

SPARSITY OBSTRUCTIONS FOR ABELIAN POWER COMPOSITIONS OF ODD BASE DEGREE

SCOTT DUKE KOMINERS

ABSTRACT. Motivated by prior work on abelian monogenic trinomials, we classify irreducible abelian trinomial power compositions of odd base degree and explore the structural results underlying the classification. If $m \geq 3$ is odd, $n \geq 1$, $1 \leq k < m$, and $a, b \in \mathbb{Q}^\times$, then

$$x^{mn} + ax^{kn} + b$$

can be irreducible with abelian Galois group only if $(m, n) = (3, 1)$; the surviving pair is realized by $x^3 - 3x + 1$.

More generally, let $f \in \mathbb{Q}[y]$ be monic of odd base degree m . If $f(x^n)$ is irreducible with abelian Galois group, then $n = 2^\ell$ for some $\ell \geq 0$. When $n \geq 2$, f has full coefficient support; the exponent and full-support conclusions are jointly sharp, since every odd m and every $n = 2^\ell$, $\ell \geq 1$, are realized. When $n = 1$ and $m \geq 3$, a gap-sensitive form of Descartes's rule requires at least $(m + 3)/2$ nonzero terms. Equality holds for every $m = 3^r$, $r \geq 1$, and also for $m = 5$.

We also characterize exponent-2 normal compositions: $f(x^2)$ is irreducible and normal exactly when a root of f is a rational nonsquare times a square in its root field and the Galois closure of that field lies in the extension obtained by adjoining the corresponding square root; this permits the lacunary normal nonabelian example $x^6 + 108$. For arbitrary n , normality forces $\varphi(n) \mid mn$; in cubic base degree we determine all n satisfying this condition and realize its two possible odd prime divisors at exponents 6 and 14.

2020 *Mathematics Subject Classification*. Primary 11R09; Secondary 11R21, 11R32, 11C08.

Key words and phrases. abelian polynomial, Descartes's rule of signs, Galois group, lacunary polynomial, monogenic polynomial, normal polynomial, power composition, trinomial.

I used LLMs to assist with the computations, analysis, and synthesis in the preparation of this article, particularly GPT-5.6 Sol and Claude Opus 5 (accessed in part via Poe with the support of Quora, where I am an advisor). The problem, final methods, and eventual written form are my own; and of course any errors remain my responsibility. This work was conducted while I was visiting the Technological Innovation, Entrepreneurship, and Strategic Management (TIES) Group at the MIT Sloan School of Management; I greatly appreciate their hospitality.

1. INTRODUCTION

1.1. **Power compositions and the motivating problem.** Let

$$f(y) = \sum_{i=0}^m c_i y^i \in \mathbb{Q}[y], \quad c_m = 1, \quad F_n(x) = f(x^n) \quad (n \geq 1).$$

We call f the *base polynomial*, m its *base degree*, and n the *composition exponent*; the total degree of F_n is mn . The composition is *nontrivial* when $n \geq 2$. We write

$$\text{supp}(f) = \{i : c_i \neq 0\}$$

for the *coefficient support* of f . We say that f has *full support* if $\text{supp}(f) = \{0, \dots, m\}$, and that it is *lacunary* otherwise. Because the substitution $y = x^n$ sends y^i to x^{ni} , the base and the composition have the same number of nonzero terms.¹

Throughout, an irreducible polynomial over $\mathbb{Q}$ is called *abelian* if the Galois group of its splitting field over $\mathbb{Q}$ is abelian. Power composition imposes a symmetry that is difficult to reconcile with abelianness: if $\alpha \neq 0$ is a root of F_n , then $\alpha\zeta$ is also a root for every n -th root of unity ζ . We examine how this rotational symmetry constrains the composition exponent and coefficient support when the base degree is odd.

The motivating problem concerns abelian *monogenic* trinomials. A monic irreducible polynomial $F \in \mathbb{Z}[x]$, with root θ , is said to be *monogenic* if $\mathcal{O}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta]$; equivalently, $\{1, \theta, \dots, \theta^{\deg F - 1}\}$ is an integral basis [1, Section 4.4.1]. A series of papers by Jones [8, 6, 7, 5] has studied trinomial power compositions that are simultaneously abelian and monogenic in several low-degree families; these problems combine an arithmetic integral-basis condition with the Galois-theoretic constraint of abelianness.

We begin with the cubic-base case and find that its obstruction extends uniformly to every odd base degree. A monic cubic trinomial with nonzero constant term has one of the two forms

$$f(y) = y^3 + ay + b \quad \text{or} \quad f(y) = y^3 + ay^2 + b,$$

with $a, b \in \mathbb{Z}$ and $ab \neq 0$; its power compositions are therefore

$$x^{3n} + ax^n + b \quad \text{and} \quad x^{3n} + ax^{2n} + b.$$

Our first main result shows that for cubic base degree, the integral-basis condition is not needed: irreducibility and abelianness already exclude every nontrivial composition in both families. In fact, the argument requires no integrality and extends uniformly to every odd base degree.

Theorem 1.1 (Trinomial classification). *Let $m \geq 3$ be odd, let $n \geq 1$, let $1 \leq k < m$, and let $a, b \in \mathbb{Q}^\times$. If*

$$x^{mn} + ax^{kn} + b$$

¹Note that we use the terms *full support* and *lacunary* relative to the base degree m . Although f and F_n have the same number of nonzero terms, F_n itself has zero coefficients at every exponent not divisible by n when $n \geq 2$.

is irreducible over $\mathbb{Q}$ with abelian Galois group, then

$$(m, n) = (3, 1).$$

The exceptional pair is realized: $x^3 - 3x + 1$ is irreducible and has Galois group cyclic of order 3. Thus Theorem 1.1 classifies the possible pairs (m, n) in every odd base degree $m \geq 3$ —and the uncomposed cubic pair is the only one that occurs. For the motivating cubic problem, this shows that the obstruction is independent of the integral-basis condition: irreducibility and abelianness already reduce both families to the uncomposed case $n = 1$ (Corollary 5.2), where Jones’s classifications of abelian monogenic cubics apply.

1.2. The abelian dichotomy. Theorem 1.1 is the smallest-support case of a more general structural dichotomy. For a nontrivial composition, abelianness forces the composition exponent to be a power of 2 and the base polynomial to have full support. In the uncomposed case, odd-degree abelianness makes the base totally real, and a gap-sensitive form of Descartes’s rule gives a weaker support bound.

Theorem 1.2 (Abelian dichotomy). *Let $f \in \mathbb{Q}[y]$ be monic of odd base degree $m \geq 3$, let $n \geq 1$, and suppose that $F_n(x) = f(x^n)$ is irreducible over $\mathbb{Q}$ with abelian Galois group. If*

$$t = |\text{supp}(f)|,$$

then $n = 2^\ell$ for some $\ell \geq 0$, and

$$t \geq \frac{m+3}{2} \quad \text{if } n = 1, \quad \text{whereas} \quad t = m+1 \quad \text{if } n \geq 2.$$

Because substitution preserves support size, t is also the number of nonzero terms of F_n . The trinomial classification is therefore the case $t = 3$: the nontrivial branch is impossible, while the uncomposed branch forces $m = 3$.

The two branches have different sharpness statements. In the uncomposed branch, the bound $(m+3)/2$ is attained for every base degree $m = 3^r$, $r \geq 1$, by the Chebyshev family in Proposition 4.3; it is also attained at $m = 5$ in Example 4.4. It remains open whether equality occurs for every odd base degree. By contrast, the nontrivial branch is sharp in complete generality: Proposition 5.4 realizes every odd $m \geq 1$ and every composition exponent $n = 2^\ell$ ($\ell \geq 1$), by a base polynomial whose coefficients are all positive. Accordingly, Theorem 1.1 gives an exact classification of the possible pairs (m, n) in all odd base degrees; the more limited sharpness assertion concerns equality in the general support bound at $n = 1$.

1.3. Ideas of the proof. Write φ for Euler’s totient function. Three mechanisms underlie Theorem 1.2. First, irreducibility and abelianness descend from F_n to F_e for every divisor $e \mid n$. If α is a root of F_e , then $\alpha\zeta_e$

is another root. For an irreducible abelian polynomial, the field generated by one root is already the splitting field, and hence

$$\zeta_e = \frac{\alpha \zeta_e}{\alpha} \in \mathbb{Q}(\alpha).$$

It follows that $\varphi(e) \mid me$. Taking $e = p$ prime gives $p - 1 \mid m$; because m is odd, this excludes every odd prime divisor of n .

Second, if $n \geq 2$, then the surviving exponent is a power of 2, and divisor descent reduces the coefficient problem to $F_2(x) = f(x^2)$. Let β be a root of f , put $E = \mathbb{Q}(\beta)$, and choose α with $\alpha^2 = \beta$. The abelian structure of $\mathbb{Q}(\alpha)/\mathbb{Q}$ yields

$$\beta = dv^2$$

for a rational nonsquare d and some $v \in E^\times$. The odd-degree abelian extension $E/\mathbb{Q}$ is totally real, so every conjugate of β has the sign of d . Vieta's formulas then force every coefficient of f to be nonzero and determine its sign pattern. Theorem 3.1, stated and proved in Section 3, records these stronger conclusions.

Finally, if $n = 1$, the splitting field of f has the odd degree m and is therefore totally real. Applying Descartes's rule simultaneously to $f(y)$ and $f(-y)$ records not only coefficient signs but also the parities of the gaps in $\text{supp}(f)$. This gap-sensitive count yields $t \geq (m + 3)/2$ and identifies the equality pattern. The distinction between these last two arguments explains why the bases of nontrivial abelian compositions have full support, whereas uncomposed abelian polynomials need not.

1.4. Related work. The problem lies at the intersection of results on power compositions, abelian polynomials, and monogenicity. At base degree $m = 1$, Schinzel [11, 12] characterized irreducible abelian binomials; in particular, the composition exponent must be a power of 2. At base degree $m = 2$, Jones classified the abelian monogenic trinomials

$$x^{2n} + ax^n + b$$

into seven explicit, pairwise-disjoint classes [8, Theorem 1.4]. At cubic base degree $m = 3$ and composition exponent $n = 2$ —hence total degree 6—Jones proved that neither cubic-base trinomial shape above can be an irreducible cyclic sextic [6, Theorem 1.1(1)]—this is the relevant abelian case because an irreducible abelian sextic has cyclic Galois group of order 6; Jones later recovered the conclusion in his work on monogenic even sextic trinomials [7, Corollary 3.2].

More generally, power compositions have been studied from the viewpoints of irreducibility, Galois groups, index questions, and monogenicity [3, 9]. Harrington and Jones constructed infinite families of nontrivial monogenic trinomial compositions [4]; thus monogenicity by itself does not produce the type of obstruction identified for abelianness here. Once Theorem 1.1 reduces the motivating problem to $n = 1$, the remaining cubic families connect directly with Jones's work on abelian monogenic cubics [5].

1.5. Normality as a boundary case. Our proof uses commutativity in two distinct ways: it forces a root field to be the splitting field, and it makes every intermediate field Galois over $\mathbb{Q}$, enabling divisor descent. To separate these roles, we also study *normal* polynomials. An irreducible polynomial $F \in \mathbb{Q}[x]$ is normal if the field generated by one, equivalently every, root is its splitting field; its Galois group need not be abelian. Root rotation therefore remains available at the original composition exponent, but normality need not descend to its divisors. Vélez studied the binomial case [13].

For exponent 2, Theorem 3.3 gives an exact criterion. If β is a root of the odd-degree irreducible base f , $E = \mathbb{Q}(\beta)$, and $\tilde{E}$ is the Galois closure of $E/\mathbb{Q}$, then $f(x^2)$ is irreducible and normal exactly when there are a rational nonsquare d and $v \in E^\times$ such that

$$\beta = dv^2 \quad \text{and} \quad \tilde{E} \subseteq E(\sqrt{d}).$$

The splitting field is then $E(\sqrt{d})$. The closure condition measures precisely what is lost when commutativity is removed. If $d > 0$, the splitting field is totally real and Vieta's formulas again force every coefficient of f to be nonzero. If $d < 0$, coefficient nonvanishing can fail: the cubic base $f(y) = y^3 + 108$ gives the irreducible normal polynomial $x^6 + 108$, whose Galois group is S_3 . Thus the abelian lacunarity obstruction does not extend to normal nonabelian compositions.

For arbitrary n , root rotation still forces $\varphi(n) \mid mn$ whenever F_n is irreducible and normal. In particular, because m is odd, no odd composition exponent $n \geq 2$ can occur. At cubic base degree, Theorem 6.6 solves the numerical condition completely: the positive integer solutions of $\varphi(n) \mid 3n$ are

$$n = 1, \quad n = 2^r, \quad n = 2^r 3^s, \quad \text{or} \quad n = 2^r 7^s,$$

where $r \geq 1$, and $s \geq 1$ in the last two families. This list is only a necessary condition, not an existence theorem for every entry. Nevertheless, the same theorem realizes its two possible odd prime divisors: for each $p \in \{3, 7\}$, it constructs a monic irreducible cubic $f_p \in \mathbb{Z}[y]$ such that $f_p(x^{2p})$ is irreducible and normal, whereas $f_p(x^p)$ is irreducible but not normal.

1.6. Organization of the paper. Section 2 proves divisor descent and the root-of-unity restriction. Section 3 analyzes exponent 2 and proves the detailed abelian structure theorem and the normal square-class criterion. Section 4 develops the gap-sensitive form of Descartes's rule and proves Theorems 1.2 and 1.1. Section 5 derives the lacunarity obstruction, applies the trinomial classification to the motivating cubic monogenic families, gives the sharpness constructions, and proves a cyclotomic consequence. Section 6 develops the normal nonabelian case and proves Theorem 6.6. Section 7 records a few remaining questions.

2. DIVISOR DESCENT AND ROOTS OF UNITY

The nontrivial-composition branch begins with two elementary mechanisms. Irreducibility and abelianness descend to every divisor of the composition exponent, while root rotation forces cyclotomic information into each descended root field. We begin with the standard fact that a root field of an irreducible abelian polynomial is already its splitting field; the short proof is included for completeness.

Lemma 2.1. *Let $F \in \mathbb{Q}[x]$ be irreducible with abelian Galois group, and let α be a root. Then $\mathbb{Q}(\alpha)$ is the splitting field of F . In particular,*

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg F.$$

Proof. Let L be the splitting field, $G = \text{Gal}(L/\mathbb{Q})$, and let $H \leq G$ be the stabilizer of α . For $g \in G$ and $h \in H$, commutativity gives

$$h(g(\alpha)) = g(h(\alpha)) = g(\alpha).$$

Thus H fixes every conjugate of α , hence fixes their splitting field L . Therefore H is trivial, and $L = \mathbb{Q}(\alpha)$. $\square$

We also record the elementary archimedean consequence of odd Galois degree.

Lemma 2.2. *Every finite Galois extension $L/\mathbb{Q}$ of odd degree is totally real.*

Proof. Fix an embedding $L \subseteq \mathbb{C}$. Since $L/\mathbb{Q}$ is Galois, complex conjugation restricts to an element of $\text{Gal}(L/\mathbb{Q})$ whose order divides 2. The group has odd order, so this element is trivial. Thus $L \subseteq \mathbb{R}$, and normality then shows that every embedding of L has real image. $\square$

We next prove divisor descent and the root-of-unity restriction together. The proposition generalizes Jones's quadratic-base argument [8, Lemma 2.1]: its first part descends to a convenient divisor of n , and its second applies root rotation there.

Proposition 2.3. *Let $f \in \mathbb{Q}[y]$ have degree $m \geq 1$, and suppose that $f(x^n)$ is irreducible over $\mathbb{Q}$ with abelian Galois group.*

- (1) *If $e \mid n$, then $f(x^e)$ is irreducible over $\mathbb{Q}$ with abelian Galois group.*
- (2) *If $e \mid n$, then $\varphi(e) \mid me$. In particular, if $p \mid n$ is prime, then $p-1 \mid m$.*

Proof. Fix $e \mid n$ and write $h = n/e$. A nontrivial factorization of $f(x^e)$ would remain nontrivial after the substitution $x \mapsto x^h$, contradicting the irreducibility of

$$f(x^n) = f((x^h)^e).$$

Let L_n and L_e be the splitting fields of $f(x^n)$ and $f(x^e)$, respectively. If γ is a root of $f(x^e)$, choose δ with $\delta^h = \gamma$. Then δ is a root of $f(x^n)$, so $\gamma = \delta^h \in L_n$. Hence $L_e \subseteq L_n$. Every subextension of an abelian Galois extension is Galois and abelian, proving the first assertion.

Having descended to e , we apply root rotation. The case $e = 1$ is immediate, so suppose that $e > 1$. By the first assertion, $f(x^e)$ is irreducible and abelian. Let α be a root and let ζ_e be a primitive e -th root of unity. Since $\deg f(x^e) = me > 1$, irreducibility forces $\alpha \neq 0$, and $f((\alpha\zeta_e)^e) = f(\alpha^e) = 0$. By Lemma 2.1,

$$\alpha\zeta_e \in \mathbb{Q}(\alpha), \quad \zeta_e = \frac{\alpha\zeta_e}{\alpha} \in \mathbb{Q}(\alpha).$$

Consequently,

$$\varphi(e) = [\mathbb{Q}(\zeta_e) : \mathbb{Q}] \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] = me.$$

Taking $e = p$ for a prime $p \mid n$ gives $p - 1 \mid mp$. Since $\gcd(p - 1, p) = 1$, it follows that $p - 1 \mid m$. $\square$

For odd base degree, the prime-divisor restriction has an immediate parity consequence.

Corollary 2.4. *Under the hypotheses of Proposition 2.3, if m is odd, then $n = 2^\ell$ for some $\ell \geq 0$.*

Proof. If an odd prime p divided n , then the even integer $p - 1$ would divide the odd integer m , which is impossible. $\square$

3. COMPOSITIONS WITH EXPONENT 2

For the abelian problem with odd base degree, Corollary 2.4 leaves only powers of 2, and divisor descent reduces every nontrivial case to $f(x^2)$. The following theorem records the resulting field and coefficient structure.

Theorem 3.1 (Abelian structure theorem). *Let $n \geq 1$, and let*

$$f(y) = y^m + c_{m-1}y^{m-1} + \cdots + c_1y + c_0 \in \mathbb{Q}[y]$$

be monic of odd base degree $m \geq 1$, and put $c_m = 1$. Suppose that $f(x^n)$ is irreducible over $\mathbb{Q}$ with abelian Galois group. Then:

- (1) *for every divisor $e \mid n$, the polynomial $f(x^e)$ is irreducible over $\mathbb{Q}$ with abelian Galois group;*
- (2) *for every divisor $e \mid n$, one has $\varphi(e) \mid me$; in particular, every prime $p \mid n$ satisfies $p - 1 \mid m$, and hence $n = 2^\ell$ for some $\ell \geq 0$;*
- (3) *if $n \geq 2$, all the roots of f are real, nonzero, and have the same sign;*
- (4) *if $n \geq 2$, every coefficient c_i is nonzero. If the roots are negative, then $c_i > 0$ for $0 \leq i \leq m$; if the roots are positive, then*

$$(-1)^{m-i}c_i > 0 \quad (0 \leq i \leq m).$$

The proof of Theorem 3.1 passes through a more general analysis of normal exponent-2 compositions. We first characterize normality and then impose commutativity to obtain the abelian square-class criterion.

The group-theoretic input is a standard consequence of the regular permutation representation; again, we include the short proof.

Lemma 3.2. *Let G be a finite group of order $2m$, where m is odd. Then G has a normal subgroup A of order m consisting exactly of the elements of odd order. It is the unique subgroup of index 2, and*

$$G = A \rtimes \langle \tau \rangle,$$

for every involution $\tau \in G$.

Proof. Embed G in the symmetric group on its underlying set by the left regular action, and let $\varepsilon : G \rightarrow \{\pm 1\}$ be the sign character. If g has order r , then its regular permutation is a product of $2m/r$ disjoint r -cycles, and hence

$$\varepsilon(g) = (-1)^{(2m/r)(r-1)}.$$

This sign is 1 when r is odd. If $r = 2s$, then $s \mid m$ and m/s is odd, so the sign is -1 . Thus $A = \ker \varepsilon$ is exactly the set of elements of odd order. Cauchy's theorem supplies an involution, so ε is surjective and $|A| = m$.

Any subgroup of index 2 has odd order and is therefore contained in A , so it equals A . For an involution τ , one has $A \cap \langle \tau \rangle = \{1\}$ and $|A\langle \tau \rangle| = 2m$, so $G = A \rtimes \langle \tau \rangle$. $\square$

For $r \geq 1$, write C_r for the cyclic group of order r , and write $\mathbb{Q}^{\times 2} = \{q^2 : q \in \mathbb{Q}^\times\}$. Let $\tilde{E}$ denote the Galois closure of a number field E inside a fixed algebraic closure of $\mathbb{Q}$. We now prove the normality criterion stated in the introduction.

Theorem 3.3 (Normal exponent-2 criterion). *Let $f \in \mathbb{Q}[y]$ be monic and irreducible of odd base degree m . Let β be a root, put $E = \mathbb{Q}(\beta)$, and let $\tilde{E}$ be the Galois closure of $E/\mathbb{Q}$. Then $f(x^2)$ is irreducible and normal if and only if there are a rational nonsquare d and an element $v \in E^\times$ such that*

$$\beta = dv^2 \quad \text{and} \quad \tilde{E} \subseteq E(\sqrt{d}).$$

When these conditions hold, the splitting field is $E(\sqrt{d})$.

Proof. Assume first that $f(x^2)$ is irreducible and normal. Choose α with $\alpha^2 = \beta$, and put $K = \mathbb{Q}(\alpha)$. Then $K/\mathbb{Q}$ is Galois and

$$[K : \mathbb{Q}] = 2m, \quad [E : \mathbb{Q}] = m, \quad [K : E] = 2.$$

Let $G = \text{Gal}(K/\mathbb{Q})$, let A be the subgroup from Lemma 3.2, and put $F = K^A$. The field F is quadratic, say $F = \mathbb{Q}(\sqrt{d})$ for a rational nonsquare d . Since $[E \cap F : \mathbb{Q}]$ divides both m and 2, one has $E \cap F = \mathbb{Q}$. Hence

$$[EF : E] = 2, \quad [EF : \mathbb{Q}] = 2m = [K : \mathbb{Q}],$$

so $K = EF = E(\sqrt{d})$. Write

$$\alpha = u + v\sqrt{d} \quad (u, v \in E).$$

The coefficient of $\sqrt{d}$ in $\alpha^2 = \beta \in E$ vanishes, so $uv = 0$. If $v = 0$, then $\alpha \in E$, contradicting $[K : E] = 2$. Thus $u = 0$, $v \neq 0$, and

$$\alpha = v\sqrt{d}, \quad \beta = dv^2.$$

Since $K/\mathbb{Q}$ is normal and contains E , it also contains $\tilde{E}$.

Conversely, suppose that $\beta = dv^2$ and $\tilde{E} \subseteq E(\sqrt{d})$. The odd degree of E implies $\sqrt{d} \notin E$. Set

$$\alpha = v\sqrt{d}, \quad K = E(\sqrt{d}).$$

Then $\alpha^2 = \beta$, and $\mathbb{Q}(\alpha)$ contains $E = \mathbb{Q}(\beta)$ and $\sqrt{d} = \alpha/v$. Therefore $\mathbb{Q}(\alpha) = K$ and

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2m = \deg f(x^2),$$

so $f(x^2)$ is the minimal polynomial of α . For every $\mathbb{Q}$ -embedding $\sigma : K \hookrightarrow \overline{\mathbb{Q}}$,

$$\sigma(E) \subseteq \tilde{E} \subseteq K, \quad \sigma(\sqrt{d}) = \pm\sqrt{d}.$$

Thus $\sigma(K) \subseteq K$, and equality follows from the degrees. Hence $K/\mathbb{Q}$ is Galois, so $f(x^2)$ is normal. $\square$

The same argument also determines the group structure and shows exactly how the Galois closure of the base field can sit inside the splitting field.

Proposition 3.4. *Assume the equivalent conditions of Theorem 3.3, and put*

$$K = E(\sqrt{d}), \quad G = \text{Gal}(K/\mathbb{Q}).$$

Let A be the subgroup from Lemma 3.2. Then

$$G \simeq A \rtimes C_2.$$

Moreover, the following are equivalent:

- (a) $G \simeq A \times C_2$;
- (b) G has a unique involution;
- (c) $E/\mathbb{Q}$ is Galois.

Exactly one of the following alternatives holds: either $E/\mathbb{Q}$ is Galois and $\tilde{E} = E$, or $E/\mathbb{Q}$ is not Galois, $[\tilde{E} : E] = 2$, and $\tilde{E} = E(\sqrt{d})$.

Proof. The semidirect-product description follows at once from Lemma 3.2. Since $\mathbb{Q}(\sqrt{d})$ is quadratic, $\text{Gal}(K/\mathbb{Q}(\sqrt{d}))$ has index 2 and hence equals A . Thus, in either direction,

$$\mathbb{Q}(\sqrt{d}) = K^A.$$

Let $H = \text{Gal}(K/E)$, which has order 2. The extension $E/\mathbb{Q}$ is Galois if and only if H is normal in G . A normal subgroup of order 2 is central, and then $G = A \times H$. The nonidentity element of H is then the unique involution because A has odd order. Conversely, if G has a unique involution, the nonidentity element of H is that involution and is central. Hence H is normal and $E/\mathbb{Q}$ is Galois. Finally,

$$E \subseteq \tilde{E} \subseteq E(\sqrt{d}), \quad [E(\sqrt{d}) : E] = 2,$$

so either $\tilde{E} = E$ or $\tilde{E} = E(\sqrt{d})$. The first equality holds exactly when $E/\mathbb{Q}$ is Galois; otherwise the second holds and $[\tilde{E} : E] = 2$. $\square$

Imposing commutativity yields the square-class criterion used in the proof of Theorem 3.1.

Proposition 3.5. *Let f , β , and E be as in Theorem 3.3. Then $f(x^2)$ is irreducible with abelian Galois group if and only if $E/\mathbb{Q}$ is abelian and*

$$\beta = dv^2$$

for some $v \in E^\times$ and $d \in \mathbb{Q}^\times \setminus \mathbb{Q}^{\times 2}$. Equivalently, the square class of β in $E^\times/E^{\times 2}$ comes from a nontrivial rational square class.

When these conditions hold, the splitting field is $E(\sqrt{d})$, its Galois group is $\text{Gal}(E/\mathbb{Q}) \times C_2$, and all the roots of f are real and have the sign of d .

Proof. If $f(x^2)$ is abelian, then it is normal, and every subextension of its splitting field is abelian. Theorem 3.3 therefore gives the stated square-class representation and shows that $E/\mathbb{Q}$ is abelian.

Conversely, suppose that $E/\mathbb{Q}$ is abelian and $\beta = dv^2$. Then $\tilde{E} = E$, so Theorem 3.3 shows that $f(x^2)$ is irreducible and normal with splitting field $E(\sqrt{d})$. The fields E and $\mathbb{Q}(\sqrt{d})$ are Galois of coprime degrees, and hence

$$\text{Gal}(E(\sqrt{d})/\mathbb{Q}) \simeq \text{Gal}(E/\mathbb{Q}) \times C_2,$$

which is abelian. Finally, by Lemma 2.2, E is totally real; hence every conjugate of $\beta = dv^2$ has the sign of d . $\square$

We can now combine divisor descent with the abelian exponent-2 criterion to prove the structure theorem.

Proof of Theorem 3.1. The first assertion is Proposition 2.3(1). The second follows from Proposition 2.3(2) and Corollary 2.4.

Now suppose that $n \geq 2$. Since n is a power of 2, we have $2 \mid n$. Proposition 2.3(1) shows that $f(x^2)$ is irreducible and abelian, so Proposition 3.5 shows that the roots $\beta_1, \dots, \beta_m$ of f are nonzero and have the same sign.

The field-theoretic part is complete; it remains to translate the common sign into coefficient information. For $1 \leq j \leq m$, let e_j denote the j -th elementary symmetric polynomial. Vieta's formulas give

$$c_{m-j} = (-1)^j e_j(\beta_1, \dots, \beta_m).$$

If all β_i are positive, each elementary symmetric function on the right is strictly positive, giving the alternating sign pattern. If all β_i are negative, write $\beta_i = -\gamma_i$ with $\gamma_i > 0$; then

$$c_{m-j} = e_j(\gamma_1, \dots, \gamma_m) > 0.$$

This proves the coefficient-sign assertions and completes the proof. $\square$

4. SPARSITY IN THE UNCOMPOSED CASE

Theorem 3.1 forces the base polynomial to have full support whenever the composition is nontrivial. We now turn to the uncomposed case $n = 1$, when the base and total degrees both equal m . An irreducible abelian polynomial

of odd degree m generates its splitting field, which also has degree m , and is therefore totally real. The coarse estimate $m \leq 2(t-1)$ is the standard sparse-polynomial consequence of Descartes's rule. The following gap-and-sign formulation retains the parity of each exponent gap and identifies the equality case; it may also be viewed as an additive support refinement of de Gua's classical rule for a block of missing terms [2].

Proposition 4.1. *Let*

$$g(x) = \sum_{j=0}^{t-1} a_j x^{e_j} \in \mathbb{R}[x], \quad 0 = e_0 < e_1 < \cdots < e_{t-1} = m,$$

where every a_j is nonzero. Let $N_{\text{nr}}(g)$ be the number of nonreal roots of g , counted with multiplicity. Let r be the number of indices $0 \leq j \leq t-2$ for which $e_{j+1} - e_j$ is odd, and let s be the number of the remaining indices for which $a_j a_{j+1} < 0$. Then

$$N_{\text{nr}}(g) \geq m - r - 2s \geq m - 2(t-1) + r.$$

Write $V(h)$ for the number of sign changes in the sequence of nonzero coefficients of h . If all the roots of g are real, then every exponent gap is 1 or 2, every gap of size 2 joins coefficients of opposite sign, and

$$m = r + 2s = 2(t-1) - r.$$

The numbers of positive and negative roots, counted with multiplicity, are then $V(g)$ and $V(g(-x))$, respectively. Consequently,

$$t \geq \left\lceil \frac{m+2}{2} \right\rceil, \quad t \geq \frac{m+3}{2} \quad \text{if } m \text{ is odd.}$$

In the odd-degree case, equality in the final bound holds exactly when there is one odd exponent gap.

Proof. Descartes's rule of signs bounds the number of positive roots of g by $V(g)$ and the number of negative roots by $V(g(-x))$, where coefficients are ordered by increasing exponent.

Consider two consecutive terms $a_j x^{e_j}$ and $a_{j+1} x^{e_{j+1}}$. Passing from $g(x)$ to $g(-x)$ preserves their relative signs when $e_{j+1} - e_j$ is even and reverses them when the gap is odd. An odd gap contributes exactly 1 to $V(g) + V(g(-x))$. An even gap contributes 2 when its endpoint coefficients have opposite signs and 0 otherwise. Hence

$$V(g) + V(g(-x)) = r + 2s.$$

Since $g(0) \neq 0$, none of its roots is zero. The number of real roots is therefore at most $r + 2s$, and

$$N_{\text{nr}}(g) \geq m - r - 2s.$$

There are $t-1-r$ even gaps, so $s \leq t-1-r$, proving the second inequality.

Now suppose that all roots are real. Each odd gap is at least 1, and each even gap is at least 2, so

$$m = \sum_{j=0}^{t-2} (e_{j+1} - e_j) \geq 2(t-1) - r \geq r + 2s.$$

Since $N_{\text{nr}}(g) = 0$, the preceding lower bound gives $m \leq r + 2s$. Combining this with the displayed chain forces equality throughout. Thus every odd gap is 1, every even gap is 2, and $s = t - 1 - r$, proving the structural assertions. Equality in both of Descartes's bounds follows because their sum is the total number of roots.

Finally, $m = 2(t-1) - r$ gives the general support bound. The integers m and r have the same parity, so $r \geq 1$ when m is odd; the odd-degree bound follows, with equality exactly when $r = 1$. $\square$

Corollary 4.2. *Let $g \in \mathbb{Q}[x]$ be irreducible, totally real, and of degree $m \geq 2$. If g has exactly t nonzero terms, then*

$$m \leq 2(t-1).$$

In particular, a totally real irreducible trinomial has degree at most 4, and if m is odd, then

$$t \geq \frac{m+3}{2}.$$

Proof. Irreducibility and $m \geq 2$ imply that the constant term of g is nonzero, so Proposition 4.1 applies. $\square$

The proposition itself requires neither irreducibility nor separability: Descartes's rule already counts roots with multiplicity. In passing to the corollary, irreducibility is used only to ensure a nonzero constant term. Without that condition, the monomial x^m shows that no degree bound in terms of support is possible.

Proof of Theorem 1.2. Suppose first that $n = 1$, which is the power 2^0 . By Lemma 2.1, the splitting field of f has degree m . Lemma 2.2 therefore shows that f is totally real, and Corollary 4.2 gives $t \geq (m+3)/2$.

If $n \geq 2$, parts (2) and (4) of Theorem 3.1 show that n is a power of 2 and every coefficient of f is nonzero. Hence $t = m + 1$. $\square$

The trinomial conclusion follows by combining the two cases of Theorem 1.2

Proof of Theorem 1.1. The base trinomial $f(y) = y^m + ay^k + b$ has $t = 3$ nonzero terms. If $n \geq 2$, then Theorem 1.2 gives $3 = m + 1$, contradicting the hypothesis that $m \geq 3$. Thus $n = 1$, and the same theorem gives $3 \geq (m+3)/2$. Hence $m \leq 3$, so $m = 3$. $\square$

The cubic realizing the exceptional pair is the first member of an infinite family that attains the odd-degree support bound.

Proposition 4.3. *For every $r \geq 1$, put $m = 3^r$, and let T_m be the Chebyshev polynomial of the first kind. Then*

$$P_m(x) = 2T_m(x/2) + 1$$

is an irreducible abelian polynomial of degree m with exactly $(m+3)/2$ nonzero terms. Its Galois group is cyclic of order m .

Proof. Let ζ be a primitive 3^{r+1} -st root of unity and put $\theta = \zeta + \zeta^{-1}$. The defining identity for T_m gives

$$2T_m(\theta/2) = \zeta^m + \zeta^{-m} = -1,$$

so $P_m(\theta) = 0$. Moreover,

$$[\mathbb{Q}(\theta) : \mathbb{Q}] = \frac{\varphi(3^{r+1})}{2} = 3^r = m.$$

Since P_m is monic of degree m , it is the minimal polynomial of θ . Its splitting field is the maximal real subfield of $\mathbb{Q}(\zeta)$, and

$$\text{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}) \simeq (\mathbb{Z}/3^{r+1}\mathbb{Z})^\times / \{\pm 1\} \simeq C_m.$$

For odd m , the coefficient formula

$$2T_m(x/2) = \sum_{j=0}^{(m-1)/2} (-1)^j \frac{m}{m-j} \binom{m-j}{j} x^{m-2j}$$

has no zero coefficient. Adding the constant term gives exactly $(m+3)/2$ nonzero terms: all exponents in the displayed sum are odd, so the added constant is a new term. In particular,

$$P_3(x) = x^3 - 3x + 1,$$

which realizes the exceptional pair in Theorem 1.1. $\square$

The next member of the Chebyshev family occurs at $m = 9$, i.e.,

$$P_9(x) = x^9 - 9x^7 + 27x^5 - 30x^3 + 9x + 1;$$

equality also occurs outside this power-of-3 family, as the next example shows.

Example 4.4. The bound in Theorem 1.2 is attained in base degree $m = 5$, where it requires 4 nonzero terms. Let ζ be a primitive 11-th root of unity and put

$$\theta = \zeta + \zeta^{-1}, \quad K = \mathbb{Q}(\theta) = \mathbb{Q}(\zeta)^+,$$

where $\mathbb{Q}(\zeta)^+$ denotes the maximal real subfield. Writing $s_j = \zeta^j + \zeta^{-j}$, the recurrence $s_j = \theta s_{j-1} - s_{j-2}$ for $j \geq 2$, together with $1 + \sum_{j=1}^5 s_j = 0$, gives

$$p(\theta) = 0, \quad p(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.$$

Moreover,

$$[K : \mathbb{Q}] = 5, \quad \text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/11\mathbb{Z})^\times / \{\pm 1\} \simeq C_5,$$

so p is the minimal polynomial of θ . To obtain a generator with a sparser minimal polynomial, set

$$\gamma = 4\theta - \theta^3.$$

Reduction modulo $p(\theta) = 0$ gives

$$\gamma^3 = 8 + 30\theta - 13\theta^2 - 8\theta^3 + 3\theta^4,$$

$$\gamma^5 = 77 + 242\theta - 143\theta^2 - 66\theta^3 + 33\theta^4.$$

Therefore

$$q(\gamma) = 0, \quad q(x) = x^5 - 11x^3 + 22x + 11.$$

Modulo 2, the polynomial q becomes $x^5 + x^3 + 1$, which has no linear factor. The only irreducible quadratic over $\mathbb{F}_2$ is $x^2 + x + 1$, and division by it leaves the nonzero remainder $x + 1$. Thus q has no factor of degree 1 or 2. Every reducible quintic has an irreducible factor of degree at most 2, so q is irreducible over $\mathbb{F}_2$, and hence over $\mathbb{Q}$.

Because q is irreducible and $q(\gamma) = 0$, one has $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 5$, and hence $\mathbb{Q}(\gamma) = K$. Since $K/\mathbb{Q}$ is Galois, it is the splitting field of q , with $\text{Gal}(K/\mathbb{Q}) \simeq C_5$. Thus q is a totally real cyclic quintic with exactly four nonzero terms. Its support is $\{0, 1, 3, 5\}$, so exactly one consecutive exponent gap is odd, while q and $q(-x)$ have respectively 2 and 3 sign changes. In particular, $5 = 2(4 - 1) - 1$, and equality holds in Proposition 4.1.

5. APPLICATIONS AND EXAMPLES

As applications, we first extract the lacunarity obstruction and apply the trinomial classification to the motivating cubic monogenic families. We then show that the full-support conclusion is sharp, first through a monogenic sextic and then through a realization theorem covering every odd base degree and every positive power-of-2 composition exponent. We close with a cyclotomic consequence.

5.1. Lacunarity and the motivating cubic families.

Corollary 5.1. *Let $f \in \mathbb{Q}[y]$ be monic and lacunary of odd base degree. Then $f(x^n)$ cannot be both irreducible over $\mathbb{Q}$ and abelian for any $n \geq 2$.*

Proof of Corollary 5.1. If $n \geq 2$ and $f(x^n)$ were irreducible and abelian, Theorem 3.1(4) would force every coefficient of f to be nonzero, contrary to the hypothesis. $\square$

Returning to the motivating cubic-base families, Theorem 1.1 gives the following reduction.

Corollary 5.2. *Let $n \geq 1$ and $a, b \in \mathbb{Z}$ with $ab \neq 0$. If either*

$$x^{3n} + ax^n + b \quad \text{or} \quad x^{3n} + ax^{2n} + b$$

is abelian monogenic, then $n = 1$.

Proof. Theorem 1.1, with $m = 3$ and $k = 1$ or 2 , forces $n = 1$ before monogenicity is used. $\square$

Corollary 5.2 reduces the monogenic question to the uncomposed cubic case $n = 1$, where Jones's classifications apply. For $A, B \in \mathbb{Z}$ with $AB \neq 0$, he proves that the only abelian monogenic polynomials of the $y^3 + Ay^2 + B$ shape are the following four [5, Theorem 1.1(2)]:

$$y^3 + 3y^2 - 3, \quad y^3 - 3y^2 + 3, \quad y^3 - 3y^2 + 1, \quad y^3 + 3y^2 - 1.$$

For the $y^3 + Ay + B$ shape, he constructs two infinite families whose members have pairwise distinct splitting fields [5, Theorem 1.1(1)]; he notes that these families are not exhaustive [5, Section 4].

5.2. Sharpness and full-support realizations. The lacunarity assumption in Corollary 5.1 cannot be removed. The converse in Proposition 3.5 suggests how to construct an example: start with an odd-degree abelian field and choose a rational nonsquare times a square in that field.

Example 5.3. Let θ be a root of $z^3 - 3z + 1$. This polynomial is irreducible and has discriminant 81, so its splitting field $E = \mathbb{Q}(\theta)$ is cyclic of degree 3. Put $\beta = -\theta^2$. The identity

$$\theta(\beta + 3) = \theta(3 - \theta^2) = 1$$

shows that $E = \mathbb{Q}(\beta)$, and squaring $\theta = (\beta + 3)^{-1}$ gives

$$\beta(\beta + 3)^2 + 1 = 0.$$

Since $E = \mathbb{Q}(\beta)$ has degree 3, this cubic relation is the minimal polynomial of β :

$$f(y) = y^3 + 6y^2 + 9y + 1.$$

Here $\beta = (-1)\theta^2$, with $-1 \in \mathbb{Q}^\times \setminus \mathbb{Q}^{\times 2}$. Since $E/\mathbb{Q}$ is cyclic, Proposition 3.5 shows that

$$f(x^2) = x^6 + 6x^4 + 9x^2 + 1$$

is irreducible, has splitting field $E(i)$, where $i^2 = -1$, and has cyclic Galois group $C_3 \times C_2 \simeq C_6$. Jones proved that this polynomial is monogenic [6, Theorem 1.1(2)]; it also appears in König's subsequent preprint, which gives a complete classification of monogenic even sextic polynomials with Galois group C_6 [10, Theorem 1.1]. Its cubic base has no zero coefficients, and all of them are positive, as Theorem 3.1 requires. Thus the lacunarity assumption in Corollary 5.1 is essential.

The sextic in Example 5.3 shows that a nontrivial abelian composition attaining the full-support conclusion can also be monogenic. Without the monogenicity requirement, that conclusion is attained for every odd base degree $m \geq 1$ and every composition exponent $n = 2^\ell$, $\ell \geq 1$.

Proposition 5.4. *For every odd integer $m \geq 1$ and every $n = 2^\ell$, with $\ell \geq 1$, there is a monic irreducible polynomial $f \in \mathbb{Z}[y]$ of degree m such that $f(x^n)$ is irreducible and abelian. Every coefficient of f is positive.*

Proof. Choose a totally real cyclic extension $E/\mathbb{Q}$ of degree m . Such an extension exists for every m : by Dirichlet's theorem on primes in arithmetic progressions, one may choose a prime $q \equiv 1 \pmod{2m}$ and take the degree- m subfield of the maximal real subfield of $\mathbb{Q}(\zeta_q)$. Choose an integral primitive element $u \in E$. After replacing u by $v = u + C$ for a sufficiently large integer C , every conjugate of v is positive; these conjugates remain pairwise distinct.

Put $\beta = -v^n$. Since the positive conjugates of v are distinct, so are their n -th powers; hence $\mathbb{Q}(\beta) = E$. Let $f \in \mathbb{Z}[y]$ be the minimal polynomial of β . Its roots are the negative numbers $-\sigma(v)^n$, with σ ranging over $\text{Gal}(E/\mathbb{Q})$, and therefore

$$f(y) = \prod_{\sigma \in \text{Gal}(E/\mathbb{Q})} (y + \sigma(v)^n)$$

has positive coefficients.

Let ξ be a primitive $2n$ -th root of unity. Since n is a power of 2,

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(2n) = n, \quad \xi^n = -1.$$

The degrees m and n are coprime, so $[E\mathbb{Q}(\xi) : \mathbb{Q}] = mn$. Set $\alpha = v\xi$. Then $\alpha^n = \beta$, whence $E = \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$; because $v \in E$, one also has $\xi = \alpha/v \in \mathbb{Q}(\alpha)$. Thus

$$\mathbb{Q}(\alpha) = E\mathbb{Q}(\xi).$$

This is an abelian extension of degree mn . The polynomial $f(x^n)$, which has α as a root and degree mn , is therefore the minimal polynomial of α . Its root field is abelian and Galois, so it is also the splitting field; hence $f(x^n)$ is abelian. $\square$

For example, let $\theta^3 - 3\theta + 1 = 0$, put $v = \theta + 2$, and take $n = 4$. The three conjugates of v are positive and distinct, and, using $\theta^3 = 3\theta - 1$, one obtains

$$\beta = -27\theta^2 - 55\theta - 8.$$

Direct reduction in the basis $1, \theta, \theta^2$ gives

$$\beta^3 + 186\beta^2 + 4725\beta + 1 = 0,$$

so the minimal polynomial of β is

$$f(y) = y^3 + 186y^2 + 4725y + 1.$$

Consequently,

$$f(x^4) = x^{12} + 186x^8 + 4725x^4 + 1$$

is irreducible and abelian. This gives a concrete cubic-base example beyond composition exponent 2.

5.3. A cyclotomic consequence. Jones's quadratic-base classification contains cyclotomic families [8, Theorem 1.4(4)–(7)], so it is natural to ask whether trinomials of odd base degree can also be cyclotomic. Theorem 1.1 reduces the question to $m = 3$ and $n = 1$; parity of cyclotomic degrees eliminates that case.

Corollary 5.5. *Let $f(y) = y^m + ay^k + b$, where the base degree $m \geq 3$ is odd, $1 \leq k < m$, and $a, b \in \mathbb{Q}^\times$. For every $n \geq 1$, the power composition $f(x^n) = x^{mn} + ax^{kn} + b$ is not cyclotomic.*

Proof. Suppose that $f(x^n)$ equals the N -th cyclotomic polynomial Φ_N . Since Φ_N is irreducible and abelian, Theorem 1.1 gives $m = 3$ and $n = 1$. Thus $\deg \Phi_N = 3$, which is impossible: $\varphi(N)$ is even for $N > 2$, while Φ_1 and Φ_2 have degree 1. $\square$

6. NORMAL COMPOSITIONS

Having established the exponent-2 normality criterion, we now draw its consequences without assuming commutativity. The rational square class persists, but its sign determines whether the coefficient obstruction survives.

Corollary 6.1. *Under the equivalent conditions of Theorem 3.3, put $K = E(\sqrt{d})$, the splitting field of $f(x^2)$. Then the sign of d has the following consequences.*

If $d > 0$, then K is totally real, every root of f is positive, and, writing

$$f(y) = y^m + c_{m-1}y^{m-1} + \cdots + c_0,$$

where $c_m = 1$, one has

$$(-1)^{m-i}c_i > 0 \quad (0 \leq i \leq m).$$

If $d < 0$, then K is totally imaginary and every real root of f is negative.

Proof. By Proposition 3.4,

$$A = \text{Gal}(K/\mathbb{Q}(\sqrt{d}))$$

is the odd-order subgroup from Lemma 3.2. In particular, $\mathbb{Q}(\sqrt{d}) = K^A$ is the unique quadratic subfield of K , so the square class of d , and hence its sign, is intrinsic. Fix an embedding $K \subseteq \mathbb{C}$, and let $c \in \text{Gal}(K/\mathbb{Q})$ be complex conjugation.

If $d > 0$, then c fixes $\sqrt{d}$, so $c \in A$. The group A has odd order and $c^2 = 1$, whence $c = 1$. Thus K is totally real. Every conjugate of $\beta = dv^2$ is positive, and the coefficient signs follow from Vieta's formulas.

If $d < 0$, then complex conjugation acts nontrivially on $\mathbb{Q}(\sqrt{d})$. Thus K is not totally real; since $K/\mathbb{Q}$ is Galois, it has no real embeddings. If β' is a real root of f , the embedding $\sigma : E \hookrightarrow \mathbb{R}$ sending β to β' gives

$$\beta' = d\sigma(v)^2 < 0. \quad \square$$

Lacunarity can occur only in the negative case, and then $E/\mathbb{Q}$ must be non-Galois.

Corollary 6.2. *Let $f \in \mathbb{Q}[y]$ be monic, irreducible, lacunary, and of odd base degree, let β be a root of f , and put $E = \mathbb{Q}(\beta)$. Suppose that $f(x^2)$ is irreducible and normal. Choose $d \in \mathbb{Q}^\times \setminus \mathbb{Q}^{\times 2}$ and $v \in E^\times$ with $\beta = dv^2$, as in Theorem 3.3, and put $K = E(\sqrt{d})$. Then $d < 0$, K is totally imaginary, $E/\mathbb{Q}$ is not Galois, and every real root of f is negative.*

Proof. If $d > 0$, Corollary 6.1 makes every coefficient of f nonzero, contrary to lacunarity. Hence $d < 0$; the same corollary then makes K totally imaginary and every real root of f negative.

If $E/\mathbb{Q}$ were Galois, then it would be totally real by Lemma 2.2. Every conjugate of $\beta = dv^2$ would then be negative, and Vieta's formulas would make every coefficient of f positive. Thus $E/\mathbb{Q}$ is not Galois. $\square$

The following example realizes the non-Galois, totally imaginary alternative in Corollary 6.2 and shows that coefficient nonvanishing can fail.

Example 6.3. Let

$$f(y) = y^3 + 108, \quad \rho = \sqrt[3]{2}, \quad s = \sqrt{-3},$$

so the base degree is 3. Put $\beta = -3\rho^2$ and $\alpha = s\rho$. Then

$$\beta^3 = -108, \quad \alpha^2 = \beta, \quad \alpha^6 = -108.$$

Moreover, $\rho = \beta^2/18$, so $E = \mathbb{Q}(\beta) = \mathbb{Q}(\rho)$. Eisenstein's criterion at 2, applied to $x^3 - 2$, gives $[E : \mathbb{Q}] = 3$. Since $E = \mathbb{Q}(\beta)$ and $f(\beta) = 0$, this proves that f is irreducible. The identities

$$s = -\frac{\alpha^3}{6}, \quad \rho = \frac{\alpha^4}{18}$$

show that

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\rho, s).$$

Since $\mathbb{Q}(\rho) \subseteq \mathbb{R}$ whereas $s \notin \mathbb{R}$, one has $[\mathbb{Q}(\rho, s) : \mathbb{Q}(\rho)] = 2$, and hence $[\mathbb{Q}(\rho, s) : \mathbb{Q}] = 6$. Thus $x^6 + 108$ is the minimal polynomial of α . Moreover, $\mathbb{Q}(\rho, s)$ is the splitting field of $x^3 - 2$, because it contains ρ and

$$\zeta_3 = \frac{-1 + s}{2}.$$

Consequently, $x^6 + 108$ is irreducible and normal, with Galois group S_3 . Here

$$\beta = (-3)\rho^2,$$

so this is the negative square-class case. The cubic root field $\mathbb{Q}(\rho)$ is not normal. Thus normality need not descend from $f(x^2)$ to f , and the abelian lacunarity obstruction therefore fails for normal nonabelian polynomials.

Since $S_3 \simeq D_3$, the example also falls under a complementary result of König: no monogenic even polynomial $g(x^2)$, with base g of odd degree $m \geq 3$, has the dihedral group D_m of order $2m$ as its Galois group in the regular action [10, Lemma 4.2]. In particular, $x^6 + 108$ is not monogenic.

The quadratic field in the criterion can sometimes be read from the discriminant, but not always.

Remark 6.4. In the non-Galois alternative of Proposition 3.4, the field $\mathbb{Q}(\sqrt{d})$ is the unique quadratic subfield of $\tilde{E}$. If the polynomial discriminant $\Delta(f)$ is not a square in $\mathbb{Q}$, then

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta(f)}).$$

Indeed, the discriminant character is then a nontrivial homomorphism from $\text{Gal}(\tilde{E}/\mathbb{Q})$ to C_2 , whose kernel must be the unique subgroup of index 2. When $\Delta(f)$ is a square, however, $\mathbb{Q}(\sqrt{\Delta(f)}) = \mathbb{Q}$, so the discriminant does not identify the quadratic subfield. For instance, a quintic with Galois group D_5 , where D_5 denotes the dihedral group of order 10, has square discriminant because the natural degree-5 action of D_5 lies in A_5 , even though its Galois closure has a quadratic subfield.

For an arbitrary composition exponent n , root rotation still yields a restriction at n , but normality need not descend to its divisors.

Proposition 6.5. *Let $f \in \mathbb{Q}[y]$ be monic and irreducible of odd base degree m , and suppose that $f(x^n)$ is irreducible and normal. Then*

$$\varphi(n) \mid mn.$$

If n is odd, then $n = 1$.

Proof. For $n = 1$, the divisibility is immediate. Suppose that $n \geq 2$, and let α be a root of $f(x^n)$, and let ζ_n be a primitive n -th root of unity. Irreducibility forces $\alpha \neq 0$. Since $\alpha\zeta_n$ is another root and $\mathbb{Q}(\alpha)$ is the splitting field,

$$\zeta_n = \frac{\alpha\zeta_n}{\alpha} \in \mathbb{Q}(\alpha).$$

Thus $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\alpha)$, and therefore $\varphi(n) \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] = mn$. If $n \geq 3$ is odd, then $\varphi(n)$ is even whereas mn is odd, a contradiction. $\square$

For base degree $m = 3$, this necessary numerical condition can be solved exactly, as follows.

Theorem 6.6. (1) *The positive integer solutions of $\varphi(n) \mid 3n$ are*

$$n = 1, \quad n = 2^r, \quad n = 2^r 3^s, \quad \text{or} \quad n = 2^r 7^s,$$

where $r \geq 1$, and $s \geq 1$ in the last two families. Consequently, every exponent occurring in an irreducible normal composition with cubic base belongs to this list.

(2) *For each $p \in \{3, 7\}$, there is a monic irreducible cubic $f_p \in \mathbb{Z}[y]$ such that $f_p(x^{2^p})$ is irreducible and normal, whereas $f_p(x^p)$ is irreducible but not normal.*

The numerical list is a necessary condition, not an existence theorem for every entry. Its two possible odd prime divisors are nevertheless realized in part (2), at composition exponents 6 and 14.

Proof of Theorem 6.6(1). Proposition 6.5 shows that every exponent in an irreducible normal cubic-base composition satisfies $\varphi(n) \mid 3n$. It remains to classify the solutions of this divisibility.

Let $R = \text{rad}(n)$ be the product of the distinct primes dividing n . Since

$$\varphi(n) = \frac{n}{R} \varphi(R),$$

the divisibility is equivalent to $\varphi(R) \mid 3R$. The case $R = 1$ gives $n = 1$. If $R > 1$ were odd, then $\varphi(R)$ would be even while $3R$ is odd. Thus $2 \mid R$ whenever $n \geq 2$.

Let S be the set of odd primes dividing R , and let v_2 denote the 2-adic valuation. Since R is squarefree and even, $v_2(3R) = 1$, whereas

$$v_2(\varphi(R)) = \sum_{p \in S} v_2(p-1).$$

Taking 2-adic valuations in $\varphi(R) \mid 3R$ therefore gives

$$\sum_{p \in S} v_2(p-1) \leq 1.$$

Every summand is at least 1, so S contains at most one prime. If $S = \{p\}$, then $p-1 \mid 6p$. Since $\gcd(p-1, p) = 1$, one has $p-1 \mid 6$, and hence $p = 3$ or $p = 7$. Conversely, $3R/\varphi(R)$ equals 6, 9, and 7 when the set of prime divisors of R is respectively $\{2\}$, $\{2, 3\}$, or $\{2, 7\}$. $\square$

We next construct the examples in Theorem 6.6(2).

Proof of Theorem 6.6(2). The ambient field. For $p = 3$, put $q = 9$; for $p = 7$, put $q = 7$. Let ζ_q be a primitive q -th root of unity, and put $\zeta_p = \zeta_q^{q/p}$. Let

$$C = \mathbb{Q}(\zeta_q), \quad E = \mathbb{Q}(\zeta_q + \zeta_q^{-1}), \quad z = 2 + \zeta_q + \zeta_q^{-1}, \quad w = \sqrt[p]{2}.$$

The field E is the maximal real subfield of C and is cyclic cubic; moreover, z is an algebraic integer generating E .

Choose $s \in C$ with $s^2 = -p$. For $p = 3$, one may take $s = 1 + 2\zeta_3$; for $p = 7$, the quadratic Gauss sum

$$s = \zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6$$

has square -7 . Put

$$K = C(w), \quad \alpha = swz, \quad \beta = \alpha^{2p} = 4(-p)^p z^{2p}.$$

For $p = 7$, degree coprimality gives $[K : \mathbb{Q}] = 42$. For $p = 3$, the intersection $C \cap \mathbb{Q}(w)$ equals $\mathbb{Q}$. Indeed, because $[\mathbb{Q}(w) : \mathbb{Q}] = 3$, a nontrivial intersection would equal $\mathbb{Q}(w)$, placing the non-Galois cubic $\mathbb{Q}(w)$ inside the abelian extension $C/\mathbb{Q}$. Hence $[K : \mathbb{Q}] = 18$. In both cases $[K : \mathbb{Q}] = 6p$, and $K/\mathbb{Q}$ is Galois because C contains ζ_p and K is the compositum of C with the splitting field of $x^p - 2$.

The root α . Every $\sigma \in \text{Gal}(K/\mathbb{Q})$ is determined by $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ and $j \in \mathbb{Z}/p\mathbb{Z}$ through

$$\sigma(\zeta_q) = \zeta_q^a, \quad \sigma(w) = \zeta_p^j w.$$

Write $\varepsilon(a) \in \{\pm 1\}$ for the sign defined by $\sigma(s) = \varepsilon(a)s$. If σ fixes α , then

$$\varepsilon(a)\zeta_p^j(2 + \zeta_q^a + \zeta_q^{-a}) = 2 + \zeta_q + \zeta_q^{-1}.$$

The three conjugates of z are positive and distinct: they have the form $2 + 2\cos(2\pi a/q) \in (0, 4)$, and distinctness follows because z generates E . Taking absolute values therefore gives $a \equiv \pm 1 \pmod{q}$. If $a \equiv 1 \pmod{q}$,

then $j = 0$. If $a \equiv -1 \pmod{q}$, the restriction of σ to C is complex conjugation, so $\sigma(s) = -s$. The displayed equality would then require $\zeta_p^j = -1$, which is impossible for odd p . Thus α has trivial stabilizer and $\mathbb{Q}(\alpha) = K$.

The cubic base. The three conjugates of $\beta = 4(-p)^p z^{2p}$ are distinct, so $\mathbb{Q}(\beta) = E$. Since z is integral, so is β . Let f_p be the minimal polynomial of β . Then f_p is a monic irreducible cubic in $\mathbb{Z}[y]$, while $f_p(x^{2p})$ has α as a root and degree $6p = [K : \mathbb{Q}]$. It is therefore the minimal polynomial of α , and it is normal because $K/\mathbb{Q}$ is Galois.

Explicit coefficients. The coefficients can also be written explicitly. Write $\text{minpoly}_{\mathbb{Q}}(u)$ for the minimal polynomial of an algebraic number u over $\mathbb{Q}$, and define A_p, B_p by

$$\text{minpoly}_{\mathbb{Q}}(z^{2p}) = U^3 - A_p U^2 + B_p U - 1,$$

and put $c_p = 4(-p)^p$. Then

$$f_p(y) = y^3 - A_p c_p y^2 + B_p c_p^2 y - c_p^3.$$

The required minimal polynomials are

p	$\text{minpoly}_{\mathbb{Q}}(z)$	$\text{minpoly}_{\mathbb{Q}}(z^{2p})$
3	$X^3 - 6X^2 + 9X - 1$	$U^3 - 2109U^2 + 324786U - 1$
7	$X^3 - 5X^2 + 6X - 1$	$U^3 - 14478659U^2 + 6994805571U - 1$

The displayed minimal polynomials of z follow by eliminating ζ_q from $\Phi_q(\zeta_q) = 0$, or equivalently by translating the minimal polynomial of $\zeta_q + \zeta_q^{-1}$. Reducing powers modulo these polynomials then gives

$$(z^{2p})^3 - A_p(z^{2p})^2 + B_p z^{2p} - 1 = 0.$$

The three positive conjugates of z are distinct, so their $2p$ -th powers are distinct. The displayed cubic is therefore the minimal polynomial of z^{2p} .

Descent. Finally, $f_p(x^p)$ is irreducible: any factorization would remain after substituting x^2 , contradicting the irreducibility of $f_p(x^{2p})$. The element $\alpha^2 = -pw^2 z^2$ is a real root of $f_p(x^p)$, so its root field is contained in $\mathbb{R}$. If this polynomial were normal, then the other root $\alpha^2 \zeta_p$ would belong to its root field, and hence

$$\zeta_p = \frac{\alpha^2 \zeta_p}{\alpha^2} \in \mathbb{Q}(\alpha^2) \subseteq \mathbb{R},$$

a contradiction. □

The construction isolates the difference between abelianness and normality. At base degree $m = 3$, the divisibility condition permits only 3 and 7 as odd prime divisors of the composition exponent. Theorem 6.6(2) realizes them at exponents 6 and 14, whereas the descended compositions at exponents 3 and 7 remain irreducible but are not normal. By contrast, in the abelian setting both irreducibility and abelianness descend and force the composition exponent to be a power of 2.

7. FURTHER QUESTIONS

The preceding results leave several natural questions:

- (1) For which odd $m \geq 3$ is the bound $(m+3)/2$ attained by an irreducible abelian polynomial of degree m ? Is it attained for every odd m ?
- (2) Can one classify all abelian monogenic trinomials of the form $y^3 + Ay + B$? Jones's two infinite families are explicitly nonexhaustive [5, Section 4].
- (3) Which mixed exponents $2^r 3^s$ and $2^r 7^s$, with $r, s \geq 1$, occur in irreducible normal cubic-base compositions?

REFERENCES

1. Henri Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.
2. Jean-Paul de Gua de Malves, *Démonstrations de la règle de Descartes, pour connoître le nombre des racines positives & négatives dans les equations qui n'ont point de racines imaginaires*, Mémoires de mathématique et de physique tirés des registres de l'Académie Royale des Sciences (1741), 72–96.
3. Joshua Harrington and Lenny Jones, *The irreducibility of power compositional sextic polynomials and their Galois groups*, Math. Scand. **120** (2017), no. 2, 181–194.
4. ———, *The irreducibility and monogenicity of power-compositional trinomials*, Math. J. Okayama Univ. **67** (2025), no. 1, 53–65.
5. Lenny Jones, *Monogenic cyclic cubic trinomials*, Bol. Soc. Mat. Mex. (3) **31** (2025), Paper No. 28.
6. ———, *Monogenic even cyclic sextic polynomials*, Math. Slovaca **75** (2025), no. 5, 1021–1034.
7. ———, *Monogenic even sextic trinomials and their Galois groups*, Arch. Math. (Brno) **62** (2026), no. 1, 19–41.
8. ———, *A note on abelian monogenic trinomials*, Bull. Aust. Math. Soc. (2026), 1–5, First View.
9. Sumandeep Kaur, Surender Kumar, and László Remete, *On the index of power compositional polynomials*, Finite Fields Appl. **107** (2025), Paper No. 102642.
10. Joachim König, *A note on monogenic even polynomials*, 2025, arXiv:2505.10119.
11. Andrzej Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), no. 3, 245–274.
12. ———, *Addendum and corrigendum to the paper “Abelian binomials, power residues and exponential congruences”*, Acta Arith. **36** (1980), no. 1, 101–104.
13. William Yslas Vélez, *On normal binomials*, Acta Arith. **36** (1980), no. 2, 113–124.

HARVARD BUSINESS SCHOOL; DEPARTMENT OF ECONOMICS AND CENTER OF MATHEMATICAL SCIENCES AND APPLICATIONS, HARVARD UNIVERSITY; AND A16Z CRYPTO
 Email address: `kominers@fas.harvard.edu`