Spring 2014

Prime Decomposition in Iterated Towers and Discriminant Formulae

Thomas Alden Gassert
University of Massachusetts - Amherst

PRIME DECOMPOSITION IN ITERATED TOWERS AND DISCRIMINANT FORMULAE

A Dissertation Presented

by

T. ALDEN GASSERT

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2014

Department of Mathematics and Statistics

PRIME DECOMPOSITION IN ITERATED TOWERS AND DISCRIMINANT FORMULAE

A Dissertation Presented

by

T. ALDEN GASSERT

Approved as to style and content by:

Farshid Hajir, Chair

Tom Weston, Member

Siman Wong, Member

Hossein Pishro-Nik
Electrical and Computer Engineering, Outside Member

Michael Lavine, Department Head
Mathematics and Statistics

DEDICATION

To Pop.

ACKNOWLEDGEMENTS

First and foremost, I must thank my advisor, Farshid Hajir, for his guidance and support over the past three years. Farshid has been a great font of knowledge, and he has been exceedingly generous with his time, meeting with me on a regular biweekly schedule (which is four times more often than I receive my biweekly paycheck). From the beginning, my meetings with Farshid have been completely devoid of any anxiety, stress, or sense of failure, and I would like to think that this mental security is the primary reason for my success as a graduate student. Of course, Farshid's gift as a storyteller and his sense of humor made our meetings all the more pleasurable. Nowadays, I cannot conclude an encounter with Farshid without getting at least one good chuckle out of him. In fact, in a draft of this document, I jokingly wrote "Dedekated to Dedekind" on the dedication page, much to Farshid's approval. I almost feel bad about having changed it.

I would also like to thank Siman Wong, for if not for a meeting with Siman in the McDonalds on King Street back in 2011, it is highly unlikely that I would have reached out to Farshid in the first place, or even completed graduate school. On the other hand, I cannot, for the life of me, get Siman to laugh. I suppose, (to use Siman's words) he is not laughing "for all the obvious reasons."

Thank you to Tom Weston, David Cox, and Ilona Trousdale for their support while I was on the job market. Additional thank you's to Ilona and the rest of the department staff—particularly Jake, Sarah, and Carla—for their assistance and expertise for all things related to teaching, travel, and graduation.

Extra thanks to Caleb Shor at Western New England University for his advise and support, especially while I was on the job market. Your friendship has been invaluable. Also, thanks for sharing your home with me, and trusting me to look after your dogs. Rocky and Jack have been great companions as well as a regular reminder that I go outside at least three times each day. Postscript: it rained a lot two weekends ago, and the roof above the guest room leaked. You should look into that.

To all my classmates: Luke, Holley, Julie, Jen, Anna, Jeff, Nico, ... our successes undoubtedly grew out of our companionship. To Zach, Pace, and all my other friends outside of school: You guys are the best. Thank you all.

Special thanks to Sally and Sonny at The Foundry. Best of luck with your business.

Finally, I am eternally indebted to my family for providing me the freedom and support to pursue my own course.

This thesis is dedicated to my grandfather. Since I was a child, I sought to emulate him. When I was five, my mother signed me up for violin lessons, and I adamantly refused. I wanted to play the piano like Pop. My grandfather liked to say that there were two types of people he disliked: doctors and lawyers, despite the fact that he was a lawyer and his eldest son (my father) was a medical doctor. I think I found a loophole. Though if he were still around today, I am sure he would ask, "you know what you are? You're full of prune juice."

ABSTRACT

PRIME DECOMPOSITION IN ITERATED TOWERS
AND DISCRIMINANT FORMULAE
MAY 2014
T. ALDEN GASSERT, B.S. BOWDOIN COLLEGE
M.S., UNIVERSITY OF MASSACHUSETTS AMHERST
Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST
Directed by: Professor FARSHID HAJIR

We explore certain arithmetic properties of iterated extensions. Namely, we compute the index associated to certain families of iterated polynomials and determine the decomposition of prime ideals in others.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

One of the fundamental objects in number theory is the number field, which is a finite extension of the rational numbers $\mathbf{Q}$. We can isolate any number field K of degree d over $\mathbf{Q}$ by identifying an algebraic integer θ in K for which $K = \mathbf{Q}(\theta)$. That is to say that θ is the root of a monic polynomial f of degree d with integer coefficients, and every element of K may be expressed as a $\mathbf{Q}$-linear combination of powers of θ. The algebraic integer θ is not unique. In fact, there are infinitely many θ—and hence infinitely many (monic, irreducible, degree d) polynomials—which generate K. It is therefore a fundamental problem in number theory to identify an "optimal" representative f with which to model K.

The quality of such a model may be judged, for example, by a ratio of discriminants: $\frac{\operatorname{disc}(f)}{\operatorname{disc}(K)}$. These values may be computed using the following formulas:

$$\operatorname{disc}(f) = \prod_{1 \le i < j \le d} (\theta_j - \theta_i)^2,$$

where $\theta_1, \ldots, \theta_d$ are the roots of f, and

$$\operatorname{disc}(K) = \det(\operatorname{tr}_{K/\mathbf{Q}}(\alpha_i \alpha_j)),$$

where $\alpha_1, \ldots, \alpha_d$ is a basis for the ring of integers $\mathcal{O}_K$. A precise understanding of these formulas is not necessary for this discussion. Rather, the formulas are given to illustrate the connection between these objects and their underlying rings: $\mathbf{Z}[\theta]$ in the case of f (where θ is a root of f), and $\mathcal{O}_K$ in the case of K. In a way, the discriminant provides a measure on the arithmetic complexity of these rings, where the relative complexity scales in proportion to the square of the index of one ring inside the other:

$$[\mathcal{O}_K : \mathbf{Z}[\theta]]^2 = \frac{\operatorname{disc}(f)}{\operatorname{disc}(K)}. \tag{1.1}$$

Throughout, we use $\mathrm{ind}(f)$ to denote the index $[\mathcal{O}_K : \mathbf{Z}[\theta]]$.

Given Equation (1.1), it is natural to ask if for each K there is an f for which $\mathrm{disc}(f) = \mathrm{disc}(K)$. The answer to this question is "no". One of the simplest counter-example, attributed to Dedekind, is the number field generated by a root of $x^3 - x^2 - 2x - 8$. We are then left to wonder, what are the fields K for which there is a monic, irreducible f such that $\mathrm{disc}(K) = \mathrm{disc}(f)$? More generally, given a monic irreducible polynomial f, are there efficient methods for stripping the "parasitic" factors of $\mathrm{disc}(f)$ to recover $\mathrm{disc}(K)$? In this paper, we will answer these questions for certain families of dynamically generated number fields. In order to discuss these fields, we will use some basic terminology from dynamics.

Let S be a set, and let f be a map from S to itself. We denote by f^n the n-fold composition (or *iterate*) of f, which is defined by

$$f^n(x) = f(f^{n-1}(x)), \quad \text{where} \quad f^0(x) = x.$$

In order to distinguish between the n-fold iterate and the n-th power of f, we will always write the exponent before the argument to indicate the n-fold iterate, while the exponent after the argument will denote the n-th product:

$$f^n(x) = \big(\underbrace{f \circ \cdots \circ f}_{n}\big)(x); \qquad f(x)^n = \big(f(x)\big)^n.$$

Given an element $a \in S$, the *forward orbit* of a is the set

$$\mathcal{O}_f(a) = \{f^n(a) : n \geq 0\}.$$

We say that $a \in S$ is *periodic* if there exists an integer $n > 0$ such that $f^n(a) = a$. The *period* of a is the least positive integer for which this relationship holds, and we say that a is *n-periodic* if the period of a is n. If $\mathcal{O}_f(a)$ contains a finitely many elements, then a is *preperiodic*, and the *preperiod* of a is the least positive integer $m \geq 0$ such that $f^m(a)$ is periodic. We say that a is *m-preperiodic* to mean that a is preperiodic of preperiod m, and if $m > 0$, then a is *strictly preperiodic*.

The *preimages* (or *backwards orbit*) of a is

$$\leftarrow O_f(a) = \{f^{-n}(a) : n \geq 0\}, \quad \text{where} \quad f^{-n}(a) = \{b \in S : f^n(b) = a\}.$$

Note that if $f \in \mathbf{Z}[x]$ is monic, then by taking preimages of a fixed integer t, we have the potential to produce algebraic integers of increasingly large degree over $\mathbf{Q}$. This dynamical construction offers new insights into the structure of number fields.

1.1 Iterated extensions

Let K be a number field and f be monic polynomial of degree at least 2 with coefficients in $\mathcal{O}_K$, the ring of integers of K. For a fixed $t \in \mathcal{O}_K$, if $f^n(x) - t$ is irreducible for all $n \geq 1$, one can obtain, very naturally, a tower of fields over K in the following way. Let $\{\theta_0 = t, \theta_1, \theta_2, \ldots\}$ be a compatible sequence of preimages of t satisfying $f(\theta_n) = \theta_{n-1}$ (and hence $f^n(\theta_n) - t = 0$), then we obtain an *iterated tower of fields*

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots,$$

where $K_n := K(\theta_n)$ and $[K_n \colon K] = (\deg f)^n$. Throughout this paper, we will always work under the assumption that

$$\boxed{t \text{ is a fixed integer for which } f^n(x) - t \text{ is irreducible for every } n \geq 1.}$$

Over the past decade these towers have received increasing attention, in part because the Galois groups associated to these fields are equipped with a natural action on rooted trees. If K_f is the field obtained by adjoining all the roots of $f^n(x) - t$ for $n \geq 1$ (in a fixed algebraic closure $\overline{K}$), then the Galois group $\mathrm{Gal}(K_f/K)$ is the *iterated monodromy group* of f (see Nekrashevych [30]). At any finite level, the Galois group $\mathrm{Gal}(K_n/K)$ is non-abelian and is isomorphic to a subgroup of the wreath product $\mathbf{Z}/n\mathbf{Z} \wr S_d$ ([38], Theorem 3.56). This action is in contrast to the action of Galois groups on p-adic vector spaces coming from torsion points on abelian varieties and more generally from étale cohomology.

Aitken, Hajir, and Maire [2] have shown that this process may be used to construct infinite, yet finitely ramified, extensions. Let

$$\mathcal{R}_f := \{r \in \overline{K} \colon f'(x) = 0\}, \quad \text{and} \quad \mathcal{B}_f := \{f(r) \colon r \in \mathcal{R}_f\}$$

denote the *ramification points* and *branch points* of f, respectively. The elements of $\mathcal{R}_f$ are also known as the *critical points* of f, and the elements of $\mathcal{B}_f$ are also known as the *critical values* of f. The polynomial f is *postcritically finite* if every critical point of f is preperiodic.

Note that $b \in \mathcal{B}_f$ if and only if $f(x) - b$ and $f'(x)$ share a common root. Hence r is a critical point of f if and only if r is a multiple root of $f(x) - b$. We denote the multiplicity of this root by

$$f'(x) = a\, d \prod_{r \in \mathcal{R}_f} (x - r)^{m_r(f)},$$

where a is the leading coefficient of f and $d = \deg(f)$. For each $b \in \mathcal{B}_f$ we define

$$\mathcal{M}_b(f) = \sum_{r \in \mathcal{R}_f, f(r)=b} m_r(f).$$

Consider the polynomial $\Phi_n(x) = f^n(x) - t$, where $t \in \mathcal{O}_K$ is chosen so that $f^n(x) - t$ is irreducible for every $n \geq 1$.

Proposition 1.1.1. *We have*

$$\operatorname{disc}(\Phi_n) = (-1)^{(d^n-1)(d^n-2)/2} d^{nd^n} a^{(d^n-1)^2/(d-1)} \prod_{b \in \mathcal{B}_{f^n}} (t-b)^{\mathcal{M}_b(f^n)}.$$

Proof. [2, Proposition 3.2]. □

Note that if $f \in \mathbf{Z}[x]$ is postcritically finite, the number of primes dividing $\operatorname{disc}(\Phi_n)$ stabilizes once n is sufficiently large. That is, there is a finite set of primes S such that the set of primes dividing $\operatorname{disc}(\Phi_n)$ is contained in S for every $n \geq 1$. From Equation (1.1), we know that the discriminant of the number field generated by Φ_n divides $\operatorname{disc}(\Phi_n)$. Moreover, the primes that ramify in a number field are precisely the primes that divide the discriminant of that field. Thus we can conclude that postcritically finite polynomials generate infinite finitely ramified towers. However, our question regarding the parasitic factors of $\operatorname{disc}(\Phi_n)$ still stands, with potentially significant consequences.

The *root discriminant* of a number field K of degree n over $\mathbf{Q}$ is the n-th root of $\operatorname{disc}(K)$, and we call an algebraic extension L over a number field K *asymptotically good* if (i) L is an infinite extension of K, and (ii) for every sequence of distinct intermediate subfields of L/K, the root discriminant remains bounded. In [2], it is asked if there are any asymptotically good iterated towers. If yes, then the iterated tower would give the first construction of infinite tamely and finitely ramified extensions. A "no" answer would imply that all iterated towers are deeply ramified at the primes dividing the degree of the generating function, yielding a dynamical version of the Fontaine-Mazur conjecture [11, Conjecture 5a]. Hajir has conjectured that the latter to be the case: iterated extensions cannot give rise to tamely ramified infinite extensions. In either case, one would need a careful understanding of $\operatorname{ind}(\Phi_n)$ to derive an answer from Proposition 1.1.1.

In this paper we compute the index associated to four families of polynomials: the power maps, the Chebyshev polynomials, the Dickson-(-1) polynomials, and the generalized Rikuna polynomials. (We will discuss these families of maps in more detail in the following chapter.) These

index calculations allow us to recover discriminant formulas for the iterated towers generated by these polynomials.

1.2 Field discriminants

Recall that a number field is *monogenic* if its ring of integers has a basis consisting of the powers of a single algebraic integer. Moreover, if $K = \mathbf{Q}(\theta)$ where θ is an algebraic integer with minimal polynomial θ, and $\operatorname{disc}(K) = \operatorname{disc}(f)$, then K is monogenic as $\mathcal{O}_K = \mathbf{Z}[\theta]$.

The classic example of a monogenic field is the cyclotomic field $\mathbf{Q}(\zeta_d)$, where ζ_d is a primitive d-th root of unity; the ring of integers of $\mathbf{Q}(\zeta_d)$ is $\mathbf{Z}[\zeta_d]$. The maximal totally real subfields of the cyclotomic fields are also known to be monogenic (see Liang [23]). Quadratic fields $\mathbf{Q}(\sqrt{D})$, where D is a square-free integer, are also monogenic; the ring of integers being

$$\mathcal{O}_{\mathbf{Q}(\sqrt{D})} = \begin{cases} \mathbf{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \pmod 4 \\ \mathbf{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Although the extension $\mathbf{Q}(\sqrt{D})$ is generated by $x^2 - D$, when $D \equiv 1 \pmod 4$, the ring of integers if not generated by a root of $x^2 - D$. In fact, $\operatorname{ind}(x^2 - D) = 2$, and so we see that in general, $\operatorname{ind} f = 1$ is a sufficient, but not necessary, condition for monogeneity.

Determining whether a number field is monogenic is a difficult and largely open question. Computational evidence of Ash, Brakenhoff, and Zarrabi supports a conjecture of Lenstra [3] that suggests that monogenic fields are abundant. However, the majority of results are known only for extensions of small degree (see Gras [15], Nakahara [28], Shah [35], Gaál [12], among others). A general survey of recent results can be found in Narkiewicz [29, pp. 79–81].

As part of this work, we identify large families of monogenic towers of iterated extensions by showing that $\operatorname{ind} \Phi_n = 1$, where $\Phi_n(x) = f^n(x) - t$, and f is a polynomial of odd prime power degree in the power, Chebyshev, or Dickson family. Two special cases of the types of polynomials that we consider are worth highlighting: the maps $x^{\ell^n} - 1$ and $T_\ell^n(x) - 2$, where ℓ is a prime, and T_ℓ denoted the Chebyshev polynomial of degree ℓ. The splitting fields of these polynomials are the cyclotomic field $\mathbf{Q}(\zeta_{\ell^n})$ and the maximal real subfield of the cyclotomic field $\mathbf{Q}(\zeta_{\ell^n}^+)$, respectively. Hence we have placed these classical one-parameter families of monogenic towers (parametrized by ℓ) into two-parameter families of monogenic towers parametrized by ℓ and t. The following is a generalization of [2, Proposition 6.2].

Theorem 1.2.1. *Let ℓ be a prime and let $K = \mathbf{Q}(\theta)$, where θ is a root of $T_\ell^n(x) - t$. If $T_\ell(t) - t \not\equiv 0 \pmod{\ell^2}$ and both $t-2$ and $t+2$ are square-free, then K is monogenic, as $[\mathcal{O}_K : \mathbf{Z}[\theta]] = 1$.*

The main tool for identifying when $\operatorname{ind}(\Phi_n) = 1$ is Dedekind's criterion, which gives a condition for when a prime divides the index. However, beyond determining that a prime divides $\operatorname{ind}(\Phi_n)$, the Dedekind criterion has no mechanism for computing the multiplicity of that prime divisor, and we are left to turn to other techniques.

About ten years ago, Montes proposed some new ideas on how one may compute the ring of integers of a number field. His method, which we refer to as the *Montes algorithm*, is carried out in a series of papers by Guàrdia, Montes, and Nart [16, 17, 18]. The algorithm was initially developed as a computational tool, taking a specified field as an input. But we have found that the techniques of the algorithm are well suited for and are highly effective at computing the index associated to iterated polynomials, though it is not a straight forward computation.

The algorithm employs a refined variation of the Newton polygon, called the *ϕ-Newton polygon*, which captures arithmetic data attached to each irreducible factor ϕ of Φ_n modulo a prime p. Similar to usual Newton polygon, the ϕ-Newton polygon is determined by the p-adic valuations of the coefficients of a polynomial. In this case, the polynomial of interest is a particular polynomial in ϕ. Before we can apply the key result of Guàrdia, Montes, and Nart (Theorem 4.2.2), we must carefully construct these polygons and show that they satisfy a certain technical condition. The resulting formulas can be quite complex; the index for the Cheybshev polynomial T_ℓ^n and the Rikuna polynomial $r_n(x, t; 3)$ are as follows.

Theorem 1.2.2. *Let ℓ be an odd prime and $K = \mathbf{Q}(\theta)$, where θ is a root of $T_\ell^n(x) - t$, with $t \not\equiv \pm 2 \pmod{\ell^2}$ and $t \not\equiv 2 \pmod 4$. Write $t^2 - 4 = A^2 B$, where B issquare-free. Then*

$$\operatorname{ind}(T_\ell^n(x) - t) = \begin{cases} \ell^E A^{(\ell^n-1)/2} & \text{if } t \text{ is odd} \\ \ell^E (A/2)^{(\ell^n-1)/2} & \text{if } t \equiv 0 \pmod 4, \end{cases}$$

where E is a constant defined in Theorem 6.2.11. Moreover,

$$\Delta_K = \begin{cases} \ell^{n\ell^n - 2E} B^{(\ell^n-1)/2} & \text{if } t \text{ is odd} \\ \ell^{n\ell^n - 2E} (4B)^{(\ell^n-1)/2} & \text{if } t \equiv 0 \pmod 4. \end{cases}$$

Theorem 1.2.3. *Write $t^2 + t + 1 = A^3 B$, where $\gcd(A, B) = 1$. Then*

$$\operatorname{ind} r_n(x, t; 3) = 3^{(3^n-1)(3^n-3)/4 + E} \prod_{p \mid AB} p^{(3^n-1)(\nu_p(t^2+t+1)-1)/2} \prod_{p \mid A} p,$$

$$\textit{where} \quad E = \begin{cases} \frac{1}{2}\left(3^n - 1 + V + \sum_{k=0}^{V-1} 3^{n-k}\right) & \textit{if } t \equiv 1 \pmod 3 \\ 0 & \textit{otherwise,} \end{cases}$$

for a constant V, which we specify in Theorem 7.3.3.

1.3 Finite field dynamics

Both of the methods mentioned above—Dedekind's criterion and the Montes algorithm—require some knowledge of the factorization of our polynomials modulo primes. Our understanding of the factorization of our polynomials comes from analyzing the dynamics of the polynomials over finite fields (or in the case of the generalized Rikuna polynomial, the action of a rational map).

The dynamics of a map f over a finite field $\mathbf{F}_q$ can be captured in a graph, which is constructed as follows: each element $a \in \mathbf{F}_q$ corresponds to a vertex in the graph, and the graph contains the directed edge (a, b) if $f(a) = b$. For each of the four types of maps that we study (power, Chebyshev, Dickson, and generalized Rikuna), the components of the graph display a surprising degree of symmetry. (See Figure 1.) Moreover, we are able to give a complete description of the structure of these graphs. For example, the cycle structure for the Chebyshev polynomials is as follows.

Theorem 1.3.1. *Let ℓ be a prime, and $q = p^k$ a prime power. Write $q - 1 = \ell^{\lambda_1}\omega_1$ and $q + 1 = \ell^{\lambda_2}\omega_2$, where $\gcd(\omega_1, \ell) = \gcd(\omega_2, \ell) = 1$. The number of periodic vertices in the graph of T_ℓ over $\mathbf{F}_q$ is $(\omega_1 + \omega_2)/2$.*

The study of maps over finite fields has a long history. *Permutation polynomials*—polynomials that permute the elements of $\mathbf{F}_q$—are of particular interest due to their number theoretic properties and cryptographic applications. The *Dickson polynomials*, a one-parameter family of polynomials defined by

$$\mathcal{D}_{d,a}(z + a/z) = z^d + (a/z)^d,$$

provide the classic examples. It is known, for example, that for $a \in \mathbf{F}_q^\times$, the polynomial $\mathcal{D}_{d,a}$ permutes $\mathbf{F}_q$ if and only if $\gcd(d, q^2 - 1) = 1$, and $\mathcal{D}_{d,0}$ permutes $\mathbf{F}_q$ if and only if $\gcd(d, q - 1) = 1$ ([25], Theorem 3.2 and Theorem 3.1, respectively). Furthermore, the cycle structures of the

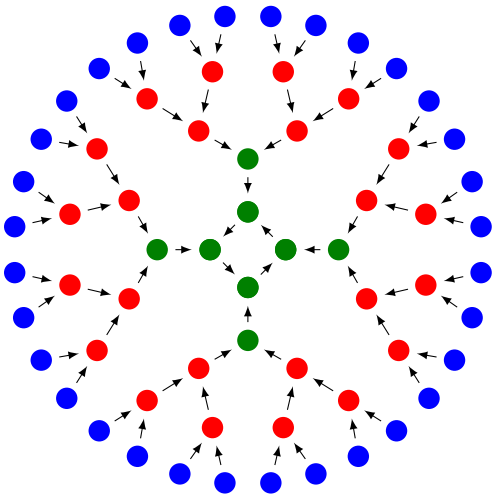


Figure 1: A component of the graph of T_2 over the finite field of order 29^4. The color of the vertex corresponds to the smallest field containing the element associated to the vertex: green – $\mathbf{F}_{29}$; red – $\mathbf{F}_{29^2}$; blue – $\mathbf{F}_{29^4}$.

permutation maps for $a \in \{-1, 0, 1\}$ are given in Lidl and Mullen [24]. For more on permutation polynomials, see Section 7 of Lidl and Niederreiter [26].

One may also graph the action of rational maps over the projective space $\mathbb{P}^1(\mathbf{F}_q)$. However, much less work has been done in this vein. Ugolini showed that when $\mathbf{F}_q$ is a finite field of characteristic 2, 3, or 5, the components of the graph of $x \mapsto x + x^{-1}$ are highly symmetric [40, 41].

In general, our maps will not give a permutation of the field, so we require a theory that includes a description of the vertices that are not contained in cycles. These graphs also give a visualization of the decomposition of primes in these extension, an idea that was proposed in [2].

The key finding is that the decomposition of a prime in the full tower can be determined solely be considering the graph over a finite extensions of $\mathbf{F}_p$. For example, consider the decomposition of $p\mathbf{Z}$ in the iterated extensions coming from $T_\ell^n(x) - t$, where T_ℓ is the Chebyshev polynomial of prime degree ℓ, and $p \neq \ell$. We remind the reader that t is chosen so that $T_\ell^n(x) - t$ is irreducible for each $n \geq 1$. Let ρ denote the preperiod of $\bar{t} \in \mathbf{F}_p$, and let m_p denote the maximal preperiod of elements of $\mathbf{F}_p$ under the action of T_ℓ.

Theorem 1.3.2. *Let ℓ be an odd prime, let p be a prime that does not divide the discriminant of $T_\ell^n(x) - t$, and let $K_n = \mathbf{Q}(\theta)$, where θ is a root of $T_\ell^n(x) - t$. If $0 < \rho \leq m_p$, then $p\mathbf{Z}$ splits completely in K_n for each $0 \leq n \leq m_p - \rho$, after which all primes above $p\mathbf{Z}$ are totally inert.*

In the case of the special extensions coming from $x^{\ell^n} - 1$ and $T_\ell^n(x) - 2$, we are able to recover the cyclotomic reciprocity law. Thus our decomposition result may be viewed as an extension of cyclotomic reciprocity to certain non-abelian extensions of $\mathbf{Q}$.

$\star \quad \star \quad \star$

The general outline of the paper is as follows. In the following chapter, we describe in more detail the power, Chebyshev, Dickson, and Rikuna families of polynomials. In Chapter 3, we describe the graphs of these maps over finites fields to determine the decomposition of primes in our iterated extensions. We outline the key tools for computing the index computations in Chapter 4, and the remainder of the paper is dedicated to carrying out these careful computations.

CHAPTER 2

SPECIAL FAMILIES OF POLYNOMIALS

In this chapter we give a brief overview of the families of polynomials on which this paper focuses. We mentioned previously that the Galois groups of iterated extensions can be quite large. However, the special extensions that we study at have Galois groups that are relatively small. The power map $x^d - t$ yields Kummer a extension, which are cyclic over $\mathbf{Q}(\zeta_d)$, where ζ_d is a primitive d-th root of unity. The Galois groups for the Chebyshev extensions are known to be dihedral ([4, Proposition 5.6]); the Galois groups of Rikuna polynomials are also known [5, 32, Theorem 1 and Theorem 2.5, respectively].

2.1 Power maps

The power maps are the polynomials $P_d(x) = x^d$. The iterated extensions arising from the polynomials $P_d^n(x) - t = x^{d^n} - t$ are well studied as they give rise to Kummer extensions. Our discussion of these maps primarily serves as a model for analyzing the extensions generated by the other families of maps.

2.2 Chebyshev polynomials

The Chebyshev polynomials of the first kind, $T_d(x)$, and second kind, $U_d(x)$, are another well-studied family of maps. These polynomial are defined by

$$T_d(z + z^{-1}) = z^d + z^{-d}, \quad \text{and} \quad U_d(x) = \frac{d}{dx}\frac{T_{d+1}(x)}{d+1}$$

The Chebyshev family is uniquely rich in that the polynomials satisfy a variety of relations, which we state here without proof. An interested reader may refer to Rivlin's book on the subject [33]

and Silverman [38, Chapter 7].

Proposition 2.2.1.

1. *$T_d(T_e(x)) = T_{de}(x)$ for all $d, e \geq 0$.*

2. *$T_d(-x) = (-1)^d T_d(x), \quad U_d(-x) = (-1)^d U_d(x)$.*

3. *For all $d \geq 0$, the Chebyshev polynomials satisfy the recurrence relation*

$$T_{d+2}(x) = xT_{d+1}(x) - T_d(x), \qquad U_{d+2}(x) = xU_{d+1}(x) - U_d(x).$$

4. *For all $d \geq 0$, the Chebyshev polynomials satisfy the trigonometric relations*

$$T_d(2\cos(\theta)) = 2\cos(d\theta), \qquad U_d(2\cos(\theta)) = \frac{\sin((d+1)\theta)}{\sin(\theta)}.$$

5. *For all $d \geq 1$, the Chebyshev polynomials are given by the explicit formulas*

$$T_d(x) = \sum_{k=0}^{\lfloor d/2 \rfloor} (-1)^k \frac{d}{d-k} \binom{d-k}{k} x^{d-2k}, \qquad U_d(x) = \sum_{k=0}^{\lfloor d/2 \rfloor} (-1)^k \binom{d-k}{k} x^{d-2k}.$$

6. *Equivalently,*

$$U_d(x) = \frac{\left(x + \sqrt{x^2-4}\right)^{d+1} - \left(x - \sqrt{x^2-4}\right)^{d+1}}{2^{d+1}\sqrt{x^2-4}} \quad \text{if} \quad x \neq \pm 2.$$

The key property is that these polynomials, like the power maps, commute under composition, leading to many interesting dynamical properties. For example, the Chebyshev polynomials are a rich source of permutation polynomials (see Lidl and Neideritter [26, Chapter 7]). It is also known that the iterated monodromy group of any Chebyshev polynomial is infinite dihedral [4, Proposition 5.6]. Other results relating to the dynamics of these polynomials can be found in Silverman [38, Chapter 6], Ih [19], and Ih and Tucker [20]. For our iterated towers, we take advantage of the fact that $T_\ell^n(x) = T_{\ell^n}(x)$, which gives us intimate access to the number fields at every level.

2.3 Dickson-(-1) polynomials

The Dickson polynomials have also been studied to the point where a book has been written on the subject [25]. As stated in the introduction, the Dickson polynomials are defined by

$$\mathcal{D}_{d,a}(z + a/z) = z^d + (a/z)^d,$$

which closely resembles the definition for $T_d(x)$. In fact, the Dickson family encompasses each of the previously mentioned families of maps. The specializations at $a = 0$ and $a = 1$ give the power maps and Chebyshev polynomials of the first kind, respectively:

$$\mathcal{D}_{d,0}(z) = z^d, \quad \text{and} \quad \mathcal{D}_{d,1}(z + 1/z) = z^d + z^{-d}.$$

There is also a Dickson polynomial of the second kind $\mathcal{E}_{d,a}(x)$, and like the Chebyshev polynomials, these Dickson polynomials satisfy a variety of relations.

Proposition 2.3.1.

1. $\mathcal{D}_{d,a^2}(ax) = a^d T_d(x), \quad \mathcal{E}_{d,a^2}(ax) = a^n U_n(x).$
2. $\mathcal{D}_{d,a}(x) = \sum_{k=0}^{\lfloor d/2 \rfloor} (-a)^k \frac{d}{d-k} \binom{d-k}{k} x^{d-2k}, \quad \mathcal{E}_{d,a}(x) = \sum_{k=0}^{\lfloor d/2 \rfloor} (-a)^k \binom{d-k}{k} x^{d-2k}.$
3. $\mathcal{D}_{d+2,a}(x) = x\mathcal{D}_{d+1,a}(x) - a\mathcal{D}_{d,a}(x), \quad \mathcal{E}_{d+2,a}(x) = x\mathcal{E}_{d+1,a}(x) - a\mathcal{E}_{d,a}(x).$
4. $\mathcal{D}_{de,a}(x) = \mathcal{D}_{d,a^n}(\mathcal{D}_{e,a}(x)).$

From now on, we will use $\mathcal{D}_d(x)$ to denote the Dickson polynomial of degree d specialized at $a = -1$. The Dickson-(-1) polynomials of odd degree are a third set of polynomials which commute under composition and thus are ideally situated for our study.

2.4 Generalized Rikuna polynomials

The generalized Rikuna polynomials differ from the previous families in that they are generated by the iteration of a rational map. Let $d > 2$ be a positive integer, and let K be a field of characteristic coprime to d. Let ζ be a primitive d-th root of unity in a fixed algebraic closure $\overline{K}$ of K. Assume further that $\zeta^+ := \zeta + \zeta^{-1} \in K$ but $\zeta \notin K$. Define the polynomials $P(x)$ and $Q(x) \in K[x]$ by

$$P(x;d) = \frac{\zeta^{-1}(x-\zeta)^d - \zeta(x-\zeta^{-1})^\ell}{\zeta^{-1} - \zeta} \quad \text{and} \quad Q(x;d) = \frac{(x-\zeta)^d - (x-\zeta^{-1})^d}{\zeta^{-1} - \zeta}.$$

In [32], Rikuna introduced an interesting family of simple polynomials defined by

$$r(x,t;d) = P(x;d) - tQ(x;d) \in K(t)[x],$$

where t is an indeterminate over K. The special case $d = 3$ and $t = s/3$ yields Shanks' "simplest cubic" polynomial, which parametrizes the cubic extensions of $\mathbf{Q}$. More generally, the Rikuna polynomial gives rise to cyclic extensions of order d over $K(t)$ that are not Kummer (since $\zeta \notin K$).

In [5], Chonoles, Cullinan, Hausman, Pacelli, Pegado, and Wei extend Rikuna's work to study dynamically generated extensions of $K(t)$, which are produced as follows. Set $\gamma(x; d) = P(x; d)/Q(x; d)$, then the *generalized Rikuna polynomial* is

$$r_n(x, t; d) = P_n(x; d) - tQ_n(x; d), \quad \text{where} \quad \gamma^n(x; d) = \frac{P_n(x; d)}{Q_n(x; d)} \tag{2.1}$$

is the n-fold iterate of γ expressed in lowest terms, and $P_n(x; d)$ is monic.

Prior to Rikuna, Shen and Washington [36, 37] we able to identify some units in extensions of $\mathbf{Q}(\zeta^+)$ generated by $r_n(x, a/p^n; d)$. The polynomials $P_n(x; d)$ and $Q_n(x; d)$ defined above coincide with the polynomials $R_n(x)$ and $S_n(x)$, respectively, defined in [37].

Here, we derive two expressions for $r_n(x, t; d)$ that do not appear in [5, 37]. These expressions give us a firm handle on the generalized Rikuna polynomials of large degree, which is key to studying the iterated extensions arising from these maps. The first is a generalization of [32, Corollary 2.6].

Proposition 2.4.1. *The generalized Rikuna polynomial is given by*

$$r_n(x, t; d) = \frac{(t - \zeta)(x - \zeta^{-1})^{d^n} - (t - \zeta^{-1})(x - \zeta)^{d^n}}{\zeta^{-1} - \zeta}.$$

Proof. Note that

$$\gamma(x; d) - \zeta = \frac{(\zeta^{-1} - \zeta)(x - \zeta)^d}{(x - \zeta)^d - (x - \zeta^{-1})^d}, \quad \text{and} \quad \gamma(x; d) - \zeta^{-1} = \frac{(\zeta^{-1} - \zeta)(x - \zeta^{-1})^d}{(x - \zeta)^d - (x - \zeta^{-1})^d}.$$

It now follows by induction on n that

$$\gamma^n(x; d) = \frac{\zeta^{-1}(x - \zeta)^{d^n} - \zeta(x - \zeta^{-1})^{d^n}}{(x - \zeta)^{d^n} - (x - \zeta^{-1})^{d^n}}.$$

We introduce a normalizing factor so that the numerator is monic:

$$P_n(x; d) = \frac{\zeta^{-1}(x - \zeta)^{d^n} - \zeta(x - \zeta^{-1})^{d^n}}{\zeta^{-1} - \zeta}, \quad Q_n(x; d) = \frac{(x - \zeta)^{d^n} - (x - \zeta^{-1})^{d^n}}{\zeta^{-1} - \zeta},$$

from which the result follows. □

The generalized Rikuna polynomial can also be expressed in terms of Chebyshev polynomials of the second kind.

Proposition 2.4.2. *The generalized Rikuna polynomial is given by*

$$r_n(x,t;d) = x^{d^n} - d^n t x^{d^n-1} + \sum_{k=2}^{d^n} (-1)^k \binom{d^n}{k} \Big(t\, U_{k-1}(\zeta^+) - U_{k-2}(\zeta^+) \Big) x^{d^n-k}.$$

Proof. Using binomial expansion and Proposition 2.2.1 (6), it is straightforward to see that

$$\begin{aligned} P_n(x;d) &= \frac{\zeta^{-1}(x-\zeta)^{d^n} - \zeta(x-\zeta^{-1})^{d^n}}{\zeta^{-1}-\zeta} = \sum_{k=0}^{d^n} (-1)^k \binom{d^n}{k} \frac{\zeta^{k-1} - \zeta^{-(k-1)}}{\zeta^{-1}-\zeta} x^{d^n-k} \\ &= x^{d^n} - \sum_{k=2}^{d^n} (-1)^k \binom{d^n}{k} U_{k-2}(\zeta^+) x^{d^n-k}, \quad \text{and} \\ Q_n(x;d) &= \frac{(x-\zeta)^{d^n} - (x-\zeta^{-1})^{d^n}}{\zeta^{-1}-\zeta} = \sum_{k=0}^{d^n} (-1)^k \binom{d^n}{k} \frac{\zeta^{k} - \zeta^{-k}}{\zeta^{-1}-\zeta} x^{d^n-k} \\ &= d^n x^{d^n-1} - \sum_{k=2}^{d^n} (-1)^k \binom{d^n}{k} U_{k-1}(\zeta^+) x^{d^n-k}. \end{aligned}$$

The result follows from Equation (2.1). □

CHAPTER 3

PRIME DECOMPOSITION

In this chapter we focus on the action of our maps (power, Chebyshev, Dickson, and generalized Rikuna) over finite fields. The graphs of these maps display a remarkable degree of symmetry, which we seek to describe. Some of these descriptions of graphs are already known. In addition to the graphs of permutation polynomials [24, 26], the graphs of the power maps over finite fields are described in [1, 6, 34, 42]; the graph of T_2 over $\mathbf{F}_p$ is also worked out in [42]. In this chapter, we determine the structure of the graphs for polynomials in the odd prime degree case. The graphs of the power maps, though already known, are here to serve as a model for the other cases. The graphs of the Chebyshev polynomials were worked out by the author in [14].

There is a certain uniformity across all of these graphs. In each graph, the periodic points are arranged into cycles of varying lengths. The preperiodic values are arranged into rooted trees, where the root is a periodic point in the graph. The *height* of a tree is the length of the longest path in the tree. In other words 'height' is synonymous with 'maximum preperiod'. For each component, every tree is *maximally branched* of a fixed height h. That is, the *indegree*—the number of incoming edges—of each vertex in the component of preperiod less than h is equal to the degree of the map; the indegree of the vertices of preperiod h is zero.

In each case, the orbits of the elements in a fixed finite field $\mathbf{F}_q$ are determined by the orders of elements in some cyclic subgroup of units in some finite extension of $\mathbf{F}_q$. The preperiods of the elements in $\mathbf{F}_q$ are determined by the ℓ-adic valuation of the order of this cyclic group.

The graphs give a visualization of the roots of our map modulo p, and thus we can determine the factorization of our polynomials modulo primes. By a classical result of Dedekind, the factorization gives the decomposition of the primes ideal $p\mathbf{Z}$ in the corresponding extensions. Dedekind's result may be stated as follows.

Theorem 3.0.3. *Let $K = \mathbf{Q}(\theta)$ be a number field, where θ is an algebraic integer with minimal polynomial f. Let p be a prime that does not divide* $\mathrm{ind}(f)$. *Write*

$$f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \pmod{p},$$

where $f_1, \ldots, f_r$ are distinct irreducible factors of f in $\mathbf{F}_p[x]$. Then the decomposition of $p\mathbf{Z}$ into prime ideals of $\mathcal{O}_K$ is $p\mathbf{Z} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where $\mathrm{norm}(\mathfrak{p}_i) = p^{\deg f_i}$.

3.1 Description of graphs

Throughout this chapter we fix ℓ to be an odd prime and $\mathbf{F}_q$ a finite field of characteristic p coprime to ℓ. We will always work with maps of prime degree, and from now on we use f to denote one of these maps:

$$f \in \{P_\ell, T_\ell, \mathcal{D}_\ell(x), \gamma(x;\ell)\}.$$

For each of these maps (P_ℓ, T_ℓ, $\mathcal{D}_\ell$, and γ), the forward orbits of the elements in $\mathbf{F}_q$ are determined by the orders of elements in some cyclic group, depending on the family of map.

We use $\mathrm{ord}(a, G)$ denote the order of a in the group G, we let ν_ℓ denote the usual ℓ-adic valuation. The graph of f over the field $\mathbf{F}_q$ will be denoted by $\mathcal{G}(f, q)$.

3.1.1 The graph $\mathcal{G}(P_\ell, q)$

In the case of the power map, the orbit of each unit $a \in \mathbf{F}_q^\times$ is determined by its multiplicative order in the group; the element 0 is fixed by the power map.

Proposition 3.1.1. *Let $a \in \mathbf{F}_q^\times$, and write* $\mathrm{ord}(a, \mathbf{F}_q^\times) = \ell^\lambda d$, *where* $\gcd(\ell, d) = 1$. *Then a is λ-preperiodic, and $P_\ell^\lambda(a)$ is* $\mathrm{ord}(\ell, (\mathbf{Z}/d\mathbf{Z})^\times)$*-periodic for P_ℓ.*

Proof. Suppose that a is m-preperiodic and $P_\ell^m(a)$ is n-periodic. Then

$$\begin{aligned} & P_\ell^{m+n}(a) - P_\ell^m(a) = 0 \\ \Leftrightarrow\ & a^{\ell^{m+n}} - a^{\ell^m} = 0 \\ \Leftrightarrow\ & a^{\ell^m}(a^{\ell^m(\ell^n-1)} - 1) = 0. \end{aligned}$$

Since a is a unit, the order of a divides $\ell^m(\ell^n - 1)$. Due to the minimality of m and n, it follows that $m = \lambda$ and $n = \mathrm{ord}(\ell, (\mathbf{Z}/\omega\mathbf{Z})^\times)$. □

Let φ denote the Euler totient function.

Theorem 3.1.2. *Write $q-1=\ell^\lambda\omega$, where $\gcd(\ell,\omega)=1$. The graph $\mathcal{G}(P_\ell,q)$ contains*

- *one fixed point: 0,*
- *$\varphi(d)$ periodic values of period $\operatorname{ord}(\ell,(\mathbf{Z}/d\mathbf{Z})^\times)$ for each divisor d of ω,*
- *$\omega(\ell-1)\ell^{k-1}$ k-preperiodic values for each $1\le k\le\lambda$.*

Moreover, for each preperiod k, the indegree is constant—the only exception being the vertex 0.

Proof. By Proposition 3.1.1, the orbits of the elements of $\mathbf{F}_q$ are determined by the orders of these elements in $\mathbf{F}_q^\times$. This group is cyclic of order $q-1$, hence there are $\varphi(d)$ elements of order d for each divisor d of $q-1$. The preperiod of each of these elements is determined by $\nu_\ell(d)$; the periodic elements correspond to the divisors coprime to ℓ. The constant indegree essentially follows from the fact that the indegree of any vertex cannot exceed the degree of the map. □

3.1.2 The graph $\mathcal{G}(T_\ell,q)$

The critical points for the Chebyshev polynomials are -2 and 2. For all other elements of $a\in\mathbf{F}_q$, the orbit of a is determined by the order of $\alpha\in\mathbf{F}_{q^2}^\times$, where α is a root of $u_a(x)=x^2-ax+1$. That is, $a=\alpha+\alpha^{-1}$.

Proposition 3.1.3. *Let $a\in\mathbf{F}_q\setminus\{\pm2\}$ and $\alpha\in\mathbf{F}_{q^2}^\times$ be a root of $u_a(x)$. Write $\operatorname{ord}(\alpha,\mathbf{F}_{q^2}^\times)=\ell^\lambda d$, where $\gcd(\ell,d)=1$. Then a is λ-preperiodic, and $T_\ell^\lambda(a)$ is $\operatorname{ord}(\ell,(\mathbf{Z}/d\mathbf{Z})^\times/(\pm1))$-preperiodic.*

Proof. Suppose that a is m-preperiodic, and $T_\ell^m(a)$ is n-periodic. Then

$$\begin{aligned}
T_\ell^{n+m}(a)=T_\ell^m(a) \quad &\Leftrightarrow \quad \alpha^{\ell^{n+m}}+\alpha^{-\ell^{n+m}}=\alpha^{\ell^m}+\alpha^{-\ell^m}\\
&\Leftrightarrow \quad \alpha^{\ell^{n+m}}\alpha^{\ell^{n+m}}-\alpha^{\ell^m}\alpha^{\ell^{n+m}}-\alpha^{-\ell^m}\alpha^{\ell^{n+m}}+1=0\\
&\Leftrightarrow \quad \left(\alpha^{\ell^{n+m}}-\alpha^{\ell^m}\right)\left(\alpha^{\ell^{n+m}}-\alpha^{-\ell^m}\right)=0\\
&\Leftrightarrow \quad \alpha^{\ell^{n+m}}=\alpha^{\ell^m} \quad \text{or} \quad \alpha^{\ell^{n+m}}=\alpha^{-\ell^m}\\
&\Leftrightarrow \quad \alpha^{\ell^m(\ell^n-1)}=1 \quad \text{or} \quad \alpha^{\ell^m(\ell^n+1)}=1\\
&\Leftrightarrow \quad \ell^\lambda d\mid\ell^m(\ell^n-1) \quad \text{or} \quad \ell^\lambda d\mid\ell^m(\ell^n+1),
\end{aligned}$$

which implies that $\lambda\mid m$ and $\ell^n\equiv\pm1\pmod d$. Due to the minimality of n and m, it follows that $m=\lambda$ and $n=\operatorname{ord}(\ell,(\mathbf{Z}/d\mathbf{Z})^\times/(\pm1))$. □

Note that if u_a is irreducible, the roots of u_a are permuted by the Frobenius endomorphism. That is, $\alpha^q = \alpha^{-1}$, hence α is an element of the cyclic subgroup of order $q+1$. Otherwise u_a is reducible, and $\alpha \in \mathbf{F}_q^\times$. Thus the orbits of the elements in $\mathbf{F}_q$ are determined by the orders of the $q+1$ and $q-1$ roots of unity in $\mathbf{F}_{q^2}^\times$. Note that there is a correspondence between pairs $(\alpha, \alpha^{-1}) \in \mathbf{F}_{q^2} \times \mathbf{F}_{q^2}$ and elements $a \in \mathbf{F}_q$, with exception when $\alpha = \alpha^{-1}$. That is, $\alpha \in \{-1, 1\}$ which corresponds to the critical points of T_ℓ: $a \in \{-2, 2\}$. Since these unit groups are cyclic, we can easily count the number of elements of each cycle type. Set

$$q - 1 = \ell^{\lambda^-}\omega^- \quad \text{and} \quad q + 1 = \ell^{\lambda^+}\omega^+$$

where $\gcd(\ell, \omega^-) = \gcd(\ell, \omega^+) = 1$.

Theorem 3.1.4. *The graph $\mathcal{G}(T_\ell, q)$ contains*

- *two fixed points: -2 and 2; the height of the trees attached to these fixed points is $\max\{\lambda^-, \lambda^+\}$,*
- *$\varphi(d)/2$ periodic elements of period $\operatorname{ord}(\ell, (\mathbf{Z}/d\mathbf{Z})^\times/(\pm 1))$ for each divisor d of ω^-; the height of the trees attached to these periodic values is λ^-,*
- *$\varphi(d)/2$ periodic elements of period $\operatorname{ord}(\ell, (\mathbf{Z}/d\mathbf{Z})^\times/(\pm 1))$ for each divisor d of ω^+; the height of the trees attached to these periodic values is λ^+.*

In other words,

- *the components containing -2 and 2 each contain $(\ell-1)\ell^{k-1}/2$ preperiodic elements of preperiod k for each $1 \le k \le \max\{\lambda^-, \lambda^+\}$;*
- *there are a total of $(\ell-1)\ell^{k-1}$ elements of preperiod k for each $1 \le k \le \lambda^-$ contained in the components corresponding to divisors of ω^-;*
- *there are a total of $(\ell-1)\ell^{k-1}$ elements of preperiod k for each $1 \le k \le \lambda^+$ contained in the components corresponding to divisors of ω^+.*

Proof. The proof is similar to Theorem 3.1.2 using Proposition 3.1.3 and the theory cyclic groups—the difference begin that each divisor d only corresponds to $\varphi(d)/2$ elements, which comes from the 2-to-1 correspondence between elements of $\mathbf{F}_{q^2}^\times$ and elements of $\mathbf{F}_q$. □

Example 3.1.5. Using Theorem 3.1.4 we determine the structure of the graph of T_3 over $\mathbf{F}_{53}$ by considering the divisors of 52 and 54 ($p-1$ and $p+1$, respectively). The graph is shown in Figure

2. When the degree of the Chebyshev polynomial is odd, the values -2, 0, and 2 are fixed, and we have labeled these values on the graph. Double arrows indicate double roots.

$\ell = 3, p = 53, n = 1$				
Divisors of 52	Number of points in $\mathbf{F}_{53}$	Period	Preperiod	Cycles of this type
4	1	1	0	1
13	6	3	0	2
26	6	3	0	2
52	12	6	0	2
Divisors 54				
1	1	1	0	1
3	1	-	1	
9	3	-	2	
27	9	-	3	
2	1	1	0	1
6	1	-	1	
18	3	-	2	
54	9	-	3	

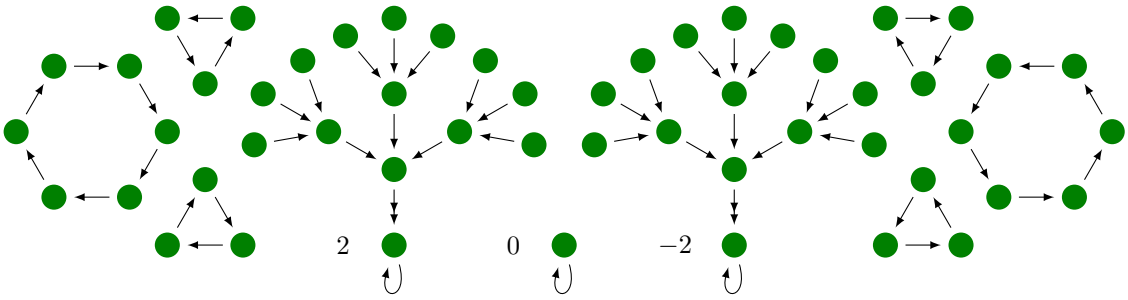


Figure 2: $\mathcal{G}(T_3, 53)$.

3.1.3 The graph $\mathcal{G}(\mathcal{D}_\ell, q)$

The critical points of the Dickson polynomial are $\pm\sqrt{-4}$, which may or may not be contained in $\mathbf{F}_q$, depending on the equivalence class of q modulo 4. Regardless, for the elements of $a \in \mathbf{F}_q \setminus \{\pm\sqrt{-4}\}$, the orbit of a is determined by the order of $\alpha \in \mathbf{F}_{q^2}^\times$, where α is a root of $u_a(x) = x^2 - ax - 1$. That is, $a = \alpha - \alpha^{-1}$. Although this is similar to the Chebyshev case, the twist adds an rather significant nuance. In the Chebyshev case, the orders of α and α^{-1} are always equal. For the Dickson maps, that is not the case: the order of α may differ by a factor of 2 from the order of α^{-1}. Define $c_d(\ell)$ to be the smallest positive integer for which

$$\ell^{c_d(\ell)} \equiv 1 \pmod{d} \quad \text{or} \quad \ell^{c_d(\ell)} \equiv d/2 - 1 \pmod{d}.$$

Proposition 3.1.6. *For any $a \in \mathbf{F}_q$, write $a = \alpha - \alpha^{-1}$ as above, and put $\operatorname{ord}(\alpha) = \ell^\lambda d$ where $\gcd(\ell, d) = 1$. Then a is λ-preperiodic and $\mathcal{D}_\ell^\lambda(a)$ is $c_d(\ell)$-periodic.*

Proof. Suppose that $a \in \mathbf{F}_q$ is m-preperiodic and $\mathcal{D}_\ell^m(a)$ is n-periodic. Then

$$\begin{aligned}
\mathcal{D}_\ell^{m+n}(\alpha - \alpha^{-1}) - \mathcal{D}_\ell^m(\alpha - \alpha^{-1}) &= 0 \\
\alpha^{\ell^{m+n}} - \alpha^{-\ell^{m+n}} - \alpha^{\ell^m} + \alpha^{-\ell^m} &= 0 \\
\alpha^{\ell^{m+n}+\ell^m} - \alpha^{-\ell^{m+n}+\ell^m} - \alpha^{\ell^m+\ell^m} + \alpha^{-\ell^m+\ell^m} &= 0 \\
\alpha^{2\ell^m} - \alpha^{\ell^m}\alpha^{\ell^{m+n}} + \alpha^{\ell^m}\alpha^{-\ell^{m+n}} - 1 &= 0 \\
\left(\alpha^{\ell^m} - \alpha^{\ell^{m+n}}\right)\left(\alpha^{\ell^m} + \alpha^{-\ell^{m+n}}\right) &= 0.
\end{aligned}$$

Thus either

$$\begin{aligned}
&\text{Case 1: } \alpha^{\ell^m} = \alpha^{\ell^{m+n}} \Leftrightarrow \alpha^{\ell^m(\ell^n-1)} = 1 \Leftrightarrow \ell^\lambda d \mid \ell^m(\ell^n - 1) \Leftrightarrow \lambda \mid m \text{ and } d \mid \ell^n - 1; \quad \text{or} \\
&\text{Case 2: } \alpha^{\ell^m} = -\alpha^{-\ell^{m+n}} \Leftrightarrow \alpha^{\ell^m(\ell^n+1)} = -1 \Leftrightarrow \ell^\lambda d \mid 2\ell^m(\ell^n + 1) \text{ and } \ell^\lambda d \nmid \ell^m(\ell^n + 1) \\
&\qquad \Leftrightarrow \lambda \mid m \text{ and } \omega \mid 2(\ell^n + 1) \text{ and } d \nmid \ell^n + 1.
\end{aligned}$$

By the minimality of m, we have $\lambda = m$, and by the minimality of n, we have $n = c_d(\ell)$. □

Note that $u(x) = x^2 - ax - 1$ is reducible modulo p if and only if $\alpha \in \mathbf{F}_q^\times$, if and only if $\operatorname{ord}(\alpha) \mid q - 1$. Additionally, $u(x) = x^2 - ax - 1$ is irreducible modulo p if and only if α is a $2(q+1)$ root of unity, but not a $(q+1)$ root of unity. Since these groups are cyclic, the elements of the group can be categorized by divisors of $q - 1$ and $2(q + 1)$.

Let D_q^- be the set of divisors of $q - 1$, and let D_q^+ be the set of divisors of $2(q + 1)$ that do not divide $q + 1$. Each divisor $d \in D_q^- \cup D_q^+$ corresponds to $\varphi(d)$ elements of $\mathbf{F}_{q^2}^\times$. The map $\tau\colon \mathbf{F}_{q^2}^\times \to \mathbf{F}_q$ defined by $\tau(\alpha) = \alpha - \alpha^{-1}$ is two-to-one everywhere except where $\alpha = -\alpha^{-1}$, that is, $\alpha = \pm\sqrt{-1}$. Furthermore, it is easy to check that the order $\operatorname{ord}(\alpha)$ is odd if and only if $\operatorname{ord}(-\alpha^{-1}) = 2\operatorname{ord}(\alpha)$. Otherwise $\operatorname{ord}(\alpha) = \operatorname{ord}(-\alpha^{-1})$.

Notation 3.1.7. Write $q - 1 = \ell^{\lambda^-}\omega^-$ and $2(q + 1) = \ell^{\lambda^+}\omega^+$, and define the additional sets of divisors

$$\begin{aligned}
S_1 &= \{d \mid \omega^- \colon \nu_2(d) = 0\} \\
S_2 &= \{d \mid \omega^- \colon \nu_2(d) \geq 2\} \\
S_3 &= \{d \mid \omega^+ \colon d \nmid q + 1\}.
\end{aligned}$$

The periodic elements of $\mathbf{F}_q$ are in correspondence with the divisors $d \in S_1 \cup S_2 \cup S_3$ according to the table in Figure 3. By Proposition 3.1.6, the preperiodic values attached to cycles of length $c_d(\ell)$ correspond to the divisors of the form $\ell^\lambda d$ where $d \in S_1 \cup S_2 \cup S_3$ and $1 \leq \lambda \leq \lambda^\pm$. If $d \in S_1$, the divisor $\ell^\lambda d$ corresponds to $\varphi(\ell^\lambda d) = (\ell-1)\ell^{\lambda-1}\varphi(d)$ elements. Else, if $d \neq 4$, $\ell^\lambda d$ corresponds to $\varphi(\ell^\lambda d)/2 = (\ell-1)\ell^{\lambda-1}\varphi(d)/2$ elements. In both of these cases, we see that there are $(\ell-1)\ell^{\lambda-1}$ elements of preperiod λ for each $c_d(\ell)$-periodic value. The divisor $d = 4$ corresponds to the special values $\pm 2\sqrt{-1} \in \mathbf{F}_q$; all but one of the preimages of $\pm 2\sqrt{-1}$ have multiplicity 2. It follows that the indegree of every vertex in the graph, counting multiplicity, is ℓ if and only if the vertex is not of maximal preperiod in its component. The maximal preperiod for each component is determined by the divisor d, and is given in the table in Figure 3. In summary,

Theorem 3.1.8. *Let $c_d(\ell)$, S_1, S_2, and S_3 be defined as above. The graph of $\mathcal{D}_\ell$ over $\mathbf{F}_q$ contains*

- *$\varphi(d)/c_d(\ell)$ cycles of length $c_d(\ell)$ for each divisor $d \in S_1$; the height of the trees attached to these cycles is λ^-,*
- *$\varphi(d)/(2c_d(\ell))$ cycles of length $c_d(\ell)$ for each divisor $d \in S_2 \setminus \{4\}$; the height of the trees attached to these cycles is λ^-,*
- *$\varphi(d)/(2c_d(\ell))$ cycles of length $c_d(\ell)$ for each divisor $d \in S_3 \setminus \{4\}$; the height of the trees attached to these cycles is λ^+,*
- *2 periodic elements of period $c_4(\ell)$ if $4 \in S_2 \cup S_3$; the height of the trees attached to these periodic values is $\max\{\lambda^-, \lambda^+\}$.*

Divisor	# elements in $\mathbf{F}_q$	Period	Maximal preperiod
$d \in S_1$	$\varphi(d)$	$c_d(\ell)$	λ^-
$d \in S_2 \setminus \{4\}$	$\varphi(d)/2$	$c_d(\ell)$	λ^-
$d \in S_3 \setminus \{4\}$	$\varphi(d)/2$	$c_d(\ell)$	λ^+
$d = 4 \in S_2 \cup S_3$	2	$c_d(\ell)$	$\max\{\lambda^-, \lambda^+\}$

Figure 3: Periodic elements categorized by divisor.

3.1.4 The graph $\mathcal{G}(\gamma, q)$

Let ℓ be an odd prime, ζ be a primitive ℓ-th root of unity, and $\zeta^+ = \zeta + \zeta^{-1}$. Since γ is a rational map, we work over $\mathbb{P}^1(\mathbf{F}_q) := \mathbf{F}_q \cup \{\infty\}$.

Proposition 3.1.9. *Fix a representative ζ in a fixed algebraic closure $\overline{\mathbf{F}}_q$. For $a \in \mathbb{P}^1(\mathbf{F}_q) \setminus \{\zeta, \zeta^{-1}\}$, let $\alpha_a = (a-\zeta)/(a-\zeta^{-1}) \in \mathbf{F}_q(\zeta)^\times$, and write $\operatorname{ord}(\alpha_a, \mathbf{F}_q(\zeta)^\times) = \ell^\lambda d$, where $\gcd(\ell, \omega) = 1$. Then a is λ-prepperiodic, and $\gamma^\lambda(a)$ is $\operatorname{ord}(\ell, (\mathbf{Z}/d\mathbf{Z})^\times))$-periodic.*

Proof. Suppose $a \in \mathbf{F}_q$ is m-prepperiodic and $\varphi^m(a)$ is n-periodic. Then

$$\begin{aligned} 0 &= \varphi^{m+n}(a) - \varphi^m(a) \\ &= \frac{\zeta^{-1}(x-\zeta)^{\ell^{m+n}} - \zeta(a-\zeta^{-1})^{\ell^{m+n}}}{(a-\zeta)^{\ell^{m+n}} - (a-\zeta^{-1})^{\ell^{m+n}}} - \frac{\zeta^{-1}(a-\zeta)^{\ell^m} - \zeta(a-\zeta^{-1})^{\ell^m}}{(a-\zeta)^{\ell^m} - (a-\zeta^{-1})^{\ell^m}}, \end{aligned}$$

which simplifies to

$$(\zeta - \zeta^{-1}) \left[(a-\zeta)(a-\zeta^{-1})\right]^{\ell^m} \left((a-\zeta)^{\ell^m(\ell^n-1)} - (a-\zeta^{-1})^{\ell^m(\ell^n-1)}\right) = 0.$$

Since $a \notin \{\zeta, \zeta^{-1}\}$, we conclude that

$$\left(\frac{a-\zeta}{a-\zeta^{-1}}\right)^{\ell^m(\ell^n-1)} = 1.$$

By the minimality of m and n, it follows that $m = \nu_\ell(\operatorname{ord}\alpha)$ and $n = c_d(\ell)$. □

We are now able to describe the orbits of every element of $\mathbb{P}^1(\mathbf{F}_q) := \mathbf{F}_q \cup \{\infty\}$.

Theorem 3.1.10. *Let $\mathbf{F}_q$ be a finite field of characteristic $p \neq \ell$ containing ζ, a primitive ℓ-th root of unity. Write $q - 1 = \ell^\lambda \omega$. The graph of γ over $\mathbb{P}^1(\mathbf{F}_q)$ contains*

- *two fixed points, ζ and ζ^{-1},*
- *$\varphi(d)$ periodic values of period $\operatorname{ord}(\ell, (\mathbf{Z}/d\mathbf{Z})^\times)$ for each divisor d of ω,*
- *$\omega(\ell-1)\ell^{k-1}$ values of preperiod k for each $1 \leq k \leq \lambda$.*

Proof. The transformation $x \mapsto \frac{x-\zeta}{x-\zeta^{-1}}$ is a homomorphism of $\mathbb{P}^1(\mathbf{F}_q)$, and in particular $\{\alpha_x : x \in \mathbb{P}^1(\mathbf{F}_q) \setminus \{\zeta, \zeta^{-1}\}\} = \mathbf{F}_q^\times$, which is a cyclic group of order $q-1$. The result now follows from Proposition 3.1.9 and the theory of cyclic groups. □

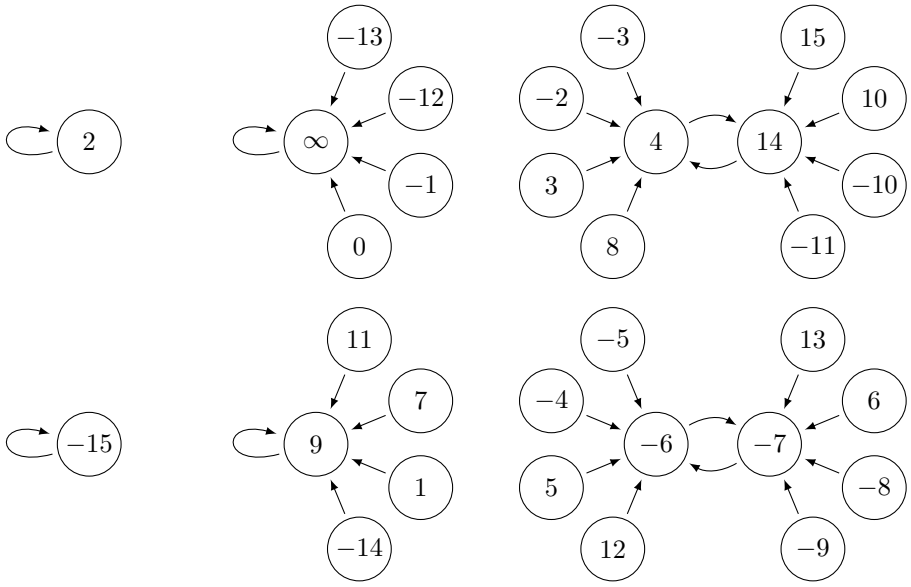
Example 3.1.11. Consider the action of $\varphi(x;5)$ acting on $\mathbb{P}^1(\mathbf{F}_{31})$. Fix 2 as our representative for a primitive 5-th root of unity so that

$$\varphi(x;5) = \frac{\frac{1}{2}(x-2)^5 - 2(x-\frac{1}{2})^5}{(x-2)^5 - (x-\frac{1}{2})^5} \in \mathbf{F}_{31}[x].$$

By Theorem 3.1.10 the cycle structure is determined by the divisors of 30 as follows.

Divisor of 30 d	Number of elements $\varphi(d)$	Period $\mathrm{ord}(\ell, (\mathbf{Z}/d\mathbf{Z})^\times)$ if $\gcd(\ell, d) = 1$	Preperiod $\nu_\ell(d)$
1	1	1	0
5	4	-	1
2	1	1	0
10	4	-	1
3	2	2	0
15	8	-	1
6	2	2	0
30	8	-	1

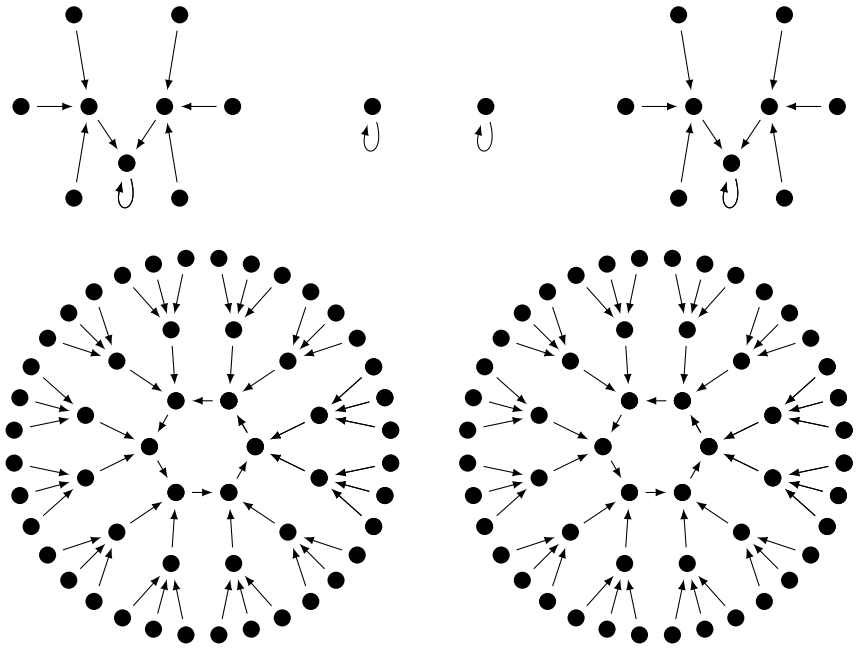
The graph of $\gamma(x; 5)$ over $\mathbb{P}^1(\mathbf{F}_{31})$:



Example 3.1.12. Consider the map $\gamma(x; 3)$ over $\mathbb{P}^1(\mathbf{F}_{127})$, and take 19 as our representative for a primitive cube root of unity. According to Theorem 3.1.10, the cycle structure is as follows.

Divisor of 126 d	Number of elements $\varphi(d)$	Period $\mathrm{ord}(\ell, (\mathbf{Z}/d\mathbf{Z})^\times)$ if $\gcd(\ell, d) = 1$	Preperiod $\nu_\ell(d)$
1	1	1	0
3	2	-	1
9	6	-	2
2	1	1	0
6	2	-	1
18	6	-	2
7	6	6	0
21	12	-	1
63	36	-	2
14	6	6	0
42	12	-	1
126	36	-	2

The graph of $\gamma(x; 3)$ over $\mathbb{P}^1(\mathbf{F}_{127})$:



3.2 Weights

We now turn to the factorization of our maps modulo primes using the graphs described in the previous section. The key observation is that $a \in \mathbf{F}_q$ is a root of $f^n(x) - t$ if and only if there is a path of length n from a to $\bar{t}$. Thus one way to recognize the roots of $f^n(x) - t$ is to determine the smallest q for which the graph of f over $\mathbf{F}_q$ contains all the roots of $f^n(x) - t$. It is possible that the various roots of $f^n(x) - t$ are contained different subfields of $\mathbf{F}_q$, so as we construct these graphs, we must keep track of the degree of the extension each root generates. To avoid any confusion between the graph theoretic and number theoretic notions of 'degree', we use the term *weight* to denote the exact degree of a vertex over $\mathbf{F}_p$. That is, for $a \in \mathcal{G}(f, q)$,

$$\text{weight}(a) = [\mathbf{F}_p(a) \colon \mathbf{F}_p].$$

In order to ensure that the graph of f over $\mathbf{F}_q$ contains paths of length n terminating at $\bar{t}$, we must look for a graph that contains preperiodic elements with preperiod equal to n plus the preperiod of $\bar{t}$. From the previous section, we know that the preperiod of an element is determined by the ℓ-adic valuation of $q \pm 1$, depending on the map. Thus this question is reduced to understanding the ℓ-adic valuation of $p^n \pm 1$ as n varies.

For any prime p different than ℓ, let μ^- be the minimal positive integer for which $p^{\mu^-} \equiv 1 \pmod{\ell}$, and let μ^+ be the minimal positive integer for which $p^{\mu^+} \equiv -1 \pmod{\ell}$, if it exists. Otherwise, set $\mu^+ = \infty$.

Lemma 3.2.1. *We have*

$$\nu_\ell(p^n - 1) = \begin{cases} \nu_\ell(p^{\mu^-} - 1) + \nu_\ell(n) & \text{if } \mu^- \mid n \\ 0 & \text{otherwise;} \end{cases} \tag{3.1}$$

$$\nu_\ell(p^n + 1) = \begin{cases} \nu_\ell(p^{\mu^+} + 1) + \nu_\ell(n) & \text{if } \mu^+ \mid n \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

Proof. For (3.1), $p^n \equiv 1 \pmod{\ell}$ if and only if $\mu^- \mid n$. Assume $\mu^- \mid n$ and write $n = k\mu^-$. Then

$$p^n - 1 = p^{k\mu^-} - 1 = (p^{\mu^-} - 1)\Big((p^{\mu^-})^{k-1} + (p^{\mu^-})^{k-2} + \cdots + 1\Big),$$

thus

$$\nu_\ell(p^n - 1) = \nu_\ell(p^{\mu^-} - 1) + \nu_\ell\Big((p^{\mu^-})^{k-1} + (p^{\mu^-})^{k-2} + \cdots + 1\Big)$$

$$= \nu_\ell(p^{\mu^-} - 1) + \nu_\ell(k) = \nu_\ell(p^{\mu^-} - 1) + \nu_\ell(k\mu^-) = \nu_\ell(p^{\mu^-} - 1) + \nu_\ell(n).$$

For (3.2), μ^+ exists only if the order of p in $\mathbf{F}_\ell^\times$ is even. If the order of p is even, then $p^n \equiv -1 \pmod{\ell}$ if and only if $\mu^+ \mid n$. In fact, n must be an odd multiple of μ^+ since the order of p is $2\mu^+$. Write $n = k\mu^+$, where k is an odd integer. Then

$$p^n + 1 = (p^{\mu^+} + 1)\Big((p^{\mu^+})^{k-1} - (p^{\mu^+})^{k-2} + (p^{\mu^+})^{k-3} - \cdots + 1\Big).$$

It follows form the same argument as above that $\nu_\ell(p^n + 1) = \nu_\ell(p^{\mu^+} + 1) + \nu_\ell(n)$. □

This lemma tells us that, initially, there is a jump in preperiod that is dictated by the ℓ-adic valuation of $p^{\mu^-} - 1$ and $p^{\mu^+} + 1$. Afterwards, the maximum preperiod can only be increased by increasing the degree of the extension by ℓ. Thus we have the following correspondence between the weight and preperiod of the vertices in the graphs.

Proposition 3.2.2. *Consider the components of $\mathcal{G}(P, q)$ that contain elements of $\mathbf{F}_p$. The weights of elements in these components is given by*

	Components of $\mathcal{G}(P, q)$ corresponding to divisors of $p^{\mu^-} - 1$
Preperiod ρ	Weight
$\rho = 0$	1
$1 \le \rho \le \nu_\ell(p^{\lambda^-} - 1)$	μ^-
$\rho = \nu_\ell(p^{\lambda^-} - 1) + k$	$\ell^k\mu^-$

Proof. The result follows from Theorem 3.1.2 and Lemma 3.2.1. □

Proposition 3.2.3. *Consider the components of $\mathcal{G}(T, q)$ that contain elements of $\mathbf{F}_p$. The weights of elements in these components is given by*

If $\mu^- < \mu^+$	Components of $\mathcal{G}(T, q)$ corresponding to divisors of $p^{\mu^-} - 1$	Components of $\mathcal{G}(T, q)$ corresponding to divisors of $p^{\mu^-} + 1$
Preperiod ρ	Weight	Weight
$\rho = 0$	1	1
$1 \le \rho \le \nu_\ell(p^{\lambda^-} - 1)$	μ^-	$2\mu^-$
$\rho = \nu_\ell(p^{\lambda^-} - 1) + k$	$\ell^k\mu^-$	$2\ell^k\mu^-$

If $\mu^+ < \mu^-$	Components of $\mathcal{G}(T,q)$ corresponding to divisors of $p^{\mu^+}+1$	Components of $\mathcal{G}(T,q)$ corresponding to divisors of $p^{\mu^+}-1$
Preperiod ρ	Weight	Weight
$\rho = 0$	1	1
$1 \le \rho \le \nu_\ell(p^{\lambda^+}+1)$	μ^+	$2\mu^+$
$\rho = \nu_\ell(p^{\lambda^+}+1)+k$	$\ell^k\mu^+$	$2\ell^k\mu^+$

Proof. The result follows from Theorem 3.1.4 and Lemma 3.2.1. □

Example 3.2.4. Returning to the previous example where $\ell = 3$ and $p = 53$, we have $\mu^+ = 1$ and $\mu^- = 2$. As we saw in Figure 2, the cycles corresponding to divisors of 54 have trees of height 3, and the cycles corresponding to divisors of 52 have trees of height 0. Over the finite field of order 53^{18}, all components have trees of height 5. A table of weights is given in Figure 4. Also see Figure 5.

Preperiod	Weights of elements in components corresponding to divisors of 54	Weights of elements in components corresponding to divisors of 52
0	1	1
1	1	2
2	1	2
3	1	2
4	3	6
5	9	18

Figure 4: Table of weights for $\mathcal{G}(T_3, 53^{18})$.

Proposition 3.2.5. *Consider the components of $\mathcal{G}(\mathcal{D},q)$ that contain elements of $\mathbf{F}_p$. The weights of elements in these components is given by*

If $\mu^- < \mu^+$	Components of $\mathcal{G}(\mathcal{D},q)$ corresponding to divisors of $p^{\mu^-}-1$	Components of $\mathcal{G}(\mathcal{D},q)$ corresponding to divisors of $2(p^{\mu^-}+1)$
Preperiod ρ	Weight	Weight
$\rho = 0$	1	1
$1 \le \rho \le \nu_\ell(\lambda^- - 1)$	μ^-	$2\mu^-$
$\rho = \nu_\ell(\lambda^- - 1)+k$	$\ell^k\mu^-$	$2\ell^k\mu^-$

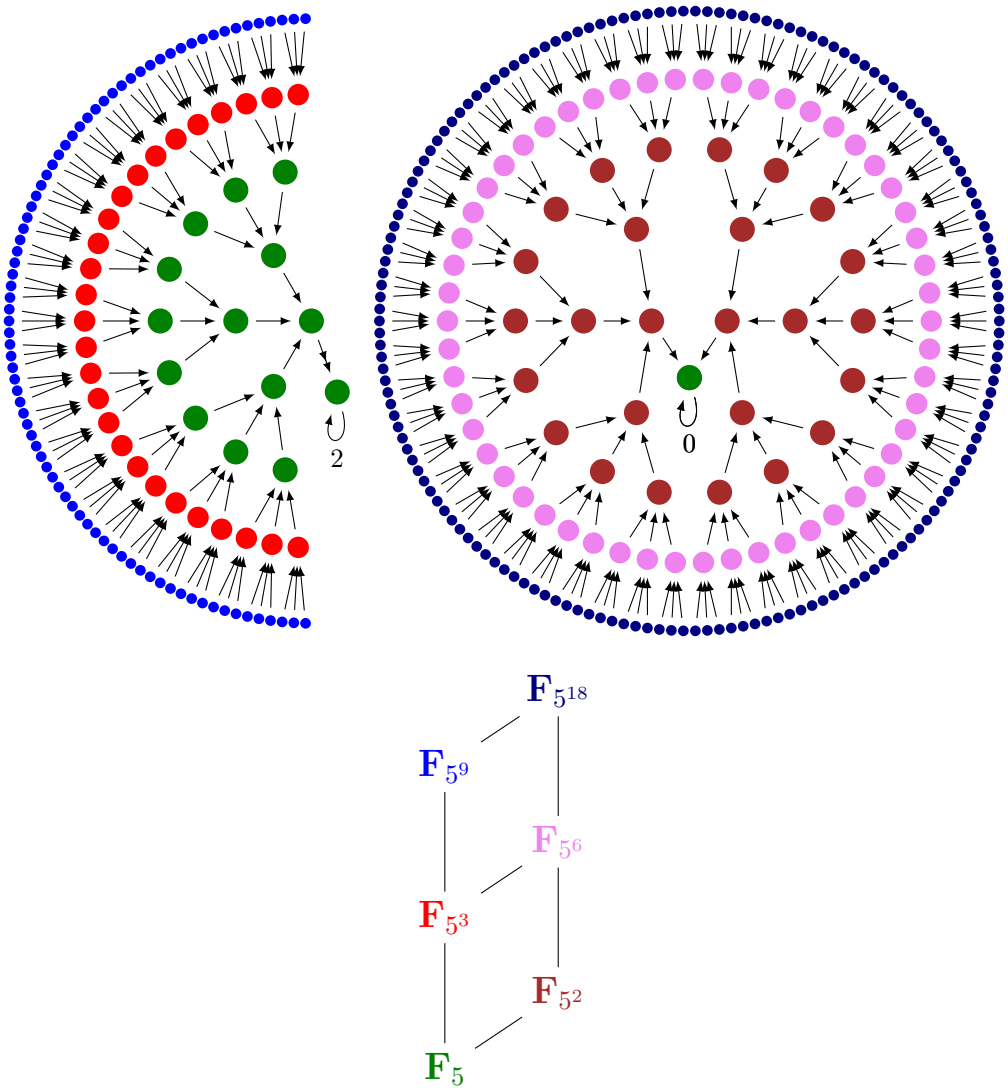


Figure 5: Selected components of $\mathcal{G}(T_3, 53^{18})$ colored by weight.

If $\mu^+ < \mu^-$	Components of $\mathcal{G}(\mathcal{D}, q)$ corresponding to divisors of $p^{\mu^+} - 1$	Components of $\mathcal{G}(\mathcal{D}, q)$ corresponding to divisors of $2(p^{\mu^+} + 1)$
Preperiod ρ	Weight	Weight
$\rho = 0$	1	1
$1 \leq \rho \leq \nu_\ell(\lambda^+ + 1)$	$2\mu^+$	μ^+
$\rho = \nu_\ell(\lambda^+ + 1) + k$	$2\ell^k\mu^+$	$\ell^k\mu^+$

Proof. The result follows from Theorem 3.1.8 and Lemma 3.2.1. □

Example 3.2.6. We consider the graphs of $\mathcal{D}_3$ over finite fields of characteristic 7. Here $7^1 - 1 \equiv 0 \pmod 7$, so $\mu^- = 3$ and $\mu^+ = \infty$. Recall that the structure of the components of the graph of determined by the divisors of $q-1$ and the divisors of $2(q+1)$ that do not divide $q+1$. Each divisor d corresponds to $\varphi(d)/2$ elements (with exception to $d = 4$). Each odd divisor d is in correspondence with the divisor $2d$, so together, the pair of divisors $(d, 2d)$ corresponds to $\varphi(d)$ elements. The preperiod of each element is the ℓ-valuation of its divisor, and each periodic element has period $c_d(\ell)$. The divisors corresponding to the elements of $\mathbf{F}_7$ are shown in Figure 6. The components of $G(\mathcal{D}_3, 7^{18})$ containing elements of $\mathbf{F}_7$ are shown in Figure **??**.

Divisors of D_7^-	# of elements of $\mathbf{F}_7$	Period	Preperiod	Weight
1, 2	1	1	0	1
3, 6	2	-	1	1
Divisors of D_7^+				
16	4	4	0	1

Figure 6: Components of $\mathcal{G}(\mathcal{D}_3, 7)$.

3.3 Decomposition of primes.

We now use Theorem 3.0.3 in conjunction with the theory of the graphs developed in the previous section to describe the decomposition of primes in our iterated extensions.

3.3.1 Decomposition in radical extensions

Theorem 3.3.1. *Let ℓ be an odd prime and let p be a prime different from ℓ. Let $\mu = \operatorname{ord}(p, (\mathbf{Z}/\ell\mathbf{Z})^\times)$, let $m_p = \nu_\ell(p^\mu - 1)$, and let ρ be the preperiod of $\bar{t} \in \mathbf{F}_p$. The factorization of $P_\ell^n(x) - t$ modulo p is as follows.*

1. *If $t \equiv 0 \pmod p$, then $P_\ell^n(x) - t \equiv x^{\ell^n} \pmod p$.*
2. *If $t \not\equiv 0 \pmod p$ is periodic ($\rho = 0$), and $n \leq m_p$, then $P_\ell^n(x) - t$ factors into*
   (a) *one factor of degree 1, and*
   (b) *$\sum_{k=1}^{n} (\ell - 1)\ell^{k-1}/\mu$ factors of degree μ.*
3. *If $t \not\equiv 0 \pmod p$ is periodic ($\rho = 0$), and $n > m_p$, then $P_\ell^n(x) - t$ factors into*

(a) *one factor of degree 1,*

(b) $\sum_{k=1}^{m_p}(\ell-1)\ell^{k-1}/\mu$ *factors of degree* μ*, and*

(c) $(\ell-1)\ell^{m_p-1}/\mu$ *factors of degree* $\mu\ell^k$ *for each* $1 \le k \le n-m_p$.

4. *If* t *is strictly preperiodic* ($\rho > 0$) *and* $n \le m_p - \rho$*, then* $P_\ell^n(x) - t$ *splits completely into factors of degree 1.*

5. *If* t *is strictly preperiodic* ($\rho > 0$) *and* $n > m_p - \rho$*, then* $P_\ell^n(x) - t$ *factors into* $\ell^{m_p-\rho}$ *factors of degree* $\ell^{n-m_p+\rho}$.

Proof. The result is essentially a direct consequence of Proposition 3.2.2. Again, the roots of $P_\ell^n(x) - t$ are precisely the elements in the graph whose distance from $\bar{t}$ is n. These roots will lie at varying preperiods, and from Proposition 3.2.2, we known their weights. These weights correspond to the degrees of the irreducible factors of $P_\ell^n(x) - t$. If $\bar{t}$ is preperiodic, then all the roots of $P_\ell^n(x) - t$ are $\rho + n$-preperiodic, hence all of the irreducible factors of $P_\ell^n(x) - t$ have the same degree. If $\bar{t}$ is periodic, then $P_\ell^n(x) - t$ has roots at every preperiod up to n, and the degrees of the irreducible factors of $P_\ell^n(x) - t$ will vary. □

From this factorization result, we can determine the decomposition of primes in the radical extensions. Let ℓ be an odd prime, and let t be an integer for which $P_\ell^n(x) - t$ is irreducible for each $n \ge 1$. Fix an iterated tower generated by preimages of t, and let K_n denote the field at the n-th level. That is, $K_n = \mathbf{Q}(\theta_n)$ where θ_n is a root of $P_\ell^n(x) - t$.

Corollary 3.3.2. *Let* p *be a prime that does not divide the discriminant of* $P_\ell^n(x) - t$*, and let* ρ *denote the preperiod of* $\bar{t} \in \mathbf{F}_p$*. The decomposition of* $p\mathbf{Z}$ *is as follows.*

1. *If* $\rho > 0$*, then* $p\mathbf{Z}$ *splits in* $K_1, \ldots, K_{m_p-\rho}$ *and is totally inert afterwards.*

2. *If* $\rho = 0$*, then there is at least one prime of degree 1 above* $p\mathbf{Z}$ *at every level.*

Proof. This result follows directly from Theorem 3.0.3 and Theorem 3.3.1. □

3.3.2 Decomposition in Chebyshev radical extensions

For the Chebyshev polynomials, the weights depend on the cycle type. We use the following notation to describe the factorizations. Let ℓ be an odd prime and let p be a prime different from

ℓ. Let μ be the minimal integer for which $p^\mu \equiv \pm 1 \pmod{\ell}$. Let $D_1, D_2 \in \{p^\mu - 1, p^\mu + 1\}$ be the number with the larger and smaller ℓ-valuation, respectively.

Theorem 3.3.3. *Let ℓ be an odd prime, and let p be a prime different from ℓ. Let μ, D_1, and D_2 as just defined. Put $m_p = \nu_\ell(D_1)$ and let ρ denote the preperiod of $\bar{t} \in \mathbf{F}_p$. The factorization of $T_\ell^n(x) - t$ modulo p is as follows.*

1. *If $\rho > 0$, then $T_\ell^n(x) - t$ factors into*
   (a) *ℓ^n factors of degree 1 if $1 \le n \le m_p - \rho$, or*
   (b) *$\ell^{v-\rho}$ factors of degree $\ell^{n-m_p+\rho}$ if $n > m_p - \rho$.*

   In particular, if $\rho = m_p$, then $T_\ell^n(x) - t$ is irreducible modulo p.
2. *If $\bar{t} \in \{-2, 2\}$, then $T_\ell^n(x) - t$ factors into*
   (a) *one degree 1 factor, and*
   (b) *$\sum_{k=0}^{n-1} \frac{\ell-1}{2\mu}\ell^k$ additional factors of degree μ if $1 \le n \le m_p$, and*
   (c) *$\frac{\ell-1}{2\mu}\ell^{m_p-1}$ additional factors of degree $\mu\ell^k$ for each $k \in \{1, 2, \ldots, n - m_p\}$.*

   Each of the factors from parts (b) and (c) have multiplicity 2.
3. *If $\bar{t} \notin \{-2, 2\}$ is periodic and $\bar{t}$ corresponds to a divisor of D_1, then $T_\ell^n(x) - t$ factors into*
   (a) *one degree 1 factor, and*
   (b) *$\sum_{k=0}^{n-1} \frac{\ell-1}{\mu}\ell^k$ additional factors of degree μ if $1 \le n \le m_p$, and*
   (c) *$\frac{\ell-1}{\mu}\ell^{m_p-1}$ additional factors of degree $\mu\ell^k$ for each $k \in \{1, 2, \ldots, n - m_p\}$.*
4. *If $\bar{t} \notin \{-2, 2\}$ is periodic and corresponds to a divisor of D_2, then $T_\ell^n(x) - t$ factors into*
   (a) *one degree 1 factor, and*
   (b) *$\sum_{k=0}^{n-1} \frac{\ell-1}{2\mu}\ell^k$ additional factors of degree 2μ if $1 \le n \le m_p$, and*
   (c) *$\frac{\ell-1}{2\mu}\ell^{m_p-1}$ additional factors of degree $2\mu\ell^k$ for each $k \in \{1, 2, \ldots, n - m_p\}$.*

Proof. The idea of the proof is the same as in Theorem 3.3.1: the roots of $T_\ell^n(x) - t$ modulo p are precisely the elements whose distance from $\bar{t}$ is n. The weights of these elements are derived from Proposition 3.2.3, and these weights give the degrees of the irreducible factors. □

Consider the tower generated by the iterates $T_\ell^n(x) - t$, and let K_n denote the field at the n-th level of the tower.

Corollary 3.3.4. *Let ℓ be an odd prime, let p be a prime that does not divide the discriminant of $T_\ell^n(x) - t$, and let ρ denote the preperiod of $\bar{t} \in \mathbf{F}_p$. Then $p\mathbf{Z}$ decomposes as follows.*

1. *If $\rho > 0$, then p splits in $K_1, \ldots, K_{m_p - \rho}$ and is totally inert afterwards.*
2. *If $\rho = 0$, then there is at least one prime of degree 1 above p at every level.*

Proof. The result follows from Theorem 3.0.3 and Theorem 3.3.3. □

In our introduction, we noted the special case $T_\ell^n(x) - 2$ for its connection to cyclotomic fields. Namely, the iterated towers are $K_n = \mathbf{Q}(\zeta_{\ell^n} + \zeta_{\ell^n}^{-1})$, which are the totally real subfields of the cyclotomic fields. We show that our result regarding the decomposition of primes coincides with cyclotomic reciprocity in these cases.

Example 3.3.5 (Cyclotomic $\mathbf{Z}_\ell$ extension)**.** Let ℓ be an odd prime, then the iterated extension generated by the iterates $T_\ell^n(x) - 2$ is the cyclotomic $\mathbf{Z}_\ell$ extension of $\mathbf{Q}$. If follows that a prime $p\mathbf{Z}$ splits completely at the n-th level in the tower if and only if $T_\ell^n(x) - 2$ splits completely modulo p. By Theorem 3.3.3, the polynomial $T_\ell^n(x) - 2$ splits completely into linear factors if and only if $m_p \geq n$. Thus $p\mathbf{Z}$ splits completely in K_n if and only if $p \equiv \pm 1 \pmod{\ell^n}$.

We note that Theorem 3.3.1(5) and Theorem 3.3.1(1) give a rather interesting irreducibility criterion. Namely, if $\bar{t}$ attains the maximal preperiod of elements in $\mathcal{G}(P, p)$, (resp. $\mathcal{G}(T, p)$), and $\bar{t}$ is strictly preperiodic, then $P_\ell^n(x) - t$ (resp. $T_\ell^n(x) - t$) has only one irreducible factor. In other words, $P_\ell^n(x) - t$ (resp. $T_\ell^n(x) - t$) is irreducible modulo p for each $n \geq 1$.

Corollary 3.3.6. *Let ℓ be an odd prime.*

1. *$P_\ell^n(x) - t$ is irreducible for every $n \geq 1$ if there exists a prime $p \equiv 1 \pmod{\ell}$ such that $\bar{t}$ is maximally preperiodic in $\mathcal{G}(P, p)$.*
2. *$T_\ell^n(x) - t$ is irreducible for every $n \geq 1$ if there exists a prime $p \equiv \pm 1 \pmod{\ell}$ such that $\bar{t}$ is maximally preperiodic in $\mathcal{G}(T, p)$.*

In particular, this shows that for a fixed prime ℓ, there are infinitely many values t such that every iterate $P_\ell^n(x) - t$ (resp. $T_\ell^n(x) - t$) is irreducible. By Dirichlet's theorem on arithmetic

progressions, there are infinitely many primes p satisfying the congruence condition modulo ℓ. For any one of these primes, Theorem 3.1.2 and Theorem 3.1.2 guarantee a large number of equivalence classes modulo p that generate irreducible families.

A similar factorization result for $\mathcal{D}_\ell$ modulo primes can easily be obtained from Theorem 3.1.8 and Proposition 3.2.5, from which a decomposition result can be obtained by applying Theorem 3.0.3.

Likewise, a factorization result may be obtained for the generalized Rikuna polynomials. However, since the polynomial $r_n(x,t;\ell)$ is defined over $\mathbf{Q}(\zeta^+)$ (where $\zeta^+ = \zeta+\zeta^{-1}$ and ζ is a primitive ℓ-th root of unity), a careful analysis is required to understand how each prime above $p\mathbf{Z}$ in $\mathcal{O}_{\mathbf{Q}(\zeta^+)}$ decomposes in the iterated extensions over $\mathbf{Q}(\zeta^+)$. We leave this analysis for a future project.

3.4 Discriminant formulæ

We point out that the decomposition result, Theorem 3.0.3, applies to all but finitely many primes. Specifically, it does not address the primes that divide $\mathrm{ind}(f)$. As we know from Equation (1.1), we know that $\mathrm{ind}(f)$ divides $\mathrm{disc}(f)$. Thus by omitting the primes dividing $\mathrm{disc}(f)$—as we did in Corollaries 3.3.2 and 3.3.4—we avoid any trouble. In this section, give the discriminant formulas for the power, Chebyshev, Dickson, and generalized Rikuna maps so as to identify the potentially troublesome primes. In the next section, we begin to to address the index calculations, and these discriminants will be necessary for determining formulas for the corresponding number fields.

It is relatively easy to verify that the power maps, Chebyshev polynomials, Dickson-(-1) polynomial of odd degree, and generalized Rikuna polynomials of prime power degree are post-critically finite. Thus we may apply [2, Proposition 3.2] (see Proposition 1.1.1), and in the case of the generalized Rikuna maps, [9, Proposition 1].

Proposition 3.4.1. *Let ℓ be an odd prime. We have*

1. $\mathrm{disc}(P_\ell^n(x) - t) = \pm \ell^{n\ell^n} t^{\ell^n - 1}$,
2. $\mathrm{disc}(T_\ell^n(x) - t) = \pm \ell^{n\ell^n} (4 - t^2)^{(\ell^n-1)/2}$,
3. $\mathrm{disc}(\mathcal{D}_{\ell^n}(x) - t) = \pm \ell^{n\ell^n} (t^2 + 4)^{(\ell^n-1)/2}$.

4. $\operatorname{disc} r_n(x,t;\ell) = \pm \ell^{n\ell^n} (\zeta - \zeta^{-1})^{(\ell^n-2)(\ell^n-1)} (t^2 - (\zeta+\zeta^{-1})t + 1)^{\ell^n - 1}$, *where* ζ *is a primitive* ℓ*-th root of unity.*

Proof. The discriminant of $P_\ell^n(x) - t$ is well known and can easily be derived from Proposition 1.1.1. This map has one critical point ($x = 0$), and $\frac{d}{dx} P_\ell^n(x) = \ell^n x^{\ell^n - 1}$, hence $\mathcal{M}_0(P_\ell^n) = \ell^n - 1$.

The Chebyshev polynomial has two distinct critical values: 2 and -2. It is easy to verify that the critical points of $T_\ell^n(x)$ are at $2\cos(k\pi/\ell^n)$ for $k = 1, \ldots, \ell^n - 1$, where half of these critical values map to -2 and the other half to 2. Hence $\mathcal{M}_2(T_\ell^n) = \mathcal{M}_{-2}(T_\ell^n) = (\ell^n - 1)/2$.

The discriminant of the Dickson polynomials may be computed similarly; its critical values are $\pm\sqrt{-4}$. The discriminant for the generalized Rikuna polynomial appears in [5, p. 9]. □

CHAPTER 4

PRELIMINARIES FOR INDEX COMPUTATIONS

4.1 Dedekind's criterion

We now outline the computational tools that we will use throughout this paper beginning with Dedekind's criterion. The version of Dedekind's criterion stated here is a generalized version where the base field is an arbitrary number field. This theorem appears in Cohen [8, Theorem 2.4.8]. The classical result with base field $\mathbf{Q}$ can be found in Cohen [7, Theorem 6.1.4].

Let $\overline{\ }$ denote reduction modulo a prime ideal.

Theorem 4.1.1. *Let L/K be a relative extension, with $L = K(\theta)$ and θ an algebraic integer with minimal polynomial $\Psi(x) \in K[x]$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and let β be a uniformizer of $\mathfrak{p}^{-1}$, so that $\beta \in \mathcal{O}_K \setminus \mathfrak{p}^{-1}$. Let $\overline{\Psi}(x) = \prod_{1\le i\le r} \overline{\psi}_i(x)^{e_i}$ be the factorization of $\overline{\Psi}(x)$ in $(\mathcal{O}_K/\mathfrak{p})[x]$ with the ψ_i monic. Set*

$$g(x) = \prod_{1\le i\le r} \psi_i(x), \quad h(x) = \prod_{1\le i\le r} \psi_i(x)^{e_i-1}, \quad \text{and} \quad f(x) = \beta(g(x)h(x) - \Psi(x)).$$

The ring $\mathcal{O}_K[\theta] \subseteq \mathcal{O}_L$ is $\mathfrak{p}$-maximal if and only if $\gcd(\overline{f}, \overline{g}, \overline{h}) = 1$ in $(\mathcal{O}_K/\mathfrak{p})[x]$.

Remark 4.1.2. Dedekind's result is independent of the choice of lifts and the choice of uniformizer. Moreover, an order is $\mathfrak{p}$-*maximal* if the discriminant of the order is not contained in $\mathfrak{p}$.

As we mentioned previously, Dedekind's critterion is powerless once $\gcd(\overline{f}, \overline{g}, \overline{h}) \neq 1$, and we must turn to other methods.

4.2 Montes algorithm

In order to compute the index $\mathrm{ind}(f)$ and prove Theorem 1.2.2 and Theorem 1.2.3, we apply the Montes algorithm, which is explained in a series of papers [16, 17, 18]. This algorithm employs

a refined variation of the Newton polygon, called the *ϕ-Newton polygon*, which captures arithmetic data attached to each irreducible factor ϕ of f. We begin this section by outlining their methods and terminology following the presentation of El Fadil, Montes, and Nart [10]. As with the usual Newton polygon, the ϕ-Newton polygon requires knowledge of valuations of coefficients of a particular polynomial in ϕ. We follow up this section with some useful results for computing the p-adic valuations of certain numbers.

We fix the following notation. Let p be a prime and let $\phi(x) \in \mathbf{Z}[x]$ be a monic polynomial whose reduction modulo p is irreducible. We denote by $\mathbf{F}_\phi$ the finite field $\mathbf{Z}[x]/(p, \phi)$, and by

$$\overline{}\colon \mathbf{Z}[x] \to \mathbf{F}_p[x], \quad \text{red}\colon \mathbf{Z}[x] \to \mathbf{F}_\phi$$

the respective homomorphisms of reduction modulo p and modulo (p, ϕ). We extend the usual p-adic valuation to polynomials by

$$\nu_p(c_0 + \cdots + c_r x^r) := \min_{0 \le i \le r} \{\nu_p(c_i)\}.$$

Any $f(x) \in \mathbf{Z}[x]$ admits a unique *ϕ-adic development*:

$$f(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_r(x)\phi(x)^r,$$

with $a_i(x) \in \mathbf{Z}[x]$ and $\deg(a_i) < \deg(\phi)$. To each coefficient $a_i(x)$ we attach the p-adic value

$$u_i = \nu_p(a_i(x)) \in \mathbf{Z} \cup \{\infty\}$$

and the point of the plane (i, u_i), if $u_i < \infty$.

The *ϕ-Newton polygon* of $f(x)$ is the lower convex envelope of the set of points $(i, u_i), u_i < \infty$, in the Euclidean plane. We denote this open polygon by $N_\phi(f)$. The ϕ-Newton polygon is the union of different adjacent sides $S_1, \ldots, S_g$ with increasing slopes $\lambda_1 < \cdots < \lambda_g$. We shall write $N_\phi(f) = S_1 + \cdots + S_g$. The end points of the sides are called the vertices of the polygon.

The polygon determined by the sides of negative slope of $N_\phi(f)$ is called the *principal ϕ-polygon* of $f(x)$ and will be denoted by $N_\phi^-(f)$. The length, of $N_\phi^-(f)$, denoted $\ell(N_\phi^-(f))$, is always equal to the highest exponent a such that $\overline{\phi}(x)^a$ divides $\overline{f}(x)$ in $\mathbf{F}_p[x]$. See Figure 7.

From now on, any reference to the ϕ-Newton polygon of $f(x)$ will be taken to mean the principal ϕ-polygon, and for simplicity, we will write $N_\phi(f) := N_\phi^-(f)$.

A simple script can be used to obtain the ϕ-development and polygon. For example, the following code is written for `PARI` [39].

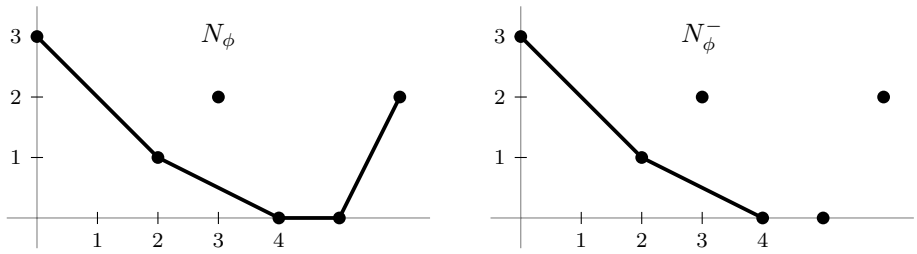


Figure 7: A ϕ-Newton polygon (right) and its principal part (left).

```
// returns the phi-development of f as a polynomial in y.
phidev(f,phi) = {
    local(V);
    f = Pol(Vec(f),y);
    phi = Pol(Vec(phi),y);
    V = vector(floor(poldegree(f)/poldegree(phi))+1,\
        i,(lift(Mod(f,phi^i))-lift(Mod(f,phi^(i-1))))/phi^(i-1));
    sum(i=0,length(V)-1,V[i+1]*x^i);
}

// returns the phi-Newton polygon of f at the prime p.
phiPoly(f,phi,p) = {
    newtonpoly(phidev(f,phi),p);
}
```

We attach to any abscissa $0 \le i \le \ell(N_\phi)$ the following *residual coefficient* $c_i \in \mathbf{F}_p[x]/(\phi)$.

$$c_i = \begin{cases} 0 & \text{if } (i, u_i) \text{ lies strictly above } N_\phi \text{ or } u_i = \infty, \\ \mathrm{red}(a_i(x)/p^{u_i}) & \text{if } (i, u_i) \text{ lies on } N_\phi. \end{cases}$$

Note that c_i is always nonzero in the latter case, because $\deg(a_i(x)) < \deg(\phi)$.

Let S be one of the sides of N_ϕ, with slope $\lambda = -h/e$, where e and h are relatively prime, positive integers. The length of S is the length, $\ell(S)$, of the projection of S to the horizontal axis, the degree of S is $d(S) := \ell(S)/e$, the ramification index of S is $e(S) := e$.

Let s be the initial abscissa of S, and let $d := d(S)$. We define the *residual polynomial* attached

to S (or to λ) to be the polynomial

$$R_\lambda(f)(y) := c_s + c_{s+e}y + \cdots + c_{s+(d-1)e}y^{d-1} + c_{s+de}y^d \in \mathbf{F}_\phi[y].$$

Example 4.2.1. Consider the irreducible polynomial $f(x) = x^4 + 23x^3 + 12x^2 + 11x + 7$, which factors over $\mathbf{F}_3[x]$ into $f(x) \equiv (x+2)^4 \pmod 3$. Set $\phi(x) = x+2$, then the ϕ-development of f is

$$f(x) = -135 + 207(x+2) - 102(x+2)^2 + 15(x+2)^3 + (x+2)^4.$$

The ϕ-Newton polygon is two-sided: one side of slope -1 and length 2, the other side of slope $-1/2$ and length 1. The residual coefficients are $c_0 = 1$, $c_1 = -1$, $c_2 = -1$, $c_3 = 0$, and $c_4 = 1$, and the residual polynomials attached to the sides S_1 and S_2 are $R_{-1}(f)(y) = -y^2 + 1$ and $R_{-1/2}(f)(y) = y - 1$, respectively. See Figure 8.

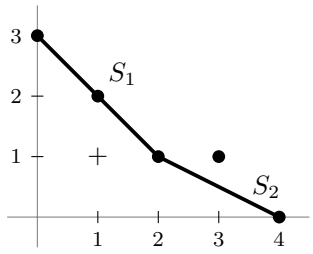


Figure 8: The ϕ-polygon for $f(x) = x^4 + 23x^3 + 12x^2 + 11x + 7$ and $\phi(x) = x + 2$.

Let $\phi(x) \in \mathbf{Z}[x]$ be a monic polynomial, irreducible modulo p. We say that $f(x)$ is *ϕ-regular* if for every side $N_\phi(f)$, the residual polynomial attached to the side is separable. For any monic polynomials $\phi_1(x), \ldots, \phi_r(x) \in \mathbf{Z}[x]$ whose reduction modulo p are the different irreducible factors of $\overline{f}(x) \in \mathbf{F}_p[x]$. We say that $f(x)$ is *p-regular* with respect to this choice if $f(x)$ is ϕ_i-regular for every $1 \le i \le r$.

The *ϕ-index* of $f(x)$ is $\deg \phi$ times the number of points with integral coordinates that lie below or on the polygon $N_\phi(f)$, strictly above the horizontal axis, and strictly to the right of the vertical axis. We denote this number by $\mathrm{ind}_\phi(f)$.

Let θ be an algebraic integer with minimal polynomial $f(x) \in \mathbf{Z}[x]$, and let $\mathrm{ind}(f) = [\mathcal{O}_{\mathbf{Q}(\theta)} \colon \mathbf{Z}[\theta]]$. We denote by $\mathrm{ind}_p(f)$ the p-adic valuation of the index of the polynomial $f(x)$:

$$\mathrm{ind}_p(f) := \nu_p(\mathrm{ind}(f)).$$

Theorem 4.2.2. *Theorem of the index:*

$$\mathrm{ind}_p(f) \ge \mathrm{ind}_{\phi_1}(f) + \cdots + \mathrm{ind}_{\phi_r}(f),$$

and equality holds if $f(x)$ is p-regular.

Proof. See [18, Section 4.4]. □

Example 4.2.1 (continued)**.** Returning to the previous example with $f(x) = x^4 + 23x^3 + 12x^2 + 11x + 7$, both of the residual polynomials R_{-1} and $R_{-1/2}$ are separable over $\mathbf{F}_3[x]$. Hence f is 3-regular, and by Theorem 4.2.2, we have $\mathrm{ind}_3(f) = \mathrm{ind}_\phi(f) = 3$, since $\deg \phi = 1$ and there are three points with integral coordinates on or below the polygon. This result is verified by `PARI`.

4.3 Valuations

For any prime p and any integer a, the *p-adic expansion* of a is

$$a = a_0 p^0 + a_1 p^1 + a_2 p^2 + \cdots + a_r p^r$$

with $0 \leq a_i < p$. We define the function

$$\sigma_p(a) = \sum_{i=0}^{\infty} a_i.$$

Lemma 4.3.1 (Kummer)**.** *Let p be a prime, and let σ_p be the function defined above.*

1. *Let a and b be integers written in base p. The number of "carries" performed when summing $a + b$ in base p is*

$$\#\mathit{carries} = \frac{\sigma_p(a) + \sigma_p(b) - \sigma_p(a+b)}{p-1}.$$

2. $\nu_p(a) = \dfrac{1 + \sigma_p(a-1) - \sigma_p(a)}{p-1}$.

3. $\nu_p(a!) = \dfrac{n - \sigma_p(a)}{p-1}$.

4. $\nu_p\dbinom{a+b}{b} = \#\mathit{carries\ in\ } a+b \mathit{\ summed\ in\ base\ } p.$

Though these are well-known, for the convenience of the reader, we provide proofs, as they are short.

Proof.

1. Write a and b in their base p expansions: $a = \sum a_i p^i$ and $b = \sum b_i p^i$. If ever $c_i := a_i + b_i \geq p$, then perform a "carry": subtract p from c_i and add 1 to c_{i+1}, repeating until all c_i are less than p. These c_i are the coefficients for the base p expansion of $a+b$: $a+b = \sum c_i p^i$. Each carry reduces the sum $\sigma_p(a) + \sigma_p(b)$ by $p-1$, and the result follows.

2. This follows immediately from part (1). If k is the smallest integer for which $a - 1 \equiv -1 \pmod{p^k}$, then the sum $(a-1)+1$ requires k carries in base p.

3. By part (2), we have the telescoping sum

$$\nu_p(a!) = \sum_{i=1}^{a} \nu_p(i) = \sum_{i=1}^{a} \frac{1 + \sigma_p(i-1) - \sigma_p(i)}{p-1} = \frac{a - \sigma_p(a)}{p-1}.$$

4. By part (3)

$$\begin{aligned} \nu_p\binom{a+b}{b} &= \nu_p\left(\frac{(a+b)!}{a!b!}\right) = \nu_p((a+b)!) - \nu_p(a!) - \nu(b!) \\ &= \frac{a+b-\sigma_p(a+b)}{p-1} + \frac{a-\sigma_p(a)}{p-1} - \frac{b-\sigma_p(b)}{p-1} \\ &= \frac{\sigma_p(a) + \sigma_p(b) - \sigma_p(a+b)}{p-1}. \end{aligned}$$

   The result follows from part (1).

□

Another important tool for determining whether a binomial coefficient is divisible by a prime is the following result of Lucas.

Lemma 4.3.2. *Let p be a prime, and let $0 \leq m \leq n$ with $n = \sum_{j=0}^{r} n_j p^j$ and $m = \sum_{j=0}^{r} m_j p^j$. Then*

$$\binom{n}{m} \equiv \prod_{j=0}^{r} \binom{n_j}{m_j} \pmod{p}.$$

Proof. See [27, Section 3]. □

The Montes algorithm requires that we count the number of lattice points below the polygon. Pick's Theorem is a convenient tool for this.

Lemma 4.3.3 (Pick's theorem)**.** *The area A of a simple polygon whose vertices lie on a lattice is given by*

$$A = I + B/2 - 1,$$

where I is the number of lattice points on the interior of the polygon, and B is the number of lattice points on the boundary of the polygon.

Proof. See [31]. □

CHAPTER 5

RADICAL EXTENSIONS

As motivation for the coming sections, we briefly discuss the extensions generated by the polynomial $P_\ell^n(x) - t$. We remind the reader that ℓ is an odd prime, and $t \in \mathbf{Z}$ is chosen so the polynomial is irreducible for each $n \geq 1$. The radical polynomials and the fields that they generate are well-studied as they generate *Kummer extensions* (see, for example [21]), and they will serve as a model for our analysis of other families of maps.

Using Dedekind's criterion, we are able to identify large families of monogenic towers by showing $\text{ind}(P_\ell^n(x) - t) = 1$. In order to identify towers of monogenic fields, we find that we only need to check to see if the first level of the tower is monogenic. This idea of only having to check for monogeneity at the first level will carry over to the other families.

5.1 Monogenic towers

Recall from Proposition 3.4.1 that $\text{disc}(P_\ell^n(x) - t) = \ell^{n\ell^n} t^{\ell^n - 1}$. Thus in order to compute $\text{ind}(P_\ell^n(x) - t)$, we are only concerned with the primes ℓ and the primes that divide t. The following results are elementary.

Lemma 5.1.1. *If a divides t, then $P_\ell^n(x) \equiv x^{\ell^n} \pmod{a}$. Moreover, $P_\ell^n(x) \equiv (x-t)^{\ell^n} \pmod{\ell}$.*

Lemma 5.1.2. *$P_\ell(a) \equiv P_\ell(b) \pmod{\ell^2}$ if and only if $a \equiv b \pmod{\ell}$.*

Proof. If $a^\ell \equiv b^\ell \pmod{\ell^2}$, then $a^\ell \equiv b^\ell \pmod{\ell}$, whence $a \equiv b \pmod{\ell}$. For the converse, it suffices to show that $P_\ell(a) \equiv P_\ell(r) \pmod{\ell^2}$, where $a = \ell q + r$ and $0 \leq r < \ell$. This follows easily: $a^\ell = (\ell q + r)^\ell \equiv r^\ell \pmod{\ell^2}$. □

Lemma 5.1.3. *$P_\ell^n(t) \equiv t \pmod{\ell^2}$ if and only if $P_\ell(t) \equiv t \pmod{\ell^2}$.*

Proof. Since $P_\ell^{n-1}(t) \equiv t \pmod{\ell}$, it follows from Lemma 5.1.2 that $P_\ell^n(t) \equiv P_\ell(t) \pmod{\ell^2}$. □

We are now in position to apply Dedekind's criterion (Theorem 4.1.1). Let K_n denote a radical extension at the n-th level. That is, $K_n = \mathbf{Q}(\theta_n)$, where θ_n is a root of $P_\ell^n(x) - t$.

Theorem 5.1.4. *If ℓ is an odd prime, t is square-free, and $P_\ell(t) - t \not\equiv 0 \pmod{\ell^2}$, then K_n is monogenic as* $\operatorname{disc}(P_\ell^n(x) - t) = \operatorname{disc}(K_n)$.

Proof. We begin by showing that ℓ does not divide $\operatorname{ind}(P_\ell^n(x) - t)$. Set

$$g(x) = x - t, \quad h(x) = (x-t)^{\ell^n - 1}, \quad \text{and} \quad f(x) = \frac{(x-t)^{\ell^n} - (x^{\ell^n} - t)}{\ell}.$$

By Theorem 4.1.1, the index $\operatorname{ind}(P_\ell^n(x) - t)$ is divisible by ℓ if and only if t is a root of $f(x)$ modulo ℓ. Note that $f(t) = -(P_\ell^n(t) - t)/\ell$, and hence t is a root of f modulo ℓ if and only if $P_\ell^n(t) - t \equiv 0 \pmod{\ell^2}$. But by our assumption and Lemma 5.1.3, t cannot be a root of f modulo ℓ. Thus $\ell \nmid \operatorname{ind}(P_\ell^n(x) - t)$.

Now for all other primes: let p be a prime dividing t. Set

$$g(x) = x, \quad h(x) = x^{\ell^n - 1}, \quad \text{and} \quad f(x) = \frac{x^{\ell^n} - (x^{\ell^n} - t)}{p}.$$

Theorem 4.1.1 tells us that p divides the index if and only if 0 is a root of f modulo p. Here, $f(0) = t/p$, hence 0 is a root of f modulo p if and only if $t \equiv 0 \pmod{p^2}$. However, our assumption is that t is square-free, thus $p \nmid \operatorname{ind}(P_\ell^n(x) - t)$. □

5.2 Index calculation

In the non-monogenic case, we can apply the Montes algorithm. In some cases, Theorem 4.2.2 renders the index calculation nearly trivial.

Proposition 5.2.1. *Let p be a prime dividing t, and let $v = \nu_p(t)$. If $\gcd(\ell, v) = 1$, then*

$$\operatorname{ind}_p(P_\ell^n(x) - t) = \frac{(\ell^n - 1)(v-1)}{2}.$$

Proof. Applying the Montes algorithm, we see from Lemma 5.1.1 that there is only one irreducible factor of $P_\ell^n(x) - t$ modulo p: $\phi(x) = x$. Hence $P_\ell^n(x) - t$ is the ϕ-development, and the ϕ-Newton polygon is one-sided with vertices $(0, v)$ and $(\ell^n, 0)$. If $\gcd(\ell, v) = 1$, then the length of this side is 1, hence P_ℓ^n is p-regular, and by the Theorem 4.2.2, the p-adic valuation of the index is the

number of lattice points under the polygon, which we obtain using Lemma 4.3.3. The region under the polygon is a triangle, and the only lattice points on the boundary are the lattice points on the axes. Hence by Lemma 4.3.3,

$$\mathrm{ind}_p(P^n) = I = A - B/2 + 1 = \frac{\ell^n v}{2} - \frac{\ell^n + v + 1}{2} + 1 = \frac{\ell^n v - \ell^n - v + 1}{2} = \frac{(\ell^n - 1)(v-1)}{2}.$$

□

Remark 5.2.2. If $\gcd(\ell^n, v) > 1$, the p-adic valuation of the index can be computed using Newton polygons of higher order, which are explained in [16, 17, 18]. However, we will not address these cases in this paper.

Theorem 5.2.3. *Suppose* $t \not\equiv 0 \pmod{\ell}$. *Set* $v = \nu_\ell(P_\ell^n(t) - t)$. *Then*

$$\mathrm{ind}_\ell(P_\ell^n(x) - t) = \sum_{i=1}^{\min\{v-1,n\}} \ell^{n-i}.$$

Proof. By Lemma 5.1.1, we have $P_\ell^n(x) = x^{\ell^n} - t \equiv (x-t)^{\ell^n} \pmod{\ell}$. Set $\phi(x) = x - t$, then the ϕ-development of P^n is

$$\begin{aligned} P_\ell^n(x) = P_\ell^n(\phi(x) + t) &= (\phi(x) + t)^{\ell^n} - t = -t + \sum_{k=0}^{\ell^n} \binom{\ell^n}{k} t^{\ell^n - k} \phi(x)^k \\ &= P_\ell^n(t) + \sum_{k=1}^{\ell^n} \binom{\ell^n}{k} t^{\ell^n - k} \phi(x)^k. \end{aligned}$$

Set $a_i = \binom{\ell^n}{k} t^{\ell^n - k}$ for $1 \le i \le \ell^n$. To construct the ϕ-Newton polygon, we must determine the valuations of the a_i's. Since $t \not\equiv 0 \pmod{\ell}$, we have $\nu_\ell(a_i) = \nu_\ell\binom{\ell^n}{k}$.

Lemma 5.2.4. *Suppose* $\ell^m \le k < \ell^{m+1}$ *for some* $m < n$. *Then* $\nu_\ell\binom{\ell^n}{k} \ge n - m$ *with equality if* $k = \ell^m$.

Proof. Write $k = \ell^m + \varepsilon$ for some $0 \le \varepsilon < \ell^m(\ell - 1)$. Then

$$\begin{aligned} \binom{\ell^n}{k} = \binom{\ell^n}{\ell^m + \varepsilon} &= \frac{\ell^n!}{(\ell^m + \varepsilon)!(\ell^n - \ell^m - \varepsilon)!} = \frac{\ell^n!}{\ell^m!(\ell^n - \ell^m)!} \frac{\ell^m!\varepsilon!}{(\ell^m + \varepsilon)!} \frac{(\ell^n - \ell^m)!}{(\ell^n - \ell^m - \varepsilon)!\varepsilon!} \\ &= \binom{\ell^n}{\ell^m} \binom{\ell^m + \varepsilon}{\varepsilon}^{-1} \binom{\ell^n - \ell^m}{\varepsilon}. \end{aligned}$$

It is straightforward to verify that the sum $(\ell^n - \ell^m) + \ell^m$ requires $n - m$ carries in base ℓ, while $\ell^m + \varepsilon$ requires no carries. Hence by Lemma 4.3.1

$$\nu_\ell\binom{\ell^n}{k} = \nu_\ell\binom{\ell^n}{\ell^m} - \nu_\ell\binom{\ell^m + \varepsilon}{\varepsilon} + \nu_\ell\binom{\ell^n - \ell^m}{\varepsilon}$$

$$\geq \nu_\ell\binom{\ell^n}{\ell^m} - \nu_\ell\binom{\ell^m+\varepsilon}{\varepsilon}$$
$$= n - m.$$

Note that when $\varepsilon = 0$, we have equality throughout. □

Returning to the proof of Theorem 5.2.3, it follows from Lemma 5.2.4 that the ϕ-Newton polygon of P_ℓ^n is the lower convex hull of the set of points $\{(0,v)\} \cup \{(i, n-i) \colon 1 \leq i \leq n\}$. Each side of this polygon has length 1, hence P_ℓ^n is ℓ-regular. The lattice points under this polygon are arranged into rows whose lengths are decreasing powers of ℓ, and the formula for $\mathrm{ind}_\ell(P_\ell^n)$ follows. □

CHAPTER 6

CHEBYSHEV RADICAL EXTENSIONS

We now turn to the computation of the index $\mathrm{ind}(T_\ell^n(x) - t)$. We remind the reader that ℓ is an odd prime, and $t \in \mathbf{Z}$ is chosen so that $T_\ell^n(x) - t$ is irreducible for each $n \geq 1$. For ease of notation, we set $\Phi(x) := T_\ell^n(x) - t$ for the remainder of this section. This chapter closely follows previous work of the author: [13].

Our first approach is to apply Dedekind's criterion, Theorem 4.1.1, in order to identify conditions on t that yield monogenic towers. We then carry out the Montes algorithm in the non-monogenic case.

6.1 Monogenic number fields

In this section we give a proof of Theorem 1.2.1 based on Dedekind's criterion. Dedekind's result gives local conditions for when a prime divides $\mathrm{ind}(\Phi)$, and combined with the factorization results from the previous section, we obtain conditions for when $\mathrm{ind}(\Phi) = 1$. The then prove a proposition that will allow us to show that $\mathrm{ind}(\Phi) = 1$ if and only if $\mathrm{ind}(T_\ell(x) - t) = 1$. This particular result also applies to the case $\ell = 2$, thus our method gives an alternative proof of [2, Proposition 6.2].

We highlight the pertinent factorization results from earlier in the paper.

Lemma 6.1.1. *We have* $\Phi(x) \equiv (x - t)^{\ell^n} \pmod{\ell}$. *Moreover, if* p *is a prime different from* ℓ *such that* $t \equiv \pm 2 \pmod{p}$, *then*

$$\Phi(x) \equiv (x - t)\phi_1(x)^2 \cdots \phi_r(x)^2 \pmod{p},$$

where $\phi_1, \ldots, \phi_r$ *are distinct irreducible factors in* $\mathbf{F}_p[x]$.

Proof. These are special cases of Theorem 3.3.3. □

We now prove a weak version of Theorem 1.2.1.

Theorem 6.1.2. *Let $K = \mathbf{Q}(\theta)$, where θ is a root of Φ. Then $D_\Phi = \Delta_K$ if and only if $\Phi(t) \not\equiv 0 \pmod{\ell^2}$ and both $t-2$ and $t+2$ are square-free.*

Proof. By Proposition 3.4.1, we are only concerned with the prime ℓ and the primes dividing t^2-4. We first address the prime ℓ. By Lemma 6.1.1, $\Phi(x) \equiv (x-t)^{\ell^n} \pmod{\ell}$, so we set

$$g(x) = x - t, \quad h(x) = (x-t)^{\ell^n - 1}, \quad \text{and} \quad f(x) = \frac{(x-t)^{\ell^n} - \Phi(x)}{\ell}.$$

Hence $\gcd(\overline{f}, \overline{g}, \overline{h}) = 1$ if and only if $f(t) \not\equiv 0 \pmod{\ell}$, and it follows from Theorem 4.1.1 that

$$\ell \nmid \operatorname{ind}(\Psi) \quad \text{if and only if} \quad \Phi(t) \not\equiv 0 \pmod{\ell^2}.$$

Now let p be a prime dividing t^2-4. By Lemma 6.1.1, we have $\Phi(x) \equiv (x-\overline{t})\tau(x)^2 \pmod{p}$, for some separable polynomial $\tau \in \mathbf{F}_p[x]$. Set

$$g(x) = (x-\overline{t})\tau(x), \quad h(x) = \tau(x), \quad \text{and} \quad f(x) = \frac{(x-\overline{t})\tau(x)^2 - \Phi(x)}{p}.$$

In this case, $\gcd(\overline{f}, \overline{g}, \overline{h}) = 1$ if and only if the roots of τ are not roots of f modulo p. Let α be a root of τ modulo p. Then

$$f(\alpha) \not\equiv 0 \pmod{p} \quad \text{if and only if} \quad \Phi(\alpha) \not\equiv 0 \pmod{p^2}.$$

Note that

$$\Phi(\alpha) = T_\ell^n(\alpha) - \overline{t} + \overline{t} - t = (\alpha - \overline{t})\tau(\alpha)^2 + \overline{t} - t \equiv t - \overline{t} \pmod{p^2}.$$

Since $\overline{t} \equiv \pm 2 \pmod{p}$, we conclude by Theorem 4.1.1 that

$$p \nmid \operatorname{ind}(\Phi) \quad \text{if and only if} \quad t \not\equiv \pm 2 \pmod{p^2},$$

completing the proof. □

In order to prove Theorem 1.2.1, we are left to show that the condition $\Phi(t) \not\equiv 0 \pmod{\ell^2}$ in Theorem 6.1.2 is equivalent to the condition $T_\ell(t) - t \not\equiv 0 \pmod{\ell^2}$. The following result will allow us to bridge this gap.

Proposition 6.1.3. *For any integers a and b,*

$$T_\ell(a) \equiv T_\ell(b) \pmod{\ell^2} \quad \text{if and only if} \quad a \equiv b \pmod{\ell}.$$

Proof. Suppose that $T_\ell(a) \equiv T_\ell(b) \pmod{\ell^2}$. By Proposition 2.2.1 (1), $T_\ell(x) = x^\ell + \ell g(x)$, where $g(x)$ is a polynomial of degree $\ell - 2$. Hence

$$\begin{aligned} T_\ell(a) \equiv T_\ell(b) \pmod{\ell^2} &\Rightarrow a^\ell + \ell\, g(a) \equiv b^\ell + \ell\, g(b) \pmod{\ell^2} \\ &\Rightarrow a^\ell \equiv b^\ell \pmod{\ell} \\ &\Rightarrow a \equiv b \pmod{\ell}. \end{aligned}$$

For the converse statement, let $a \in \mathbf{Z}$ and write $a = q\ell + r$ such that $0 \leq r < \ell$. It suffices to show that $T_\ell(a) \equiv T_\ell(r) \pmod{\ell^2}$. We have

$$\begin{aligned} T_\ell(a) = T_\ell(q\ell + r) &= \sum_{k=0}^{\lfloor \ell/2 \rfloor} (-1)^k \frac{(\ell - k - 1)!}{k!(\ell - 2k)!} \ell (q\ell + r)^{\ell - 2k} \\ &= \sum_{k=0}^{\lfloor \ell/2 \rfloor} (-1)^k \frac{(\ell - k - 1)!}{k!(\ell - 2k)!} \sum_{i=0}^{\ell - 2k} \binom{\ell - 2k}{i} q^i \ell^{i+1} r^{\ell - 2k - i} \\ &\equiv \sum_{k=0}^{\lfloor \ell/2 \rfloor} (-1)^k \frac{(\ell - k - 1)!}{k!(\ell - 2k)!} \ell r^{\ell - 2k} \\ &\equiv T_\ell(r) \pmod{\ell^2}. \end{aligned}$$

□

Proof of Theorem 1.2.1. By Lemma 6.1.1, we have $T_\ell^{n-1}(t) \equiv t \pmod{\ell}$, so by Proposition 6.1.3,

$$T_\ell^n(t) = T_\ell(T_\ell^{n-1}(t)) \equiv T_\ell(t) \pmod{\ell^2}.$$

Thus

$$T_\ell^n(t) \equiv t \pmod{\ell^2} \quad \text{if and only if} \quad T_\ell(t) \equiv t \pmod{\ell^2}.$$

The result is now an immediate consequence of Theorem 6.1.2. □

We conclude this section by identifying the equivalence classes for which $T_\ell(t) \equiv t \pmod{\ell^2}$.

Corollary 6.1.4. *$T_\ell(t) \equiv t \pmod{\ell^2}$ if and only if $T_\ell(a) \equiv t \pmod{\ell^2}$ for some $a \in \{0, 1, \ldots, \ell - 1\}$.*

Proof. Suppose that $T_\ell(a) \equiv t \pmod{\ell^2}$ for some $a \in \{0, \ldots, \ell-1\}$. Then $T_\ell(a) \equiv t \pmod{\ell}$, and by Lemma 6.1.1, $a \equiv t \pmod{\ell}$. Now by Proposition 6.1.3, $T_\ell(a) \equiv T_\ell(t) \pmod{\ell}$. The converse statement is satisfied by setting a to be the representative of t modulo ℓ in $\{0, \ldots, \ell-1\}$, then applying Proposition 6.1.3. □

In other words, $\ell \mid \mathrm{ind}(\Phi)$ if and only if the reduction of t modulo ℓ^2 has a representative in $\{T_\ell(0), T_\ell(1), \ldots, T_\ell(\ell-1)\}$.

6.2 The multiplicity of ℓ

For the remainder of the paper, we assume that ℓ is an odd prime and $t \not\equiv \pm 2 \pmod{\ell^2}$. We address the proof of Theorem 1.2.2 in two parts. In this section we compute $\mathrm{ind}_\ell(\Phi)$, the ℓ-adic valuation of $\mathrm{ind}(\Phi)$, and in the following section we compute $\mathrm{ind}_p(\Phi)$ for the primes dividing $t^2 - 4$. We remind the reader of our notation that $\Phi(x) = T_\ell^n(x) - t$, and $\mathrm{ind}(\Phi) = [\mathcal{O}_K : \mathbf{Z}[\theta]]$, where θ is a root of Φ, $K = \mathbf{Q}(\theta)$, and t is chosen so that $T_\ell^n(x) - t$ is irreducible for each $n \geq 1$. From Theorem 6.1.2, we know that $\Phi(t) \equiv 0 \pmod{\ell^2}$ is the necessary and sufficient condition for which $\mathrm{ind}_\ell(\Phi) > 1$. We recover this condition using the method of Guàrdia, Montes, Nart.

We tackle the computation of $\mathrm{ind}_\ell(\Phi)$ in two cases: first in the special case for $t \equiv 0 \pmod{\ell}$, and then in the general case where $t \not\equiv \pm 2 \pmod{\ell^2}$. Recall from Lemma 6.1.1 that $\Phi(x) \equiv (x-t)^{\ell^n} \pmod{\ell}$, so we only have one factor, $\phi(x) = x - t$, to consider in our analysis. The case where $t \equiv 0 \pmod{\ell}$ is simpler since the ϕ-Newton polygon is the standard Newton polygon of Φ, and a result of Kummer [22] will be sufficient for computing the ℓ-adic valuations of the coefficients of Φ. When $t \not\equiv 2 \pmod{\ell^2}$, we must derive the ϕ-development of Φ. We then use a series of lemmas, including a result of Lucas [27], in order to determine the ℓ-adic valuations of the coefficients in the ϕ-development. Once we construct the ϕ-Newton polygon, we apply Theorem 4.2.2 to give a formula for $\mathrm{ind}_\ell(\Phi)$.

We consider the case where $t \equiv 0 \pmod{\ell}$ and proceed by computing the Newton polygon of $T_\ell^n(x)$. By Proposition 2.2.1 (1), we have

$$T_\ell^n(x) = \sum_{k=0}^{\lfloor \ell^n/2 \rfloor} c_i x^{\ell^n - 2k}, \quad \text{where} \quad c_i = \frac{2\ell^n}{\ell^n + i}\binom{(\ell^n + i)/2}{(\ell^n - i)/2}.$$

Proposition 6.2.1. *For any integer $0 < i \leq \ell^m \leq \ell^n$, $\nu_\ell(c_i) \geq n - m$ with equality only if $i = \ell^m$.*

Proof. When $i = \ell^m$,

$$\nu_\ell(c_{\ell^m}) = n + \nu_\ell\binom{(\ell^n + \ell^m)/2}{(\ell^n - \ell^m)/2} - \nu_\ell(\ell^n + \ell^m).$$

Note that

$$\binom{(\ell^n + \ell^m)/2}{(\ell^n - \ell^m)/2} = \binom{(\ell^n + \ell^m)/2}{(\ell^n + \ell^m)/2 - (\ell^n - \ell^m)/2} = \binom{(\ell^n + \ell^m)/2}{\ell^m}.$$

The ℓ-adic valuation of this number can be determined using Lemma 4.3.1 by considering a sum in base ℓ. Writing

$$\frac{\ell^n + \ell^m}{2} - \ell^m = \frac{\ell - 1}{2} \cdot \ell^m + \frac{\ell - 1}{2} \cdot \ell^{m+1} + \cdots + \frac{\ell - 1}{2} \cdot \ell^n,$$

it is easy to see that

$$\left(\frac{\ell^n + \ell^m}{2} - \ell^m\right) + \ell^m = \frac{\ell + 1}{2} \cdot \ell^m + \frac{\ell - 1}{2} \cdot \ell^{m+1} + \cdots + \frac{\ell - 1}{2} \cdot \ell^n$$

requires no carries when summed in base ℓ. Thus by Lemma 4.3.1

$$\nu_\ell\binom{(\ell^n + \ell^m)/2}{(\ell^n - \ell^m)/2} = 0.$$

Furthermore,

$$\nu_\ell(\ell^n + \ell^m) = \nu_\ell(\ell^m) + \nu_\ell(\ell^{n-m} + 1) = m,$$

proving that $\nu_\ell(c_{\ell^m}) = n - m$.

If $0 < i < \ell^m$, then $\nu_\ell(\ell^n + i) = \nu_\ell(i) < m$. Hence

$$\nu_\ell(c_i) = n + \nu_\ell\binom{(\ell^n + i)/2}{(\ell^n - i)/2} - \nu_\ell(\ell^n + i) > n - m,$$

concluding the proof. □

Corollary 6.2.2. *The Newton polygon of $T_\ell^n(x)$ at ℓ is $\sum_{m=1}^n S_m$ where S_m is the edge with endpoints $(\ell^{m-1}, n - m + 1)$ and $(\ell^m, n - m)$.*

Proof. By Proposition 6.2.1, the polygon $\sum_{m=1}^n S_m$ is a tight lower bound for the points $\{(i, \nu_\ell(c_i)\}$. It is easily verified that this polygon is convex by considering the slope of S_m. □

Now that we have the Newton polygon for T_ℓ^n, we must only consider the ℓ-adic valuation of t to obtain the Newton polygon for Φ.

Corollary 6.2.3. *Suppose $t \equiv 0 \pmod{\ell}$, and let $v = \nu_\ell(t)$. Let S_m be the edge defined in Corollary 6.2.2. Define S' to be the edge with endpoints $(0, v)$ and $(\ell^{n-v+1}, v-1)$. Then*

$$N_\phi(\Phi) = S' + S_{n-v+2} + S_{n-v+3} + \cdots + S_n.$$

Proof. Let λ_m be the slope of S_m and λ' be the slope of S'. It suffices to show that $\lambda_{n-v+1} < \lambda' < \lambda_{n-v+2}$. This is easily verified:

$$\lambda_{n-v} = \frac{-1}{\ell^{n-v}(\ell-1)} \quad < \quad \lambda' = \frac{-1}{\ell^{n-v+1}} \quad < \quad \lambda_{n-v+2} = \frac{-1}{\ell^{n-v+1}(\ell-1)}.$$

□

We give a brief example to illustrate these results.

Example 6.2.4. Consider the polynomial $T_3^3(x) - t$. By Corollary 6.2.2, the Newton polygon of $T_3^3(x)$ is dictated by the points whose abscissa are powers of 3. From here, the Newton polygon of $T_3^3(x) - t$ is easily obtained. See Figure 9.

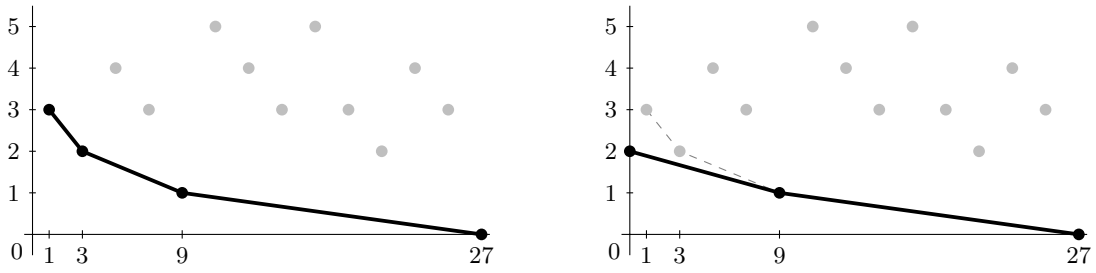


Figure 9: The Newton polygon of $T_3^3(x)$ (left) and the Newton polygon of $T_3^3(x) - 24$ (right) at 3. The 3-adic valuations of the other coefficients are marked in gray.

Now that we have determined the Newton polygon in the case where $t \equiv 0 \pmod{\ell}$, we move on to the case where $t \not\equiv \pm 2 \pmod{\ell^2}$. We begin by establishing the ϕ-development of Φ, where $\phi(x) = x - t$. Writing $\Phi(x) = \Phi(\phi(x) + t)$ and using the expression for T_d in Proposition 2.2.1 (1), we have

$$\begin{aligned} T_\ell^n(\phi + t) - t &= -t + \sum_{k=0}^{\lfloor \ell^n/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \frac{\ell^n}{\ell^n - k} (\phi + t)^{\ell^n - 2k} \\ &= -t + \sum_{k=0}^{\lfloor \ell^n/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \frac{\ell^n}{\ell^n - k} \sum_{i=0}^{\ell^n - 2k} \binom{\ell^n - 2k}{i} t^{\ell^n - 2k - i} \phi^i \\ &= -t + \sum_{i=0}^{\ell^n} \sum_{k=0}^{\lfloor (\ell^n - i)/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \binom{\ell^n - 2k}{i} \frac{\ell^n}{\ell^n - k} t^{\ell^n - 2k - i} \phi^i \end{aligned}$$

$$
\begin{aligned}
&= -t + \sum_{k=0}^{\lfloor \ell^n/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \frac{\ell^n}{\ell^n - k} t^{\ell^n - 2k} \\
&\qquad + \sum_{i=1}^{\ell^n} \sum_{k=0}^{\lfloor (\ell^n - i)/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \binom{\ell^n - 2k}{i} \frac{\ell^n}{\ell^n - k} t^{\ell^n - 2k - i} \phi^i \\
&= T_\ell^n(t) - t + \sum_{i=1}^{\ell^n} \sum_{k=0}^{\lfloor (\ell^n - i)/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \binom{\ell^n - 2k}{i} \frac{\ell^n}{\ell^n - k} t^{\ell^n - 2k - i} \phi^i \\
&= \Phi(t) + \sum_{i=1}^{\ell^n} \sum_{k=0}^{\lfloor (\ell^n - i)/2 \rfloor} (-1)^k \binom{\ell^n - k}{k} \binom{\ell^n - 2k}{i} \frac{\ell^n}{\ell^n - k} t^{\ell^n - 2k - i} \phi^i. \qquad (6.1)
\end{aligned}
$$

For ease, we will let

$$
b_i := \ell^n \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \binom{\ell^n - k}{k} \binom{\ell^n - 2k}{i} \frac{t^{\ell^n - 2k - i}}{\ell^n - k}
$$

denote the coefficient of ϕ^i for $1 \leq i \leq \ell^n$.

Lemma 6.2.5. *For positive integers a, b, and c satisfying $0 \leq b \leq \frac{a-c}{2}$, the binomial coefficients satisfy the following relationship:*

$$
\binom{a-b}{b}\binom{a-2b}{c} = \binom{a-b-c}{b}\binom{a-b}{c}.
$$

Proof.

$$
\begin{aligned}
\binom{a-b}{b}\binom{a-2b}{c} &= \frac{(a-b)!}{b!(a-2b!)} \cdot \frac{(a-2b)!}{c!(a-2b-c)!} = \frac{(a-b)!}{c!(a-b-c)!} \cdot \frac{(a-b-c)!}{b!(a-2b-c)!} \\
&= \binom{a-b-c}{b}\binom{a-b}{c}.
\end{aligned}
$$

□

We use this lemma to rewrite b_i in the following way.

$$
\begin{aligned}
b_i &= \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \frac{\ell^n}{\ell^n - k} \binom{\ell^n - k}{k} \binom{\ell^n - 2k}{i} t^{\ell^n - 2k - i} \\
&= \frac{\ell^n}{i} \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \binom{\ell^n - i - k}{k} \binom{\ell^n - k - 1}{i - 1} t^{\ell^n - 2k - i}.
\end{aligned}
$$

This new expression simplifies the ℓ-adic expansions of the numbers in the binomial coefficients, which set us up nicely to apply Lemma 4.3.2 for computing the ℓ-adic valuations of these numbers.

Lemma 6.2.6. *Let ℓ be an odd prime. If $x \neq \pm 2 \bmod \ell$, then $U_{\ell-1}(x) = \pm 1 \bmod \ell$.*

Proof. Let $x \in \mathbf{F}_\ell$ and $x \neq \pm 2$. Set $\alpha = \frac{x+\sqrt{x^2-4}}{2} \in \mathbf{F}_{\ell^2}$ and $\beta = \frac{x-\sqrt{x^2-4}}{2} \in \mathbf{F}_{\ell^2}$. From Proposition 2.2.1 (2), we have

$$U_d(x) = \frac{\left(x+\sqrt{x^2-4}\right)^{d+1} - \left(x-\sqrt{x^2-4}\right)^{d+1}}{2^{d+1}\sqrt{x^2-4}}.$$

Recall that the Frobenius map on $\mathbf{F}_{\ell^2}$ fixes $\mathbf{F}_\ell$ and acts by conjugation away from $\mathbf{F}_\ell$. Hence, if $\sqrt{x^2-4} \in \mathbf{F}_\ell$, then $\alpha^\ell = \alpha$, $\beta^\ell = \beta$, and

$$U_{\ell-1}(x) = \frac{\alpha - \beta}{\sqrt{x^2-4}} = 1 \bmod \ell.$$

Otherwise, if $\sqrt{x^2-4} \notin \mathbf{F}_\ell$, then $\alpha^\ell = \beta$, $\beta^\ell = \alpha$, and

$$U_{\ell-1}(x) = \frac{\beta - \alpha}{\sqrt{x^2-4}} = -1 \bmod \ell.$$

□

Theorem 6.2.7. *Suppose that $t \not\equiv \pm 2 \pmod{\ell^2}$, $\Phi(t) \equiv 0 \pmod{\ell^2}$, and let i be an integer satisfying $\ell^m \leq i < \ell^{m+1}$ and $m < n$. Then $\nu_\ell(b_i) \geq n - m$ with equality if $i = \ell^m$.*

Proof. Assume first that $i = \ell^m + \varepsilon$ for some integer $0 < \varepsilon < (\ell-1)\ell^m$. We show that $\nu_\ell(b_i) \geq n - m$. Note that

$$\begin{aligned}
\binom{\ell^n - k - 1}{\ell^m + \varepsilon - 1} &= \frac{(\ell^n - k - 1)!}{(\ell^m + \varepsilon)!(\ell^n - \ell^m - k - \varepsilon)!} \\
&= \frac{(\ell^n - k - 1)!}{\ell^m(\ell^m - 1)!(\ell^n - \ell^m - k)!} \frac{\ell^m!\varepsilon!}{(\ell^m + \varepsilon)!} \frac{(\ell^n - \ell^m - k)!}{\varepsilon!(\ell^n - \ell^m - k - \varepsilon)!} \\
&= \frac{\binom{\ell^n - k - 1}{\ell^m - 1}\binom{\ell^n - \ell^m - k}{\varepsilon}}{\binom{\ell^m + \varepsilon}{\ell^m}}.
\end{aligned}$$

Hence,

$$\begin{aligned}
b_i &= \frac{\ell^n}{\ell^m + \varepsilon} \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \binom{\ell^n - i - k}{k} \binom{\ell^n - k - 1}{\ell^m + \varepsilon - 1} t^{\ell^n - 2k - i} \\
&= \frac{\ell^{n-m}}{\binom{\ell^m + \varepsilon}{\ell^m}} \sum_{k=0}^{\lfloor \frac{\ell^n - i}{2} \rfloor} (-1)^k \binom{\ell^n - i - k}{k} \binom{\ell^n - k - 1}{\ell^m - 1} \binom{\ell^n - \ell^m - k}{\varepsilon} t^{\ell^n - 2k - i}.
\end{aligned}$$

By Lemma 4.3.1, $\nu_\ell\binom{\ell^m + \varepsilon}{\ell^m} = 0$ since $\ell^m + \varepsilon$ requires no carries in base ℓ. Furthermore, the summation evaluates to an integer, so its valuation is non-negative. Thus $\nu_\ell(b_i) \geq n - m$.

Assume now that $i = \ell^m$, and consider

$$b_{\ell^m} = \ell^{n-m} \sum_{k=0}^{\frac{\ell^n - \ell^m}{2}} (-1)^k \binom{\ell^n - \ell^m - k}{k} \binom{\ell^n - k - 1}{\ell^m - 1} t^{\ell^n - \ell^m - 2k}. \tag{6.2}$$

To show that $\nu_\ell(b_{\ell^m}) = n - m$, we show that $\ell^{m-n} b_{\ell^m}$ is relatively prime to ℓ. It suffices to sum over the terms that are relatively prime to ℓ and show that the sum of these terms is not divisible by ℓ. We write the following numbers in their base-ℓ expansions.

$$k = \sum_{j=0}^{n-1} k_j \ell^j; \qquad \ell^m - 1 = \sum_{j=0}^{m-1} (\ell - 1)\ell^j; \qquad \ell^n - k - 1 = \sum_{j=0}^{n-1} (\ell - k_j - 1)\ell^j.$$

By Lemma 4.3.2, the second binomial coefficient in Equation (6.2) satisfies

$$\begin{aligned}\binom{\ell^n - k - 1}{\ell^m - 1} &\equiv \binom{\ell - k_0 - 1}{\ell - 1} \cdots \binom{\ell - k_{m-1} - 1}{\ell - 1} \binom{\ell - k_m - 1}{0} \cdots \binom{\ell - k_{n-1} - 1}{0} \pmod{\ell} \\ &\equiv \begin{cases} 1 \pmod{\ell} & \text{if } k_0 = \cdots = k_{m-1} = 0 \\ 0 \pmod{\ell} & \text{otherwise.} \end{cases}\end{aligned}$$

That is, $\binom{\ell^n - k - 1}{\ell^m - 1}$ is relatively prime to ℓ if and only if $\ell^m \mid k$. Since we are only interested in the terms that are relatively prime to ℓ, we continue with the additional assumption that ℓ^m divides k. Now, the base-ℓ expansion of $\ell^n - \ell^m - k$ is

$$\ell^n - \ell^m - k = \sum_{j=m}^{n-1} (\ell - k_j - 1)\ell^j.$$

Applying Lemma 4.3.2 to the first binomial coefficient in Equation (6.2), we see that

$$\binom{\ell^n - \ell^m - k}{k} \equiv \binom{\ell - k_m - 1}{k_m} \cdots \binom{\ell - k_{n-1} - 1}{k_{n-1}} \pmod{\ell},$$

which is nonzero if and only if $0 \le k_j \le (\ell - 1)/2$ for each $j = m, m+1, \ldots, n-1$. We have the following:

$$\begin{aligned}\ell^{m-n} b_{\ell^m} &= \sum_{k=0}^{\frac{\ell^n - \ell^m}{2}} (-1)^k \binom{\ell^n - \ell^m - k}{k} \binom{\ell^n - k - 1}{\ell^m - 1} t^{\ell^n - \ell^m - 2k} \\ &\equiv \sum_{k=0}^{\frac{\ell^n - \ell^m}{2}} (-1)^k \binom{\ell - k_m - 1}{k_m} \cdots \binom{\ell - k_{n-1} - 1}{k_{n-1}} t^{\ell^n - \ell^m - 2k} \\ &\equiv \prod_{j=m}^{n-1} \sum_{k_j=0}^{\frac{\ell-1}{2}} (-1)^{k_j} \binom{\ell - k_j - 1}{k_j} t^{\ell - 2k_j - 1} \\ &\equiv (U_{\ell-1}(t))^{n-m} \equiv \pm 1 \pmod{\ell}.\end{aligned}$$

The second to last step takes advantage of the fact that $t^{\ell^n - \ell^m} \equiv t^{\ell - 1} \equiv 1 \pmod{\ell}$, and the final step follows from Proposition 2.2.1 (1) and Lemma 6.2.6. This concludes the proof. □

Remark 6.2.8. We note that Theorem 6.2.7 assumes that $t \not\equiv \pm 2 \pmod{\ell^2}$, yet in the proof we apply Lemma 6.2.6, which requires that $t \not\equiv \pm 2 \pmod{\ell}$. However, since we are assuming

that $\Phi(t) \equiv 0 \pmod{\ell^2}$, these conditions are equivalent thanks to Corollary 6.1.4. Specifically, if $t \equiv \pm 2 \pmod{\ell^2}$ and $T_\ell(t) - t \equiv 0 \pmod{\ell^2}$, then $t \equiv \pm 2 \pmod{\ell}$.

Remark 6.2.9. We note that in this case, an alternative method for obtaining the ϕ-development is given by the Taylor expansion formula:

$$\Phi(x) = \Phi(t) + \Phi'(t)\phi(x) + \frac{1}{2}\Phi''(t)\phi(x)^2 + \cdots + \frac{1}{\ell^n!}\Phi^{(\ell^n)}(t)\phi(x)^{\ell^n}.$$

In fact, Theorem 6.2.7 subsumes Proposition 6.2.1 as it includes the case $t \equiv 0 \pmod{\ell}$, and we see that, except for the constant term, the ℓ-adic valuations of the coefficients of $T_\ell^n(x)$ are invariant under the shift $T_\ell^n(x) \mapsto T_\ell^n(x-t)$ whenever $\Phi(t) \equiv 0 \pmod{\ell^2}$ and $t \not\equiv \pm 2 \pmod{\ell^2}$. Similar to Corollary 6.2.3, we only need to consider the ℓ-adic valuation of $\Phi(t)$ (see Equation (6.1)) to obtain the ϕ-Newton polygon of Φ.

Corollary 6.2.10. *Suppose $t \not\equiv \pm 2 \pmod{\ell^2}$. Let $v = \nu_\ell(\Phi(t))$, and let S_m denote the edge from $(\ell^{m-1}, n-m+1)$ to $(\ell^m, n-m)$ and S' to be the edge from $(0, v)$ to $(\ell^{n-v+1}, v-1)$. Then the ϕ-Newton polygon of Φ is*

$$N_\phi(\Phi) = S' + S_{n-v+2} + \cdots + S_n.$$

Proof. The proof is the same as in Corollary 6.2.3. □

Theorem 6.2.11. *Suppose $t \not\equiv \pm 2 \pmod{\ell^2}$, and set $v = \nu_\ell(\Phi(t))$. Then*

$$\mathrm{ind}_\ell(\Phi) = \sum_{i=1}^{\min\{v-1,n\}} \ell^{n-i}.$$

Proof. It is easy to verify that each side of the ϕ-Newton polygon given in Corollary 6.2.10 has length 1. Hence every residual polynomial attached to the polygon has degree 1, and it follows that Φ is ℓ-regular. By Theorem 4.2.2, the ℓ-adic valuation of the index is equal to the number of points with integral coordinates under the polygon. The lattice points are arranged into rows whose lengths are decreasing powers of ℓ, giving the formula for $\mathrm{ind}_\ell(\Phi)$. □

Remark 6.2.12. We note that $\nu_\ell(\Phi(t)) \geq 1$ since $\Phi(t)$ is the constant term in the ϕ-development of Φ, and $\Phi(x) \equiv (x-t)^{\ell^n} \equiv \phi(x)^{\ell^n} \pmod{\ell}$. Hence if $\Phi(t) \not\equiv 0 \pmod{\ell^2}$, then $\nu_\ell(\Phi(t)) = 1$, and the ϕ-Newton polygon of Φ is one-sided with vertices $(0,1)$ and $(\ell^n, 0)$. There are no lattice points on or under this side, so by Theorem 4.2.2, we have $\mathrm{ind}_\ell(\Phi) = 0$. We have thus recovered the condition in Theorem 6.1.2 that $\ell \mid \mathrm{ind}(\Phi)$ if and only if $\Phi(t) \equiv 0 \pmod{\ell^2}$.

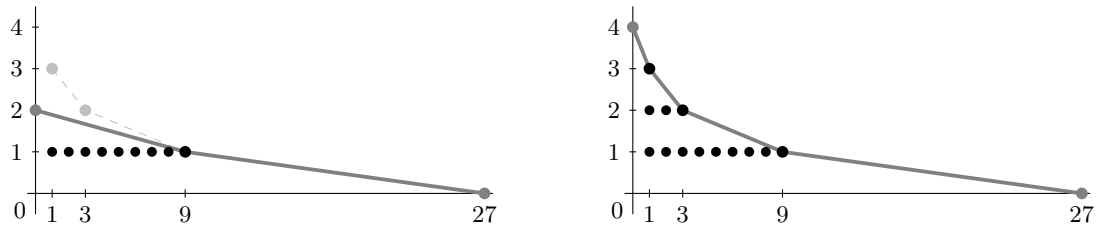


Figure 10: Left: the ϕ-Newton polygon for $T_3^3(x) - 24$. We have $\mathrm{ind}_3(T_3^3(x) - 24) = 9$. Right: the ϕ-Newton polygon for $T_3^3(x) - 81$. It follows that $\mathrm{ind}_3(T_3^3(x) - 81) = 13$.

We illustrate Theorem 6.2.11 with an example.

Example 6.2.13. Consider the polynomial $T_3^3(x) - t$. From Corollary 6.2.10, we see that the sides of the polygon are length 1, meaning that each side does not intersect any integral lattice points other than its endpoints. The points with integral coordinates on or under the polygon are arranged into rows whose lengths are decreasing powers of 3. See Figure 10.

6.3 The multiplicity of p

As in the previous section, we maintain the assumption that ℓ is an odd prime and $t \not\equiv \pm 2 \pmod{\ell^2}$. Moreover, we assume that p is an odd prime different from ℓ for which $t \equiv \pm 2 \pmod{p^2}$. By Theorem 6.1.2, the condition $t \equiv \pm 2 \pmod{p^2}$ is the necessary and sufficient condition for which $p \mid \mathrm{ind}(\Phi)$. In this section, we compute $\mathrm{ind}_p(\Phi)$, again using Theorem 4.2.2, completing the proof of Theorem 1.2.2. In the previous section, we found that the ℓ-regularity of Φ comes immediately from the shape of the ϕ-Newton polygon. In this case, there is no guarantee that Φ is p-regular. However by taking appropriate lifts of the irreducible factors of Φ, we find that the lower bound given by Theorem 4.2.2 meets the upper bound provided by p-adic valuation of D_Φ, giving the result. Consider the following example.

Example 6.3.1. Let $t_0 = 29284$, and consider the polynomial $T_5(x) - t_0$. We have chosen the constant term so that $t_0 - 2$ and $t_0 + 2$ are not square-free:

$$t_0 - 2 = 2 \cdot 3^2 \cdot 1627 \quad \text{and} \quad t_0 + 2 = 2 \cdot 11^4,$$

By Theorem 6.1.2, the primes 3 and 11 divide $\mathrm{ind}(T_5(x) - t_0)$, and 5 does not. We have

$$T_5(x) - t_0 \equiv (x+2)(x^2 - x - 1)^2 \pmod{3}, \quad \text{and}$$

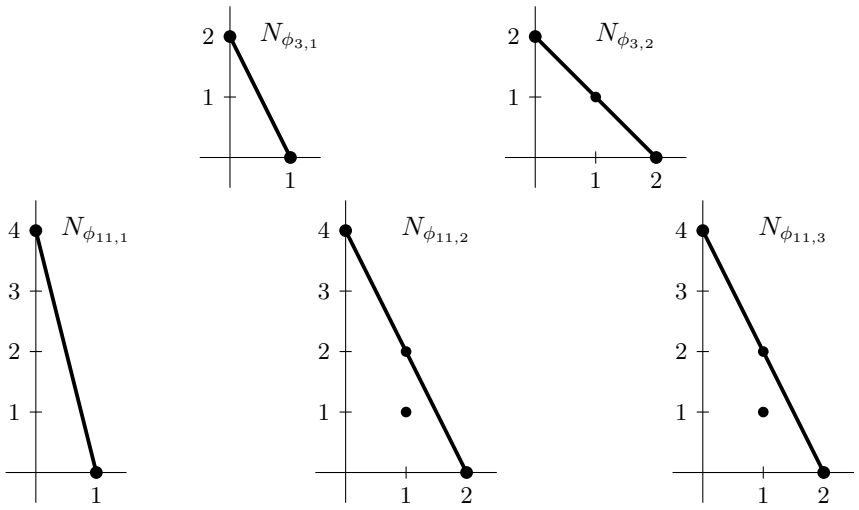


Figure 11: ϕ-Newton polygons associated to $T_5(x) - t_0$ in Example 6.3.1.

$$T_5(x) - t_0 \equiv (x-2)(x-3)^2(x+4)^2 \pmod{11}.$$

Take

$$\phi_{3,1}(x) = x + 2, \qquad \phi_{3,2}(x) = x^2 - x - 1,$$
$$\phi_{11,1}(x) = x - 2, \qquad \phi_{11,2}(x) = x - 4029, \qquad \phi_{11,3}(x) = x + 4030,$$

as lifts of the irreducible factors of $T_5(x) - t_0$ modulo 3 and 11. Each lift ϕ is chosen so as to "maximize" the valuation of the constant term in the ϕ-development. The ϕ-developments of $T_5(x) - t_0$ are

$$\begin{aligned}
T_5(x) - t_0 &= -29286 + 25\,\phi_{3,1}(x) - 50\,\phi_{3,1}(x)^2 + 35\,\phi_{3,1}(x)^3 - 10\,\phi_{3,1}(x)^4 + \phi_{5,1}(x)^5,\\
T_5(x) - t_0 &= -29286 + (x+2)\phi_{3,2}(x)^2,\\
T_5(x) - t_0 &= -29282 + 25\,\phi_{11,1}(x) + 50\,\phi_{11,1}(x)^2 + 35\,\phi_{11,1}(x)^3 + 10\,\phi_{11,1}(x)^4 + \phi_{11,1}(x)^5,\\
T_5(x) - t_0 &= 1061661829395540065 + 1317525391163795\,\phi_{11,2}(x) + 654021103455\,\phi_{11,2}(x)^2\\
&\qquad + 162328405\,\phi_{11,2}(x)^3 + 20145\,\phi_{11,2}(x)^4 + \phi_{11,2}(x)^5,\\
T_5(x) - t_0 &= -1062980008970214434 + 1318833920436505\,\phi_{11,3}(x) - 654508209550\,\phi_{11,3}(x)^2\\
&\qquad + 162408995\,\phi_{11,3}(x)^3 - 20150\,\phi_{11,3}(x)^4 + \phi_{11,3}(x)^5.
\end{aligned}$$

From the ϕ-Newton polygons (Figure 11), we see that the factors $\phi_{3,1}$ and $\phi_{11,1}$ do not contribute to the index since there are no lattice points on or under their polygons. Let R_ϕ denote the

residual polynomial attached to ϕ. The residual polynomials attached to the other factors are

$$R_{\phi_{3,2}}(y) = (\theta_{3,2} - 1)y^2 + 1, \quad \text{where } \theta_{3,2} \text{ is a root of } \phi_{3,2},$$
$$R_{\phi_{11,2}}(y) = 5y^2 + 5y - 2, \quad \text{and} \quad R_{\phi_{11,3}}(y) = 3y^2 - 3y - 2.$$

The residual polynomials $R_{\phi_{3,2}}$ and $R_{\phi_{11,2}}$ are separable, but $R_{\phi_{11,3}}$ is not. Hence $T_5(x) - t_0$ is 3-regular, but not 11-regular. In fact, it is not possible to find a lift of $x - 4$ for which $T_5(x) - t_0$ is 11-regular. By Theorem 4.2.2, we have

$$\operatorname{ind}_3(T_5(x) - t_0) = 2 \quad \text{and} \quad \operatorname{ind}_{11}(T_5(x) - t_0) \geq 4.$$

But, by Proposition 3.4.1, we also have

$$\operatorname{ind}_{11}(T_5(x) - t_0) \leq \frac{1}{2}\nu_{11}(D_{T_5(x)-t_0}) = \nu_{11}(t_0^2 - 4) = 4.$$

Thus $\operatorname{ind}(T_5(x) - t_0) = 3^2 \cdot 11^4$. This result is verified by `PARI`.

In this example, we see that there is a certain uniformity to the ϕ-Newton polygons provided that we pick suitable lifts for each of the irreducible factors. Following Lemma 6.1.1, we write

$$\Phi(x) \equiv (x \pm 2)\phi_1(x)^2 \cdots \phi_r(x)^2 \pmod{p}, \tag{6.3}$$

where $\phi_i(x)$ are irreducible factors modulo p. We prove the following.

Proposition 6.3.2. *Let $p \neq \ell$ be an odd prime such that $t \equiv \pm 2 \pmod{p^2}$. Then for each irreducible factor ϕ_i in Equation (6.3), there exists a monic lift $\hat{\phi}_i$ of ϕ_i such that $\hat{\phi}_i \equiv \phi_i \pmod{p}$, and the $\hat{\phi}_i$-polynomial is one-sided with vertices $(0, \nu_p(t^2 - 4))$ and $(2, 0)$. Hence*

$$\operatorname{ind}_{\hat{\phi}_i}(\Phi) = \left\lfloor \frac{\nu_p(t^2 - 4)}{2} \right\rfloor \deg(\hat{\phi}_i).$$

Moreover, the factor $x \pm 2$ does not contribute to $\operatorname{ind}_p(\Phi)$, that is, $\operatorname{ind}_{(x\pm 2)}(\Phi) = 0$.

Consequently, if $\nu_p(t^2 - 4)$ is odd, then the residual polynomial associated with the $\hat{\phi}_i$-polygon is degree 1. Hence Φ is p-regular, and by Theorem 4.2.2,

$$\operatorname{ind}_p(\Phi) = \sum_{i=1}^{r} \left\lfloor \frac{\nu_p(t^2 - 4)}{2} \right\rfloor \deg(\hat{\phi}_i) = \left\lfloor \frac{\nu_p(t^2 - 4)}{2} \right\rfloor \frac{\ell^n - 1}{2}.$$

If $\nu_p(t^2 - 4)$ is even, regularity is not guaranteed since the residual polynomial is degree 2, so at best, we have from Theorem 4.2.2 that

$$\operatorname{ind}_p(\Phi) \geq \sum_{i=1}^{r} \left\lfloor \frac{\nu_p(t^2 - 4)}{2} \right\rfloor \deg(\hat{\phi}_i) = \frac{\nu_p(t^2 - 4)}{2} \frac{\ell^n - 1}{2}.$$

On the other hand, the valuation of the index is bounded by the p-adic valuation of D_Φ. Namely by Proposition 3.4.1

$$\mathrm{ind}_p(\Phi) \leq \frac{1}{2}\nu_p\left((t^2-4)^{(\ell^n-1)/2}\right) = \frac{\nu_p(t^2-4)}{2}\frac{\ell^n-1}{2}.$$

Thus we have derived the following result.

Corollary 6.3.3. *If $p \neq \ell$ is an odd prime and $t \equiv \pm 2 \pmod{p^2}$, then*

$$\mathrm{ind}_p(\Phi) = \left\lfloor \frac{\nu_p(t^2-4)}{2} \right\rfloor \frac{\ell^n-1}{2}.$$

Proof of Theorem 1.2.2. The multiplicity of each odd prime divisor of $\mathrm{ind}(\Phi)$ are given by Theorem 6.2.11 and Corollary 6.3.3. The formula for Δ_K follows form Equation (1.1). □

We conclude this section with the proof of Proposition 6.3.2.

Proof. (Proposition 6.3.2) From Lemma 6.1.1, $T_\ell^n(x) \pm 2 = (x \pm 2)\tau(x)^2$ where

$$\tau(x) \equiv \phi_1(x)\cdots\phi_r(x) \pmod{p}.$$

Since τ has no repeated roots modulo p, Hensel lifting ensures that there exist lifts $\hat{\phi}_1, \ldots, \hat{\phi}_r$ such that

$$\tau(x) \equiv \hat{\phi}_1(x)\cdots\hat{\phi}_r(x) \pmod{p^e}$$

for e arbitrarily large. Take $e > \nu_p(t^2-4)$ (although $e > \nu_p(t^2-4)/2$ would be sufficient) and fix a lift $\phi = \hat{\phi}_i$. Then the ϕ-development of $T_\ell^n(x) \pm 2$ is

$$T_\ell^n(x) \pm 2 = A_0(x) + A_1(x)\phi(x) + A_2(x)\phi(x)^2 + \cdots.$$

Note that $T_\ell^n(x) \pm 2 = (x \pm 2)\tau(x)^2 \equiv (x \pm 2)\hat{\phi}_1(x)^2\cdots\hat{\phi}_r(x)^2 \pmod{p^e}$, hence $\nu_p(A_2) = 0$ and

$$A_0(x) + A_1(x)\phi(x) \equiv 0 \pmod{p^e}.$$

In particular, since ϕ is monic, $\nu_p(A_0) \geq \nu_p(A_1) \geq e > \nu_p(t^2-4)$. Thus the ϕ-development of Φ is

$$\begin{aligned}\Phi(x) &= T_\ell^n(x) - t = T_\ell^n(x) - \overline{t} + \overline{t} - t \\ &= \overline{t} - t + A_0(x) + A_1(x)\phi(x) + A_2(x)\phi(x)^2 + \cdots,\end{aligned}$$

where $\nu_p(\overline{t} - t + A_0) = \nu_p(\overline{t} - t) = \nu_p(t^2 - 4), \nu_p(A_1) > \nu_p(t^2 - 4)$, and $\nu_p(A_2) = 0$, and therefore $\hat{\phi}_1, \ldots, \hat{\phi}_r$ provide desired lifts.

We now show that $\mathrm{ind}_{(x\pm 2)}(\Phi) = 0$. The $(x \pm 2)$-development is given by Taylor's expansion centered at ± 2:

$$\begin{aligned}\Phi(x) &= \Phi(\pm 2) + \Phi'(\pm 2)(x \pm 2) + \cdots \\ &= \Phi(\pm 2) + \ell^n U_{\ell^n - 1}(\pm 2)(x \pm 2) + \cdots,\end{aligned}$$

where U_d denotes the degree-d Chebyshev polynomial of the second kind. By the recursion formula in Proposition 2.2.1 (3), it is a straightforward induction to show that $U_d(2) = d + 1$. Moreover, since $U_{\ell^n - 1}$ is an even function (Proposition 2.2.1 (4)), it follows that $\nu_p(\ell^n U_{\ell^n - 1}(\pm 2)) = \nu_p(\ell^{2n}) = 0$, and thus the $(x \pm 2)$-polygon is one-sided with vertices $(0, \nu_p(\Phi(\pm 2)))$ and $(1, 0)$. We conclude that $\mathrm{ind}_{(x\pm 2)}(\Phi) = 0$. □

6.4 Integral basis

The Montes algorithm also provides an efficient method for determining an integral basis for the ring of integers $\mathcal{O}_K$. In this section we summarize their procedure as it pertains to our situation.

For this discussion we assume that Φ is regular with respect to every prime. Fix a prime p for which $\mathbf{Z}[\theta]$ is not maximal. Let $\hat{\phi}_i$ be a lift of an irreducible factor of $\overline{\Phi}$ for which Φ is $\hat{\phi}_i$-regular. We define the quotients attached to the $\hat{\phi}_i$-developement of Φ to be the polynomials

$$\begin{aligned}\Phi(x) &= \hat{\phi}_i(x) q_{i,1}(x) + a_{i,0}(x) \\ q_{i,1}(x) &= \hat{\phi}_i(x) q_{i,2}(x) + a_{i,1}(x) \\ &\vdots \\ q_{i,r-1}(x) &= \hat{\phi}_i(x) q_{i,r}(x) + a_{i,r-1}(x) \\ q_{i,r}(x) &= a_{i,r}(x).\end{aligned}$$

Additionally, for $1 \leq j \leq r$, we identify the points $(j, y_{i,j})$ on the polygon $N_{\hat{\phi}_i}(\Phi)$.

Proposition 6.4.1. *The collection $\{q_{i,j}(\theta)/p^{\lfloor y_{i,j} \rfloor}\}$ contains a p-integral basis for $\mathcal{O}_K$.*

Proof. This is a specialization of [10, Theorem 2.6]. □

In Corollary 6.2.10, we determined the ϕ-polygon for Φ for certain values of t. Under these same conditions, we determine a basis for the ring $\mathcal{O}_K$.

Proposition 6.4.2. *Suppose that $t-2$ and $t+2$ are square-free, $\Phi(t) \equiv 0 \pmod{\ell^2}$. Let $v = \min\{\nu_\ell(\Phi(t)) - 1, n\}$. Then a basis for $\mathcal{O}_K$ is*

$$\left\{\theta, \frac{q_{\ell^{n-1}}(\theta)}{\ell}, \frac{q_{\ell^{n-2}}(\theta)}{\ell^2}, \ldots, \frac{q_{\ell^{n-v}}(\theta)}{\ell^v}\right\}.$$

Proof. Recall that $\Phi(x) = T_\ell^n(x) - t \equiv (x-t)^{\ell^n} \pmod{\ell}$, so let $\phi(x) = x - \overline{t}$. In Corollary 6.2.10 we determined $N_\phi(\Phi)$ and showed that Φ is ℓ-regular. For each $1 \leq j \leq \ell^n$, the quotient $q_j(x)$ is a monic polynomial of degree $\ell^n - j$, and these quotients satisfy the recursion $q_j(x) = \phi(x)q_{j+1}(x) + a_j$ where $q_{\ell^n}(x) = 1$. By definition, $\nu_\ell(a_j) \geq \lfloor y_j \rfloor$. Hence if $\lfloor y_{j+1} \rfloor = \lfloor y_j \rfloor$, then $q_{j+1}(\theta)/\ell^{\lfloor y_{j+1} \rfloor} \in \mathcal{O}_K$ implies that $q_j(\theta)/\ell^{\lfloor y_j \rfloor} \in \mathcal{O}_K$. It follows that

$$\mathcal{O}_K = \mathbf{Z}\left[\frac{q_{\ell^n}(\theta)}{\ell^{\lfloor y_{\ell^n} \rfloor}}, \ldots, \frac{q_1(\theta)}{\ell^{\lfloor y_1 \rfloor}}\right] = \mathbf{Z}\left[\theta, \frac{q_{\ell^{n-1}}(\theta)}{\ell}, \frac{q_{\ell^{n-2}}(\theta)}{\ell^2}, \ldots, \frac{q_{\ell^{n-v}}(\theta)}{\ell^v}\right].$$

□

6.5 Dickson-(-1) extensions

Having done the calculations for the Chebyshev polynomials, we obtain the same results for the Dickson-(-1) maps essentially for free. The coefficients of the Dickson-(-1) polynomials only differ from the coefficients of the Chebyshev polynomials by a sign, and thus all the arguments in the previous section can be adapted to the Dickson-(-1) case by simply removing the $(-1)^k$ at every step, and replacing U_d with $\mathcal{E}_d$ where appropriate.

As before, let ℓ be an odd prime, and let $t \in \mathbf{Z}$ be chosen such that $\mathcal{D}_\ell^n(x) - t$ is irreducible for each $n \geq 1$. Moreover, we make the additional simplifying assumption that t is an odd integer. This assumption will allow us to avoid any additional difficulties in dealing with the prime 2. From Proposition 3.4.1, the primes that divide $\operatorname{disc}(\mathcal{D}_\ell^n(x) - t)$ are the primes dividing $t^2 + 4$ and the prime ℓ.

Lemma 6.5.1. *We have $\mathcal{D}_\ell^n(x) - t \equiv (x-t)^{\ell^n} \pmod{\ell}$. For any odd prime p dividing t^2+4, we have $\mathcal{D}_\ell^n(x) - t \equiv (x-t)\tau(x)^2 \pmod{p}$ for some $\tau \in \mathbf{F}_p[x]$.*

Proof. The result may be obtained by applying the twist from Propositionprop:d prop (1) to Lemma 6.1.1. This result may also be derived from the theory of the graphs (Theorem 3.1.8). □

Once again, Dedekind's criterion (Theorem 4.1.1) gives conditions on t that yield monogenic towers.

Theorem 6.5.2. *Let ℓ be a prime and let $K = \mathbf{Q}(\theta)$, where θ is a root of $\mathcal{D}_\ell^n(x) - t$. If $\mathcal{D}_\ell(t) - t \not\equiv 0 \pmod{\ell^2}$ and $t^2 + 4$ is square-free, then K is monogenic, as $[\mathcal{O}_K : \mathbf{Z}[\theta]] = 1$.*

Proof. The result can be obtained by mirroring the proof of Theorem 1.2.1. See Section 6.1. □

Likewise, we can apply the Montes algorithm to obtain an explicit formula for the index.

Theorem 6.5.3. *Let ℓ be an odd prime and $K = \mathbf{Q}(\theta)$, where θ is a root of $\mathcal{D}_\ell^n(x) - t$, t is an odd integer, and $t^2 + 4 \not\equiv 0 \pmod{\ell^2}$. Write $t^2 + 4 = A^2 B$, where B is square-free. Then*

$$\operatorname{ind}(\mathcal{D}_\ell^n(x) - t) = \ell^E A^{(\ell^n - 1)/2}, \quad \text{where} \quad E = \sum_{i=1}^{\min\{\nu_\ell(\mathcal{D}_{\ell^n}(t) - t) - 1, n\}} \ell^{n-i}.$$

Moreover, $\Delta_K = \ell^{n\ell^n - 2E} B^{(\ell^n - 1)/2}$.

Proof. The result can be obtained by mirroring the proof of Theorem 1.2.2. See Section 6.2 and Section 6.3. □

CHAPTER 7

GENERALIZED RIKUNA EXTENSIONS

Finally, we address the iterated extensions arising from generalized Rikuna polynomials $r_n(x,t;\ell)$. As before, ℓ is an odd prime, and t is chosen so that $r_n(x,t;\ell)$ is irreducible for each $n \geq 1$. Unlike for the previous families of polynomials, Dedekind's criterion only identifies a single case where the generalized Rikuna polynomial admits a monogenic extension. We then apply the Montes algorithm to compute the index for the case $\ell = 3$.

7.1 Factorization results

Here we give two small, but useful, factorization results. We recall from Proposition 2.4.1 and Proposition 2.4.2 that the generalized Rikuna polynomial is given by

$$r_n(x,t;\ell) = \frac{(t-\zeta)(x-\zeta^{-1})^{\ell^n} - (t-\zeta^{-1})(x-\zeta)^{\ell^n}}{\zeta^{-1}-\zeta}$$

and

$$r_n(x,t;\ell) = x^{\ell^n} - \ell^n t x^{\ell^n-1} + \sum_{k=2}^{\ell^n} (-1)^k \binom{\ell^n}{k} \Big(t\, U_{k-1}(\zeta^+) - U_{k-2}(\zeta^+) \Big) x^{\ell^n-k},$$

where ζ is a primitive ℓ-th root of unity, and $\zeta^+ := \zeta + \zeta^{-1}$.

Lemma 7.1.1. *Let $\mathfrak{a} \subset \mathcal{O}_K$ be any ideal for which $t = \zeta \bmod \mathfrak{a}$. Then $r_n(x,t;\ell) = (x-t)^{\ell^n} \in (\mathcal{O}_K/\mathfrak{a})[x]$.*

Proof. The result follows immediately from Proposition 2.4.1. □

Note that if ℓ is an odd prime, then the ideal (ℓ) is totally ramified in $K = \mathbf{Q}(\zeta^+)$.

Lemma 7.1.2. *Let ℓ be an odd prime, and let $\mathfrak{l} \subset \mathcal{O}_K$ be the prime ideal containing (ℓ). Then $r_n(x,t;\ell) = (x-1)^{\ell^n} \in (\mathcal{O}_K/\mathfrak{l})[x]$.*

Proof. Note that $\zeta^+ = 2\cos(2n/\ell)$, so by Proposition 2.2.1 (4),

$$U_{\ell^n-1}(\zeta^+) = \frac{\sin(2n\ell^{n-1})}{\sin(2n/\ell)} = 0, \quad \text{and} \quad U_{\ell^n-2}(\zeta^+) = \frac{\sin(2n\ell^{n-1} - 2n/\ell)}{\sin(2n/\ell)} = -1.$$

Combined with Proposition 2.4.2, we have

$$r_n(x,t;\ell) = x^{\ell^n} - t\,U_{\ell^n-1}(\zeta^+) + U_{\ell^n-2}(\zeta^+) = x^{\ell^n} - 1 = (x-1)^{\ell^n} \in (\mathcal{O}_K/\mathfrak{l})[x].$$

□

7.2 Monogenic extensions of degree 3

Unlike the previous families of maps, Dedekind's criterion is unable to find monogenic towers coming from the generalized Rikuna polynomials.

Theorem 7.2.1. *Suppose* $t^2-(\zeta+\zeta^{-1})t+1 \in \mathfrak{p}$. *Then* $\operatorname{ind} r_n(x,t;\ell) \in \mathfrak{p}$ *if and only if* $r_n(t,t;\ell) \in \mathfrak{p}^2$. *Furthermore,* $\ell \mid \operatorname{norm}(\operatorname{ind} r_n(x,t;\ell))$ *in all cases except* $\ell = 3$, $n = 1$, *and* $t \not\equiv 1 \pmod 3$.

Proof. Suppose that $t^2 - (\zeta + \zeta^{-1}) + 1 = (t-\zeta)(t-\zeta^{-1}) \in \mathfrak{p}$. Then t is a primitive ℓ-th root of unity modulo $\mathfrak{p}$, hence by Lemma 7.1.1, we have $r_n(x,t;\ell) = (x-t)^{\ell^n} \in (\mathcal{O}_K/\mathfrak{p})[x]$. Set

$$g(x) = x - t, \quad h(x) = (x-t)^{\ell^n-1}, \quad \text{and} \quad f(x) = \beta((x-t)^{\ell^n} - r_n(x,t;\ell)),$$

where β is a uniformizer of $\mathfrak{p}^{-1}$. By Theorem 4.1.1, $\operatorname{ind} r_n(x,t;\ell) \in \mathfrak{p}$ if and only if t is a root of $f(x)$ modulo $\mathfrak{p}$. It follows that $\operatorname{ind} r_n(x,t;\ell) \in \mathfrak{p}$ if and only if $r_n(t,t;\ell) \in \mathfrak{p}^2$.

To determine if $\operatorname{ind} r_n(x,t;\ell) \in \mathfrak{l}$, we have $r_n(x,t;\ell) = (x-1)^{\ell^n} \in (\mathcal{O}_K/\mathfrak{l})[x]$ by Lemma 7.1.2, and we set

$$g(x) = x - 1, \quad h(x) = (x-1)^{\ell^n-1}, \quad f(x) = \frac{(x-1)^{\ell^n} - r_n(x,t;\ell)}{\zeta + \zeta^{-1}}.$$

By Theorem 4.1.1, $\operatorname{ind} r_n(x,t;\ell) \in \mathfrak{l}$ if and only if $f(1) \equiv 0 \pmod{\mathfrak{l}}$. It is well known that $(1-\zeta)^{\ell-1} = u\ell$ for some unit $u \in \mathbf{Z}[\zeta]$, and taking complex conjugates, we have $(1-\zeta^{-1})^{\ell-1} = u^*\ell$, where * denotes complex conjugation. Now using Proposition 2.4.1,

$$\begin{aligned} f(1) &= \frac{(t-\zeta)(1-\zeta^{-1})^{\ell^n} - (t-\zeta^{-1})(1-\zeta)^{\ell^n}}{(\zeta+\zeta^{-1}-2)(\zeta^{-1}-\zeta)} \\ &= \frac{(t-\zeta)(1-\zeta^{-1})(1-\zeta^{-1})^{\ell^n-1} - (t-\zeta^{-1})(1-\zeta)(1-\zeta)^{\ell^n-1}}{(\zeta+\zeta^{-1}-2)(\zeta^{-1}-\zeta)} \end{aligned}$$

$$= \frac{(t-\zeta)(1-\zeta^{-1})(1-\zeta^{-1})^{(\ell-1)(\ell^{n-1}+\cdots+1)} - (t-\zeta^{-1})(1-\zeta)(1-\zeta)^{(\ell-1)(\ell^{n-1}+\cdots+1)}}{(\zeta+\zeta^{-1}-2)(\zeta^{-1}-\zeta)}$$
$$= \frac{(t-\zeta)(1-\zeta^{-1})(u^*\ell)^{\ell^{n-1}+\cdots+1} - (t-\zeta^{-1})(1-\zeta)(u\ell)^{\ell^{n-1}+\cdots+1}}{(\zeta+\zeta^{-1}-2)(\zeta^{-1}-\zeta)}.$$

Note that the numerator is divisible by ℓ, hence the $\mathfrak{l}$-adic valuation of the numerator is, in general, much larger than the $\mathfrak{l}$-adic valuation of the denominator, which is 1. In particular, if $n > 1$, then $f(1) \equiv 0 \pmod{\mathfrak{l}}$, regardless of ℓ. The only exception is when $\ell = 3$ and $n = 1$. In this case the base field is $\mathbf{Q}$, and $f(x) = (t-1)x^2 + (t+2)x$. From here, it is straightforward to show that $f(1) \equiv 0 \pmod 3$ if and only if $t \equiv 1 \pmod 3$. □

Remark 7.2.2. Even though $\mathrm{ind}(r_n(x,t;\ell)) \neq 1$ (with one exception), this does not exclude the possibility that these extensions are monogenic.

7.3 Shanks' specialization: $\ell = 3$

In this section, we examine extensions of $\mathbf{Q}$ generated by roots of the generalized Rikuna polynomial for the prime $\ell = 3$. Unless otherwise noted, we set $r_n(x,t) := r_n(x,t;3)$ throughout this section. From the discriminant formula in Propositoin 3.4.1, we know that the only primes that could divide the index are 3 and the primes dividing t^2+t+1. As with the Chebyshev polynomials, we apply the Montes algorithm in two steps: first to compute the 3-adic valuation of $\mathrm{ind}(r_n(x,t))$, and then to compute the p-adic valuation for the primes p dividing t^2+t+1.

7.3.1 Index calculation: $p = 3$

Let $u_n := U_n(1)$. From Proposition 2.4.2,

$$r_n(x,t) = \sum_{k=0}^{3^n} \binom{3^n}{k} \Big(tu_{k+2} + u_{k+1}\Big) x^{3^n-k} = \sum_{k=0}^{3^n} \binom{3^n}{k} \Big(tu_{k+2} - u_k\Big) x^k. \tag{7.1}$$

Recall that $r_n(x,t) \equiv (x-1)^{3^n} \pmod 3$. We use Taylor expansion to determine the $(x-1)$-development of $r_n(x,t)$. Namely,

$$r_n(x,t) = \sum_{m=0}^{3^n} \frac{r_n^{(m)}(1,t)}{m!}(x-1)^m,$$

where $r_n^{(m)}(x,t)$ denotes the m-th derivative of $r_n(x,t)$ with respect to x. By Equation (7.1), it is a straight-forward computation to show that

$$\begin{aligned} r_n^{(m)}(x,t) &= \sum_{k=0}^{3^n-m} \binom{3^n}{k+m} \frac{(k+m)!}{k!} \Big(tu_{k+m+2} - u_{k+m}\Big) x^k \\ &= \frac{3^n!}{(3^n-m)!} \sum_{k=0}^{3^n-m} \binom{3^n-m}{k} \Big(tu_{k+m+2} - u_{k+m}\Big) x^k. \end{aligned}$$

The coefficients in this expression are given by two known sequences of values (A057681, A057083). Namely,

$$-\sum_{k=0}^{3^n-m} \binom{3^n-m}{k} u_{k+m} = \sum_{k=0}^{\lfloor \frac{3^n-m+1}{3} \rfloor} (-1)^k \binom{3^n-m+1}{3k} = \begin{cases} (-27)^d & \text{if } e \equiv 0 \pmod 6 \\ (-27)^d & \text{if } e \equiv 1 \pmod 6 \\ 0 & \text{if } e \equiv 2 \pmod 6 \\ -3(-27)^d & \text{if } e \equiv 3 \pmod 6 \\ -9(-27)^d & \text{if } e \equiv 4 \pmod 6 \\ -18(-27)^d & \text{if } e \equiv 5 \pmod 6, \end{cases}$$

$$\sum_{k=0}^{3^n-m} \binom{3^n-m}{k} u_{k+m+2} = \sum_{k=0}^{\lfloor \frac{3^n-m-1}{3} \rfloor} (-1)^{k+1} \binom{3^n-m+1}{3k+2} = \begin{cases} 0 & \text{if } e \equiv 0 \pmod 6 \\ -(-27)^d & \text{if } e \equiv 1 \pmod 6 \\ -3(-27)^d & \text{if } e \equiv 2 \pmod 6 \\ -6(-27)^d & \text{if } e \equiv 3 \pmod 6 \\ -9(-27)^d & \text{if } e \equiv 4 \pmod 6 \\ -9(-27)^d & \text{if } e \equiv 5 \pmod 6. \end{cases}$$

where $3^n - m = 6d + e$. Thus setting

$$a_{n,m} = \binom{3^n}{m} \sum_{k=0}^{3^n-m} \binom{3^n-m}{k} \Big(tu_{k+m+2} - u_{k+m}\Big),$$

we have

$$a_{n,m} = (-1)^{n+\lfloor m/6 \rfloor} \binom{3^n}{m} 3^{\lfloor (3^n-m)/2 \rfloor} b_m(t), \tag{7.2}$$

where

$$b_m(t) = \begin{cases} 2t+1 & \text{if } m \equiv 0 \pmod 6 \\ t & \text{if } m \equiv 1 \pmod 6 \\ t-1 & \text{if } m \equiv 2 \pmod 6 \\ -1 & \text{if } m \equiv 3 \pmod 6 \\ -(t+2) & \text{if } m \equiv 4 \pmod 6 \\ -(t+1) & \text{if } m \equiv 5 \pmod 6. \end{cases}$$

Now by Taylor's formula, we have

$$r_n(x,t) = \sum_{m=0}^{3^n} \frac{r_n^{(m)}(1,t)}{m!}(x-1)^m = \sum_{m=0}^{3^n} a_{n,m}(x-1)^m.$$

From equation (7.2), we see that

$$\begin{aligned} &\nu_3(a_{n,0}) = \frac{3^n-1}{2} + \nu_3(2t+1), \quad \nu_3(a_{n,3^n}) = 0, \quad \text{and} \\ &\nu_3(a_{n,m}) \geq \frac{3^n-m+1}{2} \quad \text{for } 0 < m < 3^n. \end{aligned} \tag{7.3}$$

Theorem 7.3.1. *If* $t \not\equiv 1 \pmod 3$*, then* $\operatorname{ind}_3 r_n(x,t) = (3^n-1)(3^n-3)/4$.

Proof. By Equations (7.3), the $(x-1)$-polygon is one-sided of slope $(1-3^n)/(2\cdot 3^n)$, so the associated residual polynomial is degree 1. By Montes, the 3-adic valuation of the index is equal to the number of lattice points under the polygon. □

Note that for even values of m, the 3-adic valuation of $a_{n,m}$ can be made arbitrarily large by taking appropriate values of t congruent to 1 modulo 3. For the same values of t, the 3-adic valuation of $a_{n,m}$, where m is odd, remains unchanged. Hence, as t varies, the $(x-1)$-polygon is dictated by the vertices at odd ordinates. In fact, it is enough to consider the ordinates that are powers of 3.

Proposition 7.3.2. *If* $t \equiv 1 \pmod 3$*, then the* $(x-1)$*-polygon is the lower convex hull of the set of points*

$$\left\{\left(0, \nu_3(a_{n,0})\right)\right\} \cup \left\{\left(3^k, \frac{3^n-3^k}{2} + n - k\right) : 1 \leq k \leq n\right\}.$$

Proof. It is a simple exercise to show that $\nu_3\binom{3^n}{m} = n - \nu_3(m)$. It follows from Equation (7.2) that for odd m,

$$\nu_3(a_{n,m}) = \frac{3^n-m}{2} + n - \nu_3(m).$$

Now for $3^k < m < 3^{k+1}$, it is easy to verify that the point $(m, \nu_3(a_{n,m}))$ lies strictly above the line segment joining $(3^k, \nu_3(a_{n,3^k}))$ and $(3^{k+1}, \nu_3(a_{n,3^{k+1}}))$. □

Theorem 7.3.3. *Suppose* $t \equiv 1 \pmod 3$. *Set* $V = \min\{\nu_3(a_{n,0}) - \frac{3^n+1}{2}, n\}$. *Then*

$$\operatorname{ind}_3 r_n(x,t) = \frac{(3^n-3)(3^n+1)}{4} + \frac{V}{2} + 1 + \frac{1}{2}\sum_{k=0}^{V-1} 3^{n-k}.$$

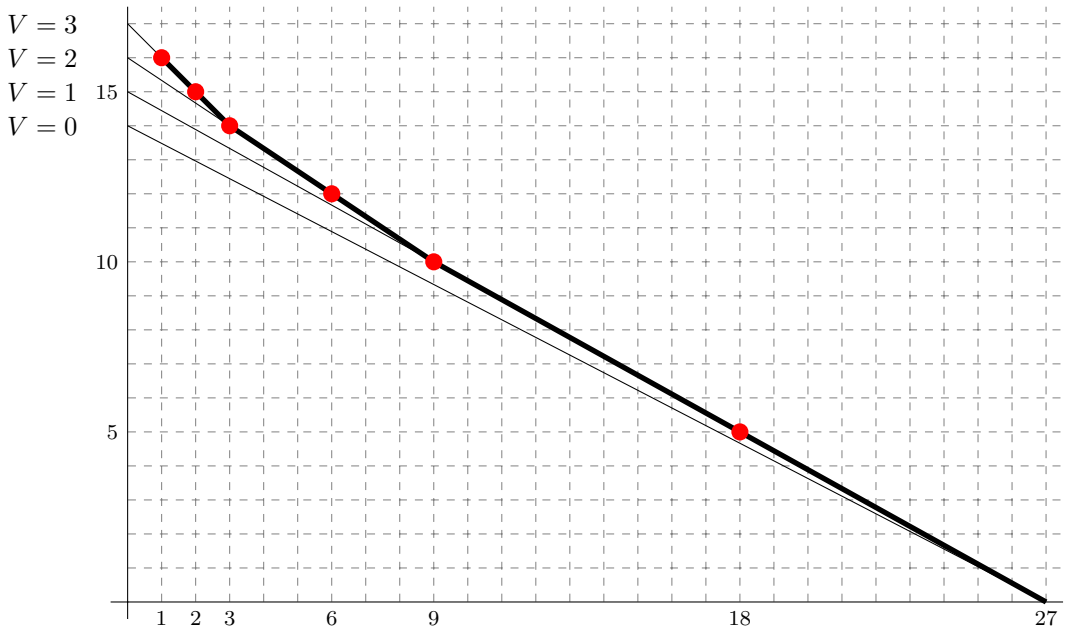
Proof. Let N denote the $(x-1)$-polygon determined in Proposition 7.3.2. The polygon N is composed of V sides, and the length of each side is at most 3. The residual polynomials associated to each side is $y \pm 1$, $y^2 \pm 1$, and $y^3 \pm y \pm 1$, depending on the length of the side. Regardless, each residual polynomial is separable over $\overline{\mathbf{F}}_3$, hence $r_n(x,t)$ is ℓ-regular. By Theorem 4.2.2 we are left to count the number of lattice points on or under the polygon. The number of lattice points inside the region bounded by N in the first quadrant can be determined by Pick's Theorem (Lemma 4.3.3), which states that the number of lattice points I in the interior of the region is given by

$$I = A - B/2 + 1,$$

where A is the area of the region, and B is the number of lattice points on the boundary of the region. The region A can be broken up into $V+1$ triangles, where the area of the first triangle is $3^n(3^n+1)/4$, and the area of each successive triangle is $3^{n-i}/2$ for $i = 1, \ldots, V$. The number of points on the boundary is given by

$$\begin{aligned} B &= \#\{\text{lattice points on } x \text{ and } y \text{ axes}\} + \#\{\text{lattice points on the polygon}\} \\ &= 3^n + \frac{3^n+1}{2} + V + 1 + 2V \\ &= \frac{3(3^n+2V+1)}{2}. \end{aligned}$$

□



7.3.2 Index calculation: $p \neq 3$

Recall that if $p \mid t^2+t+1$, then $r_n(x,t) \equiv (x-t)^{3^n} \pmod{p}$. Once again, we may use Taylor expansion to determine the $(x-t)$-development:

$$r_n(x,t) = \sum_{m=0}^{3^n} a_{n,m}(x-t)^m, \quad \text{where} \quad a_{n,m} = \frac{r_n^{(m)}(t)}{m!}.$$

By Proposition 2.4.1, it follows that

$$r_n^{(m)}(t,t) = \frac{3^n!}{(3^n-m)!}\frac{(t-\zeta)(t-\zeta^{-1})^{3^n-m} - (t-\zeta^{-1})(t-\zeta)^{3^n-m}}{\zeta^{-1}-\zeta}.$$

Hence for $0 \leq m < 3^n$,

$$a_{n,m} = \binom{3^n}{m}(t^2+t+1)\frac{(t-\zeta^{-1})^{3^n-m-1} - (t-\zeta)^{3^n-m-1}}{\zeta^{-1}-\zeta},$$

and $\nu_p(a_{n,m}) \geq \nu_p(t^2+t+1)$. In fact,

$$\nu_p(a_{m,n}) = \nu_p\binom{3^n}{m} + \nu_p(t^2+t+1)$$

since $t \equiv \zeta^{\pm 1} \pmod{p}$ and

$$\frac{(t-\zeta^{-1})^{3^n-m-1} - (t-\zeta)^{3^n-m-1}}{\zeta^{-1}-\zeta} \equiv \pm(\zeta^{-1}-\zeta)^{3^n-m-2} \equiv \pm\sqrt{-3}^{3^n-m-2} \pmod{p}.$$

It follows that the $(x-t)$-polygon is one sided with vertices $(0, \nu_p(a_{n,0}))$ and $(3^n, 0)$.

Theorem 7.3.4. *Suppose* $p \mid t^2 + t + 1$. *Then*

$$\operatorname{ind}_p r_n(x,t) = \begin{cases} \frac{(3^n-1)(\nu_p(t^2+t+1)-1)}{2} + 1 & \text{if } \nu_p(t^2+t+1) \equiv 0 \pmod 3 \\ \frac{(3^n-1)(\nu_p(t^2+t+1)-1)}{2} & \text{otherwise.} \end{cases}$$

Proof. If $\nu_p(t^2 + t + 1) \not\equiv 0 \pmod 3$, then the residual polynomial is degree one. By Theorem 4.2.2, the index is equal to the number of lattice points under the polygon. If $\nu_p(t^2 + t + 1) \equiv 0 \pmod 3$, the residual polynomial has the form $y^3 + c$, where c is a constant relative prime to p. The discriminant of this polynomial is $-27c^2$, hence this polynomial is separable over $\overline{\mathbf{F}}_p$. By Theorem 4.2.2, the index is given by the number of lattice points under the polygon, plus the two lattice points on the polygon. □

Theorem 1.2.3 now follows from Theorems 7.3.1, 7.3.3, and 7.3.4.

BIBLIOGRAPHY

[1] Shair Ahmad. Cycle structure of automorphisms of finite cyclic groups. *J. Combinatorial Theory*, 6:370–374, 1969.

[2] Wayne Aitken, Farshid Hajir, and Christian Maire. Finitely ramified iterated extensions. *Int. Math. Res. Not.*, (14):855–880, 2005.

[3] Avner Ash, Jos Brakenhoff, and Theodore Zarrabi. Equality of polynomial and field discriminants. *Experiment. Math.*, 16(3):367–374, 2007.

[4] Laurent Bartholdi, Rostislav Grigorchuk, and Volodymyr Nekrashevych. From fractal groups to fractal sets. In *Fractals in Graz 2001*, Trends Math., pages 25–118. Birkhäuser, Basel, 2003.

[5] Z. Chonoles, J. Cullinan, H. Hausman, A.M. Pacelli, S. Pegado, and F. Wei. Arithmetic properties of generalized Rikuna polynomials. In *Publications mathématiques de Besançon. Algèbre et théorie des nombres*, Publ. Math. Besançon Algèbre Théorie Nr. Presses Univ. Franche-Comté, Besançon, (to appear).

[6] Wun-Seng Chou and Igor E. Shparlinski. On the cycle structure of repeated exponentiation modulo a prime. *J. Number Theory*, 107(2):345–356, 2004.

[7] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[8] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[9] John Cullinan and Farshid Hajir. Ramification in iterated towers for rational functions. *Manuscripta Math.*, 137(3-4):273–286, 2012.

[10] Lhoussain El Fadil, Jesus Montes, and Enric Nart. Newton polygons and p-integral bases, 2009. arxiv.org/pdf/0906.2629.

[11] Jean-Marc Fontaine and Barry Mazur. Geometric Galois representations. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 41–78. Int. Press, Cambridge, MA, 1995.

[12] István Gaál. *Diophantine equations and power integral bases*. Birkhäuser Boston Inc., Boston, MA, 2002. New computational methods.

[13] T. Alden Gassert. Discriminants of chebyshev radical extensions, 2013. arXiv:1304.6055.

[14] T. Alden Gassert. Chebyshev action on finite fields. *Disc. Math.*, 315–316:83–94, 2014.

[15] Marie-Nicole Gras. Algorithmes numériques relatifs aux corps cubiques cycliques. In *Séminaire Delange-Pisot-Poitou, 14e anée (1972/72), No. 2, Exp. No.* G*15*, page 2. Secrétariat Mathématique, Paris, 1973.

[16] Jordi Guàrdia, Jesús Montes, and Enric Nart. Higher newton polygons and integral bases, 2009. arxiv.org/pdf/0902.3428.

[17] Jordi Guàrdia, Jesús Montes, and Enric Nart. Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *J. Théor. Nombres Bordeaux*, 23(3):667–696, 2011.

[18] Jordi Guàrdia, Jesús Montes, and Enric Nart. Newton polygons of higher order in algebraic number theory. *Trans. Amer. Math. Soc.*, 364(1):361–416, 2012.

[19] Su-Ion Ih. A nondensity property of preperiodic points on Chebyshev dynamical systems. *J. Number Theory*, 131(4):750–780, 2011.

[20] Su-Ion Ih and Thomas J. Tucker. A finiteness property for preperiodic points of Chebyshev polynomials. *Int. J. Number Theory*, 6(5):1011–1025, 2010.

[21] Kenzô Komatsu. An integral basis of the algebraic number field $Q(\sqrt[t]{a}, \sqrt[t]{1})$. *J. Reine Angew. Math.*, 288:152–153, 1976.

[22] Ernst Kummer. Über die ergänzungssätze zu den allgemeinen reziprokcitäusgesetzten. *Journal für die reine und angewandte Mathematik*, 44:93–146, 1852.

[23] Joseph Liang. On the integral basis of the maximal real subfield of a cyclotomic field. *J. Reine Angew. Math.*, 286/287:223–226, 1976.

[24] Rudolf Lidl and Gary L. Mullen. Cycle structure of Dickson permutation polynomials. *Math. J. Okayama Univ.*, 33:1–11, 1991.

[25] Rudolf Lidl, Gary L. Mullen, and Gerhard Turnwald. *Dickson polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, Harlow, 1993.

[26] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[27] Édouard Lucas. Sur les congruences des nombres eulériens et les coefficients différentiels des functions trigonométriques suivant un module premier. *Bull. Soc. Math. France*, 6:49–54, 1878.

[28] Toru Nakahara. On the indices and integral bases of noncyclic but abelian biquadratic fields. *Arch. Math. (Basel)*, 41(6):504–508, 1983.

[29] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[30] V. V. Nekrashevich. Iterated monodromy groups. *Dopov. Nats. Akad. Nauk Ukr. Mat. Prirodozn. Tekh. Nauki*, (4):18–20, 2003.

[31] Georg Pick. Geometrisches zur Zahlenlehre. *Sitzungsberichte des Deutschen Naturwissenschaftleich-Medicinischen Vereines für Böhmen 'Lotos' in Prag, Series 2*, 19:311–319, 1899.

[32] Yūichi Rikuna. On simple families of cyclic polynomials. *Proc. Amer. Math. Soc.*, 130(8):2215–2218 (electronic), 2002.

[33] Theodore J. Rivlin. *Chebyshev polynomials*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, second edition, 1990. From approximation theory to algebra and number theory.

[34] Min Sha and Su Hu. Monomial dynamical systems of dimension one over finite fields. *Acta Arith.*, 148(4):309–331, 2011.

[35] Syed Inayat Ali Shah. Monogenesis of the rings of integers in a cyclic sextic field of a prime conductor. *Rep. Fac. Sci. Engrg. Saga Univ. Math.*, 29(1):9, 2000.

[36] Yuan Yuan Shen and Lawrence C. Washington. A family of real 2^n-tic fields. *Trans. Amer. Math. Soc.*, 345(1):413–434, 1994.

[37] Yuan Yuan Shen and Lawrence C. Washington. A family of real p^n-tic fields. *Canad. J. Math.*, 47(3):655–672, 1995.

[38] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[39] The PARI Group, Bordeaux. *PARI/GP, version* `2.5.5`, 2013. available from `http://pari.math.u-bordeaux.fr/`.

[40] Simone Ugolini. Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic two. In *Theory and applications of finite fields*, volume 579 of *Contemp. Math.*, pages 187–204. Amer. Math. Soc., Providence, RI, 2012.

[41] Simone Ugolini. Graphs associated with the map $X \mapsto X + X^{-1}$ in finite fields of characteristic three and five. *J. Number Theory*, 133(4):1207–1228, 2013.

[42] Troy Vasiga and Jeffrey Shallit. On the iteration of certain quadratic maps over GF(p). *Discrete Math.*, 277(1-3):219–240, 2004.