TAIWANESE JOURNAL OF MATHEMATICS
Vol. 24, No. 5, pp. 1073–1090, October 2020
DOI: 10.11650/tjm/200201

Monogenic Binomial Compositions

Joshua Harrington and Lenny Jones*

Abstract. We say a monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$ is *monogenic* if $f(x)$ is irreducible over $\mathbb{Q}$ and $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a basis for the ring of integers of $\mathbb{Q}(\theta)$, where $f(\theta) = 0$. In this article, we investigate when a pair of polynomials $f(x) = x^n - a$ and $g(x) = x^m - b$ has the property that $f(x)$ and $f(g(x))$ are monogenic.

1. Introduction

In this article, unless stated otherwise, when we say a polynomial $f(x) \in \mathbb{Z}[x]$ is "irreducible", we mean irreducible over $\mathbb{Q}$. Suppose that $f(x)$ is irreducible with $\deg(f) = n \geq 2$ and $f(\theta) = 0$. We let $\Delta(*)$ denote the discriminant over $\mathbb{Q}$ of $* \in \{\theta, f, K\}$, where $K = \mathbb{Q}(\theta)$. Then the following equation is well-known [6]:

$$\Delta(f) = \Delta(\theta) = \big[\mathbb{Z}_K : \mathbb{Z}[\theta]\big]^2 \Delta(K), \tag{1.1}$$

where $\mathbb{Z}_K$ is the ring of integers of K. We say a monic polynomial $f(x) \in \mathbb{Z}[x]$ is *monogenic* if $f(x)$ is irreducible and $\big[\mathbb{Z}_K : \mathbb{Z}[\theta]\big] = 1$; or, equivalently from (1.1), that $\Delta(f) = \Delta(K)$. In this situation, $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a basis for $\mathbb{Z}_K$ referred to as a *power basis*. We say that a field K is *monogenic*, if there exists an irreducible polynomial $f(x)$ with $f(\alpha) = 0$, such that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $\mathbb{Z}_K$. There is a subtle difference here and we caution the reader that although $f(x)$ being monogenic implies that $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$, is monogenic, the converse is false. For example, let $f(x) = x^2 - 5$ with $f(\alpha) = 0$ and $g(x) = x^2 - x - 1$ with $g(\beta) = 0$. Observe that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, and let $K = \mathbb{Q}(\alpha)$. Note that $g(x)$ is monogenic since it is well-known [21] that $\{1, \beta\}$ is an integral basis for $\mathbb{Z}_K$. Consequently, K is monogenic. However $f(x)$ is not monogenic since $\{1, \alpha\}$ is not an integral basis for $\mathbb{Z}_K$ [21].

The existence of a power basis facilitates calculations in $\mathbb{Z}_K$. A classic example is the cyclotomic field $K = \mathbb{Q}(\zeta)$, where ζ is a primitive nth root of unity [30]. We see from (1.1) that if $\Delta(f)$ is squarefree (that is, an integer not divisible by the square of any integer larger than 1), then f is monogenic. For any fixed degree $n \geq 2$, the density of monogenic

Received November 6, 2019; Accepted February 5, 2020.
Communicated by Yu-Ru Liu.
2010 *Mathematics Subject Classification.* Primary: 11R04; Secondary: 11R09.
Key words and phrases. monogenic, irreducible, composition.
*Corresponding author.

polynomials is $6/\pi^2 \approx .607927$ [4]. However, determining infinite families of degree-n monogenic polynomials can be difficult, and much research has been done to locate such families [1, 2, 5, 8, 10, 12, 13, 16, 17, 23, 29].

Despite the difficulty in determining conditions under which a single family of degree-n monogenic polynomials exists, we are inspired by research concerning power bases of relative extensions [9, 11, 14, 15, 19, 26] to ask the following related question:

$$\begin{gathered}\text{Is it possible to characterize polynomial pairs } (f,g)\\ \text{such that both } f(x) \text{ and } f(g(x)) \text{ are monogenic?}\end{gathered} \tag{1.2}$$

We see that, with $g(x) = x$, (1.2) encompasses the original question concerning the search for infinite families of degree-n monogenic polynomials. Therefore, we would expect a complete answer to (1.2) to be intractable. Nevertheless, progress is possible under suitable restrictions. We focus here on the situation when both $f(x)$ and $g(x)$ in (1.2) are binomials. It is perhaps somewhat surprising that, without further restrictions, even this seemingly easy setting is extremely complicated. The following recent result of Gassert [17], which can be viewed as the special case of (1.2) with $g(x) = x$ and $f(x) = x^n - a$, provides both evidence for this complexity and motivation for our investigations.

Theorem 1.1. [17] *For any integer $n > 1$, the polynomial $x^n - a \in \mathbb{Z}[x]$ is monogenic if and only if a is squarefree and $a^p \not\equiv a \pmod{p^2}$ for all primes p dividing n.*

Remark 1.2. Bardestani [3] had previously examined the situation when both n and a are primes.

In this article, we use Theorem 1.1 and some additional new machinery to give sets of conditions for when both $f(x) = x^n - a$ and $\mathcal{T}(x) := f(g(x)) = (x^m - b)^n - a$ are monogenic, under certain restrictions on a, b, m, n. Each of our three main theorems provides an easy and quick algorithmic test to determine when $f(x)$ and $\mathcal{T}(x)$ are monogenic; and, with the exception of the calculation of primitive sixth roots of unity modulo a prime in the third theorem, these tests involve only the coefficients and the degrees of the polynomials in the composition. More precisely, we prove

Theorem 1.3. *Let $a, b, m, n \in \mathbb{Z}$ with $m, n \geq 2$, and let $\kappa(*)$ denote the squarefree kernel of $*$. Let $f(x) = x^n - a$, $g(x) = x^m - b$ and $\mathcal{T}(x) = f(g(x))$. If*

(1) *a is squarefree,*

(2) *$a^p \not\equiv a \pmod{p^2}$ for all primes p dividing n, and*

(3) *$\kappa(|m((-b)^n - a)|)$ divides an,*

then $f(x)$ and $\mathcal{T}(x)$ are monogenic.

While the conditions given in Theorem 1.3 are sufficient, the conditions given in Theorems 1.4 and 1.5 are both necessary and sufficient.

Theorem 1.4. *Let $a, b, m \in \mathbb{Z}$ with $a \neq 0$ and $m \geq 2$, and let $\widehat{m} = m/\gcd(2a, m)$. Let $f(x) = x^2 - a$, $g(x) = x^m - b$, $\mathcal{T}(x) = f(g(x))$ and suppose that $\kappa(|am|) = \kappa(|b^2 - a|)$, where $\kappa(*)$ denotes the squarefree kernel of the positive integer $*$. Then $f(x)$ and $\mathcal{T}(x)$ are monogenic if and only if all of the following conditions hold:*

(1) *a is squarefree,*

(2) *$a \not\equiv 1 \pmod 4$,*

(3) *$b^2 - a \not\equiv 0 \pmod{p^2}$ for all primes p dividing $\widehat{m}$,*

(4) *$-(2b)^{p+1} + 3b^2 + a \not\equiv 0 \pmod{p^2}$ for all primes p dividing $\widehat{m}$.*

The polynomials $\mathcal{T}(x)$ in Theorem 1.4 are trinomials and much research has been conducted concerning the mongeneity of trinomials (see [24] and the references therein). Although necessary and sufficient conditions for a trinomial to be monogenic have been given in [22], Theorem 1.4 gives easier and more straightforward conditions to check the monogeneity of the particular trinomials in Theorem 1.4. We should also point out that there is no overlap with the trinomials in a more recent examination in [25] and the trinomials arising from Theorem 1.4.

Theorem 1.5. *Let $a, b, m \in \mathbb{Z}$ with $a \neq 0$ and $m \geq 2$, and let $\widehat{m} = m/\gcd(3a, m)$. Let $f(x) = x^3 - a$, $g(x) = x^m - b$, $\mathcal{T}(x) = f(g(x))$ and suppose that $\kappa(|am|) = \kappa(|b^3 + a|)$, where $\kappa(*)$ denotes the squarefree kernel of the positive integer $*$. Then $f(x)$ and $\mathcal{T}(x)$ are monogenic if and only if all of the following conditions hold:*

(1) *a is squarefree,*

(2) *$a \not\equiv \pm 1 \pmod 9$,*

(3) *$b^3 + a \not\equiv 0 \pmod{p^2}$ for all primes p dividing $\widehat{m}$,*

(4) *$a \not\equiv 3 \pmod 4$ or $b \not\equiv 3 \pmod 4$ if $\widehat{m} \equiv 0 \pmod 2$,*

(5) *$A\zeta + B + b^3 + a \not\equiv 0 \pmod{p^2}$ for all primes p dividing $\widehat{m}$ with $p \equiv 1 \pmod 6$ and each primitive sixth root of unity ζ modulo p, where*

$$A = (-1)^{(p+1)/2} 2 \cdot 3^{(3p-1)/2} b^{3p} + 3^{p+1} b^{2p+1} + (-3)^{(p+1)/2} b^{p+2},$$
$$B = (-1)^{(p-1)/2} 3^{(3p-1)/2} b^{3p} + (-3)^{(p+1)/2}.$$

Although the following corollary, whose proof we omit, is not much more than an observation from Theorems 1.4 and 1.5, we state it formally to point out the fact that it prescribes a method for constructing infinite collections of monogenic or non-monogenic polynomials from these theorems. These collections are not "families" in the traditional sense of the literature since the members of each collection here have distinct degree.

Corollary 1.6. *Suppose that $f(x)$ and $\mathcal{T}(x) = f(x^m - b)$ are polynomials such that all hypotheses and conditions of Theorem* 1.4*, respectively Theorem* 1.5*, are satisfied. Then the polynomial $\mathcal{T}(x^{m^k})$ is monogenic for all integers $k \geq 1$. Similarly, suppose that $f(x)$ and $\mathcal{T}(x) = f(x^m - b)$ are polynomials such that all hypotheses of Theorem* 1.4*, respectively Theorem* 1.5*, are satisfied, but that at least one of the conditions of Theorem* 1.4*, respectively Theorem* 1.5*, fails to hold. Then the polynomial $\mathcal{T}(x^{m^k})$ is not monogenic for all integers $k \geq 1$.*

All computer computations in this article were done using either MAGMA, Maple or Sage.

2. Basic preliminaries

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

Theorem 2.1. *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Q}[x]$ with $f(x)$ irreducible. Suppose that $f(\alpha) = 0$. Then $f(g(x))$ is reducible over $\mathbb{Q}$ if and only if $g(x) - \alpha$ is reducible over $\mathbb{Q}(\alpha)$.*

Theorem 2.2. *Let $r \in \mathbb{Z}$ with $r \geq 2$, and let $\alpha \in \mathbb{C}$ be algebraic. Then $x^r - \alpha$ is reducible over $\mathbb{Q}(\alpha)$ if and only if either there is a prime p dividing r such that $\alpha = \beta^p$ for some $\beta \in \mathbb{Q}(\alpha)$ or $4 \mid r$ and $\alpha = -4\beta^4$ for some $\beta \in \mathbb{Q}(\alpha)$.*

Theorem 2.3. (Dedekind [6]) *Let $K = \mathbb{Q}(\theta)$ be a number field, $T(x) \in \mathbb{Z}[x]$ the monic minimal polynomial of θ, and $\mathbb{Z}_K$ the ring of integers of K. Let p be a prime number and let $\overline{*}$ denote reduction of $*$ modulo p (in $\mathbb{Z}$, $\mathbb{Z}[x]$ or $\mathbb{Z}[\theta]$). Let*

$$\overline{T}(x) = \prod_{i=1}^{k} \overline{t_i}(x)^{e_i}$$

be the factorization of $T(x)$ modulo p in $\mathbb{F}_p[x]$, and set

$$g(x) = \prod_{i=1}^{k} t_i(x),$$

where the $t_i(x) \in \mathbb{Z}[x]$ *are arbitrary monic lifts of the* $\overline{t_i}(x)$*. Let* $h(x) \in \mathbb{Z}[x]$ *be a monic lift of* $\overline{T}(x)/\overline{g}(x)$ *and set*

$$F(x) = \frac{g(x)h(x) - T(x)}{p} \in \mathbb{Z}[x].$$

Then

$$\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \not\equiv 0 \pmod{p} \iff \gcd(\overline{F}, \overline{g}, \overline{h}) = 1 \quad \text{in } \mathbb{F}_p[x].$$

In general, Theorem 2.3 does not give enough information to determine if K is monogenic. However, Theorem 2.3 does give precisely the information needed to determine if $T(x)$ is monogenic. That is,

Corollary 2.4. *$T(x)$ is monogenic if and only if* $\gcd(\overline{F}, \overline{g}, \overline{h}) = 1$ *in Theorem 2.3 for every prime p such that* $\Delta(T) \equiv 0 \pmod{p}$.

3. Proofs of Theorems 1.3, 1.4 and 1.5

Before embarking on the proof of the main theorems, we require some additional machinery. The first lemma, which we state without proof, gives a formula for the absolute value of the discriminant of the composition of two monic binomials.

Lemma 3.1. *Let* $a, b, m, n \in \mathbb{Z}$ *with* $m, n \geq 1$*. Let* $f(x) = x^n - a$*,* $g(x) = x^m - b$ *and* $\mathcal{T}(x) = f(g(x))$*. Then*

$$|\Delta(\mathcal{T})| = |(mn)^{mn} a^{m(n-1)} ((-b)^n - a)^{m-1}|.$$

Lemma 3.1 follows from the formula for the discriminant of the composition of two arbitrary polynomials which is, as far as we can determine, originally due to John Cullinan [7]. A proof of Lemma 3.1, as well as a proof of the more general result, can be found in [19].

The following lemma gives sufficient conditions for the irreducibility of $\mathcal{T}(x)$ when $f(x)$ is irreducible.

Lemma 3.2. *Let* $a, b, m, n \in \mathbb{Z}$ *with* $m, n \geq 1$*. Let* $f(x) = x^n - a$ *and* $g(x) = x^m - b$ *with $f(x)$ irreducible. If* $|(-b)^n - a| \neq y^p$ *and* $|(-b)^n - a| \neq 4^n y^4$ *for any integer* $y \geq 1$ *and any prime p dividing m, then $\mathcal{T}(x)$ is irreducible.*

Proof. By way of contradiction, assume that $\mathcal{T}(x) = f(g(x))$ is reducible. Suppose that $f(\alpha) = 0$ so that $\alpha^n = a$. Then, by Theorem 2.1, $g(x) - \alpha$ is reducible over $\mathbb{Q}(\alpha)$. Thus, by Theorem 2.2, we have that either $\alpha + b = \beta^p$ for some $\beta \in \mathbb{Q}(\alpha)$ and some prime p dividing m, or $m \equiv 0 \pmod{4}$ and $\alpha + b = -4\beta^4$ for some $\beta \in \mathbb{Q}(\alpha)$. Suppose that $\alpha + b = \beta^p$

for some $\beta \in \mathbb{Q}(\alpha)$ and some prime p dividing m. Then, since $(x-b)^n - a$ is the minimal polynomial for $\alpha + b$, we deduce by taking the norm, which we denote as $\mathcal{N}$, that

$$|(-b)^n - a| = |\mathcal{N}(\alpha + b) = |\mathcal{N}(\beta)|^p,$$

which is a contradiction since $|\mathcal{N}(\beta)| \in \mathbb{Z}$. A similar contradiction is reached using Theorem 2.2 if $m \equiv 0 \pmod 4$ and $\alpha + b = -4\beta^4$ for some $\beta \in \mathbb{Q}(\alpha)$. □

In the next two lemmas, we examine the relationship between the monogeneity of $f(x) = x^n - a$ and the monogeneity of $\mathcal{T}(x) = f(g(x))$. In particular, the first lemma shows that the monogeneity of $f(x)$ is necessary for the monogeneity of $\mathcal{T}(x)$.

Lemma 3.3. *Let $f(x) = x^n - a \in \mathbb{Z}[x]$, $g(x) \in \mathbb{Z}[x]$, and $\mathcal{T}(x) = f(g(x))$. If $\mathcal{T}(x)$ is monogenic then $f(x)$ is monogenic.*

Proof. We prove the contrapositive. If $\mathcal{T}(x)$ is reducible, then $\mathcal{T}(x)$ is not monogenic. So, suppose that $\mathcal{T}(x)$ is irreducible. Let $\mathcal{T}(\theta) = 0$, $K = \mathbb{Q}(\theta)$ and $\mathbb{Z}_K$ denote the ring of integers of K. Since $f(x)$ is not monogenic, we have by Theorem 1.1 that either a is not squarefree or $a^p \equiv a \pmod{p^2}$ for some prime p dividing n. In each of these two cases, we calculate for $\mathcal{T}(x)$ the polynomial $F(x)$ in Theorem 2.3, and we denote it as $F_{\mathcal{T}}(x)$. Suppose first that a is not squarefree and that p is a prime such that $a \equiv 0 \pmod{p^2}$. Then

$$\overline{\mathcal{T}}(x) \equiv g(x)^n \equiv \left(\prod_i \overline{\tau_i}(x)^{e_i} \right)^n \pmod p, \tag{3.1}$$

where the $\overline{\tau_i}(x)$ are irreducible modulo p. Thus,

$$F_{\mathcal{T}}(x) = \frac{\left(\prod_i \tau_i(x)^{e_i}\right)^n - (g(x)^n - a)}{p} = \frac{\left(\prod_i \tau_i(x)^{e_i}\right)^n - g(x)^n}{p} + \frac{a}{p},$$

where the $\tau_i(x)$ are arbitrary monic lifts of the $\overline{\tau_i}(x)$. If α is a zero of any $\overline{\tau_i}(x)$ in an algebraic closure of $\mathbb{F}_p$, then $\tau_i(\alpha) \equiv 0 \pmod p$. Therefore, from (3.1), we have that

$$\left(\prod_i \tau_i(\alpha)^{e_i} \right)^n \equiv g(\alpha)^n \equiv 0 \pmod{p^2},$$

since $n \geq 2$. Consequently, $\overline{F_{\mathcal{T}}}(\alpha) \equiv 0 \pmod p$, which implies that $\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \equiv 0 \pmod p$ and $\mathcal{T}(x)$ is not monogenic by Corollary 2.4.

Now, suppose that $a^p \equiv a \pmod{p^2}$ for some prime p dividing n. Then

$$\overline{\mathcal{T}}(x) \equiv (g(x)^{n/p} - a)^p \equiv \left(\prod_i \overline{\tau_i}(x)^{e_i} \right)^p \pmod p, \tag{3.2}$$

where the $\overline{\tau_i}(x)$ are irreducible modulo p. Hence,

$$F_{\mathcal{T}}(x) = \frac{\left(\prod_i \tau_i(x)^{e_i}\right)^p - (g(x)^n - a)}{p},$$

where the $\tau_i(x)$ are arbitrary monic lifts of the $\overline{\tau_i}(x)$. If α is a zero of any $\overline{\tau_i}(x)$ in an algebraic closure of $\mathbb{F}_p$, then $\tau_i(\alpha) \equiv 0 \pmod{p}$ so that $\left(\prod_i \tau_i(x)^{e_i}\right)^p \equiv 0 \pmod{p^2}$ since $p \geq 2$. Additionally, from (3.2), we have that $g(\alpha)^{n/p} \equiv a \pmod{p}$, which implies that

$$g(\alpha)^n \equiv a^p \equiv a \pmod{p^2}.$$

Thus,

$$\overline{F_{\mathcal{T}}}(\alpha) \equiv \frac{\left(\prod_i \tau_i(\alpha)^{e_i}\right)^p}{p} - \frac{g(\alpha)^n - a}{p} \equiv 0 \pmod{p},$$

so that $\mathcal{T}(x)$ is not monogenic by Corollary 2.4 in this case as well. □

Although the full converse of Lemma 3.3 is not true, the next result shows that, if $f(x) = x^n - a$ is monogenic, we only need to check primes that do not divide $\Delta(f)$ when using Corollary 2.4 to determine whether $\mathcal{T}(x) = f(g(x))$ is monogenic.

Lemma 3.4. *Let $f(x) = x^n - a \in \mathbb{Z}[x]$ and $g(x) \in \mathbb{Z}[x]$. Suppose that $\mathcal{T}(x) = f(g(x))$ is irreducible, $\mathcal{T}(\theta) = 0$, $K = \mathbb{Q}(\theta)$ and $\mathbb{Z}_K$ is the ring of integers of K. If $f(x)$ is monogenic, then*

$$\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \not\equiv 0 \pmod{p} \quad \textit{for all primes } p \textit{ such that } \Delta(f) \equiv 0 \pmod{p}.$$

Proof. From Lemma 3.1, we have that

$$|\Delta(f)| = |n^n a^{n-1}|.$$

For each of the polynomials $\mathcal{T}(x)$ and $f(x)$, we calculate the polynomial $F(x)$ in Theorem 2.3, first for a prime divisor of n, and then for a prime divisor of a. For each of these primes, we denote this polynomial $F(x)$ respectively as $F_{\mathcal{T}}(x)$ and $F_f(x)$. Suppose first that p is a prime that divides n. Then

$$\overline{\mathcal{T}}(x) \equiv (g(x)^{n/p} - a)^p \equiv \left(\prod_i \overline{\tau_i}(x)^{e_i}\right)^p \pmod{p},$$

where the $\overline{\tau_i}(x)$ are irreducible modulo p. Thus,

$$\prod_i \tau_i(x)^{e_i} = g(x)^{n/p} - a + pr(x)$$

for some polynomial $r(x)$, where the $\tau_i(x)$ are arbitrary monic lifts of the $\overline{\tau}_i(x)$. Hence, in Theorem 2.3, we have that

$$\begin{aligned} F_{\mathcal{T}}(x) &= \frac{\left(\prod_{i=1}^{k}\tau_i(x)^{e_i}\right)^p - (g(x)^n - a)}{p} \\ &= \frac{(g(x)^{n/p} - a + pr(x))^p - (g(x)^n - a)}{p} \\ &= \frac{a + (-a)^p}{p} + \sum_{j=1}^{p-1}\frac{\binom{p}{j}}{p}(-1)^j a^j (g(x)^{n/p})^{p-j} \\ &\quad + \sum_{j=1}^{p-1}\frac{\binom{p}{j}}{p}p^j r(x)^j (g(x)^{n/p} - a)^{p-j} + p^{p-1}r(x)^p. \end{aligned}$$

Therefore,

$$\overline{F_{\mathcal{T}}}(x) \equiv \frac{a + (-a)^p}{p} + \sum_{j=1}^{p-1}\frac{\binom{p}{j}}{p}(-1)^j a^j (g(x)^{n/p})^{p-j} \pmod{p}. \tag{3.3}$$

Similarly, we have that

$$\overline{f}(x) \equiv (x^{n/p} - a)^p \equiv \left(\prod_i t_i(x)^{e_i}\right)^p \equiv (x^{n/p} - a + ps(x))^p \pmod{p} \tag{3.4}$$

for some polynomial $s(x)$, where the $t_i(x)$ are arbitrary monic lifts of the irreducible factors $\overline{t}_i(x)$ of $\overline{f}(x)$. Then the expansion of the right-hand side of (3.4) yields

$$\overline{F_f}(x) \equiv \frac{a + (-a)^p}{p} + \sum_{j=1}^{p-1}\frac{\binom{p}{j}}{p}(-1)^j a^j (x^{n/p})^{p-j} \pmod{p}. \tag{3.5}$$

Now, if $\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \equiv 0 \pmod{p}$, then there exists α in an algebraic closure of $\mathbb{F}_p$ such that

$$\overline{F_{\mathcal{T}}}(\alpha) \equiv \overline{\tau}_i(\alpha) \equiv 0 \pmod{p} \quad \text{for some } i.$$

Hence, $g(\alpha)^{n/p} - a \equiv 0 \pmod{p}$, which implies that the sum in (3.3) is identically zero at $x = \alpha$. We conclude that

$$\frac{a + (-a)^p}{p} \equiv \overline{F_{\mathcal{T}}}(\alpha) \equiv 0 \pmod{p}. \tag{3.6}$$

Let $\beta = g(\alpha)$. Then $\beta^{n/p} - a \equiv 0 \pmod{p}$, from which we deduce that $\overline{t}_i(\beta) \equiv 0 \pmod{p}$ for some i, and that $\overline{F_f}(\beta) \equiv \frac{a+(-a)^p}{p} \pmod{p}$, since the sum in (3.5) is identically zero at $x = \beta$. But then (3.6) implies that $\overline{F_f}(\beta) \equiv 0 \pmod{p}$ so that $\gcd(\overline{F_f}, \overline{t}_i) \neq 1$, which, from Corollary 2.4, contradicts the fact that $f(x)$ is monogenic. Consequently, $\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \not\equiv 0 \pmod{p}$, and the lemma is established for primes dividing n.

Next, suppose that p is a prime that divides a. Then

$$\overline{\mathcal{T}}(x) \equiv g(x)^n \equiv \left(\prod_i \overline{\tau_i}(x)^{e_i}\right)^n \pmod{p},$$

where the $\overline{\tau_i}(x)$ are irreducible modulo p, and

$$F_{\mathcal{T}}(x) = \frac{\left(\prod_i \tau_i(x)^{e_i}\right)^n - (g(x)^n - a)}{p} = \frac{\left(\prod_i \tau_i(x)^{e_i}\right)^n - g(x)^n}{p} + \frac{a}{p}, \tag{3.7}$$

where the $\tau_i(x)$ are arbitrary monic lifts of the $\overline{\tau_i}(x)$. If $\left[\mathbb{Z}_K : \mathbb{Z}[\theta]\right] \equiv 0 \pmod{p}$, then there exists α in an algebraic closure of $\mathbb{F}_p$ such that

$$\overline{\tau}_i(\alpha) \equiv \overline{F_{\mathcal{T}}}(\alpha) \equiv 0 \pmod{p} \quad \text{for some } i. \tag{3.8}$$

Hence,

$$\left(\prod_i \tau_i(\alpha)^{e_i}\right)^n \equiv g(\alpha)^n \equiv 0 \pmod{p^2}$$

since $n \geq 2$. Consequently, from (3.8) and (3.7), it follows that $a \equiv 0 \pmod{p^2}$. However, $\overline{f}(x) \equiv x^n \pmod{p}$, so that

$$F_f(x) = \frac{x^n - (x^n - a)}{p} = \frac{a}{p}.$$

Since $f(x)$ is monogenic, we deduce from Theorem 1.1 that a is squarefree, which implies that $a \not\equiv 0 \pmod{p^2}$. This contradiction completes the proof. □

We are now in a position to present proofs of our main theorems.

Proof of Theorem 1.3. Conditions (1) and (2) imply that $f(x)$ is monogenic by Theorem 1.1. To show that $\mathcal{T}(x)$ is monogenic, we show first that $\mathcal{T}(x)$ is irreducible. To do this, we examine the prime divisors of $(-b)^n - a$. Let p be a prime such that $(-b)^n - a \equiv 0 \pmod{p}$. Then condition (3) implies that $p \mid an$. If $p \mid a$, then $p \mid b$, which implies that $p \mid\mid (-b)^n - a$ since $n \geq 2$ and a is squarefree. If $p \mid n$ and $p \nmid a$, then $p \nmid b$. That is, $\gcd(ab, p) = 1$. Then, if $p^2 \mid (-b)^n - a$, it follows from Euler's generalization of Fermat's Little Theorem that

$$a^{p-1} \equiv \left(((-b)^{n/p})^p\right)^{p-1} \equiv ((-b)^{n/p})^{\phi(p^2)} \equiv 1 \pmod{p^2}.$$

Hence, $a^p \equiv a \pmod{p^2}$, which contradicts condition (2). Thus, $(-b)^n - a$ is squarefree, and by Lemma 3.2, we conclude that $\mathcal{T}(x)$ is irreducible.

Finally, Lemma 3.1 and condition (3) imply that all prime divisors of $\Delta(\mathcal{T})$ divide $\Delta(f)$. Then, since $f(x)$ is monogenic, we deduce from Lemma 3.4 that $\mathcal{T}(x)$ is monogenic. □

Proof of Theorem 1.4. First note that since $n = 2$, conditions (1) and (2) are equivalent to $f(x)$ being monogenic, according to Theorem 1.1. We show next that $\mathcal{T}(x)$ is irreducible, assuming conditions (1), (2) and (3) hold. If $|b^2 - a| = y^p$ for some integer $y \geq 1$ and some prime p dividing m, then $y > 1$ since

$$\kappa(|b^2 - a|) = \kappa(am) > 1.$$

Thus, since $p \mid m$, we have that $p \mid b^2 - a$ so that

$$y^p \equiv b^2 - a \equiv 0 \pmod{p},$$

which implies that $p \mid y$, contradicting condition (3). Similarly, $|b^2 - a| \neq 16y^p$ for any integer $y \geq 1$ and any prime p dividing m. Hence, we conclude from Lemma 3.2 that $\mathcal{T}(x)$ is irreducible.

Next, we examine primes that divide $|\Delta(\mathcal{T})|$. By Lemma 3.1, we have that

$$|\Delta(\mathcal{T})| = |(2m)^{2m} a^m (b^2 - a)^{m-1}|.$$

Thus, to determine when $\mathcal{T}(x)$ is monogenic, it follows from Lemma 3.4 and the fact that $\kappa(am) = \kappa(|b^2 - a|)$ that we only need to check primes p that divide $\widehat{m}$. So, let p be such a prime. Then, since $\mathcal{T}(x) = x^{2m} - 2bx^m + b^2 - a$, we have that

$$\overline{\mathcal{T}}(x) \equiv x^m(x^m - 2b) \equiv x^m(x^{m/p} - 2b)^p \equiv x^m \left(\prod_i \overline{\tau_i}(x)^{e_i} \right)^p \pmod{p}, \tag{3.9}$$

where the $\overline{\tau_i}(x)$ are irreducible modulo p. Thus,

$$\prod_i \tau_i(x)^{e_i} = x^{m/p} - 2b + ps(x)$$

for some polynomial $s(x)$, where $\tau_i(x)$ is an arbitrary monic lift of $\overline{\tau_i}(x)$. Therefore, the polynomial $F_{\mathcal{T}}(x) := F(x)$ in Theorem 2.3 is

$$F_{\mathcal{T}}(x) = \frac{x^m(x^{m/p} - 2b + ps(x))^p - (x^{2m} - 2bx^m + b^2 - a)}{p},$$

so that

$$\begin{aligned} \overline{F_{\mathcal{T}}}(x) \equiv{}& \frac{(-2b)^p - (-2b)}{p} x^m \\ &+ x^m \sum_{j=1}^{p-1} \frac{\binom{p}{j}}{p} (x^{m/p})^{p-j} (-2b)^j - \frac{(b^2 - a)}{p} \pmod{p}. \end{aligned} \tag{3.10}$$

We see from (3.9) that if $\overline{\mathcal{T}}(\alpha) \equiv 0 \pmod{p}$, then either $\alpha \equiv 0 \pmod{p}$, or $\overline{\tau_i}(\alpha) \equiv 0 \pmod{p}$ for some i, in which case

$$2b \equiv \alpha^{m/p} \equiv (\alpha^{m/p})^p \equiv \alpha^m \pmod{p}$$

and the sum in (3.10) is identically zero. Consequently,

$$\overline{F_{\mathcal{T}}}(\alpha) \equiv \begin{cases} -\frac{(b^2-a)}{p} \pmod p & \text{if } \alpha = 0, \\ \frac{(-2b)^p-(-2b)}{p}(2b) - \frac{(b^2-a)}{p} \pmod p & \text{otherwise.} \end{cases} \tag{3.11}$$

We have from Corollary 2.4 that $\mathcal{T}(x)$ is monogenic if and only if neither of the quantities on the right-hand side of (3.11) is zero, which is easily seen to be equivalent to conditions (3) and (4). □

Proof of Theorem 1.5. First note that since $n = 3$, conditions (1) and (2) are equivalent to $f(x)$ being monogenic, according to Theorem 1.1. Under the assumption that conditions (1), (2), and (3) hold, an argument similar to the one used in the proof of Theorem 1.4 shows that $\mathcal{T}(x)$ is irreducible by Lemma 3.2.

Using Corollary 2.4 to determine when $\mathcal{T}(x)$ is monogenic, we only need to examine primes p dividing $\widehat{m}$ by Lemma 3.4. Let p be such a prime. Since

$$\mathcal{T}(x) = x^{3m} - 3bx^{2m} + 3b^2x^m - b^3 - a,$$

we have that

$$\begin{aligned} \overline{\mathcal{T}}(x) &\equiv x^m\big((x^{m/p})^2 - 3b(x^{m/p}) + 3b^2\big)^p \pmod p \\ &\equiv x^m \left(\prod_i \overline{\tau_i}(x)^{e_i}\right)^p \pmod p, \end{aligned} \tag{3.12}$$

where the $\overline{\tau_i}(x)$ are irreducible modulo p. Then, expanding (3.12), we get that

$$\begin{aligned} pF_{\mathcal{T}}(x) &= x^m\big(((x^{m/p})^2 - 3b(x^{m/p}))^p + (3b^2)^p + V\big) - \mathcal{T}(x) \\ &= x^m\big(x^{2m} + (-3b)^p x^m + U + (3b^2)^p + V\big) - \mathcal{T}(x) \\ &= ((-3b)^p + 3b)x^{2m} + ((3b^2)^p - 3b^2 + U + V)x^m + b^3 + a, \end{aligned} \tag{3.13}$$

where

$$U = \sum_{j=1}^{p-1} \binom{p}{j} ((x^{m/p})^2)^{p-j}(-3bx^{m/p})^j \quad \text{and} \quad V = \sum_{j=1}^{p-1} \binom{p}{j} ((x^{m/p})^2 - 3b(x^{m/p}))^{p-j}(3b^2)^j.$$

If $\overline{\mathcal{T}}(\alpha) \equiv 0 \pmod p$ for some α in an algebraic closure of $\mathbb{F}_p$, we see from (3.12) that either

$$\alpha \equiv 0 \pmod p \quad \text{or} \quad \alpha^{m/p} \equiv b(\zeta + 1) \pmod p,$$

where ζ is a primitive sixth root of unity modulo p.

If $\alpha \equiv 0 \pmod p$, then we see from (3.13) that $\overline{F_{\mathcal{T}}}(\alpha) \equiv 0 \pmod p$ if and only if $b^3 + a \equiv 0 \pmod{p^2}$, which is condition (3). Suppose then that $\alpha^{m/p} \equiv b(\zeta + 1) \not\equiv 0$

$(\mathrm{mod}\ p)$. We make use of the fact that $\zeta^2-\zeta+1\equiv 0\ (\mathrm{mod}\ p)$, and split our analysis into three cases: $p=2$, $p\equiv 1\ (\mathrm{mod}\ 6)$ and $p\equiv 5\ (\mathrm{mod}\ 6)$. Straightforward computations and induction arguments yield

$$\alpha^m \equiv \begin{cases} 3b^p\zeta \pmod p & \text{if } p=2,\\ (-3)^{(p-1)/2}b^p(\zeta+1) \pmod p & \text{if } p\equiv 1 \pmod 6,\\ (-3)^{(p-1)/2}b^p(\zeta-2) \pmod p & \text{if } p\equiv 5 \pmod 6, \end{cases} \tag{3.14}$$

$$\alpha^{2m} \equiv \begin{cases} 9b^{2p}(\zeta-1) \pmod p & \text{if } p=2,\\ 3^pb^{2p}\zeta \pmod p & \text{if } p\equiv 1 \pmod 6,\\ (-3)^pb^{2p}(\zeta-1) \pmod p & \text{if } p\equiv 5 \pmod 6 \end{cases} \tag{3.15}$$

and

$$V\big|_{x=\alpha} = \begin{cases} -18b^4 & \text{if } p=2,\\ 0 & \text{otherwise.} \end{cases} \tag{3.16}$$

Since

$$\begin{aligned} U\big|_{x=\alpha} &= \sum_{j=1}^{p-1}\binom{p}{j}(3b^2\zeta)^{p-j}(-3b^2(\zeta+1))^j = \sum_{j=1}^{p-1}\binom{p}{j}(3b^2)^{p-j}\zeta^{p-j}(3b^2)^j(-\zeta-1)^j\\ &= 3^pb^{2p}\zeta^p\sum_{j=1}^{p-1}\binom{p}{j}(\zeta^{-1}(-\zeta-1))^j = 3^pb^{2p}\zeta^p\sum_{j=1}^{p-1}\binom{p}{j}(\zeta^{-1}(\zeta^2-2\zeta))^j\\ &= 3^pb^{2p}\zeta^p\sum_{j=1}^{p-1}\binom{p}{j}(\zeta-2)^j = 3^pb^{2p}\zeta^p((\zeta-1)^p-(\zeta-2)^p-1), \end{aligned}$$

we also have that

$$U\big|_{x=\alpha} = \begin{cases} 3^pb^{2p}(-4\zeta+2) & \text{if } p=2,\\ 3^pb^{2p}((-3)^{(p-1)/2}-1)(\zeta+1) & \text{if } p\equiv 1 \pmod 6,\\ 3^pb^{2p}((-3)^{(p-1)/2}+1)(\zeta-2) & \text{if } p\equiv 5 \pmod 6. \end{cases} \tag{3.17}$$

Combining (3.14), (3.15), (3.16) and (3.17), and using (3.13), we get, after some manipulation, that

$$pF_{\mathcal{T}}(\alpha) = \begin{cases} (27b^5-9b^4)\zeta+27b^6-27b^5+b^3+a & \text{if } p=2,\\ A\zeta+B+b^3+a & \text{if } p\equiv 1 \pmod 6,\\ C\zeta+D+b^3+a & \text{if } p\equiv 5 \pmod 6, \end{cases} \tag{3.18}$$

where

$$A = (-1)^{(p+1)/2}2 \cdot 3^{(3p-1)/2}b^{3p} + 3^{p+1}b^{2p+1} + (-3)^{(p+1)/2}b^{p+2},$$
$$B = (-1)^{(p-1)/2}3^{(3p-1)/2}b^{3p} + (-3)^{(p+1)/2},$$
$$C = (-1)^{(p+1)/2}2 \cdot 3^{(3p-1)/2}b^{3p} - 3^{p+1}b^{2p+1} + (-3)^{(p+1)/2}b^{p+2},$$
$$D = (-1)^{(p-1)/2}3^{(3p-1)/2}b^{3p} + 3^{p+1}b^{2p+1} + (-1)^{(p-1)/2}2 \cdot 3^{(p+1)/2}b^{p+2}.$$

When $p = 2$, the minimal polynomial for ζ has degree 2, and we see from (3.18) that

$$\begin{aligned} pF_{\mathcal{T}}(\alpha) \equiv 0 \pmod 4 \quad &\Longrightarrow \quad 27b^5 - 9b^4 \equiv 0 \pmod 4 \\ &\Longrightarrow \quad b \equiv 0 \pmod 2 \quad \text{or} \quad b \equiv 3 \pmod 4. \end{aligned}$$

However, $b \equiv 0 \pmod 2$ implies that $a \equiv 0 \pmod 4$, which contradicts condition (1). Thus, $b \equiv 3 \pmod 4$, which in turn implies that $a \equiv 3 \pmod 4$. It is easy to see that if $a \equiv b \equiv 3 \pmod 4$, then $pF_{\mathcal{T}}(\alpha) \equiv 0 \pmod 4$. Hence, we arrive at condition (4).

In the case when $p \equiv 1 \pmod 6$, we have that $\zeta \in \mathbb{F}_p$ so that the minimal polynomial for ζ is a linear polynomial. Thus, we just have from (3.18) that

$$pF_{\mathcal{T}}(\alpha) \equiv 0 \pmod{p^2} \quad \Longleftrightarrow \quad A\zeta + B + b^3 + a \equiv 0 \pmod{p^2},$$

which simply yields condition (5).

Finally, when $p \equiv 5 \pmod 6$, we see from (3.18) that

$$pF_{\mathcal{T}}(\alpha) \equiv 0 \pmod{p^2} \quad \Longrightarrow \quad C \equiv 0 \pmod{p^2},$$

since the minimal polynomial for ζ has degree 2. We claim that

$$C \equiv 0 \pmod{p^2} \quad \Longrightarrow \quad D \equiv 0 \pmod{p^2}. \tag{3.19}$$

To see this claim, tedious, but straightforward calculations show that

$$\begin{aligned} C &= (-3)^{(p+1)/2}b^{p+2}((-3b^2)^{(p-1)/2} + 1)(2(-3b^2)^{(p-1)/2} + 1), \\ D &= (-1)^{(p-1)/2}3^{(p+1)/2}b^{p+2}((-3b^2)^{(p-1)/2} + 1)((-3b^2)^{(p-1)/2} + 2). \end{aligned} \tag{3.20}$$

By Euler's criterion, we have that

$$2(-3b^2)^{(p-1)/2} + 1 \not\equiv 0 \pmod p \quad \text{and} \quad (-3b^2)^{(p-1)/2} + 2 \not\equiv 0 \pmod p.$$

Thus, if $C \equiv 0 \pmod{p^2}$, then either

$$b^{p+2} \equiv 0 \pmod{p^2} \quad \text{or} \quad (-3b^2)^{(p-1)/2} + 1 \equiv 0 \pmod{p^2}.$$

In either case, it follows from (3.20) that $D \equiv 0 \pmod{p^2}$, and the claim (3.19) is established. Consequently,

$$pF_{\mathcal{T}}(\alpha) \equiv 0 \pmod{p^2} \quad \Longrightarrow \quad b^3 + a \equiv 0 \pmod{p^2}.$$

As previously pointed out, if $b^3 + a \equiv 0 \pmod{p^2}$, then $pF_{\mathcal{T}}(0) \equiv 0 \pmod{p^2}$. Therefore, in this case, no additional conditions are required since condition (3) covers this situation. □

4. Examples

Using the ideas from Corollary 1.6, the following example illustrates how to construct infinite collections of monogenic and non-monogenic polynomials in the setting of Theorem 1.4.

Example 4.1. Let p be an odd prime such that $p-1$ is squarefree. (Note that it is well-known that infinitely many such primes exist [20, 27].) Let $k \geq 1$ be an integer. Let $a = b = 1 - p$ and $m = p^k$, so that

$$\kappa(|am|) = \kappa(p(p-1)) = \kappa(|b^2 - a|).$$

Then $f(x) = x^2 - (1-p)$, $g(x) = x^{p^k} - (1-p)$ and

$$\mathcal{T}(x) := f(g(x)) = (x^p - (1-p))^2 - (1-p) = x^{2p^k} - 2(1-p)x^{p^k} + p(p-1).$$

We use Theorem 1.4 to determine when $\mathcal{T}(x)$ is monogenic. Condition (1) of Theorem 1.4 is satisfied by assumption. Note also that $p \equiv 3 \pmod 4$ and $a \equiv 2 \pmod 4$, so that condition (2) is satisfied. For conditions (3) and (4), we only need to check the prime p using Corollary 2.4. Clearly, $b^2 - a = p(p-1) \not\equiv 0 \pmod{p^2}$ so that condition (3) is satisfied. For condition (4), we see that

$$-2^{p+1}(1-p)^{p+1} + 3(1-p)^2 + (1-p) \equiv (p-1)(2^{p+1} + 3p - 4) \pmod{p^2},$$

and therefore, $\mathcal{T}(x)$ is monogenic if and only if

$$2^{p+1} + 3p - 4 \not\equiv 0 \pmod{p^2}. \tag{4.1}$$

Interestingly, a computer search of the first ten million primes reveals that the only exception to (4.1) among primes $p \equiv 3 \pmod 4$, such that $p-1$ is squarefree, is $p = 79$.

Finally, we observe that for each such prime p for which (4.1) holds, there exist infinitely many pairs of binomials $f(x)$ and $g(x)$ such that both $f(x)$ and $\mathcal{T}(x)$ are monogenic, simply by letting the exponent k range on $m = p^k$ to Corollary 1.6. Similarly, from Corollary 1.6, the polynomials $\mathcal{T}(x^{79^k})$ are not monogenic for all $k \geq 1$.

We now give some examples of polynomials that satisfy the conditions of Theorem 1.5. We outline an algorithm for constructing these polynomials. First choose $a \not\equiv 3 \pmod 4$ in such a way that a satisfies Theorem 1.1. Then choose b to be a multiple of a such that $b^3 + a$ is squarefree. If $\kappa(|b^3 + a|)/a$ has no prime factors $p \equiv 1 \pmod 6$, then all conditions of Theorem 1.5 are trivially satisfied and $\mathcal{T}$ is monogenic. An example of such a polynomial is

$$\mathcal{T}(x) = x^{1908162} + 258x^{1272108} + 22188x^{636054} + 636054.$$

If $\kappa(|b^3 + a|)/a$ has a prime factor $p \equiv 1 \pmod 6$, then we go on to examine condition (5) of Theorem 1.5. If condition (5) holds, then we deduce that $\mathcal{T}$ is monogenic. An infinite family of such polynomials is given by

$$\mathcal{T}(x) = x^{3\cdot 37^k} - 18x^{2\cdot 37^k} + 108x^{37^k} - 222.$$

The final example shows that there exist infinitely many pairs of binomials that do not satisfy the conditions of Theorem 1.5.

Example 4.2. Let k be a positive integer, and let $m = 217^k$. Let $a = 29$, and $b = -58$, so that $|b^3 + a| = 7 \cdot 29 \cdot 31^2$ and $\kappa(|am|) = \kappa(|b^3 + a|) = 7 \cdot 29 \cdot 31$. Then $f(x) = x^3 - 29$, $g(x) = x^{217^k} + 58$ and

$$\mathcal{T}(x) = x^{3\cdot 217^k} + 174x^{2\cdot 217^k} + 10092x^{217^k} + 195083.$$

Conditions (1) and (2) of Theorem 1.5 are easily confirmed to be true. However, condition (3) is not satisfied with $p = 31$. Thus, although $f(x)$ is monogenic, we have that $\mathcal{T}(x)$ is not monogenic.

Since k was arbitrary, we have found an infinite collection of pairs of binomials $f(x) = x^3 - a$ and $g(x) = x^m - b$ such that $f(x)$ is monogenic but $f(g(x))$ is not monogenic. Note that this process can be duplicated for any other single pair satisfying conditions (1) and (2), but not condition (3) to arrive at other such infinite collections.

5. Final comments

Although generalizing Theorem 1.5 to $\mathcal{T}(x) = f(g(x)) = (x^m - b)^n - a$, where $n > 3$ is arbitrary, seems to be theoretically possible, there appear to be severe computational obstacles. Even the case when m and n are both arbitrary odd primes presents extreme difficulty. Nevertheless, along these lines we make the following conjecture.

Conjecture 5.1. *Let $a, b \in \mathbb{Z}$. Let p and q be odd primes with $p \equiv -1 \pmod q$. Let $f(x) = x^q - a$, $g(x) = x^p - b$, $\mathcal{T}(x) = f(g(x))$ and suppose that $\kappa(|ap|) = \kappa(|b^q + a|)$, where $\kappa(*)$ denotes the squarefree kernel of the positive integer $*$. Then $f(x)$ and $\mathcal{T}(x)$ are monogenic if and only if all of the following conditions hold:*

(1) *a is squarefree,*

(2) $a^q - a \not\equiv 0 \pmod{q^2}$,

(3) $b^q + a \not\equiv 0 \pmod{p^2}$.

Let ζ be a primitive $2q$th root of unity modulo p. Since $p \equiv -1 \pmod{q}$, the minimal polynomial for ζ has degree 2 [18], and therefore we can write

$$(b^{p-1}(\zeta+1)^p - 1)^q + 1 \equiv A\zeta + B \pmod{p^2}. \tag{5.1}$$

Conjecture 5.1 will then follow if it can be established that

$$A \equiv 0 \pmod{p^2} \quad \Longrightarrow \quad B \equiv 0 \pmod{p^2}$$

in (5.1).

Acknowledgments

The authors thank the anonymous referee for the many valuable suggestions.

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] M. Bardestani, *The density of a family of monogenic number fields*, arXiv:1202.2047.

[4] M. Bhargava, A. Shankar and X. Wang, *Squarefree values of polynomial discriminants I*, arXiv:1611.09806.

[5] D. W. Boyd, G. Martin and M. Thom, *Squarefree values of trinomial discriminants*, LMS J. Comput. Math. **18** (2015), no. 1, 148–169.

[6] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics **138**, Springer-Verlag, Berlin, 1993.

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

[8] D. Eloff, B. K. Spearman and K. S. Williams, *A_4-sextic fields with a power basis*, Missouri J. Math. Sci. **19** (2007), no. 3, 188–194.

[9] I. Gaál, *Power integral bases in cubic relative extensions*, Experiment. Math. **10** (2001), no. 1, 133–139.

[10] ———, *Diophantine Equations and Power Integral Bases: New computational methods*, Birkhäuser Boston, Boston, MA, 2002.

[11] I. Gaál and M. Pohst, *Computing power integral bases in quartic relative extensions*, J. Number Theory **85** (2000), no. 2, 201–219.

[12] 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.

[13] ———, *Integral bases and monogenity of pure fields*, J. Number Theory **173** (2017), 129–146.

[14] I. Gaál, L. Remete and T. Szabó, *Calculating power integral bases by using relative power integral bases*, Funct. Approx. Comment. Math. **54** (2016), no. 2, 141–149.

[15] I. Gaál and T. Szabó, *Relative power integral bases in infinite families of quartic extensions of quadratic fields*, JP J. Algebra Number Theory Appl. **29** (2013), no. 1, 31–43.

[16] T. A. Gassert, *Discriminants of Chebyshev radical extensions*, J. Théor. Nombres Bordeaux **26** (2014), no. 3, 607–634.

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

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

[19] J. Harrington and L. Jones, *Monogenic cyclotomic compositions*, arXiv:1909.03541.

[20] H. A. Helfgott, *Square-free values of $f(p)$, f cubic*, Acta Math. **213** (2014), no. 1, 107–135.

[21] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Second edition, Graduate Texts in Mathematics **84**, Springer-Verlag, New York, 1990.

[22] A. Jakhar, S. K. Khanduja and N. Sangwan, *Characterization of primes dividing the index of a trinomial*, Int. J. Number Theory **13** (2017), no. 10, 2505–2514.

[23] B. Jhorar and S. K. Khanduja, *On power basis of a class of algebraic number fields*, Int. J. Number Theory **12** (2016), no. 8, 2317–2321.

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

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

[26] T. Nakahara, *Hasse's problem for monogenic fields*, Ann. Math. Blaise Pascal **16** (2009), no. 1, 47–56.

[27] H. Pasten, *The ABC conjecture, arithmetic progressions of primes and squarefree values of polynomials at prime arguments*, Int. J. Number Theory **11** (2015), no. 3, 721–737.

[28] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications **77**, Cambridge University Press, Cambridge, 2000.

[29] B. K. Spearman, *Monogenic A_4 quartic fields*, Int. Math. Forum **1**, (2006), no. 37-40, 1969–1974.

[30] L. C. Washington, *Introduction to Cyclotomic Fields*, Second edition, Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997.

Joshua Harrington
Department of Mathematics, Cedar Crest College, Allentown, Pennsylvania, USA
E-mail address: Joshua.Harrington@cedarcrest.edu

Lenny Jones
Department of Mathematics, Shippensburg University, Shippensburg, Pennsylvania 17257, USA
E-mail address: lkjone@ship.edu