms. It is our hope that these results will serve as building blocks for future work in this field.

1.1 Summary of Content

The primary purpose of Chapter II is to provide the reader with the local field theory that is pertinent to the material in the later chapters of this thesis. We begin by defining local fields and the associated concepts of valuation and absolute value. From there, we convey the core definitions and facts regarding extensions of local fields. Following a brief discussion of Hensel lifting and Newton polygons, we delve further into the topic of totally ramified extensions with special attention given to tamely ramified extensions and their Galois groups. Finally, we conclude this chapter's background information with an examination of ramification groups.

We close the second chapter with a presentation of our new method for finding the compositum of tamely ramified extensions over a common field. This constructive method quickly determines concrete generating polynomials, for the additional extensions needed, without relying on expensive factoring and/or root finding routines.

It is in the third chapter that we begin discussing Eisenstein polynomials in earnest. In particular, we principally examine two invariants of the extension generated by an Eisenstein polynomial: the ramification polygon and the (related) residual polynomial classes. The first two sections of this chapter define and convey basic facts about the two invariants. After that, the bulk of the chapter is dedicated to explaining some of the results of Christian Greve's doctoral research [32][33]. The third section describes how the ramification polygon of an Eisenstein polynomial φ gives way to a collection of blocks that can be used to construct a chain of subfields of the extension generated by φ. In the following section, we examine how invariants of these subfields relate to the invariants of the extension that φ generates. Next, over the course of two sections, we address how Greve was able to compute the splitting field and the Galois group for an Eisenstein polynomial whose ramification polygon is comprised of a single segment. In the seventh section, we consider splitting field information that can be determined for an Eisenstein polynomial whose ramification polygon has more than one segment.

We close the third chapter with a section that details how we have expanded upon the collection of blocks mentioned above. While Greve considered blocks defined solely by the slopes of the ramification polygon, we have found that additional blocks may be found by also using the residual polynomial classes. Additionally, we find

that for normal, totally ramified extensions we can refine the ramification filtration of the extension's Galois group.

Our fourth chapter focuses exclusively on resolvent polynomials. Following a brief section that establishes basic definitions and concepts, we begin our discussion of resolvents with a review of Stauduhar's classic method [82]. Once this method has been explained, we hone in on a couple of the approach's computational shortcomings. These are used to motivate our examination of aspects of more recent approaches [24, 29] to computing Galois groups with relative resolvents. Of particular interest to us is the possible use of a wreath product as the starting point.

Finally, we conclude Chapter IV with an implementation-centric sampling of the work of Leonard Soicher [80]. After providing background information on resultants, we focus on two topics that are utilized in Chapter V of this thesis: how the degrees of the irreducible factors of a resolvent aid in the determination of Galois groups, and how five specific absolute resolvents can be computed with resultants.

We present our algorithm for computing Galois groups of Eisenstein polynomials over $\mathbb{Q}_p$ in Chapter V. Our algorithm is made up of a series of iterative stages in each of which we compute the Galois group of a tower of two extensions. An outline of the algorithm, depicting this iterative behavior, is provided at the outset of the chapter. The exact steps taken in each iterative stage are given in the sections that follow.

We have also included three appendices that cover topics from Group theory that the reader must be familiar with when reading the main chapters of this thesis. The first appendix provides a list of key definitions and results concerning Galois groups over an arbitrary field. The second appendix covers the fundamentals of direct

and semidirect products while providing examples that are referenced in Chapters II and III. Finally, the third appendix briefly introduces the wreath product, a specific example of a semidirect product.

CHAPTER II

LOCAL FIELDS

The first five sections of this chapter provide the reader with an introduction to the rich subject of local fields. The topics include extensions of local fields, factoring techniques like Hensel Lifting, and ramification groups. Most of the information can be found in [78], [23], and [13].

The final section of this chapter is centered around a new and original method for computing composites of local field extensions of a certain type. The method we present is constructive and computationally inexpensive.

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 is called the *ultrametric inequality*. It is stronger than the better known triangle inequality of norms: $\|x + y\| \leq \|x\| + \|y\|$. Absolute values that fail to satisfy the ultrametric inequality are classified as *archimedian absolute values*.

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

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

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

Lemma 2.3. *Let v be a discrete valuation on the field K, and let $a, b \in \mathsf{K}$ with $v(a) \neq v(b)$. Then $v(a + b) = \min\{v(a), v(b)\}$.*

Proof. Without loss of generality, we assume that $v(a) > v(b)$. If we rewrite b as $b + a - a$, then we find that

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

In light of our opening assumption, the only way that the above inequality could be true would be for $v(a+b) < v(a)$ to hold. Thus we know that $v(b) \geq v(a+b)$. If we apply this to the final part of the last definition, we obtain

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

Therefore $v(a + b) = v(b)$. □

Definition 2.4. Let p be a rational prime. Every rational number r can be uniquely written in the form $r = p^k(a/b)$ where a and b are relatively prime, and neither are divisible by p. In this context, we have the following terminology:

- The *p-adic absolute value* on $\mathbb{Q}$ is the non-archimedian absolute value given by $\|r\|_p = p^{-k}$.
- The *p-adic valuation* on $\mathbb{Q}$ is the discrete valuation given by $v_p(r) = k$.
- The field $\mathbb{Q}_p$ of *p-adic numbers* is the completion of the rational numbers by $\|\cdot\|_p$.

Definition 2.5. A *local field* is a field complete with respect to a discrete non-archimedian absolute value.

Let K be a local field that is complete with respect to some non-archimedian absolute value $\|\cdot\|$. The *valuation ring* of K is the local ring

$$\mathcal{O}_\mathsf{K} = \{\alpha \in \mathsf{K} : \|\alpha\| \leq 1\}$$

whose unique, maximal ideal

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

is principal. Every element of K that generates $\mathfrak{p}$ is called a *prime element* or *uniformizer*. We write v_K for the valuation of K that is normalized such that $v_\mathsf{K}(\pi_\mathsf{K}) = 1$ where $\pi = \pi_\mathsf{K}$ is a uniformizing element in $\mathcal{O}_\mathsf{K}$. We define the *residue class field* of K to be the quotient

$$\underline{\mathsf{K}} = \mathcal{O}_\mathsf{K}/\mathfrak{p}.$$

For $\gamma \in \mathcal{O}_\mathsf{K}$ we denote by $\underline{\gamma}$ the class $\gamma + (\pi)$ in $\underline{\mathsf{K}} = \mathcal{O}_\mathsf{K}/(\pi)$, by $R_{\underline{\mathsf{K}}}$ a complete set of representatives of $\underline{\mathsf{K}}$ in $\mathcal{O}_\mathsf{K}$, and by $R_{\underline{\mathsf{K}}}^\times$ the set $R_{\underline{\mathsf{K}}}$ without the representative designated for $\underline{0} \in \underline{\mathsf{K}}$.

Every element $\gamma \in \mathsf{K}$ can be expressed as a linear combination of powers of π_{K}:

$$\gamma = \sum_{i=v_{\mathsf{K}}(\gamma)}^{\infty} a_i \pi_{\mathsf{K}}^i \text{ where } a_i \in \underline{\mathsf{K}}.$$

This sum is called the π_{K}-*adic expansion* of the element γ.

Example 2.6. If p is a prime number, then $\mathbb{Q}_p$ is a local field. The *p-adic integers*, denoted by $\mathbb{Z}_p$, is the set of elements of $\mathbb{Q}_p$ that have nonnegative p-adic valuation:

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : v_p(\alpha) \geq 0\}.$$

Since $v_p(\alpha) \geq 0$ implies that $\|\alpha\|_p \leq 1$, $\mathbb{Z}_p$ is the valuation ring of $\mathbb{Q}_p$. The sole maximal ideal of $\mathbb{Z}_p$ is generated by p which makes p a uniformizer of $\mathbb{Q}_p$. Furthermore, we have that $\mathbb{F}_p \cong \mathbb{Z}_p/(p)$ is the residue class field of $\mathbb{Q}_p$.

2.2 Extensions of Local Fields

Let K be a local field, and let φ be a monic and separable polynomial of degree n that is irreducible over K. We construct the algebraic extension $\mathsf{L} = \mathsf{K}(\alpha)$ by adjoining to K a single root α of φ. As such, $L \cong \mathsf{K}[x]/(\varphi)$ and L/K has degree n.

Definition 2.7. Let $\overline{\mathsf{K}}$ be an algebraic closure of K. Denote the roots of φ in $\overline{\mathsf{K}}$ by $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ where $\alpha^{(1)} = \alpha$. We say that $\alpha^{(i)}$ is the *i-th conjugate* of α.

By definition, our extension L/K is a dimension n vector space over K with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Every $\gamma \in \mathsf{L}$ can be uniquely written as a linear combination of basis elements:

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

For $1 \leq j \leq n$ we can write the j-th conjugate of γ as $\gamma^{(j)} = \sum_{i=0}^{n-1} g_i \left(\alpha^{(j)}\right)^i$. In this context, we define the *norm* of γ to be the product $\mathrm{N}_{\mathsf{L}/\mathsf{K}}(\gamma) = \prod_{j=1}^{n} \gamma^{(j)}$.

Theorem 2.8. *Let K be a local field with valuation v_{K}, and let L/K be a finite algebraic extension of degree n. Then there exists a unique extension of the valuation v_{K} to a valuation $v_{\mathsf{L}} : \mathsf{L} \to \mathbb{Q} \cup \{\infty\}$ with the restriction of v_{L} to K coinciding with v_{K}. The local field L is complete with respect to v_{L}. Finally, $v_{\mathsf{L}}(\gamma) = v_{\mathsf{K}}(\mathrm{N}_{\mathsf{L}/\mathsf{K}}(\gamma))/n$ for $\gamma \in \mathsf{L}$.*

To ease notation, this unique extension of $v = v_{\mathsf{K}}$ to a valuation on an algebraic closure $\overline{\mathsf{K}}$ of K (or to any intermediate field) is also denoted v. Below is an equivalence relation on $\overline{\mathsf{K}}$ that reflects our choice of notation.

Definition 2.9. For $\gamma \in \overline{\mathsf{K}}^{\times}$ and $\delta \in \overline{\mathsf{K}}^{\times}$ we write $\gamma \sim \delta$ if

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

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

$$\min{}_{0 \leq i \leq n}\, v(c_i - b_i) \;>\; \min{}_{0 \leq i \leq n}\, v(c_i).$$

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}. Then v_{L} denotes the valuation that is normalized such that $v_{\mathsf{L}}(\pi_{\mathsf{L}}) = 1$. Two elements $\gamma = \gamma_0 \pi_{\mathsf{L}}^u \in \mathsf{L}$ and $\delta = \delta_0 \pi_{\mathsf{L}}^w \in \mathsf{L}$ with $v(\gamma_0) = v(\delta_0) = 0$ are equivalent with respect to $\sim$ if and only if $u = w$ and $\gamma_0 \equiv \delta_0 \bmod (\pi_{\mathsf{L}})$.

Definition 2.10. A local field that is a finite extension of $\mathbb{Q}_p$ is called a *p-adic field*.

Definition 2.11. If L/K is an algebraic extension of degree n, then $\mathcal{O}_\mathsf{L}$ is a free $\mathcal{O}_\mathsf{K}$-module of degree n, and we say that a basis for $\mathcal{O}_\mathsf{L}$ over $\mathcal{O}_\mathsf{K}$ is an *integral basis* of L/K.

Definition 2.12. Let $\varphi \in \mathsf{K}[x]$ be a monic polynomial of degree n with factorization $\varphi(x) = \prod_{i=1}^{n}(x - \alpha^{(i)})$ in $\overline{\mathsf{K}}$. We define the *discriminant* of φ to be

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

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

Definition 2.13. 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 $\operatorname{disc}(\mathsf{L}/\mathsf{K}) = \left(\det(\delta_j^{(i)})\right)^2$.

Definition 2.14. Let L be an algebraic extension of K. If $[\mathsf{L} : \mathsf{K}] = [\underline{\mathsf{L}} : \underline{\mathsf{K}}]$, then L/K is *unramified*. If $[\underline{\mathsf{L}} : \underline{\mathsf{K}}] = 1$, then L/K is *totally ramified*.

For all $f \in \mathbb{N}$ there is, up to isomorphism, a unique unramified extension of K of degree f. Such an extension can be generated by any monic polynomial of degree f that is irreducible over $\underline{\mathsf{K}}$. All one would have to do is find some irreducible $\tau \in \underline{\mathsf{K}}[x]$ of the desired degree and then take some monic lift of τ to $\mathsf{K}[x]$ as the generating polynomial. This, however, is often unnecessary since a Conway polynomial [43] or cyclotomic polynomial with the correct degree would be adequate. If a cyclotomic polynomial is chosen to generate an unramified extension then every primitive element of the extension is a primitive root of unity.

If L/K is an unramified extension, then L and K have the same uniformizer $\pi_\mathsf{L} = \pi_\mathsf{K}$ and $\mathrm{Gal}(\mathsf{L}/\mathsf{K}) = \mathrm{Gal}(\underline{\mathsf{L}}/\underline{\mathsf{K}})$. Furthermore, if $[L : K] = m$ then $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$ is a cyclic group of order m, generated by the Frobenius automorphism.

For any finite extension L/K, one can construct an intermediate, unramified extension of degree $[\underline{\mathsf{L}} : \underline{\mathsf{K}}]$. We will refer to this, possibly trivial, extension as $\mathsf{L}^{ur}/\mathsf{K}$. Constructing L^{ur} yields a decomposition of the initial extension into a tower of extensions $\mathsf{L}/\mathsf{L}^{ur}/\mathsf{K}$ where the top relative extension $\mathsf{L}/\mathsf{L}^{ur}$ is totally ramified.

Definition 2.15. Let L be a finite algebraic extension of K. We say that the *inertia degree* of L/K is $f_{\mathsf{L}/\mathsf{K}} = [\underline{\mathsf{L}} : \underline{\mathsf{K}}]$ and that the *ramification index* of L/K is $e_{\mathsf{L}/\mathsf{K}} = [\mathsf{L} : \mathsf{L}^{ur}]$. The degree of the extension L/K is $n = e_{\mathsf{L}/\mathsf{K}} \cdot f_{\mathsf{L}/\mathsf{K}}$.

Proposition 2.16. *Let K be a local field and let $\tau \in \mathsf{K}[x]$. If $\underline{\tau} \in \underline{\mathsf{K}}[x]$ is squarefree, then the unramified extension of K of degree*

$$\operatorname{lcm}\{\deg(a) \mid \ a \text{ is an irreducible factor of } \underline{\tau} \ \}$$

is the splitting field of τ.

2.3 Hensel Lifting and Newton Polygons

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

Theorem 2.17 (Hensel's Lemma)**.** *Let $\Phi \in \mathcal{O}_{\mathsf{K}}[x]$ 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 $\Phi_1 \equiv \varphi_1 \bmod (\pi)$ and $\Phi_2 \equiv \varphi_2 \bmod (\pi)$.*

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 [85]. 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 $\mathcal{O}_{\mathsf{K}}[x]/(\Phi)$.

Definition 2.18. Let $\Phi(x) = \prod_{j=1}^{N}(x - \theta_j) \in \mathcal{O}_{\mathsf{K}}[x]$. For $\varphi \in \mathsf{K}[x]$ we define

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

Proposition 2.19. *Let $\gamma \in \mathsf{K}[x]$ with $\chi_{\gamma} \in \mathcal{O}_{\mathsf{K}}[y]$. If $\underline{\chi}_{\gamma}$ has at least two distinct irreducible factors, then $\Phi(x)$ is reducible in $\mathcal{O}_{\mathsf{K}}[x]$.*

Proof. Suppose $\underline{\chi}_{\gamma}$ has at least two irreducible factors. Then, Hensel's Lemma gives relatively prime monic polynomials $\chi_1 \in \mathcal{O}_{\mathsf{K}}[y]$ and $\chi_2 \in \mathcal{O}_{\mathsf{K}}[y]$ 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 2.20 (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 2.19 yields a constructive method for finding a factorization of Φ if χ_φ has more than one segment.

Corollary 2.21. *Let $\varphi \in \mathsf{K}[x]$ with $\chi_\varphi \in \mathcal{O}_\mathsf{K}[y]$. 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 $\Phi(x)$ over $\mathcal{O}_\mathsf{K}[x]$.*

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 2.19 yields a factorization of Φ. □

Another widely used method for factoring polynomials over local fields is Newton lifting, a method based on the following lemma. For more information, including a constructive proof, see [13].

Lemma 2.22 (Newton Lifting)**.** *Let K be a field complete with respect to a non-archimedian absolute value $|\cdot|$, with $\mathcal{O}_\mathsf{K}$ its valuation ring and $\mathfrak{p}$ its prime ideal. Let $\Phi(x) \in \mathcal{O}_\mathsf{K}[x]$ and assume there exists $\alpha \in \mathcal{O}_\mathsf{K}$ satisfying $|\Phi(\alpha)| < |\Phi'(\alpha)|^2$. Then Φ has a root in $\mathcal{O}_\mathsf{K}$ congruent to α modulo $\mathfrak{p}$.*

2.4 Totally Ramified Extensions

Definition 2.23. We call a monic polynomial $\varphi \in \mathcal{O}_\mathsf{K}[x]$ with $\varphi(x) = \sum \varphi_i x^i$ an *Eisenstein polynomial* if $v_\mathsf{K}(\varphi_0) = 1$ and $v_\mathsf{K}(\varphi_i) \geq 1$ for $1 \leq i \leq n-1$.

The Newton polygon of an Eisenstein polynomial has a particular shape that depends entirely on the polynomial's degree.

Proposition 2.24. *Let $\varphi \in \mathcal{O}_{\mathsf{K}}[x]$ be an Eisenstein polynomial with* $\deg \varphi = n$. *Then the Newton polygon of φ is a line with slope $-1/n$.*

Every Eisenstein polynomial is irreducible and thus can be used to generate a local field extension. To determine the type of extension, we consider another important, well-known result regarding Newton polygons.

Proposition 2.25. *Let $\mathcal{N}$ denote the Newton polygon for some $\rho(x) \in \mathcal{O}_{\mathsf{K}}[x]$. If the slopes of the segments of $\mathcal{N}$ are in lowest terms, then their denominators divide the ramification indices of the extensions defined by the irreducible factors of ρ.*

Taking the last two propositions together, we conclude that every Eisenstein polynomial generates a totally ramified extension. The converse is also true. If L/K is totally ramified and finite then any prime element of the extension is the root of an Eisenstein polynomial. Such a polynomial would generate L/K. On a related note, it can be shown that for a local field element $\alpha \in \mathsf{K}$ and $m \in \mathbb{N}$, $v_{\mathsf{K}}(\alpha) = 1/m$ implies that the minimal polynomial of α generates a totally ramified extension of K of degree m.

Let K be a local field whose residue class field $\underline{\mathsf{K}}$ has characteristic p. We define an extension L/K to be *tamely ramified* if $p \nmid e_{\mathsf{L}/\mathsf{K}}$ and *wildly ramified* otherwise. In certain cases we can obtain a generating polynomial of a tamely ramified subextension from a polynomial generating a totally ramified extension.

Proposition 2.26. *Let $n = e_0 p^m$ with $p \nmid e_0$, and let*

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

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

We have included the proof of this result from [33, Proposition 2.1] with some additional details that have been added to aide the reader.

Proof. As the Newton polygon of $\varphi(x)$ is a line, all roots α of $\varphi(x)$ have the same valuation, namely $v(\alpha)=h/n$. Because $\gcd(h,n)=1$, for each root α of $\varphi(x)$, n is a factor of the ramification index of $\mathsf{K}(\alpha)/\mathsf{K}$. Thus each extension $\mathsf{K}(\alpha)/\mathsf{K}$ is totally ramified and has degree n, which implies that $\varphi(x)$ is irreducible. Since $n=e_0p^m$ with $\gcd(e_0,p)=1$, the maximum tamely ramified subextension M over K has degree $[\mathsf{M}:\mathsf{K}]=e_0$.

We first show that ψ_0 can be written as the product of a principal unit and φ_0. Because $v(\varphi_0)=h$, we know that π^h divides φ_0. So $\exists\gamma\in\overline{\mathsf{K}}$ so that $\varphi_0=\gamma\pi^h$. We are given that $\psi_0\equiv\varphi_0 \bmod (\pi^{h+1})$, implying that π^{h+1} divides $\psi_0-\varphi_0$. So there exists $\mu\in\mathcal{O}_{\mathsf{K}}$ so that:

$$\begin{aligned}\psi_0-\varphi_0 &= \mu\pi^{h+1}\\ &= \mu\pi\cdot\frac{\varphi_0}{\gamma}\\ &= \frac{\mu}{\gamma}\cdot\pi\varphi_0.\end{aligned}$$

Let $\varepsilon=\frac{\mu}{\gamma}$. Then there is a principal unit $1+\pi\varepsilon\in\mathcal{O}_{\mathsf{K}}$ such that $\psi_0=(1+\pi\varepsilon)\varphi_0$. Next, we will show that α^n can be written as a similar product in L. Since α is a root

of φ, we have that

$$0 = \alpha^n + \sum_{i=1}^{n-1} \varphi_i \alpha^i + \varphi_0.$$

Subtracting α^n from both sides and then multiplying through by -1 we obtain:

$$\alpha^n = -\varphi_0 - \sum_{i=1}^{n-1} \varphi_i \alpha^i.$$

We want to determine $v\left(\sum_{i=1}^{n-1} \varphi_i \alpha^i\right)$, using the equation of the segment (line). The slope is $-h/n$ and it contains the point $(0, v(\varphi_0))$. So our line is $y = v(\varphi_0) - \frac{h}{n}x$. As our polygon is comprised of a single segment and $\gcd(h, n) = 1$, we know that for $1 \leq i \leq n-1$, $v(\varphi_i)$ must exceed the y-coordinate of i on the line. In short, $v(\varphi_i) > v(\varphi_0) - \frac{h}{n} \cdot i$. This leads us to

$$\begin{aligned} v(\varphi_i \alpha^i) &= v(\varphi_i) + iv(\alpha) \\ &= v(\varphi_i) + \frac{h}{n} \cdot i \\ &> v(\varphi_0) - \frac{h}{n} \cdot i + \frac{h}{n} \cdot i \\ &= v(\varphi_0) \end{aligned}$$

for $1 \leq i \leq n-1$. We conclude that

$$\begin{aligned} v\left(\sum_{i=1}^{n-1} \varphi_i \alpha^i\right) &\geq \min\{v(\varphi_1 \alpha), v(\varphi_2 \alpha^2), \ldots, v(\varphi_{n-1} \alpha^{n-1})\} \\ &> v(\varphi_0). \end{aligned}$$

Thus there exists $\delta \in \mathcal{O}_{\mathsf{L}}$ such that $\pi_{\mathsf{L}}\delta\varphi_0 = \sum_{i=1}^{n-1} \varphi_i\alpha^i$, where π_{L} is a uniformizer of the valuation ring $\mathcal{O}_{\mathsf{L}}$ of L. This, in turn, implies that

$$\begin{aligned}\alpha^n &= -\varphi_0 - \sum_{i=1}^{n-1} \varphi_i\alpha^i \\ &= -\varphi_0 - \pi_{\mathsf{L}}\delta\ \varphi_0 \\ &= -(1+\pi_{\mathsf{L}}\delta)\varphi_0\end{aligned}$$

for some principal unit $1 + \pi_{\mathsf{L}}\delta \in \mathcal{O}_{\mathsf{L}}$.

The polynomial $x^{e_0} + \psi_0$ has a root over L if and only if $(\alpha^{p^m}x)^{e_0} + \psi_0$ has a root over L. Dividing the latter polynomial by α^n yields

$$x^{e_0} + \frac{\psi_0}{\alpha^n} = x^{e_0} - \frac{(1+\pi\varepsilon)\varphi_0}{(1+\pi_{\mathsf{L}}\delta)\varphi_0}.$$

Since π_{L} divides π, there exists $k \in \mathcal{O}_{\mathsf{L}}$ such that

$$x^{e_0} + \frac{\psi_0}{\alpha^n} = x^{e_0} - \frac{(1+\pi_{\mathsf{L}}k\varepsilon)}{(1+\pi_{\mathsf{L}}\delta)}.$$

It can be proven that both $1 + (\pi)$ and $1 + (\pi_{\mathsf{L}})$ are multiplicative groups. Thus, the above simplifies to

$$x^{e_0} + \frac{\psi_0}{\alpha^n} \equiv x^{e_0} - 1 \bmod \pi_{\mathsf{L}}\mathcal{O}_{\mathsf{L}}[x].$$

Obviously $\rho(x) = x^{e_0} - 1 \in \underline{\mathsf{L}}[x]$ is square free and $\rho(1) = 0$. With Newton lifting (and by reversing the transformations above), we obtain a root of $x^{e_0} + \psi_0$ in

L. Let β be this root of $x^{e_0} + \psi_0$. Then

$$\begin{aligned} v(\beta^b \pi^a) &= v(\beta^b) + v(\pi^a) \\ &= bv(\beta) + av(\pi) \\ &= bv(\beta) + a. \end{aligned}$$

Since β is a root of $x^{e_0} + \psi_0$, we have that $\beta^{e_0} = -\psi_0$. In fact, we obtain

$$\begin{aligned} e_0 v(\beta) &= v(\beta^{e_0}) \\ &= v(\psi_0) \\ &= v((1 + \pi\varepsilon)\varphi_0) \\ &= v(\varphi_0 + \pi\varepsilon \cdot \varphi_0) \\ &= \min\{v(\varphi_0), v(\pi\varepsilon \cdot \varphi_0)\} \\ &= v(\varphi_0) \\ &= h \end{aligned}$$

since $v(\pi\varepsilon \cdot \varphi_0) \geq h + 1$. Therefore $v(\beta) = \frac{h}{e_0}$ and

$$\begin{aligned} v(\beta^b \pi^a) &= bv(\beta) + a \\ &= \frac{bh}{e_0} + a \\ &= \frac{ae_0 + bh}{e_0} \\ &= \frac{1}{e_0}. \end{aligned}$$

So, $\mathsf{K}(\beta) = \mathsf{K}(\beta^b\pi^a)$ is a tamely ramified extension of degree e_0. Thus $\mathsf{M} = \mathsf{K}(\beta^b\pi^a)$. Furthermore,

$$\beta^{e_0 b}\pi^{e_0 a} = (\beta^{e_0})^b\pi^{e_0 a} = (-\psi_0)^b\pi^{e_0 a}.$$

So we have $\beta^b\pi^a$ is a root of $x^{e_0} - (-\psi_0)^b\pi^{e_0 a} \in \mathcal{O}_\mathsf{K}[x]$. □

This proposition informs us that each totally and tamely ramified extension of degree e can be generated by a polynomial of the form $x^e - \gamma\pi_\mathsf{K}$ where $v(\gamma) = 0$.

Corollary 2.27. *Let $\varphi(x) = \sum_{i=0}^{e}\varphi_i x^i \in \mathcal{O}_\mathsf{K}[x]$ be an Eisenstein polynomial and assume $p \nmid e$. If $\psi(x) = x^e + \psi_0$ with $\psi_0 \equiv \varphi_0 \bmod (\pi^2)$, then the extensions generated by $\varphi(x)$ and $\psi(x)$ are isomorphic.*

Proof. Since φ is Eisenstein, its Newton Polygon has slope $-h/e = -1/e$. Thus the proof follows from setting $a = 0$, $b = 1$ in Proposition 2.26. □

Let $\varphi \in \mathcal{O}_\mathsf{K}[x]$ be the degree e Eisenstein polynomial in Corollary 2.27. If ζ_e denotes a primitive e-th root of unity, then Corollary 2.27 tells us that the splitting field of φ is $\mathsf{N} = \mathsf{K}(\zeta_e, \sqrt[e]{-\varphi_0})$. The structure of $\mathrm{Gal}(\mathsf{N}/\mathsf{K})$ is well known (see [39, Chapter 16] for more).

Theorem 2.28. *Let K be a local field, and let q be the number of elements of its residue class field. Let N/K be a normal, tamely ramified extension with ramification index e and inertia degree f. There exists an integer r with $r(q-1) \equiv 0 \bmod e$ such that $\mathsf{N} = \mathsf{K}(\zeta, \sqrt[e]{\zeta^r\pi})$, where ζ is a (q^f-1)-st root of unity and $q^f - 1 \equiv 0 \bmod e$. Let $k = \frac{r(q-1)}{e}$. The generators of the Galois group are the automorphisms*

$$s : \zeta \mapsto \zeta,\ \sqrt[e]{\zeta^r\pi} \mapsto \zeta^{(q^f-1)/e}\sqrt[e]{\zeta^r\pi} \quad \textit{and} \quad t : \zeta \mapsto \zeta^q,\ \sqrt[e]{\zeta^r\pi} \mapsto \zeta^k\sqrt[e]{\zeta^r\pi}.$$

The Galois group of N/K *as a finitely presented group is*

$$\mathrm{Gal}(\mathsf{N}/\mathsf{K}) \cong \langle s, t \mid s^e = 1, t^f = s^r, st = ts^q \rangle.$$

Remark. Let ζ be a primitive $(q^f - 1)$-st root of unity and let $q = \#\underline{\mathsf{K}}$. The extension $\mathsf{K}(\zeta, \sqrt[e]{\zeta^r \pi_{\mathsf{K}}})$ is Galois if and only if e divides both $q^f - 1$ and $r(q-1)$. For more information, see part (c) of [32, Satz 3.2].

In the event that a tamely ramified extension L/K is not normal, we can compute its normal closure by increasing the inertia degree. This gives us a Galois group with a similar presentation. Compare to [32, Satz 3.6] and [46, Proposition 3.5.1].

Theorem 2.29. *Let* ζ *denote a primitive* $(q^f - 1)$*-st root of unity and let* $\mathsf{L} = \mathsf{K}(\zeta, \sqrt[e]{\zeta^r \pi})$ *be tamely ramified. Let* $g = \gcd(q^f - 1, r(q-1))$*, and let* $u \in \mathbb{N}$ *be minimal such that*

$$q^{fu} - 1 \equiv 0 \bmod (e(q^f - 1)/g).$$

Let ξ *be a primitive* $(q^{fu} - 1)$*-st root of unity, and let* $s = r(q^{fu} - 1)/(q^f - 1)$*. Then*

$$\mathsf{N} = \mathsf{K}(\xi, \sqrt[e]{\xi^s \pi})$$

is the normal closure of L/K*, and the Galois group of* L/K *is*

$$\mathrm{Gal}(\mathsf{L}/\mathsf{K}) \cong \langle x, y \mid x^e = 1, y^{fu} = x^s, xy = yx^q \rangle.$$

In Theorems 2.28 and 2.29, the third relation in the Galois group is equivalent to one group generator acting on the other through conjugation. This action is the same as raising one of the generators to a power q that is coprime to its order e.

This is remarkably similar to Example B.15. It is tempting to believe that the Galois group of a tamely ramified extension is the semidirect product of nontrivial, cyclic groups. As our next example demonstrates, this is not always true.

Example 2.30. Let ζ be a primitive eighth root of unity. We consider the local field $\mathsf{L} = \mathbb{Q}_3(\zeta, \sqrt[4]{\zeta^2 \cdot 3})$. The extension $\mathsf{L}/\mathbb{Q}_3$ has ramification index $e = 4$ and inertia degree $f = 2$. Futhermore, the exponent of ζ in the radicand of $\sqrt[4]{\zeta^2 \cdot 3}$ is $r = 2$ and the number of elements in the residue class field of $\mathbb{Q}_3$ is $q = 3$.

In order to compute the Galois group of $\mathsf{L}/\mathbb{Q}_3$ we must first determine if the extension is normal. We can quickly verify that $\mathsf{L}/\mathbb{Q}_3$ is normal since e divides both $q^f - 1$ and $r(q-1)$. Thus Theorem 2.28 tells us that

$$\mathrm{Gal}(\mathsf{L}/\mathbb{Q}_3) \cong \langle s, t \mid s^4 = 1, t^2 = s^2, st = ts^3 \rangle.$$

The quaternion group of 8 elements has multiple presentations. One of them is

$$Q_8 \cong \langle x, y \mid x^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle.$$

In the above presentation for Q_8 we have that $x^{-1} = x^3$. Thus it is clear that $\mathrm{Gal}(\mathsf{L}/\mathbb{Q}_3) \cong Q_8$. According to Proposition B.20, this group is not a semidirect product of cyclic groups.

Remark. The extension $\mathbb{Q}_3(\zeta, \sqrt[4]{\zeta^2 \cdot 3})$ in the preceding example can be generated by $x^8 + 9x^4 + 36 \in \mathbb{Z}_3[x]$.

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 p-adic field. For the duration of this section, we assume that L/K is a Galois extension for local fields L and K and that G is the Galois group of this extension.

Definition 2.31. Let L/K be a Galois extension with Galois group G. Let v_{L} be the discrete valuation on L. For an integer $i \geq -1$, the *i-th ramification group* of G is

$$G_i = \{\sigma \in G \mid v_{\mathsf{L}}(\sigma(\beta) - \beta) \geq i + 1 \text{ for all } \beta \in \mathcal{O}_{\mathsf{L}}\} \quad (i \geq -1).$$

It is clear that $G_{-1} = G$. By convention, G_0 is called the *inertia subgroup* of G and G_1 is referred to as the *ramification subgroup* of G. Furthermore, $G_0 = \{\mathrm{id}\}$ if and only if L/K is unramified and $G_1 = \{\mathrm{id}\}$ if and only if L/K is tamely ramified.

For $i > 1$, the subgroups G_i are known as the *higher ramification groups* of L/K. Each group G_i satisfies $G_i \trianglelefteq G_j$ whenever $i > j$. For large enough values of i, the group G_i has order 1.

Proposition 2.32. *Let L/K be Galois. Denote by G the Galois group of L/K and by G_i the i-th ramification group of G. Let π be a uniformizer of L. Let $U_0 = \mathcal{O}_{\mathsf{L}}{}^{\times}$, and let $U_i = \langle 1 + (\pi^i) \rangle$ for $i \geq 1$. Then*

(1) *For $i \geq 0$, the group G_i/G_{i+1} is isomorphic to a subgroup of U_i/U_{i+1} and thus is abelian.*

(2) *The quotient G_0/G_1 is cyclic with order coprime to the characteristic p of L.*

(3) *For $i \geq 0$, the group G_i/G_{i+1} is a direct product of cyclic groups of order p. The group G_1 is a p-group.*

(4) *The inertia subgroup G_0 is the semi-direct product of a cyclic group of order coprime to p and a normal subgroup which is a p-group.*

(5) *Both G and G_0 are solvable.*

(6) *The quotient U_0/U_1 is isomorphic to the multiplicative group of $\underline{\mathsf{L}}$.*

(7) *If $\mathcal{O}_{\mathsf{L}} = \mathcal{O}_{\mathsf{K}}[\alpha]$ then $G_i = \{\sigma \in G \mid v_{\mathsf{L}}(\sigma(\alpha) - \alpha) \geq i + 1\}$.*

If $\mathsf{K} = \mathbb{Q}_p$, then the order of G_0/G_1 divides $p^{[G:G_0]} - 1$. This is a direct result from parts (1) and (6) of Proposition 2.32.

Proposition 2.33. *Let L/K be Galois. Let π be a uniformizer of L, and let U_i for $i \geq 0$ be defined as they are in Proposition* 2.32. *Then, for $i \geq 1$, the group U_i/U_{i+1} is canonically isomorphic to the group $(\pi^i)/(\pi^{i+1})$, which is itself isomorphic (non-canonically) to the additive group of the residue class field $\underline{\mathsf{L}}$.*

The ramification groups of G form the sequence

$$G \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_k = 1.$$

Such a sequence of subobjects is called a *filtration* of G. An important aspect of this sequence is when it is strictly decreasing, i.e., when consecutive groups are not equal. As such, a great deal of attention has been spent to determining the values of the index i for which $G_i \neq G_{i+1}$.

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 $\underline{\mathsf{L}}$, and let i and j be any two ramification breaks of L/K. Then $i \equiv j \mod p$.*

Because the ramification groups are subgroups of $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$, we know that they must correspond to subfields of L/K. In the cases of G_0 and G_1 these subfields are well known.

Proposition 2.37. *Let L/K be Galois. Denote by G_i the i-th ramification group of* $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$.

(1) *The maximal unramified subfield L^{ur} of L/K is the fixed field of the inertia group G_0. So $G_0 = \mathrm{Gal}(\mathsf{L}/\mathsf{L}^{ur})$. Also, G_0 is a normal subgroup of order $e_{\mathsf{L}/\mathsf{K}}$ with cyclic quotient of order $f_{\mathsf{L}/\mathsf{K}}$.*

(2) *The maximal tamely ramified subfield T of L/K is the fixed field of the first ramification subgroup G_1. So $G_1 = \mathrm{Gal}(\mathsf{L}/\mathsf{T})$.*

2.6 Composites of Tamely Ramified Extensions

Let K be a local field with uniformizing element π, and assume that the characteristic of $\underline{\mathsf{K}}$ is p. In this section we will introduce a method for computing the composite of tamely, totally ramified extensions of a common and possibly trivial unramified extension of K. In later sections, this particular type of calculation will be used to compute a subextension of an Eisenstein polynomial's splitting field. The advantage of this method is that we are able to quickly write down explicit generating polynomials for the necessary extensions avoiding expensive factoring and/or root finding algorithms.

Before we can introduce our method, we need to recall some well-known results regarding composites of extensions of different types and norms of polynomials.

Proposition 2.38. *Let* T/K *be totally ramified with* $\mathsf{T} = \mathsf{K}(\alpha)$ *and let* U/K *be unramified with* $\mathsf{U} = \mathsf{K}(\beta)$*. Also let* TU *denote the composite of* T *and* U*. Then*

(a) $\mathsf{TU} \cong \mathsf{U}(\alpha)$,

(b) $\mathsf{TU} \cong \mathsf{T}(\beta)$.

Proof. Let $\varphi(x)$ denote an Eisenstein polynomial that generates T/K. Because the uniformizers of U and K are the same, $\varphi(x)$ is Eisenstein over U as well. Thus, (a) follows from the fact that all Eisenstein polynomials are irreducible.

Let $\psi(x)$ be the generating polynomial of U/K. Then we have that $\psi(x)$ is irreducible over the residue class field $\underline{\mathsf{K}}$. Furthermore, since T/K is totally ramified, we have that $\underline{\mathsf{T}} = \underline{\mathsf{K}}$. It follows that $\psi(x)$ generates an unramified extension of T of degree $[\mathsf{U} : \mathsf{K}]$. Part (b) has been proven. □

Proposition 2.39. *Let* T/K *be totally and tamely ramified with* $\mathsf{T} = \mathsf{K}(\alpha)$*, and let* L/K *be a wildly, totally ramified p-extension with* $\mathsf{L} = \mathsf{K}(\beta)$*. Let* TL *denote the composite of* T *and* L*. Then*

(a) $\mathsf{TL} \cong \mathsf{L}(\alpha)$,

(b) $\mathsf{TL} \cong \mathsf{T}(\beta)$.

Proof. Suppose $\varphi(x)$ is an Eisenstein polynomial that generates T/K, and let θ be a root of $\varphi(x)$. Then we know that $v_{\mathsf{K}}(\theta) = 1/e$ for some natural number e satisfying $p \nmid e$. Because e and p are coprime, $v_{\mathsf{L}}(\theta)$ has a denominator of e as well. Thus, we have that $\varphi(x)$ generates a degree e extension of L. This proves (a). A similar argument proves (b). □

Definition 2.40. Let L/K be an algebraic extension, and let $\varphi(x) = \sum_{i=0}^{n} c_i x^i \in \mathsf{L}[x]$. Then we define the *norm* of $\varphi(x)$ to be

$$\mathrm{N}_{\mathsf{L}/\mathsf{K}}(\varphi(x)) = \prod_{j=1}^{[\mathsf{L}:\mathsf{K}]} \left(\sum_{i=0}^{n} c_i^{(j)} x^i \right)$$

where $c_i^{(j)}$ is the j-th conjugate of c_i.

As $\mathrm{N}_{\mathsf{L}/\mathsf{K}}(\varphi(x))$ is invariant under conjugation, its coefficients are in K.

Proposition 2.41. *Let* $\mathsf{M} \supseteq \mathsf{L} \supseteq \mathsf{K}$ *be a tower of totally ramified extensions where* $\mathsf{M} \cong \mathsf{L}[x]/(\varphi(x))$. *Then* $\mathrm{N}_{\mathsf{L}/\mathsf{K}}(\varphi(x))$ *generates* M/K.

Remark.

(a) If $\varphi(x) \in \mathsf{L}[x]$ is Eisenstein, then $\mathrm{N}_{\mathsf{L}/\mathsf{K}}(\varphi(x))$ is Eisenstein.

(b) If $x^e - \gamma\pi_{\mathsf{L}}$ is Eisenstein for $p \nmid e$, then

$$\begin{aligned} \mathsf{K}[x]/\left(\mathrm{N}_{\mathsf{L}/\mathsf{K}}(x^e - \gamma\pi_{\mathsf{L}})\right) &= \mathsf{K}[x]/\left((x^e)^{[\mathsf{L}:\mathsf{K}]} + \ldots + \mathrm{N}_{\mathsf{L}/\mathsf{K}}(-\gamma\pi_{\mathsf{L}})\right) \\ &\cong \mathsf{K}[x]/\left((x^e)^{[\mathsf{L}:\mathsf{K}]} + \mathrm{N}_{\mathsf{L}/\mathsf{K}}(-\gamma\pi_{\mathsf{L}})\right) \end{aligned}$$

by Corollary 2.27.

We will now begin to discuss our method by establishing some notation. For our purposes, tamely, totally ramified extensions will be generated by binomial Eisenstein polynomials of the form $x^e - \gamma\pi$ where $v(\gamma) = 0$, a convention permitted by Corollary 2.27. We have adopted this convention for three reasons. First, since the degree is often obvious in the context of the problem, this reduces the task of determining generating polynomials to determining the polynomial's constant term. Second, in our future applications of composites of tamely, totally ramified extensions

all of the generating polynomials will be binomials. Finally, it allows us to make use of Remark 2.6 and the following result.

Remark. $\mathsf{T} = \mathsf{K}[x]/(x^n - a)$ contains the subfields $\mathsf{K}[x]/(x^m - a)$ where $m \mid n$.

Our current, primary focus is determining the composite of two tamely, totally ramified extensions. We generalize this to composites of three or more extensions later. We start with the simple cases where the degrees of the extensions are equal or coprime.

Proposition 2.42. *Let $\varphi_1(x) = x^e - \gamma_1\pi \in \mathcal{O}_\mathsf{K}[x]$ and $\varphi_2(x) = x^e - \gamma_2\pi \in \mathcal{O}_\mathsf{K}[x]$ with $p \nmid e$ and $v(\gamma_1) = v(\gamma_2) = 0$. Let θ_1 and θ_2 be roots of φ_1 and φ_2 respectively. Then the composite of $\mathsf{K}(\theta_1)$ and $\mathsf{K}(\theta_2)$ is the unramified extension of $\mathsf{K}(\theta_1)$ whose degree is the least common multiple f of the degrees of the irreducible factors of $z^e - \underline{\left(\frac{\gamma_2}{\gamma_1}\right)} \in \underline{\mathsf{K}}[z]$.*

Proof. Since all of the roots for both φ_1 and φ_2 have the same valuation, there exists a unit $\delta \in \mathsf{K}(\theta_1, \theta_2)$ so that $\theta_1\delta$ is a root of $\varphi_2(x)$. We have

$$\begin{aligned} 0 &= (\theta_1\delta)^e - \gamma_2\pi \\ &= \theta_1^e\delta^e - \gamma_2\pi \\ &= (\gamma_1\pi)\delta^e - \gamma_2\pi. \end{aligned}$$

Dividing by $\gamma_1\pi$ yields $\delta^e - \frac{\gamma_2}{\gamma_1} = 0$. So the composite of $\mathsf{K}(\theta_1)$ and $\mathsf{K}(\theta_2)$ is the extension of $\mathsf{K}(\theta_1)$ that contains the roots of $\tau(x) = x^e - \frac{\gamma_2}{\gamma_1}$. Since

$$\gcd\left(x^e - \frac{\gamma_2}{\gamma_1}, \frac{d}{dx}\left(x^e - \frac{\gamma_2}{\gamma_1}\right)\right) = \gcd\left(x^e - \frac{\gamma_2}{\gamma_1}, ex^{e-1}\right) = 1$$

the polynomial $\underline{\tau}(z) = z^e - \underline{\frac{\gamma_2}{\gamma_1}} \in \underline{K(\theta_1)}[z]$ is squarefree. Denote by f the least common multiple of the degrees of the irreducible factors of $\underline{\tau}$. Then Proposition 2.16 tells us

that τ splits into linear factors in the unramified extension of $\mathsf{K}(\theta_1)$ of degree f, which is the composite of $\mathsf{K}(\theta_1)$ and $\mathsf{K}(\theta_2)$. □

Proposition 2.43. *Let $\varphi_1(x) = x^n - d\pi \in \mathcal{O}_\mathsf{K}[x]$, and let $\varphi_2(x) = x^m - c\pi \in \mathcal{O}_\mathsf{K}[x]$ where $v(c) = v(d) = 0$ and m, n are coprime to p and one another. Let θ_1 and θ_2 be roots of φ_1 and φ_2 respectively. Then the composite of $\mathsf{K}(\theta_1)$ and $\mathsf{K}(\theta_2)$ is the totally ramified extension of $\mathsf{K}(\theta_1)$ generated by the polynomial $x^m - (\frac{c}{d})^b\theta_1$ where a, b are integers such that $am + bn = 1$.*

Proof. If we evaluate φ_1 and φ_2 at their given roots we obtain $\theta_1^n - d\pi = 0$ and $\theta_2^m - c\pi = 0$. Solving the former equation for π we find that $\pi = \frac{\theta_1^n}{d}$. Substituting this into the second equation yields $\theta_2^m - \frac{c}{d}\theta_1^n = 0$. So the composite of $\mathsf{K}(\theta_1)$ and $\mathsf{K}(\theta_2)$ is the extension of $\mathsf{K}(\theta_1)$ that contains the roots of $\tau(x) = x^m - \frac{c}{d}\theta_1^n$.

The Newton Polygon of τ is a line connecting the points $(m, 0)$ and $(0, n)$. In lowest terms, this line has slope $-\frac{n}{m}$. Observing that θ_1 is a uniformizer for $\mathsf{K}(\theta_1)$, it follows from Proposition 2.26 that the composite $\mathsf{K}(\theta_1)(\theta_2)$ can be generated by the Eisenstein polynomial $x^m + (-1)^{b+1}\left(-\frac{c}{d}\theta_1^n\right)^b\theta_1^{ma}$. Furthermore:

$$\begin{aligned} x^m + (-1)^{b+1}\left(-\frac{c}{d}\theta_1^n\right)^b\theta_1^{ma} &= x^m + (-1)^{b+1}\left(-\frac{c}{d}\right)^b\theta_1^{am+bn} \\ &= x^m + (-1)^{b+1}\left(-\frac{c}{d}\right)^b\theta_1 \\ &= x^m - \left(\frac{c}{d}\right)^b\theta_1. \end{aligned}$$

□

Let K' be an unramified extension of K with uniformizer $\pi_{\mathsf{K}'} = \pi$, and let T_1 and T_2 be tamely, totally ramified extensions of K'. If T_1/K' and T_2/K' have the same degree or coprime degrees, we have seen that computing the composite $\mathsf{T}_1\mathsf{T}_2$ involves

constructing a single unramified extension or a single totally ramified extension. In the event that $[\mathsf{T}_1 : \mathsf{K}']$ and $[\mathsf{T}_2 : \mathsf{K}']$ are distinct and have a nontrivial divisor, we must construct extensions of both types in order to compute the composite. The proposition below describes this approach as a mixture of the ideas presented earlier in this section.

Proposition 2.44. *For an unramified extension K'/K, let $\varphi_1(x) = x^{e_1} - \gamma_1\pi \in \mathsf{K}'[x]$, and let $\varphi_2(x) = x^{e_2} - \gamma_2\pi \in \mathsf{K}'[x]$, where $p \nmid e_1$, $p \nmid e_2$, $v(\gamma_1) = v(\gamma_2) = 0$, and $m := \gcd(e_1, e_2) > 1$. Let $\mathsf{T}_1 = \mathsf{K}'[x]/(\varphi_1)$, and let $\mathsf{T}_2 = \mathsf{K}'[x]/(\varphi_2)$.*

For $i \in \{1, 2\}$

(a) T_i/K' has a subfield $\mathsf{S}_i = \mathsf{K}'[x]/(x^m - \gamma_i\pi)$.

(b) $\mathsf{T}_i \cong \mathsf{S}_i[x]/(x^{e_i/m} - \gamma_i'\pi_{\mathsf{S}_i})$ where $\gamma_i' \in \mathsf{K}'$ is a lift of a root of $x^m - \frac{(-1)^{m+1}\gamma_i\pi}{\mathrm{N}_{\mathsf{S}_i/\mathsf{K}'}(\pi_{\mathsf{S}_i})}$ in $\underline{\mathsf{K}}'$.

The composite $\mathsf{S}_1\mathsf{S}_2$ of S_1 and S_2 can be constructed as an extension of S_1 using Proposition 2.42.

(c) $\mathsf{S}_1\mathsf{S}_2\mathsf{T}_1 \cong \mathsf{S}_1\mathsf{S}_2[x]/(x^{e_1/m} - \gamma_1'\pi_{\mathsf{S}_1})$.

(d) $\mathsf{S}_1\mathsf{S}_2\mathsf{T}_2 \cong \mathsf{S}_1\mathsf{S}_2[x]/(x^{e_2/m} - \gamma_2'\pi_s)$ where π_s is a root of $x^m - \gamma_2\pi$ in $\mathsf{S}_1\mathsf{S}_2$.

The composite of T_1/K' and T_2/K' is the composite of $\mathsf{S}_1\mathsf{S}_2\mathsf{T}_1$ and $\mathsf{S}_1\mathsf{S}_2\mathsf{T}_2$.

Proof. We begin by observing that (a) follows from Remark 2.6. For (b), we will prove the $i = 2$ case. Specifically, we wish to find the generating polynomial for the top extension in the tower T_2/K' below

$$\mathsf{T}_2 \supseteq \mathsf{S}_2 \supseteq \mathsf{K}'.$$

We know that $[\mathsf{T}_2 : \mathsf{S}_2]$ must be e_2/m, so the extension can be generated by a polynomial of the form $x^{e_2/m} - \gamma_2'\pi_{\mathsf{S}_2}$ where the uniformizer of S_2, π_{S_2}, is a root of $x^m - \gamma_2\pi$. According to Proposition 2.41 $\mathrm{N}_{\mathsf{S}_2/\mathsf{K}'}(x^{e_2/m} - \gamma_2'\pi_{\mathsf{S}_2})$ generates T_2/K'. As T_2/K' is also generated by $x^{e_2} - \gamma_2\pi$, part (b) of Remark 2.6 informs us that we can choose γ_2' such that $\mathrm{N}(-\gamma_2'\pi_{\mathsf{S}_2}) = -\gamma_2\pi$ for $\mathrm{N} = \mathrm{N}_{\mathsf{S}_2/\mathsf{K}'}$. From this we obtain:

$$\begin{aligned}
-\gamma_2\pi &= \mathrm{N}(-\gamma_2'\pi_{\mathsf{S}_2}) \\
&= \mathrm{N}(-\gamma_2')\mathrm{N}(\pi_{\mathsf{S}_2}) \\
&= (-\gamma_2')^{[\mathsf{S}_2:\mathsf{K}']}\mathrm{N}(\pi_{\mathsf{S}_2}) \\
&= (-\gamma_2')^m\mathrm{N}(\pi_{\mathsf{S}_2}) \\
&= (-1)^m(\gamma_2')^m\mathrm{N}(\pi_{\mathsf{S}_2}).
\end{aligned}$$

Solving this for $(\gamma_2')^m$ we get

$$(\gamma_2')^m = \frac{(-1)^{m+1}\gamma_2\pi}{\mathrm{N}(\pi_{\mathsf{S}_2})}.$$

A similar result holds for $i = 1$. Thus (b) has been proven. All that remains is to prove the formulations of the composites of $\mathsf{S}_1\mathsf{S}_2$ with T_1 and T_2.

Since $\mathsf{S}_1\mathsf{S}_2/\mathsf{S}_1$ is unramified, we have that $\pi_{\mathsf{S}_1\mathsf{S}_2} = \pi_{\mathsf{S}_1}$. Thus, by Proposition 2.38, the composite of $\mathsf{S}_1\mathsf{S}_2/\mathsf{S}_1$ with $\mathsf{T}_1/\mathsf{S}_1$ is the extension of $\mathsf{S}_1\mathsf{S}_2$ generated by the polynomial that generates $\mathsf{T}_1/\mathsf{S}_1$. This proves (c).

Because $\mathsf{S}_1\mathsf{S}_2$ was computed as an unramified extension of S_1 instead of S_2, demonstrating (d) requires more work. In order to use the same argument that we utilized for (c), we must find a way to write π_{S_2} in terms of elements in $\mathsf{S}_1\mathsf{S}_2$. To this end, we look at the minimal polynomial of π_{S_2} which is $x^m - \gamma_2\pi$. Specifically, we

find a root of this polynomial in $\mathsf{S}_1\mathsf{S}_2$ and call it π_s. The result follows from replacing π_{S_2} in $x^{e_2/m} - \gamma_2'\pi_{\mathsf{S}_2}$ by π_s. □

Remark. Because $\gcd([\mathsf{S}_1\mathsf{S}_2\mathsf{T}_1 : \mathsf{S}_1\mathsf{S}_2], [\mathsf{S}_1\mathsf{S}_2\mathsf{T}_2 : \mathsf{S}_1\mathsf{S}_2]) = 1$, the composite of $\mathsf{S}_1\mathsf{S}_2\mathsf{T}_1$ and $\mathsf{S}_1\mathsf{S}_2\mathsf{T}_2$ can be constructed as an extension of $\mathsf{S}_1\mathsf{S}_2\mathsf{T}_1$ using Proposition 2.43.

As mentioned in Section 2.2, we can write the composite in any of the above cases as a tower of extensions $\mathsf{T}/\mathsf{U}/\mathsf{K}$ where T/U is totally ramified and U/K is unramified. This restructuring can be accomplished through the use of norms and embeddings. To find the composite of the towers $\mathsf{T}/\mathsf{U}/\mathsf{K}$ and $\mathsf{T}'/\mathsf{U}'/\mathsf{K}$ one forms the unramified extension $\mathsf{U}\mathsf{U}'/\mathsf{K}$ of degree $\mathrm{lcm}([\mathsf{U} : \mathsf{K}], [\mathsf{U}' : \mathsf{K}])$ and finds the composite of T and T' as extensions of $\mathsf{U}\mathsf{U}'$.

Suppose that $\mathsf{L}_1, \mathsf{L}_2, \ldots, \mathsf{L}_m$ are tamely, totally ramified extensions of K' and that we need to compute their composite. We begin by computing the composite $\mathsf{L}_1\mathsf{L}_2$ and restructuring it in the form described in the preceding paragraph. Next, we take this extension of K and find its composite with L_3. Once this extension is restructured, we find its composite with L_4, and the process would continue in this way until we include L_m. In short, the composite of the m extensions is computed by recursively computing the composite of two extensions.

CHAPTER III

RAMIFICATION POLYGONS AND RESIDUAL POLYNOMIALS

In this chapter, we examine two invariants of a totally ramified extension: the ramification polygon and the residual polynomial classes of the extension. Particular attention is given to subfields of the extension and how they relate to splitting fields and Galois groups. Most of this material will be used, in a later chapter, in a new algorithm for computing Galois groups of Eisenstein polynomials.

The material in the first seven sections can be found in prior publications by Christian Greve [32][33] and Brian Sinclair [68] [79]. In the final section, we improve on one of Greve's results and give a new refinement of the ramification filtration from Section 2.5. Throughout, we let K be a local field whose residue class field $\underline{\mathsf{K}}$ has characteristic p.

3.1 Residual Polynomials

Residual (or associated) polynomials were first introduced by Ore [61, 65]. They yield information about the unramified part of the extension generated by the zeros of a polynomial. They have proven to be helpful in the factorization of polynomials [38, 70] over an assortment of local fields as well as in computing both integral bases and ideal decompositions [35, 60, 61]. Recently they have been utilized in computing splitting fields for polynomials over local fields [57]. In later sections, we will use them to compute Galois groups and, in special cases, splitting fields for Eisenstein polynomials. For now we will focus on the derivation and basic properties of residual polynomials.

For the remainder of this section, $\rho(x) = \sum_{i=0}^{n} \rho_i x^i$ is a monic polynomial in $\mathcal{O}_{\mathsf{K}}[x]$. We will assume that the Newton polygon $\mathcal{N}_\rho$ of ρ is made up by ℓ segments:

$$(a_0, b_0) \leftrightarrow (a_1, b_1) \leftrightarrow \ldots \leftrightarrow (a_{\ell-1}, b_{\ell-1}) \leftrightarrow (a_\ell, b_\ell)$$

with slopes:

$$-m_1 < -m_2 < \cdots < -m_{\ell-1} < -m_\ell.$$

For each of these segments, there is a corresponding residual polynomial that is the result of transformations of ρ that shift the particular segment to the x-axis. For now we will focus on one particular segment. Let r be some positive integer between 1 and ℓ (inclusive). Then the r-th segment of $\mathcal{N}_\rho$ has slope $-h_r/e_r$ with $\gcd(h_r, e_r) = 1$ and has endpoints (a_{r-1}, b_{r-1}) and (a_r, b_r). There exists a root β of $\rho(x)$ which has valuation h_r/e_r. If we set $\mathsf{L} = \mathsf{K}(\beta)$ then we have established enough notation to derive the equation of the residual polynomial that corresponds to the r-th segment of $\mathcal{N}_\rho$.

We apply a series of transformations to ρ so that the r-th segment of $\mathcal{N}_\rho$ will lie on the x-axis. We begin by replacing x by βx. This causes the r-th segment of $\mathcal{N}_\rho$ to become horizontal and rise up $v(\beta^{a_{r-1}})$ units. We next divide by $\beta^{a_{r-1}}$. This results in the segment being lowered to its original height. Finally, dividing by $\pi^{b_{r-1}}$, where π is the uniformizer for K, drops the segment to the x-axis. Thus the r-th segment of the Newton polygon for $\frac{\rho(\beta x)}{\pi^{b_{r-1}}\beta^{a_{r-1}}}$ is horizontal and lies on the x-axis. We have

$$\frac{\rho(\beta x)}{\pi^{b_{r-1}}\beta^{a_{r-1}}} = \sum_{i=0}^{n} \frac{\rho_i \beta^i x^i}{\pi^{b_{r-1}}\beta^{a_{r-1}}}.$$

The other segments of $\frac{\rho(\beta x)}{\pi^{b_{r-1}}\beta^{a_{r-1}}}$ are off of the x-axis and thus disappear if we mod by π_{L}. The x-coordinates of our original segment can be parameterized as $a_{r-1} + je_r$ where j takes on the integral values 0 through $(a_r - a_{r-1})/e_r$. We obtain

$$\begin{aligned}\frac{\rho(\beta x)}{\pi^{b_{r-1}}\beta^{a_{r-1}}} &\equiv \sum_{i=a_{r-1}}^{a_r} \frac{\rho_i \beta^i x^i}{\pi^{b_{r-1}}\beta^{a_{r-1}}} \bmod \pi_{\mathsf{L}}\mathcal{O}_{\mathsf{L}}[x] \\ &\equiv \sum_{j=0}^{d_r/e_r} \frac{\rho_{je_r+a_{r-1}}\beta^{je_r+a_{r-1}}x^{je_r+a_{r-1}}}{\pi^{b_{r-1}}\beta^{a_{r-1}}} \bmod \pi_{\mathsf{L}}\mathcal{O}_{\mathsf{L}}[x]\end{aligned}$$

where $d_r = a_r - a_{r-1}$. In an effort to reduce the amount of clutter in this relation, we cancel the common factor of $\beta^{a_{r-1}}$ on the right hand side and then divide both sides by $x^{a_{r-1}}$ to find that

$$\frac{\rho(\beta x)}{\pi^{b_{r-1}}\beta^{a_{r-1}}x^{a_{r-1}}} \equiv \sum_{j=0}^{d_r/e_r} \frac{\rho_{je_r+a_{r-1}}\beta^{je_r}x^{je_r}}{\pi^{b_{r-1}}} \bmod \pi_{\mathsf{L}}\mathcal{O}_{\mathsf{L}}[x].$$

If we set $\gamma = \beta^{e_r}/\pi^{h_r}$ then $v(\gamma) = e_r v(\beta) - h_r v(\pi) = 0$. If we replace β^{e_r} with $\gamma\pi^{h_r}$ we get

$$\frac{\rho(\beta x)}{\pi^{b_{r-1}}\beta^{a_{r-1}}x^{a_{r-1}}} \equiv \sum_{j=0}^{d_r/e_r} \frac{\rho_{je_r+a_{r-1}}\pi^{jh_r}(\gamma x^{e_r})^j}{\pi^{b_{r-1}}} \bmod \pi_{\mathsf{L}}\mathcal{O}_{\mathsf{L}}[x].$$

Our last step is a change of variable. If we substitute y for γx^{e_r} in the right hand side of the preceding relation then we can define

$$\underline{A}_r(y) := \sum_{j=0}^{d_r/e_r} \underline{\rho_{je_r+a_{r-1}}\pi^{jh_r-b_{r-1}}}y^j \in \underline{\mathsf{K}}[y].$$

to be the *residual polynomial* of $\rho(x)$ that corresponds to the r-th segment of $\mathcal{N}_\rho$.

From our derivation we know the form of the roots of our residual polynomials.

Lemma 3.1 ([33, Lemma 3.1])**.** *Let $\beta_1, \ldots, \beta_n$ be the roots of $\rho(x)$. The roots of $\underline{A}(y) \in \underline{\mathsf{K}}[y]$ are of the form*

$$\underline{\left(\frac{\beta_i^{e_j}}{\pi^{h_j}}\right)}$$

for some $1 \leq i \leq n$ and some $1 \leq j \leq \ell$.

Proof. Without Loss of Generality, assume $\underline{A}(y)$ is the residual polynomial of the j-th segment of the Newton Polygon of ρ. For $1 \leq i \leq n$ let $x_i := \frac{\beta_i}{\beta}$. Then $\rho(\beta x_i) = \rho(\beta \cdot \frac{\beta_i}{\beta}) = \rho(\beta_i) = 0$. Thus βx_i is a root of $\rho(x)$ for $1 \leq i \leq n$. Therefore, x_i is a root of $\rho(\beta x)$ for $1 \leq i \leq n$.

Since we have a congruence relation $(\mathrm{mod}\pi_{\mathsf{L}}\mathcal{O}_{\mathsf{L}}[x])$ between $\rho(\beta x)$ and $\underline{A}(y)$, it stands to reason that if $\rho(\beta x)$ is zero then $\underline{A}(y)$ is as well. Thus it just remains to determine which values of y correspond to $x = x_i$.

The following substitutions were made in deriving $\underline{A}$: $\beta^{e_j} = \gamma\pi^{h_j}$ and $y = \gamma x^{e_j}$. So $y = \gamma x^{e_j} = \frac{\beta^{e_j}}{\pi^{h_j}} x^{e_j}$. Our roots correspond to $x = x_i$. So the roots of $\underline{A}(y)$ are

$$\underline{y} \;=\; \underline{\frac{\beta^{e_j}}{\pi^{h_j}} \cdot x_i^{e_j}} \;=\; \underline{\frac{\beta^{e_j}}{\pi^{h_j}} \cdot \left(\frac{\beta_i}{\beta}\right)^{e_j}} \;=\; \underline{\left(\frac{\beta_i^{e_j}}{\pi^{h_j}}\right)}$$

□

Definition 3.2. Let $\underline{A}(y) \in \underline{\mathsf{K}}[y]$ be the residual polynomial of a segment S of $\mathcal{N}_\rho$ and $\underline{\gamma}$ a root of $\underline{A}(y)$. We call the degree of the splitting field of $\underline{A}_r(y) \in \underline{\mathsf{K}}[y]$ over $\underline{\mathsf{K}}$ the *segmental inertia degree* of S.

3.2 Ramification Polygons

We obtain the ramification data of a totally ramified extension from its ramification polygon. In the past, ramification polygons have been utilized to explain

maximal abelian extensions [54], study reciprocity and ramification groups [75], compute Galois groups [33], and classify extensions [59][68].

Definition 3.3. Assume that the Eisenstein polynomial φ defines the extension 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.

It is clear from construction that the constant term of the ramification polynomial is 0. This implies that the ramification polygon has no y-intercept. Its first, leftmost point is $(1, J_0)$ where $n + J_0 - 1$ is the valuation of $\mathrm{disc}\,(\varphi)$ (see [79]). The other basic properties of the ramification polygon's shape can be attributed to the information in the following lemma.

Lemma 3.4 ([75, Lemma 1])**.** *Let $\varphi(x) = \sum_{i=0}^{n} \varphi_i x^i \in \mathsf{K}[x]$ be an Eisenstein polynomial and $n = e_0 p^m$ with $p \nmid e_0$. Denote by α a root of $\varphi(x)$ and set $\mathsf{L} = \mathsf{K}(\alpha)$. Then the following hold for the coefficients of the polynomial $\psi(x) = \sum_{i=0}^{n} \psi_i x^i := \varphi(\alpha x + \alpha) \in L[x]$:*

(a) $v_{\mathsf{L}}(\psi_i) \geq n$ *for all* i.

(b) $v_{\mathsf{L}}(\psi_{p^m}) = v_{\mathsf{L}}(\psi_n) = n$.

(c) $v_{\mathsf{L}}(\psi_i) \geq v_{\mathsf{L}}(\psi_{p^s})$ *for* $p^s \leq i < p^{s+1}$ *and* $s < m$.

The general shape of a ramification polygon is given in Figure 1. For the purpose of general discussions, the polygon will consist of ℓ non-horizontal segments when $n = p^{v_p(n)}$. Otherwise, the polygon will have $\ell + 1$ segments with the right most segment being horizontal.

As the next proposition shows, the ramification polygon $\mathcal{R}_\varphi$ of an Eisenstein polynomial φ is an invariant of the extension generated by φ.

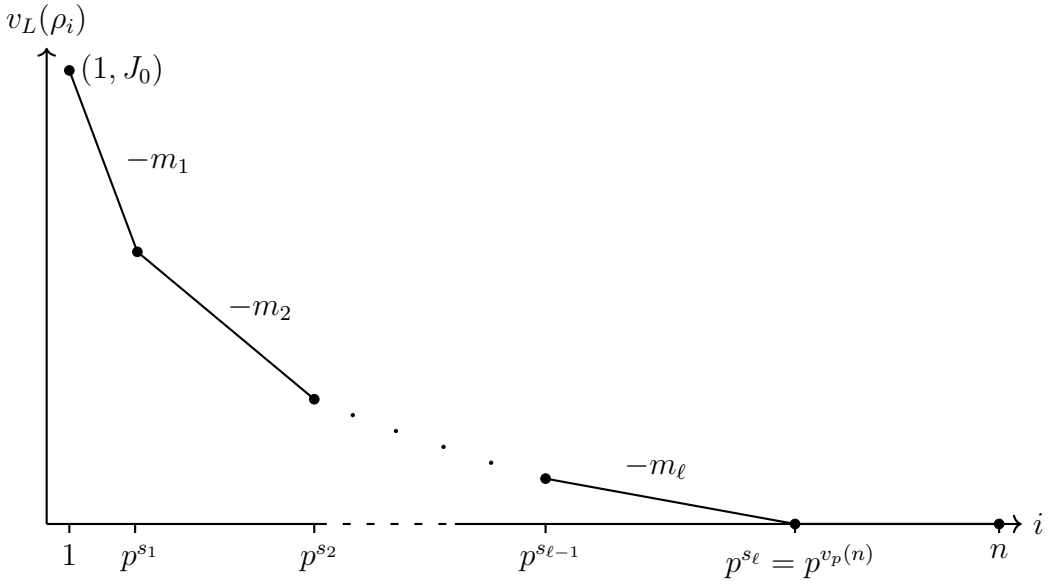

Figure 1. General shape of the ramification polygon of an Eisenstein polynomial of degree n with discriminant $(\pi)^{n+J_0-1}$. Consists of $\ell + 1$ segments.

Proposition 3.5 ([33, Proposition 4.4])**.** *Let* L/K *be totally ramified and* α *a prime element of* L *and* $\varphi(x)$ *the minimal polynomial of* α*. Then* $\mathcal{R}_\varphi$ *and the segmental inertia degree of its segments are invariants of* L/K*. We call* $\mathcal{R}_{\mathsf{L}/\mathsf{K}} := \mathcal{R}_\varphi$ *the ramification polygon of* L/K*.*

We have included the original proof of this result with additional details that have been added to aide the reader.

Proof. To prove that the ramification polygon is an invariant of L/K, we must demonstrate that it is not dependent on the choice of the uniformizing element of L. To this end, we will take two prime elements of L and show that their minimal polynomials have the same ramification polygon. Since we are given α as a prime element, we need only to consider one additional element. We will let β denote this second prime element. By definition, this means that α and β generate the same ideal. Therefore,

there must exist $\delta \in \mathcal{O}_{\mathsf{L}} = \mathcal{O}_{\mathsf{K}}[\alpha]$ with $v_{\mathsf{L}}(\delta) = 0$ so that $\beta = \delta\alpha$. In short, β is the product of α and a unit.

Let $\alpha = \alpha_1, \ldots, \alpha_n$ denote the roots of $\varphi(x)$ in some algebraic closure of K. We can write $\delta = \delta(\alpha) = \delta_0 + \delta_1\alpha + \delta_2\alpha^2 + \ldots$ with $\delta_i \in \mathcal{O}_{\mathsf{K}}$. Let $\beta = \beta_1, \ldots, \beta_n$ be the conjugates of β and let $\widetilde{\varphi}(x)$ be the minimal polynomial of β. We compare the roots of the ramification polynomials (ρ and $\widetilde{\rho}$ respectively) of $\varphi(x)$ and $\widetilde{\varphi}(x)$

$$\rho(x) = x\prod_{i=2}^{n}\left(x - \frac{\alpha_i - \alpha}{\alpha}\right) = x\prod_{i=2}^{n}\left(x - \left(-1 + \frac{\alpha_i}{\alpha}\right)\right)$$

and

$$\widetilde{\rho}(x) = x\prod_{i=2}^{n}\left(x - \frac{\beta_i - \beta}{\beta}\right) = x\prod_{i=2}^{n}\left(x - \left(-1 + \frac{\beta_i}{\beta}\right)\right).$$

For $1 \leq i \leq n$ long division yields

$$\frac{\beta_i}{\beta} = \frac{\delta(\alpha_i)\cdot\alpha_i}{\delta(\alpha)\cdot\alpha} = \frac{\delta_0\alpha_i + \delta_1\alpha_i^2 + \ldots}{\delta_0\alpha + \delta_1\alpha^2 + \ldots} = \frac{\alpha_i}{\alpha} + \frac{\delta_1(\alpha_i - \alpha)\alpha_i + \ldots}{\delta_0\alpha + \delta_1\alpha^2 + \ldots}.$$

Since adding 1 and negating gives us an equivalent equation, we have that

$$1 - \frac{\beta_i}{\beta} = 1 - \frac{\alpha_i}{\alpha} - \frac{\delta_1(\alpha_i - \alpha)\alpha_i + \ldots}{\delta_0\alpha + \delta_1\alpha^2 + \ldots}. \tag{3.1}$$

Since $-1 + \frac{\alpha_i}{\alpha}$ is a root of ρ, $v_{\mathsf{L}}(-1 + \alpha_i/\alpha) = m$ where $-m \in \mathbb{Q} \cup \{\infty\}$ is the slope of a segment of the Newton Polygon of ρ (i.e. $\mathcal{R}_\varphi$). We have that

$$\begin{aligned} v_{\mathsf{L}}((\alpha_i - \alpha)\alpha_i) &= v_{\mathsf{L}}\left(\alpha\alpha_i\left(-1 + \frac{\alpha_i}{\alpha}\right)\right) \\ &= v_{\mathsf{L}}(\alpha\alpha_i) + v_{\mathsf{L}}\left(-1 + \frac{\alpha_i}{\alpha}\right) \\ &= v_{\mathsf{L}}(\alpha) + v_{\mathsf{L}}(\alpha_i) + m \\ &= m + 2. \end{aligned}$$

As a result, $\delta_1(\alpha_i - \alpha)\alpha_i$ has valuation $m+2$ and $\frac{\delta_1(\alpha_i-\alpha)\alpha_i+\ldots}{\delta_0\alpha+\delta_1\alpha^2+\ldots}$ has valuation $m+1$. So

$$\begin{aligned} v_{\mathsf{L}}\left(1-\frac{\alpha_i}{\alpha}\right) &= v_{\mathsf{L}}\left(-1+\frac{\alpha_i}{\alpha}\right) \\ &= m \\ &< m+1 \\ &= v_{\mathsf{L}}\left(-\frac{\delta_1(\alpha_i-\alpha)\alpha_i+\ldots}{\delta_0\alpha+\delta_1\alpha^2+\ldots}\right) \\ &= v_{\mathsf{L}}\left(1-\frac{\beta_i}{\beta}-\left(1-\frac{\alpha_i}{\alpha}\right)\right) \text{ by (3.1).} \end{aligned}$$

Hence, we have that $1-\beta_i/\beta \sim 1-\alpha_i/\alpha$. As we noted in our comments following Definition 2.9 this implies that $v_{\mathsf{L}}(1-\beta_i/\beta) = v_{\mathsf{L}}(1-\alpha_i/\alpha) = m$. Because $-1+\beta_i/\beta$ is a root of $\widetilde{\rho}$, we know that $\mathcal{R}_{\widetilde{\varphi}}$ has a segment of slope $-m$. Thus, the segments of $\mathcal{R}_{\widetilde{\varphi}}$ have the same slopes as those of $\mathcal{R}_{\varphi}$. Furthermore, since $v_{\mathsf{L}}(-1+\beta_i/\beta) = v_{\mathsf{L}}(-1+\alpha_i/\alpha)$ for $1 \le i \le n$, the segments have the same length and endpoints.

It follows that the slopes of the ramification polygon are independent of the choice of the uniformizing (prime) element of L and therefore invariants of L.

To prove that the segmental inertia degree is an invariant of L/K we consider the segment with slope $-m = -h/e$ of the Newton polygons of $\rho(x)$ and $\widetilde{\rho}(x)$.

According to Lemma 3.1, the roots of the corresponding residual polynomials $\underline{A}(y) \in \underline{\mathsf{L}}[y]$ and $\underline{\widetilde{A}}(y) \in \underline{\mathsf{L}}[y]$ with respect to the segment with slope $-m$ are of the form:

$$\underline{\left(\frac{(-1+\alpha_i/\alpha)^e}{\alpha^h}\right)} \quad \text{and} \quad \underline{\left(\frac{(-1+\beta_i/\beta)^e}{\beta^h}\right)}.$$

Because $-1+\beta_i/\beta \sim -1+\alpha_i/\alpha$ we have

$$\frac{(-1+\beta_i/\beta)^e}{\beta^h} \sim \frac{(-1+\alpha_i/\alpha)^e}{\beta^h} = \frac{1}{\delta^h}\frac{(-1+\alpha_i/\alpha)^e}{\alpha^h}.$$

This tells us that the roots of the residual polynomial can change by a factor of δ^{-h} if we change the uniformizer by a factor of δ. Therefore the roots of $\underline{A}(y)$ and $\widetilde{\underline{A}}(y)$ differ only by the factor $\underline{\delta}^{-h} \in \underline{\mathsf{L}} = \underline{\mathsf{K}}$. So, if $\underline{A}(y) = \prod_{i=1}^{d}(y-\gamma_i)$ then $\widetilde{\underline{A}}(y) = \prod_{i=1}^{d}(y-\gamma_i\underline{\delta}^{-h})$. Clearly the polynomials $\underline{A}(y)$ and $\widetilde{\underline{A}}(y)$ have the same splitting fields which implies that the segmental inertia degrees are the same. □

Thus the zeros of the residual polynomials of the ramification polygon change by powers of the same element $\underline{\delta}$ when transitioning from a uniformizer α to a uniformizer $\delta\alpha$. By [68, Theorem 4.8] this yields an invariant of L/K.

Definition 3.6. Let $\mathcal{S}_1,\dots,\mathcal{S}_\ell$ be the segments of the ramification polygon $\mathcal{R}$ of an Eisenstein polynomial $\varphi \in \mathcal{O}_\mathsf{K}[x]$. For $1 \le i \le \ell$ let $-h_i/e_i$ be the slope of $\mathcal{S}_i$ and $\underline{A}_i(x)$ its residual polynomial. The *residual polynomial classes* of the extension $\mathsf{K}[x]/(\varphi)$ are

$$\mathcal{A} = \left\{ \left(\gamma_{\delta,1}\underline{A}_1(\underline{\delta}^{h_1}x),\dots,\gamma_{\delta,\ell}\underline{A}_\ell(\underline{\delta}^{h_\ell}x)\right) : \underline{\delta} \in \underline{\mathsf{K}}^\times \right\} \tag{3.2}$$

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 $1 \le i \le \ell-1$.

The segmental inertia degree of a segment can be computed as the least common multiple of the degrees of the irreducible factors of the corresponding entry in a representative of $\mathcal{A}$. So using the residual polynomial classes results in a refinement of the segmental inertia degrees. See [68] for an algorithm that enumerates representatives of $\underline{A}_1,\dots,\underline{A}_\ell$ for possible residual polynomial classes $\mathcal{A}$.

In future sections, we will be interested in ramification polygons for composites of wildly and tamely ramified extensions. The following result and its proof will be essential to future discussions.

Lemma 3.7 ([33, Lemma 4.5])**.** *Let* L/K *be totally ramified of degree* p^m *and let* $-m_1, \ldots, -m_\ell$ *be the slopes of* $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$*. Let* T/K *be tamely ramified with ramification index* e_0 *and* $\mathsf{N} = \mathsf{TL}$*. Then the slopes of* $\mathcal{R}_{\mathsf{N}/\mathsf{T}}$ *are* $-e_0 \cdot m_1, \ldots, -e_0 \cdot m_\ell$*.*

Proof. Let α and β denote prime elements of L and T respectively. Also, let $\varphi(x)$ be the minimal polynomial of α and $\alpha = \alpha_1, \ldots, \alpha_{p^m}$ its roots in some algebraic closure of K. Then according to Proposition 2.38 and Proposition 2.39 the extension N/K has the subfield diagram shown in Figure 2.

Because $\gcd(e_0, p^m) = 1$, there exist integers a and b that satisfy $ae_0 - bp^m = 1$. Using these cofactors we have that

$$\begin{aligned} v_{\mathsf{T}}(\alpha^a/\beta^b) &= e_0 \cdot v_{\mathsf{K}}(\alpha^a/\beta^b) \\ &= e_0 \left[v_{\mathsf{K}}(\alpha^a) - v_{\mathsf{K}}(\beta^b) \right] \\ &= e_0 \left[a \cdot v_{\mathsf{K}}(\alpha) - b \cdot v_{\mathsf{K}}(\beta) \right] \\ &= e_0 \left[a \cdot \frac{1}{p^m} - b \cdot \frac{1}{e_0} \right] \\ &= e_0 \left[\frac{ae_0 - bp^m}{e_0 p^m} \right] \\ &= \frac{ae_0 - bp^m}{p^m} = \frac{1}{p^m}. \end{aligned}$$

Thus if we let $\psi(x)$ denote the minimal polynomial of α^a/β^b we find that $\mathsf{N} \cong \mathsf{T}[x]/(\psi(x))$. Furthermore, the roots of ψ are α_i^a/β^b for $1 \leq i \leq p^m$.

The ramification polynomial of $\psi(x)$ is an element of $\mathcal{O}_{\mathsf{N}}[x]$ of the form

$$\begin{aligned}\widetilde{\rho}(x) :&= x\prod_{i=2}^{p^m}\left(x-\left(-1+\frac{\alpha_i^a}{\beta^b}\div\frac{\alpha^a}{\beta^b}\right)\right)\\ &= x\prod_{i=2}^{p^m}\left(x-\left(-1+\frac{\alpha_i^a}{\beta^b}\cdot\frac{\beta^b}{\alpha^a}\right)\right)\\ &= x\prod_{i=2}^{p^m}\left(x+1-\frac{\alpha_i^a}{\alpha^a}\right).\end{aligned}$$

For each $1\leq i\leq p^m$, $v_{\mathsf{L}}(-1+\alpha_i/\alpha)=m_q$ for some $1\leq q\leq \ell$. Thus, there exists a unit δ_i such that $\alpha_i/\alpha = 1+\delta_i\alpha^{m_q}$. Because $1=e_0a+(-bp^{m-1})p$ we have that a and p are coprime. This implies that $(1+\delta_i\alpha^{m_q})^a\sim 1+a\delta_i\alpha^{m_q}$.

The slopes of the segments of $\mathcal{R}_{\mathsf{N}/\mathsf{T}}$ are the negatives of the valuations of the roots of $\widetilde{\rho}(x)\in\mathcal{O}_{\mathsf{N}}[x]$:

$$\begin{aligned}v_{\mathsf{N}}\left(-1+\frac{\alpha_i^a}{\alpha^a}\right) &= v_{\mathsf{N}}(-1+(1+a\delta_i\alpha^{m_q}))\\ &= v_{\mathsf{N}}(a\delta_i\alpha^{m_q})\\ &= e_0\cdot v_{\mathsf{L}}(a\delta_i\alpha^{m_q})\\ &= e_0\left[v_{\mathsf{L}}(a\delta_i)+v_{\mathsf{L}}(\alpha^{m_q})\right]\\ &= e_0\cdot m_q\cdot v_{\mathsf{L}}(\alpha)\\ &= e_0\cdot m_q\end{aligned}$$

for some $1\leq q\leq\ell$. The result follows from the fact that there is a one to one correspondence between the roots of the ramification polynomial of $\varphi(x)$ of valuation m_q and the roots of $\widetilde{\rho}(x)$ of valuation $e_0\cdot m_q$. □

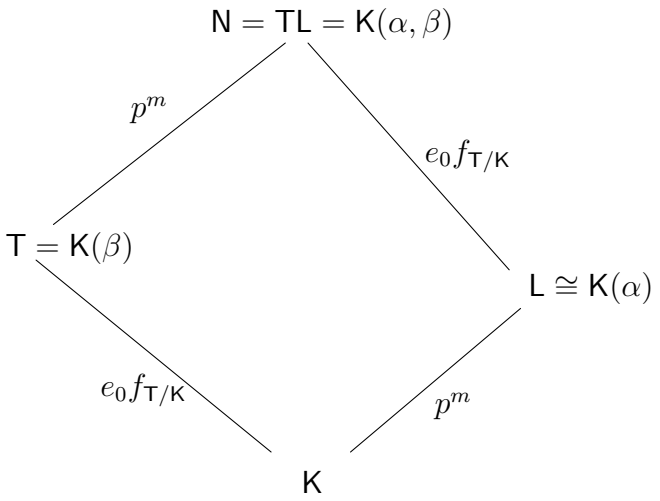

Figure 2. Composite of a wildly ramified extension L/K of degree p^m and a tamely ramified extension T/K with ramification index e_0.

3.3 Blocks and Subfields

Let $\varphi(x) \in \mathcal{O}_\mathsf{K}[x]$ be Eisenstein, α a root of φ and $\mathsf{L} = \mathsf{K}(\alpha)$. In this section, we discuss the connection between the ramification polygon $\mathcal{R}_\varphi$ of φ and a corresponding collection of blocks of the Galois group $G = \mathrm{Gal}(\varphi) = \mathrm{Gal}(\mathsf{L}/\mathsf{K})$. These blocks, in turn, will be used to compute a chain of subfields of the extension L/K.

Let $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ be the set of roots of φ in some algebraic closure of K. Since φ is irreducible, G acts transitively on Ω.

Definition 3.8. A non-empty subset Δ of Ω is called a *block*, if $\sigma(\Delta) \cap \Delta \in \{\emptyset, \Delta\}$ for all $\sigma \in G$. The group $G_\Delta := \{\sigma \in G \mid \sigma(\Delta) = \Delta\}$ is called the *stabilizer* of Δ. The set $\{\Delta = \Delta^{(1)}, \ldots, \Delta^{(k)}\} := \{\sigma(\Delta) \mid \sigma \in G\}$ is the *block system* with respect to Δ. It constitutes a partition of Ω, thus $n = k \cdot |\Delta|$.

Before we can introduce the aforementioned blocks, some notation must be established. We denote by $\rho(x) = \sum_{j=0}^{n} \rho_j x^j$ the ramification polynomial of φ where

the degree of φ is $n = e_0 p^m$ with $p \nmid e_0$. We will also assume that $\mathcal{R}_\varphi$ has $\ell + 1$ segments and the last segment $(p^m, 0) \leftrightarrow (n, 0)$ is horizontal. Astute readers will note that for every result in this section there is an analogous result for the case where $\mathcal{R}_\varphi$ consists of ℓ non-horizontal segments.

From Lemma 3.4 we know that the x-coordinates of the endpoints of the segments in $\mathcal{R}_\varphi$ are of the form p^s where s is a whole number. We will set $0 = s_0 < s_1 < \ldots < s_\ell = m$ so that for $1 \leq i \leq \ell + 1$ the i-th segment of $\mathcal{R}_\varphi$ is

$$(p^{s_{i-1}}, \nu_{\mathsf{L}}(\rho_{p^{s_{i-1}}})) \leftrightarrow (p^{s_i}, \nu_{\mathsf{L}}(\rho_{p^{s_i}})).$$

In addition, the slopes of $\mathcal{R}_\varphi$ will be denoted by $-m_1 < -m_2 < \ldots < -m_{\ell+1} = 0$.

In the last section, we saw that each root α_i of φ corresponds to a root $\frac{\alpha_i - \alpha_1}{\alpha_1}$ of $\rho(x)$ when we set $\alpha_1 = \alpha$. We will use this to renumber the roots in Ω so that the roots α_i satisfying $v_{\mathsf{L}}(\frac{\alpha_i - \alpha_1}{\alpha_1}) = m_j$ will precede those satisfying $v_{\mathsf{L}}(\frac{\alpha_i - \alpha_1}{\alpha_1}) = m_{j+1}$ for $1 \leq j \leq \ell$. In other words, for the i-th segment of $\mathcal{R}_\varphi$ we get

$$v_{\mathsf{L}}\left(\frac{\alpha_{p^{s_{i-1}+1}} - \alpha_1}{\alpha_1}\right) = \ \ldots \ = v_{\mathsf{L}}\left(\frac{\alpha_{p^{s_i}} - \alpha_1}{\alpha_1}\right) = m_i.$$

In the lemma below, we define a collection of blocks of G whose block systems refine the prescribed root ordering above.

Lemma 3.9 ([32, Lemma 4.16])**.** *The Galois group of $\varphi(x)$ has the blocks*

$$\Delta_i = \{\alpha_1, \ldots, \alpha_{p^{s_i}}\} = \{\alpha' \in \overline{\mathsf{K}} \mid \varphi(\alpha') = 0 \text{ and } v_{\mathsf{L}}(\alpha' - \alpha_1) \geq m_i + 1\} \quad (1 \leq i \leq \ell).$$

We can order the roots $\alpha_1, \ldots, \alpha_n$ such that $\Delta_i^{(r)} = \left\{\alpha_{(r-1)p^{s_i}+1}, \ldots, \alpha_{rp^{s_i}}\right\}$ for $1 \leq r \leq k$ and $k = n/p^{s_i}$.

Proof. Assume $\sigma \in \mathrm{Gal}(\varphi)$. We have that $\alpha_1 \in \Delta_i$ regardless of the value of i, so we are interested in α_1 and $\sigma(\alpha_1)$. There are 2 cases to consider.

Case 1: $\sigma(\alpha_1) \in \Delta_i$.

Then we have $v_{\mathsf{L}}(\sigma(\alpha_1) - \alpha_1) \geq m_i + 1$. Let $\alpha_k \in \Delta_i$ be arbitrary. Then

$$\begin{aligned} v_{\mathsf{L}}(\sigma(\alpha_k) - \alpha_1) &= v_{\mathsf{L}}(\sigma(\alpha_k) - \sigma(\alpha_1) + \sigma(\alpha_1) - \alpha_1) \\ &= v_{\mathsf{L}}(\sigma(\alpha_k - \alpha_1) + (\sigma(\alpha_1) - \alpha_1)) \quad \text{since } \sigma \text{ is a homomorphism.} \end{aligned}$$

Since $\alpha_k \in \Delta_i$ we know that $v_{\mathsf{L}}(\alpha_k - \alpha_1) \geq m_i + 1$. Because σ is an automorphism, $\sigma(\alpha_k - \alpha_1)$ and $\alpha_k - \alpha_1$ have the same minimal polynomial and the negative of the slope of its Newton Polygon gives its valuation, thus $v_{\mathsf{L}}(\sigma(\alpha_k - \alpha_1)) = v_{\mathsf{L}}(\alpha_k - \alpha_1) \geq m_i + 1$. Hence we find that:

$$\begin{aligned} v_{\mathsf{L}}(\sigma(\alpha_k) - \alpha_1) &= v_{\mathsf{L}}(\sigma(\alpha_k - \alpha_1) + (\sigma(\alpha_1) - \alpha_1)) \\ &\geq \min\{v_{\mathsf{L}}(\sigma(\alpha_k - \alpha_1)), v_{\mathsf{L}}(\sigma(\alpha_1) - \alpha_1)\} \\ &\geq m_i + 1 \end{aligned}$$

which implies that $\sigma(\alpha_k) \in \Delta_i$. Since α_k was selected arbitrarily, we conclude that $\sigma(\alpha_k) \in \Delta_i$ for all $\alpha_k \in \Delta_i$. Therefore, $\sigma(\Delta_i) \cap \Delta_i = \Delta_i$.

Case 2: $\sigma(\alpha_1) \notin \Delta_i$.

Then we have $v_{\mathsf{L}}(\sigma(\alpha_1) - \alpha_1) < m_i + 1$. If we choose $\alpha_k \in \Delta_i$ arbitrarily, then $v_{\mathsf{L}}(\sigma(\alpha_k - \alpha_1)) \geq m_i + 1$ and

$$\begin{aligned} v_{\mathsf{L}}(\sigma(\alpha_k) - \alpha_1) &= v_{\mathsf{L}}(\sigma(\alpha_k - \alpha_1) + (\sigma(\alpha_1) - \alpha_1)) \\ &= \min\{v_{\mathsf{L}}(\sigma(\alpha_k - \alpha_1)), v_{\mathsf{L}}(\sigma(\alpha_1) - \alpha_1)\} \\ &= v_{\mathsf{L}}(\sigma(\alpha_1) - \alpha_1) \\ &< m_i + 1. \end{aligned}$$

As a result, we have that $\sigma(\alpha_k) \notin \Delta_i$. Because α_k was chosen arbitrarily, we conclude that $\sigma(\alpha_k) \notin \Delta_i$ for all $\alpha_k \in \Delta_i$. Therefore, $\sigma(\Delta_i) \cap \Delta_i = \emptyset$.

In all cases, $\sigma(\Delta_i) \cap \Delta_i \in \{\emptyset, \Delta_i\}$. □

From Galois Theory, we know that there exists a correspondence between blocks of $\mathrm{Gal}(\varphi)$ and the fixed fields of the stabilizers of the blocks. Since $\mathrm{Gal}(\varphi) = \mathrm{Gal}(\mathsf{L}/\mathsf{K})$, these fixed fields are subfields of L/K. If $H \leq \mathrm{Gal}(\varphi)$ then $\mathrm{Fix}(H)$ will be used to denote the fixed field under H. We summarize this correspondence in the theorem below. Its proof can be located in [48].

Theorem 3.10. *Let $\varphi(x) \in \mathsf{K}[x]$ be irreducible of degree n, $\varphi(\alpha) = 0$, $\mathsf{L} = \mathsf{K}(\alpha)$, and G the Galois group of L/K.*

(a) The correspondence $\Delta \mapsto \mathrm{Fix}(G_\Delta)$ is a bijection between the set of blocks containing α and the set of subfields of L/K.

(b) For two blocks Δ_1, Δ_2 with corresponding subfields $\mathsf{L}_1, \mathsf{L}_2$ we have $\mathsf{L}_1 \subseteq \mathsf{L}_2$ if and only if $\Delta_2 \subseteq \Delta_1$.

$$
\begin{array}{rll}
 & \mathsf{L} = \mathsf{K}(\alpha_1) = \mathsf{L}_0 & \Delta_0 = \{\alpha_1\} \\
p^{s_1} & \cup & \cap \\
 & \mathsf{L}_1 = \mathsf{K}(\alpha_1 \cdots \alpha_{p^{s_1}}) & \Delta_1 = \{\alpha_1, \ldots, \alpha_{p^{s_1}}\} \\
p^{s_2 - s_1} & \cup & \cap \\
 & \vdots & \vdots \\
p^{s_{\ell-1} - s_{\ell-2}} & \cup & \cap \\
 & \mathsf{L}_{\ell-1} = \mathsf{K}(\alpha_1 \cdots \alpha_{p^{s_{\ell-1}}}) & \Delta_{\ell-1} = \{\alpha_1, \ldots, \alpha_{p^{s_{\ell-1}}}\} \\
p^{s_\ell - s_{\ell-1}} & \cup & \cap \\
 & \mathsf{L}_\ell = \mathsf{K}(\alpha_1 \cdots \alpha_{p^{s_\ell}}) & \Delta_\ell = \{\alpha_1, \ldots, \alpha_{p^{s_\ell}}\} \\
e_0 & \cup & \cap \\
 & \mathsf{K} = \mathsf{L}_{\ell+1} & \Delta_{\ell+1} = \{\alpha_1, \ldots, \alpha_n\}
\end{array}
$$

Figure 3. Subfields of $\mathsf{L} = \mathsf{K}(\alpha_1)$ and the corresponding blocks, where the roots of $\alpha_1, \ldots, \alpha_n$ of $\varphi(x) \in \mathcal{O}_\mathsf{K}[x]$ are ordered as in Lemma 3.9 and $n = e_0 p^{s_\ell}$ with $p \nmid e_0$.

(c) If Δ is a block and the characteristic polynomial of $\delta = \prod_{\beta \in \Delta} \beta$ is square free then $\mathrm{Fix}(G_\Delta) = \mathsf{K}(\delta)$.

In the next theorem, we elaborate further on the form of the aforementioned subfields of L/K. Consult Figure 3.

Theorem 3.11 ([32, Satz 4.17])**.** *Let the roots $\alpha_1, \ldots, \alpha_n$ of $\varphi(x)$ be ordered as in Lemma 3.9. Let $\mathsf{L} = \mathsf{K}(\alpha)$ and for $0 \leq i \leq \ell$ let $\mathsf{L}_i = \mathsf{K}(\beta_i)$ with $\beta_i = \alpha_1 \cdot \ldots \cdot \alpha_{p^{s_i}}$. Then $\mathsf{L} = \mathsf{L}_0 \supset \mathsf{L}_1 \supset \ldots \supset \mathsf{L}_\ell \supset \mathsf{K}$ with $[\mathsf{L}_i : \mathsf{L}_{i+1}] = p^{s_{i+1} - s_i}$ for $i \leq \ell - 1$ and $[\mathsf{L}_\ell : \mathsf{K}] = e_0$.*

Proof. We will demonstrate that $\mathsf{L}_i = \mathrm{Fix}(G_{\Delta_i})$ for $\Delta_i = \{\alpha_1, \ldots, \alpha_{p^{s_i}}\}$. Since $\sigma(\beta_i) = \beta_i$ for all $\sigma \in G_{\Delta_i}$, and $\mathsf{L}_i = \mathsf{K}(\beta_i)$, we have $\mathsf{L}_i \subseteq \mathrm{Fix}(G_{\Delta_i}) \subseteq \mathsf{L}$. It remains now to

show that $[\mathrm{Fix}(G_{\Delta_i}) : \mathsf{L}_i] = 1$. We begin by finding the valuation of β_i. We have that

$$\begin{aligned} v_{\mathsf{K}}(\beta_i) &= v_{\mathsf{K}}(\alpha_1 \cdot \ldots \cdot \alpha_{p^{s_i}}) \\ &= \sum_{j=1}^{p^{s_i}} v_{\mathsf{K}}(\alpha_j) \\ &= \sum_{j=1}^{p^{s_i}} \frac{1}{n} \quad \text{since } \varphi \text{ is Eisenstein.} \\ &= p^{s_i}/n \\ &= 1/w \quad \text{for some } w \in \mathbb{N}. \end{aligned}$$

Since L/K is totally ramified, all of its subfields are totally ramified. Thus $v_{\mathsf{K}}(\beta_i) = 1/w$ implies that $\mathsf{L}_i = \mathsf{K}(\beta_i)$ is totally ramified with degree $[\mathsf{L}_i : \mathsf{K}] = w = n/p^{s_i}$. Furthermore, since $\mathsf{L}_i \subseteq \mathrm{Fix}(G_{\Delta_i})$ we have that $[\mathsf{L}_i : \mathsf{K}]$ divides $[\mathrm{Fix}(G_{\Delta_i}) : \mathsf{K}]$. Thus there exists $c_1 \in \mathbb{N}$ so that $[\mathrm{Fix}(G_{\Delta_i}) : \mathsf{K}] = c_1[\mathsf{L}_i : \mathsf{K}] = c_1 \cdot (n/p^{s_i})$.

Let $\psi(x) = \prod_{\alpha_k \in \Delta_i}(x - \alpha_k)$ and let $\sigma \in G_{\Delta_i}$. Then $\prod_{\alpha_k \in \Delta_i}(x - \sigma(\alpha_k)) = \psi(x)$. In short, $\psi(x) \in \mathrm{Fix}(G_{\Delta_i})[x]$. Because $\deg(\psi) = p^{s_i}$ and ψ divides φ, we have that ψ is the minimal polynomial of α_1. Thus, because L contains a root of ψ, p^{s_i} divides $[L : \mathrm{Fix}(G_{\Delta_i})]$. Therefore, there exists $c_2 \in \mathbb{N}$ so that $[L : \mathrm{Fix}(G_{\Delta_i})] = c_2 p^{s_i}$. Putting these results together we have that

$$\begin{aligned} n = [\mathsf{L} : \mathsf{K}] &= [\mathsf{L} : \mathrm{Fix}(G_{\Delta_i})] \cdot [\mathrm{Fix}(G_{\Delta_i}) : \mathsf{K}] \\ &= c_2 p^{s_i} c_1 \cdot (n/p^{s_i}) \\ &= c_2 c_1 \cdot n. \end{aligned}$$

Therefore $c_2c_1 = 1$ meaning $c_1 = c_2 = 1$. Hence, $[\mathrm{Fix}(G_{\Delta_i}) : \mathsf{K}] = c_1[\mathsf{L}_i : \mathsf{K}] = [\mathsf{L}_i : \mathsf{K}]$ which tells us that

$$[\mathrm{Fix}(G_{\Delta_i}) : \mathsf{L}_i] = \frac{[\mathrm{Fix}(G_{\Delta_i}) : \mathsf{K}]}{[\mathsf{L}_i : \mathsf{K}]} = 1.$$

So, $\mathsf{L}_i = \mathrm{Fix}(G_{\Delta_i})$ and $[\mathsf{L} : \mathrm{Fix}(G_{\Delta_i})] = c_2 p^{s_i} = p^{s_i}$. The rest of the proof follows from Theorem 3.10. □

Next we describe how to compute the tower of extensions $\mathsf{L}_0 \supset \mathsf{L}_1 \supset \cdots \supset \mathsf{L}_m = \mathsf{K}$ where $m = \ell$ or $m = \ell + 1$. Since the ramification polygon $\mathcal{R}_\varphi$ of φ is the Newton polygon of the ramification polynomial $\rho(x) = \varphi(\alpha x + \alpha)/\alpha^n \in \mathsf{K}(\alpha)[x]$ it yields a factorization $\rho = \rho_1 \cdot \cdot \rho_m$ of ρ over $\mathsf{K}(\alpha)$ where for $1 \leq i \leq m$ the factor ρ_i corresponds to the i-th segment of $\mathcal{R}_\varphi$. Over $\mathsf{K}(\alpha)$ we obtain the factorization $\varphi = \varphi_1 \cdot \cdots \cdot \varphi_m$ where

$$\varphi_1(x) = (x - \alpha)\rho_1\left(\frac{x - \alpha}{\alpha}\right) \cdot \alpha^{\deg \rho_1}$$

and

$$\varphi_i(x) = \alpha^{\deg \rho_i}\rho_i\left(\frac{x - \alpha}{\alpha}\right) \quad \text{for } 2 \leq i \leq m.$$

Now let $\psi = \prod_{i=1}^{m-1} \varphi_i$. The minimal polynomial $\mu \in \mathcal{O}_\mathsf{K}[x]$ of the constant coefficient $\alpha_1 \cdot \cdots \cdot \alpha_{p^{s_{m-1}}}$. of ψ generates $\mathsf{L}_\ell = \mathsf{K}(\alpha_1 \cdot \cdots \cdot \alpha_{p^{s_{m-1}}})$ over K. We continue this process with $\psi \in \mathsf{L}_{m-1}[x]$ whose ramification polynomial has $m-1$ segments until we have reached $\mathsf{L}_0 = \mathsf{K}(\alpha_1)$.

Algorithm 3.12 (`RamificationPolygonFactors` [32, Algorithmus 4.3])**.**

Input: An Eisenstein polynomial $\varphi \in \mathsf{K}[x]$.

Output: Factors of φ corresponding to the segments of the ramification polygon of φ.

(1) $\mathsf{L} \leftarrow \mathsf{K}(\alpha)$ where α is a root φ.

(2) Determine the ramification polynomial ρ of φ.

(3) Determine the ramification polygon $\mathcal{R}_\varphi$ of φ.

(4) $\rho \leftarrow \rho/x$.

(5) Let $\rho_1(x), \ldots, \rho_{\ell+1}(x)$ be the factors of ρ corresponding to the segments $S_1, \ldots, S_{\ell+1}$ of $\mathcal{R}_\varphi$.

(6) Let $\varphi_1(x) = (x-\alpha)\rho_1(\frac{x-\alpha}{\alpha}) \cdot \alpha^{\deg \rho_1}$.

(7) For $2 \leq i \leq \ell + 1$:

- $\varphi_i \leftarrow \alpha^{\deg \rho_i} \rho_i(\frac{x-\alpha}{\alpha})$.

(8) Return $\varphi_1, \ldots, \varphi_{\ell+1} \in \mathsf{L}[x]$.

Algorithm 3.13 (`RamificationPolygonTower` [32, Algorithmus 4.5])**.**

Input: An Eisenstein polynomial $\varphi \in \mathsf{K}[x]$.

Output: The set $\{\mathsf{L}_i, \ldots, \mathsf{L}_1\}$ such that the extension $\mathsf{L} = \mathsf{K}[x]/(\varphi)$ is the tower of extensions $\mathsf{L} \supset \mathsf{L}_1 \supset \cdots \supset \mathsf{L}_i \supset \mathsf{K}$.

(1) $\mathsf{L} \leftarrow \mathsf{K}(\alpha)$ where α is a root φ.

(2) $\varphi_1, \ldots, \varphi_{i+1} \leftarrow$ `RamificationPolygonFactors`(φ).

(3) If $i = 0$: Return L.

(4) $\psi \leftarrow \varphi_1 \cdot \cdots \cdot \varphi_i$.

(5) Denote by ψ_0 the constant coefficient of ψ.

(6) Compute the minimal polynomial $\mu \in \mathsf{K}[x]$ of ψ_0 over K.

(7) $\mathsf{E} \leftarrow \mathsf{K}[x]/(\mu)$.

(8) Return [E] cat `RamificationPolygonTower`($\psi \in \mathsf{E}[x]$).

For the remainder of this section, assume L/K is Galois. Then φ splits into linear factors over L. Furthermore, since the ramification polynomial ρ is a transformation of φ, ρ also splits into linear factors over L. Thus the roots of ρ lie in L which, in turn, implies that the valuation (v_L) of the nonzero roots $\frac{\alpha_i - \alpha}{\alpha}$ of ρ are integral. Therefore, $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ must have integral slopes.

As the following remark illustrates, the negatives of the slopes of $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ are the ramification breaks of L/K. Put another way, the ramification polygon yields a ramification subgroup for each of its segments.

Remark ([33, Remark 4.1]). If the extension L/K generated by $\varphi(x)$ is Galois with Galois group G the segments of the ramification polygon $\mathcal{R}_\varphi$ correspond to the ramification subgroups of G:

$$G_j := \{\sigma \in G \mid v_{\mathsf{L}}(\sigma(\alpha) - \alpha) \geq j + 1\} \text{ for } j \geq -1.$$

Because $v_{\mathsf{L}}(\frac{\alpha_i - \alpha}{\alpha}) = v_{\mathsf{L}}(\alpha_i - \alpha) - 1$ the ramification polygon describes the filtration $G \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_k = 1$ of the Galois group, that is, a segment of slope $-m$ yields a jump at m in the filtration, which means $G_m \neq G_{m+1}$. If the extension L/K is not Galois, there is a similar interpretation for a filtration of the set of embeddings of L/K in $\overline{\mathsf{K}}$ in the context of non-Galois ramification theory (see [40]).

Before continuing on we will prove the following part of the remark: if a segment of $\mathcal{R}_\varphi$ has a slope of $-m$ then $G_m \neq G_{m+1}$.

Proof. For $m \in \mathbb{N} \cup \{0\}$ we have that $G_m = \{\sigma \in G \mid v_{\mathsf{L}}(\sigma(\alpha) - \alpha) \geq m+1\}$ and that $G_{m+1} = \{\sigma \in G \mid v_{\mathsf{L}}(\sigma(\alpha) - \alpha) \geq m+2\}$. In other words,

$$G_m = \left\{\sigma \in G \mid v_{\mathsf{L}}\left(\frac{\sigma(\alpha) - \alpha}{\alpha}\right) \geq m\right\}$$

and

$$G_{m+1} = \left\{\sigma \in G \mid v_{\mathsf{L}}\left(\frac{\sigma(\alpha) - \alpha}{\alpha}\right) \geq m+1\right\}.$$

Suppose a segment of the ramification polygon has slope $-m$. Then at least one root of ρ has valuation m. Since m is finite, that root is not 0. So there exists $j \in \{2, \ldots n\}$ so that the valuation of $\frac{\alpha_j - \alpha}{\alpha}$ is m. By definition, there exists $\sigma \in G$ so that $\sigma(\alpha) = \alpha_j$. So $v_{\mathsf{L}}\left(\frac{\sigma(\alpha)-\alpha}{\alpha}\right) = m$. Thus $\sigma \in G_m$ and $\sigma \notin G_{m+1}$. Therefore, $G_m \neq G_{m+1}$. □

It follows from the ideas in the above proof that the subfields L_i from Theorem 3.10 are the ramification subfields of our extension L/K. In other words, the subfields L_i are precisely the fixed fields for the ramification subgroups of $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$.

3.4 Ramification Polygons and Subfields

Much of Section 3.3 revolved around taking an Eisenstein polynomial φ and using information from its ramification polygon to compute generating polynomials for a chain of subfields of the field generated by φ. As we saw in the aforementioned section, the relative extensions in this chain were totally ramified and their generating polynomials were related to factors of φ. This implies the existence of a relationship

between $\mathcal{R}_\varphi$ and the ramification polygons of the relative extensions. It is the extent of this relationship that we discuss now.

Maintaining the notation from the previous section, we begin by describing the relationship between $\mathcal{R}_\varphi = \mathcal{R}_{\mathsf{L}/\mathsf{K}}$ and $\mathcal{R}_{\mathsf{L}_1/\mathsf{K}}$ (see Figure 3). Specifically, we are interested in what the segments and residual polynomials of $\mathcal{R}_\varphi$ tell us about the segments and residual polynomials of $\mathcal{R}_{\mathsf{L}_1/\mathsf{K}}$. The following lemma and its proof thoroughly elaborate on what can be determined about $\mathcal{R}_{\mathsf{L}_1/\mathsf{K}}$.

Lemma 3.14 ([33, Lemma 6.1])**.** *Assume the ramification polygon $\mathcal{R}_\varphi = \mathcal{R}_{\mathsf{L}/\mathsf{K}}$ consists of the segments $S_1, \dots, S_{\ell+1}$ of lengths $p^{s_1} - 1, p^{s_2} - p^{s_1}, \dots, n - p^{s_\ell}$ with slopes $-m_1 < \cdots < -m_{\ell+1} = 0$. Then*

(a) the ramification polygon $\mathcal{R}_{\mathsf{L}_1/\mathsf{K}}$ has exactly ℓ segments $T_1, \dots, T_\ell$ of lengths $p^{s_2}/p^{s_1} - 1, (p^{s_3} - p^{s_2})/p^{s_1}, \dots, (n - p^{s_\ell})/p^{s_1}$ with slopes $-m_2, \dots, -m_{\ell+1} = 0$,

(b) the segmental inertia degree of T_i is equal to the segmental inertia degree of S_{i+1}, and

(c) for each root $\underline{\delta}$ of $\underline{A}_{i+1}(y)$ the element $\underline{\delta}^{p^{s_1}}$ is a root of the residual polynomial of T_i.

We have included the original proof of this result with additional details that have been added to aide the reader.

Proof. We assume that the roots of $\varphi(x)$ are ordered as in Lemma 3.9. Let $\Delta_1 = \Delta_1^{(1)}, \dots, \Delta_1^{(k)}$ be the block system for the smallest block Δ_1. If $\alpha \in \Delta_1^{(r)}$ with $2 \le r \le k$, then $v_{\mathsf{L}}(\alpha - \alpha_1) = m_\lambda + 1 < m_1 + 1$ for some $\lambda \in \{2, \dots, \ell + 1\}$. Recall that by our ordering of the roots of $\varphi(x)$ we have $\alpha_i \in \Delta_1^{(1)}$ and $\alpha_{(r-1)p^{s_1}+i} \in \Delta_1^{(r)}$ for $1 \le i \le p^{s_1}$

and $2 \leq r \leq k$. Thus, for some $\lambda \in \{2, \ldots, \ell+1\}$ and some units $\varepsilon, \delta \in \overline{\mathsf{K}}$, we have $\alpha_{(r-1)p^{s_1}+i} = \alpha_1 + \varepsilon\alpha_1^{m_\lambda+1}$ and $\alpha_i = \alpha_1 + \delta\alpha_1^{m_1+1}$. Furthermore,

$$\begin{aligned}
v_{\mathsf{L}}\left(\varepsilon\alpha_1^{m_\lambda} - \left(-1 + \frac{\alpha_{(r-1)p^{s_1}+i}}{\alpha_i}\right)\right) &= v_{\mathsf{L}}\left(\varepsilon\alpha_1^{m_\lambda} + 1 - \frac{\alpha_{(r-1)p^{s_1}+i}}{\alpha_i}\right) \\
&= v_{\mathsf{L}}\left(\frac{\varepsilon\alpha_1^{m_\lambda}\alpha_i + \alpha_i - \alpha_{(r-1)p^{s_1}+i}}{\alpha_i}\right) \\
&= v_{\mathsf{L}}(\varepsilon\alpha_1^{m_\lambda}\alpha_i + \alpha_i - \alpha_{(r-1)p^{s_1}+i}) - 1 \\
&= v_{\mathsf{L}}(\varepsilon\alpha_1^{m_\lambda}\alpha_i + \alpha_1 + \delta\alpha_1^{m_1+1} - (\alpha_1 + \varepsilon\alpha_1^{m_\lambda+1})) - 1 \\
&= v_{\mathsf{L}}(\varepsilon\alpha_1^{m_\lambda}(\alpha_i - \alpha_1) + \delta\alpha_1^{m_1+1}) - 1 \\
&= v_{\mathsf{L}}(\varepsilon\alpha_1^{m_\lambda}(\alpha_1 + \delta\alpha_1^{m_1+1} - \alpha_1) + \delta\alpha_1^{m_1+1}) - 1 \\
&= v_{\mathsf{L}}(\varepsilon\alpha_1^{m_\lambda} \cdot \delta\alpha_1^{m_1+1} + \delta\alpha_1^{m_1+1}) - 1 \\
&= v_{\mathsf{L}}(\delta) + v_{\mathsf{L}}(\varepsilon\alpha_1^{m_\lambda}\alpha_1^{m_1+1} + \alpha_1^{m_1+1}) - 1 \\
&= v_{\mathsf{L}}(\varepsilon\alpha_1^{m_\lambda+m_1+1} + \alpha_1^{m_1+1}) - 1 \\
&\geq \min\{v_{\mathsf{L}}(\varepsilon\alpha_1^{m_\lambda+m_1+1}), v_{\mathsf{L}}(\alpha_1^{m_1+1})\} - 1 \\
&= \min\{m_\lambda + m_1 + 1, m_1 + 1\} - 1 \\
&= m_1 \\
&> m_\lambda \\
&= v_{\mathsf{L}}(\varepsilon\alpha_1^{m_\lambda}).
\end{aligned}$$

So we have that

$$-1 + \frac{\alpha_{(r-1)p^{s_1}+i}}{\alpha_i} \sim \varepsilon\alpha_1^{m_\lambda}. \tag{3.3}$$

For $1 \leq r \leq k$ let $\beta_r = \prod_{\alpha \in \Delta_1^{(r)}} \alpha$, so that $\mathsf{L}_1 = \mathsf{K}(\beta_1)$. Then $\psi(x) = \prod_{r=1}^{k} x - \beta_r$ is the minimal polynomial of β_1 over K. The ramification polynomial of $\psi(x)$ is:

$$\begin{aligned}
\frac{\psi(\beta_1 x + \beta_1)}{\beta_1^k} &= x \prod_{r=2}^{k} \left(x - \left(-1 + \frac{\beta_r}{\beta_1} \right) \right) \\
&= x \prod_{r=2}^{k} \left(x - \left(-1 + \frac{\prod_{\alpha \in \Delta_1^{(r)}} \alpha}{\prod_{\alpha \in \Delta_1^{(1)}} \alpha} \right) \right) \\
&= x \prod_{r=2}^{k} \left(x - \left(-1 + \frac{\alpha_{(r-1)p^{s_1}+1} \cdot \ldots \cdot \alpha_{rp^{s_1}}}{\alpha_1 \cdot \ldots \cdot \alpha_{p^{s_1}}} \right) \right) \\
&= x \prod_{r=2}^{k} \left(x - \left(-1 + \prod_{i=1}^{p^{s_1}} \frac{\alpha_{(r-1)p^{s_1}+i}}{\alpha_i} \right) \right).
\end{aligned}$$

By relation (3.3) there are $\varepsilon_r \in \overline{\mathsf{K}}$ with $v(\varepsilon_r) = 0$ and $\lambda \in \{2, \ldots, \ell + 1\}$ so that

$$\begin{aligned}
-1 + \frac{\beta_r}{\beta_1} &\sim -1 + (1 + \varepsilon_r \alpha_1^{m_\lambda})^{p^{s_1}} \\
&= -1 + \sum_{i=0}^{p^{s_1}} \binom{p^{s_1}}{i} (\varepsilon_r \alpha_1^{m_\lambda})^i \\
&= -1 + \binom{p^{s_1}}{0} (\varepsilon_r \alpha_1^{m_\lambda})^0 + \sum_{i=1}^{p^{s_1}} \binom{p^{s_1}}{i} (\varepsilon_r \alpha_1^{m_\lambda})^i \\
&= -1 + 1 + \sum_{i=1}^{p^{s_1}-1} \binom{p^{s_1}}{i} (\varepsilon_r \alpha_1^{m_\lambda})^i + \binom{p^{s_1}}{p^{s_1}} (\varepsilon_r \alpha_1^{m_\lambda})^{p^{s_1}} \\
&= \varepsilon_r^{p^{s_1}} \alpha_1^{m_\lambda p^{s_1}} + \sum_{i=1}^{p^{s_1}-1} \binom{p^{s_1}}{i} \varepsilon_r^i \alpha_1^{m_\lambda \cdot i}.
\end{aligned}$$

If we show that

$$-1 + \frac{\beta_r}{\beta_1} \sim \varepsilon^{p^{s_1}} \alpha_1^{m_\lambda p^{s_1}}, \tag{3.4}$$

then (a) is proven. For now we assume that relation (3.4) holds and prove (b) and (c) for S_2 and T_1. The results for the other segments follow analogously.

The roots of the ramification polynomial of φ with valuation m_2 are $-1 + \alpha_i/\alpha_1 \sim \varepsilon_i \alpha_1^{m_2}$ for some $\varepsilon_i \in \overline{\mathsf{K}}$ with $v(\varepsilon_i) = 0$ and $p^{s_1} + 1 \leq i \leq p^{s_2}$. By Lemma 3.1 this gives the roots

$$\underline{\left(\frac{(\varepsilon_i \alpha_1^{m_2})^{e_2}}{\alpha_1^{h_2}} \right)} = \underline{\varepsilon_i}^{e_2}$$

of the residual polynomial $\underline{A_2}(y) \in \underline{\mathsf{L}}[y]$ of S_2, where $m_2 = h_2/e_2$ with $\gcd(h_2, e_2) = 1$. For each $\underline{\varepsilon_i}^{e_2}$ of $\underline{A_2}(y)$ there is a root, by (3.4), of the ramification polynomial of $\psi(x)$ with $-1 + \beta_r/\beta_1 \sim \varepsilon_i^{p^{s_1}} \alpha_1^{m_2 \cdot p^{s_1}}$. With this we obtain the corresponding roots of the residual polynomial $\underline{B_1}(y) \in \underline{\mathsf{L}}[y]$ of T_1:

$$\underline{\left(\frac{(\varepsilon_i^{p^{s_1}} \alpha_1^{m_2 p^{s_1}})^{e_2}}{\beta_1^{h_2}} \right)} = \underline{\left(\frac{(\varepsilon_i^{e_2 p^{s_1}} \alpha_1^{h_2 p^{s_1}})}{(\alpha_1 \cdot \ldots \cdot \alpha_{p^{s_1}})^{h_2}} \right)} = \left(\underline{\varepsilon_i}^{e_2} \right)^{p^{s_1}} .$$

In short, if $\underline{\varepsilon_i}^{e_2}$ is a root of $\underline{A_2}(y)$ then $(\underline{\varepsilon_i}^{e_2})^{p^{s_1}}$ is a root of the residual polynomial of T_1. We have proven (c). As $\varepsilon \mapsto \varepsilon^p$ is an automorphism of $\underline{\mathsf{L}}$ the splitting fields of $\underline{A_2}(y)$ and $\underline{B_1}(y)$ are isomorphic, which implies (b).

To prove relation (3.4) we need to show that

$$v_{\mathsf{L}} \left(\sum_{i=1}^{p^{s_1}-1} \binom{p^{s_1}}{i} \varepsilon^i \alpha_1^{m_\lambda i} \right) > m_\lambda p^{s_1}.$$

By the ultrametric inequality, it is sufficient to show that each term in the sum has valuation greater than $m_\lambda p^{s_1}$. In other words, we just need to demonstrate that

$$v_{\mathsf{L}} \left(\binom{p^{s_1}}{i} \varepsilon^i \alpha_1^{m_\lambda i} \right) > m_\lambda p^{s_1} \quad \text{for } 1 \leq i \leq p^{s_1} - 1.$$

As $v_p\left(\binom{p^{s_1}}{i}\right) = s_1 - v_p(i)$ this simplifies to

$$\begin{aligned} m_\lambda p^{s_1} &< v_{\mathsf{L}}\left(\binom{p^{s_1}}{i}\varepsilon^i \alpha_1^{m_\lambda i}\right) \\ &= v_{\mathsf{L}}\left(\binom{p^{s_1}}{i}\right) + v_{\mathsf{L}}(\varepsilon^i \alpha_1^{m_\lambda i}) \\ &= v_{\mathsf{L}}(p) v_p\left(\binom{p^{s_1}}{i}\right) + v_{\mathsf{L}}(\varepsilon^i) + v_{\mathsf{L}}(\alpha_1^{m_\lambda i}) \\ &= v_{\mathsf{L}}(p)(s_1 - v_p(i)) + m_\lambda i. \end{aligned}$$

Subtracting $m_\lambda i$ from both sides and then dividing by $p^{s_1} - i$ we find that

$$\frac{v_L(p)(s_1 - v_p(i))}{p^{s_1} - i} > m_\lambda. \tag{3.5}$$

Furthermore, our knowledge of Ramification Polygons informs us that

$$m_1 = \frac{v_{\mathsf{L}}(p) - v_{\mathsf{L}}(p^{s_1})}{p^{s_1} - 1} \;\leq\; \frac{v_{\mathsf{L}}(p)}{p^{s_1} - 1} \;\leq\; \frac{v_{\mathsf{L}}(p)}{p^{s_1} - p^{s_1 - 1}}$$

This implies that $\frac{v_L(p)}{p^{s_1-1}(p-1)} > m_\lambda$. Replacing m_λ in (3.5) by this new upper bound we conclude that in order to prove (3.4) it is sufficient to show that

$$\frac{v_L(p)(s_1 - v_p(i))}{p^{s_1} - i} \geq \frac{v_L(p)}{p^{s_1-1}(p-1)},$$

which, upon rearrangement, is equivalent to

$$\frac{p(p^{s_1} - i)}{p^{s_1}(p-1)(s_1 - v_p(i))} \leq 1.$$

We write $i = ap^v$ with $p \nmid a$ and $v < s_1$ and obtain

$$\begin{aligned}
\frac{p(p^{s_1} - i)}{p^{s_1}(p-1)(s_1 - v_p(i))} &\leq \frac{p(p^{s_1} - p^v)}{p^{s_1}(p-1)(s_1 - v)} = \frac{p}{p-1} \cdot \frac{p^{s_1 - v} - 1}{p^{s_1 - v}(s_1 - v)} \\
&= \frac{p}{p-1} \cdot \frac{1 - (1/p)^{s_1 - v}}{s_1 - v} = \frac{1 - (1/p)^{s_1 - v}}{1 - (1/p)} \cdot \frac{1}{s_1 - v} \\
&= \left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{s_1 - v - 1}}\right) \frac{1}{s_1 - v} \leq 1.
\end{aligned}$$

This proves (3.4). Relation (3.4) and Figure 3 tell us that the valuation of the roots of the ramification polynomial of $\psi(x)$ are

$$\begin{aligned}
v_{\mathsf{L}_1}\left(-1 + \frac{\beta_r}{\beta_1}\right) &= v_{\mathsf{L}_1}(\varepsilon^{p^{s_1}} \alpha_1^{m_\lambda p^{s_1}}) \\
&= \frac{1}{p^{s_1}} \cdot v_{\mathsf{L}}(\varepsilon^{p^{s_1}} \alpha_1^{m_\lambda p^{s_1}}) \\
&= \frac{1}{p^{s_1}} \left[p^{s_1} v_{\mathsf{L}}(\varepsilon) + p^{s_1} v_{\mathsf{L}}(\alpha_1^{m_\lambda})\right] \\
&= v_{\mathsf{L}}(\varepsilon) + v_{\mathsf{L}}(\alpha_1^{m_\lambda}) \\
&= m_\lambda v_{\mathsf{L}}(\alpha_1) = m_\lambda \quad \text{for } 2 \leq \lambda \leq \ell + 1.
\end{aligned}$$

Therefore, the slopes of $\mathcal{R}_{\mathsf{L}_1/\mathsf{K}} = \mathcal{R}_\psi$ are $-m_2, \ldots, -m_{\ell+1}$. The segment lengths follow from Figure 3 and the related fact that v_{L_1} and v_{L} differ by a factor of $1/p^{s_1}$. □

One of the consequences of Lemma 3.14 is that we can compute the ramification polygon of L_1/K without looking at its generating polynomial. The slopes and segment lengths given by the lemma provide us with enough information to systematically determine the endpoints of the segments. First, we know that $\mathcal{R}_{\mathsf{L}_1/\mathsf{K}}$ has an x-intercept $([\mathsf{L}_1 : \mathsf{K}], 0) = (n/p^{s_1}, 0)$ which is the rightmost point on the polygon. The

remaining endpoints are the left endpoints of the segments. We will describe how to determine them in order up and to the left from the x-intercept.

We would start with the final, rightmost segment of $\mathcal{R}_{\mathsf{L}_1/\mathsf{K}}$. From Lemma 3.14 we know that the segment's length is $(n - p^{s_\ell})/p^{s_1}$. Since this is the length in the x-direction, we subtract it from $[\mathsf{L}_1 : \mathsf{K}]$ to get the x-coordinate of the segment's left endpoint. Next we plug the following information into the slope formula: the segment's slope, the coordinates for the right endpoint $(n/p^{s_1}, 0)$, and the x-coordinate of the left endpoint. This gives us an equation where the only unknown quantity is the y-coordinate of the left endpoint. Solving for this coordinate is straightforward.

We would then repeat the process for the next segment using the most recently found point as the right endpoint of the segment. This would continue until all of the endpoints are determined.

Remark. The leftmost point of $\mathcal{R}_{\mathsf{L}_1/\mathsf{K}}$ is $(1, J)$ where

$$J = \sum_{i=2}^{\ell} m_i \left(\frac{p^{s_i} - p^{s_{i-1}}}{p^{s_1}} \right).$$

Furthermore, if $\mathsf{L}_1 \cong \mathsf{K}[x]/(\psi(x))$ where ψ is Eisenstein, then the valuation of disc (ψ) is $\frac{n}{p^{s_1}} - 1 + J$.

Repeated use of Lemma 3.14 yields similar information for $\mathcal{R}_{\mathsf{L}_2/\mathsf{K}}, \mathcal{R}_{\mathsf{L}_3/\mathsf{K}}, \ldots$,and $\mathcal{R}_{\mathsf{L}_\ell/\mathsf{K}}$. From this we can infer analogous information about the ramification polygons of the relative extensions $\mathsf{L}_{i-1}/\mathsf{L}_i$ in our chain of subfields of L/K. This information is summarized in the following theorem.

Theorem 3.15 ([32, Satz 5.7])**.** *For $1 \leq i \leq \ell + 1$ the ramification polygon $\mathcal{R}_{\mathsf{L}_{i-1}/\mathsf{L}_i}$ consists of exactly one segment, which corresponds to the segment S_i of $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ as follows:*

(a) *The slope of* $\mathcal{R}_{\mathsf{L}_{i-1}/\mathsf{L}_i}$ *is equal to the slope of* S_i.

(b) *The segmental inertia degrees of* $\mathcal{R}_{\mathsf{L}_{i-1}/\mathsf{L}_i}$ *and* S_i *are equal.*

(c) *For each root* $\underline{\delta}$ *of the residual polynomial* $\underline{A}_i(y)$ *of* S_i *the element* $\underline{\delta}^{p^{s_{i-1}}}$ *is a root of the residual polynomial of* $\mathcal{R}_{\mathsf{L}_{i-1}/\mathsf{L}_i}$.

The proof of this theorem follows from induction on i by Lemma 3.14.

3.5 One Segment Splitting Fields

When the ramification polygon of an Eisenstein polynomial $\varphi(x) \in \mathcal{O}_{\mathsf{K}}[x]$ is comprised of exactly one segment, we can quickly determine its splitting field. According to Lemma 3.4 the only way $\mathcal{R}_\varphi$ can be a solitary line is if $p \nmid \deg(\varphi)$ or $\deg(\varphi)$ is a positive power of p. The former case was addressed in a prior chapter, so we will exclusively focus on the case where there exists $m \in \mathbb{N}$ such that $\deg(\varphi)$ is $n = p^m$.

The splitting field of $\varphi(x)$ can be determined from the splitting field of its ramification polynomial $\rho(x) \in \mathsf{K}(\alpha)[x]$. More specifically, the splitting field of $\rho(x)$ is a subfield of the splitting field of $\varphi(x)$. We find this subfield first.

Lemma 3.16 ([33, Lemma 7.1])**.** *Assume that the Newton polygon of* $\rho(x) \in \mathcal{O}_{\mathsf{L}}[x]$ *consists of one segment of slope* $-h/e$ *with* $\gcd(h,e) = 1 = ae + bh$ *for* $a, b \in \mathbb{Z}$ *and* $\gcd(e,p) = 1$. *Assume that its residual polynomial* $\underline{A}(y) \in \underline{\mathsf{L}}[y]$ *is square free and let* f *be its segmental inertia degree. Let* I/L *be the unramified extension of degree* $\operatorname{lcm}(f, [\mathsf{L}(\zeta_e) : \mathsf{L}])$ *and let* $\varepsilon \in \mathcal{O}_{\mathsf{I}}$ *with* $\underline{A}(\underline{\varepsilon}) = 0$. *Then*

$$\mathsf{N} = \mathsf{I}\left(\sqrt[e]{\varepsilon^b \pi_{\mathsf{L}}}\right)$$

is the splitting field of $\rho(x)$.

We have included the original proof of this result with additional details that have been added to aide the reader.

Proof. Denote by $A(x) \in \mathcal{O}_{\mathsf{L}}[x]$ a lift of $\underline{A}(y)$. Let M/L be the minimal unramified extension over which $A(y)$ splits into linear factors, say $A(y) = (y-\gamma_1)\cdot\ldots\cdot(y-\gamma_{\frac{n-1}{e}})$ over M. Let $\mathsf{N} = \mathsf{M}(\beta, \zeta_e)$ where β is a root of $\rho(x)$ and ζ_e is an e-th root of unity. Let $\gamma = \beta^e/\pi_{\mathsf{L}}^h$. Then $\underline{A}(\underline{\gamma}) = 0$ by Lemma 3.1. The field N is the splitting field of $\rho(x)$ if $\rho(x)$, or equivalently $\frac{\rho(\beta x)}{\beta x(\gamma\pi_{\mathsf{L}}^h)^{(n-1)/e}}$, splits into linear factors over N.

In Section 3.1 we found that for the r-th segment $(a_{r-1}, b_{r-1}) \leftrightarrow (a_r, b_r)$ of the Newton polygon $\mathcal{N}_\rho$ we had the following equivalence:

$$\frac{\rho(\beta x)}{\pi_{\mathsf{L}}^{b_{r-1}}\beta^{a_{r-1}}x^{a_{r-1}}} \equiv \sum_{j=0}^{d_r/e_r} \frac{\rho_{je_r+a_{r-1}}\pi_{\mathsf{L}}^{jh_r}(\gamma x^{e_r})^j}{\pi_{\mathsf{L}}^{b_{r-1}}} \bmod \pi_{\mathsf{N}}\mathcal{O}_{\mathsf{N}}[x]$$

where $d_r = a_r - a_{r-1}$ and π_{N} denotes a prime element in $\mathcal{O}_{\mathsf{N}}$. We then established our definition of $\underline{A_r}(y)$ by making the substitution $y = \gamma x^{e_r}$.

In this particular example, we only have one segment so the notation is less cumbersome: $e_r = e$, $h_r = h$, $(a_r, b_r) = (n, 0)$ and $a_{r-1} = 1$. Taking this into consideration we have that

$$\begin{aligned} A(y) &= (y-\gamma_1)\cdot\ldots\cdot(y-\gamma_{\frac{n-1}{e}}) \\ &= (\gamma x^e - \gamma_1)\cdot\ldots\cdot(\gamma x^e - \gamma_{\frac{n-1}{e}}) \\ &= \sum_{j=0}^{\frac{n-1}{e}} \frac{\rho_{je+1}\pi_{\mathsf{L}}^{jh}(\gamma x^e)^j}{\pi_{\mathsf{L}}^{b_{r-1}}} \\ &\equiv \frac{\rho(\beta x)}{\pi_{\mathsf{L}}^{b_{r-1}}\beta^1 x^1} \bmod \pi_{\mathsf{N}}\mathcal{O}_{\mathsf{N}}[x]. \end{aligned}$$

To determine the value of b_{r-1}, we look at the slope:

$$-\frac{h}{e} = \frac{0 - b_{r-1}}{n-1}.$$

Cross multiplying, we discover that $b_{r-1} = \frac{h(n-1)}{e}$. This allows us to update our above relation:

$$\frac{\rho(\beta x)}{\pi_{\mathsf{L}}^{\frac{h(n-1)}{e}} \beta x} \equiv (\gamma x^e - \gamma_1) \cdot \ldots \cdot (\gamma x^e - \gamma_{\frac{n-1}{e}}) \bmod \pi_{\mathsf{N}} \mathcal{O}_{\mathsf{N}}[x].$$

If we then divide both sides by $\gamma^{\frac{n-1}{e}}$ we determine that

$$\frac{\rho(\beta x)}{\pi_{\mathsf{L}}^{\frac{h(n-1)}{e}} \cdot \beta x \cdot \gamma^{\frac{n-1}{e}}} \equiv \left(x^e - \frac{\gamma_1}{\gamma}\right) \cdot \ldots \cdot \left(x^e - \frac{\gamma_{(n-1)/e}}{\gamma}\right) \bmod \pi_{\mathsf{N}} \mathcal{O}_{\mathsf{N}}[x],$$

or, equivalently,

$$\frac{\rho(\beta x)}{\beta x (\gamma \pi_{\mathsf{L}}^h)^{(n-1)/e}} \equiv \left(x^e - \frac{\gamma_1}{\gamma}\right) \cdot \ldots \cdot \left(x^e - \frac{\gamma_{(n-1)/e}}{\gamma}\right) \bmod \pi_{\mathsf{N}} \mathcal{O}_{\mathsf{N}}[x],$$

As $\gcd(e, p) = 1$ for $1 \leq i \leq (n-1)/e$ the polynomials $x^e - \frac{\gamma_i}{\gamma}$ are square free over $\underline{\mathsf{N}}$. Because $\zeta_e \in \mathsf{N}$, they split into linear factors over $\underline{\mathsf{N}}$. Hensel lifting yields a decomposition of $\frac{\rho(\beta x)}{\beta x (\gamma \pi_{\mathsf{L}}^h)^{(n-1)/e}}$ into linear factors. It follows that $\rho(x)$ splits into linear factors over N, thus N is the splitting field of $\rho(x)$.

Over M the polynomial $\frac{\rho(x)}{x}$ splits into irreducible factors $\theta_i(x) = \sum_{j=0}^{e} \theta_{i,j} x^j$ $(1 \leq i \leq (n-1)/e)$. Each θ_i generates a tamely ramified extension. Because such extensions can be generated by binomials, we can explicitly determine the extensions by looking at the constant coefficients $\theta_{i,0}$.

Making the substitution $z = \beta x$ in the last equivalence relation we obtain

$$\frac{\rho(z)}{z(\gamma \pi_{\mathsf{L}}^h)^{(n-1)/e}} \equiv \left(\left(\frac{z}{\beta}\right)^e - \frac{\gamma_1}{\gamma}\right) \cdot \ldots \cdot \left(\left(\frac{z}{\beta}\right)^e - \frac{\gamma_{(n-1)/e}}{\gamma}\right) \bmod \pi_{\mathsf{N}} \mathcal{O}_{\mathsf{N}}[x].$$

Since $\beta^e = \gamma\pi_{\mathsf{L}}^h$, this simplifies to

$$\frac{\rho(z)}{z(\beta^e)^{(n-1)/e}} \equiv \left(\left(\frac{z}{\beta}\right)^e - \frac{\gamma_1}{\gamma}\right) \cdot \ldots \cdot \left(\left(\frac{z}{\beta}\right)^e - \frac{\gamma_{(n-1)/e}}{\gamma}\right) \bmod \pi_{\mathsf{N}}\mathcal{O}_{\mathsf{N}}[x].$$

Multiplying through by $\beta^{n-1} = (\beta^e)^{(n-1)/e}$ gives us that

$$\frac{\rho(z)}{z} \equiv \left(z^e - \frac{\gamma_1}{\gamma}\beta^e\right) \cdot \ldots \cdot \left(z^e - \frac{\gamma_{(n-1)/e}}{\gamma}\beta^e\right) \bmod \pi_{\mathsf{N}}\mathcal{O}_{\mathsf{N}}[x].$$

So, for $1 \leq i \leq \frac{n-1}{e}$, we can set

$$\begin{aligned}\theta_i(x) &\equiv x^e - \frac{\gamma_i}{\gamma}\beta^e \bmod \pi_{\mathsf{N}}\mathcal{O}_{\mathsf{N}}[x] \\ &= x^e - \frac{\gamma_i}{\gamma} \cdot \gamma\pi_{\mathsf{L}}^h \\ &= x^e - \gamma_i\pi_{\mathsf{L}}^h.\end{aligned}$$

As θ_i is a factor of $\rho(x)/x$ and the slope of the polygon of $\rho(x)$ is $-h/e$, the slope of the polygon of θ_i is also $-h/e$. Since the leading term of ρ has valuation 0, so do the leading terms of the θ_i. This implies that the valuation of the constant term of θ_i (which has degree e) must be h. Therefore, for $1 \leq i \leq \frac{n-1}{e}$, $\theta_{i,0} \equiv -\gamma_i\pi_{\mathsf{L}}^h \bmod (\pi_{\mathsf{L}}^{h+1})$.

By Proposition 2.26 the extensions generated by the $\theta_i(x)$ are isomorphic to the extensions generated by the polynomials $x^e - (\gamma_i\pi_{\mathsf{L}}^h)^b\pi_{\mathsf{L}}^{ea} = x^e - \gamma_i^b\pi_{\mathsf{L}}$ with $ae + bh = 1$.

From Proposition 2.42, we find that the composite of the extensions generated by $x^e - \gamma_i^b\pi_{\mathsf{L}}$ would at most yield an additional unramified extension. Adjoining ζ_e takes care of this. In short, if we set $I := M(\zeta_e)$ then we only need one of the polynomials $x^e - \gamma_i^b\pi_{\mathsf{L}}$ to find the splitting field as an extension of I. Therefore, $\mathsf{N} = \mathsf{I}(\sqrt[e]{\gamma_i^b\pi_{\mathsf{L}}})$ for some $1 \leq i \leq \frac{n-1}{e}$. □

In order to construct the splitting field of $\varphi(x)$ we need some information regarding additive polynomials.

Lemma 3.17 ([33, Lemma 7.2])**.** *Let u be a power of p. Let $F(x) = \sum_{i=0}^{r} a_i x^{p^i} \in \mathbb{F}_u[x]$ be an additive polynomial and assume $e \in \mathbb{N}$ is a divisor of $u-1$ and of all p^i-1 for all $1 \leq i \leq r$ with $a_i \neq 0$. If $1 \in \mathbb{F}_u$ is a root of $G(x) = \sum_{i=0}^{r} a_i x^{(p^i-1)/e}$, then $F(x)$ splits into linear factors over $\mathbb{F}_u$, if and only if $G(x)$ splits into linear factors over $\mathbb{F}_u$.*

Theorem 3.18 ([33, Theorem 7.3])**.** *Let $\varphi(x) \in \mathcal{O}_{\mathsf{K}}[x]$ be an Eisenstein polynomial of degree $n = p^m$ and assume that its ramification polygon $\mathcal{R}_\varphi$ consists of one segment of slope $-h/e$ where $\gcd(h,e) = 1 = ae + bh$ for $a, b \in \mathbb{Z}$. Let α be a root of $\varphi(x)$, $\mathsf{L} = \mathsf{K}(\alpha)$ and let $\underline{A}(y) \in \underline{\mathsf{L}}[y]$ be the residual polynomial of $\mathcal{R}_\varphi$ with segmental inertia degree f. Let I/L be the unramified extension of degree $\operatorname{lcm}(f, [\mathsf{L}(\zeta_e) : \mathsf{L}])$ and choose an $\varepsilon \in \overline{\mathsf{K}}$ with $\underline{A}(\underline{\varepsilon}) = 0$. Then*

$$\mathsf{N} = \mathsf{I}\left(\sqrt[e]{\varepsilon^b \alpha}\right)$$

is the splitting field of $\varphi(x)$.

We have included the original proof of this result with additional details that have been added to aide the reader.

Proof. By the construction of the ramification polynomial $\rho(x)$, the splitting field of $\rho(x)$ over L is the splitting field of $\varphi(x)$ over K. To be able to use Lemma 3.16 to find the splitting field of $\rho(x)$, we need to show that $\underline{A}(y)$ is square free.

Let $\rho(x) = \sum_{i=0}^{n} \rho_i x^i \in \mathcal{O}_{\mathsf{L}}[x]$ be the ramification polynomial of $\varphi(x)$. Then the residual polynomial of $\mathcal{R}_\varphi$ is

$$\underline{A}(y) = \sum_{j=0}^{(n-1)/e} \underline{A}_j y^j = \sum_{j=0}^{(n-1)/e} \underline{\rho_{je+1}\alpha^{h(j-(n-1)/e)}} y^j \in \underline{\mathsf{L}}[y].$$

We consider the polynomial $\underline{B}(x) = \sum_{i=0}^{n} \underline{B}_i x^i = x\underline{A}(\underline{\gamma}x^e)$ for a root $\underline{\gamma}$ of $\underline{A}(y)$. We find that

$$\underline{B}(x) = x \sum_{j=0}^{(n-1)/e} \underline{\rho_{je+1}\alpha^{h(j-(n-1)/e)}\gamma^j}\, x^{je} = \sum_{j=0}^{(n-1)/e} \underline{A_j\gamma^j}\, x^{je+1}.$$

We consider a nonzero coefficient $\underline{B_i}$. Then $i \in \{1, e+1, 2e+1, \ldots, n\}$. So there exists $j \in \{0, \ldots, \frac{n-1}{e}\}$ so that $i = je + 1$. Thus

$$0 \neq \underline{B_i} x^i = \underline{B_{je+1}}\, x^{je+1} = \underline{A_j\gamma^j}\, x^{je+1}.$$

So $\underline{A_j} \neq 0$. It follows from the construction of $\underline{A}(y)$ that $A_j \neq 0$ if the corresponding coefficient ρ_{je+1} of $\rho(x)$ yields a vertex of $\mathcal{R}_\varphi$. By Lemma 3.4, this occurs when $je + 1 = p^s$ for some $s \in \{0, \ldots, m\}$. Therefore $i = p^s$. Since our choice of coefficient was arbitrary, we conclude that if a term $\underline{B_i}x^i$ of $\underline{B}(x)$ is nonzero then i is a power of p.

Thus $\underline{B}(x)$ is an additive polynomial. Furthermore $\underline{B}'(x) = \underline{B_1} = \underline{A_0}$ since nontrivial powers of p vanish over the residue class field. So, $\gcd(\underline{B}(x), \underline{B}'(x)) = 1$ and therefore $\underline{B}(x)$ and $\underline{A}(x)$ are square free.

It remains to be shown that $\widetilde{F} = [\mathsf{I} : \mathsf{L}] = \operatorname{lcm}(f, [\mathsf{L}(\zeta_e) : \mathsf{L}])$ is the degree of the splitting field of $\underline{A}(\underline{\gamma}x^e)$ over $\mathbb{F}_q \cong \underline{\mathsf{L}}$. We have that $e \mid (q^{\widetilde{F}} - 1)$. Let $u := q^{\widetilde{F}}$, $F(x) := \underline{B}(x)$ and $G(x) := \underline{A}(\underline{\gamma}x)$. Then $F(x) = \sum_{j=0}^{(n-1)/e} \underline{A_j\gamma^j}\, x^{je+1}$. Let $a_j = \underline{A_j\gamma^j}$.

Then

$$F(x) = \sum_{j=0}^{(n-1)/e} a_j x^{je+1} \quad \text{and} \quad G(x) = \sum_{j=0}^{(n-1)/e} a_j x^j = \sum_{j=0}^{(n-1)/e} a_j x^{\frac{(je+1)-1}{e}}.$$

As shown earlier, if $a_j \neq 0$ then $je+1$ is a power of p. Through renumbering our coefficients we get $F(x) = \sum_{i=0}^{r} a_i x^{p^i}$, $G(x) = \sum_{i=0}^{r} a_i x^{(p^i-1)/e}$ and, as shown earlier, F is additive. Furthermore, $G(1) = \underline{A}(\underline{\gamma}) = 0$.

As $\underline{A}(y)$ is squarefree and $\mathbb{F}_{q^f}$ is the splitting field of $\underline{A}$, we have that $G(x) = \underline{A}(\underline{\gamma}x)$ splits into (distinct) linear factors over $\mathbb{F}_u$. Hence, Lemma 3.17 tells us that $F(x)$ splits over $\mathbb{F}_u$. Therefore, $\underline{A}(\underline{\gamma}x^e) = \frac{B(x)}{x}$ splits over $\mathbb{F}_u$. □

Remark. In the above Theorem, as $p \nmid e$ and L/K is totally ramified we have that $[\mathsf{L}(\zeta_e) : \mathsf{L}] = [\mathsf{K}(\zeta_e) : \mathsf{K}]$.

3.6 One Segment Galois Groups

When the ramification polygon of an Eisenstein polynomial consists of one segment, we can explicitly give its Galois group. If the segment is horizontal then the polynomial generates a tamely ramified extension and its Galois group can computed using either Theorem 2.28 or Theorem 2.29. If, on the other hand, the segment isn't horizontal then we can use the results from Sections 3.5 and 2.4 to compute the Galois group. The purpose of this section is to elaborate on how this can be done.

Let $\varphi(x) \in \mathcal{O}_{\mathsf{K}}[x]$ be Eisenstein of degree p^m, α a root of φ and $\mathsf{L} = \mathsf{K}(\alpha)$. We will assume that $\mathcal{R}_\varphi$ is a solitary line segment $\mathcal{S}$ with residual polynomial $\underline{A}(y) \in \underline{\mathsf{L}}[y]$ and slope $-h/e$ in lowest terms. In this context, we can compute the splitting field N of $\varphi(x)$ using Theorem 3.18. If we let T denote the maximal tamely ramified subfield of N/K then Theorem 3.18 tells us that T/K has ramification index e and inertia

degree $f = \mathrm{lcm}(f_1, [\mathsf{L}(\zeta_e) : \mathsf{L}])$ where f_1 is the segmental inertia degree of $\mathcal{S}$ and ζ_e is an e-th root of unity.

We will denote by G the group $\mathrm{Gal}(\varphi) = \mathrm{Gal}(\mathsf{N}/\mathsf{K})$ and by $\{G_i\}_{i\geq -1}$ the ramification filtration of G. Then, by Proposition 2.37 we have that $G_1 = \mathrm{Gal}(\mathsf{N}/\mathsf{T})$. We also set $H = \mathrm{Gal}(\mathsf{N}/\mathsf{L})$.

It is clear from construction that $\mathsf{N} = \mathsf{TL}$ (see Figure 2) and $\mathsf{T} \cap \mathsf{L} = \mathsf{K}$. Hence, by Theorem A.17 we have that $G_1 \cap H = \{\mathrm{id}\}$ and $G_1 H = G$. Therefore $G = G_1 \rtimes H$. This gives us a theoretical structure of G but more detail is needed. We begin by determining G_1.

Lemma 3.19 ([33, Lemma 8.1])**.** *The ramification filtration of* $G = \mathrm{Gal}(\varphi)$ *is*

$$G \geq G_0 \geq G_1 = G_2 = \ldots = G_h > G_{h+1} = \{\mathrm{id}\}$$

The group $G_1 = \mathrm{Gal}(\mathsf{N}/\mathsf{T})$ *is isomorphic to the additive group of* $\mathbb{F}_{p^m}$*.*

Proof. It follows from Proposition 2.37 that $|G/G_0| = f$ and $|G_0/G_1| = e$. We have confirmed the left part of the filtration: $G \geq G_0 \geq G_1$. In order to verify that $G_1 = G_h$, we examine the ramification polygon for N/T.

Since $\mathcal{R}_{\mathsf{N}/\mathsf{T}}$ is not dependent on the choice of the uniformizing element of N, we will choose π_{N} to satisfy $\mathsf{N} = \mathsf{T}(\pi_{\mathsf{N}})$. We will additionally let $\psi(x)$ denote the minimal polynomial of π_{N} over T. Then the roots of the ramification polynomial of ψ are $\frac{\sigma(\pi_{\mathsf{N}})-\pi_{\mathsf{N}}}{\pi_{\mathsf{N}}}$ where $\sigma \in \mathrm{Gal}(\mathsf{N}/\mathsf{T}) = G_1$.

According to Lemma 3.7, $\mathcal{R}_{\mathsf{N}/\mathsf{T}}$ is comprised of a single line with slope $-e \cdot \frac{h}{e} = -h$. This means that the roots of the ramification polynomial of ψ all have valuation

h. From this we conclude that for all $\sigma \in G_1$ we have

$$\begin{aligned} v_{\mathsf{N}}(\sigma(\pi_{\mathsf{N}}) - \pi_{\mathsf{N}}) &= v_{\mathsf{N}}\left(\frac{\sigma(\pi_{\mathsf{N}}) - \pi_{\mathsf{N}}}{\pi_{\mathsf{N}}} \cdot \pi_{\mathsf{N}}\right) \\ &= v_{\mathsf{N}}\left(\frac{\sigma(\pi_{\mathsf{N}}) - \pi_{\mathsf{N}}}{\pi_{\mathsf{N}}}\right) + v_{\mathsf{N}}(\pi_{\mathsf{N}}) \\ &= h + 1. \end{aligned}$$

In other words, $\sigma \in G_h$ for all $\sigma \in G_1$. Hence $G_1 \leq G_h$ which implies that $G_1 = G_h$. Finally, from the construction of N it is clear that we can't have another ramification break. So $G_{h+1} = \{\mathrm{id}\}$ and $G_1 = G_h = G_h/G_{h+1}$.

According to Proposition 2.33 and Proposition 2.32, G_h/G_{h+1} is isomorphic to a subgroup of $(\pi_{\mathsf{N}}^h)/(\pi_{\mathsf{N}}^{h+1})$ which, as an additive group, is isomorphic to the additive group of $\underline{\mathsf{N}}$. The characteristic of $\underline{\mathsf{N}}$ is p so we have $G_1 = G_h/G_{h+1}$ is isomorphic to the additive group of $\mathbb{F}_{p^r}$ for some $r \in \mathbb{N}$. To determine r we must find the order of G_1.

Since N is the splitting field of φ we know that N/K is Galois. Furthermore, by Theorem A.17 we have that N/T is Galois. This implies that $|\mathrm{Gal}(\mathsf{N}/\mathsf{T})| = [\mathsf{N} : \mathsf{T}] = p^m$. Therefore, G_1 is isomorphic to the additive group of $\mathbb{F}_{p^m}$.

The additive group of a finite field $\mathbb{F}_{p^r}$ is isomorphic to a $\mathbb{F}_p$-vector space. This implies that G_1 is elementary abelian. □

In order to make our description of $G = G_1 \rtimes H$ more explicit we have to determine the action of the elements of H on the elements of G_1. We know that once the group G has been found this action will be conjugation: for $\sigma \in G_1$ and $\tau \in H$ we say $\sigma^\tau = \tau\sigma\tau^{-1}$. Unfortunately, simply stating that amounts to working backward from a point we haven't reached. Instead, we will determine the action in a

roundabout fashion. More specifically, we will determine the action of H on a group isomorphic to G_1 and, in time, show that H must act the same way on both.

Before we delve into these details we need some notation and definitions. The unique maximal ideal of $\mathcal{O}_{\mathsf{N}}$ will be represented by $\wp = (\pi_{\mathsf{N}})$. With this in mind, Proposition 2.32 and Proposition 2.33 tell us that for $i \geq 1$ the quotients G_i/G_{i+1} embed into the additive groups $(\wp^i/\wp^{i+1}, +)$ which are isomorphic to the additive group of $\underline{\mathsf{N}}$. We will define the embedding maps by

$$\Theta_i : G_i/G_{i+1} \to (\wp^i/\wp^{i+1}, +) : \sigma G_{i+1} \mapsto \left(\frac{\sigma(\pi_{\mathsf{N}})}{\pi_{\mathsf{N}}} - 1\right) + \wp^{i+1}.$$

Some essential properties of the homomorphisms Θ_i for $i \geq 1$ are given in the lemma below.

Lemma 3.20 ([32, Lemma 6.2])**.** *The maps Θ_i for $i \geq 1$ are:*

(a) Independent of the choice of the prime element.

(b) In agreement with the operation of G on G_i/G_{i+1}. That is, for all $\sigma \in G_i$ and for all $\tau \in G$

$$\tau(\Theta_i(\sigma G_{i+1})) = \Theta_i(\sigma^\tau G_{i+1})$$

where $\sigma^\tau = \tau\sigma\tau^{-1}$.

Proof. (a) Let $\sigma \in G_i$. Then Θ_i sends σ to $\left(\frac{\sigma(\pi_{\mathsf{N}})}{\pi_{\mathsf{N}}} - 1\right) \in \wp^i$. If we identify this element of $\wp^i$ by d we have $\sigma(\pi_{\mathsf{N}}) = \pi_{\mathsf{N}}(1 + d)$.

Let π'_{N} be another prime element of N. If we defined Θ_i in terms of π'_{N} we would find that σ is mapped to $\left(\frac{\sigma(\pi'_{\mathsf{N}})}{\pi'_{\mathsf{N}}} - 1\right) \in \wp^i$. If we identify this element of $\wp^i$ by d' we have $\sigma(\pi'_{\mathsf{N}}) = \pi'_{\mathsf{N}}(1 + d')$.

In order to prove that replacing π_{N} by π'_{N} doesn't change the homomorphism Θ_i we have to demonstrate that σ is sent to the same coset in $\wp^i/\wp^{i+1}$. We start by establishing how the two uniformizers π_{N} and π'_{N} are related. Since π_{N} and π'_{N} generate the same ideal of $\mathcal{O}_{\mathsf{N}}$ there exists $\varepsilon \in {\mathcal{O}_{\mathsf{N}}}^{\times}$ such that $\pi'_{\mathsf{N}} = \varepsilon\pi_{\mathsf{N}}$. Furthermore, since $\sigma \in G_i$ we have that $\sigma(\varepsilon) \equiv \varepsilon \bmod \wp^{i+1}$. Putting this all together we have

$$\begin{aligned}
\pi'_{\mathsf{N}}(1+d') &= \sigma(\pi'_{\mathsf{N}}) \\
&= \sigma(\varepsilon\pi_{\mathsf{N}}) \\
&= \sigma(\varepsilon)\sigma(\pi_{\mathsf{N}}) \\
&= \sigma(\varepsilon)\pi_{\mathsf{N}}(1+d) \\
&\equiv \varepsilon\pi_{\mathsf{N}}(1+d) \bmod \wp^{i+1} \\
&\equiv \pi'_{\mathsf{N}}(1+d) \bmod \wp^{i+1}.
\end{aligned}$$

This implies that $d \equiv d' \bmod \wp^{i+1}$. Thus σ is sent to the same coset.

(b) Let $\sigma \in G_i$ and $\tau \in G$. As we saw earlier, there exists an element $d \in \wp^i$ so that $\sigma(\pi_{\mathsf{N}}) = \pi_{\mathsf{N}}(1+d)$ and $\Theta_i(\sigma G_{i+1}) = d \bmod \wp^{i+1}$. This directly implies that

$$\tau(\Theta_i(\sigma G_{i+1})) = \tau(d) \bmod \wp^{i+1}.$$

Because τ^{-1} is an automorphism, $\tau^{-1}(\pi_{\mathsf{N}})$ and π_{N} have the same minimal polynomial. The slope of this polynomial's Newton polygon gives its valuation. This implies that $\tau^{-1}(\pi_{\mathsf{N}})$ and π_{N} have the same valuation. Thus, there exists $\varepsilon \in {\mathcal{O}_{\mathsf{N}}}^{\times}$ such that $\tau^{-1}(\pi_{\mathsf{N}}) = \varepsilon\pi_{\mathsf{N}}$. Utilizing this to compute $\sigma^{\tau}(\pi_{\mathsf{N}})$ we find that

$$\sigma^{\tau}(\pi_{\mathsf{N}}) = \tau(\sigma(\tau^{-1}(\pi_{\mathsf{N}}))) = \tau(\sigma(\varepsilon\pi_{\mathsf{N}})).$$

As before, $\sigma \in G_i$ implies that $\sigma(\varepsilon) \equiv \varepsilon \bmod \wp^{i+1}$. This, in turn, implies that

$$\begin{aligned}\sigma^\tau(\pi_{\mathsf{N}}) &= \tau(\sigma(\varepsilon\pi_{\mathsf{N}})) \\ &= \tau(\sigma(\varepsilon)\sigma(\pi_{\mathsf{N}})) \\ &= \tau(\sigma(\varepsilon)\pi_{\mathsf{N}}(1+d)) \\ &\equiv \tau(\varepsilon\pi_{\mathsf{N}}(1+d)) \bmod \wp^{i+1}.\end{aligned}$$

If we apply τ to both sides of $\tau^{-1}(\pi_{\mathsf{N}}) = \varepsilon\pi_{\mathsf{N}}$ we obtain $\pi_{\mathsf{N}} = \tau(\varepsilon\pi_{\mathsf{N}})$. This informs us that $\sigma^\tau(\pi_{\mathsf{N}})$ is modulo $\wp^{i+1}$ congruent to

$$\begin{aligned}\tau(\varepsilon\pi_{\mathsf{N}}(1+d)) &= \tau(\varepsilon\pi_{\mathsf{N}})\tau(1+d) \\ &= \pi_{\mathsf{N}}\tau(1+d) \\ &= \pi_{\mathsf{N}}(1+\tau(d)).\end{aligned}$$

Now that we have an equivalence relation for $\sigma^\tau(\pi_{\mathsf{N}})$, we can find the image of σ^τ under Θ_i:

$$\begin{aligned}\Theta_i(\sigma^\tau G_{i+1}) &= \left(\frac{\sigma^\tau(\pi_{\mathsf{N}})}{\pi_{\mathsf{N}}} - 1\right) \bmod \wp^{i+1} \\ &\equiv \left(\frac{\pi_{\mathsf{N}}(1+\tau(d))}{\pi_{\mathsf{N}}} - 1\right) \bmod \wp^{i+1} \\ &= \tau(d) \bmod \wp^{i+1} \\ &= \tau(\Theta_i(\sigma G_{i+1})).\end{aligned}$$

□

As we established in Lemma 3.19, $G_1 = G_h/G_{h+1}$. This allows us to restate Θ_h as

$$\Theta_h : G_1 \to \wp^h/\wp^{h+1} : \sigma \mapsto \left(\frac{\sigma(\pi_{\mathsf{N}})}{\pi_{\mathsf{N}}} - 1\right) \bmod \wp^{h+1}.$$

Since H acts naturally on $\wp^h/\wp^{h+1}$, we can investigate the action of H on $\Theta_h(G_1) \leq \wp^h/\wp^{h+1}$. Later, we will relate this action to the action of H on G_1.

First, we recall that $H = \mathrm{Gal}(\mathsf{N}/\mathsf{L})$ where N/L is normal and tamely ramified with ramification index e and inertia degree f (see again Figure 2). From our discussion in Section 2.4 we can explicitly give the splitting field N. For $q = |\underline{\mathsf{K}}| = |\underline{\mathsf{L}}|$, we have $\mathsf{N} = \mathsf{L}(\zeta, \pi_{\mathsf{N}}) = \mathsf{K}(\alpha)(\zeta, \pi_{\mathsf{N}})$ where ζ is a $(q^f - 1)$-st root of unity and $\pi_{\mathsf{N}} = \sqrt[e]{\zeta^r \alpha}$. To see how the generators s and t of H act on ζ and π_{N}, see Theorem 2.28.

Second, we compute $\Theta_h(G_1)$ in a form that can be easily acted upon by $H = \langle s, t \rangle$. If we let $\widetilde{f}$ represent the inertia degree of $\mathsf{K}/\mathbb{Q}_p$ then

$$\underline{\mathsf{N}} = \mathbb{F}_{q^f} = \mathbb{F}_{p^{f\widetilde{f}}} = \mathbb{F}_p(\zeta). \tag{3.6}$$

Thus, Proposition 2.33 tells us that $(\wp^h/\wp^{h+1}, +)$ is isomorphic to $\mathbb{F}^+_{p^{f\widetilde{f}}}$, an additive group that contains an isomorphic copy of $\Theta_h(G_1)$. Since Θ_h is injective, $\Theta_h(G_1)$ has order p^m. This implies that $\Theta_h(G_1) \cong \mathbb{F}^+_{p^m}$.

As H acts on $\wp^h/\wp^{h+1}$ we must compute the submodule $\Theta_h(G_1)$ of $(\wp^h/\wp^{h+1}, +) \cong \mathbb{F}^+_{q^f}$. The proposition below explains how $\Theta_h(G_1)$ can be computed using the roots of $\underline{A}(y)$, our residual polynomial. The proposition also details how the automorphisms $s, t \in H$ act on $\Theta_h(G_1)$.

Proposition 3.21 ([33, Proposition 8.3])**.** *Let $d = \frac{p^m-1}{e}$ be the degree of the residual polynomial $\underline{A}(y)$. Also let $\underline{u}_1, \ldots, \underline{u}_d$ be the zeros of $\underline{A}(y)$ in $\underline{\mathsf{N}}$ and $a, b \in \mathbb{N}$ with $ae - bp^m = 1$. Then:*

(a) For $1 \leq i \leq d$ the residue class field $\underline{\mathsf{N}}$ contains the e-th roots of $\frac{\underline{u}_i}{\underline{\zeta^{rh}}}$ which we denote by $\underline{u}_{i,1}, \ldots, \underline{u}_{i,e}$.

(b) The images of G_1 under Θ_h are

$$\{0 + \wp^{h+1}, au_{i,j}\pi_{\mathsf{N}}^h + \wp^{h+1} | 1 \leq i \leq d, 1 \leq j \leq e\},$$

where $u_{i,j}$ denotes a lift of $\underline{u}_{i,j} \in \underline{\mathsf{N}}$ to $\mathcal{O}_{\mathsf{N}}$.

(c) The operations of the automorphisms s and t (see Theorem 2.28) on $\Theta_h(G_1)$ are given by $s(\zeta^i\pi_{\mathsf{N}}^h + \wp^{h+1}) = \zeta^{\ell h+i}\pi_{\mathsf{N}}^h + \wp^{h+1}$ and $t(\zeta^i\pi_{\mathsf{N}}^h + \wp^{h+1}) = \zeta^{hk+qi}\pi_{\mathsf{N}}^h + \wp^{h+1}$ with $k = \frac{r(q-1)}{e}$ and $\ell = \frac{q^f-1}{e}$.

Proof. (a) Let $\rho(x) \in \mathcal{O}_{\mathsf{L}}[x]$ denote the ramification polynomial of φ. If the roots of φ, in some algebraic closure, are $\alpha = \alpha_1, \ldots, \alpha_{p^m}$ then the nonzero roots of ρ are $-1 + \frac{\alpha_i}{\alpha}$ for $2 \leq i \leq p^m$. The N-valuation of these roots is

$$v_{\mathsf{N}}\left(-1 + \frac{\alpha_i}{\alpha}\right) = ev_{\mathsf{L}}\left(-1 + \frac{\alpha_i}{\alpha}\right) = h.$$

Hence the roots of ρ have the form $\gamma\pi_{\mathsf{N}}^h$ for some $\gamma \in \mathcal{O}_{\mathsf{N}}{}^{\times}$.

According to Lemma 3.1 the roots of $\underline{A}(y)$ must have the form

$$\begin{aligned}\underline{\left(\frac{(\gamma\pi_{\mathsf{N}}^h)^e}{\alpha^h}\right)} &= \underline{\left(\frac{(\gamma\sqrt[e]{\zeta^r\alpha}^h)^e}{\alpha^h}\right)} \\ &= \underline{\left(\frac{\gamma^e(\zeta^r\alpha)^h}{\alpha^h}\right)} \\ &= \underline{\gamma^e\zeta^{rh}}.\end{aligned}$$

As each γ^e has up to e e-th roots, we have up to e possibilities for $\gamma\pi_{\mathsf{N}}^h$. Since ρ has p^m-1 nonzero roots, the only way to distribute these roots is for e of them to correspond to each of the $d=\frac{p^m-1}{e}$ roots of $\underline{A}$.

(b) According to part (a) of Lemma 3.20, Θ_h is independent of the uniformizer used. So, we are going to use the prime element from the proof of Lemma 3.7: $\pi'_{\mathsf{N}}=\alpha^a/\beta^b$ where β is a prime element of T. In addition, we further mimic the aforementioned proof by representing each quotient α_i/α by $1+\delta_i\alpha^{h/e}$ where $v(\delta_i)=0$.

Let $\sigma\in G_1$ be such that $\sigma(\alpha)=\alpha_i$ for some $2\le i\le p^m$. Since a and p are coprime, we have that

$$\begin{aligned}\frac{\sigma(\pi'_{\mathsf{N}})}{\pi'_{\mathsf{N}}}-1 &= \frac{(\sigma(\alpha))^a}{(\sigma(\beta))^b}\cdot\frac{\beta^b}{\alpha^a}-1 \\ &= \frac{\alpha_i^a}{\beta^b}\frac{\beta^b}{\alpha^a}-1 \qquad \text{since } \sigma(\beta)=\beta \\ &= \left(\frac{\alpha_i}{\alpha}\right)^a-1 \\ &= a\delta_i\alpha^{h/e}+\dots.\end{aligned}$$

This informs us that $\Theta_h(\sigma)$ is $a\delta_i\alpha^{h/e}+\ldots \bmod \wp^{h+1}$.

Unfortunately, δ_i and $\alpha^{h/e}$ are not generally in N. So we have to do some work to represent $\Theta_h(\sigma)$ in N. Since $\delta_i\alpha^{h/e}$ and $\gamma\pi_{\mathsf{N}}^h$ both represent a root of ρ, we equate

them. What we get is an equation equivalent to $\delta_i = \gamma(\sqrt[e]{\zeta^r})^h$. This permits us to update our formulation of $\Theta_h(\sigma)$:

$$\begin{aligned}\frac{\sigma(\pi'_{\mathsf{N}})}{\pi'_{\mathsf{N}}} - 1 &= a\gamma \sqrt[e]{\zeta^r}^h \sqrt[e]{\alpha^h} + \dots \\ &= a\gamma \sqrt[e]{\zeta^r \alpha}^h + \dots \\ &= a\gamma \pi_{\mathsf{N}}^h + \dots \\ &\equiv a\gamma \pi_{\mathsf{N}}^h \bmod \wp^{h+1}\end{aligned}$$

since $\gamma \in \mathcal{O}_{\mathsf{N}}{}^{\times}$.

As we stated earlier, the roots of $\underline{A}(y)$ give $p^m - 1$ values of γ. Thus, $\Theta_h(G_1)$ is $0 + \wp^{h+1}$ along with the elements $a\gamma\pi_{\mathsf{N}}^h + \wp^{h+1}$.

(c) This follows directly from Theorem 2.28. □

According to Proposition A.18, every finite field $\mathbb{F}_{p^r}$ is a Galois extension of $\mathbb{F}_p$ with $[\mathbb{F}_{p^r} : \mathbb{F}_p] = r$. From basic field theory, we then know that $\mathbb{F}_{p^r}$ is a vector space over $\mathbb{F}_p$ with dimension r. Furthermore, if we denote by $(\mathbb{F}_p)^r$ the set of $r \times 1$ column matrices with entries in $\mathbb{F}_p$, we have that $(\mathbb{F}_p)^r \cong \mathbb{F}_{p^r}$.

In light of this, our next step in finding $G = \mathrm{Gal}(\varphi)$ is to find an $\mathbb{F}_p$-basis of $\Theta_h(G_1)$. Because $\Theta_h(G_1) \leq \mathbb{F}_{q^f}^+$, equation (3.6) implies that this basis B can be a set of powers of ζ.

Similarly, we will utilize the representation of H which has dimension $f\widetilde{f}$ over $\mathbb{F}_p$. From Proposition 3.21, we know how the elements of $H = \langle s, t \rangle$ act on elements of the form ζ^i:

$$s : \zeta^i \mapsto \zeta^{\ell h + i} \qquad \text{and} \qquad t : \zeta^i \mapsto \zeta^{hk + qi}.$$

This allows us to represent H as a subgroup H' of $\mathrm{GL}(m,p)$. If $a \in H$ then the action of a on each element of B yields a linear combination of the elements of B. This gives way to a corresponding $m \times m$ matrix $A \in H'$ where the jth row of A is made up of the coefficients of the linear combination from a acting on the jth element of B. It follows that H' will be computed as $\langle S, T\rangle \leq \mathrm{GL}(m,p)$ where S and T are the matrices corresponding to s and t respectively.

The above considerations provide us with a framework within which we can compute $\mathrm{Gal}(\varphi)$. In the theorem below, we describe $\mathrm{Gal}(\varphi)$ as a subgroup of $\mathrm{AGL}(m,p)$ (see Example B.16).

Theorem 3.22 ([33, Theorem 8.2])**.** *Let $\varphi(x) \in \mathcal{O}_{\mathsf{K}}[x]$ be an Eisenstein polynomial of degree p^m, whose ramification polygon consists of one single segment of slope $-\frac{h}{e}$ with $\gcd(h,e) = 1$. Then $\mathrm{Gal}(\varphi) = G_1 \rtimes H$, where G_1 is the first ramification group and H corresponds to the maximal tamely ramified subfield of the splitting field of $\varphi(x)$ (see Proposition 3.18). Moreover, $\mathrm{Gal}(\varphi)$ is isomorphic to the group*

$$\widetilde{G} = \{t_{A,v} : (\mathbb{F}_p)^m \to (\mathbb{F}_p)^m : x \mapsto Ax + v \mid A \in H' \leq \mathrm{GL}(m,p),\ v \in (\mathbb{F}_p)^m\}$$

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

Proof. Let $\widetilde{G}_1 = \{s_v : (\mathbb{F}_p)^m \to (\mathbb{F}_p)^m : x \mapsto x + v \mid v \in (\mathbb{F}_p)^m\}$ be the set of maps on $(\mathbb{F}_p)^m$ defined by addition by a vector. Then, by Lemma 3.19 we have that $G_1 \cong \mathbb{F}_{p^m}^+ \cong \widetilde{G}_1$.

The next step is to establish how H acts on G_1. According to part (b) of Lemma 3.20 we have that $\tau(\Theta_h(\sigma)) = \Theta_h(\sigma^\tau)$ for $\sigma \in G_1$ and $\tau \in H$. This implies

that H acts in the same way on both G_1 and $\Theta_h(G_1)$. Furthermore, the action of H on $G_1 \cong \Theta_h(G_1)$ is faithful.

Let $H' \leq \mathrm{GL}(m,p)$ denote the group of matrices that describe how the elements of H act on the submodule $\Theta_h(G_1)$. Then $H \cong H'$. Also, set $\widetilde{H} = \{u_A : (\mathbb{F}_p)^m \to (\mathbb{F}_p)^m : x \mapsto Ax \mid A \in H'\}$. It follows immediately that $H' \cong \widetilde{H}$. Thus, $\mathrm{Gal}(\varphi) \cong \widetilde{G_1} \rtimes \widetilde{H} = \widetilde{G}$.

We conclude this proof by describing how $\widetilde{H}$ acts on $\widetilde{G_1}$. For $s_v \in \widetilde{G}_1$, $u_A \in \widetilde{H}$ and $x \in (\mathbb{F}_p)^m$ we obtain

$$\begin{aligned} s_v^{u_A}(x) &= u_A(s_v(u_{A^{-1}}(x))) \\ &= u_A(s_v(A^{-1}x)) \\ &= u_A(A^{-1}x + v) \\ &= A(A^{-1}x + v) \\ &= x + Av. \end{aligned}$$

In general, we have $s_v^{u_A} : (\mathbb{F}_p)^m \to (\mathbb{F}_p)^m : x \mapsto x + Av$. □

The results and discussions above are summarized in the following algorithm. The reader should note that steps (11) and (12) of the algorithm detail how the submodule $M = \Theta_h(G_1)$ of $\mathbb{F}_{q^f}^+$ is computed. To date, this algorithm has been applied to polynomials of degree as high as 3481.

Algorithm 3.23 (`GaloisGroupOne` [32, Algorithm 6.1])**.**

Input: $\varphi \in \mathcal{O}_\mathsf{K}[x]$ Eisenstein of degree p^m such that $\mathcal{R}_\varphi$ has one segment

Output: $\mathrm{Gal}(\varphi)$ as a subgroup of $\mathrm{AGL}(m,p)$

(1) Let $-h/e$ be the slope of the segment $\mathcal{S}$ of $\mathcal{R}_\varphi$.

(2) Let $\underline{A} \in \underline{\mathsf{L}}[x] = \mathbb{F}_q[x]$ be the residual polynomial of $\mathcal{S}$.

(3) Let $f_1 = \operatorname{lcm}\{\deg \rho \mid \rho | \underline{A} \text{ and } \rho \text{ is irreducible}\}$ be the segmental inertia degree of $\mathcal{S}$.

(4) Let $f = \operatorname{lcm}(f_1, [\mathsf{K}(\zeta_e) : \mathsf{K}])$.

(5) Find $a, \widetilde{a}, b, \widetilde{b} \in \mathbb{N}$ such that $ae - \widetilde{a}p^m = 1$ and $bh - \widetilde{b}e = 1$

(6) Let $\mathbb{F}_q(\zeta) \cong \mathbb{F}_{q^f}$.

(7) Let $u_1, \ldots, u_d \in \mathbb{F}_q(\zeta)$ be the roots of $\underline{A}$.

(8) Find $r' \in \mathbb{N}$ such that $\zeta^{r'} = u_1^b$.

(9) Find $r \in \{0, \ldots, e-1\}$ such that $r \equiv r' \bmod e$.

(10) Initialize $M \leftarrow \langle 1 \rangle \leq \mathbb{F}_{q^f}^+$, $i \leftarrow 1$.

(11) Repeat until $\#M = p^m$:

  (a) Compute the e-th roots $u_{i,1}, \ldots, u_{i,e}$ of u_i/ζ^{rh}.

  (b) $M \leftarrow \langle M, au_{i,1}, \ldots, au_{i,e} \rangle \leq \mathbb{F}_{q^f}^+$.

  (c) $i \leftarrow i + 1$.

(12) Let B be an $\mathbb{F}_p$-basis of M.

(13) $\ell \leftarrow (q^f - 1)/e$, $k \leftarrow r(q-1)/e$.

(14) Find the automorphism s of M induced by $\zeta^j \mapsto \zeta^{\ell h + j}$ where ζ^j is a generator of M.

(15) Find the matrix $S \in GL(m, p)$ representing s with respect to B.

(16) Find the automorphism t of M induced by $\zeta^j \mapsto \zeta^{hk+qj}$ where ζ^j is a generator of M.

(17) Find the matrix $T \in GL(m,p)$ representing t with respect to B.

(18) Return $G = \{t_{A,v} : (\mathbb{F}_p)^m \to (\mathbb{F}_p)^m : x \mapsto Ax + v \mid A \in \langle S, T\rangle,\ v \in (\mathbb{F}_p)^m\}$.

As the above algorithm illustrates, the only information required to compute $\mathrm{Gal}(\varphi)$ is: the base field K, the residual polynomial $\underline{A}(y)$ and the ramification polygon of φ. Every computational step in the algorithm can be performed using data based on those three things.

Example 3.24. We compute the Galois group of $\varphi(x) = x^{25} + 5x^6 + 5 \in \mathbb{Q}_5[x]$. Let α denote a root of $\varphi(x)$ and set $\mathsf{L} := \mathbb{Q}_5(\alpha)$. The ramification polygon $\mathcal{R}_\varphi$ is comprised of a single line segment with endpoints at $(1,6)$ and $(25,0)$. The slope of this line is $-\frac{h}{e} = -\frac{1}{4}$. The residual polynomial for this segment is

$$\underline{A}(y) = y^6 + 4 = (y+1)(y+4)(y^2+y+1)(y^2+4y+1) \in \underline{\mathsf{L}}[y]$$

It follows that the segmental inertia degree is 2. Because $[\mathbb{Q}_5(\zeta_4) : \mathbb{Q}_5] = 1$, the inertia degree of the splitting field is $f = \mathrm{lcm}(2,1) = 2$.

Let ζ be a primitive $(5^2 - 1)$ -st root of unity. Since $\zeta^0 = 1$ is a root of $\underline{A}(y)$, Theorem 3.18 tells us that the splitting field of $\varphi(x)$ over $\mathbb{Q}_5$ is $\mathsf{N} = \mathsf{L}(\zeta, \sqrt[4]{\alpha})$. Because N/L is normal and tamely ramified we can use Theorem 2.28 to determine $H = \mathrm{Gal}(\mathsf{N}/\mathsf{L})$. Using $e = 4$, $f = 2$, and $r = 0$ we find that $H \cong C_4 \times C_2$ and is generated by

$$s : \zeta \mapsto \zeta,\ \sqrt[4]{\alpha} \mapsto \zeta^6 \sqrt[4]{\alpha} \qquad \text{and} \qquad t : \zeta \mapsto \zeta^5,\ \sqrt[4]{\alpha} \mapsto \sqrt[4]{\alpha}.$$

From part (c) of Proposition 3.21 we obtain the representation matrix $S \in \mathrm{GL}(2,5)$ for the automorphism on $\mathbb{F}_{5^2}^+$ defined by $\zeta^i \mapsto \zeta^{6+i}$. In addition, Proposition 3.21

gives us the representation matrix $T \in \mathrm{GL}(2,5)$ for the automorphism $\zeta^i \mapsto \zeta^{5i}$. For the basis $1, \zeta$ of $\wp/\wp^2 \cong (\mathbb{F}_{5^2}, +)$ we have that

$$S = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 0 \\ 1 & 4 \end{pmatrix}$$

describe the action of the automorphisms s and t on $G_1 \cong C_5^2$. Thus, Theorem 3.22 gives us that $\mathrm{Gal}(\varphi)$ is isomorphic to

$$\begin{aligned} G &= \left\{ t_{A,v} : (\mathbb{F}_5)^2 \to (\mathbb{F}_5)^2 : x \mapsto Ax + v \;\middle|\; A \in \langle S, T \rangle,\ v \in (\mathbb{F}_5)^2 \right\} \\ &\cong C_5^2 \rtimes (C_4 \times C_2). \end{aligned}$$

3.7 The Maximum Tamely Ramified Subextension

When the ramification polygon of an Eisenstein polynomial $\varphi(x) \in \mathcal{O}_{\mathsf{K}}[x]$ has more than one segment, we do not have a closed form description of the splitting field of φ or of $\mathrm{Gal}(\varphi)$. We can, however, use $\mathcal{R}_\varphi$ and its residual polynomials to obtain information about the structure of the splitting field of φ. Using the concepts and results of the last three sections, we can compute a subfield T of the splitting field N of $\varphi(x)$. The extension T is the maximum tamely ramified subextension of N/K. That is, N is a p-extension of T.

Theorem 3.25 ([32, Satz 5.8])**.** *Let $\varphi(x) = x^n + \sum_{i=0}^{n-1} \varphi_i x^i \in \mathcal{O}_{\mathsf{K}}[x]$ be Eisenstein of degree $n = e_0 p^m$ with $p \nmid e_0$ and $m > 0$. Assume the ramification polygon $\mathcal{R}_\varphi$ of $\varphi(x)$ consists of $\ell + 1$ segments $S_1, \ldots, S_{\ell+1}$. For $1 \le i \le \ell$ let*

- *$m_i = -h_i/e_i$ be the slope of S_i with $\gcd(h_i, e_i) = 1 = d_i e_i + b_i h_i$ for $d_i, b_i \in \mathbb{Z}$,*

- $A_i(y) \in \mathcal{O}_{\mathsf{L}}[y]$ *be the residual polynomial and* f_i *the segmental inertia degree of* S_i,
- $\gamma_i \in \overline{\mathsf{K}}$ *such that* $\underline{A}_i(\gamma_i) = 0$, *and*
- $v_i = e_0 \cdot p^{m-s_{i-1}} + n + 1$.

Moreover we denote by I *the unramified extension of* K *of degree*

$$f = \operatorname{lcm}(f_1, \ldots, f_\ell, [\mathsf{K}(\zeta_{e_1 e_0}) : \mathsf{K}], \ldots, [\mathsf{K}(\zeta_{e_\ell e_0}) : \mathsf{K}]) \tag{3.7}$$

and by N *the splitting field of* $\varphi(x)$. *Let* α *be a root of* $\varphi(x)$ *and* $\mathsf{K}(\alpha) = \mathsf{L}_0 \supset \mathsf{L}_1 \supset \cdots \supset \mathsf{L}_\ell \supset \mathsf{K}$ *as in Theorem* 3.15 *be the tower of subfields corresponding to* $\mathcal{R}_\varphi$. *Then:*

(a) The field

$$\mathsf{T} = \mathsf{I}\left(\sqrt[e_1 e_0]{(-1)^{v_1}\gamma_1^{b_1 n}\varphi_0}, \ldots, \sqrt[e_\ell e_0]{(-1)^{v_\ell}\gamma_\ell^{b_\ell n}\varphi_0} \right)$$

is a subfield of N/K, *such that* N/T *is a p-extension.*

(b) For $1 \le i \le \ell - 1$ *the extensions* $\mathsf{TL}_{i-1}/\mathsf{TL}_i$ *are elementary abelian.*

(c) The extension T/K *is Galois and tamely ramified with ramification index* $e_0 \cdot \operatorname{lcm}(e_1, \ldots, e_\ell)$. *Furthermore* $[\mathsf{T} : \mathsf{K}] < n^2$.

We have included the original proof of this result with additional details that have been added to aide the reader.

Proof. Assume that the roots $\alpha = \alpha_1, \ldots, \alpha_n$ of $\varphi(x)$ are ordered as in Lemma 3.9. For $1 \le i \le \ell$ we have $\mathsf{L}_i = \mathsf{K}(\beta_i)$ with $\beta_i = \alpha_1 \cdots \alpha_{p^{s_i}}$. The conjugates of β_i, under this ordering, are of the form $\beta_i^{(j)} = \alpha_{(j-1)p^{s_i}+1} \cdot \ldots \cdot \alpha_{jp^{s_i}}$ for $1 \le j \le n/p^{s_i}$.

For $1 \leq i \leq \ell$ let N_i denote the normal closure of $\mathsf{L}_{i-1}/\mathsf{L}_i$. According to Theorem 3.15, $\mathcal{R}_{\mathsf{L}_{i-1}/\mathsf{L}_i}$ consists of exactly one segment of slope $m_i = -h_i/e_i$ with $\gcd(h_i, e_i) = 1 = d_i e_i + b_i h_i$ for $d_i, b_i \in \mathbb{Z}$. Furthermore, the segmental inertia degree of $\mathcal{R}_{\mathsf{L}_{i-1}/\mathsf{L}_i}$ is f_i. If ε_i is a root of $\underline{A}_i(y)$ then part (c) of Theorem 3.15 tells us that $\varepsilon_i^{p^{s_{i-1}}}$ is a root of the residual polynomial of $\mathcal{R}_{\mathsf{L}_{i-1}/\mathsf{L}_i}$. Since β_{i-1} generates the extension $\mathsf{L}_{i-1}/\mathsf{L}_i$, Theorem 3.18 yields

$$\mathsf{N}_i = \mathsf{I}_i \left(\sqrt[e_i]{\left(\varepsilon_i^{p^{s_{i-1}}}\right)^{b_i} \beta_{i-1}} \right)$$

with $\mathsf{I}_i/\mathsf{L}_{i-1}$ unramified of degree $\operatorname{lcm}(f_i, [\mathsf{L}_{i-1}(\zeta_{e_i}) : \mathsf{L}_{i-1}]) = \operatorname{lcm}(f_i, [\mathsf{K}_{i-1}(\zeta_{e_i}) : \mathsf{K}_{i-1}])$. By Lemma 3.19 the first ramification group and therefore the wildly ramified part of $\mathsf{N}_i/\mathsf{L}_i$ is elementary abelian. For the tamely ramified extension $\mathsf{L}_\ell/\mathsf{K}$ we set $\mathsf{N}_{\ell+1} = \mathsf{I}_{\ell+1} = \mathsf{L}_\ell(\zeta_{e_0})$.

We now collect all unramified extensions over K and consider the tower of extensions

$$\mathsf{IL} \supset \mathsf{IL}_1 \supset \cdots \supset \mathsf{IL}_\ell \supset \mathsf{I} \supset \mathsf{K}. \tag{3.8}$$

By the definition of I, the extensions $\mathsf{IN}_i/\mathsf{IL}_i$ are Galois and totally ramified. Their tamely ramified part $\mathsf{IN}_i/\mathsf{IL}_{i-1}$ is generated by $x^{e_i} - \varepsilon_i^{b_i p^{s_{i-1}}} \beta_{i-1}$.

Similarly to the unramified parts we now consider the tamely ramified parts over I. We will determine the tamely ramified part of IN_i/I for $1 \leq i \leq \ell$. This will be accomplished by finding a generating polynomial for IN_i/I and using Proposition 2.26 to find the tamely ramified part.

For a particular choice of i we have the tower of extensions

$$\mathsf{IN}_i \supset \mathsf{IL}_{i-1} \supset \mathsf{IL}_i \supset \mathsf{I}$$

where the top extension $\mathsf{IN}_i/\mathsf{IL}_{i-1}$ is generated by $x^{e_i} - \varepsilon_i^{b_i p^{s_{i-1}}} \beta_{i-1}$. Hence, by Proposition 2.41, we can use the norm $\mathrm{N}_{\mathsf{IL}_{i-1}/\mathsf{I}}(x^{e_i} - \varepsilon_i^{b_i p^{s_{i-1}}} \beta_{i-1})$ to generate IN_i/I.

The resulting polynomial, τ, is Eisenstein and has degree $e_i \cdot [\mathsf{IL}_{i-1} : \mathsf{I}]$. Its constant term is $\left(-\varepsilon_i^{b_i p^{s_{i-1}}}\right)^{[\mathsf{IL}_{i-1}:\mathsf{I}]} (-1)^n \varphi_0$ since the product of the conjugates of β_{i-1} is up to sign equal to $\prod_{i=1}^n \alpha_i = \pm\varphi_0$. All that remains to determine τ is to find $[\mathsf{IL}_{i-1} : \mathsf{I}]$. Since I/K is unramified, $\mathsf{IK} = \mathsf{I}$ and Figure 3 gives way to the following indices in (3.8): $[\mathsf{IL} : \mathsf{IL}_1] = p^{s_1}, [\mathsf{IL}_1 : \mathsf{IL}_2] = p^{s_2 - s_1}, \ldots [\mathsf{IL}_{\ell-2} : \mathsf{IL}_{\ell-1}] = p^{s_{\ell-1} - s_{\ell-2}}, [\mathsf{IL}_{\ell-1} : \mathsf{IL}_\ell] = p^{s_\ell - s_{\ell-1}}, [\mathsf{IL}_\ell : \mathsf{I}] = e_0, [\mathsf{I} : \mathsf{K}] = f$.

As a result

$$\begin{aligned}
[\mathsf{IL}_{i-1} : \mathsf{I}] &= [\mathsf{IL}_{i-1} : \mathsf{IL}_i] \cdot [\mathsf{IL}_i : \mathsf{IL}_{i+1}] \cdots [\mathsf{IL}_{\ell-1} : \mathsf{IL}_\ell] \cdot [\mathsf{IL}_\ell : \mathsf{I}] \\
&= p^{s_i - s_{i-1}} \cdot p^{s_{i+1} - s_i} \cdots p^{s_\ell - s_{\ell-1}} \cdot e_0 \\
&= p^{s_\ell - s_{i-1}} \cdot e_0 \\
&= e_0 \cdot p^{m - s_{i-1}}.
\end{aligned}$$

Thus, the constant term of τ is

$$\begin{aligned}
\left(-\varepsilon_i^{b_i p^{s_{i-1}}}\right)^{[\mathsf{IL}_{i-1}:\mathsf{I}]} (-1)^n \varphi_0 &= \left((-1)\varepsilon_i^{b_i p^{s_{i-1}}}\right)^{e_0 \cdot p^{m - s_{i-1}}} (-1)^n \varphi_0 \\
&= (-1)^{e_0 \cdot p^{m-s_{i-1}}} \ \varepsilon_i^{p^{s_{i-1}} b_i e_0 \cdot p^{m-s_{i-1}}} (-1)^n \varphi_0 \\
&= (-1)^{e_0 \cdot p^{m-s_{i-1}} + n} \ \varepsilon_i^{b_i e_0 p^m} \varphi_0 \\
&= (-1)^{e_0 \cdot p^{m-s_{i-1}} + n} \ \varepsilon_i^{b_i n} \varphi_0
\end{aligned}$$

and τ has degree $e_i \cdot [\mathsf{IL}_{i-1} : \mathsf{I}] = e_i \cdot e_0 \cdot p^{m - s_{i-1}}$.

By Proposition 2.26 and Corollary 2.27 we have that the tamely ramified part of IN_i/I is generated by $x^{e_i e_0} + (-1)^{e_0 \cdot p^{m-s_{i-1}} + n} \ \varepsilon_i^{b_i n} \varphi_0$. If we let $v_i := e_0 \cdot p^{m - s_{i-1}} + n + 1$,

then this polynomial is $x^{e_i e_0} + (-1)^{v_i - 1} \varepsilon_i^{b_i n} \varphi_0$. So

$$\mathsf{T}_i = \mathsf{I}\left(\sqrt[e_i e_0]{(-1)^{v_i} \varepsilon_i^{b_i n} \varphi_0} \right)$$

is Galois and the tamely ramified part of IN_i/I $(1 \leq i \leq \ell)$. Each of these extensions contains $\mathsf{IL}_\ell/\mathsf{I}$ of degree e_0. The field T is the compositum of the T_i and can thus be computed using the approach described in Section 2.6. If we let $\gamma_i = \varepsilon_i$ for $1 \leq i \leq \ell$ we have that

$$\mathsf{T} = \mathsf{I}\left(\sqrt[e_1 e_0]{(-1)^{v_1} \gamma_1^{b_1 n} \varphi_0}, \ldots, \sqrt[e_\ell e_0]{(-1)^{v_\ell} \gamma_\ell^{b_\ell n} \varphi_0} \right).$$

The extension T/K is Galois, because it is the compositum of Galois extensions.

From Proposition 2.39 we get the new tower of extensions

$$\mathsf{TL} = \mathsf{TL}_0 \supset \mathsf{TL}_1 \supset \cdots \supset \mathsf{TL}_{\ell-1} \supset \mathsf{T} \supset \mathsf{I} \supset \mathsf{K}. \tag{3.9}$$

Each relative extension $\mathsf{TL}_{i-1}/\mathsf{TL}_i$ is wildly and totally ramified and has a ramification polygon that consists of a single line segment with integral slope. Since

$$[\mathsf{TL}_{i-1} : \mathsf{TL}_i] = [\mathsf{L}_{i-1} : \mathsf{L}_i] = p^{s_i - s_{i-1}}$$

it can be easily shown (compare to Lemma 3.19) that $\mathrm{Gal}(\mathsf{TL}_{i-1}/\mathsf{TL}_i) \cong C_p^{s_i - s_{i-1}}$. Thus $\mathsf{TL}_{i-1}/\mathsf{TL}_i$ is an elementary abelian p-extension which proves (b). It follows by induction that N/T is a p-extension. Therefore, (a) has been proven.

The stated ramification index for T/K can be attributed to the calculation of the compositum of the extensions T_i/K (see again, Section 2.6). A first, obvious, bound for $[\mathsf{T} : \mathsf{K}]$ is $e_0 \cdot [\mathsf{K}(\zeta_{e_0}) : \mathsf{K}] \cdot \prod_{i=1}^{\ell} n_i$ with $n_i = e_i f_i \cdot [\mathsf{K}(\zeta_{e_i}) : \mathsf{K}]$. By Theorem

3.15 we can use the extension $\mathsf{L}_{i-1}/\mathsf{L}_i$ to estimate n_i for $1 \le i \le \ell$. We obtain

$$\prod_{i=1}^{\ell} n_i < (p^{s_1} p^{s_2 - s_1} \cdot \ldots \cdot p^{s_\ell - s_{\ell-1}})^2 = (p^{s_\ell})^2 = (p^m)^2.$$

With $e_0 \cdot [\mathsf{K}(\zeta_{e_0}) : \mathsf{K}] < e_0^2$ we obtain (c). □

We can use the tower of extensions in (3.9) to describe the normal closure N and its relationship to T. This has been summarized in Figure 4.

$$\begin{array}{rlcl}
 & & & \mathsf{N} = \mathsf{K}(\alpha_1, \ldots, \alpha_n) \\
 & & & \cup\ p\text{-extension} \\
 & \mathsf{L} = \mathsf{K}(\alpha_1) = \mathsf{L}_0 & \subset & \mathsf{TL}_0 = \mathsf{T}(\alpha_1) \\
p^{s_1} & \cup & & \cup \text{ elementary abelian} \\
 & \mathsf{L}_1 = \mathsf{K}(\alpha_1 \cdots \alpha_{p^{s_1}}) & \subset & \mathsf{TL}_1 = \mathsf{T}(\alpha_1 \cdots \alpha_{p^{s_1}}) \\
p^{s_2 - s_1} & \cup & & \cup \text{ elementary abelian} \\
 & \vdots & & \vdots \\
p^{s_{\ell-1} - s_{\ell-2}} & \cup & & \cup \text{ elementary abelian} \\
 & \mathsf{L}_{\ell-1} = \mathsf{K}(\alpha_1 \cdots \alpha_{p^{s_{\ell-1}}}) & \subset & \mathsf{TL}_{\ell-1} = \mathsf{T}(\alpha_1 \cdots \alpha_{p^{s_{\ell-1}}}) \\
p^{s_\ell - s_{\ell-1}} & \cup & & \cup \text{ elementary abelian} \\
 & \mathsf{L}_\ell = \mathsf{K}(\alpha_1 \cdots \alpha_{p^{s_\ell}}) & \subset & \mathsf{T} \\
e_0 & \cup & & \cup\ e_0 \cdot \operatorname{lcm}(e_1, \ldots, e_\ell) \text{ tamely ramified} \\
 & \mathsf{K} = \mathsf{L}_{\ell+1} & \subset & \mathsf{I} \\
 & & f & \text{unramified}
\end{array}$$

Figure 4. Subfields of a totally ramified extension $\mathsf{L} = \mathsf{K}(\alpha_1)$ and its normal closure N in the notation of Theorem 3.25.

Remark. If the ramification polygon $\mathcal{R}_\varphi$ consists of ℓ non-horizontal segments, then the extension T/K in Theorem 3.25 would be calculated using $e_0 = 1$. Further changes would not be required.

3.8 New Blocks and a Refinement of Ramification Groups

Most of the subject matter in this chapter was predicated on the blocks Δ_i that were introduced in Section 3.3. This makes the prospect of refining these blocks very appealing. Using this as motivation, we introduce a refinement of the blocks by incorporating the roots of the residual polynomials of the ramification polygon. Specifically, for a totally ramified extension L/K, we get additional blocks for each non-horizontal segment of $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ that satisfies two conditions: it has integral slope and its residual polynomial has a root in $\underline{\mathsf{L}} \cong \underline{\mathsf{K}}$.

Lemma 3.26. *Let $\varphi \in \mathcal{O}_\mathsf{K}[x]$ be Eisenstein, α a root of φ, $\mathsf{L} = \mathsf{K}(\alpha)$, and $\mathcal{S}$ a segment of the ramification polygon $\mathcal{R}_\varphi$ of φ. If $\mathcal{S}$ has integral slope $\lambda \neq 0$ and the residual polynomial $\underline{A} \in \underline{\mathsf{K}}[x]$ has a root $\underline{\delta} \in \underline{K}$ then:*

$$\Delta_{\lambda,\underline{\delta}} = \left\{ \alpha' : \begin{array}{l} \varphi(\alpha') = 0 \text{ and either} \\ v_L(\alpha' - \alpha_1) > \lambda + 1 \text{ } \boldsymbol{or} \\ v_L(\alpha' - \alpha_1) = \lambda + 1 \text{ and } \dfrac{-1 + \frac{\alpha'}{\alpha_1}}{\underline{\alpha_1^\lambda}} \in \underline{\delta}\mathbb{F}_p \end{array} \right\}$$

is a block of $\mathrm{Gal}(\varphi)$.

Proof. Let $\sigma \in \mathrm{Gal}(\varphi)$. We have $\alpha_1 \in \Delta_{\lambda,\underline{\delta}}$ regardless of the values of λ and $\underline{\delta}$. So we are interested in α_1 and $\sigma(\alpha_1)$. There are 2 cases to consider.

Case 1: $\sigma(\alpha_1) \in \Delta_{\lambda,\underline{\delta}}$.

There are 2 possibilities.

Subcase 1a: $v_L(\sigma(\alpha_1) - \alpha_1) > \lambda + 1$.

Let $\alpha_k \in \Delta_{\lambda,\underline{\delta}}$ be arbitrary. Then

$$v_L(\sigma(\alpha_k)-\alpha_1) = v_L(\sigma(\alpha_k)-\sigma(\alpha_1)+\sigma(\alpha_1)-\alpha_1) = v_L(\sigma(\alpha_k-\alpha_1)+(\sigma(\alpha_1)-\alpha_1)) \quad (3.10)$$

since σ is a homomorphism.

Because σ is an automorphism, $\sigma(\alpha_k-\alpha_1)$ and $\alpha_k-\alpha_1$ have the same minimal polynomial and the slope of its Newton Polygon gives its valuation. Thus $v_L(\sigma(\alpha_k - \alpha_1)) = v_L(\alpha_k - \alpha_1)$. As $\alpha_k \in \Delta_{\lambda,\underline{\delta}}$ either $v_L(\alpha_k - \alpha_1) > \lambda + 1$ or $v_L(\alpha_k - \alpha_1) = \lambda + 1$ and $\underline{\frac{-1+\frac{\alpha_k}{\alpha_1}}{\alpha_1^\lambda}} \in \underline{\delta}\mathbb{F}_p$.

If $v_L(\alpha_k - \alpha_1) > \lambda + 1$ then by (3.10)

$$\begin{aligned} v_L(\sigma(\alpha_k) - \alpha_1) &= v_L(\sigma(\alpha_k - \alpha_1) + (\sigma(\alpha_1) - \alpha_1)) \\ &\geq \min\{v_L(\sigma(\alpha_k - \alpha_1)), v_L(\sigma(\alpha_1) - \alpha_1)\} \\ &= \min\{v_L(\alpha_k - \alpha_1), v_L(\sigma(\alpha_1) - \alpha_1)\} \\ &> \lambda + 1. \end{aligned}$$

This implies that $\sigma(\alpha_k) \in \Delta_{\lambda,\underline{\delta}}$.

If, instead, $v_L(\alpha_k - \alpha_1) = \lambda + 1$ and $\underline{\frac{-1+\frac{\alpha_k}{\alpha_1}}{\alpha_1^\lambda}} \in \underline{\delta}\mathbb{F}_p$ then by (3.10):

$$\begin{aligned} v_L(\sigma(\alpha_k) - \alpha_1) &= v_L(\sigma(\alpha_k - \alpha_1) + (\sigma(\alpha_1) - \alpha_1)) \\ &= \min\{v_L(\alpha_k - \alpha_1), v_L(\sigma(\alpha_1) - \alpha_1)\} \\ &= v_L(\alpha_k - \alpha_1) \\ &= \lambda + 1 \end{aligned}$$

since $v_L(\sigma(\alpha_k - \alpha_1)) = v_L(\alpha_k - \alpha_1) \neq v_L(\sigma(\alpha_1) - \alpha_1)$.

Since $v_L\left(\frac{-1+\frac{\alpha_k}{\alpha_1}}{\alpha_1^\lambda}\right) = 0$ and L/K is totally ramified, we have

$$\frac{-1+\frac{\alpha_k}{\alpha_1}}{\alpha_1^\lambda} \sim \sigma\left(\frac{-1+\frac{\alpha_k}{\alpha_1}}{\alpha_1^\lambda}\right) = \frac{-1+\frac{\sigma(\alpha_k)}{\sigma(\alpha_1)}}{\sigma(\alpha_1)^\lambda}.$$

Because $v_L(\sigma(\alpha_1)-\alpha_1) > \lambda+1$ we have that $\sigma(\alpha_1) \sim \alpha_1$ and

$$\frac{-1+\frac{\sigma(\alpha_k)}{\sigma(\alpha_1)}}{\sigma(\alpha_1)^\lambda} \sim \frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^\lambda}. \tag{3.11}$$

Since $v_L\left(\frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^\lambda}\right) = 0$, with Equation (3.11) we obtain

$$\underline{\frac{-1+\frac{\sigma(\alpha_k)}{\sigma(\alpha_1)}}{\sigma(\alpha_1)^\lambda}} = \underline{\frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^\lambda}}$$

So $\underline{\frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^\lambda}} = \underline{\frac{-1+\frac{\sigma(\alpha_k)}{\sigma(\alpha_1)}}{\sigma(\alpha_1)^\lambda}} = \underline{\frac{-1+\frac{\alpha_k}{\alpha_1}}{\alpha_1^\lambda}} \in \underline{\delta}\mathbb{F}_p$.

Thus $\underline{\frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^\lambda}} \in \underline{\delta}\mathbb{F}_p$ and $v_L(\sigma(\alpha_k)-\alpha_1) = \lambda+1$. So, once again, $\sigma(\alpha_k) \in \Delta_{\lambda,\underline{\delta}}$. Since α_k was chosen arbitrarily, we have that $\sigma(\Delta_{\lambda,\underline{\delta}}) \cap \Delta_{\lambda,\underline{\delta}} = \Delta_{\lambda,\underline{\delta}}$.

Subcase 1b: $v_L(\sigma(\alpha_1)-\alpha_1) = \lambda+1$ and $\underline{\frac{-1+\frac{\sigma(\alpha_1)}{\alpha_1}}{\alpha_1^\lambda}} \in \underline{\delta}\mathbb{F}_p$.

Let $\alpha_k \in \Delta_{\lambda,\underline{\delta}}$ be arbitrary. If $v_L(\alpha_k-\alpha_1) > \lambda+1$, then (3.10) gives us that

$$\begin{aligned} v_L(\sigma(\alpha_k)-\alpha_1) &= v_L(\sigma(\alpha_k-\alpha_1)+(\sigma(\alpha_1)-\alpha_1)) \\ &= \min\{v_L(\sigma(\alpha_k-\alpha_1)), v_L(\sigma(\alpha_1)-\alpha_1)\} \\ &= \min\{v_L(\alpha_k-\alpha_1), v_L(\sigma(\alpha_1)-\alpha_1)\} \\ &= v_L(\sigma(\alpha_1)-\alpha_1) \\ &= \lambda+1. \end{aligned}$$

Then there exists $\delta_k \in \overline{\mathsf{K}}$ with $v_L(\delta_k) = 0$ so that $\sigma(\alpha_k) = \alpha_1 + \delta_k \alpha_1^{\lambda+1} + \cdots$.

Because $v_L(\alpha_k - \alpha_1) > \lambda + 1$, we have that $v_L(\sigma(\alpha_k) - \sigma(\alpha_1)) = v_L(\sigma(\alpha_k - \alpha_1)) > \lambda + 1$. Thus, the expansions for $\sigma(\alpha_k)$ and $\sigma(\alpha_1)$ agree up to and including the $\alpha_1^{\lambda+1}$ term. In other words, $\sigma(\alpha_1) = \alpha_1 + \delta_k \alpha_1^{\lambda+1} + \cdots$. So

$$\frac{-1 + \frac{\sigma(\alpha_1)}{\alpha_1}}{\alpha_1^{\lambda}} \sim \frac{-1 + \frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^{\lambda}}. \tag{3.12}$$

Because $v_L\left(\frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^{\lambda}}\right) = 0$ we have that

$$\underline{\frac{-1 + \frac{\sigma(\alpha_1)}{\alpha_1}}{\alpha_1^{\lambda}}} = \underline{\frac{-1 + \frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^{\lambda}}}$$

So $\underline{\frac{-1 + \frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^{\lambda}}} = \underline{\frac{-1 + \frac{\sigma(\alpha_1)}{\alpha_1}}{\alpha_1^{\lambda}}} \in \underline{\delta}\mathbb{F}_p$. Thus $\sigma(\alpha_k) \in \Delta_{\lambda,\underline{\delta}}$.

If, instead, $v_L(\alpha_k - \alpha_1) = \lambda + 1$ and $\underline{\frac{-1 + \frac{\alpha_k}{\alpha_1}}{\alpha_1^{\lambda}}} \in \underline{\delta}\mathbb{F}_p$ then (3.10) tells us that

$$\begin{aligned} v_L(\sigma(\alpha_k) - \alpha_1) &= v_L(\sigma(\alpha_k - \alpha_1) + (\sigma(\alpha_1) - \alpha_1)) \\ &\geq \min\{v_L(\sigma(\alpha_k - \alpha_1)), v_L(\sigma(\alpha_1) - \alpha_1)\} \\ &= \min\{\lambda + 1, \lambda + 1\} \\ &= \lambda + 1. \end{aligned}$$

Thus either $v_L(\sigma(\alpha_k) - \alpha_1) > \lambda + 1$ or $v_L(\sigma(\alpha_k) - \alpha_1) = \lambda + 1$. In the former case, it follows immediately that $\sigma(\alpha_k) \in \Delta_{\lambda,\underline{\delta}}$. So we now assume that $v_L(\sigma(\alpha_k) - \alpha_1) = \lambda + 1$. It remains to show that $\underline{\frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^{\lambda}}} \in \underline{\delta}\mathbb{F}_p$.

Since $v_L(\alpha_k - \alpha_1) = \lambda + 1$, there exists $\delta_k \in \overline{\mathsf{K}}$ so that $v_L(\delta_k) = 0$ and $\alpha_k \sim \alpha_1 + \delta_k \alpha_1^{\lambda+1}$. Similarly, there exists $\delta_1 \in \overline{\mathsf{K}}$ so that $v_L(\delta_1) = 0$ and $\sigma(\alpha_1) \sim \alpha_1 + \delta_1 \alpha_1^{\lambda+1}$.

Thus

$$\frac{-1+\frac{\alpha_k}{\alpha_1}}{\alpha_1^\lambda} = \frac{-\alpha_1+\alpha_k}{\alpha_1^{\lambda+1}} \sim \frac{-\alpha_1+\alpha_1+\delta_k\alpha_1^{\lambda+1}}{\alpha_1^{\lambda+1}} = \delta_k$$

and

$$\frac{-1+\frac{\sigma(\alpha_1)}{\alpha_1}}{\alpha_1^\lambda} = \frac{-\alpha_1+\sigma(\alpha_1)}{\alpha_1^{\lambda+1}} \sim \frac{-\alpha_1+\alpha_1+\delta_1\alpha_1^{\lambda+1}}{\alpha_1^{\lambda+1}} = \delta_1.$$

Since $v_L(\delta_1) = v_L(\delta_k) = 0$, we have that

$$\underline{\delta_1} = \underline{\frac{-1+\frac{\sigma(\alpha_1)}{\alpha_1}}{\alpha_1^\lambda}} \in \underline{\delta}\mathbb{F}_p \quad \text{and} \quad \underline{\delta_k} = \underline{\frac{-1+\frac{\alpha_k}{\alpha_1}}{\alpha_1^\lambda}} \in \underline{\delta}\mathbb{F}_p.$$

By assumption, $v_L(\delta_k) = 0$ and L/K is totally ramified, we know that $\delta_k \sim \sigma(\delta_k)$. Therefore $\underline{\sigma(\delta_k)} \in \underline{\delta}\mathbb{F}_p$. Furthermore, since σ is an automorphism

$$\begin{aligned}
\sigma(\alpha_k) &= \sigma(\alpha_1 + \delta_k\alpha_1^{\lambda+1}) \\
&= \sigma(\alpha_1) + \sigma(\delta_k)\sigma(\alpha_1^{\lambda+1}) \\
&\sim \alpha_1 + \delta_1\alpha_1^{\lambda+1} + \sigma(\delta_k)\cdot[\sigma(\alpha_1)]^{\lambda+1} \\
&\sim \alpha_1 + \delta_1\alpha_1^{\lambda+1} + \sigma(\delta_k)\cdot(\alpha_1 + \delta_1\alpha_1^{\lambda+1})^{\lambda+1} \\
&\sim \alpha_1 + \delta_1\alpha_1^{\lambda+1} + \sigma(\delta_k)\cdot\alpha_1^{\lambda+1}.
\end{aligned}$$

Thus

$$\begin{aligned}\frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^{\lambda}} &= \frac{-\alpha_1+\sigma(\alpha_k)}{\alpha_1^{\lambda+1}} \\ &\sim \frac{-\alpha_1+\alpha_1+\delta_1\alpha_1^{\lambda+1}+\sigma(\delta_k)\alpha_1^{\lambda+1}}{\alpha_1^{\lambda+1}} \\ &= \frac{(\delta_1+\sigma(\delta_k))\alpha_1^{\lambda+1}}{\alpha_1^{\lambda+1}} \\ &= \delta_1+\sigma(\delta_k).\end{aligned}$$

Since $v_L\left(\frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^{\lambda}}\right)=0$, we have that

$$\underline{\frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^{\lambda}}} = \underline{\delta_1}+\underline{\sigma(\delta_k)}.$$

Furthermore, $\underline{\delta_1}$, $\underline{\sigma(\delta_k)} \in \underline{\delta}\mathbb{F}_p$ implies that $(\underline{\delta_1}+\underline{\sigma(\delta_k)}) \in \underline{\delta}\mathbb{F}_p$. Therefore $\underline{\frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^{\lambda}}} \in \underline{\delta}\mathbb{F}_p$.

Now we, again, find that $\sigma(\alpha_k) \in \Delta_{\lambda,\underline{\delta}}$. Since α_k was chosen arbitrarily, we have that $\sigma(\Delta_{\lambda,\underline{\delta}}) \cap \Delta_{\lambda,\underline{\delta}} = \Delta_{\lambda,\underline{\delta}}$.

Case 2: $\sigma(\alpha_1) \notin \Delta_{\lambda,\underline{\delta}}$.

Through negating the definition of $\Delta_{\lambda,\underline{\delta}}$ it can be shown that there are 2 possibilities for $\sigma(\alpha_1)$.

Subcase 2a: $v_L(\sigma(\alpha_1)-\alpha_1) < \lambda+1$.

If we choose $\alpha_k \in \Delta_{\lambda,\underline{\delta}}$ arbitrarily then $v_L(\sigma(\alpha_k - \alpha_1)) = v_L(\alpha_k - \alpha_1) \geq \lambda + 1$. Thus, by (3.10), we have that

$$\begin{aligned} v_L(\sigma(\alpha_k) - \alpha_1) &= v_L(\sigma(\alpha_k - \alpha_1) + (\sigma(\alpha_1) - \alpha_1)) \\ &= \min\{v_L(\sigma(\alpha_k - \alpha_1)), v_L(\sigma(\alpha_1) - \alpha_1)\} \\ &= v_L(\sigma(\alpha_1) - \alpha_1) \\ &< \lambda + 1 \end{aligned}$$

telling us that $\sigma(\alpha_k) \notin \Delta_{\lambda,\underline{\delta}}$. Because α_k was chosen arbitrarily, we conclude that $\sigma(\alpha_k) \notin \Delta_{\lambda,\underline{\delta}}$ for all $\alpha_k \in \Delta_{\lambda,\underline{\delta}}$. Therefore, $\sigma(\Delta_{\lambda,\underline{\delta}}) \cap \Delta_{\lambda,\underline{\delta}} = \emptyset$.

Subcase 2b: $v_L(\sigma(\alpha_1) - \alpha_1) = \lambda + 1$ and $\underline{\frac{-1 + \frac{\sigma(\alpha_1)}{\alpha_1}}{\alpha_1^\lambda}} \notin \underline{\delta}\mathbb{F}_p$.

Let $\alpha_k \in \Delta_{\lambda,\underline{\delta}}$ be arbitrary. If $v_L(\alpha_k - \alpha_1) > \lambda + 1$, then $v_L(\sigma(\alpha_k - \alpha_1)) > \lambda + 1$ and (3.10) tells us that

$$\begin{aligned} v_L(\sigma(\alpha_k) - \alpha_1) &= v_L(\sigma(\alpha_k - \alpha_1) + (\sigma(\alpha_1) - \alpha_1)) \\ &= \min\{v_L(\sigma(\alpha_k - \alpha_1)), v_L(\sigma(\alpha_1) - \alpha_1)\} \\ &= v_L(\sigma(\alpha_1) - \alpha_1) \\ &= \lambda + 1. \end{aligned}$$

Because $v_L(\alpha_k - \alpha_1) > \lambda + 1$, (3.12) holds again and, since $v_L\left(\frac{-1 + \frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^\lambda}\right) = 0$, we have

$$\underline{\frac{-1 + \frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^\lambda}} = \underline{\frac{-1 + \frac{\sigma(\alpha_1)}{\alpha_1}}{\alpha_1^\lambda}} \notin \underline{\delta}\mathbb{F}_p.$$

Thus, $\sigma(\alpha_k) \notin \Delta_{\lambda,\underline{\delta}}$.

If, instead, $v_L(\alpha_k - \alpha_1) = \lambda + 1$ and $\underline{\frac{-1+\frac{\alpha_k}{\alpha_1}}{\alpha_1^\lambda}} \in \underline{\delta}\mathbb{F}_p$ then (3.10) tells us that

$$\begin{aligned} v_L(\sigma(\alpha_k) - \alpha_1) &= v_L(\sigma(\alpha_k - \alpha_1) + (\sigma(\alpha_1) - \alpha_1)) \\ &\geq \min\{v_L(\sigma(\alpha_k - \alpha_1)), v_L(\sigma(\alpha_1) - \alpha_1)\} \\ &= \min\{v_L(\alpha_k - \alpha_1), v_L(\sigma(\alpha_1) - \alpha_1)\} \\ &= \min\{\lambda + 1, \lambda + 1\} \\ &= \lambda + 1. \end{aligned}$$

Let us assume that $v_L(\sigma(\alpha_k) - \alpha_1) > \lambda + 1$. Because $v_L(\alpha_k - \alpha_1) = \lambda + 1$, there exists $\delta_k \in \overline{\mathsf{K}}$ so that $v_L(\delta_k) = 0$ and $\alpha_k = \alpha_1 + \delta_k \alpha_1^{\lambda+1} + \cdots$. So $\alpha_k \sim \alpha_1 + \delta_k \alpha_1^{\lambda+1}$. Similarly, $v_L(\sigma(\alpha_1) - \alpha_1) = \lambda + 1$ implies that there exists $\delta_1 \in \overline{\mathsf{K}}$ so that $v_L(\delta_1) = 0$ and $\sigma(\alpha_1) \sim \alpha_1 + \delta_1 \alpha_1^{\lambda+1}$. We will now strive to use δ_1 and δ_k to contradict the assumption made at the outset of this paragraph: $v_L(\sigma(\alpha_k) - \alpha_1) > \lambda + 1$.

As we saw in Subcase 1b, this gives us that

$$\underline{\delta_1} = \underline{\frac{-1 + \frac{\sigma(\alpha_1)}{\alpha_1}}{\alpha_1^\lambda}} \quad \text{and} \quad \underline{\delta_k} = \underline{\frac{-1 + \frac{\alpha_k}{\alpha_1}}{\alpha_1^\lambda}}.$$

So $\underline{\delta_k} \in \underline{\delta}\mathbb{F}_p$ and $\underline{\delta_1} \notin \underline{\delta}\mathbb{F}_p$. Furthermore, since $v_L(\delta_k) = 0$ and L/K is totally ramified, we know that $\sigma(\delta_k) \sim \delta_k$. Therefore, $\underline{\sigma(\delta_k)} \in \underline{\delta}\mathbb{F}_p$.

We now consider $\sigma(\alpha_k - \alpha_1)$. Since σ is an automorphism

$$\sigma(\alpha_k - \alpha_1) \sim \sigma(\alpha_1 + \delta_k \alpha_1^{\lambda+1} - \alpha_1) = \sigma(\delta_k)\sigma(\alpha_1^{\lambda+1}) \sim \sigma(\delta_k)\alpha_1^{\lambda+1}.$$

So

$$\begin{aligned}\sigma(\alpha_k) - \alpha_1 &= \sigma(\alpha_k - \alpha_1) + (\sigma(\alpha_1) - \alpha_1) \text{ by (3.10)} \\ &= \left[\sigma(\delta_k)\alpha_1^{\lambda+1} + \cdots\right] + \left[\delta_1\alpha_1^{\lambda+1} + \cdots\right] \\ &= (\sigma(\delta_k) + \delta_1)\alpha_1^{\lambda+1} + \cdots .\end{aligned}$$

Since $v_L(\sigma(\alpha_k)-\alpha_1) > \lambda+1$ we must have that $\sigma(\delta_k)+\delta_1 = 0$. So $\sigma(\delta_k) = -\delta_1$ which means that $\underline{-\delta_1} \in \underline{\delta}\mathbb{F}_p$. This, however, contradicts the fact that $\underline{\delta_1} \notin \underline{\delta}\mathbb{F}_p$. So we must have that $v_L(\sigma(\alpha_k) - \alpha_1) = \lambda + 1$.

As we saw in Subcase 1b, we have that

$$\underline{\frac{-1 + \frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^{\lambda}}} \;=\; \underline{\delta_1} + \underline{\sigma(\delta_k)}.$$

Since $\underline{\sigma(\delta_k)} \in \underline{\delta}\mathbb{F}_p$ and $\underline{\delta_1} \notin \underline{\delta}\mathbb{F}_p$ we have that $(\underline{\delta_1} + \underline{\sigma(\delta_k)}) \notin \underline{\delta}\mathbb{F}_p$.
Therefore $\underline{\frac{-1+\frac{\sigma(\alpha_k)}{\alpha_1}}{\alpha_1^{\lambda}}} \notin \underline{\delta}\mathbb{F}_p$ and $v_L(\sigma(\alpha_k) - \alpha_1) = \lambda + 1$.

In other words, $\sigma(\alpha_k) \notin \Delta_{\lambda,\underline{\delta}}$. Because α_k was chosen arbitrarily, we conclude that $\sigma(\alpha_k) \notin \Delta_{\lambda,\underline{\delta}}$ for all $\alpha_k \in \Delta_{\lambda,\underline{\delta}}$. Therefore, $\sigma(\Delta_{\lambda,\underline{\delta}}) \cap \Delta_{\lambda,\underline{\delta}} = \emptyset$.

So we have that $\sigma(\alpha_1) \in \Delta_{\lambda,\underline{\delta}}$ implies that $\sigma(\Delta_{\lambda,\underline{\delta}}) \cap \Delta_{\lambda,\underline{\delta}} = \Delta_{\lambda,\underline{\delta}}$ and that $\sigma(\alpha_1) \notin \Delta_{\lambda,\underline{\delta}}$ implies that $\sigma(\Delta_{\lambda,\underline{\delta}}) \cap \Delta_{\lambda,\underline{\delta}} = \emptyset$. Since our choice of $\sigma \in \mathrm{Gal}(\varphi)$ was arbitrary, we conclude that $\sigma(\Delta_{\lambda,\underline{\delta}}) \cap \Delta_{\lambda,\underline{\delta}} \in \{\emptyset, \Delta_{\lambda,\underline{\delta}}\}$ for all $\sigma \in \mathrm{Gal}(\varphi)$. Thus $\Delta_{\lambda,\underline{\delta}}$ is a block of $\mathrm{Gal}(\varphi)$.

□

For the remainder of this section, we assume that L/K is a normal, totally ramified extension generated by the Eisenstein polynomial φ. In this context, we make the following claim: $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$ must have the blocks from Lemma 3.26. Since we have already established that the slopes of $\mathcal{R}_\varphi$ are integral (Section 3.3), all that

remains is to demonstrate that each segment satisfies the other criteria of our lemma. In other words, we must have that each of the residual polynomials of $\mathcal{R}_\varphi$ has a root in $\underline{\mathsf{K}}$.

To see why this last statement must be true, let's assume for a moment that it isn't. If the residual polynomial of a segment didn't have any roots then its segmental inertia degree would be greater than 1. This would indicate that the splitting field of φ would contain an unramified extension in addition to the extension L/K, a clear contradiction to the fact that L/K is normal.

We conclude this section with an application. Because L/K is normal, $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$ contains a decreasing sequence of ramification subgroups (Section 2.5) G_i $(i \geq -1)$. As we noted in section 3.3, the ramification polygon yields a ramification subgroup for each of its segments. We refine this filtration by introducing an additional group for each irreducible factor of the residual polynomial of each non-horizontal segment of the ramification polygon.

Theorem 3.27. *Let $\varphi \in \mathsf{K}[x]$ be Eisenstein of degree n and α a root of φ and $\mathsf{L} = \mathsf{K}(\alpha)$. Assume L/K is normal and let $G = \mathrm{Gal}(\mathsf{L}/\mathsf{K})$. Let S be a segment of nonzero slope $-\lambda \in \mathbb{Z}$ of the ramification polygon of φ. Let $\underline{\delta}$ be a root of the residual polynomial $\underline{A} \in \underline{\mathsf{K}}[x]$ of S. Let*

$$G_{\lambda,\underline{\delta}} = \left\{ \sigma \in G : \begin{array}{l} v_{\mathsf{L}}(\sigma(\alpha) - \alpha) > \lambda + 1 \ \textbf{\textit{or}} \\ v_{\mathsf{L}}(\sigma(\alpha) - \alpha) = \lambda + 1 \ \textit{and} \ \underline{\frac{\sigma(\alpha)-\alpha}{\alpha^{\lambda+1}}} \in \underline{\delta}\mathbb{F}_p \end{array} \right\}.$$

(1) *$G_{\lambda,\underline{\delta}}$ is a subgroup of* $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$.

(2) *$G_{\lambda,\underline{\delta}} \leq G_\lambda$.*

(3) *If $G_\mu < G_\lambda$ then $G_\mu < G_{\lambda,\underline{\delta}}$.*

(4) *$G_\lambda/G_{\lambda,\underline{\delta}}$ is isomorphic to a subgroup of* $(1+\pi_{\mathsf{L}}^{\lambda})/(1+\pi_{\mathsf{L}}^{\lambda+1})$.

(5) *If* $\underline{A}=\underline{\delta}^{\nu}$ *for some* $\nu\in\mathbb{N}$ *then* $G_{\lambda,\underline{\delta}}=G_\lambda$.

Proof. (1) follows from Lemma 3.26.

(2) and (3) are direct consequences of the definitions of G_λ and $G_{\lambda,\underline{a}}$.

(4) follows from (2) and part (1) of Proposition 2.32.

(5) Denote by $\alpha=\alpha_1,\alpha_2,\ldots,\alpha_n$ the zeros of φ. The zeros of $\underline{A}$ are $\left(-1+\frac{\alpha_i}{\alpha}\right)^e/\alpha^h$ for $1\leq i\leq n$. Thus if $\underline{A}=\underline{a}^{\nu}$ these are also zeros of $\underline{a}$ and thus $G_{\lambda,\underline{a}}=G_\lambda$. □

Example 3.28. (By Brian Sinclair) Let $\mathsf{K}/\mathbb{Q}_2$ be the unramified extension of degree 2 and $\underline{\mathsf{K}}=\mathbb{F}_2(\underline{\gamma})$. The polynomial $\varphi=x^8+2x^6+4x^3+4x+2\in\mathcal{O}_{\mathsf{K}}[x]$ has ramification polygon $\{(1,9),(2,6),(8,0)\}$ with a segment of slope -3 and length 1 and a segment of slope -1 and length 6. The residual polynomials of the segments are $z+1\in\underline{\mathsf{K}}[z]$ and $z^6+1=(z+1)^2(z+\underline{\gamma})^2(z+\underline{\gamma}^2)^2\in\underline{\mathsf{K}}[z]$. The extension $\mathsf{L}=\mathsf{K}[x]/(\varphi)$ is normal and $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$ has the subgroups G_1, $G_{1,z+1}$, $G_{1,z+\underline{\gamma}}$, $G_{1,z+\underline{\gamma}^2}$, and G_3 with

$$\{\mathrm{id}\}<G_3<\left\{\begin{array}{l}G_{1,z+1}\\ G_{1,z+\underline{\gamma}}\\ G_{1,z+\underline{\gamma}^2}\end{array}\right\}<G_1=\mathrm{Gal}(\mathsf{L}/\mathsf{K}).$$

This is the complete lattice of subgroups of $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$.

Example 3.29. (By Brian Sinclair) Let $\mathsf{K}/\mathbb{Q}_2$ be the unramified extension of degree 2 and $\underline{\mathsf{K}}=\mathbb{F}_2(\underline{\gamma})$. The polynomial $\varphi=x^8+4x^5+2x^4+2\in\mathcal{O}_{\mathsf{K}}[x]$ has ramification polygon $\{(1,13),(4,4),(8,0)\}$ with a segment of slopes -3 and length 3 and a segment of slope -1 and length 4. The residual polynomials of the segments are $z^3+1=(z+1)(z+\underline{\gamma})(z+\underline{\gamma}^2)\in\underline{\mathsf{K}}[z]$ and $z^4+1=(z+1)^4\in\underline{\mathsf{K}}[z]$. The extension $\mathsf{L}=\mathsf{K}[x]/(\varphi)$

is normal and we obtain the subgroups G_1, G_3, $G_{3,z+1}$, $G_{3,z+\underline{\gamma}}$, and $G_{3,z+\underline{\gamma}^2}$ of $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$ with

$$\{\mathrm{id}\} < \left\{ \begin{array}{l} G_{3,z+1} \\ G_{3,z+\underline{\gamma}} \\ G_{3,z+\underline{\gamma}^2} \end{array} \right\} < G_3 < G_1 = \mathrm{Gal}(\mathsf{L}/\mathsf{K}).$$

In this example we are missing two subgroups of $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$ of order 4.

CHAPTER IV

RESOLVENTS

The most efficient algorithms for computing Galois groups over the rational numbers are based on Richard Staudhuar's relative resolvent method [82]. In his original paper, Stauduhar introduced an algorithm that computed an irreducible polynomial's Galois group by transversing the subgroup lattice of S_n. His primary tool was the computation of select resolvent polynomials, a class of specialized polynomials whose simple roots dictate whether to and/or how to move along the aforementioned subgroup lattice.

In this chapter, we examine the basic properties and typical usage of resolvents. Special attention is given to computational efficiency and the implementation of particular examples. Throughout, we let Z denote an integral domain with multiplicative identity 1, and we let Q be the field of fractions of Z. We also assume that the characteristic of Q is 0.

4.1 Basic Concepts and Notation

For the remainder of this chapter we assume that we have been provided with a monic, irreducible polynomial $f \in Z[x]$ with $\deg(f) = n$ and that we wish to compute $\mathrm{Gal}(f)$, the Galois group of f. We denote by $\alpha_1, \ldots, \alpha_n$ the roots of f in some algebraic closure of Q. Since f is irreducible, its Galois group acts transitively on the set $\{\alpha_1, \ldots, \alpha_n\}$. Naturally, this implies that $\mathrm{Gal}(f)$ can be represented/regarded as a transitive permutation group acting on n elements.

We denote by S_n the symmetric group on n elements. Every element σ of S_n acts on elements of the multivariate ring $\mathbb{Z}[x_1, \ldots, x_n]$ by acting upon the subscripts of the variables

$$x_i \mapsto x_{\sigma(i)}.$$

If $F \in \mathbb{Z}[x_1, \ldots, x_n]$ and $\sigma \in S_n$, then we denote by F^σ the image of F under the action by σ. When applying a sequence of permutation elements to F, we define the action to be a right action. We illustrate this with a concrete example. If we acted upon F by $g \in S_n$ and then acted upon the result by $h \in S_n$ then we would denote this by

$$(F^g)^h = F^{gh}$$

where the product gh implies that g is applied first and then h is applied to the result.

In the event that F is fixed by every element of some $H \leq S_n$, we say that F is *H-invariant*. In symbols, this means that F is H-invariant when $F^\sigma = F$ for all $\sigma \in H$. For our purposes we are interested in the case where only the elements of H fix F.

Definition 4.1. If $H < G \leq S_n$ is a pair of subgroups then we call $F \in \mathbb{Z}[x_1, \ldots, x_n]$ a *G-relative H-invariant* if H is $\mathrm{Stab}_G F := \{\sigma \in G \mid F^\sigma = F\}$, the stabilizer of F in G.

It is clear that for $H < G \leq S_n$ every S_n-relative H-invariant is also a G-relative H-invariant. Therefore, the following lemma proves that a G-relative H-invariant can always be found for such H and G.

Lemma 4.2 ([24, Lemma 4.1]). *$F := \sum_{\sigma \in H} \left(\prod_{i=1}^{n-1} x_i^i \right)^\sigma$ is a S_n-relative H-invariant.*

In total, $\#H(n-2)$ multiplications are required to evaluate this invariant. This typically makes the invariant too expensive to use. In practice, invariants of small degree and a small number of terms are preferred. The most complete, current method for computing efficient invariants for every possible group combination $H < G$ is given in [24]. Currently this method is implemented in the Computer algebra system Magma and is considered to be accurate with high probability.

Once an invariant polynomial F has been found for a group pair $H < G$, we can say a great deal about the relationship between F and it's stabilizer H. The following two theorems offer the reader a glimpse of this relationship while providing information that will be vital to our discussion in the next section.

Theorem 4.3 ([82, Theorem 2]). *For subgroups $H < G \leq S_n$, let F be a G-relative H-invariant. If $\sigma_1, \sigma_2 \in G$ then $F^{\sigma_1} = F^{\sigma_2}$ if and only if σ_1, σ_2 lie in the same right coset of G/H.*

Proof. Suppose that $F^{\sigma_1} = F^{\sigma_2}$. If we act upon both sides by σ_2^{-1} then we have $F^{\sigma_1\sigma_2^{-1}} = F^{\sigma_2\sigma_2^{-1}} = F$. Since only the elements of H fix F, we have that $\sigma_1\sigma_2^{-1} \in H$. This implies that $H\sigma_1 = H\sigma_2$. The forward direction has been proven.

Conversely, suppose that $H\sigma_1 = H\sigma_2$. Then $\sigma_1\sigma_2^{-1} \in H$ which implies that $F^{\sigma_1\sigma_2^{-1}} = F$. Acting upon both sides by σ_2 we have that $F^{\sigma_1\sigma_2^{-1}\sigma_2} = F^{\sigma_2}$ which is equivalent to $F^{\sigma_1} = F^{\sigma_2}$. □

Theorem 4.4 ([82, Theorem 3]). *For subgroups $H < G \leq S_n$, let F be a G-relative H-invariant. If $\sigma \in G$ then F^σ is a G-relative $\sigma^{-1}H\sigma$-invariant.*

Proof. Suppose that $\sigma \in G$ and $\tau \in \sigma^{-1}H\sigma$. Then there exists $h \in H$ such that $\tau = \sigma^{-1}h\sigma$. Acting upon F^σ by τ yields

$$\begin{aligned}(F^\sigma)^\tau &= F^{\sigma\tau} \\ &= F^{\sigma\sigma^{-1}h\sigma} \\ &= F^{h\sigma} \\ &= (F^h)^\sigma \\ &= F^\sigma\end{aligned}$$

since F is H-invariant. Because τ was chosen arbitrarily, we conclude that every element of $\sigma^{-1}H\sigma$ fixes F^σ. Thus $\sigma^{-1}H\sigma \leq \mathrm{Stab}_G F^\sigma$.

Now assume that $\mu \in \mathrm{Stab}_G F^\sigma$. Then $F^\sigma = (F^\sigma)^\mu = F^{\sigma\mu}$. Thus Theorem 4.3 tells us that $\sigma(\sigma\mu)^{-1} \in H$. In other words, $\sigma\mu^{-1}\sigma^{-1} = h$ for some $h \in H$. Multiplying both sides on the left by σ^{-1} and on the right by σ we obtain

$$\mu^{-1} = \sigma^{-1}h\sigma.$$

Inversion of both sides leaves us with $\mu \in \sigma^{-1}H\sigma$. Therefore, $\mathrm{Stab}_G F^\sigma \leq \sigma^{-1}H\sigma$. □

4.2 Stauduhar's Method

Stauduhar originally formulated his method for polynomials over the integers. When needed later in our work we state generalizations of his results. When discussing some details of his method we do so for $Z = \mathbb{Z}$.

Definition 4.5. Let $f(x)$ be a monic, irreducible polynomial of degree n with coefficients in Z. Let $\alpha_1, \ldots, \alpha_n$ be an ordering of the roots of $f(x)$. Suppose $H < G$ are subgroups of S_n acting on $\{x_1, \ldots, x_n\}$ with $\mathrm{Gal}(f) \leq G$ under the given root ordering.

Let $G//H$ denote a set of representatives of right cosets of G/H. If $F \in \mathbb{Z}[x_1, \ldots, x_n]$ satisfies $H = \mathrm{Stab}_G F$ then

$$R_F(G, f) := \prod_{\sigma \in G//H} (x - F^\sigma(\alpha_1, \ldots, \alpha_n))$$

is a polynomial in x called the *resolvent polynomial* corresponding to $H < G$.

- If $G = S_n$, we call the resolvent polynomial an *absolute resolvent*.
- If $G < S_n$, we call the resolvent polynomial a *relative resolvent*.
- The resolvent polynomial is called a *linear resolvent* if $F(x_1, \ldots, x_n) = a_1 x_1 + \ldots + a_n x_n$ for some $a_1, \ldots, a_n \in \mathbb{Z}$.

One striking aspect of the immediately preceding definition is that $G//H$ is not specified beyond being a complete set of right coset representatives. The reason for this is simple: it does not matter which element is selected from a right coset of G/H. According to Theorem 4.3, if two elements lie in the same right coset then their action on F is the same. This tells us that regardless of how the coset representatives are chosen, the linear factors in the product

$$\prod_{\sigma \in G//H} (x - F^\sigma(\alpha_1, \ldots, \alpha_n))$$

are the same. At most they are in a different order.

Theorem 4.6 ([82, Theorem 4])**.** *Using the notation and assumptions of Definition* 4.5*, the coefficients of the resolvent polynomial $R_F(G, f)$ are elements of Z.*

Proof. We begin by observing that every root of f is integral over Z. Since the set of elements that are integral over Z is closed under addition and multiplication, we

know that sums and products of the roots of f are integral over Z. By construction, this implies that the coefficients of $R_F(G, f)$ are integral over Z.

Because every integral domain is a unique factorization domain, Z is integrally closed in its field of fractions Q. Thus, it is sufficient to demonstrate that the coefficients of $R_F(G, f)$ are elements of Q.

If we let $\sigma_1, \ldots, \sigma_m$ denote a set of representatives for the right cosets of H in G, then we have that

$$R_F(G, f) = \prod_{i=1}^{m} (x - F^{\sigma_i}(\alpha_1, \ldots, \alpha_n)).$$

Suppose $\tau \in \mathrm{Gal}(f)$. Then $\tau(R_F(G, f))$ has the form

$$\begin{aligned} \tau(R_F(G, f)) &= \prod_{i=1}^{m} (x - (F^{\sigma_i}(\alpha_1, \ldots, \alpha_n))^{\tau}) \\ &= \prod_{i=1}^{m} (x - F^{\sigma_i \tau}(\alpha_1, \ldots, \alpha_n)). \end{aligned}$$

Because the set $\{\sigma_1\tau, \ldots, \sigma_m\tau\}$ is also a complete set of right coset representatives of G/H, we know from Theorem 4.3 that $\tau(R_F(G, f)) = R_F(G, f)$. Since τ was selected arbitrarily, we conclude that the coefficients of $R_F(G, f)$ are unaffected by the application of elements of $\mathrm{Gal}(f)$. Thus, by the definition of $\mathrm{Gal}(f)$, we must have that the coefficients of the resolvent polynomial are elements of Q. □

Theorem 4.7 ([82, Theorem 5])**.** *Using the notation and assumptions of Definition* 4.5*, assume that $F(\alpha_1, \ldots, \alpha_n)$ is a simple root of $R_F(G, f)$. Then* $\mathrm{Gal}(f) \leq H$ *if and only if $F(\alpha_1, \ldots, \alpha_n)$ is an element of Z.*

Proof. According to Theorem 4.6, $F(\alpha_1, \ldots, \alpha_n)$ is a root of a monic polynomial in $Z[x]$. As such, $F(\alpha_1, \ldots, \alpha_n)$ is integral over Z.

Suppose $\mathrm{Gal}(f)$ is a subgroup of H. Then every element of $\mathrm{Gal}(f)$ is in the stabilizer of F in G. This implies that $F(\alpha_1, \ldots, \alpha_n)$ is unaffected by the application of any element of $\mathrm{Gal}(f)$. As previously shown in the proof of Theorem 4.6, this is enough to conclude that $F(\alpha_1, \ldots, \alpha_n) \in Z$. The forward direction has been proven.

Conversely, suppose that $F(\alpha_1, \ldots, \alpha_n)$ is in Z. Then every element of $\mathrm{Gal}(f)$ fixes $F(\alpha_1, \ldots, \alpha_n)$. Because $F(\alpha_1, \ldots, \alpha_n)$ is a simple root, only the elements of one right coset in G/H fix $F(\alpha_1, \ldots, \alpha_n)$. Furthermore, by definition, the only elements of G that fix F are those in H which is itself a coset of H in G. Taking all of this together, we conclude that only the elements of H fix $F(\alpha_1, \ldots, \alpha_n)$. Thus we have that $\mathrm{Gal}(f) \leq H$. □

Corollary 4.8. *Assume that $F^\sigma(\alpha_1, \ldots, \alpha_n)$ is a simple root of $R_F(G, f)$. Then $\mathrm{Gal}(f) \leq \sigma^{-1}H\sigma$ if and only if $F^\sigma(\alpha_1, \ldots, \alpha_n)$ is an element of Z*

The proof follows from Theorem 4.4.

Corollary 4.9. *Suppose $F^\sigma(\alpha_1, \ldots, \alpha_n)$ is an element of Z and a simple root of $R_F(G, f)$ so that $\mathrm{Gal}(f) \leq \sigma^{-1}H\sigma$. If the roots of $f(x)$ are reordered according to the rule $\alpha'_i = \alpha_{\sigma(i)}$, then $F(\alpha'_1, \ldots, \alpha'_n)$ is in Z, and with respect to this new ordering, $\mathrm{Gal}(f) \leq H$.*

In practice, we check to see if a resolvent polynomial $R_F(G, f)$ is squarefree before we determine whether or not it has a root in Z. Since $R_F(G, f)$ is monic and Q has characteristic 0, $R_F(G, f)$ is squarefree if and only if

$$\gcd(R_F(G, f), R'_F(G, f)) = 1$$

where $R'_F(G, f)$ is the formal derivative of $R_F(G, f)$. If $R_F(G, f)$ fails to be squarefree we can use a Tschirnhausen transformation to proceed one of two ways.

The first option is to replace our polynomial f with a new polynomial that has the same Galois group ([14, Algorithm 6.3.4]). The resolvent $R_F(G, f)$ would then be recalculated with respect to the new polynomial. If additional resolvents are needed to find $\mathrm{Gal}(f)$, the roots of the new polynomial would be used. In short, f would be permanently replaced.

The second option is to create $t \in \mathbb{Z}[x]$ that is at least quadratic and recompute $R_F(G, f)$ as

$$R_{F,t}(G, f) := \prod_{\sigma \in G//H} (x - F^\sigma(t(\alpha_1), \ldots, t(\alpha_n))).$$

It has been proven ([30]) that such a polynomial t can be found so that $R_{F,t}(G, f)$ is squarefree. Also, as in the case of the first option, the use of t would still lead to the correct Galois group.

Since a Tschirnhausen transformation can always be applied, we will assume for the remainder of this chapter that every resolvent polynomial is squarefree.

A well-known resolvent that is always applicable for polynomials over Z can be found in the following example.

Example 4.10. Let A_n denote the alternating group on n elements. It can be shown that

$$F(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j)$$

is an A_n-invariant. If $\sigma \in S_n$ is an odd permutation, then $F^\sigma = -F$. Thus, F is a S_n-relative A_n-invariant and its corresponding resolvent is

$$R_F(S_n, f) = x^2 - \mathrm{disc}\,(f) \in Z[x].$$

As f is irreducible, $\operatorname{disc}(f)$ is nonzero. Thus $R_F(S_n, f)$ is squarefree and a Tschirnhausen transformation is unnecessary.

It follows that $R_F(S_n, f)$ has a linear factor over Z if and only if $\operatorname{disc}(f)$ is a perfect square. Since A_n is the only subgroup of S_n that has index 2, we have that

$$\operatorname{Gal}(f) \leq A_n \iff \sqrt{\operatorname{disc}(f)} \in Z$$

by Theorem 4.7 and its first corollary.

We conclude this section with an overview of Stauduhar's classic method for determining the Galois group of a monic, irreducible polynomial $f \in \mathbb{Z}[x]$. For more detailed descriptions of this method, we suggest the following sources: [28], [29], and [24].

Stauduhar's first step was to compute high-precision, complex approximations to the roots of f. He then put the roots in an arbitrary order $\alpha_1, \ldots, \alpha_n$ and set $G := S_n$. Since S_n contains every permutation on n elements, this gave him $\operatorname{Gal}(f) \leq G$ regardless of the ordering of the roots of f.

The next phase of his method entailed either replacing G with a smaller group or verifying that $G = \operatorname{Gal}(f)$. To this end, he considered the maximal subgroups of G. For a given maximal subgroup $H < G$ he would find a G-relative H-invariant $F(x_1, \ldots, x_n)$ and compute the corresponding resolvent polynomial $R_F(G, f)$. Then he would use Corollary 4.8 to determine whether $\operatorname{Gal}(f) \leq \sigma^{-1} H \sigma$ for some right coset representative σ.

If Stauduhar determined that $\operatorname{Gal}(f)$ was not contained in a maximal subgroup of G, then he concluded that $\operatorname{Gal}(f) = G$. Otherwise, if $\operatorname{Gal}(f) \leq \sigma^{-1} H \sigma$ for $H < G$ maximal and $H\sigma \in G/H$, he would reorder the roots of f (see Corollary 4.9) so that

$\mathrm{Gal}(f) \leq H$ and repeat the above procedure with $G = H$. This would continue until $\mathrm{Gal}(f)$ was identified.

4.3 Improvements to Stauduhar's Method

In recent years, key aspects of Stauduhar's resolvent method have been improved upon. In this section, we focus on two such aspects: the approximations of polynomial roots and the selection of a starting group. For the latter, we focus exclusively on the case where the stem field $Q[x]/(f(x))$ has a non-trivial subfield.

4.3.1 Root Approximations

An important consideration when working with resolvents is how one can guarantee accuracy in the computation and testing of each resolvent polynomial. Typically, this translates to an analysis of how one goes about approximating the roots $\alpha_1, \ldots, \alpha_n$ of $f(x)$ and the corresponding roots $F^\sigma(\alpha_1, \ldots, \alpha_n)$ for a particular resolvent.

Stauduhar, for his part, used high-precison, complex approximations throughout. Since every resolvent polynomial he used had integer coefficients, he computed the roots $F^\sigma(\alpha_1, \ldots, \alpha_n)$ to a precision high enough to guarantee that, once the product in Definition 4.5 was formed, the coefficients of the resolvent would be off by at most $\pm\frac{1}{2}$. Using the approximations to $\alpha_1, \ldots, \alpha_n$, he accomplished this task by performing (potentially) a multitude of complex, floating-point arithmetic operations.

Unfortunately, this approach often requires the use of approximations with precision so high that they lead to very long run times.

Another school of thought favors the use of p-adic approximations to the roots of $f(x) \in \mathbb{Z}[x]$. This approach was first suggested in [84] and has since been adopted

and expanded upon by [29] and [24] among others. We summarize this idea in the lemma below (compare to [29, Lemma 2.16]).

Lemma 4.11. *Let $f \in \mathbb{Z}[x]$ be irreducible. Let p be a rational prime that doesn't divide the discriminant* $\operatorname{disc}(f)$*, and let $f = \prod_{i=1}^{k} f_i$ be the factorization of f over $\mathbb{F}_p$ where f_i is irreducible for $1 \leq i \leq k$. If $m = \operatorname{lcm}\{\deg(f_i) \mid 1 \leq i \leq k\}$, then f splits into linear factors over the unramified extension of $\mathbb{Q}_p$ of degree m.*

Proof. Since p does not divide $\operatorname{disc}(f)$, we know that $\operatorname{disc}(f)$ is nonzero over $\mathbb{F}_p$. It is clear from Definition 2.12 that this implies that $f(x) \bmod p$ has $\deg(f)$ distinct roots.

Put another way, $\underline{f}(z) \in \underline{\mathbb{Q}_p}[z] \cong \mathbb{F}_p[z]$ is squarefree. The result follows from Proposition 2.16. □

In practice, root approximations in p-adic fields tend to require less precision and lead to lower run times than complex approximations. For additional details, see [29, Theorem 2.17].

4.3.2 Starting Groups

As we discussed in Section 4.2, Stauduhar's method begins with $G = S_n$ and, if $\operatorname{Gal}(f) \neq S_n$, replaces G with smaller and smaller groups until it reaches the Galois group. In short, this method picks the top group in the subgroup lattice of permutation groups on n elements and works its way down to the Galois group.

The primary issue with this approach is the work required to move from S_n to one of its maximal subgroups. As n gets larger, S_n has maximal subgroups with increasingly large indices. For example, five of the six transitive maximal subgroups of S_{18} have index greater than or equal to 24310:

- $[S_{18} : 18T468] = 1307674368000$

- $[S_{18} : 18T962] = 190590400$
- $[S_{18} : 18T968] = 34459425$
- $[S_{18} : 18T977] = 2858856$
- $[S_{18} : 18T981] = 24310$.

Since the index $|S_n/H|$ of a maximal subgroup $H < S_n$ is the degree of the corresponding resolvent, this leads to massive resolvents that require a lot of time to construct and test for roots. Because of this, modern relative resolvent methods aim to avoid computing resolvents for group pairs $H < S_n$. Normally, these efforts culminate in either: confirming $\mathrm{Gal}(f) = S_n$ by examining the factorization of f over various finite fields $\mathbb{F}_p$ (see [29, Remark 2.4]) or choosing a smaller group G as the starting point on the subgroup lattice. In the event, that $Q[x]/(f)$ has a nontrivial subfield, the latter is achievable.

For the remainder of this section, we assume that $\mathsf{M} := Q[x]/(f)$ has a nontrivial subfield $\mathsf{L} = Q(\beta)$. In time, we will show that, under the correct root ordering, $\mathrm{Gal}(f) \leq \mathrm{Gal}(\mathsf{M}/\mathsf{L}) \wr \mathrm{Gal}(\mathsf{L}/Q)$. However, before we can delve into a full explanation, we first need to establish the block system of $\mathrm{Gal}(f)$ that we get from our subfield L.

If we let α denote a root of f so that $\mathsf{M} = Q(\alpha)$, then we can (see [48]) describe the precise embedding of the primitive element β into M with a polynomial $h \in Q[t]$ that satisfies $h(\alpha) = \beta$. As the theorem below demonstrates, the embedding polynomial allows us to compute a block system $\mathfrak{B} = \{B_1, \ldots, B_m\}$ of $\mathrm{Gal}(f)$ where $m = [\mathsf{L} : Q]$.

Theorem 4.12 ([29, Theorem 3.1])**.** *Let* $\mathsf{L} = Q(\beta)$, $\mathsf{M} = Q(\alpha)$ *be algebraic extensions of* Q *with* $Q \subseteq \mathsf{L} \subseteq \mathsf{M}$, *and let* g, $f \in Z[x]$ *be the minimal polynomials of* β *and* α,

respectively. Let $h \in Q[x]$ *be the embedding polynomial with* $h(\alpha) = \beta$. *Denote the conjugates of* α *and* β *in some algebraic closure with* $\alpha_1, \ldots, \alpha_n$ *and* $\beta_1, \ldots, \beta_m$, *respectively. Defining* $B_i = \{\alpha_j \mid h(\alpha_j) = \beta_i\}$ *it follows that:*

(1) $B_1, \ldots, B_m$ *form a block system of* $\mathrm{Gal}(f)$. *Furthermore,* $n = |B_i|\, m$.

(2) $\mathrm{Gal}(g)$ *is isomorphic to the permutation representation of* $\mathrm{Gal}(f)$ *with respect to* $B_1, \ldots, B_m$ *under the mapping* $\theta : \beta_i \mapsto B_i$.

Proof. (1) Let $\sigma \in \mathrm{Gal}(f)$, and let i satisfy $1 \leq i \leq m$. Since $\beta \in Q(\alpha)$ is algebraic over Q, $\sigma(\beta_i)$ is a conjugate of β. We claim that $\sigma(\beta_i) = \beta_k$ if and only if $\sigma(B_i) = B_k$.

Suppose $\sigma(\beta_i) = \beta_k$ and let $\delta \in B_i$. Since σ is an automorphism and h is a polynomial, we have that $\sigma(h(a)) = h(\sigma(a))$ for all a in the domain of h. This directly leads to

$$\begin{aligned} h(\sigma(\delta)) &= \sigma(h(\delta)) \\ &= \sigma(\beta_i) \\ &= \beta_k \end{aligned}$$

which implies that $\sigma(\delta) \in B_k$. Because δ was selected arbitrarily, we conclude that $\sigma(B_i) \subseteq B_k$. Furthermore, by a similar argument, $\beta_i = \sigma^{-1}(\beta_k)$ leads us to $\sigma^{-1}(B_k) \subseteq B_i$. This is equivalent to $B_k \subseteq \sigma(B_i)$ since σ is bijective. Therefore, the forward direction has been proven.

Conversely, suppose that $\sigma(B_i) = B_k$. Let $\tau \in \sigma(B_i)$. Then there exists $\delta \in B_i$ such that $\tau = \sigma(\delta)$. Furthermore, we have that $\delta = \sigma^{-1}(\tau)$ and $h(\delta) = \beta_i$. Putting

all of this together we can determine $\sigma(\beta_i)$:

$$\begin{aligned}\sigma(\beta_i) &= \sigma(h(\delta)) \\ &= h(\sigma(\delta)) \\ &= h(\tau) \\ &= \beta_k.\end{aligned}$$

Hence the assertion has been proven. This implies that $\sigma(B_i)$ is either B_i or another set B_j. Since the sets $B_1, \ldots, B_m$ must be disjoint we have $\sigma(B_i) \cap B_i = \{B_i, \emptyset\}$ for $\sigma \in \mathrm{Gal}(f)$. The cardinality condition on B_i follows from the fact that $\mathrm{Gal}(f)$ is transitive.

(2) We have shown that $\sigma(\beta_i) = \beta_i$ if and only if $\sigma(B_i) = B_i$. This implies that $\mathrm{Stab}_{\mathrm{Gal}(f)}(B_i)$ is exactly the set of elements in $\mathrm{Gal}(f)$ that fix β_i and hence fix all of $Q(\beta_i)$. Thus $\mathrm{Stab}_{\mathrm{Gal}(f)}(B_i)$ corresponds to $Q(\beta_i)$ under the Galois correspondence of Theorem A.17. Under this correspondence, a subgroup of $\mathrm{Gal}(f)$ corresponds to its fixed field. Therefore,

$$Q(\beta_i) = \mathrm{Fix}(\mathrm{Stab}_{\mathrm{Gal}(f)}(B_i)).$$

It follows directly from this equality that $\mathrm{Gal}(g)$ is isomorphic to the permutation representation of $\mathrm{Gal}(f)$ with respect to the block system under the suggested mapping θ. □

Let $g \in Z[x]$ be the minimal polynomial of β. According to the second part of Theorem 4.12, the action of $\mathrm{Gal}(f)$ on the blocks $B_1, \ldots, B_m$ is equivalent to the action of $\mathrm{Gal}(g)$ on the roots of g. It follows, from this equivalence, that $\mathrm{Gal}(f)$ can

be embedded as a permutation group into the wreath product $\mathrm{Gal}(\mathsf{M}/\mathsf{L}) \wr \mathrm{Gal}(\mathsf{L}/Q)$. The theorem below is a variant of the Krasner-Kaloujnine Theorem.

Theorem 4.13 ([51])**.** *Let (G, W) be a transitive, imprimitive permutation group with block system $\mathfrak{B} = \{B_1, \ldots, B_m\}$ where each block is size l. Let X and Y be finite sets such that $|X| = l$ and $|Y| = m$. Then G acts transitively on Y and there is $H \leq G$ that acts on X such that (G, W) can be embedded in $(H \wr (G, Y), X \times Y)$.*

The proof of this theorem and the subsequent corollary are modelled after the approachs in [27] and [18].

Proof. (By Sandi Rudzinski) Let $Y = \{y_1, \ldots, y_m\}$ and $X = \{x_1, \ldots, x_l\}$. Let $\theta : W \to X \times Y$ be a bijection such that $\theta(w) = (x_i, y_j) \implies w \in B_j$ for all $w \in W$.

Using θ, we can view G as a transitive, imprimitive permutation group on $X \times Y$ with blocks $B_j = X \times \{y_j\}$ for $1 \leq j \leq m$. We will write $(x, y)g$ instead of $\theta^{-1}((x, y))g$.

Let $\psi : G \to S_m$ be the permutation representation of G with respect to the action of G on $\mathfrak{B}$. Let $g \in G$ with $\psi(g) = \sigma \in S_m$. Then G acts on Y by

$$(y_i)g = (y_i)\psi(g) = (y_i)\sigma = y_{\sigma(i)}.$$

Since the action of G on W is transitive, the action of G on Y is also transitive.

Fix $y_1 \in Y$ and let $H = \mathrm{Stab}_G(y_1)$. Since $B_1 = X \times \{y_1\}$. This implies that H permutes the elements of X. Since $|X| = l$, we have that $\varphi : H \to S_l$ is the permutation representation of H. Let $h \in H$ with $\varphi(h) = \tau \in S_l$. So again H acts transitively on X by

$$x_i h = x_i \varphi(h) = (x_i)\tau = x_{\tau(i)}.$$

Fix $(x_1, y_1) \in X \times Y$ and let $g \in G$ such that $(x_1, y_1)g = (x_2, y_2)$ for some $(x_2, y_2) \in X \times Y$.

With respect to g as above, define $f \in \mathrm{Map}(Y, H) = H^Y$ and $h \in (G, Y)$ by $(y_1)h = y_2$ and $(x_1)f^h(y_1) = (x_1)f(y_1h^{-1}) = x_2$. Since G acts transitively on $X \times Y$ and H acts transitively on X, it is clear that we can define such a pair, (f, h) for each $g \in G$ given by the action of g on (x_1, y_1).

Define the map $\chi : G \to H \wr (G, Y)$ by $g \mapsto (f, h)$ defined as above by the action of g on the fixed point (x_1, y_1). Let $g \in G$ with $(x_1, y_1)g = (x_2, y_2)$ for some $(x_2, y_2) \in X \times Y$.

$$\begin{aligned}(x_1, y_1)\chi(g) &= (x_1, y_1)(f, h) \\ &= (x_1 f^h(y_1), (y_1)h) \\ &= (x_2, y_2) \\ &= (x_1, y_1)g\end{aligned}$$

This shows that $\chi(g)$ acts on $X \times Y$ as G does. We will use this to show that χ is a homomorphism. Let $g_1, g_2 \in G$ be arbitrary.

$$\begin{aligned}(x, y)\chi(g_1g_2) &= (x, y)g_1g_2 \\ &= ((x, y)g_1)\chi(g_2) \\ &= ((x, y)\chi(g_1))(\chi(g_2) \\ &= (x, y)(\chi(g_1)\chi(g_2))\end{aligned}$$

To prove that χ is injective, we will show $\ker(\chi)$ is trivial. Let $g \in G$ with $g \in \ker(\chi)$. Then we have that

$$(x, y) = (x, y)\chi(g) = (x, y)g$$

for all $(x, y) \in X \times Y$. So we must have that g is the identity element of G and the kernel is trivial as desired. □

Corollary 4.14 ([51])**.** *Let $Q \subset \mathsf{L} \subset \mathsf{M}$ be finite separable field extensions. Then the Galois group* $\mathrm{Gal}(\mathsf{M}/Q)$ *of* M *over Q can be embedded as a permutation group into the wreath product* $\mathrm{Gal}(\mathsf{M}/\mathsf{L}) \wr \mathrm{Gal}(\mathsf{L}/Q)$.

Proof. (By Sandi Rudzinski) Let $\mathsf{L} = Q(\beta)$, and let $\mathsf{M} = Q(\alpha)$ with $h(\alpha) = \beta$ for $h \in Q[t]$. Fix a normal closure N of M over Q that contains L. Let $G = \mathrm{Gal}(\mathsf{N}/Q)$. Define W to be the Q-embeddings of M into N, Y to be the Q-embeddings of L into N, and X to be the L-embeddings of M into N. Then $\mathrm{Gal}(\mathsf{M}/Q) = (G, W)$ is a transitive imprimitive permutation group with block system $\mathfrak{B} = \{B_y \mid y \in Y\}$ with each block $B_y = \{w \in W \mid h(w) = y\}$ by Theorem 4.12. Fix $y \in Y$, and set $H = \mathrm{Stab}_G(y)$. The statement follows since $\mathrm{Gal}(\mathsf{M}/\mathsf{L}) \cong (H, X)$ and $\mathrm{Gal}(\mathsf{L}/Q) = (G, Y)$. □

As we saw in the proof of Corollary 4.14, when we embed $\mathrm{Gal}(f)$ into the wreath product $P := \mathrm{Gal}(\mathsf{M}/\mathsf{L}) \wr \mathrm{Gal}(\mathsf{L}/Q)$ as a permutation group it has the block system $\mathfrak{B} = \{B_1, \ldots, B_m\}$ defined by the embedding polynomial h. This indicates that the ordering of the roots of f must align with this block system in order for $\mathrm{Gal}(f) \leq P$ to hold. To this end, we determine the block system of the wreath product P and find the permutation $\sigma \in S_n$ that maps the block system of P to $\mathfrak{B}$. Reordering the roots of f by $\alpha_i \mapsto \alpha_{\sigma(i)}$ guarantees that $\mathrm{Gal}(f) \leq P$ as desired. For more information, see [29, Algorithm 3.2].

4.4 Resultants and Orbit Length Partitions

In his 1981 thesis [80], Leonard Soicher presented a method that computed linear resolvents without resorting to the expensive root approximations that plagued Stauduhar's work. By using resultants, Soicher was able to exactly determine linear resolvents while avoiding polynomial roots altogether.

In a later chapter, we make use of five specific absolute resolvents that can be computed from Soicher's method. Since many of the finer details are beyond the scope of this thesis, we omit them and refer the reader to Soicher's thesis. Instead, we focus on providing the reader with enough tools to compute the aforementioned resolvents themselves.

This section has been split into three subsections. In the first subsection, we define the resultant of two polynomials and describe some of the ways it can be computed. The initial definition we provide is based on the roots of the inputted polynomials. This is done to demonstrate how the resultant relates to the inputted polynomials. After this, we discuss how the resultant can be computed without polynomial roots. In the second subsection, we begin by presenting some auxiliary functions, from Soicher's thesis, that we use to compute the five absolute resolvents mentioned above. Then we give, as examples, the absolute resolvents in terms of these auxiliary functions. Finally, in the third subsection, we discuss how the factorization of resolvent polynomials can be used to determine Galois groups.

4.4.1 Resultants

Definition 4.15. Let $f(x)$ and $g(x)$ be polynomials defined over Z. If $f(x) = a(x - a_1)(x - a_2)\cdots(x - a_n)$ and $g(x) = b(x - b_1)(x - b_2)\cdots(x - b_m)$ are the factorizations of f and g in some algebraic closure of Q, then the *resultant* $\mathrm{res}(f, g)$ of f and g is

given by one of the equivalent formulations:

$$\begin{aligned}\operatorname{res}(f,g) &= a^m g(a_1)\cdots g(a_n)\\ &= (-1)^{mn} b^n f(b_1)\cdots f(b_m)\\ &= a^m b^n \prod_{1\le i\le n, 1\le j\le m} (a_i - b_j).\end{aligned}$$

Remark. Let f and g be as they are in Definition 4.15.

(1) Because $\operatorname{res}(f,g)$ is a symmetric function of the roots of f and g, it must be an element of Z.

(2) The discriminant $\operatorname{disc}(f)$ of f can be computed with a resultant:

$$\operatorname{disc}(f) = \frac{(-1)^{n(n-1)/2}\operatorname{res}(f,f')}{a}$$

where f' is the formal derivative of f.

In the event that f is a polynomial in more than one variable, computing the resultant of f and g requires choosing the variable in f that will be replaced with the roots of g. By convention, this choice of variable is made known through a subscript. For example, in the resultant

$$\operatorname{res}_y(f(x,y), g(y))$$

we use a subscript of y to indicate that the roots of g will be substituted into f for y. This yields a univariate polynomial in x.

Example 4.16. Let $f(x)$ and $g(x)$ be monic polynomials defined over Z. Let $f(x) = \prod_{i=1}^{n}(x - a_i)$, and let $g(x) = \prod_{j=1}^{m}(x - b_j)$ be the factorizations of f and g in some

algebraic closure of Q. If we evaluate g at $x - y$, we obtain a bivariate polynomial. In this context, we consider the following resultant:

$$\begin{aligned}\mathrm{res}_y(f(y), g(x-y)) &= \prod_{i=1}^{n} g(x - a_i) \\ &= \prod_{j=1}^{m}\prod_{i=1}^{n}(x - (a_i + b_j)).\end{aligned}$$

We have that $\mathrm{res}_y(f(y), g(x-y))$ is a monic polynomial in x of degree $mn = \deg(f)\deg(g)$.

The resultant of two polynomials can also be computed by finding the determinant of the corresponding Sylvester matrix. As the lemma below indicates, this computation does not require any knowledge of the roots of the two polynomials.

Lemma 4.17 ([14, Lemma 3.3.4])**.** *Let* $f, g \in Z[x]$*. If* $f(x) = \sum_{i=0}^{n} f_i x^i$ *and* $g(x) = \sum_{i=0}^{m} g_i x^i$*, then the resultant* $\mathrm{res}(f, g)$ *is equal to the determinant of the following* $(n + m) \times (n + m)$ *Sylvester matrix:*

$$\begin{bmatrix}
f_n & f_{n-1} & f_{n-2} & \cdots & f_1 & f_0 & 0 & 0 & \cdots & 0 \\
0 & f_n & f_{n-1} & f_{n-2} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\
0 & 0 & f_n & f_{n-1} & f_{n-2} & \cdots & f_1 & f_0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & f_n & f_{n-1} & f_{n-2} & \cdots & f_1 & f_0 \\
g_m & g_{m-1} & \cdots & g_2 & g_1 & g_0 & 0 & 0 & \cdots & 0 \\
0 & g_m & g_{m-1} & \cdots & g_2 & g_1 & g_0 & 0 & \cdots & 0 \\
0 & 0 & g_m & g_{m-1} & \cdots & g_2 & g_1 & g_0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & g_m & g_{m-1} & \cdots & g_2 & g_1 & g_0
\end{bmatrix}$$

where the coefficients of f are repeated on $m = \deg(g)$ rows and the coefficients of g are repeated on $n = \deg(f)$ rows.

Remark. Let f and g be polynomials in $Z[x, y]$. If we regard f and g as polynomials in y whose coefficients are in x, then $\text{res}_y(f, g)$ would be the determinant of the corresponding Sylvester matrix. In this case, the entries of the matrix would be polynomials in x.

The resultant $\text{res}_x(f, g)$ can be computed in a similar fashion.

A third, widely used method for computing the resultant of two polynomials is the Sub-Resultant Algorithm. For more information, see [14, Algorithm 3.3.7].

4.4.2 Absolute Resolvents

We begin this subsection with three auxiliary functions that Soicher used in his thesis. The first function is aptly named "Multiply Zeros ". This function takes a monic polynomial $f(x)$ over Z and an element $d \in Z$ as input and returns a monic polynomial whose roots are the roots of f multiplied by d. This new polynomial is denoted by mz and is computed as follows:

$$mz(d, f) := \begin{cases} d^n f(x/d), & \text{if } d \neq 0 \\ x^n, & \text{if } d = 0. \end{cases}$$

The second auxiliary function is named "Sum Zeros" and will be denoted by sz. This function takes as input two monic polynomials $f(x)$ and $g(x)$ defined over Z, and returns a monic polynomial of degree $\deg(f)\deg(g)$. The roots of the outputted polynomial $sz(f, g)$ are the pairwise sums of the roots of f and g. As we saw in

Example 4.16, this polynomial is equal to a resultant:

$$sz(f, g) := \mathrm{res}_y(f(y), g(x - y)).$$

Since a resultant can be computed as the determinant of the corresponding Sylvester matrix, we can compute $sz(f, g)$ without approximating roots of f and g.

The third auxiliary function is named "Poly Root" and will be denoted by pr. Given $k \in \mathbb{N}$ and a monic polynomial $u \in Z[x]$, this function computes a polynomial $r \in Z[x]$ such that $u = r^k$. In other words, pr reduces the multiplicities of the roots of u by a factor of k. In Soicher's work, this was used to ensure that the resolvent would have the correct degree.

We determine the function values $pr(k, u)$ using the following algorithm from Soicher's thesis.

Algorithm 4.18 ($pr(k, u)$ [80])**.**

Input: $u(x) \in Z[x]$ monic and $k \in \mathbb{N}$, such that $u(x) = r(x)^k$ for some unknown $r(x) \in Z[x]$.
Output: $r(x) \in Z[x]$.

(1) If $k = 1$, then return $u(x)$.

(2) $t(x) \leftarrow u(x)/\gcd(u(x), u'(x))$

(3) $r(x) \leftarrow t(x)$

$s(x) \leftarrow u(x)$

(4) Repeat until $\deg(r) < (\deg(u))/k$:

(a) $s(x) \leftarrow s(x)/t(x)^k$

(b) $t(x) \leftarrow \gcd(s, t)$

(c) $r(x) \leftarrow t(x)r(x)$

(5) Return $r(x)$.

In an effort to simplify the notation for our examples, we include a fourth function that incorporates two of the above auxiliary functions:

$$lr_2(f, a, b) := \frac{sz(mz(a, f), mz(b, f))}{mz(a + b, f)}$$

where $f \in Z[x]$ is monic and $a, b \in \mathbb{Z}$ with $a \neq b$.

Utilizing the four functions above, we now give, as examples, five absolute resolvents that can be computed for any monic $f \in Z[x]$. Since all of these resolvents are computed with resultants, no mention is made of root approximations or root ordering as it pertains to the roots of the inputted polynomial $f(x)$.

Example 4.19. Let $F(x_1, \ldots, x_n) = x_1 + x_2$. It follows that $\mathrm{Stab}_{S_n} F = S_2 \times S_{n-2}$. The corresponding resolvent $dp(f)$ has degree $n(n-1)/2$ and is of the form

$$dp(f) := R_F(S_n, f) = \prod_{1 \leq i < j \leq n} (x - \alpha_i - \alpha_j).$$

Using Soicher's work, this resolvent can be computed as

$$\begin{aligned} dp(f) &= pr(2, sz(f, f)/mz(2, f)) \\ &= \left(\frac{\mathrm{res}_y(f(y), f(x - y))}{2^n f(x/2)} \right)^{1/2}. \end{aligned}$$

Example 4.20. Let $F(x_1, \ldots, x_n) = x_1 + 2x_2$. It follows that $\mathrm{Stab}_{S_n} F = S_1 \times S_1 \times S_{n-2}$. The corresponding resolvent $rl(f) := R_F(S_n, f)$ has degree $n(n-1)$. Using

Soicher's work, this resolvent can be computed as

$$\begin{aligned} rl(f) &= lr_2(f,1,2) \\ &= \frac{\mathrm{res}_y(f(y), 2^n f(\frac{x-y}{2}))}{3^n f(x/3)}. \end{aligned}$$

Example 4.21. Let $F(x_1, \ldots x_n) = x_1 + x_2 + x_3$. It follows that $\mathrm{Stab}_{S_n} F = S_3 \times S_{n-3}$. The corresponding resolvent $tp(f) := R_F(S_n, f)$ has degree $n(n-1)(n-2)/6$. Using Soicher's work, this resolvent can be computed as

$$tp(f) = pr\left(3, \frac{sz(dp(f), f)}{lr_2(f,1,2)}\right).$$

Example 4.22. Let $F(x_1, \ldots, x_n) = x_1 + x_2 + 2x_3$. It follows that $\mathrm{Stab}_{S_n} F = S_2 \times S_1 \times S_{n-3}$. The corresponding resolvent $LR(f) := R_F(S_n, f)$ has degree $n(n-1)(n-2)/2$. Using Soicher's work, this resolvent can be computed as

$$LR(f) = \frac{sz(dp(f), mz(2, f))}{lr_2(f,1,3)}.$$

Example 4.23. Let $F(x_1, \ldots, x_n) = x_1 + x_2 + x_3 + x_4$. It follows that $\mathrm{Stab}_{S_n} F = S_4 \times S_{n-4}$. The corresponding resolvent $qp(f) := R_F(S_n, f)$ has degree $n(n-1)(n-2)(n-3)/24$. Using Soicher's work, this resolvent can be computed as

$$qp(f) = pr\left(4, \frac{sz(tp(f), f)}{LR(f)}\right).$$

4.4.3 Orbit Length Partitions

As the theorem below indicates, the list of the degrees of the irreducible factors of a resolvent polynomial $R_F(G, f)$ yields information about the Galois group $\mathrm{Gal}(f)$.

Theorem 4.24 ([80, Chapter 2])**.** *Let $f \in Z[x]$ be a monic, irreducible polynomial of degree n, and let $\alpha_1, \ldots, \alpha_n$ be an ordering of the roots of f. Suppose $H < G$ are subgroups of S_n with $r := [G : H]$ such that $\mathrm{Gal}(f) \leq G$ under the given root ordering. Let F be a G-relative H-invariant, and let $G//H$ denote a set of representatives of right cosets of G/H. Let $\tau : \mathrm{Gal}(f) \to S_r$ be the permutation representation of $\mathrm{Gal}(f)$ with respect to the action of $\mathrm{Gal}(f)$ on the set $G//H$. If the resolvent $R_F(G, f)$ is squarefree, then the Galois group of $R_F(G, f)$, as a subgroup of S_r, is isomorphic to the group $\tau(\mathrm{Gal}(f))$. In particular, the list of the degrees of the irreducible factors of $R_F(G, f)$ in $Z[x]$ is the same as the list of the orbit lengths of the action of $\tau(\mathrm{Gal}(f))$ on the set $\{1, \ldots, r\}$.*

The proof below was translated from [28] by Sandi Rudzinski.

Proof. Let $\Delta = \{H\sigma_1, \ldots, H\sigma_r\}$ be a set of right cosets of H in G with $\{\sigma_1, \ldots, \sigma_r\} = G//H$ and set $\Omega = \{F^{\sigma_1}(\alpha_1, \ldots, \alpha_n), \ldots, F^{\sigma_r}(\alpha_1, \ldots, \alpha_n)\}$. Define $\overline{\psi} : \Delta \to \Omega$ by $H\sigma_i \mapsto F^{\sigma_i}(\alpha_1, \ldots, \alpha_n)$. We want to show that $\overline{\psi}$ is a bijection of sets. To see that $\overline{\psi}$ is well-defined and injective, consider the following equivalences:

$$\begin{aligned} H\sigma_i = H\widetilde{\sigma_i} &\iff \sigma_i \widetilde{\sigma_i}^{-1} \in H \\ &\iff F^{\sigma_i \widetilde{\sigma_i}^{-1}} = F \\ &\iff F^{\sigma_i}(\alpha_1, \ldots, \alpha_n) = F^{\widetilde{\sigma_i}}(\alpha_1, \ldots, \alpha_n). \end{aligned}$$

The last line follows from $R_F(G, f)$ being squarefree.

Since $|\Delta| = |\Omega|$, we have that $\overline{\psi}$ is also surjective. Under this bijection, we have an isomorphism of permutation groups S_Δ and S_Ω, $\psi : S_\Delta \to S_\Omega$ such that $\psi(\omega)((F^{\sigma_i}(\alpha_1, \ldots, \alpha_n)) = \overline{\psi}(\omega(H\sigma_i))$. Let $\sigma \in \mathrm{Gal}(f)$. Define the permutation representation τ' of $\mathrm{Gal}(f)$ to S_Δ defined by $\tau'(\sigma)(H\sigma_i)) = H\sigma_i\sigma$ and let the homomor-

phism φ be the restriction of σ to $\mathrm{Gal}(R_F(G,f))$. We want to show that the following diagram commutes:

$$\begin{array}{ccc} & \mathrm{Gal}(f) & \\ {\scriptstyle\tau'}\swarrow & & \searrow{\scriptstyle\varphi} \\ S_\Delta \geq \tau'(\mathrm{Gal}(f)) & \xrightarrow{\quad\psi\quad} & \mathrm{Gal}(R_F(G,f)) \leq S_\Omega \end{array}$$

So

$$\varphi(\sigma)(F^{\sigma_i}(\alpha_1,\ldots,\alpha_n)) = F^{\sigma_i\sigma}(\alpha_1,\ldots,\alpha_n) \text{ for } 1 \leq i \leq r$$

and we get

$$\begin{aligned} \varphi(\sigma)(F^{\sigma_i}(\alpha_1,\ldots,\alpha_n)) &= F^{\sigma_i\sigma}(\alpha_1,\ldots,\alpha_n) \\ &= \overline{\psi}(H\sigma_i\sigma) = \overline{\psi}(\tau'(\sigma)(H\sigma_i)) \\ &= \psi(\tau'(\sigma))(F^{\sigma_i}(\alpha_1,\ldots,\alpha_n)). \end{aligned}$$

Since φ is surjective, it follows that $\mathrm{Gal}(R_F(G,f)) = \varphi(\mathrm{Gal}(f)) = \psi(\tau'(\mathrm{Gal}(f))$. Identifying Δ and Ω with $\{1,\ldots,r\}$ proves the theorem. □

Suppose we have a list of possible Galois groups of f that includes the actual group $\mathrm{Gal}(f)$. Then we can use Theorem 4.24 to rule out groups in the list. For a given pair of subgroups $H < G \leq S_n$ satisfying $\mathrm{Gal}(f) \leq G$, we follow a very simple procedure. First, for each possible Galois group we determine the list of orbit lengths for the corresponding action on $\{1,\ldots,[G:H]\}$. Second, we check to see if any of these lists differ. If such a difference exists, we factor the resolvent corresponding to $H < G$ and rule out each possible Galois group whose list of orbit lengths is different than the list of the degrees of the irreducible factors of the resolvent. If, on the other

hand, each possible Galois group has the same list of orbit lengths, then we don't compute the resolvent since its factorization could not possibly lead to a group being ruled out.

In the event that more possible Galois groups need to be ruled out, we can pick a different subgroup H of G and repeat the process.

CHAPTER V

COMPUTING GALOIS GROUPS

Let $\mathbb{Q}_p$ be the field of p-adic numbers, K a finite extension of $\mathbb{Q}_p$, $\varphi \in \mathsf{K}[x]$ Eisenstein, and α a root of φ. In this chapter, we discuss methods for finding the Galois group $\mathrm{Gal}(\mathsf{K}(\alpha)/\mathsf{K}) = \mathrm{Gal}(\varphi)$ that is the automorphism group $\mathrm{Aut}(\mathsf{N}/\mathsf{K})$ of the normal closure N of $\mathsf{K}(\alpha)/\mathsf{K}$. In the case where $\mathsf{K} = \mathbb{Q}_p$, we give a complete algorithm for computing the Galois group of φ. Many of the steps and considerations in this algorithm hold when $\mathsf{K} \neq \mathbb{Q}_p$ and thus are presented over K.

Our algorithm is a blending of the material found in the last two chapters. An essential ingredient is the tower of subfields that correspond to the ramification polygon of φ (Section 3.3). In the remainder of this chapter we will fill in the details of the following algorithm:

Algorithm 5.1 (GaloisGroup)**.**

Input: $\varphi \in \mathbb{Z}_p[x]$ Eisenstein

Output: $\mathrm{Gal}(\varphi)$

(1) $G = \{\mathrm{id}\}$.

(2) Find the tower of subfields $\mathbb{Q}_p = \mathsf{L}_{\ell+1} \subseteq \mathsf{L}_\ell \subset \mathsf{L}_{\ell-1} \subset \ldots \mathsf{L}_1 \subset \mathsf{L}_0 = \mathbb{Q}_p(\alpha)$ corresponding to the ramification polygon of φ such that the ramification polygon of $\mathsf{L}_i/\mathsf{L}_{i+1}$ $(0 \leq i \leq \ell)$ consists of one segment.

(3) For i from ℓ to 0 by -1:

(a) Determine $\mathrm{Gal}(\mathsf{L}_i/\mathsf{L}_{i+1})$ using Theorem 2.29 or Algorithm 3.23.

(b) Find a small set $\mathcal{G}$ of subgroups of $\mathrm{Gal}(\mathsf{L}_i/\mathsf{L}_{i+1}) \wr G$ that contains the Galois group of $\mathsf{L}_i/\mathbb{Q}_p$.

(c) If $\#\mathcal{G} \neq 1$ use resolvents to determine the $G \in \mathcal{G}$ that is the Galois group of $\mathsf{L}_i/\mathbb{Q}_p$.

(4) Return G.

For each relative extension $\mathsf{L}_i/\mathsf{L}_{i+1}$ in the aforementioned tower, the ramification polygon consists of one segment and the Galois group can be efficiently computed using methods from earlier chapters. In Algorithm 5.1, we take advantage of this and iteratively compute Galois groups of towers of extensions consisting of an extension whose generating polynomial has a ramification polygon consisting of one segment over an extension with a known Galois group. At each iterative stage, the Galois group of the tower is contained in the wreath product of two Galois groups. In section 5.1 we give criteria that a subgroup of the wreath product must satisfy in order to possibly be the Galois group of the tower. In section 5.2, we introduce additional criteria that the Galois group must satisfy and formulate the exact steps we take to eliminate candidate groups. We will demonstrate that these steps narrow the number of possible groups considerably. If more than one candidate group is left, we use resolvents (section 5.4) to determine the Galois group.

5.1 Tower of Two Extensions

Let α be an element in some algebraic closure of K such that the minimal polynomial of α generates a totally ramified extension of K. Let $\mathsf{K} \subset \mathsf{L}_1 \subset \mathsf{L}_0 = \mathsf{K}(\alpha)$ be a tower of field extensions. We assume that the groups $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1)$ and $\mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$

are already known and $\mathcal{R}_{\mathsf{L}_0/\mathsf{L}_1}$ consists of one segment. See Figure 5 for relevant values for this tower of extensions.

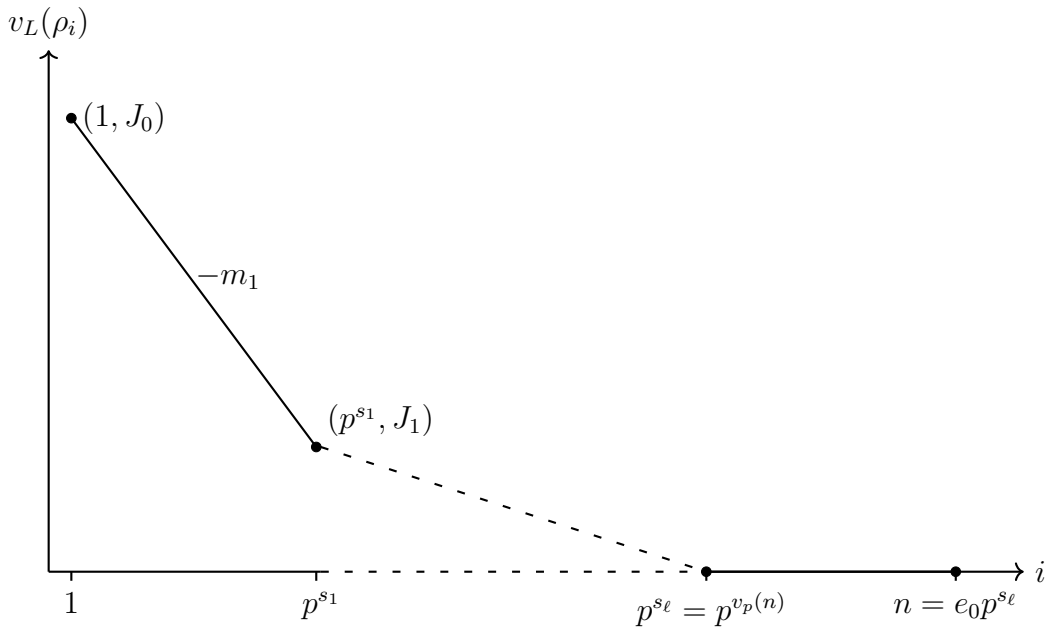

Figure 5. Ramification polygon of an Eisenstein polynomial φ of degree n with discriminant $(\pi)^{n+J_0-1}$ and ramification polynomial $\rho = \frac{\varphi(\pi x+\pi)}{\pi^n} = \sum_{i=0}^{n} \rho_i x^i$. We give the values relevant for considering the tower of extensions $\mathsf{K} \subset \mathsf{L}_1 \subset \mathsf{L}_0$, such that the ramification polygon of $\mathsf{L}_0/\mathsf{L}_1$ consists of one segment with slope $-m_1$.

In the following, we describe several criteria that have to be met for a group to be the Galois group of L_0/K. From Corollary 4.14, it must be a subgroup of $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$. Furthermore, since it is the Galois group of an irreducible polynomial, it must be transitive. Other criteria can be obtained exploring the subfield structure of the normal closure of $\mathsf{K}(\alpha)/\mathsf{K}$.

Denote by N the normal closure of L_0/K and by N_1 the normal closure of L_1/K. The maximal tamely ramified subextension of N/K is T from Theorem 3.25.

Similarly, let T_1 be the maximal tamely ramified subextension of N_1/K as determined by Theorem 3.25. Finally, with Theorem 3.25, we find the maximal tamely ramified subextension of the normal closure of $\mathsf{L}_0/\mathsf{L}_1$ and denote the tame part of this field over K by T_0. We can infer a great deal about the subfield structure of N by considering composites of the extensions we have named thus far.

From Figure 4 we have that $\mathsf{T}_1\mathsf{L}_1$ is a wildly ramified extension of T_1 of degree $[\mathsf{L}_1 : \mathsf{T}_1] = p^{s_\ell - s_1}$. As T contains T_1 and T/K is tamely ramified, the index of $\mathsf{T}\mathsf{L}_1/\mathsf{T}$ is also $p^{s_\ell - s_1}$. By construction, T_0 contains the tamely ramified subfield of L_1. Thus, $\mathsf{T}_0\mathsf{L}_1/\mathsf{T}_0$ also has index $p^{s_\ell - s_1}$.

According to Theorem 3.25 the extension $\mathsf{T}\mathsf{L}_0/\mathsf{T}\mathsf{L}_1$ is elementary abelian with degree p^{s_1} and N_1 is an extension of $\mathsf{T}_1\mathsf{L}_1$ of degree p^{w_1} for some w_1. Since N/T is a p-extension and $\mathsf{L}_1 \subset \mathsf{L}_0$, the degree of the extension $\mathsf{T}\mathsf{N}_1\mathsf{L}_0/\mathsf{T}\mathsf{L}_0$ is p^v where $v \leq w_1$. Similarly, because $\mathsf{T}\mathsf{N}_1\mathsf{L}_0/\mathsf{T}\mathsf{L}_1$ is a p-extension and its subextension $\mathsf{T}\mathsf{L}_0/\mathsf{T}\mathsf{L}_1$ is elementary abelian with degree p^{s_1}, we have that $\mathsf{T}\mathsf{N}_1\mathsf{L}_0$ is an elementary abelian extension of $\mathsf{T}\mathsf{N}_1$ with degree dividing p^{s_1}.

Using the above considerations, we obtain the subfield structure depicted in Figure 6. In this diagram, the fields $\mathsf{T}\mathsf{N}_1\mathsf{L}_0'$ are conjugates of $\mathsf{T}\mathsf{N}_1\mathsf{L}_0$ over $\mathsf{T}\mathsf{N}_1$. Furthermore, fields displayed in rectangles are explicitly known and shaded fields are normal over K. Finally, solid lines denote normal tamely ramified extensions and dashed lines normal p-extensions.

An immediate consequence of this structure is that we can enumerate the possibilities for the order of $\mathrm{Gal}(\mathsf{L}_0/\mathsf{K})$.

Proposition 5.2. *Let* T, T_1, N_1, L_0, *and* L_1 *be as they are in Figure* 6 *and* $W = \mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$. *If* $H \leq W$ *is the Galois group of* L_0/K *then* $\#H = [\mathsf{TN}_1 : \mathsf{K}] \cdot p^w$ *for some* w *satisfying* $v_p([\mathsf{TN}_1\mathsf{L}_0 : \mathsf{TN}_1]) \leq w \leq e_0 \cdot [\mathsf{N}_1 : \mathsf{T}_1] \cdot v_p([\mathsf{TN}_1\mathsf{L}_0 : \mathsf{TN}_1])$.

Proof. Let $\varphi_0 \in \mathsf{L}_1[x]$ be the generating polynomial of $\mathsf{L}_0/\mathsf{L}_1$. Since TN_1/K is normal, we obtain the normal closure of $\mathsf{TN}_1\mathsf{L}_0/\mathsf{K}$ as the composite of the conjugates of $\mathsf{TN}_1\mathsf{L}_0$ over TN_1. If $e_0 = 1$, then the polynomial $\varphi_0 \in \mathsf{L}_1[x]$ is fixed by the automorphisms of T/K. If $e_0 > 1$, then conjugation by the automorphisms of T/K yield up to e_0 distinct conjugates of φ_0. In addition to the conjugation by the automorphisms of T/K we need to consider the conjugation of φ_0 over $\mathsf{N}_1/\mathsf{T}_1\mathsf{L}_1$ and L_1/K. As $\varphi_0 \in \mathsf{L}_1[x]$, it is invariant under $\mathrm{Gal}(\mathsf{T}_1/\mathsf{K})$. Thus there are at most $[\mathsf{N}_1 : \mathsf{T}_1]$ conjugates of φ_0 by elements of $\mathrm{Gal}(\mathsf{N}_1/(\mathsf{T}_1\mathsf{L}_1))$ and elements of $\mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$. Therefore, the total number of conjugates of $\mathsf{TN}_1\mathsf{L}_0$ over TN_1 is at least 1 and at most $e_0[\mathsf{N}_1 : \mathsf{T}_1]$. □

From Galois Theory, we know that each subfield of N that contains K corresponds to a subgroup of $\mathrm{Aut}(\mathsf{N}/\mathsf{K}) = \mathrm{Gal}(\mathsf{L}_0/\mathsf{K})$. In particular, the subfields in Figure 6 are the fixed fields of subgroups of $\mathrm{Gal}(\mathsf{L}_0/\mathsf{K})$. We can, thus, use the subfield structure of N that we know to predict part of the subgroup lattice of $\mathrm{Gal}(\mathsf{L}_0/\mathsf{K})$. The first step is to name some of the subgroups.

We let B, B_1, C, D_0, and D_1 be the subgroups of $\mathrm{Gal}(\mathsf{L}_0/\mathsf{K})$ that satisfy $\mathsf{T} = \mathrm{Fix}(B)$, $\mathsf{T}_1 = \mathrm{Fix}(B_1)$, $\mathsf{N}_1 = \mathrm{Fix}(C)$, $\mathsf{T}_0\mathsf{L}_0 = \mathrm{Fix}(D_0)$, and $\mathsf{L}_1 = \mathrm{Fix}(D_1)$. Since many of the subfields of N can be formed from composites of the fixed fields we just mentioned, we can use part(2) of Theorem A.17 to determine which groups correspond to these composites. For example, because $\mathsf{T} = \mathrm{Fix}(B)$, and $\mathsf{L}_1 = \mathrm{Fix}(D_1)$, we have that $\mathsf{TL}_1 = \mathrm{Fix}(B \cap D_1)$. The subgroups identified are listed alongside their fixed fields in Figure 6.

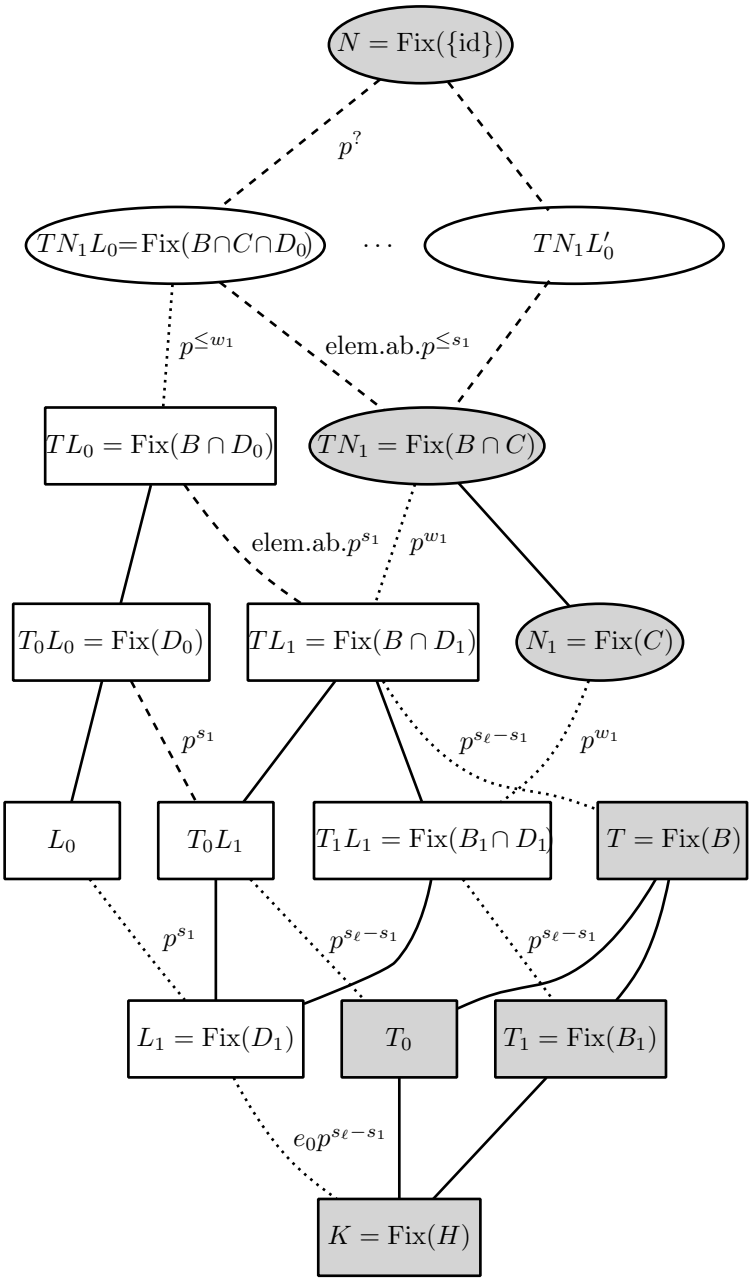

Figure 6. (Incomplete) subfield lattice of the normal closure N of L_0/K.

In Figure 6, some of the attributes of the subextensions of N/K are identified. These attributes include extension degree, normality, and/or whether an extension is elementary abelian. By Theorem A.17, we can utilize many of these characteristics to determine traits of the identified subgroups of $\mathrm{Gal}(\mathsf{L}_0/\mathsf{K})$ (see again Figure 6). This additional subgroup information, in turn, enables us to define additional criteria that the Galois group must satisfy.

Proposition 5.3. *Let* T, T_0, T_1, N_1, L_0, *and* L_1 *be as they are in Figure* 6 *and* $G = \mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$. *If* $H \leq G$ *is the Galois group of* L_0/K *then then there are subgroups* B_1, B, C, D_1, D_0 *of* H *such that*

(1) $B_1 \trianglelefteq H$ *with* $H/B_1 \cong \mathrm{Gal}(\mathsf{T}_1/\mathsf{K})$,

(2) $B \trianglelefteq H$ *with* $B \trianglelefteq B_1$ *and* $H/B \cong \mathrm{Gal}(\mathsf{T}/\mathsf{K})$,

(3) $C \trianglelefteq H$ *with* $C \leq B_1$ *and* $H/C \cong \mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$,

(4) $C/(B \cap C) \cong \mathrm{Gal}(\mathsf{T}/\mathsf{T}_1)$,

(5) $D_1 < H$ *with* $[H : D_1] = [\mathsf{L}_1 : \mathsf{K}]$,

(6) $D_1/(B_1 \cap D_1) \cong \mathrm{Gal}(\mathsf{T}_1/\mathsf{K})$ *and* $(B_1 \cap D_1)/(B \cap D_1) \cong \mathrm{Gal}(\mathsf{T}/\mathsf{T}_1)$,

(7) $D_0 \trianglelefteq D_1$ *with* $D_1/D_0 \cong \mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) = \mathrm{Aut}(\mathsf{T}_0\mathsf{L}_0/\mathsf{L}_1)$,

(8) $(B \cap D_1)/(B \cap D_0) \cong (\mathbb{Z}/p\mathbb{Z})^{s_1}$,

(9) $(B \cap C)/(B \cap C \cap D_0)$ *is an elementary abelian* p*-group of order at most* p^{s_1}.

Proof. (1) to (7) and (9) follow from Figure 6 and Galois theory (Theorem A.17). (8) is a consequence of Theorem 3.25(b). □

Remark. Since T/K and T_1/K are normal, tamely ramified extensions by Theorem 3.25, the Galois groups $\mathrm{Gal}(\mathsf{T}/\mathsf{K})$ and $\mathrm{Gal}(\mathsf{T}_1/\mathsf{K})$ can be computed using Theorem 2.28.

5.2 Candidates for Galois Groups

Let $\varphi \in \mathcal{O}_\mathsf{K}[x]$ be irreducible with degree n, and let α be a root of φ in some algebraic closure of K. We can obtain criteria that the Galois group $\mathrm{Gal}(\varphi)$ must meet by computing invariants of φ and the extension it generates. First, as the degree of $\mathsf{K}(\alpha)$ is relatively small and root finding in local fields is efficient [66], we can efficiently compute the automorphism group of $\mathsf{K}(\alpha)/\mathsf{K}$ and use the following theorem.

Theorem 5.4 ([2, Theorem 3.6])**.** *Let $\varphi \in \mathcal{O}_\mathsf{K}[x]$ be irreducible of degree n and α a root of φ in some algebraic closure of K. Let $\mathsf{L} = \mathsf{K}(\alpha)$ and $G = \mathrm{Gal}(\varphi)$. Then $\mathrm{Aut}(\mathsf{L}/\mathsf{K}) \cong \mathrm{Cen}_{S_n}(G)$, where $\mathrm{Cen}_{S_n}(G)$ is the centralizer of G in S_n.*

In Example 4.10, we saw that for an irreducible polynomial f with coefficients in an integral domain Z the Galois group of f is a subgroup of the Alternating group on $\deg(f)$ elements if and only if $\sqrt{\mathrm{disc}\,(f)} \in Z$. Since $\mathcal{O}_\mathsf{K}$ is an integral domain, we can apply this result to irreducible polynomials with coefficients in $\mathcal{O}_\mathsf{K}$. Thus we have that

$$\mathrm{Gal}(\varphi) \leq A_n \quad \Longleftrightarrow \quad \sqrt{\mathrm{disc}\,(\varphi)} \in \mathcal{O}_\mathsf{K}. \tag{5.1}$$

For subgroups $G \leq S_n$, we define the *parity* of G to be $+1$ if $G \leq A_n$ and -1 otherwise. Likewise, the *parity* of a polynomial defined over $\mathcal{O}_\mathsf{K}$ is $+1$ if its discriminant is a square in $\mathcal{O}_\mathsf{K}$ and -1 otherwise. In this context, we can rephrase the statement (5.1): the parity of $\mathrm{Gal}(\varphi)$ must be the same as the parity of φ.

Although $\mathrm{Aut}(\mathsf{K}(\alpha)/\mathsf{K})$ and $\mathrm{disc}\,(\varphi)$ provide useful information about $\mathrm{Gal}(\varphi)$, it is rare that they alone can be used to determine the Galois group. More information is needed. With this in mind, we widen our scope by considering the subfield structure of the stem field $\mathsf{K}[x]/(\varphi)$. As subfields corresponding to the segments of the ramification polygon of an Eisenstein polynomial are easily obtained (see Section 3.3), in the following we restrict ourselves to the case where φ is Eisenstein and generates the tower of extensions $\mathsf{K} \subset \mathsf{L}_1 \subset \mathsf{L}_0 = \mathsf{K}(\alpha)$ where $\mathcal{R}_{\mathsf{L}_0/\mathsf{L}_1}$ consists of one segment. Again, the relevant values for this tower are provided in Figure 5. We also assume that the groups $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1)$ and $\mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$ are already known.

Under these circumstances, our approach to finding $\mathrm{Gal}(\varphi)$ is straightforward: determine a collection of groups that must contain $\mathrm{Gal}(\varphi)$ and, then, systematically rule out the other groups. To this end, we merge the critiera from the last section with those that we have established in this section.

As previously discussed, the Galois group must be a transitive subgroup of $W := \mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$. Thus, we begin by determining all of the transitive subgroups of W, up to conjugation in W. These subgroups are then organized by their conjugacy class in S_n. Next, we form our pool of candidate groups by taking one subgroup from each S_n conjugacy class. All subgroup calculations are performed using an algorithm in [11], which has been implemented in the Computer algebra system Magma.

In order to rule out candidate groups that aren't $\mathrm{Gal}(\varphi)$, we gradually apply our list of criteria to each candidate. Once a candidate group fails to meet one of the criteria, it is permanently disregarded. The order in which the criteria are applied has been largely dictated by both how expensive the computations for a given criterion are

and the perceived likelihood that several candidates will fail to satisfy the criterion. The exact order is given in the algorithm below. In practice, each criterion is applied to all of the remaining candidates at once.

Algorithm 5.5 (CheckGroup)**.**

Input: $\varphi \in \mathsf{K}[x]$ Eisenstein with $\mathsf{K}[x]/(\varphi) \cong \mathsf{L}_0 \supset \mathsf{L}_1 \supset \mathsf{K}$ such that $\mathcal{R}_{\mathsf{L}_0/\mathsf{L}_1}$ consists of one segment and $H \leq S_{\deg(\varphi)}$.

Output: "Yes" if H might be $\mathrm{Gal}(\varphi)$; "No" otherwise.

Let $\mathsf{N}_1, \mathsf{T}_1$, and T be as they are in Figure 6 and assume that $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1)$ and $\mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$ are known. Let $n = \deg(\varphi)$.

(1) Return "No" if H is not a transitive subgroup of $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$.

(2) Return "No" if the order of H does not lie in the range indicated by Proposition 5.2.

(3) Return "No" if the parity of H differs from the parity of φ.

(4) If $\mathrm{Aut}(\mathsf{L}_0/\mathsf{K}) \ncong \mathrm{Cen}_{S_n}(H)$, then return "No".

(5) Return "No" if there do not exist normal subgroups B and B_1 of H satisfying

   (a) $H/B \cong \mathrm{Gal}(\mathsf{T}/\mathsf{K})$,

   (b) $H/B_1 \cong \mathrm{Gal}(\mathsf{T}_1/\mathsf{K})$,

   (c) $B \trianglelefteq B_1$,

   (d) B is a p-group.

(6) Return "No" if for all B_1 satisfying (5b) there does not exist a normal subgroup C of H satisfying

(a) $C \leq B_1$,

(b) $H/C \cong \mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$.

(7) Return "No" if for all possible combinations of B_1, B, and C satisfying (5a), (5b), (5c), (5d), (6a), and (6b) the following isn't true: $C/(B \cap C) \cong B_1/B \cong \mathrm{Gal}(\mathsf{T}/\mathsf{T}_1)$,

(8) Return "No" if there do not exist subgroups $D_0 \trianglelefteq D_1$ of H satisfying

(a) $[H : D_1] = [\mathsf{L}_1 : \mathsf{K}]$,

(b) $D_1/D_0 \cong \mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1)$.

(9) Return "No" if for all possible combinations of B, C, D_1, and D_0 satisfying (5a), (5d), (6a), (6b), (7), (8a), and (8b) at least one of the following fails to hold:

(a) $(B \cap D_1)/(B \cap D_0) \cong C_p^{s_1}$,

(b) $(B \cap C)/(B \cap C \cap D_0)$ is elementary abelian with order at most p^{s_1}.

Return "Yes".

Remark. The correctness of Steps (5) through (9), in the preceding algorithm, follows from Proposition 5.3.

To illustrate the effectiveness of our method in eliminating candidate groups, we give some examples. In each example, we use a table to display the changes in the total number of viable candidates. This table will be comprised of two rows. The first row contains the step numbers in Algorithm 5.5 and the second row contains the number of candidates that remain after each step. For instance, if the table contains a column

(6)
31

then there are 31 candidates remaining after step (6).

At the end of each example, we reveal the remaining candidate groups. Each of these groups is named using the transitive group notation that was first developed in [15] and is used in the Computer algebra systems GAP and Magma.

Example 5.6. Let $\varphi = x^{18} + 12x + 6 \in \mathbb{Q}_3[x]$. The ramification polygon $\mathcal{R}_\varphi$ is comprised of two segments with endpoints at $(1,1)$, $(9,0)$, and $(18,0)$. From left to right the segments of $\mathcal{R}_\varphi$ have slopes $-1/8$, 0, and residual polynomials $2y+1, y^9+2 \in \mathbb{F}_3[y]$. Using Algorithm 3.13, we compute the tower of extensions corresponding to the segments of $\mathcal{R}_\varphi$:

$$\mathbb{Q}_3 \subset \mathsf{L}_1 \subset \mathsf{L}_0 \cong \mathbb{Q}_3[x]/(\varphi)$$

where

$$\mathsf{L}_1 \cong \mathbb{Q}_3[x]/(x^2 + 12x + 6)$$

and

$$\mathsf{L}_0 \cong \mathsf{L}_1[x]/(x^9 + 2\beta x^5 + 2\beta x^4 + 2\beta x^3 + \beta x^2 + \beta x + \beta)$$

with $\beta^2 + 12\beta + 6 = 0$. We next compute the Galois groups of the relative extensions in the tower above. As $\mathsf{L}_1/\mathbb{Q}_3$ is quadratic, $\mathrm{Gal}(\mathsf{L}_1/\mathbb{Q}_3) \cong S_2$. Since $\mathcal{R}_{\mathsf{L}_0/\mathsf{L}_1}$ consists of 1 non-horizontal segment, we use Algorithm 3.23 and obtain $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \cong 9T19$.

By Corollary 4.14, $\mathrm{Gal}(\varphi)$ is a subgroup of the wreath product

$$\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathbb{Q}_3) \cong (9T19) \wr S_2.$$

After computing an initial list of candidate subgroups, we apply the decisions steps from Algorithm 5.5 to all of the candidate groups. We observe the following changes in the total number of viable candidates:

Step	(1)	(2)	(3)	(4)	(5)
Remaining Candidates	119	29	24	24	1

After 5 steps, we are left with $\mathrm{Gal}(\varphi) \cong 18T476$.

Example 5.7. Let $\varphi = x^{16}+16x^{15}+6x^{14}+12x^{13}+8x^{11}+24x^{10}+8x^8+24x^6+16x^5+8x^4+16x^3+20x^2+24x+10 \in \mathbb{Q}_2[x]$. The ramification polygon $\mathcal{R}_\varphi$ is comprised of two segments with endpoints at $(1,29)$, $(2,14)$, $(16,0)$. From left to right the segments of $\mathcal{R}_\varphi$ have slopes -15, -1, and residual polynomials $y+1$, $y^{14}+1 \in \mathbb{F}_2[y]$. Using Algorithm 3.13, we compute the tower of extensions corresponding to the segments of $\mathcal{R}_\varphi$:

$$\mathbb{Q}_2 \subset \mathsf{L}_1 \subset \mathsf{L}_0 \cong \mathbb{Q}_2[x]/(\varphi)$$

where $\mathsf{L}_1/\mathbb{Q}_2$ is generated by

$$x^8 + 10x^7 + 8x^6 + 56x^5 + 8x^4 + 40x^3 + 40x^2 + 12x + 10$$

and

$$\mathsf{L}_0 \cong \mathsf{L}_1[x]/(x^2 + (6\beta^7 + 4\beta + 6)x + \beta)$$

such that β satisfies $\mathsf{L}_1 = \mathbb{Q}_2(\beta)$. It follows that $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \cong S_2$. Additionally, since $\mathcal{R}_{\mathsf{L}_1/\mathbb{Q}_2}$ consists of one segment, we obtain from Algorithm 3.23 that $\mathrm{Gal}(\mathsf{L}_1/\mathbb{Q}_2) \cong 8T13 \cong A_4 \times S_2$.

By Corollary 4.14, $\mathrm{Gal}(\varphi)$ is a subgroup of the wreath product

$$\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathbb{Q}_2) \cong S_2 \wr (A_4 \times S_2).$$

After computing an initial list of candidate groups, we apply the decisions steps from Algorithm 5.5 to all of the candidate groups. We observe the following changes in the total number of viable candidates:

Step	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Remaining Candidates	60	23	21	5	5	5	5	5	5

After 9 steps, we are left with the following 5 candidate groups: $16T424$, $16T427$, $16T722$, $16T58$, $16T59$.

In the case that $\mathsf{K} = \mathbb{Q}_p$, we also determine the Galois group $\widetilde{H}$ of φ over $\mathbb{Q}$. This is done with an algorithm devised by Claus Fieker and Jürgen Klüners (see, [24]). This algorithm is a degree-independent, relative resolvent algorithm that builds upon Stauduhar's method [82] by incorporating subfield information and computing the necessary invariant polynomials $F \in \mathbb{Z}[x_1, \ldots, x_n]$ on the fly. An implementation of this algorithm can be found in current versions of the Computer algebra system Magma.

Since $H := \mathrm{Gal}(\mathbb{Q}_p(\alpha)/\mathbb{Q}_p)$ is the decomposition group of $\widetilde{H}$ at the prime p, it follows that $H \leq \widetilde{H}$. Thus, for this case, we add the following step to Algorithm 5.5:

(10) Return "No" if H is not isomorphic to a subgroup of $\mathrm{Gal}(\mathsf{F}/\mathbb{Q})$, where $\mathsf{F} := \mathbb{Q}[x]/(\varphi)$.

Instead of checking all subgroups of $\widetilde{H}$ for isomorphism, we check some basic properties that would occur if such an isomorphism existed. To this end, we compute some basic group-theoretic invariants. Specifically, we try to verify the following:

- The order of H divides the order of $\widetilde{H}$.
- The exponent of H divides the exponent of $\widetilde{H}$.
- If $\widetilde{H}$ is abelian, then H is abelian.
- If $\widetilde{H}$ is cyclic, then H is cyclic.

All four of these checks, taken together, constitute the tenth step in Algorithm 5.5. This choice of step numbering is reflected in the table for the following example.

Example 5.8. Let $\varphi = x^{14} + 2 \in \mathbb{Q}_2[x]$. The ramification polygon $\mathcal{R}_\varphi$ is comprised of two segments with endpoints $(1, 14)$, $(2, 0)$, and $(14, 0)$. From left to right, the segments of $\mathcal{R}_\varphi$ have slopes -14, 0, and residual polynomials $y + 1$, $y^{12} + y^{10} + y^8 + y^6 + y^4 + y^2 + 1 \in \mathbb{F}_2[y]$. Using Algorithm 3.13, we compute the tower of extensions corresponding to the segments of $\mathcal{R}_\varphi$:

$$\mathbb{Q}_2 \subset \mathsf{L}_1 \subset \mathsf{L}_0 \cong \mathbb{Q}_2[x]/(\varphi)$$

where $\mathsf{L}_1 \cong \mathbb{Q}_2[x]/(x^7 + 6)$ and $\mathsf{L}_0 \cong \mathsf{L}_1[x]/(x^2 + 5\beta)$ for β satisfying $\beta^7 + 6 = 0$. It follows that $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \cong S_2$. Additionally, since $\mathcal{R}_{\mathsf{L}_1/\mathbb{Q}_2}$ is comprised of a single non-horizontal segment, we obtain from Algorithm 3.23 that $\mathrm{Gal}(\mathsf{L}_1/\mathbb{Q}_2) \cong 7T3$.

By Corollary 4.14, $\mathrm{Gal}(\varphi)$ is a subgroup of the wreath product

$$\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathbb{Q}_2) \cong S_2 \wr (7T3).$$

After computing an initial list of candidate subgroups, we apply the decision steps from Algorithm 5.5 to all of the candidate groups. We observe the following changes in the total number of viable candidates:

Step	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Remaining Candidates	10	5	3	3	3	3	3	3	3	1

After 10 steps, we are left with $\mathrm{Gal}(\varphi) \cong 14T5$.

5.3 Invariants Approach

The methodology presented in the last two sections can be succinctly summarized as taking an Eisenstein polynomial $\varphi \in \mathcal{O}_{\mathsf{K}}[x]$ and computing enough invariants to either determine $\mathrm{Gal}(\varphi)$ or find a small collection of groups containing $\mathrm{Gal}(\varphi)$. In this section, we turn this process on its head. Instead of starting with an Eisenstein polynomial, we assume that we are only given some of the invariants of the extension generated by the polynomial. The purpose of this exercise is to explore the extent to and effectiveness with which the aforementioned methodology can be used without access to a concrete polynomial.

We begin this exploration by discussing/motivating the invariants we will be given. Assume L/K is totally ramified and generated by an unknown polynomial φ. As we noted in Section 3.6, if L/K is wildly ramified and $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ consists of one segment then $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ and its residual polynomial provide enough information to find $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$. If, instead, $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ consists of two or more segments, then we settle for finding the maximal tamely ramified subextension T of the normal closure. From Theorem 3.25, we find that T can be computed using the following information: the ramification polygon $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$, the residual polynomials, and the constant term φ_0 of the unknown polynomial φ. These will be the first three given invariants.

Remark. If L/K is tamely ramified then $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$ can be determined from the constant term φ_0, the degree of the extension and Theorem 2.29.

Recently, an algorithm was created to give generating polynomials for all of the totally ramified extensions of a certain degree over some base field K [68]. This was accomplished, in large part, by developing a means to compute all of the possible ramification polygons for the given degree and then compute all possible sets of residual polynomials for each ramification polygon found. In our examples we use this process to determine the possible combinations of ramification polygons and residual polynomials that we can be given. For more information see [68] or [79].

5.3.1 Constant Terms

If the degree of the extension L/K is a power of p, then for any choice of $\varphi_0 \pmod{\pi_{\mathsf{K}}^2}$ we can find a generating polynomial φ of L/K. Otherwise, $\varphi_0 \pmod{\pi_{\mathsf{K}}^2}$ specifies the maximal tamely ramified subextension of L (see Proposition 2.26). In order to determine the values of $\varphi_0 \pmod{\pi_{\mathsf{K}}^2}$ that give us isomorphic extensions, we investigate what is required for two Eisenstein polynomials of the same degree to generate the same tamely ramified extension. Let $\psi(x) = x^{e_0} - \delta\pi_{\mathsf{K}}$, and let $\widetilde{\psi}(x) = x^{e_0} - \widetilde{\delta}\pi_{\mathsf{K}}$ where $v(\delta) = v(\widetilde{\delta}) = 0$ and $p \nmid e_0$. Then $\mathsf{K}[x]/(\psi)$ is isomorphic to $\mathsf{K}[x]/(\widetilde{\psi})$ whenever $\delta = \gamma^{e_0}\widetilde{\delta}$ for some γ satisfying $v(\gamma) = 0$. In short, $\psi(x)$ and $\widetilde{\psi}(x)$ generate the same extension when their constant terms differ by the e_0-th power of a unit.

All elements of $\underline{\mathsf{K}}^\times$ that differ by the e_0-th power of some element are in the same class of $(\underline{\mathsf{K}}^\times)^{e_0}$. We can, thus, avoid the repetition of elements of the form $\delta\pi_{\mathsf{K}}$ by requiring δ to be a lift of a representative $\underline{\delta}$ of a class in $\underline{\mathsf{K}}^\times/(\underline{\mathsf{K}}^\times)^{e_0}$. For more information, see, for example, [68, Lemma 4.10]. In general, if φ has degree e_0p^m,

then each aforementioned δ yields a possible value for $\varphi_0 \pmod{\pi_{\mathsf{K}}^2}$:

$$\varphi_0 \equiv \delta\pi_{\mathsf{K}} \bmod \pi_{\mathsf{K}}^2.$$

Thus, $\underline{\delta}$'s chosen from the same class in $\underline{\mathsf{K}}^\times/(\underline{\mathsf{K}}^\times)^{e_0}$ yield isomorphic extensions, whereas $\underline{\delta}$'s chosen from different classes yield non-isomorphic extensions.

5.3.2 Ramification Polygons and Residual Polynomials of Subfields

Assume that $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$, the corresponding residual polynomials, and the constant term φ_0 are given. If $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ consists of one segment, then these invariants provide us with enough information to compute $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$. Thus, for the remainder of this section, we assume that $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ has at least two segments. This implies that there exists a subfield L_1 of L such that $\mathsf{K} \subset \mathsf{L}_1 \subset \mathsf{L}$ and $\mathcal{R}_{\mathsf{L}/\mathsf{L}_1}$ consists of one segment.

As we noted in our comments following Lemma 3.14, we can determine the ramification polygon $\mathcal{R}_{\mathsf{L}_1/\mathsf{K}}$ of L_1/K from $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$. In addition, Lemma 3.14 tells us the following information about each residual polynomial corresponding to a segment of $\mathcal{R}_{\mathsf{L}_1/\mathsf{K}}$: the segmental inertia degree and a root for each root of the residual polynomial for the corresponding segment of $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$. This is enough information to compute, via Theorem 3.25, the maximal tamely ramified subextension T_1 of the normal closure of L_1/K.

By Theorem 3.15, we can determine the slope of $\mathcal{R}_{\mathsf{L}/\mathsf{L}_1}$ and both the roots and segmental inertia degree of the corresponding residual polynomial. This enables us to compute $\mathrm{Gal}(\mathsf{L}/\mathsf{L}_1)$.

Set $\mathsf{L}_0 := \mathsf{L}$ and assume that $\mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$ is known. We can compute an initial list of candidate groups containing $\mathrm{Gal}(\mathsf{L}/\mathsf{K}) = \mathrm{Gal}(\mathsf{L}_0/\mathsf{K})$ by computing transitive subgroups of $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$ (see Section 5.2). Then our knowledge of T_1, T,

$\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1)$, and $\mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$ allow us to reduce the number of candidates by utilizing steps (1), (2), and (5) through (9) of Algorithm 5.5.

When pruning a list of possible Galois groups for a concrete polynomial, we also make use of the automorphism group $\mathrm{Aut}(\mathsf{L}/\mathsf{K})$ and the parity of the polynomial. In the next subsection, we investigate which values these invariants can have given $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ and the corresponding residual polynomials. Ultimately, we include $\mathrm{Aut}(\mathsf{L}/\mathsf{K})$ and the parity of φ in our list of given invariants.

5.3.3 Parity and Automorphism Group Orders

In some cases, the ramification polygon $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ can be used to determine the parity of our unknown polynomial φ. Let $(1, J_0)$ denote the leftmost point on $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$. Then we have that

$$v_{\mathsf{K}}(\mathrm{disc}\,(\varphi)) = J_0 - 1 + [\mathsf{L} : \mathsf{K}].$$

If this number is odd, then it is impossible for $\mathrm{disc}\,(\varphi)$ to be a perfect square. As such, the parity of φ would be -1. If, on the other hand, $v_{\mathsf{K}}(\mathrm{disc}\,(\varphi))$ is even, then we lack the ability to conclusively say what the parity of φ is since even valuation of $\mathrm{disc}\,(\varphi)$ does not imply that $\mathrm{disc}\,(\varphi)$ is a perfect square in general.

In general, without a concrete polynomial φ, we cannot say much about the structure of the automorphism group $\mathrm{Aut}(\mathsf{L}/\mathsf{K})$. The best we can do, with the information given, is determine a few characteristics of the group. First, we observe that $\mathrm{Aut}(\mathsf{L}/\mathsf{K})$ acts transitively on those roots of φ that are contained in L, as any of those roots can be mapped to any other of those roots. Second, since $\mathrm{Aut}(\mathsf{L}/\mathsf{K}) \leq \mathrm{Gal}(\mathsf{L}/\mathsf{K})$ and $\mathrm{Gal}(\mathsf{L}/\mathsf{K})$ is solvable by Proposition 2.32, we have that $\mathrm{Aut}(\mathsf{L}/\mathsf{K})$ is solvable.

Third, we can use $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ and the residual polynomials to enumerate the possibilities for the order of $\mathrm{Aut}(\mathsf{L}/\mathsf{K})$.

Let $\rho \in \mathcal{O}_{\mathsf{L}}[x]$ denote the ramification polynomial of φ. By construction, the number of roots of ρ that lie in L equals the number of roots of φ that lie in L. Since this number is $|\mathrm{Aut}(\mathsf{L}/\mathsf{K})|$, we can reduce the task of enumerating the possible values of $|\mathrm{Aut}(\mathsf{L}/\mathsf{K})|$ to estimating how many roots of ρ can lie in L.

Since x is a factor of $\rho(x)$, by construction, we know that ρ has a root in L. To investigate the other factors of ρ, we look at the segments of $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$.

Let $\mathcal{S}$ be a segment of $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ with slope $-\lambda$, and let $g \in \mathsf{L}[x]$ denote the corresponding factor of ρ. If $\lambda \notin \mathbb{Z}$, then the roots of g have non-integer valuation and, thus, cannot lie in L. If, on the other hand, $\lambda \in \mathbb{Z}$, then it is possible that one or more roots of g lie in L.

In the event that the slope of $\mathcal{S}$ is integral, we examine the residual polynomial $\underline{A} \in \underline{\mathsf{L}}[y]$ that corresponds to $\mathcal{S}$. More specifically, since $\underline{A}$ gives the first coefficient in the π_{L}-adic expansion of the roots of g, we look at the roots of $\underline{A}$. If the multiplicity of a root of $\underline{A}$ is 1, then we can lift to a root of ρ in L by Hensel's Lemma. If, on the other hand, a root of $\underline{A}$ has multiplicity $m > 1$, then we can only lift to a factor of ρ of degree m. In the latter case, the factor of ρ that we would obtain from lifting could have anywhere between 0 and m (inclusive) roots in L.

By considering every segment of $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ that has integral slope, we can obtain a list of the possible values for the total number of roots of ρ that lie in L. This list of possible values of $|\mathrm{Aut}(\mathsf{L}/\mathsf{K})|$ can be further restricted by the fact that $|\mathrm{Aut}(\mathsf{L}/\mathsf{K})|$ must divide $[\mathsf{L} : \mathsf{K}]$. For a more succinct description of this approach, see the algorithm below.

Algorithm 5.9 (AutomorphismGroupOrders)**.**

Input: The ramification polygon $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$ of L/K, and the list of residual polynomials of $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$.

Output: The possible orders of $\mathrm{Aut}(\mathsf{L}/\mathsf{K})$.

Let $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_{\ell+1}$ be the segments of $\mathcal{R}_{\mathsf{L}/\mathsf{K}}$.

(1) count $\leftarrow \{1\}$.

(2) For each segment $\mathcal{S}_i$ with integral slope and residual polynomial $\underline{A}_i$:

  (a) Set $T := \{(\underline{r}, m) \mid \underline{r}$ is a root of $\underline{A}_i$ of multiplicity $m\}$.

  (b) For $(\underline{r}, m)$ in T:

    (i) If $m = 1$, count $\leftarrow \{a + 1 \mid a$ in count$\}$.

    (ii) Otherwise, count $\leftarrow \{a + b \mid a$ in count, $0 \leq b \leq m\}$.

(3) Return $\{c \in$ count $\mid c$ divides $[\mathsf{L} : \mathsf{K}]\}$.

The fourth characteristic of $\mathrm{Aut}(\mathsf{L}/\mathsf{K})$ that we can determine/state is that $\mathrm{Aut}(\mathsf{L}/\mathsf{K}) \leq S_{|\mathrm{Aut}(\mathsf{L}/\mathsf{K})|}$. Putting all of this together, we can quickly determine a list of possible values for $\mathrm{Aut}(\mathsf{L}/\mathsf{K})$.

5.3.4 Examples

In order to test the effectiveness with which our given invariants of a totally ramified extension can narrow the pool of candidates for the extension's Galois group, we have generated a number of tables that will appear on my personal website in the near future. When constructing these tables, we began by picking a field of p-adic number $\mathbb{Q}_p$ and a degree n satisfying $p \mid n$. Then we used the methods and criteria

described in the preceding subsections to determine every plausible combination of invariants that could be given to describe a degree n totally ramified extension of $\mathbb{Q}_p$.

We have opted to display these tables online due to the number of rows required to describe every combination of invariants that we determined.

5.4 Eliminating Candidate Groups with Resolvents

Let $\varphi \in \mathcal{O}_{\mathsf{K}}[x]$ be Eisenstein with degree n, and let α be a root of φ in some algebraic closure of K. Assume that φ generates a tower of field extensions $\mathsf{K} \subset \mathsf{L}_1 \subset \mathsf{L}_0 = \mathsf{K}(\alpha)$ where $\mathcal{R}_{\mathsf{L}_0/\mathsf{L}_1}$ consists of one segment and both $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1)$ and $\mathrm{Gal}(\mathsf{L}_1/\mathsf{K})$ are known. We also assume that we have a list of candidate groups that includes $\mathrm{Gal}(\varphi) = \mathrm{Gal}(\mathsf{L}_0/\mathsf{K})$.

We can eliminate candidate groups that aren't $\mathrm{Gal}(\varphi)$ by using Theorem 4.24 with the five absolute resolvents from Examples 4.19 through 4.23. For a candidate group H, we add the following steps to Algorithm 5.5:

(R1) Return "No" if the list of the degrees of the irreducible factors of $dp(\varphi)$ from Example 4.19 over $\mathcal{O}_{\mathsf{K}}[x]$ is **not** the same as the list of the orbit lengths of the action of $\tau_1(H)$ on $\{1, \ldots, n(n-1)/2\}$ where τ_1 is the permutation representation of H acting on the cosets $S_n/(S_2 \times S_{n-2})$.

(R2) Return "No" if the list of the degrees of the irreducible factors of $rl(\varphi)$ from Example 4.20 over $\mathcal{O}_{\mathsf{K}}[x]$ is **not** the same as the list of the orbit lengths of the action of $\tau_2(H)$ on $\{1, \ldots, n(n-1)\}$ where τ_2 is the permutation representation of H acting on the cosets $S_n/(S_1 \times S_1 \times S_{n-2})$.

(R3) Return "No" if the list of the degrees of the irreducible factors of $tp(\varphi)$ from Example 4.21 over $\mathcal{O}_{\mathsf{K}}[x]$ is **not** the same as the list of the orbit lengths of

the action of $\tau_3(H)$ on $\{1, \ldots, n(n-1)(n-2)/6\}$ where τ_3 is the permutation representation of H acting on the cosets $S_n/(S_3 \times S_{n-3})$.

(R4) Return "No" if the list of the degrees of the irreducible factors of $LR(\varphi)$ from Example 4.22 over $\mathcal{O}_{\mathsf{K}}[x]$ is **not** the same as the list of the orbit lengths of the action of $\tau_4(H)$ on $\{1, \ldots, n(n-1)(n-2)/2\}$ where τ_4 is the permutation representation of H acting on the cosets $S_n/(S_2 \times S_1 \times S_{n-3})$.

(R5) Return "No" if the list of the degrees of the irreducible factors of $qp(\varphi)$ from Example 4.23 over $\mathcal{O}_{\mathsf{K}}[x]$ is **not** the same as the list of the orbit lengths of the action of $\tau_5(H)$ on $\{1, \ldots, n(n-1)(n-2)(n-3)/24\}$ where τ_5 is the permutation representation of H acting on the cosets $S_n/(S_4 \times S_{n-4})$.

As we stipulated in our comments following Theorem 4.24, we don't compute one of the aforementioned absolute resolvents unless we are certain that we will be able to eliminate at least one candidate group. The reader may recall that this involves first computing the orbit length list for each candidate, and then comparing these lists in search of any discrepancies. Additionally, we decline to compute one of these resolvents if we anticipate its degree being large. Thus, for large degree the latter steps above may be skipped.

In the examples below, we continue the practice from Section 5.2 of using a table to track the changes in the total number of viable candidates. The degrees of the irreducible factors of each resolvent polynomial over $\mathcal{O}_{\mathsf{K}}[x]$ are efficiently obtained with an OM-algorithm, see for example [36]. Since we do not need to derive a complete factorization, the lifting step described in [38] is omitted. In the case where $\mathsf{K} = \mathbb{Q}_p$, we use the OM algorithm from the Ideals+ package for Magma [34].

Example 5.10. Let $\varphi = x^9 + 483 \in \mathbb{Q}_3[x]$. The ramification polygon $\mathcal{R}_\varphi$ is comprised of two segments with endpoints $(1, 18)$, $(3, 9)$, and $(9, 0)$. From left to right, the segments of $\mathcal{R}_\varphi$ have slopes $-9/2$, $-3/2$ and residual polynomials $y + 1$, $y^3 + 1 \in \mathbb{F}_3[y]$. Using Algorithm 3.13, we compute the tower of extensions corresponding to the segments of $\mathcal{R}_\varphi$:

$$\mathbb{Q}_3 \subset \mathsf{L}_1 \subset \mathsf{L}_0 \cong \mathbb{Q}_3[x]/(\varphi)$$

where $\mathsf{L}_1 \cong \mathbb{Q}_3[x]/(x^3 + 3)$ and $\mathsf{L}_0 \cong \mathsf{L}_1[x]/(x^3 + \beta)$ for β satisfying $\beta^3 + 3 = 0$. It follows from Algorithm 3.23 that $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \cong \mathrm{Gal}(\mathsf{L}_1/\mathbb{Q}_3) \cong A_3$. By Corollary 4.14, $\mathrm{Gal}(\varphi)$ is a subgroup of the wreath product

$$\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathbb{Q}_3) \cong A_3 \wr A_3$$

After computing an initial list of candidate subgroups, we apply the decision steps from Algorithm 5.5 to all of the candidate groups. We observe the following changes in the total number of viable candidates:

Step(s)	(1)	(2)	(3-9)	(10)	(R1)	(R2)	(R3)
Remaining Candidates	23	10	5	4	2	2	1

After applying step (R3), we are left with $\mathrm{Gal}(\varphi) \cong 9T10$.

Example 5.11. Let $\varphi = x^{27} + 3 \in \mathbb{Q}_3[x]$. The ramification polygon $\mathcal{R}_\varphi$ is comprised of three segments with endpoints $(1, 81)$, $(3, 54)$, $(9, 27)$, $(27, 0)$. The slopes of these segments, from left to right, are $-27/2$, $-9/2$, $-3/2$. Using Algorithm 3.13, we compute the tower of extensions corresponding to the segments of $\mathcal{R}_\varphi$:

$$\mathbb{Q}_3 \subset \mathsf{L}_2 \subset \mathsf{L}_1 \subset \mathsf{L}_0 \cong \mathbb{Q}_3[x]/(\varphi).$$

It can be shown that $\mathsf{L}_1 \cong \mathbb{Q}_3[x]/(x^9+483)$. Since we determined the Galois group of $x^9+483 \in \mathbb{Q}_3[x]$ in Example 5.10, we now treat $\mathsf{L}_1/\mathbb{Q}_3$ as a single extension. Thus, we consider the tower of extensions $\mathbb{Q}_3 \subset \mathsf{L}_1 \subset \mathsf{L}_0$ where $\mathrm{Gal}(\mathsf{L}_1/\mathbb{Q}_3) \cong 9T10$ by Example 5.10 and $\mathcal{R}_{\mathsf{L}_0/\mathsf{L}_1}$ is comprised of a single segment.

Next, we compute the Galois group of the top relative extension $\mathsf{L}_0/\mathsf{L}_1$ using Algorithm 3.23. We find that $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \cong S_3$. This tells us, by Corollary 4.14, that $\mathrm{Gal}(\varphi)$ is a subgroup of the wreath product

$$\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathbb{Q}_3) \cong S_3 \wr (9T10).$$

After computing an initial list of candidate subgroups, we apply the decision steps from Algorithm 5.5 to all of the candidate groups. We observe the following changes in the total number of viable candidates:

Step	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(R1)
Remaining Candidates	200	83	60	54	54	32	32	32	32	4	1

After applying step (R1), we are left with $\mathrm{Gal}(\varphi) \cong 27T176$.

Remark. With the exception of some redundant operations, Examples 5.10 and 5.11 constitute the two iterative stages of Algorithm 5.1 required to compute the Galois group of $x^{27}+3 \in \mathbb{Z}_3[x]$ which has a ramification polygon that consists of 3 segments.

For the remainder of this section, we will assume that $\mathsf{K} = \mathbb{Q}_p$. We further assume that the steps in Algorithm 5.5 have been applied to the candidate groups and that we have failed to uniquely identify $\mathrm{Gal}(\varphi)$. At this stage of Algorithm 5.1, we rule out the other candidate groups by using relative resolvents.

In general, computing relative resolvents in order to determine the Galois group of a polynomial requires approximating the roots of that polynomial. This presents

a problem since computing the polynomial's splitting field is not always feasible. In an effort to address this problem for our polynomial φ, we adopt and expand upon an approach from [45]. From this, we obtain a polynomial that generates a tower of field extensions over the rational numbers. More specifically, we compute a tower of global fields

$$\mathbb{Q} \subset \mathsf{L}_1' \subset \mathsf{L}_0'$$

that exhibits the same relationships between its relative extensions as our tower of p-adic fields $\mathbb{Q}_p \subset \mathsf{L}_1 \subset \mathsf{L}_0$.

Before we delve into the details of this approach, we introduce some additional notation. For a polynomial $f \in \mathbb{Z}_p$, we will denote by $\mathrm{Gal}_{\mathbb{Q}}(f)$ its Galois group over the rationals, and we let $\mathrm{Gal}_{\mathbb{Q}_p}(f)$ denote the Galois group over $\mathbb{Q}_p$. In terms of this new notation, the ultimate goal of our algorithm is to compute $\mathrm{Gal}_{\mathbb{Q}_p}(\varphi)$.

Let $\varphi_1(y) \in \mathbb{Q}_p[y]$ be a degree m polynomial so that $\mathsf{L}_1 = \mathbb{Q}_p[y]/(\varphi_1) = \mathbb{Q}_p(\gamma)$, and let $\gamma = \gamma_1, \ldots, \gamma_m$ be the roots of φ_1 in some algebraic closure of $\mathbb{Q}_p$. Additionally, let $\varphi_0(x)$ be a degree n/m polynomial that satisfies $\mathsf{L}_0 = \mathsf{L}_1[x]/(\varphi_0)$. The coefficients of φ_0 are in terms of γ and elements of $\mathbb{Q}_p$. This means that we can write the generating polynomial of $\mathsf{L}_0/\mathsf{L}_1$ as $\varphi_0(x, \gamma)$.

According to Proposition 2.41, we can find a polynomial ψ that generates $\mathsf{L}_0/\mathbb{Q}_p$ by computing the norm $\mathrm{N}_{\mathsf{L}_1/\mathbb{Q}_p}(\varphi_0(x, \gamma))$. We find that

$$\begin{aligned}
\psi(x) &:= \mathrm{N}_{\mathsf{L}_1/\mathbb{Q}_p}(\varphi_0(x, \gamma)) \\
&= \prod_{i=1}^{m} \varphi_0(x, \gamma_i) \\
&= \mathrm{res}_y(\varphi_0(x, y), \varphi_1(y)).
\end{aligned}$$

$$\begin{array}{ccc} \mathsf{L}_0 = \mathsf{L}_1[x]/(\varphi_0) = \mathbb{Q}_p[x]/(\varphi) & & \mathsf{L}_0' = \mathbb{Q}[x]/(\psi) \\ | & & | \\ \mathsf{L}_1 = \mathbb{Q}_p[x]/(\varphi_1) & & \mathsf{L}_1' = \mathbb{Q}[x]/(\varphi_1) \\ | & & | \\ \mathbb{Q}_p & & \mathbb{Q} \end{array}$$

Figure 7. Subfield tower for the stem field of an Eisenstein Polynomial φ and the corresponding tower of extensions for the polynomial $\psi(x) = \mathrm{res}_y(\varphi_0(x,y), \varphi_1(y))$.

We note that since a resultant can be computed without approximating the roots of the inputted polynomials, it is unnecessary to approximate $\gamma_1, \ldots, \gamma_m$.

Since ψ and φ generate the same extension of $\mathbb{Q}_p$, we have that $\mathrm{Gal}_{\mathbb{Q}_p}(\psi) \cong \mathrm{Gal}_{\mathbb{Q}_p}(\varphi)$. Thus, we can restrict ourselves entirely to finding $\mathrm{Gal}_{\mathbb{Q}_p}(\psi)$. In other words, ψ replaces our polynomial φ.

We use $\psi(x)$ to generate a global field extension $\mathsf{L}_0'/\mathbb{Q}$. It can be shown that L_0' has a subfield L_1' such that $\mathsf{L}_1'/\mathbb{Q}$ is generated by φ_1 (see Figure 7).

Treating ψ as a polynomial with integer coefficients, we approximate the roots of ψ over an unramified extension of $\mathbb{Q}_q$ for some rational prime q. To this end, we apply Lemma 4.11 to several rational primes that don't divide $\mathrm{disc}\,(\psi)$, and choose from among these a prime q for which the prescribed unramified extension of $\mathbb{Q}_q$ has minimal degree. By minimizing the degree of our unramified extension, we reduce the precision needed to ensure accuracy in the future construction and analysis of resolvent polynomials constructed from the roots of ψ.

The next step is to compute the Galois groups of $\mathsf{L}_0'/\mathsf{L}_1'$ and $\mathsf{L}_1'/\mathbb{Q}$. Then, using Theorem 4.12, we compute the partitioning of the roots of ψ with respect to the block system $\mathfrak{B}$ of $\mathrm{Gal}_{\mathbb{Q}}(\psi)$ that we get with our subfield L_1'. From there it is straightforward to compute the block system of $W' := \mathrm{Gal}(\mathsf{L}_0'/\mathsf{L}_1') \wr \mathrm{Gal}(\mathsf{L}_1'/\mathbb{Q})$ and

find the permutation $\sigma \in S_n$ that maps the block system of W' to $\mathfrak{B}$. Reordering the roots of ψ by σ we have that $\mathrm{Gal}_{\mathbb{Q}}(\psi) \leq W'$.

If we let W denote the wreath product $\mathrm{Gal}(\mathsf{L}_0/\mathsf{L}_1) \wr \mathrm{Gal}(\mathsf{L}_1/\mathbb{Q}_p)$ from which we obtained our initial list of candidate groups, then, by construction, W' is guaranteed to contain a conjugate of W. In fact, it is not unusual for $W \leq W'$ to hold. This allows us to identify each of our candidates with subgroups of W'. It is from this list of subgroups of W' that we will find our Galois group.

In order to eliminate the extra candidate groups, we look at low index subgroups of W'. Starting with $k = 2$, we compute the set W'_k of representatives for each conjugacy class of subgroups of W' of index k. For each group $H \in W'_k$, we employ the procedure described in our comments following Theorem 4.24 to determine whether or not to form the resolvent corresponding to the group pair $H < W'$. Based upon this, we either rule out one or more candidates using the list of the degrees of the irreducible factors of the resolvent, or we move on to another group in W'_k without computing the resolvent. If we exhaust the groups in W'_k and still have multiple candidate groups, then we increase k by 1 and repeat the above process until we identify the Galois group.

5.5 Future Work: Relative Linear Resolvents

Let L/K be a finite extension, and let $\mathsf{L} \cong \mathsf{K}[x]/(\varphi)$ for an irreducible, separable polynomial $\varphi \in \mathsf{K}[x]$. Let M be a normal extension of K such that φ factors as $\prod_{i=1}^{l} \varphi_i$ over $\mathsf{M}[x]$, with $\deg(\varphi_i) = m$ for $1 \leq i \leq l$. Let

$$F(x_1, \ldots, x_n) = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n$$

be a linear multivariate polynomial with integer coefficients.

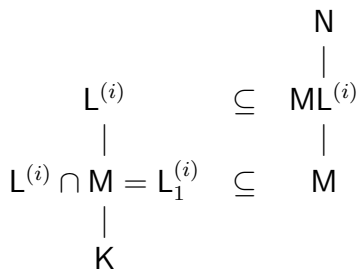

Figure 8. Subfield diagram for the proof of Proposition 5.12.

In her thesis [74], Sandi Rudzinksi presents an algorithm that computes the relative linear resolvent $R_F(S_m \wr S_l, \varphi)$ without approximating the roots of φ [74, Algorithm 7 and Theorem 4.5]. She also expands her algorithm to find $R_F(S_m \wr G, \varphi)$ where $G \leq S_l$ is a transitive permutation group [74, Proposition 4.6].

The proposition below guarantees that the necessary conditions for Rudzinksi's method can be achieved.

Proposition 5.12. *Let $\varphi \in \mathsf{K}[x]$ be irreducible and separable with degree n. Let N denote the splitting field of φ. If M/K is a normal subextension of N/K, then φ factors over M as a product of distinct irreducible polynomials of the same degree.*

Proof. Let $\alpha^{(1)}, \ldots, \alpha^{(n)}$ denote the roots of φ in some algebraic closure $\overline{\mathsf{K}}$ of K. As φ is squarefree, all factors of φ are distinct. For each root $\alpha^{(i)}$ of φ we denote by $\varphi_{j(i)}$ the irreducible factor of φ, over M, for which $\alpha^{(i)}$ is a root.

Let $\mathsf{L} = \mathsf{K}[x]/(\varphi)$, and let $\mathsf{L}_1 = \mathsf{M} \cap \mathsf{L}$. For $1 \leq i \leq n$, the conjugates of L are $\mathsf{L}^{(i)} = \mathsf{K}(\alpha^{(i)}) = \mathsf{L}_1(\alpha^{(i)})$. Similarly, the conjugates of L_1 are $\mathsf{L}_1^{(i)} = \mathsf{L}^{(i)} \cap \mathsf{M}$. Since $\mathsf{K}(\alpha^{(i)})$ is always the same up to isomorphism, we have the subfield diagram in Figure 8 for $1 \leq i \leq n$ where both $\mathsf{L}^{(i)}/\mathsf{L}_1^{(i)}$ and $\mathsf{ML}^{(i)}/\mathsf{M}$ have degree $\deg(\varphi_{j(i)})$. Thus, each $\alpha^{(i)}$ is a root of an irreducible factor of φ over M of degree $\frac{[\mathsf{L}^{(i)}:\mathsf{K}]}{[\mathsf{L}^{(i)} \cap \mathsf{M}:\mathsf{K}]}$. □

We now assume that φ is Eisenstein, and the ramification polygon $\mathcal{R}_\varphi$ consists of two segments. We claim that, under these conditions, we can apply Rudzinksi's algorithm. To justify this assertion, we consider some of the material from the later parts of Chapter III. Since $\mathcal{R}_\varphi$ consists of two segments, φ generates a tower of extensions $\mathsf{K} \subset \mathsf{L}_1 \subset \mathsf{L}_0 = \mathsf{K}[x]/(\varphi)$ where $\mathcal{R}_{\mathsf{L}_0/\mathsf{L}_1}$ and $\mathcal{R}_{\mathsf{L}_1/\mathsf{K}}$ each consist of one segment. Let T_1 be the maximal tamely ramified subextension of the normal closure of L_1/K, and let $\mathsf{M} = \mathsf{T}_1\mathsf{L}_1$ be the compositum of T_1 and L_1. If L_1/K is tamely ramified, then $\mathsf{L}_1 = \mathsf{T}_1$ and M is a normal extension of K by Theorem 3.25. Otherwise, if L_1/K is wildly ramified, M is normal since it is the splitting field of the polynomial that generates L_1/K (see Theorem 3.18). In either case, M/K is normal and our assertion follows from Proposition 5.12.

In light of the above considerations, our future work in computing Galois groups will be largely driven by three questions regarding how we could incorporate Rudzinski's work into our algorithm:

(1) Do there exist cases where this method could be applied to determining the Galois group of an Eisenstein polynomial whose ramification polygon consists of three or more segments?

(2) With what frequency can the factorization of the resolvents, computed using this method, identify the Galois group from a list of candidate groups?

(3) To what degree can the resolvents from this method be used to delay or make unnecessary the use of the polynomial ψ from Section 5.4?

REFERENCES

[1] Chad Awtrey, *Dodecic Local Fields*, PhD thesis, Arizona State University, 2010.

[2] Chad Awtrey, Nakhila Mistry, and Nicole Soltz, *Centralizers of Transitive Permutation Groups and Applications to Galois Theory*, Missouri J. Math. Sci. 27 (2015), no. 1, 16–32, `http://projecteuclid.org/euclid.mjms/1449161364`

[3] C. Awtrey, *Dodecic 3-adic fields*, Int. J. Number Theory, **8**, no. 4, 933–944, 2012.

[4] C. Awtrey, B. Barkley, N. Miles, C. Shill, and E. Strosnider, *Degree 12 2-adic fields with automorphism group of order 4*, Rocky Mountain J. Math., **45**, no. 6, 1755–1764, 2016.

[5] C. Awtrey, N. Miles, J. Milstead, C. Shill, and E. Strosnider, *Degree 14 2-adic fields*, Involve, a journal of mathematics, **8**, no. 2, 329–336 (2015).

[6] C. Awtrey, K. Mazur, S. Rodgers, N. Soltz, and J. Weed, *On Galois groups of degree 15 polynomials*, Int. J. Pure Appl. Math., **104**, no. 3, 407–420, 2015.

[7] J. Bauch, E. Nart, and D. Stainsby, *Complexity of OM Factorizations*, LMS Journal of Computation and Mathematics, **16**, 139–171.

[8] M. Bridson and C. Miller. *Structure and finiteness properties of subdirect products of groups*, Proc. Lond. Math. Soc. (3) **90** (2009), 631–651.

[9] J. Brown, R. Cass, R. Keaton, S. Parenti, and D. Shankman, *Degree 14 extensions of* $\mathbb{Q}_7$, Int. J. of Pure and Appl. Math., 100(2), 337–345 (2015).

[10] W. Bosma, J. J. Cannon, C. Fieker, and A. Steel (eds.), *Handbook of Magma functions*, Edition 2.16 (2010).

[11] J.J. Cannon, B. Cox, and D.F. Holt, *Computing the subgroups of a permutation group*, J. Symb. Comp., 31:149–161, 2001.

[12] John J. Cannon, Lucien A. Dimino, George Havas, and Jane M. Watson, *Implementation and analysis of the Todd-Coxeter algorithm*, Math. Comp., 27:463–490, 1973.

[13] J.W.S. Cassels, *Local Fields*, Cambridge University Press, Cambridge, 1986.

[14] Henri Cohen, *A course in computational algebraic number theory*. Graduate texts in mathematics, vol 138. Springer, Berlin. MR 1228206 (94i:11105) (1993).

[15] John H. Conway, Alexander Hulpke, and John McKay, *On transitive permutation groups*, LMS J. Comput. Math., 1:1–8, 1998.

[16] P. Deligne, *Les corps locaux de charactéristque p limites de corps locaux de charactéristique 0* in J.-N. Bernstein, P. Deligne, D. Kazhdan, and M.-F. Vigneras, *Représentation des groupes réductifs-sur un corps local*, Travaux en cours, Hermann, 1984.

[17] H. Derksen and G. Kemper. Computational invariant theory, *Encyclopaedia of Mathematical Sciences. Invariant Theory and Algebraic Transformation Groups*, Springer, Berlin, 2002.

[18] Bart De Smit, *Galois groups and wreath products*, `http://www.math.leidenuniv.nl/~desmit/notes/krans.pdf`, October 2007.

[19] Andreas Distler, *Ein Algorithmus zum LÃűsen einer Polynomgleichung durch Radikale* , Diplomarbeit, Universität Braunschweig, 2005, `http://www.icm.tu-bs.de/ag_algebra/software/distler/Diplom.pdf`

[20] David S. Dummit and Richard M. Foote, *Abstract Algebra*, Third Edition, John Wiley & Sons, Inc., 2004.

[21] Y. Eichenlaub. *Problemes effectifs de theorie de Galois en degres 8 a 11.* These, Universite Bordeaux 1, 1996.

[22] A.S. Elsenhans. *Invariants for the Computation of intransitive and transitive Galois Groups.* J. Symb. Comput., **47** (2012), 315–326.

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

[24] C. Fieker and J. Klüners, *Computation of Galois groups of rational polynomials*, LMS J. Comput. Math **17** (2014), 141-158.

[25] D. Ford, *On the Computation of the maximal order in a Dedekind domain*, PhD Dissertation, Ohio State University, 1978.

[26] D. Ford, S. Pauli, and X.-F. Roblot, *A Fast Algorithm for Polynomial Factorization over* $\mathbb{Q}_p$, Journal de Théorie des Nombres de Bordeaux, **14** (2002) 151–169.

[27] Katharina Geissler, *Zur berechnung von Galoisgruppen*, Master's thesis, Technische Universitat Berlin, Berlin, 1997.

[28] K. Geissler, *Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern*, Dissertation, TU Berlin, 2003.

[29] K. Geissler and J. Klüners, *Galois Group Computation for Rational Polynomials*, J. Symb. Comput. **30** (2000), 653–674.

[30] K. Girstmair, *On the computation of resolvents and Galois groups*, Manuscripta Math, **43** (1983), 289–307.

[31] Fernando Q. Gouvea, *"A Marvelous Proof"*, American Mathematical Monthly, **101** (3), March 1994, pp. 203âĂŞ-222.

[32] C. Greve, *Galoisgruppen von Eisensteinpolynomen über p-adischen Körpern*, Dissertation, Universität Paderborn, 2010.

[33] 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.

[34] J. Guardia, J, Montes, and E. Nart, *Arithmetic in big number fields: the '+ideals' package*, ArXiv e-prints (2010), arXiv:1005.4596 [math.NT].

[35] J. Guardia, J. Montes, and E. Nart, *Higher Newton polygons and integral bases*, arXiv:0902.3428 (2009).

[36] J. Guàrdia, J. Montes, and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc., **364** (2012), no. 1, 361–416.

[37] J. Guàrdia, J. Montes, E. Nart, *Okutsu Invariants and Newton Polygons*, Acta Arithmetica 145 (2010), 83–108.

[38] J. Guàrdia, E. Nart, and S. Pauli. *Single-factor lifting and factorization of polynomials over local fields*, J. Symbolic Comput., 47(11):1318–1346, 2012.

[39] H. Hasse, *Number Theory*, Springer Verlag, Berlin, 1980.

[40] Charles Helou, *Non-Galois ramification theory of local fields*, Algebra Berichte [Algebra Reports], vol. 64, Verlag Reinhard Fischer, Munich, 1990.

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

[42] M. van Hoeij, J. Klüners and A. Novocin. *Generating Subfields*, J. Symb. Comput., **52** (2013), 17–34.

[43] Derek F. Holt, Bettina Eick, Eamonn A. O'Brien, *Handbook of Computational Group Theory*, Chapman & Hall/CRC, 2005.

[44] B. Huppert, *Endliche Gruppen I*, Springer Verlage, Berlin, 1967.

[45] J. Jones and D. Roberts, *Nonic 3-adic Fields*, in ANTS VI, Springer Lecture Notes in Computer Science, 3076 (2004), 293–308.

[46] J. Jones and D. Roberts, *A Database of Local Fields*, J. Symbolic Comput., **41** (2006), 80–97, `http://math.asu.edu/~jj/localfields`.

[47] J. Jones and D. Roberts, *Octic 2-adic Fields*, J. Number Theory., **128** (2008), 1410–1429.

[48] Jürgen Klüners, *On Computing Subfields. A Detailed Description of the Algorithm*, Journal de Théorie des Nombres de Bordeaux, **10** (1998), 243–271.

[49] J. Klüners. *Über die Berechnung von Automorphismen und Teilkörpern algebraischer Zahlkörper*, PHD TU-Berlin (1997).

[50] 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.

[51] M. Krasner and L. Kaloujnine. *Produit complet des groupes de permutation et probleme d'extension de groupes II.* Acta Sci. Math. (Szeged), 14:39–66, 1951.

[52] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematic, vol. 110, Spring-Verlag, New York, 1994.

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

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

[55] Saunders MacLane and Garrett Birkhoff, *Algebra*, The Macmillian Company, London, 1967.

[56] S. MacLane, *A Construction for prime ideals as absolute values of an algebraic field*, Duke Mathematical Journal, **2** (1936), 493–510.

[57] J. Milstead, S. Pauli, and B. Sinclair, *Constructing Splitting Fields of Polynomials over Local Fields*, pp. 101-124 in Collaborative mathematics and statistics research (Greensboro, NC, 2013), vol. 109, edited by Jan Rychtar et al., Springer Proceedings in Mathematics and Statistics **64**, Springer, Cham, 2015.

[58] J.D.P. Meldrum, *Wreath products of groups and semigroups*, John Wiley and Sons, Inc., New York, NY, 1995.

[59] M. 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.

[60] J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, Dissertation, Universitat de Barcelona, 1999.

[61] J. Montes and E. Nart, *On a Theorem of Ore*, J. Algebra, **146** (1992), 318–334.

[62] Peter Müller, *HilbertâĂŹs Irreducibility Theorem for prime degree and general polynomials*, 1998

[63] W. Narkiewicz: *Elementary and Analytic Theory of Algebraic Numbers*, Springer Verlag, Berlin 2004.

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

[65] Ö. Ore, *Newtonsche Polynome in der Theorie der algebraischen Körper*, Math. Ann., **99** (1928), no. 1, 84–117.

[66] P. Panayi, *Computation of Leopoldt's p-adic regulator*, Dissertation, University of East Anglia, 1995.

[67] 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).

[68] S. Pauli and B. Sinclair, *Enumerating extensions of local fields*,International Journal of Number Theorey, Online, 2017.

[69] S. Pauli, *Factoring polynomials over local fields*, J. Symb. Comp., **32** (2001), 533–547.

[70] S. Pauli, *Factoring polynomials over local fields II*, in G. Hanrot and F. Morain and E. Thomé, *Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010*, LNCS, Springer Verlag, 2010.

[71] D. J. S. Robinson, *A Course in the Theory of Groups*, Graduate Texts in Mathematics 80, Springer Verlag Berlin-Heidelberg-New York, 1982.

[72] D. S. Romano, *Galois groups of strongly Eisenstein polynomials*, Dissertation, UC Berkeley, 2000.

[73] D. S. Romano, *Ramification polygons and Galois groups of wildly ramified extensions*, Preprint, 2007.

[74] S. Rudzinski, *Symbolic Computation of Resolvents*, MA. Thesis, UNCG, 2017.

[75] J. Scherk, *The Ramification Polygon for Curves over a Finite Field*, Canadian Mathematical Bulletin, **46**, no. 1 (2003), 149–156.

[76] B. Schmalz. Verwendung von Untergruppenleitern zur Bestimmung von Doppelnebenklassen, *Bayreuther Mathematische Schriften*, **31** (1990), 109–143.

[77] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1963.

[78] 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.

[79] Brian Sinclair, *Algorithms for enumerating invariants and extensions of local fields*, Ph.D. thesis, University of North Carolina at Greensboro, 2015.

[80] Leonard Soicher, *The computation of Galois groups*, Master's thesis, Concordia University, Montreal, 1981.

[81] L. H. Soicher, J. McKay, *Computing Galois groups over the rationals*, J. Number theory, **20** (1985), 273âĂŞ-281

[82] R. P. Stauduhar, *The Determination of Galois Groups*, Math. Comp., **27** (1973), 981-âĂŞ996.

[83] J.A. Todd and H.S.M Coxeter, *A practical method for enumerating cosets of a finite abstract group*, Proceedings of the Edinburgh Mathematical Society. Series II 5: 26âĂŞ-34, 1936.

[84] K. Yokoyama, *A modular method for computing the Galois groups of polynomials*, J. Pure Appl. Algebra, **117/118** (1997), 617âĂŞ-636.

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

APPENDIX A

GALOIS GROUPS

In this section we provide necessary background information about Galois groups. What follows is a list, with minimal commentary, of definitions and properties that were compiled primarily from [20].

Let K be a field. For an algebraic extension $\mathsf{L} = \mathsf{K}[x]/(\varphi(x))$ where $\varphi \in \mathsf{K}[x]$ is irreducible we call the smallest field over which φ splits into linear factors the *normal closure* of L. An *algebraic closure* of K is an algebraic extension of K that is algebraically closed.

Definition A.1. (1) An isomorphism σ of K with itself is called an *automorphism* of K. The collection of automorphisms of K is denoted $\mathrm{Aut}(\mathsf{K})$. If $\alpha \in \mathsf{K}$ we shall write $\sigma\alpha$ for $\sigma(\alpha)$.

(2) An automorphism $\sigma \in \mathrm{Aut}(\mathsf{K})$ is said to *fix* an element $\alpha \in \mathsf{K}$ if $\sigma\alpha = \alpha$. If F is a subset of K (for example, a subfield), then an automorphism σ is said to *fix* F if it fixes all the elements of F, i.e., $\sigma\alpha = \alpha$ for all $\alpha \in \mathsf{F}$.

Definition A.2. Let K/F be an extension of fields. Let $\mathrm{Aut}(\mathsf{K}/\mathsf{F})$ be the collection of automorphisms of K which fix F.

Proposition A.3. *The set* $\mathrm{Aut}(\mathsf{K})$ *is a group under composition and* $\mathrm{Aut}(\mathsf{K}/\mathsf{F})$ *is a subgroup.*

Proposition A.4. *Let* K/F *be a field extension and let* $\alpha \in \mathsf{K}$ *be algebraic over* F*. Then for any* $\sigma \in \mathrm{Aut}(\mathsf{K}/\mathsf{F})$*,* $\sigma\alpha$ *is a root of the minimal polynomial for* α *over* F *i.e,* $\mathrm{Aut}(\mathsf{K}/\mathsf{F})$ *permutes the roots of irreducible polynomials. Equivalently, any polynomial with coefficients in* F *having* α *as a root also has* $\sigma\alpha$ *as a root.*

Proposition A.5. *Let $H \leq \mathrm{Aut}(\mathsf{K})$ be a subgroup of the group of automorphisms of K. Then the collection F of elements of K fixed by all the elements of H is a subfield of K.*

Definition A.6. If H is a subgroup of the group of automorphisms of K, the subfield of K fixed by all the elements of H is called the *fixed field* of H.

Proposition A.7. *The association of groups to fields defined above is inclusion reversing, namely*

(1) *if $\mathsf{F}_1 \subseteq \mathsf{F}_2 \subseteq \mathsf{K}$ are two subfields of K then $\mathrm{Aut}(\mathsf{K}/\mathsf{F}_2) \leq \mathrm{Aut}(\mathsf{K}/\mathsf{F}_1)$, and*

(2) *if $H_1 \leq H_2 \leq \mathrm{Aut}(\mathsf{K})$ are two subgroups of automorphisms with associated fixed fields F_1 and F_2, respectively, then $\mathsf{F}_2 \subseteq \mathsf{F}_1$.*

Proposition A.8. *Let E be the splitting field over F of the polynomial $f(x) \in \mathsf{F}[x]$. Then $|\mathrm{Aut}(\mathsf{E}/\mathsf{F})| \leq [\mathsf{E} : \mathsf{F}]$ with equality if $f(x)$ is separable over F.*

Definition A.9. Let K/F be a finite extension. Then K is said to be *Galois* over F and K/F is a *Galois* extension if $|\mathrm{Aut}(\mathsf{K}/\mathsf{F})| = [\mathsf{K} : \mathsf{F}]$. If K/F is Galois, the group of automorphisms $\mathrm{Aut}(\mathsf{K}/\mathsf{F})$ is called the *Galois group* of K/F, denoted $\mathrm{Gal}(\mathsf{K}/\mathsf{F})$.

If K/F is not Galois, then we define the Galois group $\mathrm{Gal}(\mathsf{K}/\mathsf{F})$ to be the automorphism group $\mathrm{Aut}(\mathsf{N}/\mathsf{F})$ of the normal closure N of K/F.

Definition A.10. If $f(x)$ is a separable polynomial over F, then the *Galois group* $\mathrm{Gal}(f)$ of $f(x)$ over F is the Galois group of the splitting field of $f(x)$ over F.

Theorem A.11. *Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of automorphisms of a field K and let F be the fixed field. Then*

$$[\mathsf{K} : \mathsf{F}] = n = |G|.$$

Corollary A.12. *Let* K/F *be any finite extension. Then*

$$|\mathrm{Aut}(\mathsf{K}/\mathsf{F})| \leq [\mathsf{K} : \mathsf{F}]$$

with equality if and only if F *is the fixed field of* $\mathrm{Aut}(\mathsf{K}/\mathsf{F})$*. Put another way,* K/F *is Galois if and only if* F *is the fixed field of* $\mathrm{Aut}(\mathsf{K}/\mathsf{F})$*.*

Corollary A.13. *Let* G *be a finite subgroup of automorphisms of a field* K *and let* F *be the fixed field. Then every automorphism of* K *fixing* F *is contained in* G*, i.e.,* $\mathrm{Aut}(\mathsf{K}/\mathsf{F}) = G$*, so that* K/F *is Galois, with Galois group* G*.*

Corollary A.14. *If* $G_1 \neq G_2$ *are distinct finite subgroups of automorphisms of a field* K *then their fixed fields are also distinct.*

Theorem A.15. *The extension* K/F *is Galois if and only if* K *is the splitting field of some separable polynomial over* F*. Furthermore, if this is the case then every irreducible polynomial with coefficients in* F *which has a root in* K *is separable and has all its roots in* K *(so in particular* K/F *is a separable extension).*

Definition A.16. Let K/F be a Galois extension. If $\alpha \in \mathsf{K}$, the elements $\sigma\alpha$ for σ in $\mathrm{Gal}(\mathsf{K}/\mathsf{F})$ are called the *conjugates* of α over F. If E is a subfield of K containing F, the field $\sigma(\mathsf{E})$ is called the *conjugate field* of E over F.

Theorem A.17. *(Fundamental Theorem of Galois Theory) Let* K/F *be a Galois extension and set* $G = \mathrm{Gal}(\mathsf{K}/\mathsf{F})$*. Then there is a bijection between the set of subfields* E *of* K *containing* F *and the set of subgroups* H *of* G*. In particular, each subfield* E *corresponds to the group of elements of* G *that fix* E *and each subgroup* H *corresponds to its fixed field. Under this correspondence:*

(1) *If* E_1*,* E_2 *correspond to* H_1*,* H_2*, respectively, then* $\mathsf{E}_1 \subseteq \mathsf{E}_2$ *if and only if* $H_2 \leq H_1$*,*

(2) *If* E_1, E_2 *correspond to* H_1, H_2, *respectively, then the intersection* $\mathsf{E}_1 \cap \mathsf{E}_2$ *corresponds to the group* $\langle H_1, H_2 \rangle$ *generated by* H_1 *and* H_2 *and the composite field* $\mathsf{E}_1\mathsf{E}_2$ *corresponds to the intersection* $H_1 \cap H_2$.

Assume a field E *satisfying* $\mathsf{F} \subseteq \mathsf{E} \subseteq \mathsf{K}$ *corresponds to a subgroup* $H \leq G$.

(3) $[\mathsf{K} : \mathsf{E}] = |H|$ *and* $[\mathsf{E} : \mathsf{F}] = |G : H|$, *the index of* H *in* G.

(4) K/E *is always Galois, with Galois group* $\mathrm{Gal}(\mathsf{K}/\mathsf{E}) = H$.

(5) E *is Galois over* F *if and only if* H *is a normal subgroup in* G. *If this is the case, then the Galois group is isomorphic to the quotient group*

$$\mathrm{Gal}(\mathsf{E}/\mathsf{F}) \cong G/H.$$

If the field K has cardinality $|\mathsf{K}| < \infty$, we say that K is a *finite field* with *order* $|\mathsf{K}|$. The number of elements in a finite field is p^n where p is a rational prime and n is a natural number. Up to isomorphism, there is only one field of order p^n and it is denoted by $\mathbb{F}_{p^n}$.

A finite field $\mathbb{F}_{p^n}$ is normal over $\mathbb{F}_p$ and its Galois group is cyclic with order n:

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle$$

where $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ with $\sigma_p(\alpha) = \alpha^p$ is referred to as the *Frobenius automorphism.*

Proposition A.18. *The field* $\mathbb{F}_{p^n}$ *is the splitting field over* $\mathbb{F}_p$ *of the polynomial* $x^{p^n} - x$, *with cyclic Galois group of order* n *generated by the Frobenius automorphism* σ_p. *The subfields of* $\mathbb{F}_{p^n}$ *are all Galois over* $\mathbb{F}_p$ *and are in one to one correspondence with the divisors* d *of* n. *They are the fields* $\mathbb{F}_{p^d}$, *the fixed fields of* σ_p^d.

For natural numbers m, n and p with p prime we have that $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^n}) = \langle \sigma : x \mapsto x^{p^n} \rangle$.

APPENDIX B

DIRECT AND SEMIDIRECT PRODUCTS

When working with groups it can be desirable, if not beneficial, to construct a new group from existing ones. Doing so increases the collection of group examples at the mathematician's disposal and aides in the classification of groups. Oftentimes, such constructions can be obtained by taking so called "products" of groups. This methodology has the additional benefit of allowing one to decompose a group into smaller "factors".

We begin this section with an examination of direct products of groups. It is our expectation that much of this will be familiar to the reader. First, we will recall the basic definitions and properties. These properties have been chosen and ordered so that our discussion will naturally culminate to 2 major results: The Fundamental Theorem of Finitely Generated Abelian groups and the Recognition Theorem. We will follow this up with a brief discussion of inherent limitations of direct products. This will allow us to pivot into a similar examination of semidirect products.

The bulk of the information we present has been gathered from [20] and [55]. Furthermore, the manner in which the information is motivated and organized mimics the treatment of the material in Chapter 5 of [20].

B.0.1 Direct Products

The direct product operation on groups is a natural extension of the Cartesian Product of sets.

Definition B.1. (1) If $(A, *)$ and $(B, \diamond)$ are groups, we can form a new group $A \times B$, called their *direct product*, whose elements are those in the Cartesian

product

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$

and whose operation is defined component-wise:

$$(a_1, b_1)(a_2, b_2) = (a_1 * a_2, b_1 \diamond b_2).$$

(2) Similarly, the *direct product* $G_1 \times G_2 \times \cdots \times G_n$ of the groups $G_1, G_2, \ldots, G_n$ with operations $*_1, *_2, \ldots, *_n$, respectively, is the set of n-tuples $(g_1, g_2, \ldots, g_n)$ where $g_i \in G_i$ with operation defined component-wise:

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n).$$

Remark. (1) By convention, every abstract group is written multiplicatively. Thus, we will write the above operation as

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1 h_1, g_2 h_2, \ldots, g_n h_n).$$

Nevertheless, the reader should bear in mind that the operation may be different from one G_i to another.

(2) Rearranging the "factors" in a direct product gives us a group isomorphic to the group with the previous ordering.

In the next few results we will, for the sake of brevity and simplicity, restrict ourselves to the $n = 2$ case. It can, of course, be shown that analogous results hold for all $n \in \mathbb{N}$.

Proposition B.2. *Let G_1 and G_2 be groups and let $G = G_1 \times G_2$ be their direct product. Let 1_{G_1} and 1_{G_2} be, respectively, the identity elements of G_1 and G_2.*

(1) *The sets $H_1 = \{(g_1, 1_{G_2}) \mid g_1 \in G_1\}$ and $H_2 = \{(1_{G_1}, g_2) \mid g_2 \in G_2\}$ are subgroups of G isomorphic to, respectively, G_1 and G_2.*

(2) *If we identify G_1 and G_2 with the subgroups in (1) then $G_1 \trianglelefteq G$ and $G_2 \trianglelefteq G$. Furthermore, $G/G_1 \cong G_2$ and $G/G_2 \cong G_1$.*

Proof. (1) It is clear that H_1 and H_2 are nonempty because G_1 and G_2 are nonempty. Let $(x_1, 1_{G_2}), (y_1, 1_{G_2}) \in H_1$. Then

$$\begin{aligned}(x_1, 1_{G_2})(y_1, 1_{G_2})^{-1} &= (x_1, 1_{G_2})(y_1^{-1}, 1_{G_2}) \quad \text{since } y_1 y_1^{-1} = 1_{G_1} \\ &= (x_1 y_1^{-1}, 1_{G_2})\end{aligned}$$

which is in H_1.

Since $x_1, y_1 \in G_1$ were chosen arbitrarily, we conclude that this holds in general. Thus $H_1 \leq G$ by the Subgroup Criterion. Similarly, for $(1_{G_1}, x_2), (1_{G_1}, y_2) \in H_2$ we find that

$$\begin{aligned}(1_{G_1}, x_2)(1_{G_1}, y_2)^{-1} &= (1_{G_1}, x_2)(1_{G_1}, y_2^{-1}) \\ &= (1_{G_1}, x_2 y_2^{-1}) \in H_2\end{aligned}$$

which leads us to conclude that $H_2 \leq G$.

To prove the remainder of (1), consider the maps

$$\pi_1 : G_1 \to H_1 \text{ defined by } \pi_1(g_1) = (g_1, 1_{G_2})$$

and

$$\pi_2 : G_2 \to H_2 \text{ defined by } \pi_2(g_2) = (1_{G_1}, g_2).$$

It is clear, by construction, that π_1 and π_2 are bijections. Furthermore,

$$\begin{aligned}\pi_1(g_1h_1) &= (g_1h_1, 1_{G_2}) \\ &= (g_1, 1_{G_2})(h_1, 1_{G_2}) \\ &= \pi_1(g_1)\pi_1(h_1)\end{aligned}$$

and

$$\begin{aligned}\pi_2(g_2h_2) &= (1_{G_1}, g_2h_2) \\ &= (1_{G_1}, g_2)(1_{G_1}, h_2) \\ &= \pi_2(g_2)\pi_2(h_2).\end{aligned}$$

Therefore, π_1 and π_2 are isomorphisms.

(2) We will now identify G_1 with H_1 and G_2 with H_2. Consider the map $\varphi : G \to G_2$ defined by $\varphi(g_1, g_2) = g_2$. This map is a homomorphism because

$$\begin{aligned}\varphi((g_1, g_2)(h_1, h_2)) &= \varphi(g_1h_1, g_2h_2) \\ &= g_2h_2 \\ &= \varphi(g_1, g_2)\ \varphi(h_1, h_2).\end{aligned}$$

Since φ is a homomorphism, its kernel is a normal subgroup of G by the First Isomorphism Theorem. In particular,

$$\begin{aligned} ker\varphi &= \{(g_1, g_2) \in G \mid \varphi(g_1, g_2) = 1_{G_2}\} \\ &= \{(g_1, g_2) \in G \mid g_2 = 1_{G_2}\} \\ &= \{(g_1, 1_{G_2}) \mid g_1 \in G_1\} \\ &= G_1. \end{aligned}$$

Thus, the First Isomorphism Theorem tells us that $G_1 \trianglelefteq G$ and $G/G_1 \cong \varphi(G)$. Since φ is, clearly, surjective this becomes $G/G_1 \cong G_2$. By a similar argument, the map $\tau : G \to G_1$ defined by $\tau(g_1, g_2) = g_1$ is a surjective homomorphism with kernel $ker\tau = G_2$. A second application of the First Isomorphism Theorem gives us that $G_2 \trianglelefteq G$ and $G/G_2 \cong G_1$. □

Proposition B.3. *The direct product of* 2 *groups is abelian if and only if both of the constituent groups are abelian.*

Proof. Let G_1 and G_2 be groups and let $G = G_1 \times G_2$ be their direct product. Suppose G is abelian. Because the operation on G is component-wise, we find that

$$\begin{aligned} (g_1h_1, g_2h_2) &= (g_1, g_2)(h_1, h_2) \\ &= (h_1, h_2)(g_1, g_2) \quad \text{since } G \text{ is abelian} \\ &= (h_1g_1, h_2g_2). \end{aligned}$$

Equality between elements of G is possible only if the corresponding components are equal. In other words, the above gives us, $g_1h_1 = h_1g_1$ and $g_2h_2 = h_2g_2$. Since g_1, g_2, h_1, and h_2 were chosen arbitrarily, we conclude that the last two equa-

tions hold for all elements of G_1 and G_2. In short, we conclude that G_1 and G_2 are abelian.

Conversely, suppose that G_1 and G_2 are abelian. Then for $g_1, h_1 \in G_1$ and $g_2, h_2 \in G_2$ we obtain

$$\begin{aligned}(g_1, g_2)(h_1, h_2) &= (g_1 h_1, g_2 h_2) \\ &= (h_1 g_1, h_2 g_2) \quad \text{since } G_1, G_2 \text{ are abelian} \\ &= (h_1, h_2)(g_1, g_2).\end{aligned}$$

Since these group elements are arbitrary, we conclude that $G = G_1 \times G_2$ is an abelian group. □

A straightforward, inductive argument can be used to conclude that the direct product of groups is abelian if and only if each of the factors is abelian. In the case of finitely generated abelian groups there is a bit more to be said.

Theorem B.4. *(Fundamental Theorem of Finitely Generated Abelian Groups) Let G be a finitely generated abelian group. Then*

(1) *$G \cong C_{p_1^{r_1}} \times C_{p_2^{r_2}} \times \cdots \times C_{p_n^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ where p_i are rational primes that might not be distinct and $r_i > 0$ for each factor.*

(2) *The factorization in (1) is unique up to the rearrangement of the factors.*

(3) *If G has order $n \in \mathbb{N}$ and the unique prime factorization (distinct primes) of n is $n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ then $G \cong G_1 \times G_2 \times \cdots \times G_t$ where $|G_i| = p_i^{m_i}$.*

This result allows us to express any finitely generated abelian group as the direct product of cyclic groups. In doing so, it provides algebraists with a powerful

tool for classifying abelian groups. Sadly, there does not exist an analogous result for non-abelian groups.

Example B.5. Let S_3 denote the symmetric group of degree 3. We will show that S_3 is not a direct product of nontrivial groups. To see this, let's assume the contrary. Specifically, let us assume that $S_3 \cong H \times K$ for groups H and K with order greater than 1. According to Proposition B.2, $H \times K$ has subgroups that are isomorphic to H and K. Hence, by Lagrange's Theorem, $|H|$ and $|K|$ must divide $|S_3| = 6$. The only groups that have order 2 or 3 are the cyclic groups of those orders. This means that S_3 is the direct product of cyclic groups. Because cyclic groups are abelian, Proposition B.3 implies that S_3 is abelian. This is false.

Proposition B.3 implies that some non-abelian groups can be expressed as direct products of proper, nontrivial subgroups. What is less clear is how one determines whether or not such a decomposition is possible.

B.0.2 Recognizing Direct Products

The purpose of this subsection is to introduce a well-known criterion by which one can determine if a group can be described as the direct product of 2 of its proper subgroups. We begin with some prerequisite information regarding products of group subsets.

Definition B.6. Let H and K be subgroups of a group G and define

$$HK = \{hk \mid h \in H, k \in K\}.$$

Proposition B.7. *If H and K are subgroups of a group G, then $HK \leq G$ if and only if $HK = KH$.*

It is worth pointing out that the relation $HK = KH$ is not equivalent to saying that every element of H commutes with every element of K.

Corollary B.8. *If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.*

We now address the task at hand. Let G denote an abstract, possibly infinite group with identity element 1_G. We want to establish rules by which one can determine whether or not $G \cong H \times K$ for nontrivial subgroups H and K. Put another way, we need to specify characteristics that $H \leq G$ and $K \leq G$ must have in order for $G \cong H \times K$ to be true. A good place to start is Proposition B.2, which states that $H \times K$, and thus G if they're isomorphic, has normal subgroups that are isomorphic to H and K. So we will, first, require that H and K be normal subgroups of G.

The relation $G \cong H \times K$ implies a well-defined correspondence between elements of G and pairs (h, k) for which $h \in H$ and $k \in K$. This is where the construct HK comes in. Since we have established that $K \trianglelefteq G$, we know from Corollary B.8 that $HK \leq G$. This means that we can make the aforementioned correspondence concrete by requiring that each element of G be a product of an element of H with an element of K. In short, we will require that $G = HK$.

It is possible that some elements of HK can be written in more than one way. For an element $g \in G$ there may exist $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $g = h_1k_1$ and $g = h_2k_2$. In order to create an isomorphism between $G = HK$ and $H \times K$ we must restrict H and K further so that this cannot occur. As the next proposition shows, it is sufficient to require that $H \cap K = 1_G$.

Proposition B.9. *Let H and K be subgroups of the group G. If $H \cap K = 1_G$, then each element of HK can be written uniquely as a product hk, for some $h \in H$ and $k \in K$.*

Proof. Suppose an element of HK can be written as h_1k_1 and as h_2k_2. Then we have $h_1k_1 = h_2k_2$. Multiplying both sides on the left by h_2^{-1} and on the right by k_1^{-1} yields $h_2^{-1}h_1 = k_2k_1^{-1}$. The quantity on the left side is an element of H and the product on the right side is an element of K. Thus $h_2^{-1}h_1$ and $k_2k_1^{-1}$ are in $H \cap K$. Since $H \cap K = 1_G$ we have $h_2^{-1}h_1 = 1_G$ and $k_2k_1^{-1} = 1_G$. Respectively, these are equivalent to $h_1 = h_2$ and $k_1 = k_2$. Therefore, $h_1k_1 = h_2k_2$ implies that $h_1 = h_2$ and $k_1 = k_2$. We have proven uniqueness. □

In an effort to simplify future terminology, we introduce another definition.

Definition B.10. Let H be a subgroup of the group G. A subgroup K of G is called a *complement* for H in G if $G = HK$ and $H \cap K = 1_G$

Below, we consolidate our restrictions on H and K to formally state the sought after criterion.

Theorem B.11 (Recognition Theorem)**.** *Suppose G is a group with subgroups H and K such that*

(1) *K is a complement for H in G.*

(2) *H and K are normal in G.*

Then $G \cong H \times K$.

Proof. We will show that the map $\varphi : G \to H \times K$ defined by $\varphi(hk) = (h, k)$ is an isomorphism. By Proposition B.9, each element of $G = HK$ can be uniquely written as a product hk for some $h \in H$ and $k \in K$. This tell us that φ is well-defined and bijective. All that remains is to prove that φ is operation preserving.

Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Since $H \trianglelefteq G$, $k_1 h_2^{-1} k_1^{-1} \in H$. Thus $h_2(k_1 h_2^{-1} k_1^{-1}) \in H$. By a similar argument, $K \trianglelefteq G$ implies that $(h_2 k_1 h_2^{-1}) k_1^{-1} \in K$. So, $h_2 k_1 h_2^{-1} k_1^{-1} \in H \cap K$. It follows that $h_2 k_1 h_2^{-1} k_1^{-1} = 1_G$. Multiplying on the right by $k_1 h_2$ we obtain

$$h_2 k_1 = k_1 h_2. \tag{2.1}$$

We now apply φ to our group elements to find that

$$\begin{aligned} \varphi(h_1 k_1 h_2 k_2) &= \varphi(h_1 h_2 k_1 k_2) \quad \text{by (2.1)} \\ &= (h_1 h_2, k_1 k_2) \\ &= (h_1, k_1)(h_2, k_2) \\ &= \varphi(h_1 k_1)\varphi(h_2 k_2). \end{aligned}$$

Because h_1, h_2, k_1, k_2 were chosen arbitrarily, we conclude that this argument holds in general. Therefore, φ is a homomorphism. □

B.0.3 The Inadequacy of Direct Products

We motivated our consideration of group products, in part, by underscoring the fact that such products increase the number of group examples at our disposal. Although direct products do serve this purpose, the effectiveness with which they do so is limited. For example, Proposition B.3 informs us that if we have a collection of

abelian groups then direct products do not provide us a means by which to construct a non-abelian group. This fact alone seriously limits our pool of examples.

Further limitations are present in the Recognition Theorem. If we have 2 groups H and K, then any group $G \cong H \times K$ must have 2 normal subgroups that are isomorphic to H and K and are complements. This is quite restrictive since it dictates much of the new group's subgroup structure. It does, however, provide us with a blueprint for developing a more general, less limiting product.

B.0.4 Semidirect Products

For the purpose of motivation, let H and K be abstract groups. Suppose, furthermore, that we want to create a group G that has subgroups that are isomorphic copies of H and K in such a way that the copy of H is normal in G. We wish to place no such restriction on the copy of K. Moving forward, we will identify H and K with their copies and borrow several ideas from the previous subsections.

Like the direct product, the elements of G will be ordered pairs (h, k) for $h \in H$ and $k \in K$. All that remains is to define the binary operation on these elements. We cannot define it componentwise in a natural sense because doing so would just serve to reintroduce direct products. Instead, we will lean heavily on the desired normality. Since H is a normal subgroup, Corollary B.8 tells us that HK will be a subgroup of G . In time, just as we did with direct products, we would like to establish a correspondence between products hk in HK and pairs (h, k). For now we will assume it exists. Thus, in this environment, our search for a group operation can be reduced to defining products of elements in HK.

Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$. We seek to define $(h_1k_1)(h_2k_2)$. One approach would be to switch the order of k_1 and h_2. This is appealing since it would allow

us to define the operation for G in terms of a product in H and a product in K. Furthermore, we have a precedent for such a thing. In our proof of the Recognition Theorem we made this exact swap. Unfortunately, this was only permissible because H and K were both normal. We don't necessarily have that and we don't want to abandon our decision not to require that K be normal. A bit more ingenuity is called for.

At the heart of our current dilemma is a need to describe how elements of H interact with elements of K. For this, we make further use of our normality requirement for H. Since $H \trianglelefteq G$, we have that products of the form khk^{-1} are in H for $h \in H$ and $k \in K$. In other words, H is closed under left conjugation with respect to elements of K. With this in mind, we seek to introduce a quantity khk^{-1} into $(h_1k_1)(h_2k_2)$ in such a way that we get an element $h'k'$ for some $h' \in H$, $k' \in K$. Fortunately, this is straightforward:

$$\begin{aligned}(h_1k_1)(h_2k_2) &= (h_1k_1)h_2(k_1^{-1}k_1)k_2 \\ &= h_1(k_1h_2k_1^{-1})k_1k_2 \\ &= h'k'\end{aligned}$$

where $h' = h_1(k_1h_2k_1^{-1}) \in H$ and $k' = k_1k_2$. We have defined our product in terms of a product $k_1h_2k_1^{-1}$. As stated previously, we know that $k_1h_2k_1^{-1}$ is an element of H. What we don't know for sure, from theory, is which element of H it is. In order to define the operation on HK, we need a way to specify what the conjugate values khk^{-1} would be.

For a given $k \in K$, conjugating every element of H by k permutes the elements of H: $\{khk^{-1} : h \in H\} = H$. Coupling this with the fact that conjugation is

an isomorphism, we have an automorphism on H defined by k. This tells us that conjugation defines a mapping φ from K into $\mathrm{Aut}(H)$ where $\varphi(k)$ is the automorphism defined by k. Therefore, specifying the conjugate values khk^{-1} is the same as choosing a homomorphism φ from K into $\mathrm{Aut}(H)$. This choice of mapping is necessary and completely defines our desired group operation.

Putting this all together, we define our operation on HK as:

$$(h_1k_1)(h_2k_2) = h_1\varphi(k_1)(h_2)k_1k_2.$$

We are now prepared to define G.

Theorem B.12. *Let H and K be groups with identity elements 1_H and 1_K (respectively) and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. Let $\cdot$ denote the (left) action of K on H defined by $k \cdot h = \varphi(k)(h)$. Let G be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ and define the following multiplication on G:*

$$(h_1, k_1)(h_2, k_2) = (h_1k_1 \cdot h_2, k_1k_2).$$

(1) This multiplication makes G into a group of order $|G| = |H|\,|K|$.

(2) The sets $\widetilde{H} = \{(h, 1_K) \mid h \in H\}$ and $\widetilde{K} = \{(1_H, k) \mid k \in K\}$ are subgroups of G and the maps $h \mapsto (h, 1_K)$ for $h \in H$ and $k \mapsto (1_H, k)$ for $k \in K$ are isomorphisms of these subgroups with the groups H and K respectively:

$$H \cong \{(h, 1_K) \mid h \in H\} \quad \text{and} \quad K \cong \{(1_H, k) \mid k \in K\}.$$

Identifying H and K with their isomorphic copies in G described in (2) we have

(3) $H \trianglelefteq G$

(4) $H \cap K = 1_G$.

Remark. Because $H \cap K = 1_G$, Proposition B.9 implies that there exists a well-defined correspondence between products hk and ordered pairs (h, k).

Observant readers will notice that the preceding theorem never mentions conjugaton and allows φ to be any homomorphism from K into $\mathrm{Aut}(H)$. No attempt is even made to relate φ to conjugation. The reason for this is simple: every such φ ends up defining conjugation in G.

Corollary B.13. *Let H and K be groups and let φ be a homomorphism from K into* $\mathrm{Aut}(H)$. *Let G, $\widetilde{H}$ and $\widetilde{K}$ be defined as they are in Theorem* B.12. *If we identify H and K (respectively) with $\widetilde{H}$ and $\widetilde{K}$ then $\varphi(k)(h) = khk^{-1}$ for all $h \in H$ and $k \in K$.*

Proof. We wish to examine the all too familiar quantity khk^{-1} in terms of corresponding elements in $\widetilde{H}$ and $\widetilde{K}$. By identifying h with $(h, 1_K)$ and k with $(1_H, k)$ we have that khk^{-1} corresponds to

$$\begin{aligned}
(1_H, k)(h, 1_K)(1_H, k^{-1}) &= \left((1_H, k)(h, 1_K)\right)(1_H, k^{-1}) \\
&= (1_H k \cdot h, k1_K)(1_H, k^{-1}) \\
&= (k \cdot h, k)(1_H, k^{-1}) \\
&= \left((k \cdot h)k \cdot 1_H, kk^{-1}\right) \\
&= (k \cdot (h1_H), 1_K) \quad \text{since } \varphi \text{ is operation preserving} \\
&= (k \cdot h, 1_K).
\end{aligned}$$

We have shown that $khk^{-1} = k \cdot h = \varphi(k)(h)$. □

Definition B.14. The group G in Theorem B.12 is called the *Semidirect product* of H and K with respect to φ. Symbolically, it is written $H \rtimes_\varphi K$.

The subscript of φ is needed since different choices of $\varphi : K \to \mathrm{Aut}(H)$ correspond to different values of the quantities khk^{-1} which, in turn, define different groups G. In cases where the choice of φ is clear, it is customary to write $H \rtimes K$.

Example B.15. Let $H = C_n$, the cyclic group that has order n and let $K = C_m$. We will say that $H = \langle a \rangle$ and $K = \langle d \rangle$. We seek to form a semidirect product $G = H \rtimes_\varphi K$ for some $\varphi : K \to \mathrm{Aut}(H)$. The group G will consist of elements $(h, k) = (a^i, d^j)$ for $0 \leq i < n$ and $0 \leq j < m$. All that remains is to choose our map φ.

If $\ell \in \mathbb{Z}$ and n are relatively prime then we have $H = \langle a^\ell \rangle$. Thus $\tau : C_n \to C_n$ with $\tau(a^i) = a^{\ell i}$ is an element of $\mathrm{Aut}(H)$. This means that we can define φ by $\varphi(d) = \tau$. To see how this works, we will identify H and K by their isomorphic copies in G (see Theorem B.12 and compute da. In this context,

$$\begin{aligned}(1_H, d)(a, 1_K) &= (1_H \varphi(d)(a), d1_K) \\ &= (\varphi(d)(a), d) \\ &= (\tau(a), d) \\ &= (a^\ell, d)\end{aligned}$$

which is equivalent to $da = a^\ell d$. If we multiply both sides of this relation on the right by d^{-1} we obtain $dad^{-1} = a^\ell$. It is clear by construction that this relation, in addition to the cyclical nature of H and K, is enough to define the operation on G.

In conclusion, we have that $G = C_n \rtimes_\varphi C_m$ has presentation

$$\langle a, d \mid a^n = 1, d^m = 1, dad^{-1} = a^\ell \rangle.$$

When $m = 2$ and $\ell = -1$, this group is isomorphic to the Dihedral group of order $2n$.

Example B.16. For some rational prime p and some $m \in \mathbb{N}$, let $(\mathbb{F}_p)^m$ denote the vector space of $m \times 1$ column vectors with entries in $\mathbb{F}_p$. We also denote by $\mathrm{GL}(m,p)$ the group of invertible $m \times m$ matrices with entries in $\mathbb{F}_p$. We seek to form a semidirect product $A = (\mathbb{F}_p)^m \rtimes_\varphi \mathrm{GL}(m,p)$ for some map $\varphi : \mathrm{GL}(m,p) \to \mathrm{Aut}((\mathbb{F}_p)^m)$. The group A will consist of elements (v, M) from the Cartesian Product $(\mathbb{F}_p)^m \times \mathrm{GL}(m,p)$. All that remains is to choose our map φ.

The elements of $\mathrm{GL}(m,p)$ act naturally on $(\mathbb{F}_p)^m$ through matrix multiplication on the left. Since linear transformations are automorphisms, each $M \in \mathrm{GL}(m,p)$ defines an element of $\mathrm{Aut}((\mathbb{F}_p)^m)$. In particular, each M corresponds to the map $u_M : (\mathbb{F}_p)^m \to (\mathbb{F}_p)^m$ defined by $x \mapsto Mx$. This means we can define φ by $\varphi(M) = u_M$ for all M in $\mathrm{GL}(m,p)$.

From the definition of semidirect products,

$$(v, M)(w, N) = (v + \varphi(M)(w), MN) = (v + Mw, MN).$$

is the operation of A.

Each $v \in (\mathbb{F}_p)^m$ corresponds to a mapping on $(\mathbb{F}_p)^m$ defined by addition by v. In other words, v corresponds to $s_v : (\mathbb{F}_p)^m \to (\mathbb{F}_p)^m$ defined by $x \mapsto x + v$. Furthermore, each element (v, M) of A corresponds to the pair of maps (s_v, u_M). Thus, it follows that each element of A corresponds to a map which involves both matrix multiplication and vector addition. In short, A must be isomorphic to

$$\mathrm{AGL}(m,p) = \{t_{M,v} : (\mathbb{F}_p)^m \to (\mathbb{F}_p)^m : x \mapsto Mx + v \mid M \in \mathrm{GL}(m,p), v \in (\mathbb{F}_p)^m\},$$

the *affine group* of $(\mathbb{F}_p)^m$.

Up to this point, much has been made of how the semidirect product is less limiting than the direct product. What we have not established is the concrete relationship between the two constructs. As the following proposition illustrates, the direct product is a particular type of semidirect product.

Proposition B.17. *Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ map every element of K to the identity automorphism. Then $H \rtimes_\varphi K \cong H \times K$.*

Proof. Let $h_1, h_2 \in H$ and let $k_1, k_2 \in K$. Then the group operation of $H \rtimes_\varphi K$ yields

$$\begin{aligned}(h_1, k_1)(h_2, k_2) &= (h_1\varphi(k_1)(h_2), k_1k_2) \\ &= (h_1h_2, k_1k_2)\end{aligned}$$

which is the result of the group operation of $H \times K$. □

Given this relationship, it is not surprising that a few of the results for direct products have semidirect product analogues. Among them is the Recognition Theorem B.11. Below is a similarly formulated criteria by which one can determine when a group can be expressed as the semidirect product of two smaller groups. Its proof has been omitted due to its similarities to the proof of Theorem B.11.

Theorem B.18. *Suppose G is a group with subgroups H and K such that*

(1) *K is a complement for H in G, and*

(2) *$H \trianglelefteq G$.*

Let $\varphi : K \to \mathrm{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H. Then $G \cong H \rtimes K$.

One striking element of Theorem B.18 is its depiction of the map φ as unique. At first glance, this appears to conflict with Theorem B.12 and the beginning of this section when we emphasized that φ can take different forms. Fortunately, there is no conflict. These two characterizations of φ are both true because we are approaching things from two very different directions.

In Theorem B.12 and the buildup to it, we started with two groups H and K and worked to define their semidirect product G. In time, we were able to reduce the task of determining G's operation to that of choosing a mapping φ which would specify the values of products khk^{-1} where h and k came from (possibly isomorphic copies of) H and K respectively. From different choices of φ came different definitions of G. Thus, specifying the map when describing/establishing G was necessary.

In Theorem B.18, we start with the group G and thus know its operation the entire time. Hence, we already know which elements of H equal the products khk^{-1}. There is no ambiguity. We know exactly what each product is so there is only one φ. In short, since we know the group operation we can reverse engineer the unique φ.

The fact that φ can be determined retroactively is a compelling argument for excluding φ from Theorem B.18. A more succinct restatement of Theorem B.18 is that a group G is a semidirect product if one of its proper, normal subgroups has a complement. With this simplified metric in hand, we can revisit our earlier example of S_3. Although the group S_3 cannot be represented as a nontrivial direct product, it can be factored as a semidirect product.

Example B.19. Let A_3 denote the alternating group of degree 3 and let C_2 denote the cyclic group of order 2. We will show that S_3 can be decomposed as $A_3 \rtimes C_2$. Since A_3 has index 2 in S_3, we know that $A_3 \trianglelefteq S_3$. This means that we just have

to find a subgroup of S_3 that is isomorphic to C_2 and is a complement of A_3. This subgroup must be generated by an element of order 2 and S_3 has three such elements: (12), (13), and (23). It can be shown that $\langle(12)\rangle \cap A_3 = \{1\}$ and $A_3\langle(12)\rangle = S_3$. Hence, we have that $S_3 \cong A_3 \rtimes C_2$, with $C_2 \cong \langle(12)\rangle$. To determine the map φ, for this product, one would simply let $\langle(12)\rangle$ act on A_3 by conjugation.

By a similar argument, it can be proven that $S_n \cong A_n \rtimes C_2$ for all $n \geq 2$. In each case, C_2 can be identified with $\langle(12)\rangle$.

The symmetric group S_3 is not an isolated example. There are many groups that cannot be decomposed as a direct product of nontrivial groups but can be factored as a nontrivial semidirect product. This is not, however, all-inclusive. Not every group can be expressed as a nontrivial semidirect product. Simple groups, for instance, have no proper, normal subgroups and thus fail to satisfy the criteria in Theorem B.18. Another group for which Theorem B.18 isn't applicable is the quaternion group Q_8.

Proposition B.20. *The quaternion group Q_8 cannot be expressed as a semidirect product of nontrivial groups.*

Proof. We will assume the contrary. In other words, we will assume that $Q_8 \cong H \rtimes K$ where H and K have order greater than 1. By Theorem B.12, H either has order 4 or order 2 while K has (respectively) order 2 or 4. The possibilities for such orders are limited. Our two factors H and K must each be isomorphic to one of the following groups: C_2, $C_2 \times C_2$, and C_4. Since all three of these groups contain a subgroup isomorphic to C_2, we must conclude that H and K both contain an element with order 2.

According to Theorem B.12 there exist subgroups $\widetilde{H}$ and $\widetilde{K}$ of Q_8 that are isomorphic to H and K respectively and satisfy $\widetilde{H} \cap \widetilde{K} = \{1\}$. Since H and K each contain an element of order 2, $\widetilde{H}$ and $\widetilde{K}$ do as well. However, since the intersection of the two groups is trivial, these elements must differ. This leads us to conclude that Q_8 has multiple elements of order 2. It does not. The only element of Q_8 that has order 2 is -1. We have arrived at a contradiction which implies that our initial assumption was false. $\square$

APPENDIX C

WREATH PRODUCTS

This section consists of a condensed discussion of the wreath product, a special type of semidirect product. We begin by establishing some notation and defining multiple group actions for permutation groups. From there we pivot to the definition of the wreath product in the context of permutation groups. In order to better illustrate the group operation and group action of the wreath product, we follow this definition up with a proof concerning transitivity.

All of the content in this section can be found in either [58] or [18]. In keeping with the conventions of the former, all of the group actions we use are right actions.

Every permutation group in this section will be expressed as a pair (A, X) where A is a group acting on the set X. Let (A, X) and (B, Y) be permutation groups. For our purposes, X and Y will be finite. Thus A and B can be viewed as subgroups of $S_{|X|}$ and $S_{|Y|}$ respectively.

We denote by $A^Y = \mathrm{Map}(Y, A)$ the set of all maps from Y to A. Each element of A^Y acts on the Cartesian product $X \times Y$ by only acting on the first coordinate as follows:

$$(x, y)f = (xf(y), y) \qquad \text{for } f \in A^Y.$$

Remark. The reason for our notation A^Y is recognition of the fact that A^Y is equivalent to the direct product of isomorphic copies of A where the index of the product is formed by Y. For example, if $Y = \{y_1, \ldots, y_n\}$ then for each $f \in A^Y$ we get the tuple $(f(y_1), \ldots, f(y_n))$ in the direct product A^n.

We also define the action of B on $X \times Y$ purely through the normal action on the second coordinate. In other words, we have

$$(x, y)h = (x, yh) \qquad \text{for } h \in B.$$

Lastly, we define the action of B on A^Y by

$$f^h(y) = f(yh^{-1}) \qquad \text{for } f \in A^Y,\ y \in Y \text{ and } h \in B.$$

It is clear that for every $h \in B$ the map $\psi^h : A^Y \to A^Y$ defined by $f \mapsto f^h$ is an automorphism. This observation allows us to define a semidirect product of A^Y and B.

Definition C.1. Let (A, X) and (B, Y) be permutation groups with X and Y finite. Let $\varphi : B \to \mathrm{Aut}(A^Y)$ be defined by $\varphi(h) = \psi^h$. Then we define the *(unrestricted) (permutational) wreath product* of A and B, denoted $A \wr B$, to be the semidirect product $A^Y \rtimes_\varphi B$. As a permutation group, $A \wr B$ acts imprimitively on the Cartesian product $X \times Y$ by

$$(x, y)(f, h) = (xf^h(y), yh) \qquad \text{for } f \in A^Y,\ h \in B.$$

Theorem C.2. *Let (A, X) and (B, Y) be permutation groups with X and Y finite. Then the wreath product $(A \wr B, X \times Y)$ is a transitive group if and only if (A, X) and (B, Y) are transitive groups.*

Proof. Suppose $(A \wr B, X \times Y)$ is transitive and let (x_1, y_1) and (x_2, y_2) be elements of $X \times Y$. Then there exists an element (f, h) of $A \wr B$ such that

$$(x_1, y_1)(f, h) = (x_2, y_2) \tag{3.1}$$

From the first coordinate of Equation (3.1) we have that $x_2 = x_1 f^h(y_1)$. Since f^h is a map from Y to A, we know that $f^h(y_1) \in A$. This implies that (A, X) is transitive. From the second coordinate of Equation (3.1) we obtain $y_2 = y_1 h$ where $h \in B$. It follows that (B, Y) is transitive as well.

Suppose conversely that (A, X) and (B, Y) are transitive. Then for (x_1, y_1) and (x_2, y_2) in $X \times Y$ there must exist $c \in A$ and $h \in B$ so that $x_2 = x_1 c$ and $y_2 = y_1 h$. Let f be any map from Y to A that sends $y_1 h^{-1} \in Y$ to c. Then $f^h(y_1) = c$ and

$$\begin{aligned}(x_1, y_1)(f, h) &= (x_1 f^h(y_1), y_1 h) \\ &= (x_1 c, y_1 h) \\ &= (x_2, y_2).\end{aligned}$$

Therefore, $(A \wr B, X \times Y)$ is a transitive group. □

It can also be shown that the wreath product of solvable groups is solvable.