JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

T. Alden GASSERT

Discriminants of Chebyshev radical extensions

Tome 26, n° 3 (2014), p. 607-633.

<http://jtnb.cedram.org/item?id=JTNB_2014__26_3_607_0>

Journal de Théorie des Nombres
de Bordeaux **26** (2014), 607–633

Discriminants of Chebyshev radical extensions

par T. Alden GASSERT

Résumé. Soit t un nombre entier et $\ell \neq 2$ un nombre premier. Soit $\Phi(x) = T_\ell^n(x) - t$ la composition n-fois du polynôme de Tchebychev de degré ℓ décalée de t. Supposant que ce polynôme est irréductible, soit $K = \mathbb{Q}(\theta)$, où θ est une racine de Φ. Nous appliquons un théorème de Dedekind en conjonction avec des résultats antérieurs de l'auteur afin d'obtenir des conditions sur t qui assurent que K soit monogène. Pour d'autres valeurs de t, nous appliquons un théorème de Guàrdia, Montes, et Nart pour obtenir une formule pour le discriminant de K et calculons une base intègrale de l'anneau des entiers $\mathcal{O}_K$.

Abstract. Let t be any integer and fix an odd prime ℓ. Let $\Phi(x) = T_\ell^n(x) - t$ denote the n-fold composition of the Chebyshev polynomial of degree ℓ shifted by t. If this polynomial is irreducible, let $K = \mathbb{Q}(\theta)$, where θ is a root of Φ. We use a theorem of Dedekind in conjunction with previous results of the author to give conditions on t that ensure K is monogenic. For other values of t, we apply a result of Guàrdia, Montes, and Nart to obtain a formula for the discriminant of K and compute an integral basis for the ring of integers $\mathcal{O}_K$.

1. Introduction

Let $f \in \mathbb{Z}[x]$ be a monic, irreducible polynomial with discriminant D_f, and K a number field with discriminant Δ_K. The computation of discriminants is a classical problem in number theory, as the discriminant provides, in some sense, a measure of the arithmetic complexity of the underlying ring: $\mathbb{Z}[\theta]$ in the case of D_f, and the ring of integers $\mathcal{O}_K$ in the case of Δ_K. It is well known that if $K = \mathbb{Q}(\theta)$, where θ is an algebraic integer with minimal polynomial f, then the discriminants of f and K scale relative to the square of the index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$:

$$D_f = [\mathcal{O}_K : \mathbb{Z}[\theta]]^2 \Delta_K. \tag{1.1}$$

In recent years, dynamically generated number fields have received growing attention, in part because the Galois groups of *iterated extensions* are contained in the automorphism group of a rooted tree. Moreover, postcritically finite functions generate infinite, yet finitely ramified, extensions (see

Manuscrit reçu le 22 avril 2013, révisé le 4 septembre 2014, accepté le 22 septembre 2014.

Aitken, Hajir, and Maire [1, Theorem 1.1]). Recall that a polynomial f is postcritically finite if the forward orbit of each of its critical points is finite, that is,

$$\#\{f^n(\alpha)\colon n \geq 1, f'(\alpha) = 0\} < \infty.$$

These iterated extensions may be constructed as follows. Let K be a number field and $f \in \mathcal{O}_K[x]$ be a monic polynomial of degree at least 2, and let $t \in \mathcal{O}_K$ such that $f^n(x) - t$ is irreducible over K for each $n \geq 1$. Here, $f^n(x)$ denotes the *n-fold iterate* of f, which is defined by $f^n(x) = f(f^{n-1}(x))$, and $f^0(x) = x$. Let $\{t = \theta_0, \theta_1, \theta_2, \ldots\}$ be a compatible sequence of preimages of t satisfying $f(\theta_n) = \theta_{n-1}$ (and thus $f^n(\theta_n) - t = 0$). By adjoining these preimages of t to the base field, we obtain a tower of number fields

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

where $K_n = K(\theta_n)$ and $[K_n\colon K] = (\deg f)^n$.

In this paper, we compute the index of the iterated extensions generated by $T_\ell^n(x) - t$, where ℓ is an odd prime and T_ℓ is the Chebyshev polynomial (of the first kind) of degree ℓ, with mild restrictions on t. Additionally in the case $\ell = 2$, we provide an alternative proof of [1, Proposition 6.2] for when the index is equal to 1.

The Chebyshev family of polynomials is closed under composition, leading to many interesting dynamical properties. For example, the Chebyshev polynomials are a rich source of permutation polynomials (see Lidl and Neideritter [16, Chapter 7]). It is also known that the iterated monodromy group of any Chebyshev polynomial is infinite dihedral [3, Proposition 5.6]. Other results relating to the dynamics of these polynomials can be found in Silverman [22, Chapter 6], Ih [12], Ih and Tucker [13], and previous work of the author [7]. Here, 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 of our towers.

Throughout this paper, we maintain the global assumption that

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

It is known that for each ℓ there are infinitely many integers t that satisfy this irreducibility criterion. As a simple example, when ℓ is odd and $\nu_\ell(t) = 1$ (ν_ℓ is the standard ℓ-adic valuation), the polynomial $T_\ell^n(x) - t$ is Eisenstein at ℓ. For a more detailed result regarding irreducibility, see [7, Theorem 1.2]. We call the number fields that arise from these polynomials *Chebyshev radical extensions*, after the *radical extensions*, which are generated by polynomials of the form $x^n - t$.

Theorem 1.1. *Let ℓ be an odd prime and $K = \mathbb{Q}(\theta)$, 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 is square-free. Then

$$[\mathcal{O}_K\colon \mathbb{Z}[\theta]] = \begin{cases} \ell^E A^{(\ell^n-1)/2} & \text{if } t \text{ is odd} \\ \ell^E (A/2)^{(\ell^n-1)/2} & \text{if } t \equiv 0 \pmod 4, \end{cases}$$

where $E = \sum_{i=1}^{\min\{n,\nu_\ell(T_\ell^n(t)-t)-1\}} \ell^{n-i}$. *Moreover,*

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

Our proof relies on the work of Guàrdia, Montes, and Nart [9, 10, 11]. In particular, the computation of the index comes from an analysis of specialized Newton polygons, which we describe in Section 4. As a result, we obtain a large family of towers that are interesting in several respects.

The Chebyshev polynomials are postcritically finite, hence in accordance with [1, Theorem 1.1], the set of primes dividing Δ_K does not vary with n. Moreover, $t^2 - 4 = A^2 B$ is a Pell equation. Thus for any fixed square-free integer B, the solutions to this Pell equation give infinitely many Chebyshev radical extensions that are ramified at precisely the primes dividing ℓB and possibly 2 depending on the parity of t.

As another consequence of Theorem 1.1, we obtain conditions on t for which $[\mathcal{O}_K\colon \mathbb{Z}[\theta]] = 1$, a sufficient condition for monogeneity. Recall that a number field K is *monogenic* if $\mathcal{O}_K$ has a basis consisting of the powers of a single algebraic integer. The classical examples of monogenic fields are the cyclotomic extensions; the maximal totally real subfields of the cyclotomic fields are also known to be monogenic (see Liang [15]). In fact, the splitting field of $T_\ell^n(x) - 2$ is the maximal real subfield of $\mathbb{Q}(\zeta_{\ell^n})$, where ζ_{ℓ^n} is a primitive ℓ^n-th root of unity. Hence we have placed this classical one-parameter family of monogenic towers (parametrized by ℓ) into a two-parameter family of monogenic towers parametrized by ℓ and t. The following is a generalization of [1, Proposition 6.2].

Theorem 1.2. *Let ℓ be a prime and let $K = \mathbb{Q}(\theta)$, 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 $[\mathcal{O}_K\colon \mathbb{Z}[\theta]] = 1$, and in particular K is monogenic.*

We note that this condition for monogeneity also does not depend on n. In the case where ℓ is odd, we can already see this independence in Theorem 1.1, for if $t-2$ and $t+2$ are square-free, then $[\mathcal{O}_K\colon \mathbb{Z}[\theta]]$ is constant. However, these conditions for monogeneity can be obtained without computing the index directly, and we give a simpler proof of Theorem 1.2 using Dedekind's criterion.

Certain towers of Kummer extensions also exhibit this monogenic behavior. For example the discriminant of the polynomial $x^{2^n} - 3$ is equal to the discriminant of the number field that it generates for each $n \geq 1$. Monogenic

number fields have been studied by many authors. Ash, Brakenhoff, and Zarrabi give computational evidence supporting a conjecture of Lenstra [2] that suggests that monogenic fields are abundant. However, outside of the towers mentioned previously, the majority of results are known for extensions of small degree (see Gras [8], Nakahara [18], Shah [21], Gaál [6], among others). A general survey of recent results can be found in Narkiewicz [19, pp. 79–81].

The structure of the paper is as follows. In Section 2, we outline several properties of the Chebyshev polynomials that will be useful throughout the paper. The proof of Theorem 1.2 is presented in Section 3. In section 4, we describe the Montes algorithm and state a theorem of Guàrdia, Montes, and Nart, which is the key result for proving Theorem 1.1. The proof of Theorem 1.1 spans Sections 5 and 6. In Section 7, we determine a basis for the ring of integers $\mathcal{O}_K$ for certain values of t. Most of our results are accompanied by examples.

2. Preliminaries

For the remainder of the paper, set $\Phi(x) = T_\ell^n(x) - t$, for a fixed prime ℓ and positive integers n and t. For now we allow the case $\ell = 2$, but following the proof of Theorem 1.2 in Section 3 we will restrict ℓ to the odd primes. Let K be a Chebyshev radical extension associated with Φ, that is, $K = \mathbb{Q}(\theta)$ where θ is a root of Φ, and we write $\operatorname{ind}(\Phi)$ to denote the index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$. We remind the reader of our blanket assumption that t is chosen so that $T_\ell^n(x) - t$ is irreducible for every $n \geq 1$, so K is a number field of degree ℓ^n over $\mathbb{Q}$.

The Chebyshev polynomials are a large and uniquely rich family with connections to many areas of mathematics. For each $d \geq 1$, the Chebyshev polynomial of the first kind $T_d \in \mathbb{Z}[x]$ is the unique polynomial of degree d that satisfies $T_d(z + z^{-1}) = z^d + z^{-d}$, and the Chebyshev polynomial of the second $U_d \in \mathbb{Z}[x]$ is related to the derivative of T_{d+1} by

$$U_d(x) = \frac{1}{d+1} T'_{d+1}(x).$$

Rivlin has written a book on the subject [20], and for more on the dynamics and algebraic structure associated with Chebyshev polynomials, see [22, Chapter 6]. For this paper, the well-known representations of these polynomials will be particularly useful.

Proposition 2.1.

(1) *For each $d \geq 0$, the Chebyshev polynomials T_d and U_d are given by*

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

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

(2) *The generating function for $U_d(x)$ is*

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

(3) *$U_0(x) = 1$, $U_1(x) = x$, and for each $d \geq 2$,*

$$U_d(x) = xU_{d-1}(x) - U_{d-2}(x).$$

(4) *For each $d \geq 0$, $U_d(-x) = (-1)^d U_d(x)$.*

The discriminant of Φ will also be of critical import. Indeed, given the value of the index in Theorem 1.1, knowing D_Φ is equivalent to knowing Δ_K by Equation (1.1). As mentioned in the introduction, the Chebyshev polynomials are postcritically finite, so we may apply [1, Proposition 3.2] to obtain the following discriminant formula.

Proposition 2.2. *We have*

$$D_\Phi = \begin{cases} 2^{n2^n}(2-t)(4-t^2)^{2^{n-1}-1} & \text{if } \ell = 2, \\ \ell^{n\ell^n}(4-t^2)^{(\ell^n-1)/2} & \text{otherwise.} \end{cases}$$

Proof. [7, Corollary 3.7]. □

The methods we use to compute $\operatorname{ind}(\Phi)$ are local computations; in particular, we need to understand the factorization of Φ into irreducibles modulo the primes dividing $\operatorname{ind}(\Phi)$. A priori, we do not know the primes dividing $\operatorname{ind}(\Phi)$, but by Equation (1.1), these primes must divide D_Φ, and by Proposition 2.2, we see that the only primes that could divide $\operatorname{ind}(\Phi)$ are ℓ and the primes dividing $t^2 - 4$. Factoring Φ modulo ℓ is straightforward, and we reproduce the proof for the benefit of the reader.

Lemma 2.3. *We have $\Phi(x) \equiv (x-t)^{\ell^n} \pmod{\ell}$.*

Proof. From Proposition 2.1 (1),

$$T_\ell(x) = \sum_{k=0}^{\lfloor \ell/2 \rfloor} (-1)^k \frac{(\ell-k-1)!}{k!(\ell-2k)!} \ell x^{\ell-2k}.$$

Note that

$$\nu_\ell\left(\frac{(\ell-k-1)!}{k!(\ell-2k)!}\ell\right)=\begin{cases}0 & \text{if } k=0\\ 1 & \text{otherwise,}\end{cases}$$

and thus $T_\ell(x)\equiv x^\ell \pmod{\ell}$. It follows that $T_\ell^n(x)-t\equiv x^{\ell^n}-t\equiv (x-t)^{\ell^n} \pmod{\ell}$. □

As for the primes dividing t^2-4, we have $t\equiv\pm 2 \pmod{p}$. Thus it suffices to consider the factorization of $T_\ell^n(x)\pm 2$ modulo p, which simplifies matters significantly. The factorization of $T_\ell^n(x)\pm 2$ in $\mathbb{Z}[x]$ is well known.

Proposition 2.4.

(1) *If $d\geq 0$ is even, there exist polynomials $f(x),g(x)\in\mathbb{Z}[x]$ such that*

$$T_d(x)-2=(x^2-4)f(x)^2 \quad \textit{and} \quad T_d(x)+2=g(x)^2.$$

(2) *If $d\geq 1$ is odd, there exist polynomials $f(x),g(x)\in\mathbb{Z}[x]$ such that*

$$T_d(x)-2=(x-2)f(x)^2 \quad \textit{and} \quad T_d(x)+2=(x+2)g(x)^2.$$

As mentioned in the introduction, $T_\ell^n(x)-2$, as well as $T_\ell^n(x)+2$, splits completely in the cyclotomic field $\mathbb{Q}(\zeta_{\ell^n})$. Since the only ramified prime in this extension is ℓ, the polynomials f and g in Proposition 2.4 factor into distinct irreducible polynomials modulo p.

Lemma 2.5. *Let p be a prime different from ℓ such that $t\equiv\pm 2 \pmod{p}$. Then*

$$\Phi(x)\equiv\phi_0(x)\phi_1(x)^2\phi_2(x)^2\cdots\phi_r(x)^2 \pmod{p},$$

where $\phi_0,\ldots,\phi_r$ are distinct irreducible polynomials in $\mathbb{F}_p[x]$. Moreover,

$$\phi_0=\begin{cases}1 & \textit{if } \ell=2 \textit{ and } t\equiv -2 \pmod{p},\\ x^2-4 & \textit{if } \ell=2 \textit{ and } t\equiv 2 \pmod{p},\\ x-\bar{t} & \textit{if } \ell \textit{ is odd,}\end{cases}$$

where $\bar{t}$ denotes the reduction of t modulo p.

A general factorization result for arbitrary t and p is stated in [7, Theorem 3.1].

3. Monogenic number fields

In this section we give a proof of Theorem 1.2 based on Dedekind's criterion. Dedekind's result gives local conditions for when a prime divides $\operatorname{ind}(\Phi)$, and combined with the factorization results from the previous section, we obtain conditions for when $\operatorname{ind}(\Phi)=1$. We then prove Proposition 3.3 that will allow us conclude that $\operatorname{ind}(\Phi)=1$ if and only if $\operatorname{ind}(T_\ell(x)-t)=1$. Our method gives an alternative proof of [1, Proposition 6.2].

Denote by $\overline{\ }$ the reduction modulo a prime.

Lemma 3.1 (Dedekind's criterion)**.** *Let $K = \mathbb{Q}(\theta)$, where θ is an algebraic integer with minimal polynomial $\Psi \in \mathbb{Z}[x]$. Let p be a prime. Let*

$$\overline{\Psi} = \prod \overline{\psi}_i^{e_i}$$

be the factorization of $\overline{\Psi}$ into monic irreducible polynomials in $\mathbb{F}_p[x]$, where $\psi_i \in \mathbb{Z}[x]$ are arbitrary monic lifts of $\overline{\psi}_i$. Set

$$g = \prod \psi_i, \quad h = \prod \psi_i^{e_i - 1},$$

so that $h \in \mathbb{Z}[x]$ is a monic lift of $\overline{\Psi}/\overline{g}$. Set $f = (gh - \Psi)/p \in \mathbb{Z}[x]$. Then $p \mid [\mathcal{O}_K \colon \mathbb{Z}[\theta]]$ if and only if $\gcd(\overline{f}, \overline{g}, \overline{h}) = 1$ in $\mathbb{F}_p[x]$.

Proof. See, for example, Cohen [4, Theorem 6.1.4]. □

Remark 1. The reductions $\overline{f}$, $\overline{g}$, and $\overline{h}$ in Dedekind's criterion do not depend on the choice of lifts.

We now prove a weak version of Theorem 1.2.

Theorem 3.2. *Let $K = \mathbb{Q}(\theta)$, 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 Equation (1.1), $D_\Phi = \Delta_K$ if and only if $\operatorname{ind}(\Phi) = 1$. As mentioned in the discussion after Proposition 2.2, we are only concerned with the prime ℓ and the primes dividing $t^2 - 4$.

We first address the prime ℓ. By Lemma 2.3, $\Phi(x) \equiv (x - t)^{\ell^n} \pmod{\ell}$, 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 Lemma 3.1 that

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

Now let p be a prime dividing $t^2 - 4$. By Lemma 2.5, we have $\Phi(x) \equiv \phi_0(x)\tau(x)^2 \pmod{p}$, for some separable polynomial $\tau \in \mathbb{F}_p[x]$. Set

$$g(x) = \phi_0(x)\tau(x), \quad h(x) = \tau(x), \quad \text{and} \quad f(x) = \frac{\phi_0(x)\tau(x)^2 - \Phi(x)}{p}.$$

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

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

Recall from Proposition 2.4 that $T_\ell^n(x) - \overline{t} = r(x)s(x)^2$, where $r(x) \equiv \phi_0(x) \pmod{p}$ and $s(x) \equiv \tau(x) \pmod{p}$. Thus

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

since $s(\alpha) \equiv 0 \pmod{p}$. It now follows from Lemma 3.1 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, we are left to show that the condition $\Phi(t) \not\equiv 0 \pmod{\ell^2}$ in Theorem 3.2 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 3.3. *For any integers a and b,*

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

Proof. Suppose that $T_\ell(a) \equiv T_\ell(b) \pmod{\ell^2}$. By Proposition 2.1 (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 $a \in \mathbb{Z}$ and write $a = q\ell + r$ such that $0 \le r < \ell$. 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. By Lemma 2.3, we have $T_\ell^{n-1}(t) \equiv t \pmod{\ell}$, so by Proposition 3.3,

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

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 3.2. □

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

Corollary 3.4. *$T_\ell(t) \equiv t \pmod{\ell^2}$ 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 2.3, $a \equiv t \pmod{\ell}$. Now by Proposition 3.3, $T_\ell(a) \equiv T_\ell(t) \pmod{\ell^2}$. The converse statement is satisfied by setting a to be the representative of t modulo ℓ in $\{0, \ldots, \ell - 1\}$, then applying Proposition 3.3. □

In other words, $\ell \mid \operatorname{ind}(\Phi)$ if and only if t is equivalent to an element in $\{T_\ell(0), T_\ell(1), \ldots, T_\ell(\ell - 1)\}$ modulo ℓ^2.

4. Theorem of the index

The value of $\operatorname{ind}(\Phi)$ given in Theorem 1.1, together with the value of $\operatorname{ind}(\Phi)$ with the discriminant of Φ given in Proposition 2.2, gives us a discriminant formula for many of the Chebyshev radical extensions. We compute $\operatorname{ind}(\Phi)$ using a relatively recent algorithm derived by Guàrdia, Montez, and Nart [9, 10, 11]. Their method employs a more refined variation of the Newton polygon, called the *ϕ-Newton polygon*, which captures arithmetic data attached to each irreducible factor ϕ of $\overline{\Phi}$. In this section we outline their methods and terminology following the presentation of El Fadil, Montes, and Nart [5].

Notation 1. We fix the following notation. Let p be a prime and let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial whose reduction modulo p is irreducible. We denote by $\mathbb{F}_\phi$ the finite field $\mathbb{Z}[x]/(p, \phi)$, and by

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

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

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

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

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

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

$$u_i = \nu_p(a_i(x)) \in \mathbb{Z}^+ \cup \{\infty\}$$

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

Definition 4.1. 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 $N_\phi(f)$.

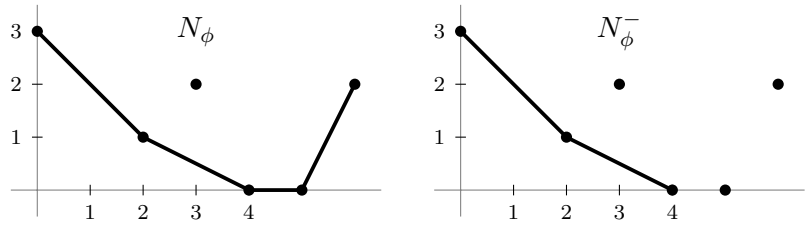

FIGURE 4.1. A ϕ-Newton polygon (left) and its principal part (right).

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.

Definition 4.2. 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 $N_\phi^-(f)$. See Figure 4.1. The length of $N_\phi^-(f)$, denoted $\text{len}(N_\phi^-(f))$, is the length of its projection onto the horizontal x-axis.

Notation 2. 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 $N_\phi(f) := N_\phi^-(f)$.

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

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

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*, denoted $\text{len}(S)$, is the length of the projection of S to the horizontal axis.

Definition 4.3. The *degree of S* is $\text{len}(S)/e$. To put it another way, the integral lattice divides each side into some number of segments. The degree of S is the number of these segments.

Definition 4.4. Let s be the initial abscissa of S, and let d be the degree of S. We define the *residual polynomial* attached to S (or to λ) to be the polynomial

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

Example 4.5. Consider the irreducible polynomial $f(x) = x^4 + 23x^3 + 12x^2 + 11x + 7$, which factors over $\mathbb{F}_3[x]$ 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 degree 2, the other side of slope $-1/2$ and degree 1. The residual coefficients are $c_0 = 1$, $c_1 = -1$, $c_2 = -1$, $c_3 = 0$, and $c_4 = 1$. 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 4.2.

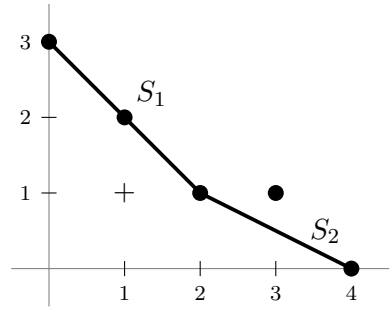

FIGURE 4.2. The ϕ-polygon for $f(x) = x^4 + 23x^3 + 12x^2 + 11x + 7$ and $\phi(x) = x + 2$.

Definition 4.6. Let $\phi(x) \in \mathbb{Z}[x]$ 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 that side is separable.

Choose monic polynomials $\phi_1(x), \ldots, \phi_r(x) \in \mathbb{Z}[x]$ whose reduction modulo p are the different irreducible factors of $\overline{f}(x) \in \mathbb{F}_p[x]$. We say that $f(x)$ is *p-regular* with respect to this choice if $f(x)$ is ϕ_i-regular for each $1 \le i \le r$.

Definition 4.7. 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 $\operatorname{ind}_\phi(f)$.

Notation 3. Let θ be an algebraic integer with minimal polynomial $f(x) \in \mathbb{Z}[x]$, and let $\operatorname{ind}(f) = [\mathcal{O}_{\mathbb{Q}(\theta)} \colon \mathbb{Z}[\theta]]$. We denote by $\operatorname{ind}_p(f)$ the p-adic valuation of $[\mathcal{O}_{\mathbb{Q}(\theta)} \colon \mathbb{Z}[\theta]]$:

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

Theorem 4.8. *Theorem of the index:*

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

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

Proof. See [11, Section 4.4]. □

Example 4.4 (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 $\mathbb{F}_3[y]$. Hence f is 3-regular, and by Theorem 4.8, we have $\operatorname{ind}_3(f) = \operatorname{ind}_\phi(f) = 3$, since $\deg\phi = 1$ and there are three points with integral coordinates on or below the polygon. This result is verified by `PARI`.

5. Computation of $\operatorname{ind}_\ell(\Phi)$

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 1.1 in two parts. In this section we compute $\operatorname{ind}_\ell(\Phi)$, the ℓ-adic valuation of $\operatorname{ind}(\Phi)$, and in the following section we compute $\operatorname{ind}_p(\Phi)$ for the primes dividing t^2-4. We remind the reader of our notation that $\Phi(x) = T_\ell^n(x) - t$, and $\operatorname{ind}(\Phi) = [\mathcal{O}_K : \mathbb{Z}[\theta]]$, where θ is a root of Φ, $K = \mathbb{Q}(\theta)$, and t is chosen so that $T_\ell^n(x) - t$ is irreducible for each $n \geq 1$. From Theorem 3.2, we know that $\Phi(t) \equiv 0 \pmod{\ell^2}$ is the necessary and sufficient condition for which $\operatorname{ind}_\ell(\Phi) > 1$. We recover this condition using the method of Guàrdia, Montes, Nart.

We tackle the computation of $\operatorname{ind}_\ell(\Phi)$ 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 2.3 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 we may take $\phi(x) = x$, and hence the ϕ-Newton polygon is the standard Newton polygon of Φ. In this case, we obtain the ϕ-Newton polygon using Lemma 5.2, a classic result of Kummer [14]. When $t \not\equiv \pm 2 \pmod{\ell^2}$, we must derive the ϕ-development of Φ, then use a series of lemmas, including a result of Lucas [17], 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 4.8 to give a formula for $\operatorname{ind}_\ell(\Phi)$.

Definition 5.1. For any prime p and any integer a, the *p-adic expansion* of a is

$$a = a_0p^0 + a_1p^1 + a_2p^2 + \cdots + a_rp^r$$

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

$$\sigma_p(a) = \sum_{i=0}^{\infty} a_i. \tag{5.1}$$

Lemma 5.2 (Kummer)**.** *Let p be a prime, and let σ_p be the function defined in Equation* (5.1)*.*

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

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

(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) $\nu_p\binom{a+b}{b} = \#$*carries in $a+b$ 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). □

We consider the case where $t \equiv 0 \pmod{\ell}$ and proceed by computing the Newton polygon of $T_\ell^n(x)$. By Proposition 2.1 (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 5.3. *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 5.2 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 5.2

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

Furthermore,

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

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 5.4. *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 5.3, 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 5.5. *Suppose $t \equiv 0 \pmod{\ell}$, and let $v = \nu_\ell(t)$. Let S_m be the edge defined in Corollary 5.4. 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 5.6. Consider the polynomial $T_3^3(x) - t$. By Corollary 5.4, 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 5.1.

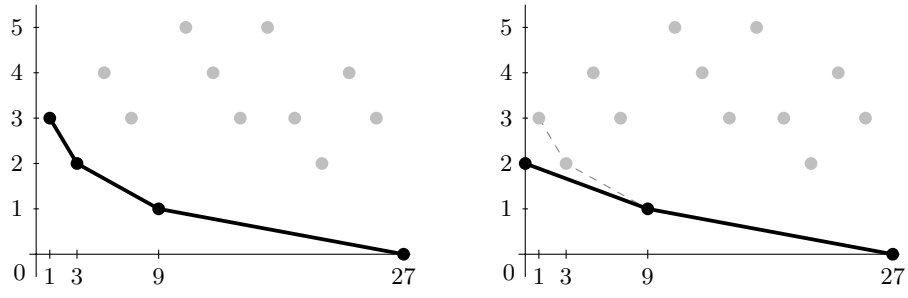

FIGURE 5.1. Left: The Newton polygon of $T_3^3(x)$. Right: the Newton polygon of $T_3^3(x) - 24$ at 3. The 3-adic valuations of the other coefficients are marked in gray.

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 2.1 (1), we have

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

$$
\begin{aligned}
&= -t + \sum_{i=0}^{\ell^n} \sum_{k=0}^{\lfloor(\ell^n-i)/2\rfloor} (-1)^k \binom{\ell^n-k}{k}\binom{\ell^n-2k}{i}\frac{\ell^n}{\ell^n-k} t^{\ell^n-2k-i}\phi^i \\
&= -t + \sum_{k=0}^{\lfloor\ell^n/2\rfloor} (-1)^k \binom{\ell^n-k}{k}\frac{\ell^n}{\ell^n-k} t^{\ell^n-2k} \\
&\qquad + \sum_{i=1}^{\ell^n} \sum_{k=0}^{\lfloor(\ell^n-i)/2\rfloor} (-1)^k \binom{\ell^n-k}{k}\binom{\ell^n-2k}{i}\frac{\ell^n}{\ell^n-k} t^{\ell^n-2k-i}\phi^i \\
&= T_\ell^n(t) - t \\
&\qquad + \sum_{i=1}^{\ell^n} \sum_{k=0}^{\lfloor(\ell^n-i)/2\rfloor} (-1)^k \binom{\ell^n-k}{k}\binom{\ell^n-2k}{i}\frac{\ell^n}{\ell^n-k} t^{\ell^n-2k-i}\phi^i \\
&= \Phi(t) + \sum_{i=1}^{\ell^n} \sum_{k=0}^{\lfloor(\ell^n-i)/2\rfloor} (-1)^k \binom{\ell^n-k}{k}\binom{\ell^n-2k}{i}\frac{\ell^n}{\ell^n-k} t^{\ell^n-2k-i}\phi^i. \qquad (5.2)
\end{aligned}
$$

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 $1 \le i \le \ell^n$.

Lemma 5.7. *For positive integers a, b, and c satisfying $0 \le b \le \frac{a-c}{2}$, 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.

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

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

This new expression simplifies the ℓ-adic expansions of the numbers in the binomial coefficients, which set us up nicely to apply the following result of Lucas.

Lemma 5.8. *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 [17, Section 3]. □

The following result will also be useful in computing $\nu_\ell(b_i)$.

Lemma 5.9. *Let ℓ be an odd prime. If $x \neq \pm 2 \bmod \ell$, then $U_{\ell-1}(x) = \pm 1 \bmod \ell$.*

Proof. Let $x \in \mathbb{F}_\ell$ and $x \neq \pm 2$. Set $\alpha = \frac{x + \sqrt{x^2 - 4}}{2} \in \mathbb{F}_{\ell^2}$ and $\beta = \frac{x - \sqrt{x^2 - 4}}{2} \in \mathbb{F}_{\ell^2}$. From Proposition 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 $\mathbb{F}_{\ell^2}$ fixes $\mathbb{F}_\ell$ and acts by conjugation away from $\mathbb{F}_\ell$. Hence, if $\sqrt{x^2 - 4} \in \mathbb{F}_\ell$, then $\alpha^\ell = \alpha$, $\beta^\ell = \beta$, and

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

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

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

□

We are now prepared to compute the ℓ-adic valuations of the coefficients in the ϕ-development of Φ.

Theorem 5.10. *Suppose that $t \not\equiv \pm 2 \pmod{\ell^2}$, $\Phi(t) \equiv 0 \pmod{\ell^2}$, and let i be an integer satisfying $\ell^m \leq i < \ell^{m+1}$ where $m < n$. 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

$$\binom{\ell^n - k - 1}{\ell^m + \varepsilon - 1} = \frac{(\ell^n - k - 1)!}{(\ell^m + \varepsilon)!(\ell^n - \ell^m - k - \varepsilon)!}$$

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

Hence,

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

By Lemma 5.2, $\nu_\ell\binom{\ell^m+\varepsilon}{\ell^m} = 0$ 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

$$b_{\ell^m} = \ell^{n-m}\sum_{k=0}^{\frac{\ell^n-\ell^m}{2}}(-1)^k\binom{\ell^n-\ell^m-k}{k}\binom{\ell^n-k-1}{\ell^m-1}t^{\ell^n-\ell^m-2k}. \tag{5.3}$$

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.

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

By Lemma 5.8, the second binomial coefficient in Equation (5.3) satisfies

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

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 5.8 to the first binomial coefficient in Equation (5.3), 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 $0 \leq k_j \leq (\ell - 1)/2$ 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 2.1 (1) and Lemma 5.9. This concludes the proof. □

Remark 2. It may appear that the condition required to apply Lemma 5.9 is stronger than the assumptions in the statement of Theorem 5.10, however we argue that the conditions are equivalent.

Lemma 5.11. *Suppose that* $\Phi(t) \equiv 0 \pmod{\ell^2}$*, then* $t \equiv \pm 2 \pmod{\ell^2}$ *if and only if* $t \equiv \pm 2 \pmod{\ell}$*.*

Proof. The first implication ($\Rightarrow$) is clear. For the reverse direction, if $t \equiv \pm 2 \pmod{\ell}$, then

$$T_\ell^n(t) \equiv T_\ell^n(\pm 2) \pmod{\ell^2}$$

by Proposition 3.3. The left side is congruent to t by assumption, and the right side is congruent to ± 2 by Proposition 2.4. □

Remark 3. 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 5.10 subsumes Proposition 5.3 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 5.5, we only need to consider the ℓ-adic valuation of $\Phi(t)$ (see Equation (5.2)) to obtain the ϕ-Newton polygon of Φ.

Corollary 5.12. *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 5.5. □

Theorem 5.13. *Suppose $t \not\equiv \pm 2 \pmod{\ell^2}$, and set $v = \nu_\ell(\Phi(t))$. Then*

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

Proof. It is easy to verify that each side of the ϕ-Newton polygon given in Corollary 5.12 has degree 1. Hence every residual polynomial attached to the polygon has degree 1, and it follows that Φ is ℓ-regular. By Theorem 4.8, 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 $\operatorname{ind}_\ell(\Phi)$. □

Remark 4. 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 4.8, we have $\operatorname{ind}_\ell(\Phi) = 0$. We have thus recovered the condition in Theorem 3.2 that $\ell \mid \operatorname{ind}(\Phi)$ if and only if $\Phi(t) \equiv 0 \pmod{\ell^2}$.

We illustrate Theorem 5.13 with an example.

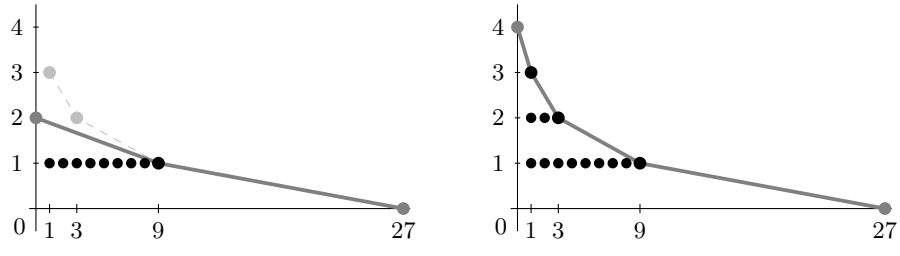

FIGURE 5.2. Left: the ϕ-Newton polygon for $T_3^3(x) - 24$. We have $\operatorname{ind}_3(T_3^3(x) - 24) = 9$. Right: the ϕ-Newton polygon for $T_3^3(x) - 81$. It follows that $\operatorname{ind}_3(T_3^3(x) - 81) = 13$.

Example 5.14. Consider the polynomial $T_3^3(x) - t$. From Corollary 5.12, we see that the degree of each side of the polygon is 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 5.2.

6. Computation of $\mathbf{ind}_p(\Phi)$

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 3.2, 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 4.8, completing the proof of Theorem 1.1. 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 4.8 meets the upper bound provided by the p-adic valuation of D_Φ, giving the result. Consider the following example.

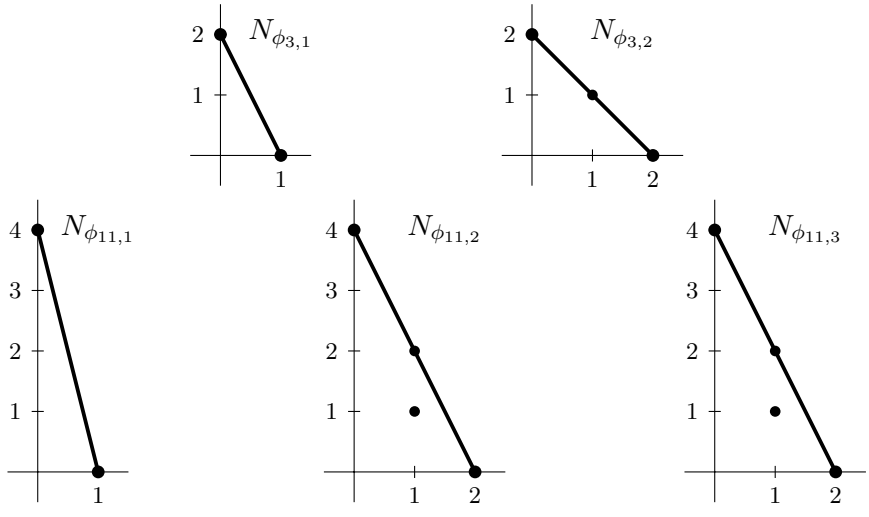

FIGURE 6.1. ϕ-Newton polygons associated to $T_5(x) - t_0$ in Example 6.1.

Example 6.1. 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 3.2, the primes 3 and 11 divide $\operatorname{ind}(T_5(x) - t_0)$, and 5 does not. We have

$$T_5(x) - t_0 \equiv (x+2)(x^2 - x - 1)^2 \pmod 3, \quad \text{and}$$
$$T_5(x) - t_0 \equiv (x-2)(x-3)^2(x+4)^2 \pmod{11}.$$

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

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

From the ϕ-Newton polygons (Figure 6.1), 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 4.8, 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 2.2, we also have

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

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 2.5, we write

$$\Phi(x) \equiv (x\pm 2)\phi_1(x)^2\cdots\phi_r(x)^2 \pmod{p}, \tag{6.1}$$

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

Proposition 6.2. *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* (6.1)*, 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, $\operatorname{ind}_{(x\pm 2)}(\Phi) = 0$.

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 4.8,

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

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 4.8 that

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

On the other hand, the valuation of the index is bounded by the p-adic valuation of D_Φ. Namely by Proposition 2.2,

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

Thus we have derived the following result.

Corollary 6.3. *If $p\neq\ell$ is an odd prime and $t\equiv\pm 2 \pmod{p^2}$, then*

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

Proof of Theorem 1.1. The multiplicity of each odd prime divisor of $\operatorname{ind}(\Phi)$ are given by Theorem 5.13 and Corollary 6.3. The formula for Δ_K follows from Equation (1.1). □

We conclude this section with the proof of Proposition 6.2.

Proof. (Proposition 6.2) From Lemma 2.5, $T_\ell^n(x) \pm 2 = (x \pm 2)\tau(x)^2$ 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

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

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

We now show that $\operatorname{ind}_{(x\pm 2)}(\Phi) = 0$. 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 2.1 (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 2.1 (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 $\operatorname{ind}_{(x\pm 2)}(\Phi) = 0$. □

7. 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 $\mathbb{Z}[\theta]$ 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 $\hat{\phi}_i$-development 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 7.1. *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 [5, Theorem 2.6]. □

In Corollary 5.12, 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 7.2. *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 $\phi(x) = x - \bar{t}$. In Corollary 5.12 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

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

□

8. Acknowledgements

The author would like to thank Farshid Hajir for his helpful conversations, continued support, and guidance. Additionally, the author extends his thanks to Jeff Hatley and Nico Aiello for their thought-provoking discussions, as well as the anonymous referee for many useful comments.

References

[1] W. Aitken, F. Hajir, and C. Maire, *Finitely ramified iterated extensions* Int. Math. Res. Not., **14**, (2005), 855–880.

[2] A. Ash, J. Brakenhoff, and T. Zarrabi, *Equality of polynomial and field discriminants*, Experiment. Math., **16**, (2007), 3, 367–374.

[3] L. Bartholdi, R. Grigorchuk, and V. Nekrashevych, *From fractal groups to fractal sets*, In Fractals in Graz 2001, Trends Math., Birkhäuser, Basel, (2003), 25–118.

[4] H. Cohen, *A course in computational algebraic number theory* of Graduate Texts in Mathematics, **138**, Springer-Verlag, Berlin, (1993).

[5] L. E. Fadil, J. Montes, and E. Nart, *Newton polygons and p-integral bases*, (2009), arxiv.org/pdf/0906.2629.

[6] I. Gaál, Diophantine equations and power integral bases, Birkhäuser Boston Inc., Boston, MA, (2002), New computational methods.

[7] T. A. Gassert, *Chebyshev action on finite fields*, Disc. Math., (2014), 315–316:83–94.

[8] M.-N. Gras, *Algorithmes numériques relatifs aux corps cubiques cycliques*, in Séminaire Delange-Pisot-Poitou, 14e année, (1972/72), No. 2, Exp. No. G15, page 2. Secrétariat Mathématique, Paris, (1973).

[9] J. Guàrdia, J. Montes, and E. Nart, *Higher newton polygons and integral bases*, (2009), arxiv.org/pdf/0902.3428.

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

[11] J. Guàrdia, J. Montes, and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc., **364**, (2012), 1, 361–416.

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

[13] S.-I. Ih and T. J. Tucker, *A finiteness property for preperiodic points of Chebyshev polynomials*, Int. J. Number Theory, **6**, (2010), 5, 1011–1025.

[14] E. Kummer, *Über die ergänzungssätze zu den allgemeinen reziprokcitäusgesetzten*, Journal für die reine und angewandte Mathematik, **44**, (1852), 93–146.

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

[16] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, Cambridge, second edition, (1997), with a foreword by P. M. Cohn.

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

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

[19] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, third edition, (2004).

[20] T. 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.

[21] S. I. A. Shah, *Monogenesis of the rings of integers in a cyclic sextic field of a prime conductor*, Rep. Fac. Sci. Engrg. Saga Univ. Math., **29**, (2000), 9.

[22] J. H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, **241**, Springer, New York, (2007).

T. Alden Gassert
University of Colorado, Boulder
Campus Box 395
Boulder, CO, USA 80309-0395
E-mail: thomas.gassert@colorado.edu