JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Hanson SMITH

Radical Dynamical Monogenicity

Tome 37, nº 1 (2025), p. 153-169.

https://doi.org/10.5802/jtnb.1317

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **37** (2025), 153–169

Radical Dynamical Monogenicity

par Hanson SMITH

Résumé. Soient a un entier et p un nombre premier tel que $f(x) = x^p - a$ est irréductible. On note $f^n(x)$ l'itéré n-ième de $f(x)$. Nous étudions la monogénéité des corps de nombres définis par les racines de $f^n(x)$ et donnons des conditions nécessaires et suffisantes pour qu'une racine de $f^n(x)$ génère une base entière de puissances pour chaque $n \geq 1$. De plus, nous généralisons ces critères à un corps de nombres quelconque.

Abstract. Let a be an integer and p a prime so that $f(x) = x^p - a$ is irreducible. Write $f^n(x)$ to indicate the n-fold composition of $f(x)$ with itself. We study the monogenicity of number fields defined by roots of $f^n(x)$ and give necessary and sufficient conditions for a root of $f^n(x)$ to yield a power integral basis for each $n \geq 1$. Further, we generalize these criteria to an arbitrary number field.

1. Results and Previous Work

Let L be a number field. We will denote the ring of integers by $\mathcal{O}_L$. Suppose M is a finite extension of L. If $\mathcal{O}_M = \mathcal{O}_L[\alpha]$ for some $\alpha \in \mathcal{O}_M$, then we say M *is monogenic over* L or $\mathcal{O}_M$ has a *power* $\mathcal{O}_L$*-integral basis.* In this case, we call α a *monogenerator.* If $f(x)$ is the minimal polynomial of α over L, then we also call $f(x)$ *monogenic.* When L is $\mathbb{Q}$ we will simply say M is *monogenic* or $\mathcal{O}_M$ has a *power integral basis.*

If $\mathfrak{p}$ is a prime of $\mathcal{O}_L$, then we write $(\mathcal{O}_L)_\mathfrak{p}$ for the localization of $\mathcal{O}_L$ at $\mathfrak{p}$. Given an $\mathcal{O}_M$-order R, we say R is $\mathfrak{p}$*-maximal* if $R \otimes (\mathcal{O}_L)_\mathfrak{p} \cong \mathcal{O}_M \otimes (\mathcal{O}_L)_\mathfrak{p}$. Indeed, if R is $\mathfrak{p}$-maximal for each prime $\mathfrak{p}$ of $\mathcal{O}_L$, then R is the maximal order $\mathcal{O}_M$.

If $f(x) \in \mathbb{Z}[x]$ is a polynomial, then we write

$$f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n\text{-times}}.$$

This paper investigates the monogenicity of extensions obtained by adjoining a root of $f^n(x)$ where $f(x) = x^p - a$ is an irreducible integer polynomial with p a prime number. In particular, we prove the following.

Manuscrit reçu le 11 août 2023, révisé le 18 septembre 2024, accepté le 8 novembre 2024.
2020 *Mathematics Subject Classification.* 11R04, 11R21, 37P05.
Mots-clefs. Monogenic, Power integral basis, Radical extension, Iteration.

Theorem 1.1. *Write α_n for a root of $f^n(x)$, and let K_n denote $\mathbb{Q}(\alpha_n)$. Fix a natural number $N \geq 1$. The ring of integers $\mathcal{O}_{K_n}$ is $\mathbb{Z}[\alpha_n]$ for all $n \leq N$ if and only if $a^p \not\equiv a \bmod p^2$ and $f^n(0)$ is squarefree for all $n \leq N$.*

The proof is local and the subject of Section 4. The prime p (Lemma 4.2) requires more subtlety than the primes ℓ that do not divide the degree of $f(x)$ (Lemma 4.3). Both arguments are via induction and use a previous result of the author (Theorem 3.1); however, for p we employ a more detailed computation with valuations and must show that p is totally ramified in K_n. The statement and proof adapt readily to an arbitrary base number field K, and a rigorous proof of the relative version of Theorem 1.1 is the subject of the appendix.

1.1. Previous Work. The literature regarding monogenic fields is vast. A recent text on monogenicity that focuses on using index form equations is Gaál's book [8]. Another modern resource is Evertse and Győry's book [5]. Radical extensions[1] also have a very extensive body of previous work. We will not undertake a general survey of the literature involving radical extensions and monogenicity here; the curious reader can see [19] for this.

Our investigation is inspired by [15] where Li studies iterates of $f(x) = x^2 - a$. Li uses novel arguments to give necessary and sufficient conditions for a root of $f^n(x)$ to be a monogenerator for all n less than or equal to a fixed positive integer N. We extend Li's results to $x^p - a$ with p an odd prime. In a similar vein, [3] investigates a family of totally real 2-towers and gives necessary and sufficient conditions for monogenicity. Castillo's result in particular considers backward orbits of integers other than 0. [1] also contains a complete discussion of the situation $x^2 - 2 = t$. In subsequent work, the author and Zack Wolske [20] have given necessary and sufficient criteria for the monogenicity of iterates of quadratic polynomials. Also subsequent to the study at hand, Sharma, Sarma, and Laishram [18] give necessary and sufficient conditions for the monogenicity of iterates of $x^m - a \in \mathbb{Z}[x]$ for any m.

Other authors have studied the monogenicity of iterates of polynomials defining radical extensions. In [13], Jones considers $h(x) = (x - t)^m + t$ for $m \geq 2$ and $t \geq 1$. This polynomial yields the same extension as $g(x) = x^m + t$; however, the fields defined by roots of $h^n(x)$ and $g^n(x)$ differ for $n \geq 2$. Indeed, $h^n(x)$ yields the same number field as $x^{m^n} + t$ for all $n \geq 1$, but $g^n(x)$ does not. For the monogenicity of iterates of Chebyshev polynomials, consult [9].

Given the simple shape of radical polynomials and the fact that $x^d + c$, up to a change of variables, represents all polynomials of degree d with

[1] These extensions are also called *pure extensions* or *root extensions*.

exactly one finite cricital point, it is not surprising that a number of authors have studied the dynamics of these polynomials. We mention a few papers which are adjacent to our note. In [2], the authors investigate the Galois groups of iterates of $x^q + c$. The work in [7] studies the basic properties of iterates and composites of polynomials, finding properties such as irreducibility, separability, complete splitting, and solubility by radicals are not necessarily preserved. The specific case of irreducibility of iterates of a radical polynomial $x^d + c$ is considered in [4]. They investigate irreducibility over a wide class of fields, but of primary interest to us will be their Corollary 5, which shows that if $h(x) = x^d + c$ is irreducible in $\mathbb{Z}[x]$, then so are its iterates.

2. Background: The Montes Algorithm and Ore's Theorems

The Montes algorithm is a powerful p-adic factorization algorithm that is based on and extends the pioneering work of Øystein Ore [17]. We do not need the full strength of the Montes algorithm here. In fact, though we use the notation and setup of the general implementation, we will only make use of the aspects developed by Ore. The following is a brief summary of the tools we will utilize; for the complete development of the Montes algorithm, see [11]. Our notation will roughly follow [6], which gives a more extensive summary than we undertake here.

Let p be an integral prime, K a number field with ring of integers $\mathcal{O}_K$, and $\mathfrak{p}$ a prime of K above p. Write $K_\mathfrak{p}$ to denote the completion of K at $\mathfrak{p}$. Suppose we have a monic, irreducible polynomial $f(x) \in \mathcal{O}_K[x]$. We extend the standard $\mathfrak{p}$-adic valuation to $\mathcal{O}_K[x]$ by defining the $\mathfrak{p}$-adic valuation of $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathcal{O}_K[x]$ to be

$$v_\mathfrak{p}(f(x)) = \min_{0 \le i \le n} (v_\mathfrak{p}(a_i)).$$

This is often called the *Gauss valuation.* If $\phi(x), f(x) \in \mathcal{O}_K[x]$ are such that $\deg \phi \le \deg f$, then we can write

$$f(x) = \sum_{i=0}^{k} a_i(x)\phi(x)^i,$$

for some k, where each $a_i(x) \in \mathcal{O}_K[x]$ has degree less than $\deg \phi$. We call the above expression the *ϕ-adic development* of $f(x)$. We associate to the ϕ-adic development of $f(x)$ an open Newton polygon by taking the lower convex hull of the integer lattice points $(i, v_p(a_i(x)))$. The sides of the Newton polygon with negative slope are the *principal ϕ-polygon.* The positive integer lattice points on or under the principal ϕ-polygon contain a wealth of arithmetic information. We denote the number of such lattice points by $\mathrm{ind}_\phi(f)$.

Write $k_\mathfrak{p}$ for the residue field $\mathcal{O}_K/\mathfrak{p}$, and let $\overline{f(x)}$ be the image of $f(x)$ in $k_\mathfrak{p}[x]$. It will often be the case that we develop $f(x)$ with respect to a lift of an irreducible factor $\phi(x)$ of $\overline{f(x)}$. In this situation, we will want to consider the extension of $k_\mathfrak{p}$ obtained by adjoining a root of $\phi(x)$. We denote this finite field by $k_{\mathfrak{p},\phi}$. We associate to each side of the principal ϕ-polygon a polynomial in $k_{\mathfrak{p},\phi}[y]$. Suppose S is a side of the principal ϕ-polygon with initial vertex $(s, v_\mathfrak{p}(a_s(x)))$, terminal vertex $(k, v_\mathfrak{p}(a_k(x)))$, and slope $-\frac{h}{e}$ written in lowest terms. Define the length of the side to be $l(S) = k - s$ and the degree to be $d \coloneqq \frac{l(S)}{e}$. Let $\text{red} : \mathcal{O}_K[x] \to k_{\mathfrak{p},\phi}$ denote the homomorphism obtained by quotienting by the ideal $(\mathfrak{p}, \phi(x))$. For each j in the range $0 \leq j \leq d$, we set $i = s + je$ and define the residual coefficient to be

$$c_i = \begin{cases} 0 & \text{if } (i, v_\mathfrak{p}(a_i(x))) \text{ lies strictly above } S \text{ or } v_\mathfrak{p}(a_i(x)) = \infty, \\ \text{red}\left(a_i(x)/\pi^{v_\mathfrak{p}(a_i(x))}\right) & \text{if } (i, v_\mathfrak{p}(a_i(x))) \text{ lies on } S. \end{cases}$$

Finally, the *residual polynomial* of the side S is the polynomial

$$R_S(y) = c_s + c_{s+e}y + \cdots + c_{s+(d-1)e}y^{d-1} + c_{s+de}y^d \in k_{\mathfrak{p},\phi}[y].$$

Notice, that c_s and c_{s+de} are always nonzero since they are the initial and terminal vertices, respectively, of the side S.

With all of these definitions in hand, we package everything into two theorems that encapsulate how we will employ the Montes algorithm. The first focuses on the indices of monogenic orders.

Theorem 2.1 (Ore's theorem of the index)**.** *Let $f(x) \in \mathcal{O}_K[x]$ be a monic irreducible polynomial and let α be a root. Choose monic polynomials $\phi_1, \ldots, \phi_s \in \mathcal{O}_K[x]$ whose reductions modulo $\mathfrak{p}$ are exactly the distinct irreducible factors of $\overline{f(x)} \in k_\mathfrak{p}[x]$. Then,*

$$v_p\left([\mathcal{O}_{K(\alpha)} : \mathcal{O}_K[\alpha]]\right) \geq \text{ind}_{\phi_1}(f) + \cdots + \text{ind}_{\phi_s}(f).$$

Further, equality holds if, for every ϕ_i, each side of the principal ϕ_i-polygon has a separable residual polynomial.

For our applications, we will employ the following equivalence.

Corollary 2.2. *The prime $\mathfrak{p}$ does not divide $[\mathcal{O}_{K(\alpha)} : \mathcal{O}_K[\alpha]]$ if and only if $\text{ind}_{\phi_i}(f) = 0$ for all i. In this case each principal ϕ_i-polygon is one-sided.*

The second theorem we state connects prime splitting and polynomial factorization. The "three dissections" that we will outline below are due to Ore, and the full Montes algorithm is an extension of this. Our statement loosely follows Theorem 1.7 of [6].

Theorem 2.3. *[Ore's Three Dissections] Let $f(x) \in \mathcal{O}_K[x]$ be a monic irreducible polynomial and let α be a root. Suppose*

$$\overline{f(x)} = \phi_1(x)^{r_1} \cdots \phi_s(x)^{r_s}$$

is a factorization into irreducibles in $k_{\mathfrak{p}}[x]$. Hensel's lemma shows $\phi_i(x)^{r_i}$ corresponds to a factor of $f(x)$ in $K_{\mathfrak{p}}[x]$ and hence to a factor $\mathfrak{m}_i$ of $\mathfrak{p}$ in $K(\alpha)$.

Choosing a lift and abusing notation, suppose the principal ϕ_i-polygon has sides $S_1, \ldots, S_g$. Each side of this polygon corresponds to a distinct factor of $\mathfrak{m}_i$.

Write $\mathfrak{n}_j$ for the factor of $\mathfrak{m}_i$ corresponding to the side S_j. Suppose S_j has slope $-\frac{h}{e}$. If the residual polynomial $R_{S_j}(y)$ is separable, then the prime factorization of $\mathfrak{n}_j$ mirrors the factorization of $R_{S_j}(y)$ in $k_{\mathfrak{p},\phi_i}[y]$, but every factor of $R_{S_j}(y)$ will have an exponent of e. In other words,

$$\text{if } R_{S_j}(y) = \gamma_1(y) \ldots \gamma_k(y) \quad \text{in} \quad k_{\mathfrak{p},\phi_i}[y], \quad \text{then} \quad \mathfrak{n}_j = \mathfrak{P}_1^e \cdots \mathfrak{P}_k^e \quad \text{in} \quad K(\alpha)$$

with $\deg(\gamma_m)$ equaling the residue class degree of $\mathfrak{P}_m$ for each $1 \leq m \leq k$. In the case where $R_{S_j}(y)$ is not separable, further developments are required to factor $\mathfrak{p}$.

3. General Radical Extensions and Lemmas

In this section we recall and restate Theorem 6.1 of [19]. This theorem will be a key lemma in our study of the monogenicity of $f^n(x)$. The notation in this section follows [19] and should not be conflated with our notation elsewhere.

Consider an arbitrary number field L and an element $\alpha \in \mathcal{O}_L$ such that $x^n - \alpha$ is irreducible over L. To avoid trivialities, we assume $n \geq 2$. One computes

$$\text{Disc}\,(x^n - \alpha) = (-1)^{\frac{n^2-n}{2}}\, n^n (-\alpha)^{n-1}. \tag{3.1}$$

The primes dividing this discriminant are the primes for which $\mathcal{O}_L\,[\sqrt[n]{\alpha}]$ may fail to be maximal.

For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ dividing (n), we write p for the residue characteristic and f for the residue class degree. We factor $n = p^e m$ with $\gcd(m, p) = 1$. Let ε be congruent to e modulo f with $1 \leq \varepsilon \leq f$, and define β to be α to the power $p^{f-\varepsilon}$:

$$\beta := \alpha^{p^{f-\varepsilon}}.$$

By construction β is a p^e-th root of α modulo $\mathfrak{p}$.

Theorem 3.1 (Theorem 6.1 of [19])**.** *If $\mathfrak{p} \mid (\alpha)$, then the order $\mathcal{O}_L\,[\sqrt[n]{\alpha}]$ is $\mathfrak{p}$-maximal if and only if $v_{\mathfrak{p}}(\alpha) = 1$. If $\mathfrak{p} \mid (n)$ and $\mathfrak{p} \nmid (\alpha)$, then the order*

$\mathcal{O}_L\left[\sqrt[n]{\alpha}\right]$ is $\mathfrak{p}$-maximal if and only if

$$v_{\mathfrak{p}}\left(\alpha - \beta^{p^e}\right) = 1.$$

If $\mathfrak{p} \nmid (\alpha n)$, then $\mathcal{O}_L\left[\sqrt[n]{\alpha}\right]$ is $\mathfrak{p}$-maximal.

When the base field is $\mathbb{Q}$, one can use results in [10] or [12]. The prime degree case ($N = 1$ in Theorem 1.1) is classical and is described in [21]. Keith Conrad's note[2] provides a nice exposition. For our work on iterates, however, we will need the generality of Theorem 3.1.

The following lemma simplifies the situation when the base field is $\mathbb{Q}$.

Lemma 3.2. *Let p be a prime and let $a \in \mathbb{Z}$, then*

$$v_p\left(a^p - a\right) = v_p\left(a^{p^m} - a\right)$$

for every $m > 0$.

Proof. Write $w = v_p(a^p - a)$. If $p \mid a$, then this is clear. Suppose $p \nmid a$. It suffices to show that

$$v_p\left(a^{p-1} - 1\right) = v_p\left(a^{p^m-1} - 1\right)$$

The smallest of Fermat's theorems tells us that the base-p expansion of a^{p-1} has the form

$$a^{p-1} = 1 + a_w p^w + (\text{higher powers of } p)$$

where $0 < a_w < p$. Clearly,

$$v_p\left(a^{p-1} - 1\right) = v_p(a_w p^w + (\text{ higher powers of } p)) = w.$$

Note $p^m - 1 = (p-1)(p^{m-1} + p^{m-2} + \cdots + p + 1)$, so

$$\begin{aligned} a^{p^m-1} &= \left(a^{p-1}\right)^{p^{m-1}+p^{m-2}+\cdots+p+1} \\ &= \left(1 + a_w p^w + (\text{higher powers of } p)\right)^{p^{m-1}+p^{m-2}+\cdots+p+1} \\ &= 1 + \left(p^{m-1} + p^{m-2} + \cdots + p + 1\right) a_w p^w + (\text{higher powers of } p). \end{aligned}$$

We can now see that

$$v_p\left(a^{p^m-1} - 1\right) = v_p(a_w p^w + (\text{higher powers of } p)) = w. \qquad \square$$

The next lemma makes our setup more amenable to induction.

Lemma 3.3. *Let $M_{\mathfrak{P}}/L_{\mathfrak{p}}$ be a finite extension of local fields that is totally ramified of degree n, where we write $\mathfrak{P}$ and $\mathfrak{p}$ for the maximal ideals of the respective valuation rings. Let $\pi_{\mathfrak{P}}$ and $\pi_{\mathfrak{p}}$ denote uniformizers so $v_{\mathfrak{P}}(\pi_{\mathfrak{p}}) = n$. If α is in the valuation ring of $M_{\mathfrak{P}}$, then*

$$v_{\mathfrak{P}}(\alpha) = v_{\mathfrak{p}}\left(\mathrm{Norm}_{M_{\mathfrak{P}}/L_{\mathfrak{p}}}(\alpha)\right).$$

[2] https://kconrad.math.uconn.edu/blurbs/gradnumthy/integersradical.pdf

Proof. Write $m_{\pi_\mathfrak{p}}(x)$ for the minimal polynomial of $\pi_\mathfrak{P}$ over $L_\mathfrak{p}$, and note that $m_{\pi_\mathfrak{p}}(x)$ is $\mathfrak{p}$-Eisenstein. Thus,

$$v_\mathfrak{p}\big(\operatorname{Norm}_{M_\mathfrak{P}/L_\mathfrak{p}}(\pi_\mathfrak{P})\big) = v_\mathfrak{p}\big(m_{\pi_\mathfrak{P}}(0)\big) = 1.$$

If $v_\mathfrak{P}(\alpha) = j$, then $\alpha = u\pi_\mathfrak{P}^j$ with u a unit. Hence

$$\begin{aligned} v_\mathfrak{p}\big(\operatorname{Norm}_{M_\mathfrak{P}/L_\mathfrak{p}}(\alpha)\big) &= v_\mathfrak{p}\Big(\operatorname{Norm}_{M_\mathfrak{P}/L_\mathfrak{p}}(u)\operatorname{Norm}_{M_\mathfrak{P}/L_\mathfrak{p}}\left(\pi_\mathfrak{P}^j\right)\Big) \\ &= j v_\mathfrak{p}\big(\operatorname{Norm}_{M_\mathfrak{P}/L_\mathfrak{p}}(\pi_\mathfrak{P})\big) = j, \end{aligned}$$

and we have our result. □

4. Necessary and Sufficient Conditions for the Monogenicity of $f^n(x)$

Recall, we take $f(x) = x^p - a$ to be irreducible, and we write

$$f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n\text{-times}}.$$

The following special case of a result of Danielson and Fein shows that we do not need to be concerned with irreducibility after the first iterate.

Proposition 4.1 ([4, Corollary 5])**.** *If $f(x) = x^p - a$ is irreducible in $\mathbb{Z}[x]$, then $f^n(x)$ is irreducible in $\mathbb{Z}[x]$ for all $n > 0$.*

For shorthand, we write α_n for a root of $f^n(x)$ with $f(\alpha_n) = \alpha_{n-1}$. Further, write K_n for $\mathbb{Q}(\alpha_n)$ and note $\mathbb{Q} \subset K_1 \subset K_2 \subset \cdots$. Motivated by [15], we wish to show the following:

Theorem 1.1. *Fix a natural number $N \geq 1$, then $\mathcal{O}_{K_n} = \mathbb{Z}[\alpha_n]$ for all $n \leq N$ if and only if $a^p \not\equiv a \bmod p^2$ and $f^n(0)$ is squarefree for all $n \leq N$.*

We will establish this theorem via two lemmas. The first considers the prime p while the second considers primes $\ell \neq p$.

Lemma 4.2. *The order $\mathbb{Z}[\alpha_n]$ is p-maximal for all $n > 0$ if and only if $a^p \not\equiv a \bmod p^2$. When this is the case, p is totally ramified in K_n. Moreover, if $a^p \equiv a \bmod p^2$, then $\mathbb{Z}[\alpha_1]$ is not p-maximal.*

Proof. First, we consider the case where $p \mid a$. In this case the x-adic development shows $\mathbb{Z}[\alpha_1]$ is p-maximal if and only if $a^p \not\equiv a \bmod p^2$. Thus this condition is necessary. Supposing now that $a^p \not\equiv a \bmod p^2$, a straightforward computation shows that $f^n(x) \equiv x^{p^n} \bmod p$ and $v_p(f^n(0)) = v_p(a)$. Considering the x-adic development again, $\mathbb{Z}[\alpha_n]$ is p-maximal if and only if $a^{p^n} \not\equiv a \bmod p^2$ which holds if and only if $a^p \not\equiv a \bmod p^2$ by Lemma 3.2. The slope of the principal x-polygon is $-\frac{1}{p^n}$ in each of these cases, so p is totally ramified. To be more succinct, in this case, each $f^n(x)$ is p-Eisenstein if and only if $f(x)$ is p-Eisenstein.

Now we consider the more subtle case where $p \nmid a$. We proceed by using induction. For the base case we want to understand the p-maximality of $f(x) = x^p - a$. Theorem 3.1 shows that $f(x)$ is p-maximal if and only if $a^p \not\equiv a \bmod p^2$. If $\mathbb{Z}[\alpha_1]$ is p-maximal, then since $x^p - a \equiv (x-a)^p \bmod p$, Dedekind–Kummer factorization shows that p is totally ramified.

For the induction step, take $n \geq 1$, and suppose that $\mathbb{Z}[\alpha_k]$ is p-maximal with p totally ramified for all $k \leq n$. We have already seen that it is necessary that $v_p(a^p - a) = 1$. We wish to show that this is sufficient for $\mathbb{Z}[\alpha_{n+1}]$ to be p-maximal with p totally ramified. It suffices to show that $\mathcal{O}_{K_n}[\alpha_{n+1}]$ is $\mathfrak{p}_n$-maximal over $\mathcal{O}_{K_n}$ with $\mathfrak{p}_n$ totally ramified. Here $\mathfrak{p}_n$ is the unique prime of $\mathcal{O}_{K_n}$ above p and $p = (\mathfrak{p}_n)^{p^n}$. To this end, we apply the Montes algorithm to the polynomial $x^p - \alpha_n - a$, the minimal polynomial of α_{n+1} over K_n.

Note the residue field of $\mathfrak{p}_n$ is $\mathbb{F}_p$. Hence, reducing $x^p - \alpha_n - a$ modulo $\mathfrak{p}_n$, we find

$$x^p - \alpha_n - a \equiv (x - \alpha_n - a)^p \bmod \mathfrak{p}_n.$$

If the constant coefficient of the $(x-\alpha_n-a)$-adic development of $x^p-\alpha_n-a$ has $\mathfrak{p}_n$-adic valuation 1, then the principal $(x-\alpha_n-a)$-polygon is one-sided with slope $-\frac{1}{p}$. This implies $\mathfrak{p}_n$ is totally ramified in K_{n+1} and $\mathcal{O}_{K_n}[\alpha_{n+1}]$ is $\mathfrak{p}_n$-maximal. We have

$$x^p = (x - \alpha_n - a + \alpha_n + a)^p = \sum_{i=0}^{p} \binom{p}{i} (x - \alpha_n - a)^{p-i} (\alpha_n + a)^i,$$

so

$$\begin{aligned} x^p - \alpha_n - a &= \sum_{i=0}^{p} \binom{p}{i} (x - \alpha_n - a)^{p-i} (\alpha_n + a)^i - \alpha_n - a \\ &= \sum_{i=0}^{p-1} \binom{p}{i} (\alpha_n + a)^i (x - \alpha_n - a)^{p-i} + (\alpha_n + a)^p - \alpha_n - a. \end{aligned}$$

From the binomial coefficients, we see the constant coefficient of the $(x - \alpha_n - a)$-adic development is

$$\alpha_n^p - \alpha_n + a^p - a + (\text{terms divisible by } p).$$

As $v_{\mathfrak{p}_n}(p) = p^n$, the terms divisible by p are not relevant, and we are interested in the $\mathfrak{p}_n$-adic valuation of $\alpha_n^p - \alpha_n + a^p - a$. Since $p \mid (a^p - a)$

and $v_{\mathfrak{p}_n}(p) = p^n$, we want the $\mathfrak{p}_n$-adic valuation of $\alpha_n^p - \alpha_n$. We compute

$$\begin{aligned}
&v_{\mathfrak{p}_n}\left(\alpha_n^p - \alpha_n\right) \\
&= v_{\mathfrak{p}_n}\left(\alpha_{n-1} + a - \alpha_n\right) && \text{since } \alpha_n^p = \alpha_{n-1} + a, \\
&= v_{\mathfrak{p}_{n-1}}\left(\mathrm{Norm}_{K_n/K_{n-1}}\left(\alpha_{n-1} + a - \alpha_n\right)\right) && \text{by Lemma 3.3,} \\
&= v_{\mathfrak{p}_{n-1}}\left(\prod_{i=1}^{p}\left(\alpha_{n-1} + a - \zeta_p^i \alpha_n\right)\right) && \text{since } \alpha_{n-1}, a \in K_{n-1}, \\
&= v_{\mathfrak{p}_{n-1}}\big(\,(\alpha_{n-1} + a)^p - \alpha_n^p\big) && \text{using the factorization of } x^p - \alpha_{n-1} - a, \\
&= v_{\mathfrak{p}_{n-1}}\big(\,(\alpha_{n-1} + a)^p - \alpha_{n-1} - a\big) && \text{since } \alpha_n^p = \alpha_{n-1} + a.
\end{aligned}$$

Note that when $n = 1$, we have $K_0 = \mathbb{Q}$, $\mathfrak{p}_0 = p$, and $\alpha_0 = 0$. In this case, the above shows

$$v_{\mathfrak{p}_1}\left(\alpha_1^p - \alpha_1\right) = v_p\left(a^p - a\right) = 1.$$

Now suppose $n > 1$. Because $\mathcal{O}_{K_{n-1}}[\alpha_n]$ is $\mathfrak{p}_{n-1}$-maximal, taking the $(x - \alpha_{n-1} - a)$-adic development of $x^p - \alpha_{n-1} - a$ shows

$$v_{\mathfrak{p}_{n-1}}\big(\,(\alpha_{n-1} + a)^p - \alpha_{n-1} - a\big) = 1.$$

Hence, $v_{\mathfrak{p}_n}\left(\alpha_n^p - \alpha\right) = 1$. We see $\mathfrak{p}_n$ is totally ramified in K_{n+1}, and $\mathcal{O}_{K_n}[\alpha_{n+1}]$ is $\mathfrak{p}_n$-maximal. □

Now we turn our attention to primes $\ell \neq p$. We roughly follow the strategy employed by [15] and aim to establish the following lemma.

Lemma 4.3. *Let ℓ be a prime not dividing p.*

1. *If $f^n(0)$ is divisible by ℓ^2, then $\mathbb{Z}[\alpha_n]$ is not ℓ-maximal.*
2. *If $f^n(0)$ is not divisible by ℓ^2, then $\mathcal{O}_{K_{n-1}}[\alpha_n]$ is an $\mathfrak{l}$-maximal $\mathcal{O}_{K_{n-1}}$-module for any prime ideal $\mathfrak{l}$ of $\mathcal{O}_{K_{n-1}}$ above ℓ.*

Proof. We begin with (1). Note that $f^n(x) \in \mathbb{Z}[x^p]$. Hence, if $\ell \mid f^n(0)$, then

$$f^n(x) \equiv x^p \prod \phi_i(x)^{e_i} \bmod \ell.$$

Taking the x-adic development, we see the initial vertex of the principal x-polygon is $\big(0, v_\ell(f^n(0))\big)$. Thus, if $\ell^2 \mid f^n(0)$, then $\mathbb{Z}[\alpha_n]$ is not ℓ-maximal.

We turn our attention to (2). We have two cases. For $n = 1$, Theorem 3.1 shows that $\mathbb{Z}[\sqrt[p]{a}]$ is ℓ-maximal if and only if ℓ^2 does not divide a.

Now, suppose $n > 1$ and let $\mathfrak{l}$ be a prime of $\mathcal{O}_{K_{n-1}}$ above ℓ. Note that $x^p - \alpha_{n-1} - a$ is the minimal polynomial of α_n over $\mathcal{O}_{K_{n-1}}$. Since $\mathfrak{l} \nmid (p)$, Theorem 3.1 shows that $\mathcal{O}_{K_{n-1}}[\alpha_n]$ is $\mathfrak{l}$-maximal if and only if $\mathfrak{l}^2$ does not divide $(\alpha_{n-1} + a)$. We will show the contrapositive of (2), so suppose $\mathcal{O}_{K_{n-1}}[\alpha_n]$ is not an $\mathfrak{l}$-maximal $\mathcal{O}_{K_{n-1}}$-module. Thus $\mathfrak{l}^2 \mid (\alpha_{n-1} + a)$. Since

$\alpha_n^p = \alpha_{n-1} + a$, we have $\mathfrak{l}^2 \mid (\alpha_n^p)$. Taking norms, we see $\mathrm{Norm}_{K_n/\mathbb{Q}}(\mathfrak{l}^2)$ divides $\mathrm{Norm}_{K_n/\mathbb{Q}}(\alpha_n^p)$. Therefore,

$$\left(\mathrm{Norm}_{K_{n-1}/\mathbb{Q}}(\mathfrak{l}^2)\right)^p \text{ divides } |f^n(0)|^p,$$
$$\text{and } \left(\mathrm{Norm}_{K_{n-1}/\mathbb{Q}}(\mathfrak{l})\right)^2 \text{ divides } |f^n(0)|.$$

Since $\ell \mid \mathrm{Norm}_{K_{n-1}/\mathbb{Q}}(\mathfrak{l})$, we see $\ell^2 \mid f^n(0)$. Hence, if $\mathcal{O}_{K_{n-1}}[\alpha_n]$ is not an $\mathfrak{l}$-maximal $\mathcal{O}_{K_{n-1}}$-module for some prime ideal $\mathfrak{l}$ of $\mathcal{O}_{K_{n-1}}$ above ℓ, then $\ell^2 \mid f^n(0)$. The contrapositive yields (2). □

With our lemmas established, we combine them to get the main theorem.

Proof of Theorem 1.1. For maximality away from p, Lemma 4.3 shows that it is necessary that $\ell^2 \nmid f^n(0)$ for every $n \leq N$ and for every prime $\ell \neq p$. Thus, suppose $\ell^2 \nmid f^n(0)$ for all $n \leq N$ and all primes $\ell \neq p$. As Lemma 4.2 already shows it is necessary that $a^p \not\equiv a \bmod p$, suppose that this also holds.

We proceed by induction. The base case is clear and already present in the literature. For the induction hypothesis, suppose $N > 1$ and $\mathcal{O}_{K_k} = \mathbb{Z}[\alpha_k]$ for all $k \leq n < N$. We wish to show that $\mathcal{O}_{K_{n+1}} = \mathbb{Z}[\alpha_{n+1}]$. Lemma 4.3 shows that $\mathcal{O}_{K_n}[\alpha_{n+1}]$ is $\mathfrak{l}$-maximal for every prime $\mathfrak{l}$ of $\mathcal{O}_{K_n}$ with $\mathfrak{l} \nmid (p)$. Lemma 4.2 shows that $\mathcal{O}_{K_n}[\alpha_{n+1}]$ is p-maximal. Thus $\mathcal{O}_{K_n}[\alpha_{n+1}] = \mathcal{O}_{K_{n+1}}$. Since $\alpha_{n+1}^p = \alpha_n + a$ and because $\mathcal{O}_{K_n} = \mathbb{Z}[\alpha_n]$, we see that $\mathbb{Z}[\alpha_{n+1}] = \mathcal{O}_{K_{n+1}}$. With induction we have our result. □

Remark 4.4. Since the proof is local, the same techniques, mutatis mutandis, can be used to give a relative version:

Theorem 4.5. *Fix a natural number $N \geq 1$. Let K be an arbitrary number field, let $f(x) = x^p - a \in \mathcal{O}_K[x]$, and suppose $f^n(x)$ is irreducible over $K[x]$ for $1 \leq n \leq N$. Write α_n for a root of $f^n(x)$ so that $f(\alpha_n) = \alpha_{n-1}$, and let L_n denote $K(\alpha_n)$. For each prime $\mathfrak{p}$ of $\mathcal{O}_K$ above p, let $\beta_\mathfrak{p} = a^{p^{f-1}}$, where f is the residue class degree of $\mathfrak{p}$.*

The ring of integers $\mathcal{O}_{L_n}$ equals $\mathcal{O}_K[\alpha_n]$ for all $n \leq N$ if and only if $\beta_\mathfrak{p}^p \not\equiv a \bmod \mathfrak{p}^2$ for any prime $\mathfrak{p}$ of $\mathcal{O}_K$ above p and $v_\mathfrak{l}(f^n(0)) \leq 1$ for every prime ideal $\mathfrak{l}$ of $\mathcal{O}_K$ not dividing p and every $n \leq N$.

A rigorous proof of Theorem 4.5 is the subject of the appendix. However, in forthcoming work, the author, Joachim König, and Zack Wolske generalize the conditions Theorem 4.5 and give straightforward necessary and sufficient criteria for iterates of a general polynomial over an arbitrary number field to be monogenic.

Remark 4.6. In [15], the author obtains a result on the divisibility of class numbers. In particular, if $f(x)$ is Eisenstein at some prime, then $h(K_n)$

divides $h(K_{n+1})$, where $h(K_n)$ is the class number of the number field generated by a root of $f^n(x)$. The key is total ramification; see Corollary 2.3 of [16]. Since Lemma 4.2 shows p is totally ramified when $a^p \not\equiv a \bmod p^2$, we obtain the following result whether or not $f(x)$ is Eisenstein at any prime.

Proposition 4.7. *Let $f(x) = x^p - a$ and suppose $a^p \not\equiv a \bmod p^2$. Keeping the notation of earlier so that $K_n = \mathbb{Q}(\alpha_n) \subset K_{n+1} = \mathbb{Q}(\alpha_{n+1})$, we write $h(K_n)$ for class number of K_n. Then $h(K_n)$ divides $h(K_{n+1})$ for all $n \geq 1$.*

5. Examples

The following examples are meant to help one get a flavor for the results above.

Example 5.1. Let $f(x) = x^3 - 5$. We have

$$\begin{aligned}
f^1(x) &= x^3 - 5,\\
f^2(x) &= x^9 - 15x^6 + 75x^3 - 130,\\
f^3(x) &= x^{27} - 45x^{24} + 900x^{21} - 10515x^{18} + 79200x^{15} - 399375x^{12}\\
&\quad + 1350075x^9 - 2954250x^6 + 3802500x^3 - 2197005,\\
f^4(x) &= x^{81} - 135x^{78} + 8775x^{75} - 365670x^{72} + 10974150x^{69}\\
&\quad - 252591750x^{66} + 4636542150x^{63} - 69676294500x^{60}\\
&\quad + 873198646875x^{57} - 9248742526140x^{54} + 83605735086975x^{51}\\
&\quad - 649601439751125x^{48} + 4359787949171700x^{45}\\
&\quad - 25355305623690000x^{42} + 127982660067337500x^{39}\\
&\quad - 560741779121461875x^{36} + 2129668434875446875x^{33}\\
&\quad - 6990730404446390625x^{30} + 19739990955501740700x^{27}\\
&\quad - 47622742788031456500x^{24} + 97226962675508036250x^{21}\\
&\quad - 165792343518924835500x^{18} + 231863628297715627500x^{15}\\
&\quad - 259125463888412765625x^{12} + 222610926346013255625x^9\\
&\quad - 138078523258432818750x^6 + 55062074290560187500x^3\\
&\quad - 10604571775299775130.
\end{aligned}$$

We can see that explicitly computing the iterates of even a relatively simple radical polynomial quickly becomes unwieldy. However, from Theorem 1.1, we know that $f^n(x)$ will always be 3-maximal since $9 \nmid (125 - 5)$. Moreover, we need only check the factorization of the constant coefficients to see that $\mathbb{Z}[\sqrt[3]{5}] = \mathcal{O}_{K_1}$, $\mathbb{Z}[\alpha_2] = \mathcal{O}_{K_2}$, $\mathbb{Z}[\alpha_3] = \mathcal{O}_{K_3}$, and $\mathbb{Z}[\alpha_4] = \mathcal{O}_{K_4}$.

Consider the following for an example where not every iterate supplies a monogenerator.

Example 5.2. Take $f(x) = x^5 - 5$. We have

$$\begin{aligned}
f^1(x) &= x^5 - 5,\\
f^2(x) &= x^{25} - 25x^{20} + 250x^{15} - 1250x^{10} + 3125x^5 - 3130,\\
f^3(x) &= x^{125} - 125x^{120} + 7500x^{115} - \cdots + 1499675775156250000x^5\\
&\qquad - 300415051279300005,\\
f^4(x) &= x^{625} - 625x^{620} + 193750x^{615} - \cdots - (300415051279300005)^5 - 5.
\end{aligned}$$

Since 5 is prime and $3130 = 2 \cdot 5 \cdot 313$ is squarefree, we see $\mathcal{O}_{K_1} = \mathbb{Z}[\sqrt{5}]$ and $\mathcal{O}_{K_2} = \mathbb{Z}[\alpha_2]$. However $300415051279300005 = 3^5 \cdot 5 \cdot 247255186238107$. Hence, Lemma 4.3 shows $\mathcal{O}_{K_3} \neq \mathbb{Z}[\alpha_3]$. In particular, $\mathbb{Z}[\alpha_3]$ is not 3-maximal. Thus we see that the first couple of iterates being monogenic does not ensure that every iterate will be monogenic. Interestingly, $f^4(0)$ is squarefree; however, one can show 3 divides $[\mathcal{O}_{K_4} : \mathbb{Z}[\alpha_4]]$.

Example 5.3. Let $f(x) = x^2 - 2$. We have

$$\begin{aligned}
f^1(x) &= x^2 - 2,\\
f^2(x) &= x^4 - 4x^2 + 2,\\
f^3(x) &= x^8 - 8x^6 + 20x^4 - 16x^2 + 2,\\
f^4(x) &= x^{16} - 16x^{14} + 104x^{12} - 352x^{10} + 660x^8 - 672x^6 + 336x^4 - 64x^2 + 2,\\
f^5(x) &= x^{32} - 32x^{30} + \cdots + 5440x^4 - 256x^2 + 2.
\end{aligned}$$

We can see that $f^n(0) = \left(f^{n-1}(0)\right)^2 - 2$, so that $f^n(0) = 2$ for all $n > 1$. Thus every iterate of $f(x)$ is monogenic!

These examples motivate the following question, a variation of which was posed by Marianela Castillo in her thesis.

Question 5.4. What are the other $f(x)$ such that $f^n(x)$ is monogenic for all $n \geq 1$?

For $x^2 - 2$, it can be show that backward orbits of other integers can supply monogenerators. The example

$$\sqrt{2 + \sqrt{2 + \cdots + \sqrt{7}}}$$

and others of a similar shape was shown to the author by Zack Wolske. A detailed study appears in [1]. When $p = 2$ and with the ABC-conjecture, [3, Corollary 4.4] shows that, for any $N > 0$, one can find infinitely many $f(x)$ such that $f^n(x)$ is monogenic for each $n \leq N$. Recent work of the author and Wolske [20] gives a partial answer to the question for quadratic

polynomials. Even more recent work of König, the author, and Wolske [14] provides a more general framework for the question and supplies diverse families of examples. However, it appears that any unconditional and more complete answer to Question 5.4 would brush against difficult problems involving squarefree values of polynomials.

Appendix: A Proof of Theorem 4.5

We devote this appendix to a rigorous proof of the relative version of Theorem 1.1. Since the proof Theorem 1.1 is local, it is no surprise that the proof of the relatively version is essentially the same.

Theorem 4.5. *Fix a natural number $N \geq 1$. Let K be an arbitrary number field, let $f(x) = x^p - a \in \mathcal{O}_K[x]$, and suppose $f^n(x)$ is irreducible over $K[x]$ for $1 \leq n \leq N$. Write α_n for a root of $f^n(x)$ so that $f(\alpha_n) = \alpha_{n-1}$, and let L_n denote $K(\alpha_n)$. For each prime $\mathfrak{p}$ of $\mathcal{O}_K$ above p, let $\beta_{\mathfrak{p}} = a^{p^{f-1}}$, where f is the residue class degree of $\mathfrak{p}$.*

The ring of integers $\mathcal{O}_{L_n}$ equals $\mathcal{O}_K[\alpha_n]$ for all $n \leq N$ if and only if $\beta_{\mathfrak{p}}^p \not\equiv a \bmod \mathfrak{p}^2$ for any prime $\mathfrak{p}$ of $\mathcal{O}_K$ above p and $v_{\mathfrak{l}}(f^n(0)) \leq 1$ for every prime ideal $\mathfrak{l}$ of $\mathcal{O}_K$ not dividing p and every $n \leq N$.

As before, we will establish this theorem via two lemmas. The first considers the primes above p while the second considers primes $\mathfrak{l} \nmid (p)$.

Lemma A.1. *Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ above p with residue class degree f. The order $\mathcal{O}_K[\alpha_n]$ is $\mathfrak{p}$-maximal for all $n > 0$ if and only if $a^{p^f} \not\equiv a \bmod \mathfrak{p}^2$. When this is the case, $\mathfrak{p}$ is totally ramified in L_n. Moreover, if $a^{p^f} \equiv a \bmod \mathfrak{p}^2$, then $\mathcal{O}_K[\alpha_1]$ is not $\mathfrak{p}$-maximal.*

Proof. First, we consider the case where $\mathfrak{p} \mid (a)$. In this case the x-adic development shows $\mathcal{O}_K[\alpha_1]$ is $\mathfrak{p}$-maximal if and only if $a^{p^f} \not\equiv a \bmod \mathfrak{p}^2$ if and only if $v_{\mathfrak{p}}(a) = 1$ if and only if $f(x)$ is $\mathfrak{p}$-Eisenstein. Thus this condition is necessary. By a lemma of Odoni or via a quick justification, we can see that iterates of Eisenstein polynomials are again Eisenstein. Thus, the condition is sufficient. Moreover, $\mathfrak{p}$ is totally ramified.

Now we consider the more subtle case where $\mathfrak{p} \nmid (a)$. We proceed by induction. For the base case we want to understand the $\mathfrak{p}$-maximality of $f(x) = x^p - a$. Theorem 3.1 shows that $f(x)$ is $\mathfrak{p}$-maximal if and only if $\beta_{\mathfrak{p}}^p = a^{p^f} \not\equiv a \bmod \mathfrak{p}^2$. If $\mathcal{O}_K[\alpha_1]$ is $\mathfrak{p}$-maximal, then since $x^p - a \equiv (x - \beta_{\mathfrak{p}})^p \bmod \mathfrak{p}$, Dedekind–Kummer factorization shows that $\mathfrak{p}$ is totally ramified.

For the induction step, take $n \geq 1$, and suppose that $\mathcal{O}_K[\alpha_k]$ is $\mathfrak{p}$-maximal with $\mathfrak{p}$ totally ramified for all $k \leq n$. We have already seen that it is necessary that $v_{\mathfrak{p}}(\beta_{\mathfrak{p}}^p - a) = 1$. We wish to show that this is sufficient for $\mathcal{O}_K[\alpha_{n+1}]$ to be $\mathfrak{p}$-maximal with $\mathfrak{p}$ totally ramified. Letting $\mathfrak{P}_n$ denote the

unique prime of $\mathcal{O}_{L_n}$ above $\mathfrak{p}$, it suffices to show that $\mathcal{O}_{L_n}[\alpha_{n+1}]$ is $\mathfrak{P}_n$-maximal over $\mathcal{O}_{L_n}$ with $\mathfrak{P}_n$ totally ramified. To this end, we apply the Montes algorithm to the polynomial $x^p - \alpha_n - a$, the minimal polynomial of α_{n+1} over L_n.

Note the residue field of $\mathfrak{P}_n$ is isomorphic to $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$, the residue field of $\mathfrak{p}$. Letting $\beta_n = \alpha_n^{p^{f-1}}$ so $\beta_n^p \equiv \alpha_n \bmod \mathfrak{P}_n$[3] and reducing $x^p - \alpha_n - a$ modulo $\mathfrak{P}_n$, we find

$$x^p - \alpha_n - a \equiv (x - \beta_n - \beta_\mathfrak{p})^p \bmod \mathfrak{P}_n.$$

If the constant coefficient of the $(x-\beta_n-\beta_\mathfrak{p})$-adic development of $x^p-\alpha_n-a$ has $\mathfrak{P}_n$-adic valuation 1, then the principal $(x-\beta_n-\beta_\mathfrak{p})$-polygon is one-sided with slope $-\frac{1}{p}$. This implies $\mathfrak{P}_n$ is totally ramified in L_{n+1} and $\mathcal{O}_{L_n}[\alpha_{n+1}]$ is $\mathfrak{P}_n$-maximal. We have

$$x^p = (x - \beta_n - \beta_\mathfrak{p} + \beta_n + \beta_\mathfrak{p})^p = \sum_{i=0}^{p} \binom{p}{i} (x - \beta_n - \beta_\mathfrak{p})^{p-i} (\beta_n + \beta_\mathfrak{p})^i,$$

so

$$\begin{aligned} x^p - \alpha_n - a &= \sum_{i=0}^{p} \binom{p}{i} (x - \beta_n - \beta_\mathfrak{p})^{p-i} (\beta_n + \beta_\mathfrak{p})^i - \alpha_n - a \\ &= \sum_{i=0}^{p-1} \binom{p}{i} (\beta_n + \beta_\mathfrak{p})^i (x - \beta_n - \beta_\mathfrak{p})^{p-i} + (\beta_n + \beta_\mathfrak{p})^p - \alpha_n - a. \end{aligned}$$

From the binomial coefficients, we see the constant coefficient of the $(x - \beta_n - \beta_\mathfrak{p})$-adic development is

$$\begin{aligned} &\beta_n^p - \alpha_n + \beta_\mathfrak{p}^p - a + (\text{terms divisible by } p) \\ &\qquad = \alpha_n^{p^f} - \alpha_n + a^{p^f} - a + (\text{terms divisible by } p). \end{aligned}$$

The terms divisible by p are not relevant, and we are interested in the $\mathfrak{P}_n$-adic valuation of $\beta_n^p - \alpha_n + \beta_\mathfrak{p}^p - a$. Since $\mathfrak{p} \mid (\beta_\mathfrak{p}^p - a)$ and $\mathfrak{P}_n^{p^n} \mid \mathfrak{p}$, we want

[3] One could think of $\beta_\mathfrak{p}$ as β_0.

the $\mathfrak{P}_n$-adic valuation of $\beta_n^p - \alpha_n$. We compute

$$\begin{aligned}
&v_{\mathfrak{P}_n}\left(\beta_n^p - \alpha_n\right)\\
&= v_{\mathfrak{P}_n}\left(\alpha_n^{p^f} - \alpha_n\right) && \text{since } \beta_n = \alpha_n^{p^{f-1}},\\
&= v_{\mathfrak{P}_n}\left((\alpha_{n-1}+a)^{p^{f-1}} - \alpha_n\right) && \text{since } \alpha_n^p = \alpha_{n-1} + a,\\
&= v_{\mathfrak{P}_{n-1}}\left(\mathrm{Norm}_{L_n/L_{n-1}}\left((\alpha_{n-1}+a)^{p^{f-1}} - \alpha_n\right)\right) && \text{by Lemma 3.3,}\\
&= v_{\mathfrak{P}_{n-1}}\left(\prod_{i=1}^{p}\left((\alpha_{n-1}+a)^{p^{f-1}} - \zeta_p^i\alpha_n\right)\right) && \text{since } \alpha_{n-1}, a \in L_{n-1},\\
&= v_{\mathfrak{P}_{n-1}}\big((\alpha_{n-1}+a)^{p^f} - \alpha_n^p\big) && \text{as } \alpha_n^p - \alpha_{n-1} - a = 0,\\
&= v_{\mathfrak{P}_{n-1}}\big((\alpha_{n-1}+a)^{p^f} - \alpha_{n-1} - a\big) && \text{since } \alpha_n^p = \alpha_{n-1} + a.
\end{aligned}$$

Note that when $n = 1$, we have $L_0 = K$, $\mathfrak{P}_0 = \mathfrak{p}$, and $\alpha_0 = 0$. In this case, the above shows

$$v_{\mathfrak{P}_1}\left(\beta_1^p - \alpha_1\right) = v_{\mathfrak{p}}\left(a^{p^f} - a\right) = 1.$$

Now suppose $n > 1$. Because $\mathcal{O}_{L_{n-1}}[\alpha_n]$ is $\mathfrak{P}_{n-1}$-maximal, taking the $(x - \beta_{n-1} - \beta_{\mathfrak{p}})$-adic development of $x^p - \alpha_{n-1} - a$ and eliminating terms divisible by p shows

$$v_{\mathfrak{P}_{n-1}}\big((\alpha_{n-1}+a)^{p^f} - \alpha_{n-1} - a\big) = v_{\mathfrak{P}_{n-1}}\big((\beta_{n-1}+\beta_{\mathfrak{p}})^p - \alpha_{n-1} - a\big) = 1.$$

Hence, $v_{\mathfrak{P}_n}\left(\beta_n^p - \alpha\right) = 1$. We see $\mathfrak{P}_n$ is totally ramified in L_{n+1} and $\mathcal{O}_{L_n}[\alpha_{n+1}]$ is $\mathfrak{P}_n$-maximal. □

Now we turn our attention to primes $\mathfrak{l} \nmid (p)$.

Lemma A.2. *Let $\mathfrak{l}$ be a prime $\mathcal{O}_K$ that is not above p.*

(1) *If $v_{\mathfrak{l}}(f^n(0)) > 1$, then $\mathcal{O}_K[\alpha_n]$ is not $\mathfrak{l}$-maximal.*
(2) *If $v_{\mathfrak{l}}(f^n(0)) \leq 1$, then $\mathcal{O}_{L_{n-1}}[\alpha_n]$ is an $\mathfrak{L}$-maximal $\mathcal{O}_{L_{n-1}}$-module for any prime ideal $\mathfrak{L}$ of $\mathcal{O}_{L_{n-1}}$ above $\mathfrak{l}$.*

Proof. We begin with (1). Note that $f^n(x) \in \mathcal{O}_K[x^p]$. Hence, if $\mathfrak{l} \mid (f^n(0))$, then

$$f^n(x) \equiv x^p \prod \phi_i(x)^{e_i} \bmod \mathfrak{l}.$$

Taking the x-adic development, we see the initial vertex of the principal x-polygon is $(0, v_{\mathfrak{l}}(f^n(0)))$. Thus, if $v_{\mathfrak{l}}(f^n(0)) > 1$, then $\mathcal{O}_K[\alpha_n]$ is not $\mathfrak{l}$-maximal.

We turn our attention to (2). We have two cases. For $n = 1$, Theorem 3.1 shows that $\mathcal{O}_K[\alpha_1]$ is $\mathfrak{l}$-maximal if and only if $\mathfrak{l}^2$ does not divide (a).

Now, suppose $n > 1$ and let $\mathfrak{L}$ be a prime of $\mathcal{O}_{L_{n-1}}$ above $\mathfrak{l}$. Note that $x^p - \alpha_{n-1} - a$ is the minimal polynomial of α_n over $\mathcal{O}_{L_{n-1}}$. Since $\mathfrak{L} \nmid (p)$, Theorem 3.1 shows that $\mathcal{O}_{L_{n-1}}[\alpha_n]$ is $\mathfrak{L}$-maximal if and only if $v_{\mathfrak{L}}(\alpha_{n-1} + a) \leq 1$. We will show the contrapositive of (2), so suppose $\mathcal{O}_{L_{n-1}}[\alpha_n]$ is not an $\mathfrak{L}$-maximal $\mathcal{O}_{L_{n-1}}$-module. Thus $\mathfrak{L}^2 \mid (\alpha_{n-1} + a)$. Since $\alpha_n^p = \alpha_{n-1} + a$, we have $\mathfrak{L}^2 \mid (\alpha_n^p)$. Taking norms, the ideal generated by $\mathrm{Norm}_{L_n/K}(\mathfrak{L}^2)$ divides the ideal generated by $\mathrm{Norm}_{L_n/K}(\alpha_n^p)$. Therefore, since $\mathfrak{L} \subset \mathcal{O}_{L_{n-1}}$, as principal ideals we see

$$\Big(\mathrm{Norm}_{L_{n-1}/K}(\mathfrak{L}^2)\Big)^p \text{ divides } |f^n(0)|^p,$$
$$\text{and } \Big(\mathrm{Norm}_{L_{n-1}/K}(\mathfrak{L})\Big)^2 \text{ divides } |f^n(0)|.$$

Since $\mathfrak{l} \mid (\mathrm{Norm}_{L_{n-1}/K}(\mathfrak{L}))$, we see $v_{\mathfrak{l}}(f^n(0)) > 1$. Hence, if $\mathcal{O}_{L_{n-1}}[\alpha_n]$ is not an $\mathfrak{L}$-maximal $\mathcal{O}_{L_{n-1}}$-module for some prime ideal $\mathfrak{L}$ of $\mathcal{O}_{L_{n-1}}$ above $\mathfrak{l}$, then $v_{\mathfrak{l}}(f^n(0)) > 1$. □

With our lemmas established, we combine them to get the relative version of our main theorem.

Proof of Theorem 4.5. For maximality away from primes dividing (p), Lemma A.2 shows that it is necessary that $v_{\mathfrak{l}}(f^n(0)) \leq 1$ for every $n \leq N$ and for every prime $\mathfrak{l} \nmid (p)$. Thus, suppose $v_{\mathfrak{l}}(f^n(0)) \leq 1$ for all $n \leq N$ and all $\mathfrak{l} \nmid (p)$. As Lemma A.1 already shows it is necessary that $a^{p^f} \not\equiv a \bmod \mathfrak{p}$ for each prime $\mathfrak{p} \mid (p)$, suppose that this also holds.

We proceed by induction. The base case is Theorem 3.1. For the induction hypothesis, suppose $N > 1$ and $\mathcal{O}_{L_k} = \mathcal{O}_K[\alpha_k]$ for all $k \leq n < N$. We wish to show that $\mathcal{O}_{L_{n+1}} = \mathcal{O}_K[\alpha_{n+1}]$. Lemma A.2 shows that $\mathcal{O}_{L_n}[\alpha_{n+1}]$ is $\mathfrak{L}$-maximal for every prime $\mathfrak{L}$ of $\mathcal{O}_{L_n}$ with $\mathfrak{L} \nmid (p)$. Lemma A.1 shows that $\mathcal{O}_{L_n}[\alpha_{n+1}]$ is $\mathfrak{p}$-maximal. Thus $\mathcal{O}_{L_n}[\alpha_{n+1}] = \mathcal{O}_{L_{n+1}}$. Since $\alpha_{n+1}^p = \alpha_n + a$ and because $\mathcal{O}_{L_n} = \mathcal{O}_K[\alpha_n]$, we see that $\mathcal{O}_K[\alpha_{n+1}] = \mathcal{O}_{L_{n+1}}$. Induction yields the result. □

Acknowledgments. The author would like to thank Kimberly Ayers for the invitation that motivated this work. The author would also like to acknowledge Caleb Springer for kindly pointing out some oversights in an earlier draft. Finally, the author would like to thank the anonymous referee for the commentary and suggestions.

References

[1] W. Aitken, F. Hajir & C. Maire, "Finitely ramified iterated extensions", *Int. Math. Res. Not.* **2005** (2005), no. 14, p. 855-880.

[2] A. Bridy, J. R. Doyle, D. Ghioca, L.-C. Hsia & T. J. Tucker, "Finite index theorems for iterated Galois groups of unicritical polynomials", *Trans. Am. Math. Soc.* **374** (2021), no. 1, p. 733-752.

[3] M. Castillo, "A dynamical characterization for monogenity at every level of some infinite 2-towers", *Can. Math. Bull.* **65** (2022), no. 3, p. 806-814.
[4] L. Danielson & B. Fein, "On the irreducibility of the iterates of $x^n - b$", *Proc. Am. Math. Soc.* **130** (2002), no. 6, p. 1589-1596.
[5] J.-H. Evertse & K. Győry, *Discriminant equations in Diophantine number theory*, New Mathematical Monographs, vol. 32, Cambridge University Press, 2017, xviii+457 pages.
[6] L. E. Fadil, J. Montes & E. Nart, "Newton polygons and p-integral bases of quartic number fields", *J. Algebra Appl.* **11** (2012), no. 4, article no. 1250073 (33 pages).
[7] B. Fein & M. Schacher, "Properties of iterates and composites of polynomials", *J. Lond. Math. Soc. (2)* **54** (1996), no. 3, p. 489-497.
[8] I. Gaál, *Diophantine equations and power integral bases*, Birkhäuser/Springer, 2019, xxii+326 pages.
[9] T. A. Gassert, "Discriminants of Chebyshev radical extensions", *J. Théor. Nombres Bordeaux* **26** (2014), no. 3, p. 607-633.
[10] ———, "A note on the monogeneity of power maps", *Albanian J. Math.* **11** (2017), no. 1, p. 3-12.
[11] J. Guàrdia, J. Montes & E. Nart, "Newton polygons of higher order in algebraic number theory", *Trans. Am. Math. Soc.* **364** (2012), no. 1, p. 361-416.
[12] A. Jakhar, S. K. Khanduja & N. Sangwan, "Characterization of primes dividing the index of a trinomial", *Int. J. Number Theory* **13** (2017), no. 10, p. 2505-2514.
[13] L. Jones, "Monogenically stable polynomials", *Albanian J. Math.* **15** (2021), no. 2, p. 85-98.
[14] J. König, H. Smith & Z. Wolske, "Critical Point Criteria and Dynamically Monogenic Polynomials", 2024, `https://arxiv.org/abs/2412.10358`.
[15] R. Li, "On number fields towers defined by iteration of polynomials", *Arch. Math.* **119** (2022), no. 4, p. 371-379.
[16] J. M. Masley, "Class numbers of real cyclic number fields with small conductor", *Compos. Math.* **37** (1978), no. 3, p. 297-319.
[17] Ø. Ore, "Newtonsche Polygone in der Theorie der algebraischen Körper", *Math. Ann.* **99** (1928), no. 1, p. 84-117.
[18] H. Sharma, R. Sarma & S. Laishram, "Monogenity of iterates of irreducible binomials", *Commun. Algebra* **52** (2024), no. 11, p. 4678-4684.
[19] H. Smith, "The monogeneity of radical extensions", *Acta Arith.* **198** (2021), no. 3, p. 313-327.
[20] H. Smith & Z. Wolske, "Iterates of Quadratics and Monogenicity", 2024, `https://arxiv.org/abs/2406.03629`.
[21] J. Westlund, "On the fundamental number of the algebraic number-field $k(\sqrt[p]{m})$", *Trans. Am. Math. Soc.* **11** (1910), no. 4, p. 388-392.

Hanson Smith
Department of Mathematics
California State University San Marcos
333 S. Twin Oaks Valley Rd.
San Marcos, CA 92096
E-mail: `hsmith@csusm.edu`