ALBANIAN JOURNAL OF MATHEMATICS
Volume 15, Number 2, Pages 85–98
ISSN: 1930-1235; (**2021**)

MONOGENICALLY STABLE POLYNOMIALS

LENNY JONES

Professor Emeritus
Department of Mathematics
Shippensburg University
Shippensburg, Pennsylvania 17257, USA

Abstract. A monic polynomial $f(x) \in \mathbb{Z}[x]$ is called *stable* if $f^n(x)$ is irreducible over $\mathbb{Q}$ for all $n \geq 1$, where $f^n(x)$ denotes the nth iterate of $f(x)$. Regardless of whether $f(x)$ is irreducible over $\mathbb{Q}$, if there exists some monic $g(x) \in \mathbb{Z}[x]$ such that $g(f^n(x))$ is irreducible over $\mathbb{Q}$ for all $n \geq 1$, we say that $f(x)$ is *g-stable*. Many authors have studied such polynomials since Odoni first introduced this concept of stability in 1985. We extend these concepts here by adding the additional restriction of monogeneity. A monic polynomial $f(x) \in \mathbb{Z}[x]$ is defined to be *monogenic* if $f(x)$ is irreducible over $\mathbb{Q}$ and $\left\{1, \theta, \theta^2, \ldots, \theta^{\deg(f)-1}\right\}$ is a basis for the ring of integers of $\mathbb{Q}(\theta)$, where $f(\theta) = 0$. We say that $f(x)$ is *g-monogenically stable*, if $g(f^n(x))$ is monogenic for all $n \geq 1$, for some monic $g(x) \in \mathbb{Z}[x]$. When $g(x) = x$, we simply say that $f(x)$ is *monogenically stable*. In this article, we provide methods for constructing g-monogenically stable polynomials $f(x)$, for various polynomials $f(x)$ and $g(x)$.

Mathematics Subject Classes 2020: 11R06; 12F05; 11R09
Keywords: stable polynomial; monogenic polynomial; irreducible polynomial

1. Introduction

Throughout this article, unless stated otherwise, when we say $f(x) \in \mathbb{Z}[x]$ is "irreducible" or "reducible", we mean over the rational numbers $\mathbb{Q}$. Let $f(x) \in \mathbb{Z}[x]$ be monic with $\deg(f) = n$. If $f(x)$ is irreducible, let $K = \mathbb{Q}(\theta)$, and let $\mathbb{Z}_K$ denote the ring of integers of K, where $f(\theta) = 0$. We then have the following well-known equation [4]:

$$\Delta(f) = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 \, \Delta(K), \tag{1}$$

where $\Delta(*)$ denotes the discriminant of $*$. We say that $f(x)$ is *monogenic* if $f(x)$ is irreducible and $[\mathbb{Z}_K : \mathbb{Z}[\theta]] = 1$ or, equivalently from (1), that $\Delta(f) = \Delta(K)$. In

E-mail address: lkjone@ship.edu.

other words, a monic polynomial $f(x) \in \mathbb{Z}[x]$ is monogenic if and only if $f(x)$ is irreducible and

$$\{1, \theta, \theta^2, \ldots, \theta^{n-1}\} \text{ is a basis for } \mathbb{Z}_K. \tag{2}$$

The basis in (2) is called a *power basis*, which facilitates calculations in $\mathbb{Z}_K$. Observe from (1) that if $\Delta(f)$ is squarefree, then $f(x)$ is monogenic. However, the converse is false, and it can be quite difficult to determine whether $f(x)$ is monogenic when $\Delta(f)$ is not squarefree. Numerous authors have constructed infinite families of monogenic polynomials [1, 2, 6–8, 12–19, 21–23, 30–32].

In 1985, Odoni's study of the prime divisors of nonlinear recurrence relations [25] led him to a Galois theory of the iterates and compositions of polynomials [26]. For his investigations, Odoni defined a polynomial $f(x) \in K[x]$, where K is a field, to be *stable over* K, or simply *stable* when K is understood, if $f^n(x)$ is irreducible over K for all $n \geq 1$, where $f^n(x)$ denotes the nth iterate of $f(x)$. An immediate consequence (using a theorem of Capelli) is that $f(x)$ is stable if and only if $f^n(x)$ is stable for some n if and only if $f^n(x)$ is stable for all n.

Remark 1. *We caution the reader that the definition of a stable characteristic polynomial of a differential equation is different from the concept of a stable polynomial given here.*

Stable polynomials $f(x) \in \mathbb{Z}[x]$ have played a role in certain questions arising in arithmetic dynamics [20, 27] concerning the prime divisors of the terms in the sequence $z, f(z), f^2(z), \ldots$ for various $z \in \mathbb{Z}$. For such investigations, it has also been useful to examine when there exists some $g(x) \in \mathbb{Z}[x]$, with $g(x) \neq f(x)$, such that $g(f^n(x))$ is irreducible for all $n \geq 1$, especially when $f(x)$ is not stable [20]. Regardless of whether $f(x)$ itself is stable, if $g(f^n(x))$ is irreducible for some $g(x) \neq f(x)$ and all $n \geq 1$, we say that $f(x)$ is *g-stable*.

In this article, we extend the concept of the stability of a polynomial by imposing the additional restriction of monogeneity. We define a monic polynomial $f(x) \in \mathbb{Z}[x]$ to be *monogenically stable* if $f^n(x)$ is monogenic for all $n \geq 1$. It is clear that if $f(x)$ is monogenically stable, then $f^n(x)$ is monogenically stable for all $n \geq 2$. Regardless of whether a monic polynomial $f(x)$ is monogenically stable itself, we say that $f(x)$ is *g-monogenically stable* if $g(f^n(x))$ is monogenic for some monic polynomial $g(x) \neq f(x)$ and all $n \geq 1$. Trivially, if $f(x)$ is monogenically stable, then $f(x)$ is g-monogenically stable, where $g(x) = x$. We also note that since the irreducibility of a monic polynomial $f(x)$ is a necessary condition for the monogeneity of $f(x)$, we then have that $f(x)$ is g-stable if $f(x)$ is g-monogenically stable.

The fact that the composition of two monic p-Eisenstein polynomials is again p-Eisenstein provides an easy method for the construction of stable polynomials. However, it is less obvious how to manufacture monogenically stable polynomials.

The purpose of this article is to develop methods that can be used to construct monogenically stable and g-monogenically stable polynomials. Our investigations are motivated primarily by [9] and [13]. The following result is a consequence of Theorem 1.1 in [9]:

Theorem 1. [9] *For any integer $m > 1$, the polynomial $x^m - t \in \mathbb{Z}[x]$ is monogenic if and only if t is squarefree and $t^p \not\equiv t \pmod{p^2}$ for all primes p dividing m.*

The second of our motivational papers [13] contains the following theorem which is of interest to us here:

Theorem 2. [13] *Let a and b be positive integers, and let p be a prime. Then the polynomial $\Phi_{p^a}(\Phi_{2^b}(x))$ is monogenic, where $\Phi_N(x)$ is the cyclotomic polynomial of index N.*

Using applications of Theorems 1 and 2, along with a modest extension of Theorem 2, we indicate methods for the construction of g-monogenically stable polynomials. From our main theorem, we deduce a corollary that gives necessary and sufficient conditions for certain polynomials to be monogenically stable. Finally, we use these results to provide specific examples of g-monogenically stable polynomials for certain $g(x) \in \mathbb{Z}[x]$. Our main theorem and corollary are as follows:

Theorem 3. *For any integer $N \geq 1$, let $\Phi_N(x)$ denote the cyclotomic polynomial of index N, and let*

$$J_N := \{j : 1 \leq j < N \text{ and } \gcd(N, j) = 1\}.$$

Let a, t and m be integers such that $a \geq 1$, $t \geq 1$ and $m \geq 2$. Define

$$f_{m,t}(x) := (x - t)^m + t. \tag{3}$$

Then $f_{m,t}(x)$ is g-monogenically stable in each of the following situations:

(1) *$g(x) = x$ (that is, $f_{m,t}(x)$ is monogenically stable); provided t is squarefree and $t^q \not\equiv t \pmod{q^2}$ for all primes q dividing m,*

(2) *$g(x) = \Phi_N(x)$; provided p and q are primes such that*

$$\begin{array}{ll} \Phi_N(t) \in \{q, 2q\}, \text{ with } q \geq 3, & \text{if } N = 2^a, \\ \Phi_N(t) \in \{q, pq\}, \text{ with } q > p \geq 3, & \text{if } N \in \{p^a, 2p^a\}, \end{array} \tag{4}$$

and one of the following specific sets of conditions is satisfied:

(A) (i) $N = 2^a$
(ii) $\Phi_N(t) \in \{q, 2q\}$
(iii) $m = q$
(iv) $\Phi_N\left((t^j - t)^q + t\right) \not\equiv 0 \pmod{q^2}$ *for all* $j \in J_N$,

(B) (i) $N \in \{p^a, 2p^a\}$
(ii) $\Phi_N(t) = pq$
(iii) $m = q$,
(iv) $\Phi_N\left((t^j - t)^q + t\right) \not\equiv 0 \pmod{q^2}$ *for all* $j \in J_N$,

(C) (i) $N = p \equiv 3 \pmod 4$
(ii) $\Phi_N(t) = q$ *is prime for some positive integer* $t \equiv 0 \pmod p$, *such that p is a primitive root modulo q^2*
(iii) $m = q$,
(iv) $\Phi_N\left((t^j - t)^q + t\right) \not\equiv 0 \pmod{q^2}$ *for all* $j \in J_N$,

(D) (i) $N \in \{p^a, 2p^a\}$
(ii) $m = p$
(iii) $t = 1$,

(E) (i) $N = p^a$
(ii) $m = 2$
(iii) $t = 1$.

Remark 2. *Regarding (C) in part (2) of Theorem 3, we conjecture, based on computer calculations, that if $a \geq 2$ and $\Phi_{p^a}(t)$ is prime for some positive integer $t \equiv 0 \pmod p$, then p is not a primitive root modulo q^2.*

Corollary 1. *Let $t \geq 1$ be an integer, and suppose that p and q are primes satisfying (4). Then $f_{q,t}(x)$ is monogenically stable if and only if t is squarefree.*

2. PRELIMINARIES

The following two theorems are due to Capelli (See Section 2.1 in [28]).

Theorem 4. *Let $G(x)$ and $H(x)$ be polynomials in $\mathbb{Q}[x]$ with $G(x)$ irreducible. Suppose that $G(\alpha) = 0$. Then $G(H(x))$ is reducible over $\mathbb{Q}$ if and only if $H(x) - \alpha$ is reducible over $\mathbb{Q}(\alpha)$.*

Theorem 5. *Let $r \in \mathbb{Z}$ with $r \geq 2$, and let $\gamma \in \mathbb{C}$ be algebraic. Then $x^r - \gamma$ is reducible over $\mathbb{Q}(\gamma)$ if and only if either there is a prime p dividing r such that $\gamma = \beta^p$ for some $\beta \in \mathbb{Q}(\gamma)$ or $4 \mid r$ and $\gamma = -4\beta^4$ for some $\beta \in \mathbb{Q}(\gamma)$.*

Theorem 6. *Let N and m be positive integers, and let ρ be a prime. Let $\Phi_N(x)$ denote the cyclotomic polynomial of index N. Then*

(1) [24]

$$\Phi_N\left(x^\rho\right) = \begin{cases} \Phi_{\rho N}(x) & \text{if } N \equiv 0 \pmod{\rho} \\ \Phi_N(x)\Phi_{\rho N}(x) & \text{if } N \not\equiv 0 \pmod{\rho}, \end{cases}$$

(2) [33]

$$\Delta\left(\Phi_{\rho^m}(x)\right) = \varepsilon\rho^{\rho^{m-1}(\rho m - m - 1)},$$

where

$$\varepsilon = \begin{cases} -1 & \text{if } \rho^m = 4 \text{ or } \rho \equiv 3 \pmod 4 \\ 1 & \text{otherwise,} \end{cases}$$

(3) [10] *Suppose that $\rho \nmid N$. Let $\operatorname{ord}_N(\rho)$ denote the order of ρ modulo N. Then $\Phi_N(x)$ factors modulo ρ into a product of $\phi(N)/\operatorname{ord}_N(\rho)$ distinct irreducible polynomials, each of degree $\operatorname{ord}_N(\rho)$. Additionally,*

$$\Phi_{\rho^m N}(x) \equiv \Phi_N(x)^{\phi(\rho^m)} \pmod{\rho}.$$

The following proposition is a special case of the main theorem in [11].

Proposition 1. *Let n and j be integers with $n \geq 1$ and $1 \leq j \leq 2^n$. Then*

$$\binom{2^n}{j} \equiv \begin{cases} 0 \pmod 4 & \text{if } j \not\equiv 0 \pmod{2^{n-1}} \\ 2 \pmod 4 & \text{if } j = 2^{n-1} \\ 1 \pmod 4 & \text{if } j = 2^n. \end{cases}$$

The following definition is one form for the resultant of two polynomials.

Definition 1. *Let $f(x) \in \mathbb{Z}[x]$ and $g(x) \in \mathbb{Z}[x]$, with $\deg(f) = d$ and $\deg(g) = e$, such that the zeros of $g(x)$ are $u_1, u_2, \ldots, u_e$. Then the* resultant *$R(f, g)$ of $f(x)$ and $g(x)$ is*

$$R(f, g) := (-1)^{de} b^d \prod_{i=1}^{e} f\left(u_i\right),$$

where b is the leading coefficient of $g(x)$.

To the best of our knowledge, the following result is originally due to John Cullinan [5]. For a proof, see [13].

Theorem 7. *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Q}[x]$, with respective leading coefficients a and b, and respective degrees d and e. Then*

$$\Delta(f \circ g) = (-1)^{d^2 e(e-1)/2} a^{n-1} b^{d(de-e-1)} \Delta(f)^e R(f \circ g, g').$$

The next theorem is a standard tool used to determine if a monic irreducible polynomial is monogenic. The method is commonly referred to as *Dedekind's Index Criterion* or simply *Dedkind's Criterion* if the context is clear.

Theorem 8 (Dedekind's Criterion [4])**.** *Let θ be an algebraic integer, and let K denote the number field $\mathbb{Q}(\theta)$ with ring of integers $\mathbb{Z}_K$. Let $\mathcal{T}(x) \in \mathbb{Z}[x]$ be the monic minimal polynomial of θ. Let ρ be a prime number and let $\overline{*}$ denote reduction of $*$ modulo ρ (in $\mathbb{Z}$, $\mathbb{Z}[x]$ or $\mathbb{Z}[\theta]$). Let*

$$\overline{\mathcal{T}}(x) = \prod_{i=1}^{s} \overline{\gamma_i}(x)^{e_i}$$

be the factorization of $\mathcal{T}(x)$ modulo ρ in $\mathbb{F}_\rho[x]$, and set

$$G(x) = \prod_{i=1}^{s} \gamma_i(x),$$

where the $\gamma_i(x) \in \mathbb{Z}[x]$ are arbitrary monic lifts of the $\overline{\gamma_i}(x)$. Let $H(x) \in \mathbb{Z}[x]$ be a monic lift of $\overline{\mathcal{T}}(x)/\overline{G}(x)$ and set

$$F(x) = \frac{G(x)H(x) - \mathcal{T}(x)}{\rho} \in \mathbb{Z}[x].$$

Then

$$[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{\rho} \iff \gcd\left(\overline{F}, \overline{G}, \overline{H}\right) = 1 \text{ in } \mathbb{F}_\rho[x].$$

3. The Proof of Theorem 3

Proof of Theorem 3. Note first that

$$f_{m,t}^n(x) = (x-t)^{m^n} + t,$$

for any integers $m \geq 2$, $n \geq 1$ and $t \geq 1$. This fact will be used throughout the proof.

For part (1), suppose that t is squarefree and $t^q \not\equiv t \pmod{q^2}$ for all primes q dividing m. Then, from Theorem 1, we have that $f(x) = x^m$ is g-monogenically stable when $g(x) = x - t$. That is, $g\left(f^n(x)\right) = x^{m^n} - t$ is monogenic for all $n \geq 1$. (Gassert made this observation in [9].) Hence,

$$g\left(f^n(x+t)\right) = (x+t)^{m^n} - t = f_{m,t}^n(x) \quad \text{is monogenic for all } n \geq 1, \tag{5}$$

which completes the proof of part (1).

For part (2), we omit the details for the sets of conditions (D) and (E) since they can be handled in a manner similar to the other sets of conditions. For the sets of conditions (A), (B) and (C), we have that $m = q$, such that p and q are primes for which (4) holds. Let

$$T_n(x) := \Phi_N\left(f_{q,t}^n(x)\right) = \Phi_N\left((x-t)^{q^n} + t\right). \tag{6}$$

We show first that $T_n(x)$ is irreducible. To accomplish this task, we assume that

$$T_n(x+t) = \Phi_N\left(x^{q^n} + t\right)$$

is reducible and proceed by way of contradiction. Then, by Theorems 4 and 5 with $G(x) = \Phi_N(x)$, $G(\alpha) = 0$ and $H(x) = x^{q^n} + t$, we have that $x^{q^n} - (-t + \alpha)$ is reducible and

$$-t + \alpha = \beta^q \tag{7}$$

for some $\beta \in \mathbb{Q}(-t + \alpha) = \mathbb{Q}(\alpha)$. Applying the algebraic norm $\mathcal{N} := \mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}$ to equation (7) yields

$$\Phi_N(t) = \mathcal{N}(-t + \alpha) = \mathcal{N}(\beta)^q = b^q,$$

for some $b \in \mathbb{Z}$, which is impossible by (4). Consequently, $T_n(x)$ is irreducible.

To complete the proof that $T_n(x)$ is monogenic, we treat parts (A), (B) and (C) separately. For part (A), we have that $N = 2^a$, where $a \geq 1$. We give details only for the case

$$\Phi_{2^a}(t) = t^{2^{a-1}} + 1 = q \geq 3, \tag{8}$$

where q is prime, since the case $\Phi_{2^a}(t) = 2q$ is handled similarly. By Theorem 7 and part (2) of Theorem 6, we have that

$$|\Delta(T_n)| = \left(2^{2^{a-1}(a-1)}\right)^{q^n} q^{nq^n 2^{a-1}} \Phi_{2^a}(t)^{q^n - 1} = 2^{2^{a-1}(a-1)q^n} q^{q^n(n2^{a-1}+1)-1}. \tag{9}$$

We see from (9) that if $a \geq 2$, then there are exactly two primes to consider when applying Theorem 8, namely $\rho = 2$ and $\rho = q$; while if $a = 1$, then the only prime to consider is $\rho = q$.

First, suppose that $a \geq 2$ and let $\rho = 2$. It will be computationally more efficient in this case to examine

$$\mathcal{T}(x) := T_n(x + t) = \Phi_{2^a}\left(x^{q^n} + t\right) = \left(x^{q^n} + t\right)^{2^{a-1}} + 1, \tag{10}$$

rather than $T_n(x)$, in Theorem 8. Let $\mathbb{Z}_K$ denote the ring of integers of $K = \mathbb{Q}(\theta)$, where $\mathcal{T}(\theta) = 0$. Observe from (8) that $t \equiv 0 \pmod 2$. Hence,

$$\mathcal{T}(x) \equiv \left(x^{q^n}\right)^{2^{a-1}} + 1 \equiv \left(x^{q^n} + 1\right)^{2^{a-1}} \pmod 2.$$

By part (3) of Theorem 6, we have that

$$x^{q^n} + 1 \equiv \prod_{d|q^n} \Phi_d(x) \equiv \prod_{d|q^n} \left(\prod_{i=1}^{\phi(d)/\operatorname{ord}_q(2)} \overline{\gamma}_{d,i}(x) \right) \pmod 2, \tag{11}$$

where $\prod_{i=1}^{\phi(d)/\operatorname{ord}_q(2)} \overline{\gamma}_{d,i}(x)$ is the factorization of $\Phi_d(x)$ into irreducibles in $\mathbb{F}_2[x]$, with the $\overline{\gamma}_{d,i}(x)$ distinct and each of degree $\operatorname{ord}_q(2)$. Hence, in Theorem 8, we may let

$$G(x) = \prod_{d|q^n} \left(\prod_{i=1}^{\phi(d)/\operatorname{ord}_q(2)} \gamma_{d,i}(x) \right) \text{ and } H(x) = \prod_{d|q^n} \left(\prod_{i=1}^{\phi(d)/\operatorname{ord}_q(2)} \gamma_{d,i}(x) \right)^{2^{a-1}-1},$$

where the $\gamma_{d,i}(x)$ are monic lifts of $\overline{\gamma}_{d,i}(x)$. Then, by (11), we have that

$$G(x)H(x) = \left(x^{q^n} + 1 + 2r(x)\right)^{2^{a-1}},$$

for some $r(x) \in \mathbb{Z}[x]$. Hence,

$$\begin{aligned} F(x) &= \frac{G(x)H(x) - \mathcal{T}(x)}{2} \\ &= \frac{\left(x^{q^n} + 1 + 2r(x)\right)^{2^{a-1}} - \left(x^{q^n} + t\right)^{2^{a-1}} - 1}{2} \\ &= \sum_{j=1}^{2^{a-1}-1} \frac{\binom{2^{a-1}}{j}}{2} (x^{q^n})^j + s(x) - \sum_{j=0}^{2^{a-1}-1} \frac{\binom{2^{a-1}}{j} t^{2^{a-1}-j}}{2} (x^{q^n})^j, \end{aligned}$$

where

$$s(x) = \sum_{j=1}^{2^{a-1}} \binom{2^{a-1}}{j} (x^{q^n} + 1)^{2^{a-1}-j} 2^{j-1} r(x)^j \equiv 0 \pmod 2.$$

Therefore, by Proposition 1, we conclude that

$$\overline{F}(x) = \overline{\left(\frac{\binom{2^{a-1}}{2^{a-2}}}{2}\right)} \left(x^{q^n}\right)^{2^{a-2}} = x^{2^{a-2}q^n}.$$

Therefore, $\gcd(\overline{F}, \overline{G}) = 1$ since $\overline{G}(0) \not\equiv 0 \pmod 2$. Hence, $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod 2$ by Theorem 8.

Now let $\rho = q$ in Theorem 8. In this case, for more simplicity in the calculations, we examine

$$\mathcal{T}(x) := T_n(x) = \Phi_{2^a}\left(f_{q,t}^n(x)\right) = \Phi_{2^a}\left((x-t)^{q^n} + t\right),$$

rather than $T_n(x+t)$. Since $t^{2^{a-1}} + 1 = q$, we conclude that $\mathrm{ord}_q(t) = 2^a$ and $\mathrm{ord}_{2^a}(q) = 1$. Hence, by part (3) of Theorem 6, $\Phi_{2^a}(x)$ factors modulo q into 2^{a-1} distinct linear factors. More precisely, we have that

$$\mathcal{T}(x) \equiv \left(\Phi_{2^a}(x)\right)^{q^n} \equiv \prod_{j \in J_{2^a}} (x - t^j)^{q^n} \pmod q. \tag{12}$$

Then, in Theorem 8, we may let

$$G(x) = \prod_{j \in J_{2^a}} (x - t^j) \quad \text{and} \quad H(x) = \prod_{j \in J_{2^a}} (x - t^j)^{q^n - 1},$$

so that

$$qF(x) = G(x)H(x) - \mathcal{T}(x) = \prod_{j \in J_{2^a}} (x - t^j)^{q^n} - \Phi_{2^a}\left((x-t)^{q^n} + t\right).$$

By condition 2((A))iv, we have that $\mathcal{T}(t^j) \not\equiv 0 \pmod{q^2}$ for each $j \in J_{2^a}$. Thus, $\gcd(\overline{F}, \overline{G}) = 1$ and, consequently, $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod q$ by Theorem 8. Hence, the proof that $\mathcal{T}(x)$ is monogenic is complete in this case.

We turn now to part (B), where $\Phi_{p^a}(x) = pq$, for some primes p and q with $3 \le p < q$, and $m = q$. We focus on the case $N = p^a$, since the case $N = 2p^a$ can be addressed using similar methods. Let

$$\mathcal{T}(x) := T_n(x) = \Phi_{p^a}\left(f_{q,t}^n(x)\right) = \Phi_{p^a}\left((x-t)^{q^n} + t\right),$$

and let $\mathbb{Z}_K$ denote the ring of integers of $K = \mathbb{Q}(\theta)$, where $\mathcal{T}(\theta) = 0$. By Theorem 7 and part (2) of Theorem 6, we have that

$$\begin{aligned} |\Delta(\mathcal{T})| &= \left(p^{p^{a-1}(pa-a-1)}\right)^{q^n} q^{nq^n p^{a-1}(p-1)} \Phi_{p^a}(t)^{q^n-1} \\ &= p^{p^{a-1}(pa-a-1)q^n+q^n-1} q^{nq^n p^{a-1}(p-1)+q^n-1}. \end{aligned} \tag{13}$$

We see from (13) that we only have to show that $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ is divisible by neither p nor q to complete the proof that $\mathcal{T}(x)$ is monogenic. To achieve this fact, we use Theorem 8.

We first address the prime $\rho = p$. Since $\Phi_{p^a}(t) = pq$ and

$$\begin{aligned} \Phi_{p^a}(t) &= t^{p^{a-1}(p-1)} + t^{p^{a-1}(p-2)} + \cdots + t^{p^{a-1}} + 1 \\ &\equiv t^{p-1} + t^{p-2} + \cdots + t + 1 \pmod{p} \\ &\equiv \begin{cases} 0 \pmod{p} & \text{if } t \equiv 1 \pmod{p} \\ t\left(\dfrac{t^{p-1}-1}{t-1}\right) + 1 \pmod{p} \equiv 1 \pmod{p} & \text{otherwise,} \end{cases} \end{aligned}$$

we conclude that $t \equiv 1 \pmod{p}$. Then, using Theorem 6, we have that

$$\begin{aligned} \mathcal{T}(x) &= \Phi_1\left(\left((x-t)^{q^n} + t\right)^{p^a}\right) \\ &\equiv \left(\Phi_1\left((x-t)^{q^n} + t\right)\right)^{p^a} \pmod{p} \\ &\equiv \left((x-t)^{q^n} + t - 1\right)^{p^a} \pmod{p} \\ &\equiv (x-1)^{p^a q^n} \pmod{p}. \end{aligned}$$

That is, we may let $G(x) = x - 1$ in Theorem 8, so that

$$F(x) = \frac{(x-1)^{p^a q^n} - \mathcal{T}(x)}{p}$$

in Theorem 8. Thus, since $(1-t)^{q^n} \equiv 0 \pmod{p^2}$, it follows that

$$\mathcal{T}(1) = \Phi_{p^a}\left((1-t)^{q^n} + t\right) \equiv \Phi_{p^a}(t) \equiv pq \not\equiv 0 \pmod{p^2}.$$

Hence, $\overline{F}(1) = -q$, which implies that $\gcd(\overline{F}, \overline{G}) = 1$. We then deduce from Theorem 8 that

$$[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{p}.$$

We now address the prime q. Since $\Phi_{p^a}(t) = pq$, we have that

$$\Phi_{p^a}(t) = t^{p^{a-1}(p-1)} + t^{p^{a-1}(p-2)} + \cdots + t^{p^{a-1}} + 1 \equiv 0 \pmod{q}. \tag{14}$$

Thus,

$$t^{p^a} - 1 = \left(t^{p^{a-1}} - 1\right)\Phi_{p^a}(t) \equiv 0 \pmod{q},$$

so that $p^a \equiv 0 \pmod{\operatorname{ord}_q(t)}$. If $\operatorname{ord}_q(t) < p^a$, then $t^{p^{a-1}} \equiv 1 \pmod{q}$. But then we have that $p \equiv 0 \pmod{q}$ from (14), which yields the contradiction that $p = q$.

Therefore, $\operatorname{ord}_q(t) = p^a$, which implies that $q \equiv 1 \pmod{p^a}$ and $\operatorname{ord}_{p^a}(q) = 1$. Thus, using part (3) of Theorem 6, it follows that

$$\overline{\mathcal{T}}(x) = \Phi_{p^a}\left((x-t)^{q^n} + t^{q^n}\right) = (\Phi_{p^a}(x))^{q^n} = \left(\prod_{j \in J_{p^a}} (x - t^j)\right)^{q^n}. \tag{15}$$

Hence, in Theorem 8, we can let

$$G(x) = \prod_{j \in J_{p^a}} (x - t^j) \quad \text{and} \quad H(x) = \left(\prod_{j \in J_{p^a}} (x - t^j)\right)^{q^n - 1},$$

so that

$$qF(x) = \left(\prod_{j \in J_{p^a}} (x - t^j)\right)^{q^n} - \mathcal{T}(x).$$

By condition 2((B))iv, we have that $\mathcal{T}(t^j) \not\equiv 0 \pmod{q^2}$. Therefore, $\gcd(\overline{F}, \overline{G}) = 1$, and so

$$[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q}$$

by Theorem 8, which completes the proof that $\mathcal{T}(x)$ is monogenic for part (B).

Finally, we address part (C) where $N = p \equiv 3 \pmod 4$ is prime, $\Phi_N(t) = q = m$ for some positive integer $t \equiv 0 \pmod p$, and prime $q > p$, such that p is a primitive root modulo q^2. Note that the condition $p \equiv 3 \pmod 4$ is necessary for p to be a primitive root modulo q^2. To see this, suppose that $p \equiv 1 \pmod 4$. Since $t \equiv 0 \pmod p$, we have that $q \equiv 1 \pmod p$. Thus, by quadratic reciprocity and Euler's criterion, it follows that

$$p^{(q-1)/2} \equiv \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{1}{p}\right) = 1 \pmod q,$$

where $\left(\frac{*}{p}\right)$ is the Legendre symbol modulo p. Thus, p is not a primitive root modulo q, and hence, not a primitive root modulo q^2.

Let

$$\mathcal{T}(x) := T_n(x+t) = \Phi_p\left(f_{q,t}^n(x)\right) = \Phi_p\left(x^{q^n} + t\right), \tag{16}$$

and let $\mathbb{Z}_K$ denote the ring of integers of $K = \mathbb{Q}(\theta)$, where $\mathcal{T}(\theta) = 0$. To complete the proof that $T_n(x)$ is monogenic, it will suffice to show that $\mathcal{T}(x)$ is monogenic. By Theorem 7 and part (2) of Theorem 6, we have that

$$|\Delta(\mathcal{T})| = p^{(p-2)q^n} q^{n(p-1)q^n + q^n - 1}. \tag{17}$$

As in the other situations, we see from (17) that to establish the monogeneity of $\mathcal{T}(x)$ we only have to show that

$$[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{\rho}$$

for $\rho \in \{p, q\}$ in Theorem 8.

Suppose first that $\rho = p$. Then, since $t \equiv 0 \pmod{p}$, we see from (16) that

$$\begin{aligned}
\mathcal{T}(x) &\equiv \Phi_p\left(x^{q^n}\right) \pmod{p} \\
&\equiv \frac{(x^{q^n})^p - 1}{x^{q^n} - 1} \pmod{p} \\
&\equiv \frac{(x^{q^n} - 1)^p}{x^{q^n} - 1} \pmod{p} \\
&\equiv (x^{q^n} - 1)^{p-1} \pmod{p} \\
&\equiv \left(\Phi_1(x)\Phi_q(x)\Phi_{q^2}(x)\cdots\Phi_{q^n}(x)\right)^{p-1} \pmod{p}.
\end{aligned}$$

Since p is a primitive root modulo q^2, we conclude that p is a primitive root modulo q^e for all $e \geq 1$ [3]. That is, $\mathrm{ord}_{q^e}(p) = \phi(q^e)$ for all $e \geq 1$, and consequently, it follows from part (3) of Theorem 6 that $\Phi_{q^e}(x)$ is irreducible modulo p. Thus, we may let

$$G(x) = \Phi_1(x)\Phi_q(x)\Phi_{q^2}(x)\cdots\Phi_{q^n}(x) = x^{q^n} - 1 \tag{18}$$

$$\text{and } H(x) = \left(\Phi_1(x)\Phi_q(x)\Phi_{q^2}(x)\cdots\Phi_{q^n}(x)\right)^{p-2} = \left(x^{q^n} - 1\right)^{p-2}$$

in Theorem 8. Then,

$$\begin{aligned}
F(x) &= \frac{G(x)H(x) - \mathcal{T}(x)}{p} \\
&= \frac{(x^{q^n} - 1)^{p-1} - \sum_{k=0}^{p-1}(x^{q^n} + t)^k}{p} \\
&= \sum_{k=1}^{p-2}(-1)^k \left(\frac{\binom{p-1}{k} + (-1)^{k-1}}{p}\right)(x^{q^n})^k - \frac{t}{p}\sum_{k=1}^{p-1} k(x^{q^n})^{k-1} - \frac{R}{p},
\end{aligned}$$

where $R \equiv 0 \pmod{p^2}$, since $t \equiv 0 \pmod{p}$ and every coefficient of R is divisible by t^2. Note also that

$$\binom{p-1}{k} \equiv \begin{cases} 1 \pmod{p} & \text{if } k \equiv 0 \pmod{2} \\ -1 \pmod{p} & \text{if } k \equiv 1 \pmod{2}, \end{cases}$$

follows easily from Wilson's theorem. Hence,

$$\overline{F}(x) = \sum_{k=1}^{p-2}(-1)^k \overline{\left(\frac{\binom{p-1}{k} + (-1)^{k-1}}{p}\right)}(x^{q^n})^k - \overline{\left(\frac{t}{p}\right)}\sum_{k=1}^{p-1} k(x^{q^n})^{k-1}. \tag{19}$$

Suppose, by way of contradiction, that $\gcd(\overline{F}, \overline{G}) > 1$. Then, there exists α in an algebraic closure of $\mathbb{F}_p$ such that

$$\overline{G}(\alpha) = \overline{F}(\alpha) = 0. \tag{20}$$

Since $\overline{G}(\alpha) = 0$, we see from (18) that $\alpha^{q^n} \equiv 1 \pmod{p}$. Thus, from (19) and the fact that $\sum_{k=1}^{p-1} k \equiv 0 \pmod{p}$, we have that

$$\begin{aligned}\overline{F}(\alpha) &= \sum_{k=1}^{p-2}(-1)^k \overline{\left(\frac{\binom{p-1}{k} + (-1)^{k-1}}{p}\right)} - \overline{\left(\frac{t}{p}\right)} \sum_{k=1}^{p-1} k \\ &= \sum_{k=1}^{p-2}(-1)^k \overline{\left(\frac{\binom{p-1}{k} + (-1)^{k-1}}{p}\right)}.\end{aligned} \tag{21}$$

Since $\sum_{k=1}^{p-2}(-1)^k \binom{p-1}{k} = -2$ and $\sum_{k=1}^{p-2}(-1)^{2k-1} = -(p-2)$, it follows that

$$\sum_{k=1}^{p-2}(-1)^k \left(\binom{p-1}{k} + (-1)^{k-1}\right) = -2 - (p-2) = -p.$$

Hence, $\overline{F}(\alpha) = -1$ from (21), which contradicts (20). Thus,

$$[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{p}$$

by Theorem 8.

When $\rho = q$ in Theorem 8, we impose condition 2((C))iv and the proof is similar to the proof when $\rho = q$ in part (B). Hence, we omit the details. □

4. Proof of Corollary 1

Proof. We give details only in the situation when $\Phi_{p^a}(t) = pq$, since the other cases are handled in a similar manner. From the proof of Theorem 3, we see that $\mathrm{ord}_q(t) = p^a$. Then, since

$$\frac{t^{p^a} - 1}{t^{p^{a-1}} - 1} = \Phi_{p^a}(t) = pq,$$

it follows that

$$\begin{aligned} t^{q-1} &= \left(t^{p^a}\right)^{(q-1)/p^a} \\ &= \left(pq\left(t^{p^{a-1}} - 1\right) + 1\right)^{(q-1)/p^a} \\ &= \sum_{j=0}^{(q-1)/p^a} \binom{(q-1)/p^a}{j} \left(pq\left(t^{p^{a-1}} - 1\right)\right)^j \\ &\equiv 1 - \frac{q}{p^{a-1}}\left(t^{p^{a-1}} - 1\right) \pmod{q^2} \\ &\not\equiv 1 \pmod{q^2}, \end{aligned}$$

since $t^{p^{a-1}} - 1 \not\equiv 0 \pmod{q}$. Thus, we conclude from part (1) of Theorem 3 that $f_{q,t}(x)$ is monogenically stable if and only if t is squarefree. □

5. EXAMPLES

Example 1 (Part (1) of Theorem 3)**.** *A prime q such that $t^{q-1} \equiv 1 \pmod{q^2}$, where $1 < t < q$, is called a* base-t Wieferich *prime [34]. If $t = 2$, then q is simply known as a Wieferich prime. Wieferich primes have a rich history, due in part to their connection to Fermat's Last Theorem [34]. Although currently the only known Wieferich primes are 1093 and 3511, it has been conjectured that there are infinitely many. Along these lines, Silverman [29] has shown that the abc-conjecture implies that, given any integer $t > 1$, there exist infinitely many primes q such that q is not a base-t Wieferich prime. It is easy to see from part (1) of Theorem 3 that if t is squarefree and q is not a base-t Wieferich prime, then $f_{q,t}(x)$ is monogenically stable. For an explicit example, let $t = 2$ and $q = 7$. Note that $2^{q-1} - 1 = 3^2 \cdot 7 \not\equiv 0 \pmod{49}$. Then*

$$f_{7,2}(x) = (x-2)^7 + 2$$

is monogenically stable.

Example 2 (Part (2), Conditions (A) of Theorem 3)**.** *Let $a = 3$ and $t = 2$, so that $N = 2^3$, $J_8 = \{1, 3, 5, 7\}$, $g(x) = \Phi_8(x) = x^4 + 1$, $q = g(2) = 17$ and $f_{17,2}(x) = (x-2)^{17} + 2$. Using a computer algebra system, it is easy to check for each $j \in J_8$ that*

$$\Phi_8\left(f_{17,2}(t^j)\right) \not\equiv 0 \pmod{17^2}.$$

Hence, $f_{17,2}(x)$ is g-monogenically stable. Note also that $f_{17,2}(x)$ is monogenically stable by either part (1) of Theorem 3, or Corollary 1.

Example 3 (Part (2), Conditions (B) of Theorem 3)**.** *Let $p = 3$, $a = 1$ and $t = 4$, so that $N = 3$, $J_3 = \{1, 2\}$, $g(x) = \Phi_3(x) = x^2 + x + 1$, $g(4) \equiv 0 \pmod 3$, $q = g(4)/3 = 7$ and $f_{7,4}(x) = (x-4)^7 + 4$. Using a computer algebra system, it is easy to check for each $j \in J_3$ that*

$$\Phi_3\left(f_{7,4}(t^j)\right) \not\equiv 0 \pmod{7^2}.$$

Hence, $f_{7,4}(x)$ is g-monogenically stable. Note also that $f_{7,4}(x)$ is **not** *monogenically stable by Corollary 1 since $t = 4$ is not squarefree.*

Example 4 (Part (2), Conditions (B) of Theorem 3)**.** *Let $p = 5$, $a = 2$ and $t = 46$, so that*

- $N = 5^2$
- $J_{25} = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$
- $g(x) = \Phi_{25}(x) = x^{20} + x^{15} + x^{10} + x^5 + 1$
- $g(t) = 5q = 5 \cdot 3599039651469197294471372718147 01.$

Using a computer algebra system, it is easy to check for each $j \in J_{25}$ that

$$\Phi_N\left(f_{q,t}(t^j)\right) \not\equiv 0 \pmod{q^2}.$$

Hence, $f_{q,t}(x)$ is g-monogenically stable. Note also that $f_{q,t}(x)$ is monogenically stable by Corollary 1 since $t = 46$ is squarefree.

Example 5 (Part (2), Conditions (C) of Theorem 3)**.** *Let $p = 7$ and $t = 126$, so that*

- $N = p = 7$
- $J_7 = \{1, 2, 3, 4, 5, 6\}$
- $g(x) = \Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
- $g(t) = q = 4033516174507$

It is easy to see, using a computer algebra system, that 7 is a primitive root modulo 4033516174507^2*, and it is also easy to check for each* $j \in J_7$ *that*

$$\Phi_7\left(f_{4033516174507,126}(126^j)\right) \not\equiv 0 \pmod{4033516174507^2}.$$

Hence, $f_{4033516174507,126}(x)$ *is g-monogenically stable. Note also that* $f_{q,t}(x)$ *is* **not** *monogenically stable by Corollary 1 since* $t = 126 = 2 \cdot 3^2 \cdot 7$ *is not squarefree.*

REFERENCES

[1] S. Ahmad, T. Nakahara and A. Hameed, On certain pure sextic fields related to a problem of Hasse, *Internat. J. Algebra Comput.* **26** (2016), no. 3, 577–583.

[2] S. Ahmad, T. Nakahara and S. M. Husnine, Power integral bases for certain pure sextic fields, *Int. J. Number Theory* **10** (2014), no. 8, 2257–2265.

[3] D. Burton, *Elementary Number Theory, 7e*, McGraw-Hill, 2011.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 2000.

[5] J. Cullinan, The discriminant of a composition of two polynomials, https://studylib.net/doc/8187082/the-discriminant-of-a-composition-of-two

[6] D. Eloff, B. Spearman and K. Williams, A_4-sextic fields with a power basis, *Missouri Journal of Mathematical Sciences* **19** (2007), 188–194.

[7] I. Gaál and L. Remete, Power integral bases in a family of sextic fields with quadratic subfields, *Tatra Mt. Math. Publ.* **64** (2015), 59–66.

[8] I. Gaál and L. Remete, Integral bases and monogenity of pure fields, *J. Number Theory* **173** (2017), 129–146.

[9] T. A. Gassert, A note on the monogeneity of power maps, *Albanian J. Math* **11** (2017), no. 1, 3–12.

[10] W. J. Guerrier, The factorization of the cyclotomic polynomials mod p, Amer. Math. Monthly **75** (1968) 46.

[11] P. Haggard and J. Kiltinen, Binomial expansions modulo prime powers, *Internat. J. Math. Math. Sci.* **3** (1980), no. 2, 397–400.

[12] J. Harrington and L. Jones, Monogenic binomial compositions, *Taiwanese J. Math.* **24** (2020), no. 5, 1073–1090.

[13] J. Harrington and L. Jones, Monogenic cyclotomic compositions, *Kodai Math. J.* **44**, (2021) 115–125.

[14] L. Jones, A brief note on some infinite families of monogenic polynomials, *Bull. Aust. Math. Soc.* **100** (2019), no. 2, 239–244.

[15] L. Jones, Monogenic polynomials with non-squarefree discriminant, *Proc. Amer. Math. Soc.* **148** (2020), no. 4, 1527–1533.

[16] L. Jones, Generating infinite families of monogenic polynomials using a new discriminant formula, *Albanian Journal of Mathematics* **14** (2020), no. 1, 37–45.

[17] L. Jones, Some new infinite families of monogenic polynomials with non-squarefree discriminant, *Acta Arith.* **197** (2021), no. 2, 213–219.

[18] L. Jones and T. Phillips, Infinite families of monogenic trinomials and their Galois groups, *Internat. J. Math.* **29** (2018), no. 5, 1850039, 11 pp.

[19] L. Jones and D. White, Monogenic trinomials with non-squarefree discriminant, arXiv:1908.07947v1.

[20] R. Jones, The density of prime divisors in the arithmetic dynamics of quadratic polynomials, *J. Lond. Math. Soc.* (2) **78** (2008), no. 2, 523–544.

[21] K. Kedlaya, A construction of polynomials with squarefree discriminants, *Proc. Amer. Math. Soc.* **140** (2012), no. 9, 3025–3033.

[22] M. Lavallee, B. Spearman and Q. Yang, $PSL(2,7)$ septimic fields with a power basis, *J. Théor. Nombres Bordeaux* **24** (2012), no. 2, 369–375.

[23] M. Lavallee, B. Spearman, K. Williams and Q. Yang, Dihedral quintic fields with a power basis, *Math. J. Okayama Univ.* **47** (2005), 75–79.

[24] T. Nagell, Introduction to Number Theory, New York: Wiley, 1951.

[25] R. Odoni, On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$, *J. London Math. Soc.* (2) **32** (1985), no. 1, 1–11.

[26] R. Odoni, The Galois theory of iterates and composites of polynomials, *Proc. London Math. Soc.* (3) **51** (1985), no. 3, 385–414.

[27] B. Rice, Primitive prime divisors in polynomial arithmetic dynamics, *Integers* **7** (2007), A26, 16 pp.
[28] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications, **77**, Cambridge University Press, Cambridge, 2000.
[29] J. H. Silverman, Wieferich's criterion and the abc-conjecture, *J. Number Theory* **30** (1988), no. 2, 226–237.
[30] B. Spearman, Monogenic A_4 quartic fields, *Int. Math. Forum* **1** (2006), no. 37–40, 1969–1974.
[31] B. Spearman, A. Watanabe and K. Williams, $PSL(2,5)$ sextic fields with a power basis, *Kodai Math. J.* **29** (2006), no. 1, 5–12.
[32] B. Spearman and K. Williams, Cubic fields with a power basis, *Rocky Mountain J. Math.* **31** (2001), no. 3, 1103–1109.
[33] L. C. Washington, *Introduction to cyclotomic fields, Second edition*, Graduate Texts in Mathematics, **83**, Springer-Verlag, New York, 1997.
[34] https://en.wikipedia.org/wiki/Wieferich_prime

Current address: 193 Summer Breeze Lane, Chambersburg, PA 17202