Canad. J. Math. 2026, pp. 1–23
http://dx.doi.org/10.4153/S0008414X26102351
© The Author(s), 2026. Published by Cambridge University Press on behalf of Canadian Mathematical Society

Critical point criteria and dynamically monogenic polynomials

Joachim König, Hanson Smith, and Zack Wolske

Abstract. Let K be a number field with ring of integers $\mathcal{O}_K$, and let $f(x) \in \mathcal{O}_K[x]$ be a monic, irreducible polynomial. We establish necessary and sufficient conditions in terms of the critical points of $f(x)$ for the iterates of $f(x)$ to be monogenic polynomials. More generally, we give necessary and sufficient conditions for the backward orbits of elements of $\mathcal{O}_K$ under $f(x)$ to be monogenerators. We apply our criteria to construct novel examples of dynamically monogenic polynomials, yielding infinite towers of monogenic number fields with the backward orbit of one monogenerator giving a monogenerator at the next level.

1 Introduction and main result

Throughout this article, let K be a number field with ring of integers $\mathcal{O}_K$. We say that K is *monogenic* if there exists some α in $\mathcal{O}_K$ so that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. In other words, K is monogenic if there exists some algebraic integer α such that the powers of α form a power integral basis $\{1, \alpha, \alpha^2, \dots \alpha^{n-1}\}$ for $\mathcal{O}_K$. In this case, we say that α is a *monogenerator*, and we call the minimal polynomial of α a *monogenic polynomial*. More generally, if L is an extension of K, we say that L *is monogenic over* K if there exists an $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

Questions regarding monogenicity[1] are both theoretically and historically fundamental to algebraic number theory. Especially with the recent growth of arithmetic dynamics, it is natural to study the monogenicity of iterates of polynomials.

In this work, we present succinct necessary and sufficient criteria for when the backward orbits of an algebraic integer under a monic, integral polynomial are monogenerators. More informally and less generally, we answer the question of when all iterates of a polynomial are monogenic.

Before stating these criteria, we need a few definitions. Let α be integral and algebraic over K. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, write $\mathcal{O}_\mathfrak{p}$ to indicate $\mathcal{O}_K$ adjoined the inverse of every element not in $\mathfrak{p}$, and write $k_\mathfrak{p}$ to indicate the residue field $\mathcal{O}_K/\mathfrak{p}$. Let L denote $K(\alpha)$. We say that $\mathcal{O}_K[\alpha]$ is $\mathfrak{p}$-*maximal* if $\mathcal{O}_K[\alpha] \otimes_{\mathcal{O}_K} \mathcal{O}_\mathfrak{p} = \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_\mathfrak{p}$. If an irreducible $f(x) \in \mathcal{O}_K[x]$ has a root $\alpha \in \mathbb{C}$, then we say that $f(x)$ is $\mathfrak{p}$-*maximal* if $\mathcal{O}_K[\alpha]$

Received by the editors April 24, 2025 UTC; revised May 28, 2026 UTC; accepted June 8, 2026 UTC. Published online on Cambridge Core June 24, 2026.

The first-named author was supported by the National Research Foundation of Korea (NRF Basic Research Grant RS-2023-00239917).

AMS subject classification: **11R04, 11R21, 37P05.**

Keywords: Monogenic, power integral basis, arithmetic dynamics, post critically finite (PCF).

[1] Also called "monogeneity" or "monogenity" in addition to some other less common terms.

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

is $\mathfrak{p}$-maximal with respect to $\mathcal{O}_{K(\alpha)}$. When $K = \mathbb{Q}$, it is equivalent to require that $\mathfrak{p} = p$ does not divide the index $\left[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]\right]$.[2] If $\mathcal{O}_K[\alpha]$ is $\mathfrak{p}$-maximal for each prime $\mathfrak{p}$, then $\mathcal{O}_K[\alpha] = \mathcal{O}_L$ and α is a monogenerator. If $\mathfrak{P}$ is a prime of L above $\mathfrak{p}$, we write $e(\mathfrak{P} \mid \mathfrak{p})$ for the ramification index. As usual, given a polynomial $f(x)$, we let $f^n(x)$ denote the n-fold composition, and for a prime $\mathfrak{p}$ of $\mathcal{O}_K$, we let $v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$ denote the $\mathfrak{p}$-adic valuation.

Our main theorem allows a uniform treatment of all but finitely many primes, all of which are relatively small. We call these finitely many primes *exceptional*. See Condition 2.13 for a precise definition. In particular, $\mathfrak{p}$ is non-exceptional if $\mathrm{char} k_\mathfrak{p} > \deg(f)$ or if each irreducible factor of $f'(x)$ in $K[x]$ remains separable in $k_\mathfrak{p}[x]$. We are now able to state the main result.

Theorem 1.1 (The critical point criteria for monogenicity) *Let K be a number field. Fix $N > 0$. Suppose $f(x) \in \mathcal{O}_K[x]$ has a leading coefficient that is a unit, and let $a \in \mathcal{O}_K$ be such that $f^n(x) - a$ is irreducible over K for $1 \le n \le N$. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. There exists a polynomial $g(x) := g_\mathfrak{p}(x) \in \mathcal{O}_K[x]$ and a natural number $N_\mathfrak{p}$ such that the following holds: Let M be an extension of K where $g(x)$ splits and $\mathfrak{P}$ a prime of M above $\mathfrak{p}$. Then the polynomial $f^n(x) - a$ is $\mathfrak{p}$-maximal for each $1 \le n \le N$ if and only if for each root $\theta \in M$ of $g(x)$ and each $1 \le n \le N_\mathfrak{p}$, one has $v_\mathfrak{P}(f^n(\theta) - a) \le e(\mathfrak{P} \mid \mathfrak{p})$. More concretely,*

1. *If $\mathfrak{p}$ is non-exceptional, one may choose $N_\mathfrak{p} = N$ and $g(x) = f'(x)$ (independently of $\mathfrak{p}$ and a).*
2. *If $\mathfrak{p}$ is exceptional but is such that $f'(x) \not\equiv 0 \bmod \mathfrak{p}$, one may choose $N_\mathfrak{p} = N$ and $g(x) = \prod_{i=1}^{r} \phi_i(x)$ (independently of a), where the $\phi_i(x)$ are lifts of the distinct irreducible factors of $f'(x)$ in $k_\mathfrak{p}[x]$ to $\mathcal{O}_K[x]$.*
3. *If $\mathfrak{p}$ is such that $f'(x) \equiv 0 \bmod \mathfrak{p}$, one may choose $g(x)$ fulfilling $f(x) - a = g(x)^p$ in $k_\mathfrak{p}[x]$ with $p = \mathrm{char}\, k_\mathfrak{p}$ and $N_\mathfrak{p} = 1$.*

Theorem 1.1 will be proved via Theorems 2.9 and 2.15. The reader may consult Corollary 2.18 for a more streamlined special case when the critical values are in K. Applications of Theorem 1.1 become particularly striking in cases where (for $f(x)$ and a suitably chosen) it can be applied simultaneously for all $n \in \mathbb{N}$, since in this case, one obtains the simultaneous monogenicity of the polynomials $f^n(x) - a$ for all $n \in \mathbb{N}$. Such a pair $(f(x), a)$ is called a *dynamically monogenic pair* (cf. Definition 2.19). Investigating such pairs connects the topic of monogenicity with the quickly expanding field of arithmetic dynamics, a central problem of which is the study of arithmetic and Galois-theoretic properties of the backward orbits $\cup_{j \in \mathbb{N}} f^{-j}(\{a\})$ of a value a under a polynomial $f(x)$.

Theorem 1.1 and the applications herein generalize and subsume several previous results on simultaneous monogenicity of $f^n(x) - a$ for all $n \in \mathbb{N}$ for various $f(x)$ and a. This work was inspired by an effort to generalize [Smi25, SW24] (and hence generalize [Cas22, Li22]). Theorem 1.1 can be seen as a generalization of other recent work, including [SSL24] (which focuses on $f(x) = x^m - a$) and [Jon21] (which considers specific families, such as $f(x) = (x - a)^m + a$). [Gas14] made an earlier

[2] Up to sign, this index is the determinant of a change of basis matrix from an integral basis to a $\mathbb{Q}$-basis given by powers of α (see [Lan94, Proposition 16 of III, Section 3]).

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

connection between monogenicity and dynamics by giving conditions to guarantee the monogenicity of $T_\ell^n(x) - a$ when $T_\ell(x)$ is the Chebyshev polynomial of prime degree ℓ and $T_\ell^n(x) - a$ is irreducible. By applying Theorem 1.1 and some additional work on irreducibility, we obtain Theorem 4.5 which gives necessary and sufficient conditions for the dynamical monogenicity of $\big(T_\ell(x), a\big)$ with no degree restriction or irreducibility assumption. From another point of view, results on the monogenicity of radical polynomials can be readily generalized by taking a dynamical perspective and considering backward orbits under the power map $f(x) = x^d$. Thus, the main result of [Smi21] (and hence of [Gas17]) can be readily obtained from Theorem 1.1.

The generality of Theorem 1.1 also demonstrates some of the difficulties in identifying dynamically monogenic pairs $(f(x), a)$. Firstly, controlling $\mathfrak{p}$-adic valuations of infinitely many values simultaneously, as often required in Conditions 1 and 2, is very difficult, and unconditional positive results should often be expected to be out of reach. However, it may happen that the set of these values is actually a finite set. This occurs precisely when the polynomial $f(x)$ is post-critically finite (PCF). We therefore dedicate special attention to such polynomials in our applications in Section 4, notably extending previous results on specific PCF polynomials, such as $f(x) = x^d$ and $T_\ell(x)$, as mentioned above. Moreover, the application of Theorem 1.1 for all $n \in \mathbb{N}$ requires a simultaneous irreducibility assumption for all polynomials $f^n(x) - a$. In many cases, proving this property is considered a difficult problem in arithmetic dynamics, and many previous studies have resorted to accepting it as a black-box assumption. A key observation of Sections 3 and 4 is that, in several important key cases, this property follows from the combination of Conditions 1 and 3 (cf. Theorems 4.1 and 4.5) or can be guaranteed for "many" values a (cf. the example given by Theorem 4.11).

2 Establishing the critical point criteria

We begin with a criterion for the monogenicity of a polynomial that is due to Uchida [Uch77]. See [VV21] for a comparison to other criteria for monogenicity.

Theorem 2.1 (Uchida's criterion) *Let R be a Dedekind ring. Let α be an element of some integral domain which contains R, and let α be integral over R. Then $R[\alpha]$ is a Dedekind ring if and only if the defining polynomial $f(x)$ of α is not contained in $\mathfrak{m}^2$ for any maximal ideal $\mathfrak{m}$ of the polynomial ring $R[x]$.*

To get a feel for Uchida's result, take $R = \mathbb{Z}$. Here, $\mathfrak{m} = \big(p, \phi(x)\big)$ for some integral prime p and some $\phi(x) \in \mathbb{Z}[x]$ with $\overline{\phi(x)} \in \mathbb{F}_p[x]$ irreducible. Thus, $\mathfrak{m}^2 = \big(p^2, p\phi(x), \phi(x)^2\big)$. We can rephrase Uchida's criterion to require that $f(x) \neq \phi(x)^2 g(x) + p\phi(x)h(x) + p^2 j(x)$ for any p and $\phi(x)$ as above and any $g(x), h(x), j(x) \in \mathbb{Z}[x]$.

Remark 2.2 Uchida's criterion is generally amicable toward localization. Indeed, let F be the field of fractions of a Dedekind domain R. We will be most interested in the case where F is a number field and $R = \mathcal{O}_F$, or R is $\mathcal{O}_F$ localized at a prime ideal. Let α be integral and algebraic over R. If $\mathfrak{p}$ is a prime ideal of R, write $R_\mathfrak{p}$ to indicate R localized at $\mathfrak{p}$. (By *localized*, we mean that we adjoin the inverse of every element not in $\mathfrak{p}$.) As mentioned above, when R is $\mathcal{O}_F$, then we will simply write $\mathcal{O}_\mathfrak{p}$. Let S be

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

the integral closure of $R[\alpha]$. We say that $R[\alpha]$ is $\mathfrak{p}$-*maximal* if $R[\alpha] \otimes_R R_\mathfrak{p} = S \otimes_R R_\mathfrak{p}$. Uchida [Uch77, Lemma] proves that if $\mathfrak{m}$ is a maximal ideal of $R[x]$ and $\mathfrak{m}$ contains an integral polynomial, then $\mathfrak{m}$ is of the form $\big(\mathfrak{p}, \phi(x)\big)$ for some maximal ideal $\mathfrak{p}$ of R and some $\phi(x) \in R[x]$ that is irreducible modulo $\mathfrak{p}$. Let $f(x)$ be the minimal polynomial of α over R, (or, equivalently, over $R_\mathfrak{p}$), and let $\pi_\mathfrak{p}$ be a generator of $\mathfrak{p}$ in $R_\mathfrak{p}$. Now, $R[\alpha]$ is $\mathfrak{p}$-maximal if and only if $f(x)$ is not contained in the square of any maximal ideal of $R_\mathfrak{p}[x]$. That is, if and only if $f(x) \notin \big(\pi_\mathfrak{p}, \phi(x)\big)^2$ for any lift $\phi(x) \in R_\mathfrak{p}[x]$ of an irreducible in $R/\mathfrak{p}[x]$. Expanding, we see that $f(x)$ is $\mathfrak{p}$-*maximal* if and only if for each $\phi(x)$ as above $f(x) \neq \phi(x)^2 g(x) + \pi_\mathfrak{p}\phi(x)h(x) + \pi_\mathfrak{p}^2 j(x)$ for any $g(x), h(x), j(x) \in R_\mathfrak{p}[x]$.

From Uchida's criterion, we see that $\mathfrak{p}$-maximality only depends on the mod- $\mathfrak{p}^2$ residue of a monic polynomial $f(x) \in R_\mathfrak{p}[x]$. Indeed, if $f_1(x)$ and $f_2(x)$ are two monic irreducible polynomials in $R_\mathfrak{p}[x]$ such that $f_1(x) \equiv f_2(x) \mod \pi_\mathfrak{p}^2$, then $f_1(x)$ is $\mathfrak{p}$-maximal if and only if $f_2(x)$ is $\mathfrak{p}$-maximal.

Let $k_\mathfrak{p}$ be the residue field of R at $\mathfrak{p}$. Since $f(x)$ and $f'(x)$ share a factor $\phi(x)$ if and only if $\phi(x)$ is a repeated factor of $f(x)$, we have the following restatement of Uchida's criterion.

Theorem 2.3 (Restatement of Uchida's criterion) *Let $f(x) \in R[x]$ be an irreducible polynomial with leading coefficient a unit, and let α be a root.*

If $f'(x) \not\equiv 0 \mod \mathfrak{p}$, then the ring $R[\alpha]$ is $\mathfrak{p}$-maximal if and only if for every factor $\overline{\phi(x)}$ of $f'(x)$ in $k_\mathfrak{p}[x]$ and any lift $\phi(x) \in R_\mathfrak{p}[x]$, one has $\phi(x) \nmid f(x)$ in $R_\mathfrak{p}/\pi_\mathfrak{p}^2[x]$.

If $f'(x) \equiv 0 \mod \mathfrak{p}$, then $R[\alpha]$ is $\mathfrak{p}$-maximal if and only if for every factor $\overline{\phi(x)}$ of $f(x)$ in $k_\mathfrak{p}[x]$ and any lift $\phi(x) \in R_\mathfrak{p}[x]$, one has $\phi(x) \nmid f(x)$ in $R_\mathfrak{p}/\pi_\mathfrak{p}^2[x]$.

Remark 2.4 Letting $R = \mathbb{Z}$ for the sake of being explicit, note that we cannot simply require that $f(x)$ and $f'(x)$ do not share a factor in $\mathbb{Z}/p^2\mathbb{Z}[x]$. If $f(x) = \phi(x)^2 g(x) + p\phi(x)h(x) + p^2 j(x)$, then we compute that

$$f'(x) = 2\phi(x)\phi'(x)g(x) + \phi(x)^2 g'(x) + p\phi'(x)h(x) + p\phi(x)h'(x) + p^2 j'(x).$$

We see that the term $p\phi'(x)h(x)$ may prevent $f'(x)$ and $f(x)$ from sharing $\phi(x)$ as a factor modulo p^2.

We will focus on the case where R is the ring of integers $\mathcal{O}_K$ or $\mathcal{O}_\mathfrak{p}$, the localization of $\mathcal{O}_K$ at a prime ideal $\mathfrak{p}$. From Remark 2.2, we see that, in investigating the $\mathfrak{p}$-maximality of $\mathcal{O}_K[\alpha]$, it is equivalent to work in $\mathcal{O}_\mathfrak{p}[\alpha]$. In what follows, our exposition centers on $\mathcal{O}_K$, though the equivalent statements hold for $\mathcal{O}_\mathfrak{p}$. We will use this in later sections when we consider the $\mathfrak{p}$-maximality of polynomials that are $\mathcal{O}_\mathfrak{p}$-integral but not $\mathcal{O}_K$-integral.

Note that $f'(x) \equiv 0 \mod \mathfrak{p}$ if and only if $f(x) = g(x)^p \mod \mathfrak{p}$, where p is the characteristic of $k_\mathfrak{p}$ and $g(x)$ is a polynomial in $k_\mathfrak{p}[x]$. As we can see, every element of $\overline{k_\mathfrak{p}}$ is a critical point and every root of $f(x)$ is a multiple root.

Definition 2.5 We call a prime $\mathfrak{p}$ such that $f'(x) \equiv 0 \mod \mathfrak{p}$ a *vanishing prime* for $f(x)$. If $f'(x) \not\equiv 0 \mod \mathfrak{p}$, then we say that $\mathfrak{p}$ is a *non-vanishing prime*.

With Theorem 2.3, the following lemma relates $\mathfrak{p}$-maximality to lifts of factors of $f'(x)$ modulo $\mathfrak{p}$, hence to lifts of the critical points of $f(x)$ in $\overline{k_\mathfrak{p}}$.

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

Lemma 2.6 (Factors, critical lifts, and valuations) *Suppose* $f'(x) \not\equiv 0 \bmod \mathfrak{p}$, *and write* $f'(x) \equiv \prod_{i=1}^{r} \phi_i(x)^{e_i} \bmod \mathfrak{p}$ *for a factorization of* $f'(x)$ *into irreducibles in* $k_\mathfrak{p}[x]$, *where we have chosen lifts* $\phi_i(x)$ *of each irreducible factor to* $\mathcal{O}_K[x]$. *Let* J *be an extension of* K *where each* $\phi_i(x)$ *splits completely, and let* $\mathfrak{P}$ *be a prime of* $\mathcal{O}_J$ *above* $\mathfrak{p}$. *Then both of the following hold:*

a) *If* $\theta \in J$ *fulfills* $v_\mathfrak{P}(\phi(\theta)) \geq e(\mathfrak{P} \mid \mathfrak{p})$[3] *for a lift* $\phi(x)$ *of some irreducible factor of* $f'(x)$ *in* $k_\mathfrak{p}[x]$ *and* $v_\mathfrak{P}\big(f(\theta)\big) > e(\mathfrak{P} \mid \mathfrak{p})$, *then* $\phi(x)$ *divides* $f(x)$ *in* $\mathcal{O}_K/\mathfrak{p}^2[x]$.
b) *If conversely a lift* $\phi(x)$ *of an irreducible factor of* $f'(x)$ *in* $k_\mathfrak{p}[x]$ *divides* $f(x)$ *in* $\mathcal{O}_K/\mathfrak{p}^2[x]$, *then* $v_\mathfrak{P}\big(f(\theta)\big) > e(\mathfrak{P} \mid \mathfrak{p})$ *for every* $\theta \in J$ *such that* $v_\mathfrak{P}\big(\phi(\theta)\big) \geq e(\mathfrak{P} \mid \mathfrak{p})$.

Proof Let $\theta \in J$ be such that $v_\mathfrak{P}\big(\phi(\theta)\big) \geq e(\mathfrak{P} \mid \mathfrak{p})$ and $v_\mathfrak{P}\big(f(\theta)\big) > e(\mathfrak{P} \mid \mathfrak{p})$. We see that $\phi(\theta), f(\theta) \equiv 0 \bmod \mathfrak{P}$. Since $k_\mathfrak{P} = \mathcal{O}_J/\mathfrak{P}$ is an extension of $k_\mathfrak{p}$, we see that $\gcd\big(f(x), \phi(x)\big) \neq 1$ in $k_\mathfrak{p}[x]$. Since $\phi(x)$ is irreducible in $k_\mathfrak{p}[x]$, we note that $\phi(x)$ divides $f(x)$ in $k_\mathfrak{p}[x]$. However, since $\phi(x)$ also divides $f'(x)$ in $k_\mathfrak{p}[x]$, we see that $\phi(x)^2$ divides $f(x)$ in $k_\mathfrak{p}[x]$. Thus, we can write $f(x) = \phi(x)^2 g(x) + bh(x)$ in $\mathcal{O}_K[x]$ for some $b \in \mathfrak{p}$ and some $h(x) \in \mathcal{O}_K[x]$. We evaluate at θ to obtain $f(\theta) = \phi(\theta)^2 g(\theta) + bh(\theta)$. Noting $v_\mathfrak{P}\big(\phi(\theta)^2 g(\theta)\big) \geq 2e(\mathfrak{P} \mid \mathfrak{p})$, we find $v_\mathfrak{P}\big(bh(\theta)\big) > e(\mathfrak{P} \mid \mathfrak{p})$. Thus, either $b \in \mathfrak{p}^2$ or $v_\mathfrak{P}\big(h(\theta)\big) > 0$. In the former case, our desired result is clear. In the latter case, we note that $\gcd\big(h(x), \phi(x)\big) \neq 1$ in $k_\mathfrak{P}[x]$ and hence in $k_\mathfrak{p}[x]$ as above. Thus, $h(x) = \phi(x)j(x) + c\ell(x)$ with $c \in \mathfrak{p}\mathcal{O}_K$. Therefore,

$$f(x) = \phi(x)^2 g(x) + bh(x) = \phi(x)^2 g(x) + b\big(\phi(x)j(x) + c\ell(x)\big),$$

and we have a).

Suppose conversely that $\phi(x)$ divides $f(x)$ in $\mathcal{O}_K/\mathfrak{p}^2[x]$. Since $\phi(x)$ is a factor of $f'(x)$ modulo $\mathfrak{p}$, we have $f(x) = \phi(x)^2 g(x) + b\phi(x)h(x) + cj(x)$, where $b \in \mathfrak{p}$ and $c \in \mathfrak{p}^2$. Evaluating at any θ such that $v_\mathfrak{P}\big(\phi(\theta)\big) \geq e(\mathfrak{P} \mid \mathfrak{p})$, we see that $v_\mathfrak{P}\big(f(\theta)\big) \geq 2e(\mathfrak{P} \mid \mathfrak{p})$, yielding b). ∎

When $\mathfrak{p}$ is a vanishing prime, we have $f(x) \equiv g(x)^p \bmod \mathfrak{p}$ for some $g(x) \in \mathcal{O}_K[x]$. The next lemma connects roots of $g(x)$ to factors of $f(x)$.

Lemma 2.7 (Vanishing primes and roots) *Let* $\mathfrak{p}$ *be a vanishing prime of residue characteristic* p, *so* $f(x) \equiv g(x)^p \bmod \mathfrak{p}$ *for some* $g(x) \in \mathcal{O}_K[x]$. *Let* L *be an extension of* K, *where* $g(x)$ *splits, and let* $\mathfrak{P}$ *be a prime of* L *above* $\mathfrak{p}$. *Then there is a lift* $\phi(x)$ *of a repeated irreducible factor of* $f(x)$ *in* $k_\mathfrak{p}[x]$ *that divides* $f(x)$ *in* $\mathcal{O}_K/\mathfrak{p}^2[x]$ *if and only if* $v_\mathfrak{P}\big(f(\tau)\big) > e(\mathfrak{P} \mid \mathfrak{p})$, *where* $\tau \in \mathcal{O}_L$ *is a root of* $g(x)$.

Proof Since $\phi(x)$ is irreducible in $k_\mathfrak{p}[x]$ and since $f(x) \equiv g(x)^p \bmod \mathfrak{p}$, we see that $\phi(x)$ divides $g(x)$ in $k_\mathfrak{p}[x]$. Thus, we can write $g(x) \equiv \phi(x)^m r(x) \bmod \mathfrak{p}$ with $\gcd\big(\phi(x), r(x)\big) = 1$ in $k_\mathfrak{p}[x]$. Since $g(x)$ splits in L, we see that there is an algebraic integer τ that is a root of $g(x)$ and such that $\phi(\tau) \equiv 0 \bmod \mathfrak{P}$. We have $0 = g(\tau) \equiv \phi(\tau)^m r(\tau) \bmod \mathfrak{p}\mathcal{O}_L$. Since $\gcd\big(\phi(x), r(x)\big) = 1$ and since $v_\mathfrak{P}\big(\phi(\tau)\big) > 0$, we see $v_\mathfrak{P}\big(r(\tau)\big) = 0$ and $v_\mathfrak{P}\big(\phi(\tau)^m\big) \geq e(\mathfrak{P} \mid \mathfrak{p})$.

[3] For example, but not necessarily, $\phi(\theta) = 0$.

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

Since $\phi(x)$ divides $f(x)$ modulo $\mathfrak{p}^2$ and since $f(x) \equiv g(x)^p \bmod \mathfrak{p}$, we have $f(x) = \big(\phi(x)^m r(x)\big)^p + bh(x)$ with $b \in \mathfrak{p}$ and either $b \in \mathfrak{p}^2$ or $\phi(x)$ dividing $h(x)$ modulo $\mathfrak{p}$. Evaluating at τ and noting $v_{\mathfrak{P}}\big(\phi(\tau)^m\big) \geq e(\mathfrak{P} \mid \mathfrak{p})$, we have our desired result.

For the converse, let $\tau \in L$ be a root of $g(x)$ such that $v_{\mathfrak{P}}\big(f(\tau)\big) > e(\mathfrak{P} \mid \mathfrak{p})$. Let $\phi(x)$ be an irreducible factor of $g(x)$ in $\mathcal{O}_K[x]$ such that $\phi(\tau) \equiv 0 \bmod \mathfrak{P}$. (Note that we can assume that the number of irreducible factors of $g(x)$ in $k_{\mathfrak{p}}[x]$ is equal to that in $\mathcal{O}_K[x]$.)

By hypothesis, $f(x) = g(x)^p + bh(x)$ with $b \in \mathfrak{p}$ and $h(x) \in \mathcal{O}_K[x]$. Evaluating at τ, we see that $v_{\mathfrak{P}}\big(bh(\tau)\big) > e(\mathfrak{P} \mid \mathfrak{p})$. Thus, either $b \in \mathfrak{p}^2$ or $\gcd\big(\phi(x), h(x)\big) > 1$ in $k_{\mathfrak{p}}[x]$. In either case, we have our result. ∎

The lemmas above yield a rephrasing of Uchida's criterion in terms of lifts of factors of $f'(x) \bmod \mathfrak{p}$.

Theorem 2.8 (Uchida's critical lift criterion) *Let $f(x) \in \mathcal{O}_K[x]$ be an irreducible polynomial with leading coefficient a unit, and let α be a root. For $\mathfrak{p} \subset \mathcal{O}_K$ a non-vanishing prime ($f'(x) \not\equiv 0 \bmod \mathfrak{p}$), write $f'(x) \equiv \prod_{i=1}^{r} \phi_i(x)^{e_i} \bmod \mathfrak{p}$ for a factorization of $f'(x)$ into irreducibles in $k_{\mathfrak{p}}[x]$, where we have chosen lifts $\phi_i(x)$ of each irreducible factor to $\mathcal{O}_K[x]$. Let J be an extension of K, where each $\phi_i(x)$ splits completely, and let $\mathfrak{P}$ be a prime of $\mathcal{O}_J$ above $\mathfrak{p}$. Then $\mathcal{O}_K[\alpha]$ is $\mathfrak{p}$-maximal if and only if for each i, one has $v_{\mathfrak{P}}\big(f(\theta_i)\big) \leq e(\mathfrak{P} \mid \mathfrak{p})$, where θ_i is an arbitrary element of J such that $v_{\mathfrak{P}}\big(\phi_i(\theta_i)\big) \geq e(\mathfrak{P} \mid \mathfrak{p})$.*

If $\mathfrak{p}$ is a vanishing prime, then we can write $f(x) \equiv g(x)^p \bmod \mathfrak{p}$ for some $g(x) \in \mathcal{O}_K[x]$. Let L be an extension of K, where $g(x)$ splits, and let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ above $\mathfrak{p}$. In this case, the ring $\mathcal{O}_K[\alpha]$ is $\mathfrak{p}$-maximal if and only if for each $\tau \in \mathcal{O}_L$ such that $g(\tau) = 0$, one has $v_{\mathfrak{P}}\big(f(\tau)\big) \leq e(\mathfrak{P} \mid \mathfrak{p})$.

Proof Combining Lemmas 2.6 and 2.7 with Theorem 2.3, we have the result. ∎

We now proceed to considering monogenicity of not just one fixed polynomial $f(x)$ but of all iterates $f^n(x) - a$, $n \in \mathbb{N}$ simultaneously (for a fixed $a \in \mathcal{O}_K$). The following is the first version of our main criterion.

Theorem 2.9 (The critical lift criteria for monogenicity) *Let K be a number field. Fix $N > 0$. Suppose $f(x) \in \mathcal{O}_K[x]$ has a leading coefficient that is a unit, and let $a \in \mathcal{O}_K$ be such that $f^n(x) - a$ is irreducible over K for $1 \leq n \leq N$.*

1. *If $\mathfrak{p}$ is not a vanishing prime (i.e., $f'(x) \not\equiv 0 \bmod \mathfrak{p}$), then we may write $f'(x) \equiv \prod_{i=1}^{r} \phi_i(x)^{e_i} \bmod \mathfrak{p}$, where each $\phi_i(x)$ is a lift of a distinct irreducible factor of $f'(x)$ in $k_{\mathfrak{p}}[x]$ to $\mathcal{O}_K[x]$. Let J be an extension of K, where each $\phi_i(x)$ splits and let $\mathfrak{P}$ be a prime of J above $\mathfrak{p}$. Then the polynomial $f^n(x) - a$ is $\mathfrak{p}$-maximal for each $1 \leq n \leq N$ if and only if for each θ in J that is a root of some $\phi_i(x)$, one has $v_{\mathfrak{P}}\big(f^n(\theta) - a\big) \leq e(\mathfrak{P} \mid \mathfrak{p})$ for each $1 \leq n \leq N$.*
2. *If $\mathfrak{p}$ is a vanishing prime (i.e., $f'(x) \equiv 0 \bmod \mathfrak{p}$), then we have $f(x) - a \equiv g(x)^p \bmod \mathfrak{p}$ for some $g(x) \in \mathcal{O}_K[x]$. Let L be an extension of K, where $g(x)$ splits. Let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ above $\mathfrak{p}$ with ramification index $e(\mathfrak{P} \mid \mathfrak{p})$. The polynomial $f^n(x) - a$ is $\mathfrak{p}$-maximal for all $1 \leq n \leq N$ if and only if for every root τ of $g(x)$ in $\mathcal{O}_L$, one has $v_{\mathfrak{P}}\big(f(\tau) - a\big) \leq e(\mathfrak{P} \mid \mathfrak{p})$.*

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

Proof First, we focus on the non-vanishing primes. Let $\mathfrak{p} \subset \mathcal{O}_K$ be such a prime. Though there is a natural proof via induction, we proceed directly. Note Lemma 2.6 and our hypothesis immediately imply that no $\phi_i(x)$ divides $f^n(x) - a$ in $\mathcal{O}_K/\mathfrak{p}^2[x]$ for any $1 \le n \le N$. Fix an n in the range $1 \le n \le N$. We wish to show that $f^n(x) - a$ is $\mathfrak{p}$-maximal. We have

$$\frac{d}{dx}\left(f^n(x) - a\right) = f'\left(f^{n-1}(x)\right)\ldots f'(x) \equiv \prod_{j=1}^{s} \gamma_j(x)^{m_j} \bmod \mathfrak{p}, \tag{2.1}$$

where the $\gamma_j(x)$ are lifts of the irreducible factors of $\frac{d}{dx}\left(f^n(x) - a\right)$ in $k_\mathfrak{p}[x]$ to $\mathcal{O}_K[x]$. Let J' be an extension of J where all the $\gamma_j(x)$ split, and let $\mathcal{P}$ be a prime of J' above $\mathfrak{P}$.

For a contradiction, suppose $f^n(x) - a$ is not $\mathfrak{p}$-maximal. Thus, Theorem 2.8 shows that there is some $\tau \in J'$ and some $\gamma_j(x) \in \mathcal{O}_K[x]$ such that $v_\mathcal{P}\left(\gamma_j(\tau)\right) \ge e(\mathcal{P} \mid \mathfrak{p})$ and $v_\mathcal{P}\left(f^n(\tau) - a\right) > e(\mathcal{P} \mid \mathfrak{p})$. Since $\gamma_j(x)$ is irreducible in $k_\mathfrak{p}[x]$, we see that $\gamma_j(x)$ divides $f'\left(f^t(x)\right)$ in $k_\mathfrak{p}[x]$ for some $0 \le t \le n-1$. Hence, $\gamma_j(x)$ divides $\phi_i\left(f^t(x)\right)$ in $k_\mathfrak{p}[x]$ for some i. Since $v_\mathcal{P}\left(\gamma_j(\tau)\right) \ge e(\mathcal{P} \mid \mathfrak{p})$, we have $v_\mathcal{P}\left(\phi_i\left(f^t(\tau)\right)\right) \ge e(\mathcal{P} \mid \mathfrak{p})$. As

$$v_\mathcal{P}\left(f^n(\tau) - a\right) = v_\mathcal{P}\left(f^{n-t}\left(f^t(\tau)\right) - a\right) > e(\mathcal{P} \mid \mathfrak{p}),$$

Lemma 2.6 shows that $\phi_i(x)$ divides $f^{n-t}(x) - a$ in $\mathcal{O}_K/\mathfrak{p}^2[x]$, yielding the desired contradiction. We have established Condition 1.

Now we turn to the vanishing primes. Suppose $f'(x) \equiv 0 \bmod \mathfrak{p}$, so $f(x) - a \equiv g(x)^p \bmod \mathfrak{p}$ for some $g(x) \in \mathcal{O}_K[x]$. Let L and $\mathfrak{P}$ be as in the theorem statement. For the monogenicity of $f^n(x) - a$, Theorem 2.8 shows that it is necessary that $v_\mathfrak{P}\left(f(\tau) - a\right) \le e(\mathfrak{P} \mid \mathfrak{p})$ for each root τ of $g(x)$. Suppose this is the case and consider $f^n(x) - a$ with $1 \le n \le N$. Since $f'(x) \equiv 0 \bmod \mathfrak{p}$, we compute

$$\frac{d}{dx}\left(f^n(x) - a\right) = f'\left(f^{n-1}(x)\right)f'\left(f^{n-2}(x)\right)\ldots f'(x) \equiv 0 \bmod \mathfrak{p}.$$

Thus, $\mathfrak{p}$ is a vanishing prime for $f^n(x) - a$, and $f^n(x) - a \equiv g\left(f^{n-1}(x)\right)^p \bmod \mathfrak{p}$. Let L' be an extension of L, where $g\left(f^{n-1}(x)\right)$ splits completely and let $\mathcal{P}$ be a prime of L' above $\mathfrak{P}$. Theorem 2.8 shows that $f^n(x) - a$ is $\mathfrak{p}$-maximal if and only if for any $\tau' \in L'$ that is a root of $g\left(f^{n-1}(x)\right)$, one has $v_\mathcal{P}\left(f^n(\tau') - a\right) \le e(\mathcal{P} \mid \mathfrak{p})$. For a contradiction, suppose τ' is a root of $g\left(f^{n-1}(x)\right)$ in L' with $v_\mathcal{P}\left(f^n(\tau') - a\right) > e(\mathcal{P} \mid \mathfrak{p})$. Now $f^{n-1}(\tau')$ is a root of $g(x)$ in L. We have $v_\mathcal{P}\left(f^n(\tau') - a\right) = e(\mathcal{P} \mid \mathfrak{P})v_\mathfrak{P}\left(f\left(f^{n-1}(\tau')\right) - a\right)$ and $e(\mathcal{P} \mid \mathfrak{p}) = e(\mathcal{P} \mid \mathfrak{P})e(\mathfrak{P} \mid \mathfrak{p})$, so $v_\mathfrak{P}\left(f\left(f^{n-1}(\tau')\right) - a\right) > e(\mathfrak{P} \mid \mathfrak{p})$. This is a contradiction. We conclude that $v_\mathcal{P}\left(f^n(\tau') - a\right) \le e(\mathcal{P} \mid \mathfrak{p})$ and $f^n(x) - a$ is $\mathfrak{p}$-maximal for all $1 \le n \le N$. ∎

Remark 2.10 Note that irreducibility is not necessarily automatic from Conditions 1 and 2 of Theorem 2.9. Hence, in general, the assumption of irreducibility cannot be dropped. An example is $f(x) = (x^2 - 2)(x^2 - 3)$, with $K = \mathbb{Q}$, $a = 0$, $N = 1$. The mod 2 roots 0 and 1 evaluate to 2 mod 4. Hence, Condition 2 holds for the only vanishing prime 2. Moreover, $f'(x) = 2x(2x^2 - 5)$, yielding the critical values are 6 and $-1/4$. These have squarefree numerators, meaning that Condition 1 holds for all non-vanishing primes.

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

Remark 2.11 Since for arithmetic dynamics applications, we intend to use results such as Theorem 2.9 for all $n \in \mathbb{N}$ simultaneously, it is worth noting the following: for any fixed prime $\mathfrak{p}$ of $\mathcal{O}_K$, assumed to be non-vanishing for $f(x)$, there exists a bound $N_\mathfrak{p} \in \mathbb{N}$ such that Condition 1 of Theorem 2.9 holds for all $n \in \mathbb{N}$ as soon as it holds for all $n \leq N_\mathfrak{p}$. Indeed, since the field generated by all roots of $f'(x) \bmod \mathfrak{p}$ is a finite extension of $k_\mathfrak{p}$ of degree less than $\deg(f)$, the sequence $\{f^n(\tau) \mid n \in \mathbb{N}\}$ is preperiodic modulo $\mathfrak{P}^{e+1}$ with $\mathfrak{P}$ as in Condition 1 and $e := e(\mathfrak{P} \mid \mathfrak{p})$. But, as soon as $f^n(\tau) \equiv f^m(\tau) \bmod \mathfrak{P}^{e+1}$, then the properties $v_\mathfrak{P}(f^n(\tau) - a) \leq e$ and $v_\mathfrak{P}(f^m(\tau) - a) \leq e$ are equivalent.

While Theorem 2.9 is already helpful for studying the monogenicity of polynomials and their iterates, the dependence of irreducible factors $\gamma_j(x)$ on the respective prime $\mathfrak{p}$ is not ideal. Instead, we hope to work with the roots of $f'(x)$ in $\overline{K}$ (i.e., the critical points of $f(x)$) independent of $\mathfrak{p}$. The following lemma is useful in determining when this can be achieved. We employ the following notation: If $g(x)$ and $\phi(x)$ are polynomials with images in $k_\mathfrak{p}[x]$, then we write $v_{\phi,\mathfrak{p}}\big(g(x)\big)$ for the multiplicity to which $\phi(x)$ divides $g(x)$ in $k_\mathfrak{p}[x]$.

Lemma 2.12 (Factors, critical points, and valuations) *Let $h(x)$ be an irreducible factor of $f'(x)$ in $K[x]$. Suppose $\phi(x)$ is a lift of an irreducible factor of $h(x)$ in $k_\mathfrak{p}[x]$ to $\mathcal{O}_K[x]$, and suppose either $v_{\phi,\mathfrak{p}}\big(f(x)\big) = 0$ or $v_{\phi,\mathfrak{p}}\big(f(x)\big) > v_{\phi,\mathfrak{p}}\big(h(x)\big)$. Let M be an extension of K, where $f'(x)$ splits completely, and let $\mathfrak{P}$ be a prime of $\mathcal{O}_M$ above $\mathfrak{p}$. Then $\phi(x)$ divides $f(x)$ in $\mathcal{O}_K/\mathfrak{p}^2[x]$ if and only if $v_\mathfrak{P}\big(f(\theta)\big) > e(\mathfrak{P} \mid \mathfrak{p})$ for some θ in M that is a root of $h(x)$ such that $\phi(\theta) \equiv 0 \bmod \mathfrak{P}$. In particular, if all the irreducible factors of $f'(x)$ in $K[x]$ satisfy the multiplicity hypothesis above, then $f(x)$ is $\mathfrak{p}$-maximal if and only if $v_\mathfrak{P}\big(f(\theta)\big) \leq e(\mathfrak{P} \mid \mathfrak{p})$ for each critical point $\theta \in M$.*

Proof For ease of notation, let $k = v_{\phi,\mathfrak{p}}\big(h(x)\big)$ and $m = v_{\phi,\mathfrak{p}}\big(f(x)\big)$. If $v_{\phi,\mathfrak{p}}\big(f(x)\big) = 0$, then the result is clear, so suppose $\phi(x)$ divides $f(x)$ in $\mathcal{O}_K/\mathfrak{p}^2[x]$. Let θ in M be a critical point such that $\phi(\theta) \equiv 0 \bmod \mathfrak{P}$. We have $h(x) = \phi(x)^k r(x) + d$ for some $r(x) \in \mathcal{O}_K[x]$ that is relatively prime to $\phi(x)$ in $k_\mathfrak{p}[x]$ and some $d \in \mathfrak{p}\mathcal{O}_K[x]$. Since $h(\theta) = 0$, we see that $v_\mathfrak{P}\big(\phi(\theta)^k\big) \geq e(\mathfrak{P} \mid \mathfrak{p})$. We can write $f(x) = \phi(x)^m g(x) + b\phi(x) + c$ with $b \in \mathfrak{p}\mathcal{O}_K[x]$ and $c \in \mathfrak{p}^2\mathcal{O}_K[x]$. Since $m > k$, we evaluate at θ to obtain $v_\mathfrak{P}\big(f(\theta)\big) > e(\mathfrak{P} \mid \mathfrak{p})$.

Conversely, suppose $v_\mathfrak{P}\big(f(\theta)\big) > e(\mathfrak{P} \mid \mathfrak{p})$ for some critical point θ in M such that $\phi(\theta) \equiv 0 \bmod \mathfrak{P}$. We have $h(x) = \phi(x)^k r(x) + d$ for some $r(x) \in \mathcal{O}_K[x]$ that is relatively prime to $\phi(x)$ in $k_\mathfrak{p}[x]$ and some $d \in \mathfrak{p}\mathcal{O}_K[x]$. Since $h(\theta) = 0$, we see that $v_\mathfrak{P}\big(\phi(\theta)^k\big) \geq e(\mathfrak{P} \mid \mathfrak{p})$. We write $f(x) = \phi(x)^m g(x) + bj(x) + c$ with $b \in \mathfrak{p}$ and $c \in \mathfrak{p}^2\mathcal{O}_K[x]$. Since $v_\mathfrak{P}\big(\phi(\theta)^m g(\theta)\big) > e(\mathfrak{P} \mid \mathfrak{p})$ and $v_\mathfrak{P}\big(f(\theta)\big) > e(\mathfrak{P} \mid \mathfrak{p})$, we see $v_\mathfrak{P}\big(bj(\theta)\big) > e(\mathfrak{P} \mid \mathfrak{p})$. By a now familiar argument, $\phi(x)$ divides $f(x)$ in $\mathcal{O}_K/\mathfrak{p}^2[x]$.

The last statement is obtained by applying Theorem 2.3 and noting that any repeated factor of $f(x)$ in $k_\mathfrak{p}[x]$ will be a factor of $f'(x)$ in $k_\mathfrak{p}[x]$. ∎

As we will see in Theorem 2.15, the conclusion of Theorem 2.9 for a non-vanishing prime $\mathfrak{p}$ remains valid if we replace the roots of the lifts $\prod_{i=1}^r \phi_i(x)^{e_i} \equiv f'(x) \bmod \mathfrak{p}$ by the global roots of $f'(x)$ itself as soon as the following condition holds.

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

Condition 2.13 *For every irreducible factor $h(x)$ of $f'(x)$ in $K[x]$, every irreducible factor $\phi(x)$ of $h(x)$ in $k_\mathfrak{p}[x]$, and every $n \in \mathbb{N}$ such that $v_{\phi(x)}(f^n(x) - a) > 0$, we have $v_{\phi(x)}(f^n(x) - a) > v_{\phi(x)}(h(x))$.*

Let us call a prime $\mathfrak{p}$ of $\mathcal{O}_K$ a *non-exceptional* prime for $(f(x), a)$, if $f'(x) \not\equiv 0 \bmod \mathfrak{p}$ and furthermore Condition 2.13 holds for the given $(f(x), a)$. If this condition holds for all $a \in \mathcal{O}_K$, we call $\mathfrak{p}$ a non-exceptional prime for $f(x)$. Naturally, we call $\mathfrak{p}$ *exceptional*, for $(f(x), a)$ or $f(x)$, if these conditions do not hold.

We collect some important observations facilitating the verification of non-exceptionality in important cases.

Lemma 2.14 *Let $\mathfrak{p}$ be a prime of K with residue characteristic p. Then the following hold:*

a) *If the cover $\mathbb{P}^1_{\overline{\mathbb{F}_p}} \to \mathbb{P}^1_{\overline{\mathbb{F}_p}}$ given by $x \mapsto f(x)$ is tamely ramified, then p is non-exceptional for $f(x)$. In particular, this holds whenever $p > \deg(f)$.*
b) *If every irreducible factor of $f'(x)$ is separable modulo $\mathfrak{p}$, then $\mathfrak{p}$ is non-exceptional for $f(x)$.*

Proof To show a), it suffices to prove that $f^n(x) - a$ has no repeated factors of multiplicity divisible by p in $k_\mathfrak{p}[x]$ for any $n \in \mathbb{N}$, since indeed then the multiplicity of any irreducible factor decreases strictly in $\frac{d}{dx}(f^n(x))$ and thus a fortiori in $f'(x)$. Since the ramification index of a place $x \mapsto \alpha \in \overline{\mathbb{F}_p}$ under the cover $x \mapsto f(x)$ is simply the multiplicity of $x - \alpha$ in $f(x) - f(\alpha)$, tame ramification translates to saying that $f(x) - a$ has no root of multiplicity divisible by p for any $a \in \overline{\mathbb{F}_p}$. This shows the claim for $n = 1$. For arbitrary n, the claim simply follows by multiplicativity of ramification indices under composition of covers.

b) follows from the definition: Let $h(x)$ be an irreducible factor of $f'(x)$ in $K[x]$. A simple factor of $h(x)$ that is a common factor of $f'(x)$ and $f^n(x) - a$ must necessarily be a repeated factor of $f^n(x) - a$. ∎

The definition of non-exceptionality implies the following simplification of Theorem 2.9 for non-exceptional primes.

Theorem 2.15 (The critical point criterion for non-exceptional primes) *Let K be a number field. Fix $N > 0$. Suppose $f(x) \in \mathcal{O}_K[x]$ has a leading coefficient that is a unit, and let $a \in \mathcal{O}_K$ be such that $f^n(x) - a$ is irreducible over K for $1 \le n \le N$. Let M be an extension of K, where $f'(x)$ splits. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$, which is non-exceptional for $(f(x), a)$, and let $\mathfrak{P}$ be a prime of M above $\mathfrak{p}$. Then the polynomial $f^n(x) - a$ is $\mathfrak{p}$-maximal for each $1 \le n \le N$ if and only if for each $1 \le n \le N$ and each critical point $\theta \in M$, one has $v_\mathfrak{P}\left(f^n(\theta) - a\right) \le e(\mathfrak{P} \mid \mathfrak{p})$.*

Proof Let $1 \le n \le N$ and consider $\frac{d}{dx}\left(f^n(x) - a\right) = f'\left(f^{n-1}(x)\right) \dots f'(x)$.

Let M' be an extension of M, where $\frac{d}{dx}(f^n(x) - a)$ splits, and let $\mathcal{P}$ be a prime of M' above $\mathfrak{P}$. If $\tau \in M'$ is a critical point of $f^n(x) - a$, then τ is a root of $f'\left(f^t(x)\right)$ for some $0 \le t \le n - 1$. Thus, $f^t(\tau)$ is a root of $f'(x)$. From this and the multiplicative nature of valuations, we see $v_\mathcal{P}\left(f^n(\tau) - a\right) > e(\mathcal{P} \mid \mathfrak{p})$ for some τ that is a critical point of $f^n(x) - a$ if and only if $v_\mathfrak{P}\left(f^{n-t}(\theta) - a\right) > e(\mathfrak{P} \mid \mathfrak{p})$ for some $\theta = f^t(\tau)$ that is a critical

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

point of $f(x) - a$. Lemma 2.12 shows $v_{\mathcal{P}}\big(f^n(\tau) - a\big) > e(\mathcal{P} \mid \mathfrak{p})$ for some τ that is a critical point of $f^n(x) - a$ if and only if $f^n(x) - a$ is not $\mathfrak{p}$-maximal. ∎

Combining Theorem 2.15 together with Theorem 2.9 to deal with the finitely many exceptional primes yields a proof of Theorem 1.1.

Remark 2.16 Theorem 1.1 gives necessary and sufficient conditions for the iterates of any monic polynomial $f(x) \in \mathcal{O}_K[x]$ to be monogenic; however, even when a polynomial fails to be monogenic, the field generated by a root may be monogenic. For a simple example consider $f(x) = x^2$ and let $a \in \mathbb{Z}^{>1}$. We see that $f^n(x) + a^{2^n} = x^{2^n} + a^{2^n}$ is not monogenic. It fails to be p-maximal at all primes dividing a. However, $f^n(x) + a^{2^n}$ generates the same field as $x^{2^n} + 1$, and the 2-power cyclotomic fields are monogenic with monogenerator $\zeta_{2^{n+1}}$. Indeed, Theorem 2.15 gives a short proof: Each odd prime p is a non-exceptional prime, and $v_p(0 + 1) = 0$. The prime 2 is a vanishing prime, and $v_2(1^2 + 1) = 1$.

Remark 2.17 The assertion of Theorem 2.15 no longer holds for (non-vanishing) exceptional primes $\mathfrak{p}$. Indeed take Dedekind's example [Ded78]. Let $f(x) = x^3 - x^2 - 2x - 8 \in \mathbb{Z}[x]$, $a = 0$, and $p = 2$. We have $f'(x) \equiv x^2 \bmod 2$, and evaluating $v_2\big(f(0)\big) = v_2(-8) = 3 > 1$, we see from Theorem 2.9 that $f(x)$ is not 2-maximal. On the other hand, the global roots of $f'(x) = 3x^2 - 2x - 2$ are $\theta = \frac{1 \pm \sqrt{7}}{3}$. Choosing $\mathfrak{P}$ as the (unique, since ramified) prime extending 2 in $\mathbb{Q}(\sqrt{7})$, we get $v_{\mathfrak{P}}\big(f(\theta)\big) = v_{\mathfrak{P}}\big(\frac{1}{27}(\pm 14\sqrt{7} - 236)\big) = 2 = e(\mathfrak{P} \mid 2)$, showing that an attempted application of Theorem 2.15 with the global roots of $f'(x)$ would lead to an erroneous result.

For many of the examples we work with, we do not need the field extensions J/K and L/K in Theorem 2.9 or M/K in Theorem 2.15. The following corollary captures this simplified situation. Note that we will assume here and in similar scenarios in the following sections that all non-vanishing primes are non-exceptional, an assumption that will be fulfilled in all of our applications. This assumption is, however, only made for sake of simplicity. Without it, finitely many further K-rationality conditions would have to be added to accommodate the finitely many (by Remark 2.11) relevant values $n \in \mathbb{N}$ for the finitely many exceptional non-vanishing primes.

Corollary 2.18 *With the hypotheses as in Theorems 2.9 and 2.15, suppose that $f(x)$ has K-rational critical values, that is, $f(\theta) \in K$ for each critical point θ of $f(x)$. Suppose further that every exceptional prime for $f(x)$ is a vanishing prime. For each such prime $\mathfrak{p}$, write $f(x) - a \equiv g(x)^p \bmod \mathfrak{p}$, where $g(x) \in \mathcal{O}_K[x]$, and suppose that for each root τ of $g(x)$, it holds that $f(\tau) \in \mathcal{O}_K$. Then, $f^n(x) - a$ is monogenic for all $n \le N$ if and only if both of the following conditions hold:*

1. *(Non-vanishing primes) If $f'(x) \not\equiv 0 \bmod \mathfrak{p}$, then $v_{\mathfrak{p}}\big(f^n(\theta) - a\big) \le 1$ for each critical point θ and each $n \le N$.*
2. *(Vanishing primes) If $f'(x) \equiv 0 \bmod \mathfrak{p}$, then $v_{\mathfrak{p}}\big(f(\tau) - a\big) \le 1$ for each root τ of $g(x)$.*

Proof For the non-vanishing primes, we let M be an extension, where $f'(x)$ splits and let $\mathfrak{P}$ be a prime of M above $\mathfrak{p}$. Since $f(\theta) \in \mathcal{O}_K$ for each critical point θ, we have $v_{\mathfrak{P}}\big(f^n(\theta) - a\big) \le e(\mathfrak{P} \mid \mathfrak{p})$ if and only if $v_{\mathfrak{p}}\big(f^n(\theta) - a\big) \le 1$.

Condition 1 follows from Theorem 2.15.

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

For the vanishing primes, we let L be an extension, where $g(x)$ splits and let $\mathfrak{P}$ be a prime of L above $\mathfrak{p}$. Since $f(\tau) \in \mathcal{O}_K$ for each root τ of $g(x)$, we have $v_{\mathfrak{P}}\big(f(\tau) - a\big) \leq e(\mathfrak{P} \mid \mathfrak{p})$ if and only if $v_{\mathfrak{p}}\big(f(\tau) - a\big) \leq 1$. Condition 2 follows from Theorem 2.9. ∎

Definition 2.19 We say that a polynomial $f(x) \in \mathcal{O}_K[x]$ is *dynamically monogenic* if $f^n(x)$ is monogenic for each $n \geq 1$. More generally, we say that a pair $f(x) \in \mathcal{O}_K[x]$ and $a \in \mathcal{O}_K$ is a *dynamically monogenic pair* if $f^n(x) - a$ is a monogenic polynomial for each $n \geq 1$. For example, classical results show that for every prime p, the pair (x^p, ζ_p) is a dynamically monogenic pair over $\mathbb{Q}(\zeta_p)$. Note that some authors use the term *monogenically stable* (cf. [Jon21]).

In a related vein, we call a polynomial $f(x)$ (resp. a pair $(f(x), a)$) *dynamically irreducible* if $f^n(x)$ (resp. $f^n(x) - a$) is irreducible for all $n \geq 1$. This is also called *stability* in the literature. Notice that dynamical irreducibility is implied by dynamical monogenicity.

Remark 2.20 A polynomial is called PCF if the forward orbits of each of its critical points are finite. Theorem 1.1 points toward how dynamical monogenicity relates to PCF polynomials. Suppose all iterates of a monic PCF polynomial $f(x) \in \mathcal{O}_K[x]$ are irreducible. Then, there are only finitely many conditions to check in order to see whether $f(x)$ is dynamically monogenic, or whether $(f(x), a)$ is a dynamically monogenic pair.

Generally, if $f^n(x)$ is monogenic, then $f^k(x)$ is monogenic for all $k \leq n$. In fact, Proposition 3.4 of [SW24] shows that $f^n(x)$ is monogenic if and only if $f^k(x)$ is monogenic for all $k \leq n$. If $f(x)$ is PCF and dynamically irreducible, then let l be the maximum length of an orbit $\left\{f^k(\theta) : k \in \mathbb{Z}^{\geq 0}\right\}$, where θ runs through the critical points of $f(x)$.

Theorem 2.8 in conjunction with [SW24, Proposition 3.4] shows that if $f^l(x)$ is monogenic, then $f^n(x)$ is monogenic for all $n \geq 1$. Thus, if $f(x)$ is dynamically irreducible, then $f(x)$ is PCF if and only if there exists some $l \geq 1$ such that (from the perspective of Theorem 1.1) the conditions for the monogenicity of $f^l(x)$ imply the monogenicity of $f^n(x)$ for all $n \geq 1$.

On the other hand, if $f(x) \in \mathbb{Z}[x]$ is not PCF, then it is known that for any critical point θ with infinite forward orbit and any a which is not a postcritical point of $f(x)$, there are infinitely many primes $\mathfrak{p}$ with $v_{\mathfrak{p}}(f^n(\theta) - a) \geq 1$ for at least one $n \in \mathbb{N}$ (see, for example, [BIJ+15, Lemma 12] for a somewhat stronger assertion). In the context of Uchida's theorem, this means that the squarefreeness conditions of Corollary 2.18, which need to be verified in order to show monogenicity for all $n \in \mathbb{N}$ simultaneously, will necessarily involve infinitely many primes.

3 Results on dynamical irreducibility

The following is a statement on when and how often the conditions for dynamical monogenicity obtained in the previous section can be fulfilled. It asserts that, for a PCF polynomial fulfilling certain extra assumptions (notably concerning dynamical irreducibility and K-rationality of the critical values), the conditions can be fulfilled as long as there are no local obstructions.

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

Lemma 3.1 *Let $f(x) \in \mathcal{O}_K[x]$ be a PCF polynomial whose leading coefficient is a unit and all of whose critical values are K-rational.*

Let $\Omega \subset K$ be the (finite) union of forward orbits of the critical points of $f(x)$. Assume that $(f(x), a)$ is dynamically irreducible for all $a \in \mathcal{O}_K$ outside of a set of relative density zero (with respect to norm). Furthermore, assume that $f(x)$ has no non-vanishing exceptional primes. Then the following are equivalent:

1. *Both of the following hold:*
   - i. *(Non-vanishing primes) For every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ with $f'(x) \not\equiv 0 \bmod \mathfrak{p}$, there exists at least one residue class modulo $\mathfrak{p}^2$ containing no element of Ω.*[4]
   - ii. *(Vanishing primes) For every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ with $f'(x) \equiv 0 \bmod \mathfrak{p}$, there exists at least one value $a \in \mathcal{O}_K$ such that $f(x) - a$ is $\mathfrak{p}$-maximal. (See Corollary 2.18, Condition 2, for an equivalent condition.)*
2. *There exists a positive density subset (with respect to norm) of values $a \in \mathcal{O}_K$ such that $(f(x), a)$ is dynamically monogenic over K.*

Proof The implication 2 ⇒1 follows directly from Corollary 2.18, so we assume 1.

For every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, let $\Omega_\mathfrak{p}$ be the set of all mod-$\mathfrak{p}^2$ reductions of elements of Ω (excluding those for which the reduction is not defined). It follows by a standard Chinese remainder argument, that the proportion of $a \in \mathcal{O}_K$ such that $(f(x), a)$ fulfills the conclusion of Corollary 2.18 is bounded below by

$$\prod_{\mathfrak{p} \text{ vanishing}} \frac{1}{N(\mathfrak{p})^2} \cdot \prod_{\mathfrak{p} \text{ non-vanishing}} \left(1 - \frac{|\Omega_\mathfrak{p}|}{N(\mathfrak{p})^2}\right).$$

Here, the factor $\prod_\mathfrak{p} \frac{1}{N(\mathfrak{p})^2}$ is due to the fact that Condition 2 of Corollary 2.18 only depends on the mod-$\mathfrak{p}^2$ residue class of a. This factor is positive since there are only finitely many vanishing primes. Furthermore, by Assumption i, we have $|\Omega_\mathfrak{p}| \leq \min\{|\Omega|, N(\mathfrak{p})^2 - 1\}$ for all non-vanishing primes $\mathfrak{p}$. From this, it follows that $\prod_\mathfrak{p} \left(1 - \frac{|\Omega_\mathfrak{p}|}{N(\mathfrak{p})^2}\right)$ is bounded below by a positive constant factor (arising from the finitely many primes $\mathfrak{p}$ with $N(\mathfrak{p})^2 - 1 < |\Omega|$) times $\prod_\mathfrak{p} \left(1 - \frac{|\Omega|}{N(\mathfrak{p})^2}\right)$, the latter product obviously being bounded away from zero. In total, the proportion of $a \in \mathcal{O}_K$ such that $(f(x), a)$ fulfills the conclusion of Corollary 2.18 is bounded away from 0. ∎

The assumption in Lemma 3.1 of $(f(x), a)$ being dynamically irreducible for "most" $a \in \mathcal{O}_K$ is not automatic but can nevertheless be guaranteed in certain key cases. We collect some results ensuring this property.

Lemma 3.2 *Let p be a prime number and $f(x) = (f_1 \circ \cdots \circ f_r)(x) \in K[x]$ be a PCF polynomial such that each $f_i(x) \in K[x]$ is linearly related to x^p, that is, $f_i(x) = (\lambda_i \circ x^p \circ \mu_i)(x)$ with suitable linear polynomials $\lambda_i(x), \mu_i(x) \in K[x]$. Then there exists $n_0 \in \mathbb{N}$ such that, for all $a \in K$ with $Gal(f^{n_0}(x) - a/K) \cong Gal\big(f^{n_0}(x) - t/K(t)\big)$, the pair $(f(x), a)$ is dynamically irreducible.*

Proof For any field $K \subset F \subset \overline{K}$, let $\mathrm{Mon}_{f,F} := \mathrm{Gal}(f(x) - t/F(t))$ denote the monodromy group of $f(x)$ over F. It is well-known that $\mathrm{Mon}_{f,F}$ embeds as a permutation

[4] Note that this condition is automatically fulfilled if $|\Omega| \leq 3$.

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

group into the iterated wreath product $\mathrm{Mon}_{f_r,F} \circ \cdots \circ \mathrm{Mon}_{f_1,F}$. Furthermore, for $F = K(\zeta_p)$ the p-th cyclotomic field, one clearly has $\mathrm{Mon}_{f_i,F} \cong C_p$, so that, in particular, $\mathrm{Mon}_{f,F} \leq C_p \wr \cdots \wr C_p$ is a p-group. The assertion is now a straightforward consequence of [BGJT25, Theorem 1.3]. ∎

Remark 3.3 Note that the assumption on the Galois group of $f^{n_0}(x) - a$ is fulfilled for all but a density zero set of integral values $a \in \mathcal{O}_K$, by a sufficiently strong version of Hilbert's irreducibility theorem, see, for example, [Coh79, Theorem 1].

The following lemma collects a number of relatively well-known statements on the dynamics of Eisenstein polynomials. It is also useful in ensuring dynamical irreducibility, and eventually dynamical monogenicity.

Lemma 3.4 *Let $\mathfrak{p}$ be a prime of K. If a polynomial $f(x) \in K[x]$ is $\mathfrak{p}$-Eisenstein, then it is $\mathfrak{p}$-maximal. Moreover, the extension generated by $f(x)$ is totally ramified at $\mathfrak{p}$. Conversely, if an extension L/K is totally ramified at $\mathfrak{p}$, then L/K is generated by a polynomial, that is, $\mathfrak{p}$-Eisenstein. Finally, if $f(x)$ is $\mathfrak{p}$-Eisenstein and has degree greater than 1, then $f^n(x)$ is $\mathfrak{p}$-Eisenstein for all $n \geq 1$.*

We include a brief proof for completeness.

Proof For the first claim, suppose $f(x)$ has degree d. Note that $f(x) \equiv x^d \bmod \mathfrak{p}$. However, x does not divide $f(x)$ modulo $\mathfrak{p}^2$. Thus, $f(x)$ is $\mathfrak{p}$-maximal. Alternatively, one can use the Montes algorithm/Ore's theorem to see that the principal x-polygon is one-sided with slope $-\frac{1}{d}$. This also shows that $\mathfrak{p}$ has ramification index d. The fact that iterates of a $\mathfrak{p}$-Eisenstein polynomial are $\mathfrak{p}$-Eisenstein is implied by Lemma 2.3 of [Odo85], though a direct proof via analysis of the valuations of the coefficients of $f^n(x)$ is possible.

To see that an extension totally ramified over $\mathfrak{p}$ is given by a $\mathfrak{p}$-Eisenstein polynomial, suppose we are in that setup, and let $\mathfrak{P}$ denote the unique prime of $\mathcal{O}_L$ above $\mathfrak{p}$. Let $\pi_{\mathfrak{P}} \in \mathcal{O}_L$ be an element with $\mathfrak{P}$-adic valuation 1. We see that $K\left(\pi_{\mathfrak{P}}\right) = L$. Moreover, the minimal polynomial of $\pi_{\mathfrak{P}}$ over K is $\mathfrak{p}$-Eisenstein. This can be generalized a good deal; the interested reader should consult Proposition 12 in Section 6 of Chapter III of [Ser79]. ∎

Combining Lemma 3.4 with Theorem 1.1, we obtain a sufficient criterion for monogenicity of the *fields* generated by roots of polynomials $f^n(x) - a$, for all $n \in \mathbb{N}$. First, we need a lemma that classifies when units are monogenerators.

Lemma 3.5 *Let R be a Dedekind domain, and let α be a root of an irreducible polynomial $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in R[x]$ with $c_n \in R^\times$. Let F be the field of fractions of R, and let $L = F(\alpha)$. Write $\mathcal{O}_L$ for the ring of elements of L which are integral over R. The following are equivalent:*

(1) $\alpha \in \mathcal{O}_L^\times$.
(2) $c_0 \in R^\times$.
(3) $\alpha^{-1} \in R[\alpha]$.
(4) $R[\alpha] = R[\alpha^{-1}]$.

Proof For (1) $\implies$ (2), note that if $\alpha \in \mathcal{O}_L^\times$, then there exists $\alpha^{-1} \in \mathcal{O}_L^\times$ so that $\alpha \cdot \alpha^{-1} = 1$. Taking norms, we have $\mathrm{Norm}_{L/F}(\alpha)\mathrm{Norm}_{L/F}(\alpha^{-1}) = 1$. Thus, $c_0 \in R^\times$. ✓

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

For (2) $\Longrightarrow$ (3), we have $c_n\alpha^n + \cdots + c_1\alpha + c_0 = 0$, so

$$1 = -c_0^{-1}c_n\alpha^n - \cdots - c_0^{-1}c_1\alpha. \text{ Thus } \alpha^{-1} = -c_0^{-1}c_n\alpha^{n-1} - \cdots - c_0^{-1}c_1. \checkmark$$

For (3) $\Longrightarrow$ (4), we have $\alpha^{-1} = b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$ for some $b_i \in R$. Multiplying by α^{1-n} and subtracting, we obtain

$$\alpha^{-n} - b_0\alpha^{1-n} - b_1\alpha^{2-n} - \cdots - b_{n-3}\alpha^{-2} - b_{n-2}\alpha^{-1} - b_{n-1} = 0.$$

Since α^{-1} is a unit and since it generates the same extension field as α, we see that $x^n - b_0x^{n-1} - \cdots - b_{n-2}x - b_{n-1}$ is the minimal polynomial. (1) $\Longrightarrow$ (2) shows that $b_{n-1} \in R^\times$. Thus,

$$b_{n-1}^{-1}\alpha^{1-n} - b_{n-1}^{-1}b_0\alpha^{2-n} - b_{n-1}^{-1}b_1\alpha^{3-n} - \cdots - b_{n-1}^{-1}b_{n-3}\alpha^{-1} - b_{n-1}^{-1}b_{n-2} = \alpha$$

is an R-linear expression of α in powers of α^{-1}. Hence, $R[\alpha] = R[\alpha^{-1}]$. $\checkmark$

Finally, (4) $\Longrightarrow$ (1) is clear since $R[\alpha] = R[\alpha^{-1}] \subset \mathcal{O}_L$. $\checkmark$ ∎

Theorem 3.6 *Let $f(x) \in \mathcal{O}_K[x]$ have a leading coefficient that is a unit and let $\gamma \in \mathcal{O}_K$ be periodic under $f(x)$. Assume that all exceptional primes for $f(x)$ are vanishing.*

Given a non-unit $b \in \mathcal{O}_K$, let $K \subset K_1 \subset K_2 \subset \ldots$ be a chain of fields such that K_n is generated over K by a root of $f^n(x) - \frac{1+b\gamma}{b}$. For any non-vanishing prime $\mathfrak{p} \subset \mathcal{O}_K$ of $f(x)$, let $\mathfrak{P}$ denote a prime extending $\mathfrak{p}$ in the splitting field of $f'(x)$. For any vanishing prime $\mathfrak{p}$ of $f(x)$ not dividing b, fix $g(x) \in K[x]$ such that $f(x) - \frac{1+b\gamma}{b} \equiv g(x)^p \bmod \mathfrak{p}$ (with p the residue characteristic of $\mathfrak{p}$), and let $\mathfrak{P}$ denote a prime extending $\mathfrak{p}$ in the splitting field of $g(x)$. Assume that all of the following are fulfilled:

- **i.** *$v_\mathfrak{p}(b) \le 1$ for all primes $\mathfrak{p}$ of $\mathcal{O}_K$.*
- **ii.** *For every critical point θ of $f(x)$, every $k \in \mathbb{N}$, and every prime $\mathfrak{p}$ of $\mathcal{O}_K$ not dividing b which is a non-vanishing prime for $f(x)$, one has $v_\mathfrak{P}\big(1 + (\gamma - f^k(\theta))b\big) \le e(\mathfrak{P} \mid \mathfrak{p})$.*
- **iii.** *For every prime $\mathfrak{p}$ of $\mathcal{O}_K$ not dividing b which is a vanishing prime for $f(x)$, and for any root τ of $g(x)$, one has $v_\mathfrak{P}\big(f(\tau) - \frac{1+b\gamma}{b}\big) \le e(\mathfrak{P} \mid \mathfrak{p})$.*

Then K_n is monogenic over K for all $n \in \mathbb{N}$.

Proof For $n \in \mathbb{N}$, let α_n be a root of $f^n(x) - \frac{1+b\gamma}{b}$, let $c_n \in \mathcal{O}_K$ be such that $f^n(c_n) = \gamma$ (note that such a c_n exists due to γ being periodic), and let $\beta_n := \frac{1}{\alpha_n - c_n}$. In particular, β_n is a root of the polynomial $h_n(x) := \big(-bf^n(\frac{1}{x} + c_n) + 1 + b\gamma\big) \cdot x^{\deg(f)^n}$ (i.e., the reciprocal of the polynomial $-bf^n(x + c_n) + 1 + b\gamma$). We will show that, under the conditions of the theorem, $\mathcal{O}_{K_n} = \mathcal{O}_K[\beta_n]$ for all $n \in \mathbb{N}$.

First, we make sure that $h_n(x)$ is indeed monic. This amounts to verifying that the constant coefficient of $-bf^n(x + c_n) + 1 + b\gamma$ equals 1, which follows directly from the fact that $f^n(c_n) = \gamma$. Next, since the leading coefficient of $f(x)$ is a unit and $v_\mathfrak{p}(b) \le 1$, we see that $h_n(x)$ is a $\mathfrak{p}$-Eisenstein polynomial and hence $\mathfrak{p}$-maximal for all primes $\mathfrak{p} \mid b$ by Lemma 3.4. Since b is a non-unit, there is at least one such prime $\mathfrak{p}$ with $v_\mathfrak{p}(b) = 1$. In particular, $h_n(x)$ is irreducible.

Next, pick a prime $\mathfrak{p}$ not dividing b which is a non-vanishing prime for $f(x)$. We wish to show that the polynomial $g_n(x) := f^n(x + c_n) - \frac{1+b\gamma}{b} \in \mathcal{O}_\mathfrak{p}[x]$ is $\mathfrak{p}$-maximal. Since translating by $c_n \in \mathcal{O}_K$ does not affect whether an element of $\mathcal{O}_{K_n}$ is a monogenerator for $\mathcal{O}_{K_n} \otimes \mathcal{O}_\mathfrak{p}$, we may replace $g_n(x)$ by $f^n(x) - \frac{1+b\gamma}{b}$. Let $\pi_\mathfrak{p}$ denote a generator

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

of the maximal ideal of $\mathcal{O}_{\mathfrak{p}}$. To apply Theorem 1.1, we fix $N \in \mathbb{N}$ and choose $a := a(N) \in \mathcal{O}_K$ such that $a \equiv \frac{1+b\gamma}{b} \bmod \pi_{\mathfrak{p}}^2$ and such that $f^n(x) - a$ is irreducible for all $1 \le n \le N$. (For a fixed N, there are infinitely many such a by Hilbert's irreducibility theorem.)

From Remark 2.2, we see that $f^N(x) - \frac{1+b\gamma}{b}$ is $\mathfrak{p}$-maximal if and only if $f^N(x) - a$ is $\mathfrak{p}$-maximal. Now Assumption ii shows that, for every critical point θ of $f(x)$ and every $k \in \mathbb{N}$,

$$v_{\mathfrak{P}}\left(f^k(\theta) - a\right) = v_{\mathfrak{P}}\left(f^k(\theta) - \frac{1+b\gamma}{b}\right) \le e(\mathfrak{P} \mid \mathfrak{p}),$$

where the former equality comes from the fact that $a \equiv \frac{1+b\gamma}{b} \bmod \pi_{\mathfrak{p}}^2$ so $v_{\mathfrak{P}}(a - \frac{1+b\gamma}{b}) \ge 2e(\mathfrak{P} \mid \mathfrak{p})$. Thus, Condition 1 of Theorem 1.1 applied to the pair $\big(f(x), a\big)$ shows that $f^N(x) - a$ is $\mathfrak{p}$-maximal. Since $N \in \mathbb{N}$ was arbitrary, we have obtained that $f^n(x) - \frac{1+b\gamma}{b}$, and thus $g_n(x)$, is $\mathfrak{p}$-maximal for all $n \in \mathbb{N}$. Since $g_n(x)$ has constant coefficient $f^n(c_n) - \frac{1+b\gamma}{b} = -\frac{1}{b}$, which is a unit in $\mathcal{O}_{K_{\mathfrak{p}}}$, it follows from Lemma 3.5 that $\mathfrak{p} \nmid \big[\mathcal{O}_{K_n} : \mathcal{O}_K[\beta_n]\big]$.

Suppose now that $\mathfrak{p}$ is a vanishing prime not dividing b. As above, given $N \in \mathbb{N}$, we take any $a := a(N) \equiv \frac{1+b\gamma}{b} \bmod \pi_{\mathfrak{p}}^2$ such that $f^n(x) - a$ is irreducible for all $1 \le n \le N$. Hence, $f(x) - a \equiv f(x) - \frac{1+b\gamma}{b} \equiv g(x)^p \bmod \mathfrak{p}$. Assumption iii yields

$$v_{\mathfrak{P}}\big(f(\tau) - a\big) = v_{\mathfrak{P}}\left(f(\tau) - \frac{1+b\gamma}{b}\right) \le e(\mathfrak{P} \mid \mathfrak{p}).$$

It follows from Theorem 1.1 that the polynomial $f^N(x) - a(N)$ is $\mathfrak{p}$-maximal. Hence, by Remark 2.2 and since $N \in \mathbb{N}$ was arbitrary, $f^n(x) - \frac{1+b\gamma}{b}$ and $g_n(x)$ are $\mathfrak{p}$-maximal for all $n \in \mathbb{N}$. Thus, $\mathfrak{p} \nmid \big[\mathcal{O}_{K_n} : \mathcal{O}_K[\beta_n]\big]$.

In conclusion, $\mathcal{O}_K[\beta_n]$ is $\mathfrak{p}$-maximal for *all* primes $\mathfrak{p}$. Thus, β_n is a monogenerator of $\mathcal{O}_{K_n}$ over $\mathcal{O}_K$. ∎

4 Applications to specific families of polynomials

4.1 Unicritical polynomials

Arguably the most obvious family of PCF polynomials is given by the monomials x^d (which are unicritical and critically fixed). Investigation of dynamical monogenicity for pairs (x^d, a) with $a \in \mathbb{Z}$ has been carried out in [Jon21] (e.g., Corollary 1). Here, we generalize this widely to unicritical PCF polynomials $f(x) = ux^d + b \in \mathcal{O}_K[x]$. Our key observation is that, for polynomials of this shape, dynamical irreducibility follows automatically from the two conditions of Corollary 2.18 and thus does not have to be assumed additionally.

Theorem 4.1 *Let $a \in \mathcal{O}_K$ and $f(x) = ux^d + b \in \mathcal{O}_K[x]$, where u is a unit. Then $(f(x), a)$ is dynamically monogenic (and in particular, dynamically irreducible) if and only if both of the following hold:*

1. *For each $n \in \mathbb{N}$ and each prime $\mathfrak{p}$ of $\mathcal{O}_K$ not dividing d, one has $v_{\mathfrak{p}}\big(f^n(0) - a\big) \le 1$.*
2. *For each prime $\mathfrak{p}$ of $\mathcal{O}_K$ of residue characteristic p dividing d, the ratio $\frac{a-b}{u}$ is not congruent to any p-th power modulo $\mathfrak{p}^2$.*

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

Proof Note that Condition 1 amounts to Condition 1 of Corollary 2.18, since 0 is the unique critical point of $f(x)$. Moreover, Condition 2 is equivalent to Condition 2 of the same corollary due to the following: for $\mathfrak{p}|(d)$ of residue characteristic p and any $v, c \in \mathcal{O}_K$ such that $v^p \equiv u \bmod \mathfrak{p}$ and $c^p \equiv a - b \bmod \mathfrak{p}$, we have $f(x) - a \equiv (vx^{d/p} - c)^p \bmod \mathfrak{p}$. Choose any root θ of $vx^{d/p} - c$ in an extension of K. Condition 2 of Corollary 2.18 then implies that $f(\theta) - a = u(\frac{c}{v})^p + b - a \not\equiv 0 \bmod \mathfrak{p}^2$, so in particular $\frac{a-b}{u}$ is not congruent modulo $\mathfrak{p}^2$ to the p-th power of $\frac{c}{v}$. But on the other hand, the mod- $\mathfrak{p}$ residue class of elements $\gamma \in \mathcal{O}_K$ such that $\gamma^p \equiv \frac{a-b}{u} \bmod \mathfrak{p}$ is unique, and must be the one of $\frac{c}{v}$ by definition. This shows the claimed equivalence.

Since we have verified that our Conditions 1 and 2 amount to those of Corollary 2.18, we are left with showing that the two conditions here imply that $f^n(x) - a$ is irreducible for all $n \in \mathbb{N}$. We will show this inductively. Let α_n denote a root of $f^n(x) - a$ and set $K_n = K(\alpha_n)$. For the base case $n = 1$, note that by the so-called Vahlen–Capelli theorem (see [Tur98, Theorem 3.1]), $f(x) - a$ being reducible implies either $\frac{a-b}{u}$ being a p-th power in $\mathcal{O}_K$ for some prime divisor p of d, or $4 \mid d$ and $4 \cdot \frac{b-a}{u}$ is a 4-th power.

In the former case, we see directly that $\frac{a-b}{u}$ would have to be a p-th power modulo $\mathfrak{p}^2$, which was excluded by Condition 2.

In the latter case, we may as well assume that $\mathfrak{p}^2$ divides 2, since if $v_\mathfrak{p}(2) = 1$, then $4 \cdot \frac{b-a}{u}$ being a 4-th power implies that its $\mathfrak{p}$-adic valuation is a positive multiple of 4. Thus, $v_\mathfrak{p}(\frac{b-a}{u}) \geq 2$, and we have a contradiction. However, assuming $\mathfrak{p}^2$ divides 2 implies that -1 is a square modulo $\mathfrak{p}^2$. Thus, $4 \cdot \frac{b-a}{u}$ being a 4-th power implies that $\frac{a-b}{u}$ is a square modulo $\mathfrak{p}^2$, again a contradiction. This concludes the proof of the base case $n = 1$.

Assume now inductively that $f^n(x) - a$ is irreducible. Then it is also monogenic over K by Corollary 2.18, that is, $\mathcal{O}_K[\alpha_n] = \mathcal{O}_{K_n}$. To verify that $f^{n+1}(x) - a$ is irreducible, it suffices to show that $f(x) - \alpha_n$ is irreducible over $\mathcal{O}_{K_n}$. Set $\beta_n = \frac{\alpha_n - b}{u}$. Clearly, $f(x) - \alpha_n$ is reducible if and only if $x^d - \beta_n$ is. By the Vahlen–Capelli theorem, this can only happen if there exists some prime divisor p of d such that β_n or $-\beta_n$ (the latter being needed only in the case that $p = 2$ and $4 \mid d$) is a p-th power in $\mathcal{O}_{K_n} = \mathcal{O}_K[\alpha_n] = \mathcal{O}_K[x]/(f^n(x) - a)$. The latter implies the existence of a polynomial $g(x) \in \mathcal{O}_K[x]$ such that $g(x)^p \equiv \pm(x - b)/u \bmod (f^n(x) - a)$. But consider this congruence over the residue field $k_\mathfrak{p}$ of $\mathfrak{p}$, for a prime $\mathfrak{p}$ of $\mathcal{O}_K$ extending the rational prime p. Then both $g(x)^p$ and $f^n(x) - a$ become polynomials in x^p, and hence so does the remainder after division of one of them by the other. But clearly this is not the case for the degree-1 remainder $\pm(x - b)/u$. This contradiction concludes the proof. ∎

Applying Theorem 4.1, we obtain a particularly nice result for the family of unicritical polynomials $f(x) = 1 - x^d \in \mathbb{Z}[x]$. Note that the iterated extensions defined by $f^n(x) - a$ behave quite differently from those defined by $x^{a^n} - a$; in particular, the Galois group of the former is in general far from cyclic even after adjoining roots of unity, meaning that the theorem below yields many monogenic extensions with "interesting" Galois groups.

Theorem 4.2 *Let $d \geq 2$ be an integer, $f(x) = 1 - x^d$, and $a \in \mathbb{Z}$. Then the following are equivalent:*

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

1. $(f(x), a)$ *is dynamically monogenic.*
2. $f^2(x) - a$ *is monogenic.*
3. *Both of the following hold:*
  i. a *and* $1 - a$ *are both squarefree;*
  ii. $(1-a)^{p-1} \not\equiv 1 \bmod p^2$ *for all prime divisors* p *of* d.

In particular, the set of values $a \in \mathbb{Z}$ *such that* $(f(x), a)$ *is dynamically monogenic has positive density*

$$\frac{\varphi(d)}{d} \cdot \prod_{\substack{\ell \text{ prime} \\ \ell \nmid d}} \left(1 - \frac{2}{\ell^2}\right).$$

Proof Note that $f(x) = 1 - x^d$ is a unicritical PCF polynomial with critical orbit $\{0, 1\}$ of length 2. From Theorem 4.1, dynamical monogenicity of $(f(x), a)$ is equivalent to the following two conditions being fulfilled for all primes p:

A. If p is a non-vanishing prime for $f(x)$ (i.e., a prime not dividing d), then p^2 does not divide any of the integers a and $1 - a$.
B. If p is a vanishing prime, then $1 - a$ is not a p-th power modulo p^2.

Note that B implies the following:

C. Neither a nor $1 - a$ is divisible by p^2.

Hence, dynamical monogenicity is equivalent to all Conditions A–C being fulfilled. But A and C together are equivalent to Condition 3i. On the other hand, note that the *nonzero* p-th powers in $\mathbb{Z}/p^2\mathbb{Z}$ are exactly the p-th powers which are coprime to p, that is, the elements of $(\mathbb{Z}/p^2\mathbb{Z})^\times \cong C_{p(p-1)}$ whose multiplicative order divides $p - 1$. Hence, B and C together are equivalent to 3ii.

In total, we have obtained that the dynamical monogenicity of $(f(x), a)$ is equivalent to a fulfilling both Conditions 3i and 3ii of the theorem. On the other hand, Conditions 3i and 3ii are exactly the conditions obtained from setting $N = 2$ in Corollary 2.18, whence 2 implies 3. The implication $1 \Rightarrow 2$ is trivial.

Lastly, the density assertion follows by a Chinese remainder argument as in the proof of Lemma 3.1. Explicitly, we notice that Condition 3i excludes exactly two residue classes modulo ℓ^2 for all primes ℓ not dividing d. Whereas, for primes $p|d$, $1 - a$ satisfies 3ii in $p(p-1)$ of the possible $p^2 - 1$ nonzero residue classes modulo p^2, and 3i additionally excludes only $1 - a \equiv 0 \bmod p^2$. Thus, a total of exactly $p(p-1)$ out of p^2 residue classes are allowed. ∎

For pairs $(f(x), a)$ with $f(x) = 1 - x^d$ and a not necessarily integral, we can use Theorem 3.6 to obtain results on dynamic monogenicity for the *fields* generated by roots of $f^n(x) - a$ (rather than monogenicity of the polynomials themselves).

Concretely, we have the following.

Theorem 4.3 *Let* $d \in \mathbb{N}$ *and* $b \in \mathbb{N}$ *be positive integers such that all of the following hold:*

i. b *and* $b - 1$ *are squarefree.*
ii. *For all primes* p *which divide* d*, but not* b*, one has* $(1 - 1/b)^{p-1} \not\equiv 1 \bmod p^2$.

Let $f(x) = 1 - x^d$*, and write* K_n *for an extension of* $\mathbb{Q}$ *generated by a root of* $f^n(x) - 1/b$*. Then* K_n *is monogenic for all* $n \in \mathbb{N}$.

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

Proof This follows from Theorem 3.6 via using the periodic point $\gamma = 0$. We only need to verify that Assumptions i and ii here imply Assumptions i–iii of Theorem 3.6. Indeed, since the set of postcritical points of $f(x)$ is $\{0, 1\}$, the squarefreeness of b and of $b-1$ amounts to Conditions i and ii of Theorem 3.6, respectively. Further, Condition ii here amounts to Condition ii of Theorem 3.6, as explained in the proof of Theorem 4.2. ∎

Unicritical PCF polynomials defined over $\mathbb{Q}$ only produce critical orbits with fixed points or 2-cycles (cf. [AMT20, Theorems 2.1 and 2.3]). In order to construct critical orbits containing an n-cycle, we find quadratic polynomials $h(x) = x^2 + \alpha_n$, where α_n is defined by $h^n(\alpha_n) = 0$ and $h^k(\alpha_n) \neq 0$ for $0 \leq k < n$. The fields of definition for α_n are given by the Gleason polynomials for order n, and α_n is a Misiurewicz point of period $(1, n)$. (See [Buf18, Gok19, HT15] for additional exposition.)

Example 4.4 Let $K = \mathbb{Q}(\theta)$ be the number field defined by $\theta^3 - \theta^2 + 1 = 0$ (note that $\mathcal{O}_K = \mathbb{Z}[\theta]$), and let $f(x) = x^2 + \theta - 1$. Then $f(x)$ is PCF, since $f(0) = \theta - 1, f(\theta - 1) = \theta^2 - \theta$, and $f(\theta^2 - \theta) = 0$, and hence has a 3-cycle as its critical orbit.

Let $a \in \mathcal{O}_K$ such that $\{a, a - \theta + 1, a - \theta^2 + \theta\}$ are squarefree (as principal ideals of $\mathcal{O}_K$) and $a - \theta + 1$ is not a square in $\mathcal{O}_K/4\mathcal{O}_K$. Note that 2 is inert in $\mathcal{O}_K$ and is the only vanishing prime. Then, by Theorem 4.1, $(f(x), a)$ is dynamically monogenic over K.

4.2 Chebyshev polynomials

In this section, we determine all dynamically monogenic pairs $(T_d(x), a)$, where $a \in \mathbb{Z}$ and $T_d(x)$ is the (normalized) degree d Chebyshev polynomial, thereby generalizing [Gas14, Theorem 1.2] which deals with the case where d is prime, and characterize those pairs which generate totally real fields. Using the notation and results from [Sil07], the normalized Chebyshev polynomials $T_d(x) \in \mathbb{Z}[x]$ have the following properties:

(1) They satisfy the recurrence $T_{d+1}(x) = xT_d(x) - T_{d-1}(x)$, with $T_0(x) = 2$, $T_1(x) = x$.
(2) They are monic.
(3) They commute: $T_d\big(T_e(x)\big) = T_{de}(x) = T_e\big(T_d(x)\big)$. Note, composition gives $T_d^n(x) = T_{d^n}(x)$, so iterates of Chebyshev polynomials are also Chebyshev polynomials.
(4) Their derivatives are $T_d'(x) = dU_{d-1}(x)$, where $U_{d+1}(x) = xU_d(x) - U_{d-1}(x)$ with $U_{-1} = 0$ and $U_0(x) = 1$. The $U_i(x)$ are the normalized Chebyshev polynomials of the second kind. Together $T_d(x)$ and $U_{d-1}(x)$ satisfy the quadratic relation

$$T_d(x)^2 = 4 + (x^2 - 4)U_{d-1}(x)^2.$$

Using this last relation, we see the $T_d(x)$ are PCF. Indeed, if $U_{d-1}(\alpha) = 0$, then $T_d(\alpha) = \pm 2$ and $T_d(\pm 2)^2 = 4$. Using the recurrence, we have $T_d(2) = 2$, $T_d(-2) = (-1)^d 2$. Further, the roots of $T_d(x)$ and $U_d(x)$ are real, belong to the interval $[-2, 2]$, and are simple. They are given, respectively, by

$$2\cos\left(\frac{(2k-1)\pi}{2d}\right) = \zeta_{4d}^{2k-1} + \zeta_{4d}^{1-2k} \quad \text{and} \quad 2\cos\left(\frac{k\pi}{d+1}\right) = \zeta_{2(d+1)}^{k} + \zeta_{2(d+1)}^{-k},$$

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

where $1 \le k \le d$, and ζ_n is a primitive n-th root of unity. The main result of this section is the following.

Theorem 4.5 *Let $d \ge 2$, and let $T_d(x)$ be the normalized Chebyshev polynomial of degree d. Then, for $a \in \mathbb{Z}$, the pair $(T_d(x), a)$ is dynamically monogenic if and only if all of the following hold:*

i. *For all primes p not dividing d, one has $a \not\equiv \pm 2 \bmod p^2$.*
ii. *For all primes $p|d$, one has $T_p(a) \not\equiv a \bmod p^2$.*

We prove Theorem 4.5 by first assuming a pair is dynamically irreducible and applying the main theorem, then showing that the conditions required for the pair to be dynamically monogenic are sufficient to imply they are dynamically irreducible.

Lemma 4.6 *Let $d \ge 2$ and $a \in \mathbb{Z}$ such that $(T_d(x), a)$ is dynamically irreducible. Then $(T_d(x), a)$ is dynamically monogenic if and only if*

- *for all primes p not dividing d, one has $a \not\equiv \pm 2 \bmod p^2$, and*
- *for all primes $p|d$, $T_p(a) \not\equiv a \bmod p^2$.*

Proof Suppose first that p is a prime not dividing d. Then $T_d'(x) = dU_{d-1}(x)$ is not identically 0 in $\mathbb{F}_p$, so p is a non-vanishing prime. Furthermore, every root of $T_d'(x)$ is of the form $\zeta^k + \zeta^{-k}$ for some $2d$-th root of unity ζ. These elements are well-known to be monogenerators for the field they generate over $\mathbb{Q}$, meaning in particular that their minimal polynomial remains separable modulo all primes not dividing the field discriminant. But prime divisors of the field discriminant have to ramify in $\mathbb{Q}(\zeta_{2d})$, that is, have to divide d. We have therefore shown that all non-vanishing primes are in fact non-exceptional.

The PCF properties of $T_d(x)$ show that $T_d^n(\theta) \in \{-2, 2\}$ for any critical point θ, so we can apply Corollary 2.18 for the non-vanishing primes. Thus, $T_d^n(x) - a$ is p-maximal if and only if p^2 does not divide $-2 - a$ or $2 - a$.

Next, suppose p is a prime dividing d. We have $T_d'(x) \equiv 0 \bmod p$, so p is a vanishing prime. Let $v_p(d) = k$, and note $T_{p^k}(x) \equiv x^{p^k} \bmod p$. Let $e = d/p^k$, so $T_d(x) = T_p^k(T_e(x))$. In particular,

$$T_d(x) - a \equiv T_e(x)^{p^k} - a \equiv (T_e(x) - a)^{p^k} \bmod p.$$

To apply Corollary 2.18, we need to consider $T_d(\tau) - a$, where $\tau \in \overline{\mathbb{Q}}$ is a root of $T_e(x) - a$. More precisely, $T_d(x) - a$ is p-maximal if and only if $T_d(\tau) - a = T_p^k(a) - a \in \mathbb{Z}$ is not divisible by p^2. We reduce to $T_p(a)$ by applying Proposition 3.4 of [Gas14]: for p an odd prime,

$$T_p(b) \equiv T_p(c) \bmod p^2 \iff b \equiv c \bmod p$$

with $b = T_{p^{k-1}}(a)$ and $c = a$. The extension to $p = 2$ is immediate from $T_2(x) = x^2 - 2$. ∎

Remark 4.7 As seen in the above proof, the condition $T_p(a) \not\equiv a \bmod p^2$ is in fact equivalent to a not being in the image of $T_p(x)$ modulo p^2, which leaves a total of $p^2 - p$ residue classes modulo p^2. In particular, Theorem 4.5 then implies that the set

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

of $a \in \mathbb{Z}$ with $(T_d(x), a)$ dynamically monogenic is of density

$$\begin{cases} \frac{\varphi(d)}{d} \cdot \prod_\ell (1 - \frac{2}{\ell^2}) & \text{if } d \text{ is even} \\ \frac{\varphi(d)}{d} \cdot \frac{3}{4} \prod_{\ell \neq 2} (1 - \frac{2}{\ell^2}) & \text{if } d \text{ is odd,} \end{cases}$$

where, in both cases, the product is over primes ℓ not dividing d.

To obtain Theorem 4.5, it remains to prove that the dynamical irreducibility assumption made in Lemma 4.6 follows from Condition ii of Theorem 4.5. Note this generalizes [Gas14] even in the prime degree case.

Lemma 4.8 *Assume that $a \in \mathbb{Z}$ is such that $T_p(a) \not\equiv a \bmod p^2$ for all primes $p|d$. Then $(T_d(x), a)$ is dynamically irreducible.*

Proof Since $T_d^n(x) = T_{d^n}(x)$, it suffices to deduce irreducibility of $T_d(x) - a$ for any d. By the main theorem of [Tur98], the latter is equivalent to a not being a rational value of any polynomial $T_p(x)$ for any prime p dividing d. Further, in the case that $4|d$ there is the additional requirement that a is not of the form $-4c^4 + 8c^2 - 2$ with $c \in \mathbb{Q}$. (This latter condition is equivalent to the irreducibility of $T_4(x) - a$.) As already noted, the condition $T_p(a) \not\equiv a \bmod p^2$ is equivalent to a not being a value of $T_p(x)$ modulo p^2, which implies in particular that $T_p(x) - a$ has no rational root for any $p|d$. Furthermore, in the case where $2|d$, we have the requirement $a \not\equiv 2, 3 \bmod 4$, which in particular prevents the shape $a = -4c^4 + 8c^2 - 2$. This concludes the proof. ∎

We conclude this section with considerations about totally real monogenic extensions.

Theorem 4.9 *Let $d \geq 3$ and $a \in \mathbb{Z}$. The polynomial $T_d(x) - a$ generates a totally real monogenic field of degree d if and only if one of the following holds:*

1. *$a = 1$ and $d = 2^b 3^c$ with $b, c \geq 0$;*
2. *$a = -1$ and $d = 3^c$ with $c \geq 1$;*
3. *$a = 0$ and $d = 2^b$ with $b \geq 2$.*

Proof Since $d \geq 3$, the critical values of $T_d(x)$ are exactly ± 2. It is well-known that all of the roots of $T_d(x)$ are real, and since the number of real roots of $T_d(x) - a$ can only change as a passes a critical value, it follows that the splitting field of $T_d(x) \pm 1$ is real as well. On the other hand, a polynomial $f(x) - a$ of degree ≥ 3 can never have all of its roots real as $a \to \pm\infty$. Thus, $T_d(x) - a$ cannot generate a totally real field for $|a| > 2$. Moreover, $T_d(x) - a$ is reducible for $a = \pm 2$ a critical value. This leaves only the values $a \in \{-1, 0, 1\}$.

The polynomial $T_d(x)$ is odd when d is odd, hence $T_d(0) = 0$. This means that $T_d(x)$ is reducible for any odd integer $d \geq 3$, and thus also for any d with at least one odd prime factor, due to the relation $T_d(T_e(x)) = T_{de}(x)$.

Moreover, if $d \equiv \pm 1 \bmod 6$, then $T_d(1) = 1$, since the recurrence $T_{d+1}(x) = xT_d(x) - T_{d-1}(x)$ has period 6 when $x = 1$. Again, since $T_d(x)$ is odd when d is odd, one also gets $T_d(-1) = -1$. This means that if $p > 3$ is prime, the polynomials $T_p(x) - a$ are also reducible for $a = \pm 1$, and hence, so are the polynomials $T_d(x) - a$ for any d divisible by at least one prime $p > 3$. Lastly, $T_2(x) + 1 = x^2 - 1$ is reducible, and thus, so is $T_d(x) + 1$ for every even integer d. This leaves the values $(d, a) = (2^b 3^c, 1)$ for $b, c \geq 0$ arbitrary, $(d, a) = (3^b, -1)$, and $(d, a) = (2^b, 0)$.

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

For Cases 1 and 2, monogenicity follows from Theorem 4.5 since $T_2(x) = x^2 - 2$ maps 1 to -1, and $T_3(x) = x^3 - 3x$ maps 1 to -2 and -1 to 2. Finally, for Case 3, monogenicity follows since $T_2(x) = x^2 - 2$ does not fix 0 modulo 4. ∎

Note that the polynomials $T_d(x) - a$ in Theorem 4.9 all generate abelian extensions of $\mathbb{Q}$; indeed, as a special case of [AP20, Theorem 13], the dynamical Galois group $\varprojlim_n \mathrm{Gal}(T_{d^n}(x) - a/\mathbb{Q})$ is abelian exactly for $a \in \{-2, -1, 0, 1, 2\}$. A wider variety of totally real monogenic fields (in particular, nonabelian ones) can be obtained via resorting to non-integral specialization values.

Theorem 4.10 *Let d be a positive integer and $b < -1$ a negative integer such that all of the following are fulfilled:*

- **i.** *b and $1 + 4b$ are squarefree.*
- **ii.** *For all prime divisors p of d which do not divide b, one has $T_p(2 + \frac{1}{b}) \not\equiv 2 + \frac{1}{b} \bmod p^2$.*

Then the field generated over $\mathbb{Q}$ by a root of $T_d(x) - (2 + \frac{1}{b})$ is monogenic and totally real.

Proof Monogenicity is a straightforward consequence of Theorem 3.6 with $\gamma = 2$ (which is a fixed point of $T_d(x)$), upon noting again that the postcritical points of $T_d(x)$ are exactly ± 2 and that Condition ii here is the translation of Condition iii in Theorem 3.6, as already shown in the proof of Theorem 4.5. That the field is totally real is immediate from $|2 + \frac{1}{b}| < 2$ (due to b being negative), as noted in the proof of Theorem 4.9. ∎

4.3 PCF compositions of several polynomials

We describe a family of PCF polynomials arising as compositions of two polynomials in a nontrivial way. In particular, the polynomial $f(x)$ below is not obtained as a composition of two PCF polynomials of degree > 1, so in particular this family is not derived from any of the families considered in the previous sections. These polynomials are defined over cyclotomic fields and can be constructed to have any number of critical points. Let d be a positive integer, write ζ for a primitive d-th root of unity, and μ for a primitive $(2d-1)$-th root of unity if d is odd, or a primitive $(4d-2)$-th root if d is even. Let $K = \mathbb{Q}(\mu)$. Then

$$f(x) = x^{2d} + 2\mu x^d = x^d(x^d + 2\mu) = (x^2 + 2\mu x) \circ x^d \quad \text{with} \quad f'(x) = 2dx^{d-1}(x^d + \mu)$$

has $d+1$ critical points: 0 and $(-1)^d \mu^2 \zeta^k$ for each $0 \le k < d$. Each nonzero critical point is mapped by $f(x)$ to $-\mu^2$, which is fixed by $f(x)$, while 0 is mapped to 0. For each prime p dividing $2d$ and each $a \in \mathcal{O}_K$, μ is a p-th power in $\mathcal{O}_K$ because $(p, 2d-1) = 1$, and we have

$$f(x) - a \equiv \left(x^{\frac{2d}{p}} + 2\mu^{\frac{1}{p}} x^{\frac{d}{p}} - a\right)^p \bmod p.$$

When $d = 2^k$, this becomes a power of a linear polynomial in $\mathcal{O}_K[x]$, so we can apply Lemma 3.2 to find values of a, where $(f(x), a)$ is dynamically irreducible, and Corollary 2.18 to restrict to those that are dynamically monogenic.

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

Theorem 4.11 *For $k \geq 1$, let $d = 2^k$, μ a primitive $(4d-2)$-th root of unity, $K = \mathbb{Q}(\mu)$, and $f(x) = x^{2d} + 2\mu x^d$. Then the following hold:*

1. *The set of all $a \in \mathcal{O}_K$ such that $(f(x), a)$ is dynamically irreducible, (a) and $(a + \mu^2)$ are squarefree, and $f(a) - a$ is not divisible by $\mathfrak{p}^2$ for any prime ideal $\mathfrak{p}$ above 2, is a positive density subset of $\mathcal{O}_K$.*
2. *For all $a \in \mathcal{O}_K$ with the above properties, $(f(x), a)$ is dynamically monogenic over K.*

Proof Since $f(x)$ is a composition of quadratic polynomials, it follows from Lemma 3.2 and Remark 3.3 that $(f(x), a)$ is dynamically irreducible for all but a density zero set of values $a \in \mathcal{O}_K$. To apply Corollary 2.18 and Lemma 3.1, note that the prime ideals above 2 in $\mathcal{O}_K$ are vanishing primes, and since for all primes $\mathfrak{p}$ not dividing 2, the polynomial $x^d + \mu$ remains separable modulo $\mathfrak{p}$, all non-vanishing primes are non-exceptional.

The PCF properties of $f(x)$ and the squarefree conditions on (a) and $(a + \mu^2)$ ensure that the non-vanishing primes condition holds, and here clearly Condition i of Lemma 3.1 holds (with $|\Omega| = 2$).

Shifting to the vanishing primes, the primes above 2, the field K is also the $(2^{k+1} - 1)$-th cyclotomic field, so (2) factors into $\phi(2^{k+1} - 1)/(k+1)$ distinct prime ideals, each with inertia degree $k+1$. Let $\mathfrak{p}$ be one such prime. The assumption that $f(a) - a$ is not divisible by $\mathfrak{p}^2$ is precisely what the vanishing prime condition of Corollary 2.18 requires. In order for Condition ii of Lemma 3.1 to hold, it suffices to find one value $a \in \mathcal{O}_K$ for which $f(a) - a$ has this property. But note that, if $\mathfrak{p}$ divides (a) and (a) is squarefree, then $f(a) - a$ is not divisible by $\mathfrak{p}^2$, since $v_\mathfrak{p}\big(f(a)\big) = 2^k + 1$ and $v_\mathfrak{p}(a) = 1$. Hence, the assumption holds if $\mathfrak{p}$ strictly divides a. In particular, $a = 2$ works for all such $\mathfrak{p}$.

It thus follows from Lemma 3.1 that a positive density of values $a \in \mathcal{O}_K$ fulfill all the conditions in 1 and hence render $(f(x), a)$ dynamically monogenic. ∎

Question 4.12 *Is dynamical irreducibility in fact implied by the remaining assumptions of Theorem 4.11? We are not aware of a counterexample, although our criteria (such as Theorem 4.1) are not applicable to compositions of arbitrary quadratic polynomials, as shown by the example in Remark 2.10.*

Acknowledgements The authors are especially grateful to Sebastian Bozlee for the insightful suggestion that Uchida's criterion could be used to create a general connection between critical points and monogenicity. The authors would also like to thank the anonymous referee for the helpful comments.

References

[AMT20] J. Anderson, M. Manes, and B. Tobin, *Cubic post-critically finite polynomials defined over $\mathbb{Q}$*. Open Book Series **4**(2020), no. 1, 23–38. https://doi.org/10.2140/obs.2020.4.23

[AP20] J. Andrews and C. Petsche, *Abelian extensions in dynamical Galois theory*. Algebra Number Theory **14**(2020), no. 7, 1981–1999. https://doi.org/10.2140/ant.2020.14.1981

[BGJT25] R. L. Benedetto, D. Ghioca, J. Juul, and T. J. Tucker, *Specializations of iterated Galois groups of PCF rational functions*. Math. Ann. **392**(2025), 1031–1050.

[BIJ+15] A. Bridy, P. Ingram, R. Jones, J. Juul, A. Levy, M. Manes, S. Rubinstein-Salzedo, and J. Silverman, *Finite ramification for preimage fields of postcritically finite morphisms*. Math. Res. Lett. **24**(2015), 10. https://doi.org/10.4310/mrl.2017.v24.n6.a3

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press

[Buf18] X. Buff, *On postcritically finite unicritical polynomials*. New York J. Math. **24**(2018), 1111–1122. nyjm.albany.edu/j/2018/24-54p.pdf

[Cas22] M. Castillo, *A dynamical characterization for monogenity at every level of some infinite 2-towers*. Canad. Math. Bull. **65**(2022), no. 3, 806–814. https://doi.org/10.4153/S0008439521000874

[Coh79] S. D. Cohen, *The distribution of the Galois groups of integral polynomials*. Illinois J. Math. **23**(1979), no. 1, 135–152. https://doi.org/10.1215/ijm/1256048323

[Ded78] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*. Abh. Königl. Ges. Wiss. Göttingen **23**(1878), no. 3, 3–38.

[Gas14] T. Alden Gassert, *Discriminants of Chebyshev radical extensions*. J. Théor. Nombres Bordx. **26**(2014), no. 3, 607–633. https://doi.org/10.5802/jtnb.882

[Gas17] T. Alden Gassert, *A note on the monogeneity of power maps*. Albanian J. Math. **11**(2017), no. 1, 3–12. https://doi.org/10.51286/albjm/1495919797

[Gok19] V. Goksel, *On the orbit of a post-critically finite polynomial of the form $x^d + c$*. Funct. Approx. Comment. Math. **62**(2019). https://doi.org/10.7169/facm/1799

[HT15] B. Hutz and A. Towsley, *Misiurewicz points for polynomial maps and transversality*. New York J. Math. **21**(2015), 297–319. nyjm.albany.edu/j/2015/21-13v.pdf

[Jon21] L. Jones, *Monogenically stable polynomials*. Albanian J. Math. **15**(2021), no. 2, 85–98. https://doi.org/10.51286/albjm/1635847634

[Lan94] S. Lang, Algebraic number theory. 2nd ed., volume 110 of Graduate Texts in Mathematics, Springer-Verlag, New York, NY, 1994.

[Li22] R. Li, *On number fields towers defined by iteration of polynomials*. Arch. Math. **119**(2022), no. 4, 371–379. https://doi.org/10.1007/s00013-022-01770-w

[Odo85] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*. Proc. Lond. Math. Soc. **s3-51**(1985), no. 3, 385–414. https://doi.org/10.1112/plms/s3-51.3.385

[Ser79] J. P. Serre, Local fields, Graduate Texts in Mathematics, Springer, 1979. https://doi.org/10.1007/978-1-4757-5673-9

[Sil07] J. H. Silverman, *The arithmetic of dynamical systems*, Springer, New York, NY, 2007. https://doi.org/10.1007/978-0-387-69904-2

[Smi21] H. Smith, *The monogeneity of radical extensions*. Acta Arith. **198**(2021), no. 3, 313–327. https://doi.org/10.4064/aa200811-7-10

[Smi25] H. Smith, *Radical dynamical monogenicity*. J. Théor. Nombres Bordeaux **37**(2025), no. 1, 153–169. https://doi.org/10.5802/jtnb.1317

[SSL24] H. Sharma, R. Sarma, and S. Laishram, *Monogenity of iterates of irreducible binomials*. Commun. Algebra **52**(2024), no. 11, 4678–4684. https://doi.org/10.1080/00927872.2024.2356250

[SW24] H. Smith and Z. Wolske, *Iterates of quadratics and monogenicity*. Preprint, 2024. https://arxiv.org/abs/2406.03629 (to appear in Rocky Mountain Journal of Mathematics)

[Tur98] G. Turnwald, *Reducibility of translates of Dickson polynomials*. Proc. Amer. Math. Soc. **126**(1998), no. 4, 965–971. https://doi.org/10.1090/S0002-9939-98-04363-9

[Uch77] K. Uchida, *When is $\mathbb{Z}[\alpha]$ the ring of the integers?* Osaka J. Math. **14**(1977), 155–157. https://doi.org/10.18910/8668

[VV21] X. Vidaux and C. R. Videla, *Dedekind's criterion for the monogenicity of a number field versus Uchida's and Lüneburg's*. Tohoku Math. J. **73**(2021), no. 3, 433–447. https://doi.org/10.2748/tmj.20200602

Korea National University of Education, Republic of Korea
e-mail: jkoenig@knue.ac.kr

California State University San Marcos, USA
e-mail: hsmith@csusm.edu

e-mail: zackwolske@gmail.com

https://doi.org/10.4153/S0008414X26102351 Published online by Cambridge University Press