ALBANIAN JOURNAL OF MATHEMATICS
Volume 11, Number 1, Pages 3–12
ISSN: 1930-1235; (**2017**)

A NOTE ON THE MONOGENEITY OF POWER MAPS

T. ALDEN GASSERT

Western New England University
Department of Mathematics
1215 Wilbraham Road
Springfield, MA 01119

Abstract. Let $\varphi(x) = x^d - t \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $d \geq 2$, and let θ be a root of φ. The purpose of this paper is to establish necessary and sufficient conditions for $\varphi(x)$ to be monogenic, meaning the ring of integers of $\mathbb{Q}(\theta)$ is generated by the powers of a root of $\varphi(x)$. Sufficient conditions for monogeneity are established using Dedekind's criterion. We then apply the Montes algorithm to give an explicit formula for the discriminant of $\mathbb{Q}(\theta)$. Together, these results can be used to determine when $\varphi(x)$ is not monogenic.

Mathematics Subject Classes 2010: Primary: 11E21, Secondary: 12F05
Keywords: power map, monogeneity, monogenic field, Montes algorithm

1. Introduction

Let K be a number field and $\mathcal{O}_K$ its ring of integers. The field K is *monogenic* if it contains an algebraic integer α whose powers generate the ring of integers of K, that is $\mathcal{O}_K = \mathbb{Z}[\alpha]$. The classification of monogenic fields is a long-standing problem that has been studied by many (see for example [3, 7, 12]). As a starting point, given an algebraic integer θ with minimal polynomial φ, one can test whether $K = \mathbb{Q}(\theta)$ is monogenic by comparing the discriminant of the polynomial φ to the discriminant of the field K. These discriminants are equal up to a square factor:

$$\operatorname{disc}\varphi = (\operatorname{ind}\varphi)^2 \operatorname{disc} K, \tag{1}$$

where $\operatorname{ind}\varphi := [\mathcal{O}_K : \mathbb{Z}[\theta]]$. From this identity, we see that $\operatorname{disc}\varphi = \operatorname{disc} K$ is a sufficient condition for K to be monogenic, and we say that φ is monogenic whenever this is the case. In particular, φ is monogenic whenever $\operatorname{disc}\varphi$ is square-free. However, when $\operatorname{disc}\varphi$ is not square-free, determining how the factors are distributed between $\operatorname{ind}\varphi$ and $\operatorname{disc} K$ is often quite challenging, especially when the degree of K is large.

E-mail address: thomas.gassert@wne.edu.
Date: Received: March 31, 2017. Accepted: May 16, 2017.

In this paper, we prove that the polynomial $\varphi(x) = x^d - t$, where $d > 1$, $t \in \mathbb{Z}$, and φ is irreducible, is monogenic for many values of d and t. This result may be seen as a generalization of a result of Bardestani [1, Theorem 1], who proved that when d and t are prime, φ is often monogenic.

Theorem 1.1. *For any integer $d > 1$ and any square-free integer t satisfying $t^p \not\equiv t \pmod{p^2}$ for all primes p dividing d, the polynomial $x^d - t$ is monogenic.*

Remark. We will assume throughout this paper that $\varphi(x) := x^d - t$ is an irreducible polynomial with $d > 1$. Although Theorem 1.1 does not explicitly state that φ is irreducible, we have ensured that it is by requiring that t is square-free (thus φ is Eisenstein at every prime dividing t) and $t^p \not\equiv t \pmod{p^2}$ for any prime p dividing d (in particular, $t \neq 1$).

It is well known that $\operatorname{disc}\varphi = \pm d^d t^{d-1}$, but despite the large square factors in this discriminant, we are able to prove, quite easily, that φ is monogenic using a classical result: Dedekind's criterion. The criterion gives a condition for when a prime p divides $\operatorname{ind}\varphi$ that depends on the factorization of the polynomial modulo p. Given the simple nature of our polynomials, the result follows without difficulty. (See Section 2.)

On the other hand, Dedekind's criterion does not determine the multiplicities of the primes dividing $\operatorname{ind}\varphi$. So in particular, the criterion gives no indication of the conditions necessary for K to be monogenic. The remainder of the paper is focused on addressing this concern. In Section 3, we compute the exact multiplicities of the primes dividing $\operatorname{ind}\varphi$ via an application of the Montes algorithm. These results are summarized in Theorem 1.2.

Theorem 1.2. *Suppose $\varphi(x) = x^d - t$ is irreducible with $d > 1$, and $\gcd(d, p, \nu_p(t)) = 1$ for each prime p dividing t. Then*

$$(\operatorname{ind}\varphi)^2 = \prod_{p \mid dt} p^{E_p}, \quad \textit{where}$$

$$E_p = \begin{cases} (d-1)(\nu_p(t)-1) + \gcd(\nu_p(t), d) - 1 & \textit{if } p \mid t \\ \displaystyle\sum_{j=1}^{\min\{\nu_p(t^p - t)-1, k\}} 2dp^{-j}, \quad \textit{where } k = \nu_p(d) & \textit{otherwise.} \end{cases}$$

This theorem, which is a direct result of Proposition 3.2 and Proposition 3.5, gives a second proof of Theorem 1.1. Namely, we see that $E_p = 1$ if and only if t is square-free and $\nu_\ell(t^\ell - t) = 1$ for every prime ℓ dividing d.

The idea to apply the Montes algorithm to these maps is due to the author's work computing discriminants of *iterated extensions* arising from the Chebyshev [4] and Rikuna polynomials [6]. To be precise, if $f(x) \in \mathbb{Z}[x]$ is a monic polynomial where $\deg f \geq 2$, and we let $f^n(x)$ denote the n-fold composition of f with itself, then the number fields generated by $f^n(x) - t$ are iterated extensions (assuming $f^n(x) - t$ is irreducible). Moreover, if $\{\theta_0 = t, \theta_1, \theta_2, \ldots\}$ is a sequence of algebraic numbers chosen so that $f^n(\theta_n) = \theta_{n-1}$, then the number fields $K_n = \mathbb{Q}(\theta_n)$ form a tower—that is, $K_{n-1} \subseteq K_n$ for all n—and one may ask what algebraic properties are shared by this tower.

In the context of these power maps, we see that if $f(x) = x^d$, then $f^n(x) = x^{d^n}$. Consequently, if $f(x) - t = x^d - t$ is monogenic by Theorem 1.1, then so is $f^n(x) - t$

for all n. Thus the condition of monogeneity should not just be thought of in the context of isolated pairs (d,t), but also as a condition on the tower of fields that arise from each of these pairs.

While the question of monogeneity requires that $\operatorname{ind} f = 1$, it is an equally interesting question to ask how large $\operatorname{ind} f$ can be relative to $\operatorname{disc} f$. In particular, it would be exceptional if one could find an example of iterated extensions whose *root discriminant* is bounded. To rephrase this question in the language of this paper: does there exist a function $f(x)$ for which

$$\lim_{n\to\infty}\left(\frac{\operatorname{disc} f^n(x)}{(\operatorname{ind} f^n(x))^2}\right)^{\deg f^n}$$

is finite (assuming $f^n(x)$ is irreducible for all n)? According to Theorem 1.2, the answer for the power maps is no, their root discriminants are not bounded. More generally, it is expected that that the answer for all maps is no, but as of yet, this is still an open question. Perhaps a careful study of $\operatorname{ind} f$ via the Montes algorithm can lead to progress on this question.

Acknowledgements. The author would like to thank the anonymous referees for their helpful comments.

2. Monogenic number fields

In this section we apply Dedekind's criterion (Lemma 2.1) to prove Theorem 1.1. The criterion detects when the index $\operatorname{ind}\varphi$ is nontrivial based on a local condition. As we mentioned in the introduction, $\operatorname{disc}\varphi = d^d t^{d-1}$, so it is sufficient to check the criterion for the primes dividing dt. The criterion is as follows.

Lemma 2.1 (Dedekind's criterion)**.** *Let θ be an algebraic integer with minimal polynomial ϕ and set $K=\mathbb{Q}(\theta)$. Let p be prime, and write*

$$\phi(x)\equiv\prod_{i=1}^{r}\phi_i(x)^{e_i}\pmod p$$

where the $\phi_i\in\mathbb{Z}[x]$ are monic, irreducible lifts of the irreducible factors of ϕ modulo p. Set

$$g(x)=\prod_{1\le i\le r}\phi_i(x),\quad h(x)=\prod_{1\le i\le r}\phi_i(x)^{e_i-1},\quad \text{and}\quad f(x)=\frac{g(x)h(x)-\phi(x)}{p}.$$

Then $p\mid\operatorname{ind}\phi$ if and only if $\gcd(\overline{f},\overline{g},\overline{h})=1$, where $\overline{\ }$ denotes reduction modulo p.

Proof. [2, Theorem 6.1.4]. □

Remark. We note that the existence of a shared root modulo p in Dedekind's criterion does not depend on the choice of lifts of the irreducible factors. We also point out that the roots of f modulo p are the roots of $pf(x)$ modulo p^2. The following two lemmas will be useful for transitioning between reduction modulo p and reduction modulo p^2.

Lemma 2.2. *For any prime p, $a^p\equiv b^p\pmod{p^2}$ if and only if $a\equiv b\pmod p$.*

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

Lemma 2.3. *For any prime p, $t^{p^k} \equiv t \pmod{p^2}$ if and only if $t^p \equiv t \pmod{p^2}$.*

Proof. Since $t^{p^{k-1}} \equiv t \pmod{p}$, it follows from Lemma 2.2 that $t^{p^k} \equiv t^p \pmod{p^2}$. □

2.1. **Proof of Theorem 1.1.** For the benefit of the reader, we recall the assumptions of Theorem 1.1. Set $\varphi(x) = x^d - t$, where $d \geq 2$, t is square-free, and $t^\ell \not\equiv t \pmod{\ell^2}$ for any prime ℓ dividing d. Let $\operatorname{ind}\varphi := [\mathcal{O}_K : \mathbb{Z}[\theta]]$, where θ is a root of φ, and $K = \mathbb{Q}(\theta)$.

Proof. Let ℓ be a prime dividing d, and write $d = m\ell^k$ where $\gcd(m, \ell) = 1$. We begin by showing that $\ell \nmid \operatorname{ind}\varphi$. Note that $\varphi(x) \equiv (x^m - t)^{\ell^k} \pmod{\ell}$, where $x^m - t$ is separable modulo ℓ, and set

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

Let β be a root of g modulo ℓ. According to Dedekind's criterion, $\ell \mid \operatorname{ind}\varphi$ if and only if β is root of $\ell f(x)$ modulo ℓ^2, where

$$\ell f(\beta) \equiv (\beta^m)^{\ell^k} - t \pmod{\ell^2}.$$

Moreover, since $\beta^m \equiv t \pmod{\ell}$, we have $(\beta^m)^\ell \equiv t^\ell \equiv t \pmod{\ell}$. Applying Lemma 2.3, we see that

$$(\beta^m)^{\ell^k} \equiv t^{\ell^k} \equiv t \pmod{\ell^2} \quad \text{if and only if} \quad t^\ell \equiv t \pmod{\ell}^2.$$

However $t^\ell \not\equiv t \pmod{\ell^2}$ by assumption, so $\ell \nmid \operatorname{ind}\varphi$.

We now show that if $p \mid t$, then $p \nmid \operatorname{ind}\varphi$. Set

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

In this case, $p \mid \operatorname{ind}\varphi$ if and only if $f(0) = t/p \equiv 0 \pmod{p}$. It follows immediately that 0 is a root of f modulo p if and only if $t \equiv 0 \pmod{p^2}$. However, our assumption that t is square-free eliminates this possibility. Thus $p \nmid \operatorname{ind}\varphi$, and we conclude that $\operatorname{ind}\varphi = 1$.

□

Corollary 2.4. *Suppose $t = s^k$ where s is square-free, $\gcd(k, d) = 1$, and $s^\ell \not\equiv s \pmod{\ell^2}$ for each prime ℓ dividing d. Let θ be a root of $x^d - t$. Then $K = \mathbb{Q}(\theta)$ is monogenic.*

Proof. For each root θ of $x^d - s^k$, there is a root α of $x^d - s$ satisfying $\alpha^k = \theta$. It is easily verified that $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha)$, which is monogenic by Theorem 1.1.

□

Finally, we remark that the condition $t^\ell \equiv t \pmod{\ell^2}$ will only be satisfied if t is contained in one of ℓ equivalence classes modulo ℓ^2.

Proposition 2.5. *Let $[t]$ denote the equivalence class of t modulo ℓ^2. Then $t^\ell \equiv t \pmod{\ell^2}$ if and only if $[t] \in \{[0^\ell], [1^\ell], [2^\ell], [3^\ell], \ldots, [(\ell-1)^\ell]\}$.*

Proof. Writing $t = q\ell + r$, where $0 \leq r < \ell$, we have $t^\ell \equiv r^\ell \pmod{\ell^2}$ by Lemma 2.2. Thus $t^\ell \equiv t \pmod{\ell^2}$ if and only if $t \equiv r^\ell \pmod{\ell^2}$.

□

3. Field discriminant

In the proof of Theorem 1.1, we saw that $p \mid \operatorname{ind}\varphi$ if and only if $t \equiv 0 \pmod{p^2}$, and $\ell \mid \operatorname{ind}\varphi$ if $t^\ell \equiv t \pmod{\ell^2}$ for any ℓ dividing d. In this section, we apply the Montes algorithm to determine the exact multiplicity of each prime divisor of the index. The Montes algorithm is described extensively in a series of papers [8, 9, 10, 11], however for this paper, we will not need to full power of their algorithm. The key result is Theorem 3.1, which provides a lower bound on the p-adic valuation of the index. By restricting to the cases where this lower bound is an equality (which it will be for most choices of d and t), we can distill the algorithm to a few steps.

We begin by giving a summary of the algorithm as it pertains to this paper. Following that, we apply the algorithm in two cases, first for the primes dividing t (Proposition 3.2), then to the primes dividing d but not t (Proposition 3.5). Together, these results give Theorem 1.2.

3.1. **Montes algorithm.** Let $\Phi \in \mathbb{Z}[x]$ be a monic irreducible polynomial, and let $\operatorname{ind}_p \Phi = \nu_p(\operatorname{ind}\Phi)$ denote the p-adic valuation of $\operatorname{ind}\Phi$. The value $\operatorname{ind}_p \Phi$ may be computed as follows.

First, factor Φ modulo p and write

$$\Phi(x) \equiv \phi_1(x)^{e_1} \cdots \phi_r(x)^{e_r} \pmod{p},$$

where the ϕ_i are monic lifts of the irreducible factors of Φ modulo p. The algorithm will terminate regardless of the choice of lifts, however the choice of lift may simplify the computations significantly.

For each factor ϕ_i, there is a unique expression

$$\Phi(x) = a_0(x) + a_1(x)\phi_i(x) + a_2(x)\phi_i(x)^2 + \cdots + a_s(x)\phi_i(x)^s$$

where the a_j are integral polynomials satisfying $\deg a_j < \deg \phi_i$. This expression is called the *ϕ_i-development* of Φ.

From the ϕ_i-development, construct the *ϕ_i-Newton polygon* by taking the lower convex hull of the points

$$\left\{ \left(j, \nu_p(a_j(x))\right) : 0 \le j \le s \right\}, \tag{2}$$

where $\nu_p(a_j(x))$ is defined to be the minimal p-adic valuation of the coefficients of $a_j(x)$. Only the sides of negative slope are of import, and we call the set of sides of negative slope the *ϕ_i-polygon*. The set of lattice points under the ϕ_i-polygon carries important arithmetic data, and to keep track of these points, we define

$$\operatorname{ind}_{\phi_i}(\Phi) = (\deg \phi_i) \cdot \#\{(x,y) \in \mathbb{Z}^2 : x > 0, y > 0, \\ (x,y) \text{ is on or under the } \phi_i\text{-polygon}\}.$$

To each lattice point on the ϕ_i-polygon, we attach a *residual coefficient*

$$\operatorname{res}(j) = \begin{cases} \operatorname{red}(a_j(x)/p^{\nu_p(a_j(x))}) & \text{if } \left(j, \nu_p(a_j(x))\right) \text{ is on the } \phi_i\text{-polygon}, \\ 0 & \text{otherwise}, \end{cases}$$

where $\operatorname{red} : \mathbb{Z}[x] \to \mathbb{F}_p[x]/(\phi_i(x))$ denotes the reduction map modulo p and ϕ_i. For any side S of the ϕ_i-polygon, denote the left and right endpoints of S by (x_0, y_0) and (x_1, y_1), respectively. We define the *degree* of S to be $\deg S = \gcd(y_1 - y_0, x_1 - x_0)$.

In other words, $\deg S$ is equal to the number of segments into which the integral lattice divides S. We associate to S a *residual polynomial*

$$R_S(y) = \sum_{i=0}^{\deg S} \operatorname{res}\left(x_0 + i\frac{(x_1 - x_0)}{\deg S}\right) y^i \in \mathbb{F}_p[y]/(\phi_i(y)).$$

We note that $\operatorname{res}(x_0)$ and $\operatorname{res}(x_1)$ are necessarily non-zero, and in particular, it is always the case that $\deg S = \deg R_S$.

Finally, if R_S is separable for each S of the ϕ_i-polygon, then Φ is *ϕ_i-regular*, and if Φ is ϕ_i-regular for each factor ϕ_i, then Φ is *p-regular*.

Theorem 3.1 (Theorem of the index)**.** *We have*

$$\operatorname{ind}_p \Phi \geq \sum_{i=1}^{r} \operatorname{ind}_{\phi_i}(\Phi)$$

with equality if Φ is p-regular.

Proof. See [9, Section 4.4]. □

3.2. **Index contributions from primes dividing t.** Suppose $\varphi(x) = x^d - t$ (which is assumed to be irreducible), and let p be a prime dividing t. Note that $\varphi(x) = x^d - t \equiv x^d \pmod{p}$, so we have one factor $\phi(x) := x$ to consider in the Montes algorithm. In this case, the ϕ-polygon of φ is the usual Newton polygon of φ, which is one-sided with endpoints $(0, \nu_p(t))$ and $(d, 0)$. The residual polynomial associated to this side is $R_S(y) = y^g + c_0$, where $g = \gcd(\nu_p(t), d)$.

Note that the residual polynomial $R_S(y)$ is separable modulo p if and only if $\gcd(g, p) = 1$. Therefore, φ is p-regular if and only if $\gcd(d, p, \nu_p(t)) = 1$.

Proposition 3.2. *Let p be a prime dividing t, and suppose $\gcd(d, p, \nu_p(t)) = 1$. Then*

$$\operatorname{ind}_p(x^d - t) = \frac{(d-1)(\nu_p(t) - 1) + \gcd(d, \nu_p(t)) - 1}{2}.$$

Proof. By Theorem 3.1, the p-adic valuation of the index is equal to the number of lattice points in the first quadrant that are on or under the Newton polygon. The number of lattice points on the polygon is $\gcd(d, \nu_p(t)) - 1$.

For the lattice points under the polygon, we note that these are the lattice points that are contained in the triangle given by the vertices $(0, 0)$, $(0, \nu_p(t))$, and $(d, 0)$. By Pick's theorem, the number of lattice points on the interior of this triangle I is given by the formula

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

where A is the area of the triangle, and B is the number of lattice points on its perimeter. Here, we have $A = d\nu_p(t)/2$ and $B = d + \nu_p(t) + \gcd(d, \nu_p(t))$. Thus

$$I = \frac{(d-1)(\nu_p(t) - 1) + 1 - \gcd(d, \nu_p(t))}{2}.$$

Adding I to the number of lattice points on the polygon completes the proof.

□

Remark. Evaluating $\operatorname{ind}_p \varphi$ in the cases where $\gcd(d, \nu_p(t), p) > 1$ requires further iterations of this algorithm using Newton polygons of higher order. We will not address these cases in this paper, and instead we refer the reader to [9, Section 2] for more details.

Remark. Note that $\operatorname{ind}_p(x^d - t) = 0$ for every prime p dividing t if and only if t is square-free, which corroborates the result obtained from Dedekind's criterion.

3.3. **Index contributions from primes dividing d (but not t).** Suppose that $\varphi(x) = x^d - t$ is irreducible, and let ℓ be a prime dividing d that does not divide t. Writing $d = m\ell^k$, where $\gcd(m, \ell) = 1$, we have $x^d - t \equiv (x^m - t)^{\ell^k} \pmod{\ell}$. It may be that $x^m - t$ is reducible modulo ℓ, however the $(x^m - t)$-development of φ will be useful in computing the developments for each of the irreducible factors of φ. The $(x^m - t)$-development of φ may be computed via binomial expansion:

$$\begin{aligned}\varphi(x) &= (x^m)^{\ell^k} - t \\ &= (x^m - t + t)^{\ell^k} - t \\ &= -t + \sum_{j=0}^{\ell^k} \binom{\ell^k}{j} t^{\ell^k - j}(x^m - t)^j \\ &= t^{\ell^k} - t + \sum_{j=1}^{\ell^k} \binom{\ell^k}{j} t^{\ell^k - j}(x^m - t)^j.\end{aligned} \tag{3}$$

Setting $a_j = \binom{\ell^k}{j} t^{\ell^k - j}$, we have the following.

Lemma 3.3. *Let $0 \le c \le k$. If $j < \ell^c$, then $\nu_\ell(a_j) > k - c$. If $j = \ell^c$, then $\nu_\ell(a_j) = k - c$.*

Proof. Note that $\nu_\ell(a_j) = \nu_\ell\binom{\ell^k}{j}$ since t is relatively prime to ℓ. The result now follows by [5, Lemma 5.2.4]. □

Since $\gcd(m, \ell) = 1$, the polynomial $x^m - t$ is separable in $\mathbb{F}_\ell[x]$, hence we have

$$x^d - t \equiv (x^m - t)^{\ell^k} \equiv (\phi_1(x)\phi_2(x)\cdots\phi_s(x))^{\ell^k} \pmod{\ell}.$$

Using equation (3), we compute the ϕ_i-developments of φ.

Proposition 3.4. *For any irreducible factor ϕ of φ modulo ℓ, the ϕ-polygon is the lower convex hull of the set of points*

$$\{(0, \nu_\ell(t^\ell - t)\} \cup \{(\ell^c, k - c) : 1 \le c \le k\}.$$

In particular, the ϕ-polygon of φ does not depend on ϕ.

Proof. Fix an irreducible factor ϕ of φ modulo ℓ. Then there exists a polynomial $h(x)$ with constant coefficient coprime to ℓ that satisfies $\phi(x)h(x) = x^m - t$. For each $1 \le j \le \ell^k$, we compute the ϕ-development of $h(x)^j$:

$$h(x)^j = \sum_{n=0}^{s_j} b_{j,n}(x)\phi(x)^n,$$

where each $b_{j,n}(x)$ satisfies $\deg b_{j,n} < \deg \phi$. Combined with equation (3), we derive the ϕ-development of φ:

$$\varphi(x) = t^{\ell^k} - t + \sum_{j=1}^{\ell^k} a_j(x^m - t)^j$$

$$
\begin{aligned}
&= t^{\ell^k} - t + \sum_{j=1}^{\ell^k} a_j \phi(x)^j \sum_{n=0}^{s_j} b_{j,n}(x)\phi(x)^n \\
&= t^{\ell^k} - t + a_1\phi(x)\left(b_{1,0}(x) + b_{1,1}(x)\phi(x) + \cdots + b_{1,s_1}(x)\phi(x)^{s_1}\right) \\
&\quad + a_2\phi(x)^2\left(b_{2,0}(x) + b_{2,1}(x)\phi(x) + \cdots + b_{2,s_2}\phi(x)^{s_2}\right) \\
&\quad + a_3\phi(x)^3\left(b_{3,0}(x) + b_{3,1}(x)\phi(x) + \cdots + b_{3,s_3}(x)\phi(x)^{s_3}\right) \\
&\quad\quad \vdots \\
&\quad + a_{\ell^k}\phi(x)^{\ell^k}\left(b_{\ell^k,0}(x) + b_{\ell^k,1}(x)\phi(x) + \cdots + b_{\ell^k,s_{\ell^k}}(x)\phi(x)^{s_{\ell^k}}\right) \\
&= t^{\ell^k} - t + \sum_{j=1}^{\ell^k s_{\ell^k}} \left(\sum_{i=1}^{j} a_i b_{i,j-i}(x)\right)\phi(x)^j.
\end{aligned}
$$

Setting $\alpha_j(x) = \sum_{i=1}^{j} a_i b_{i,j-i}(x)$, it is clear that the ℓ-adic valuations of the α_j are determined by the ℓ-adic valuations of the a_j. Noting that $\nu_\ell(b_{i,0}) = 0$, it follows from Lemma 3.3 that whenever $c \le k$,

$$
\begin{aligned}
\nu_\ell(\alpha_{\ell^c}(x)) = \nu_\ell(a_{\ell^c}) = k - c \quad &\text{if } j = \ell^c, \\
\nu_\ell(\alpha_j(x)) > \nu_\ell(a_{\ell^c}) = k - c \quad &\text{if } j < \ell^c.
\end{aligned}
$$

Thus for $1 \le j \le \ell^k$, the vertices $(j, \nu_\ell(\alpha_j(x)))$ all lie on or above the lower convex hull of the set of points

$$\{(\ell^c, k-c) : 1 \le c \le k\}.$$

Finally, we include the constant term of the ϕ-development of φ into consideration. Since $\ell \nmid t$, we have $\nu_\ell(t^{\ell^k} - t) = \nu_\ell(t^\ell - t)$, concluding the proof.

□

It is straightforward to check that for any prime ℓ, the degree of each side of this polygon is 1 (and therefore φ is ℓ-regular) with one exception. When $\ell = 2$ and $2 \le \nu_2(t^{2^k} - t) \le k+1$, each side of the polygon is degree 1 except for the leftmost side, which is degree 2. Namely, setting $v = \nu_2(t^{2^k} - t)$, the leftmost edge passes through three vertices on the polygon: $(0, v)$, $(2^{k+1-v}, v-1)$, and $(2^{k+2-v}, v-2)$. The residual polynomial associated to this side is $y^2 + y + 1$, which is separable over $\mathbb{F}_2[y]$, and thus φ is ℓ-regular in this case as well. See Example 3.6.

Proposition 3.5. *Let ℓ be a prime dividing d that does not divide t, write $d = m\ell^k$ where $\gcd(m, \ell) = 1$, and set $v = \nu_\ell(t^\ell - t)$. Then*

$$\operatorname{ind}_\ell(x^d - t) = \sum_{j=1}^{\min\{v-1,k\}} m\ell^{k-j}.$$

Proof. Since φ is ℓ-regular, it follows by Theorem 3.1 that

$$\operatorname{ind}_\ell \varphi = \sum_{i=1}^{s} \operatorname{ind}_{\phi_i}(\varphi).$$

As we have noted previously, $x^d - t \equiv (x^m - t)^{\ell^k} \equiv (\phi_1(x)\phi_2(x)\cdots\phi_s(x))^{\ell^k} \pmod{\ell}$. By Proposition 3.4, the ϕ_i-polygons are independent ϕ_i, so letting L denote the

number of lattice points on and under the polygon, we have

$$\operatorname{ind}_\ell \varphi = L \sum_{i=1}^{s} \deg \phi_i = mL.$$

To compute L, we note that the lattice points on and under the polygon are

$$\{(x, y) \in \mathbb{Z}^2 : 0 < x < v, 0 < y \leq \ell^{k-x}\},$$

where $v = \nu_\ell(t^\ell - t)$. In particular, the lattice points are arranged into $\min\{v-1, k\}$ rows, where the number of lattice points in j-th row (counting up from the x-axis) is ℓ^{k-j}.

□

We conclude this paper with an example.

Example 3.6. Suppose $\varphi_0(x) = x^{6^3} - t$ is irreducible and $\gcd(t, 6) = 1$. By Proposition 3.5, the index $\operatorname{ind} \varphi_0$ is potentially divisible by large powers of 2 and 3. The possible ϕ-polygons for the prime 2 are shown in Figure 1, and the possible ϕ-polygons for the prime 3 are shown in Figure 2. The 2-adic and 3-adic valuations of the index are given in the following tables.

$\nu_2(t^2 - t)$	$\operatorname{ind}_2 \varphi_0$
1	0
2	$4 \cdot 27$
3	$6 \cdot 27$
4+	$7 \cdot 27$

$\nu_3(t^2 - t)$	$\operatorname{ind}_3 \varphi_0$
1	0
2	$9 \cdot 8$
3	$12 \cdot 8$
4+	$13 \cdot 8$

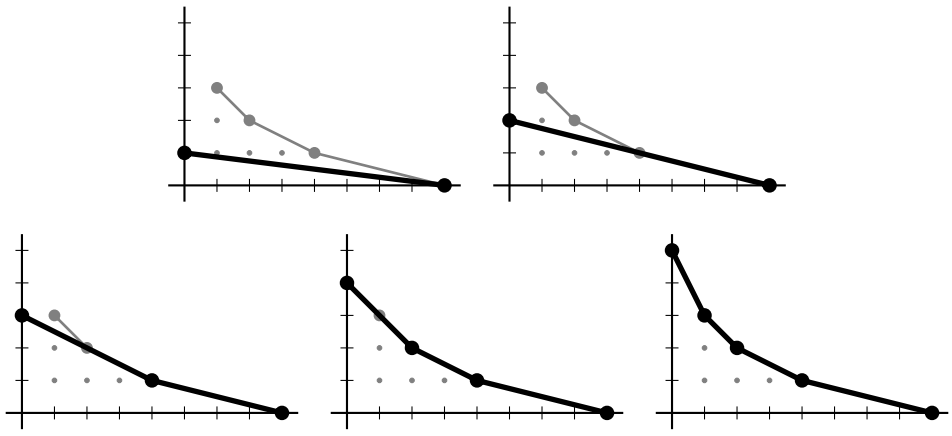

Figure 1. ϕ-polygons of $x^{6^3} - t$ at $p = 2$.

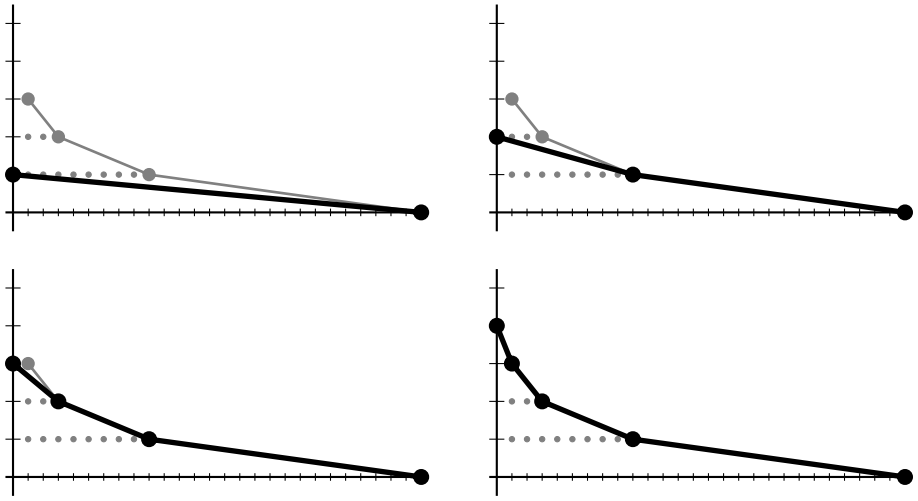

FIGURE 2. ϕ-polygons of $x^{6^3} - t$ at $p = 3$.

REFERENCES

[1] M. Bardestani. The density of a family of monogenic number fields. arXiv:1202.2047, June 2014.

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

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

[4] T. A. Gassert. Discriminants of Chebyshev radical extensions. *J. Théor. Nombres Bordeaux*, 26(3):607–633, 2014.

[5] T. A. Gassert. *Prime decomposition in iterated towers and discriminant formulae*. PhD thesis, University of Massachusetts Amherst, 2014.

[6] T. A. Gassert. Discriminants of simplest 3^n-tic extensions. *Funct. Approx. Comment. Math.*, 52(2):193–214, 2015.

[7] M.-N. Gras. Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbf{Q}$ de degré premier $l \geq 5$. *J. Number Theory*, 23(3):347–353, 1986.

[8] 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(3):667–696, 2011.

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

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

[11] J. Guàrdia, J. Montes, and E. Nart. Higher Newton polygons and integral bases. *J. Number Theory*, 147:549–589, 2015.

[12] 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(1):9, 2000.