ARCHIVUM MATHEMATICUM (BRNO)
Tomus 62 (2026), 19–41

MONOGENIC EVEN SEXTIC TRINOMIALS AND THEIR GALOIS GROUPS

Lenny Jones

Abstract. Let $f(x)=x^6+Ax^{2k}+B\in\mathbb{Z}[x]$, with $A\neq 0$ and $k\in\{1,2\}$. We say that $f(x)$ is *monogenic* if $f(x)$ is irreducible over $\mathbb{Q}$ and $\{1,\theta,\theta^2,\theta^3,\theta^4,\theta^5\}$ is a basis for the ring of integers of $\mathbb{Q}(\theta)$, where $f(\theta)=0$.

For each value of k and each possible Galois group G of $f(x)$ over $\mathbb{Q}$, we use a theorem of Jakhar, Khanduja and Sangwan to give explicit descriptions of all monogenic trinomials $f(x)$ having Galois group G. We also determine when these descriptions provide infinitely many such trinomials, and we investigate when these trinomials generate distinct sextic fields.

These results extend recent work on monogenic power-compositional sextic trinomials of the form $g(x^3)$ to the situation $g(x^2)$, and thereby complete the characterization, in terms of their Galois groups, of monogenic power-compositional sextic trinomials.

1. Introduction

Let

$$f(x)=x^6+Ax^{2k}+B\in\mathbb{Z}[x],\quad \text{where } A\neq 0 \text{ and } k\in\{1,2\}. \tag{1.1}$$

If $f(x)$ is irreducible over $\mathbb{Q}$, then we define $f(x)$ to be *monogenic* if

$$\mathcal{B}=\{1,\theta,\theta^2,\theta^3,\theta^4,\theta^5\}$$

is a basis for the ring of integers of $\mathbb{Q}(\theta)$, where $f(\theta)=0$. Such a basis $\mathcal{B}$ is sometimes referred to in the literature as a *power basis*. We say that two such monogenic sextic trinomials $f_1(x)\neq f_2(x)$ having isomorphic Galois groups over $\mathbb{Q}$ are *distinct* if $K_1\neq K_2$, where $K_i=\mathbb{Q}(\theta_i)$ with $f_i(\theta_i)=0$.

The goal of this article is to provide a characterization of the monogenic sextic trinomials $f(x)$ described in (1.1) in terms of their Galois groups over $\mathbb{Q}$, which we denote $\mathrm{Gal}(f)$. More explicitly, for each possible Galois group G, we use a theorem of Jakhar, Khanduja and Sangwan [15] to derive conditions that allow us to present an explicit description of all such monogenic sextic trinomials $f(x)$ in (1.1) with $\mathrm{Gal}(f)\simeq G$. We also investigate when these trinomials generate distinct sextic fields.

2020 *Mathematics Subject Classification*: primary 11R09; secondary 11R32, 11R21.
Key words and phrases: monogenic, even sextic, trinomial, Galois, power-compositional.
Received January 30, 2026. Editor C. Greither.
DOI: 10.5817/AM2026-1-19

We point out that similar research involving the monogenicity and/or Galois groups of trinomials of various degrees has been conducted by many authors [1, 2, 4, 5, 6, 11, 12, 14, 16, 17, 18, 19, 20, 21, 22, 23, 24, 26]. The results in this article extend previous work on sextic trinomials of the form $g(x^3) = x^6 + Ax^3 + B$ [11,17,18] to sextic trinomials of the form $g(x^2)$, and thereby complete the characterization, in terms of their Galois groups, of monogenic power-compositional sextic trinomials. In particular, in this article, for $f(x)$ as defined in (1.1), we see that

$$f(x) = g(x^2), \quad \text{where} \quad g(x) = x^3 + Ax^k + B. \tag{1.2}$$

We make some additional notational remarks. Let $m, n \in \mathbb{Z}$, with $m \geq 2$. We let the notation "$n \bmod m$" denote the unique integer $z \in \{0, 1, 2, \ldots, m-1\}$ such that $n \equiv z \pmod m$. That is, $n \bmod m = z$. We let $\nu_p(n)$ be the p-adic valuation of n, and for $n > 0$, we let $\operatorname{rad}(n)$, called the "radical" of n, be the product of all distinct prime divisors of n. We let C_n denote the cyclic group of order n, A_n denote the alternating group of order $n!/2$ and S_n denote the symmetric group of order $n!$. Furthermore, S_4^+ denotes the symmetric group S_4 as a subgroup of S_6 embedded in A_6, and S_4^- denotes the group S_4 as a subgroup of S_6 that is not contained in A_6.

Using the familiar group names as previously described, we provide in Table 1 the eight possible Galois groups over $\mathbb{Q}$ for a general irreducible even sextic polynomial [1, Table 2]. For the convenience of the reader, we include the "T"-notation, 6Tn, [7] for these groups in Table 1, since Maple also gives the T-notation when computing the Galois group.

Familiar Name	C_6	S_3	$C_2 \times S_3$	A_4	$C_2 \times A_4$	S_4^+	S_4^-	$C_2 \times S_4$
T-notation	6T1	6T2	6T3	6T4	6T6	6T7	6T8	6T11

Tab. 1: Possible Galois groups for even sextic polynomials

Our main theorem is:

Theorem 1.1. *Let $A, B, k \in \mathbb{Z}$, with $AB \neq 0$ and $k \in \{1, 2\}$. Let*

$$f(x) = x^6 + Ax^{2k} + B \quad \text{and} \quad \delta = 4A^3 + 27B^{3-k}.$$

Suppose that $f(x)$ is irreducible over $\mathbb{Q}$. Then $f(x)$ is monogenic with $\operatorname{Gal}(f) \simeq$

(1) C_6 never occurs;

(2) S_3 never occurs;

(3) $C_2 \times S_3$ if and only if $k = 2$ with $(A, B) \in \{(-2, 2),\ (2, -2)\}$;

(4) A_4 if and only if $(k, A, B) \in \{(1, -3, -1),\ (2, -3, -1)\}$;

(5) $C_2 \times A_4$ if and only if

$$2 \nmid AB, \quad B \text{ is squarefree}, \quad B \neq -1, \quad \operatorname{rad}(|\delta|) \mid A, \quad \text{such that}$$

(a) $k = 1$ with $f(x) \in \mathcal{F}_1$, where

$$\mathcal{F}_1 = \{f(x) : 3 \nmid A \text{ or } (A \bmod 9,\ B \bmod 9) \in \{(6, 1), (6, 4), (6, 5), (6, 8)\}\},$$

(b) $k = 2$ *with* $(A, B) \in \{(-3, 1), (-3, 3), (3, -3)\}$*;*

(6) S_4^+ *if and only if* $f(x) \in \mathcal{F}_2$*, where*

$$\mathcal{F}_2 = \{f(x) : B = -1,\ A \neq (-1)^k 3,\ 4 \nmid A,\ 9 \nmid A,\ \delta/3^{\nu_3(\delta)} \text{ is squarefree}\};$$

(7) S_4^- *if and only if*

(a) $k = 1$ *with* $(A, B) = (-9, -6)$*,*

(b) $k = 2$ *with* $f(x) \in \mathcal{F}_3$*, where*

$$\mathcal{F}_3 = \{f(x) : 3 \mid A,\ 4 \nmid A,\ B \neq -1,\ B = 3 - 4(A/3)^3 \text{ is squarefree}\};$$

(8) $C_2 \times S_4$ *if and only if*

$$B \text{ and } \delta/\prod_{p \mid 2AB} p^{\nu_p(\delta)} \quad \text{are squarefree,} \quad B \neq -1,$$
$$-B^{k-1}\delta \quad \text{is not a square,}$$
$$(A \bmod 4,\ B \bmod 4) = (3, 2) \quad \text{if } 2 \nmid A \text{ and } 2 \mid B,$$
$$(A \bmod 4,\ B \bmod 4) \in \{(0, 1),\ (2, 3)\} \quad \text{if } 2 \mid A \text{ and } 2 \nmid B,$$

and additionally, when

(a) $k = 1$

$$(A \bmod 9,\ B \bmod 9) \in \mathcal{R}_1 \quad \text{if } 3 \mid A \text{ and } 3 \nmid B;$$

(b) $k = 2$

$$(A, B) \notin \{(-2, 2), (2, -2)\}, \quad f(x) \notin \mathcal{F}_3 \quad \text{and}$$
$$(A \bmod 9,\ B \bmod 9) \in \mathcal{R}_2 \quad \text{if } 3 \mid A \text{ and } 3 \nmid B,$$

where
$$\mathcal{R}_k = \{(0, 2),\ (0, 4),\ (0, 5),\ (0, 7),\ (3, 1),\ (3, 2),\ (3, 8),\ (3, 10 - 3k),\ (6, 1),\ (6, 5),\ (6, 8),\ (6, 3k + 1)\};$$

Observe that the conditions given in Theorem 2.8 for a monogenic trinomial $f(x)$ with $\mathrm{Gal}(f) \simeq C_2 \times S_4$ do not include a parametric description of all such monogenic trinomials for either value of $k \in \{1, 2\}$. However, in the proof of the following corollary, we construct infinite parametric families from these conditions, such that the members of these families generate distinct sextic fields. Furthermore, we show that each of the parametric families $\mathcal{F}_1$, $\mathcal{F}_2$ and $\mathcal{F}_3$ given in Theorem 2.8, for the respective Galois groups $C_2 \times A_4$, S_4^+ and S_4^-, contains an infinite subfamily such that all elements of the subfamily generate distinct sextic fields. More formally, we state the following corollary of Theorem 1.1.

Corollary 1.2.

(1) *The families $\mathcal{F}_1$, $\mathcal{F}_2$ and $\mathcal{F}_3$ of monogenic trinomials given in Theorem 1.1 are infinite, and each of these families contains at least one infinite single-parameter subfamily such that all elements of the subfamily generate distinct sextic fields.*

(2) *For each value of* $k \in \{1,2\}$*, there exists an infinite single-parameter family of trinomials* $f(x)$ *such that* $f(x)$ *is monogenic with* $\mathrm{Gal}(f) \simeq C_2 \times S_4$*, and no two elements in a family generate the same sextic field.*

2. Preliminaries

Throughout this article, with $k \in \{1,2\}$ and $AB \neq 0$, we let

$$\begin{aligned} f(x) &= x^6 + Ax^{2k} + B, \\ g(x) &= x^3 + Ax^k + B, \\ h(x) &= x^6 + (-1)^k AB^{k-1}x^{6-2k} - B^2, \\ \widehat{h}(x) &= x^3 + (-1)^k AB^{k-1}x^{3-k} - B^2 \text{ and} \\ \delta &= 4A^3 + 27B^{3-k}. \end{aligned} \tag{2.1}$$

Note, from (2.1), that $f(x) = g(x^2)$ and $h(x) = \widehat{h}(x^2)$.

The next two lemmas provide some nontrivial information that exists among $f(x)$, $\widehat{h}(x)$ and $h(x)$ concerning their irreducibility.

Lemma 2.1. *If* $f(x)$ *is irreducible over* $\mathbb{Q}$*, then* $\widehat{h}(x)$ *is irreducible over* $\mathbb{Q}$*.*

Proof. By way of contradiction, assume that $\widehat{h}(x)$ is reducible. Then $\widehat{h}(r) = 0$ for some nonzero integer r. If $k = 1$, then $r^2(r - A) = B^2$, which implies that $r - A = s^2$ for some nonzero integer s. Thus, $B = \pm rs$, and

$$f(x) = x^6 + (r - s^2)x^2 \pm rs = (x^2 \pm s)(x^4 \mp sx^2 + r),$$

which contradicts the fact that $f(x)$ is irreducible. If $k = 2$, then

$$r(r^2 + AB) = B^2. \tag{2.2}$$

Let $z = \gcd(r, B)$. Then we can write $r = z\ell$ and $B = zs$ for some integers ℓ and s with $\gcd(\ell, s) = 1$. Thus, it follows from (2.2) that

$$\ell(z\ell^2 + As) = s^2,$$

which implies that $\ell \mid s^2$. Hence, $\ell = \pm 1$ since ℓ and s are coprime. Therefore, $r \mid B$ and $B = \pm rs$. Then, from (2.2), we see that $A = (s^2 - r)/(\pm s)$, which implies that $s \mid r$. Consequently,

$$f(x) = x^6 \pm (s - r/s)x^4 \pm rs = (x^2 \pm s)(x^4 \mp (r/s)x^2 + r),$$

which again contradicts the fact that $f(x)$ is irreducible. Hence, we have established that $\widehat{h}(x)$ is irreducible in either case of $k \in \{1,2\}$. □

The next lemma follows from [13, Theorem 3.3 and Corollary 3.4].

Lemma 2.2. *Suppose that* $\widehat{h}(x)$ *is irreducible over* $\mathbb{Q}$*. If* $h(x)$ *is reducible over* $\mathbb{Q}$*, then*

$$M(x) := x^4 + 2(k-2)Ax^2 - 8Bx + A^{3-k}(-4B)^{k-1} \tag{2.3}$$

has a unique integer zero μ, and $h(x)$ factors into irreducibles over $\mathbb{Z}$ as

$$\left(x^3+\mu x^2+\left(\frac{\mu^2+(k-2)A}{2}\right)x+B\right)\left(x^3-\mu x^2+\left(\frac{\mu^2+(k-2)A}{2}\right)x-B\right).$$

The following theorem, due to Swan [25], gives the formula for the discriminant of an arbitrary trinomial.

Theorem 2.3. *Let $\mathfrak{F}(x)=x^n+Ax^m+B\in\mathbb{Z}[x]$, where $0<m<n$, and let $d=\gcd(n,m)$. Then*

$$\Delta(\mathfrak{F})=(-1)^{n(n-1)/2}B^{m-1}\left(n^{n/d}B^{(n-m)/d}-(-1)^{n/d}(n-m)^{(n-m)/d}m^{m/d}A^{n/d}\right)^d.$$

Applying Theorem 2.3 to $f(x)$ and $g(x)$ yields

Corollary 2.4.

$$\Delta(f)=-64B^{2k-1}\delta^2 \quad \textit{and} \quad \Delta(g)=-B^{k-1}\delta.$$

The next theorem is an adaptation of the work in [1] to the particular trinomials $f(x)$ in (2.1), and gives precise criteria to determine $\mathrm{Gal}(f)$.

Theorem 2.5. *Suppose that $f(x)$ is irreducible over $\mathbb{Q}$. Then, with $\Delta(g)$ as given in Corollary 2.4, we have*

$$\mathrm{Gal}(f)\simeq\begin{cases} C_6 & \textit{if and only if } -B \textit{ is not a square, } \Delta(g) \textit{ is a square} \\ & \textit{and } h(x) \textit{ is reducible;} \\ S_3 & \textit{if and only if neither } -B \textit{ nor } \Delta(g) \textit{ is a square,} \\ & -B\Delta(g) \textit{ is a square and } h(x) \textit{ is reducible;} \\ C_2\times S_3 & \textit{if and only if neither } -B \textit{ nor } \Delta(g) \textit{ nor } -B\Delta(g) \\ & \textit{is a square and } h(x) \textit{ is reducible;} \\ A_4 & \textit{if and only if } -B \textit{ and } \Delta(g) \textit{ are squares} \\ & \textit{and } h(x) \textit{ is irreducible;} \\ C_2\times A_4 & \textit{if and only if } -B \textit{ is not a square, } \Delta(g) \textit{ is a square} \\ & \textit{and } h(x) \textit{ is irreducible;} \\ S_4^+ & \textit{if and only if } -B \textit{ is a square, } \Delta(g) \textit{ is not a square} \\ & \textit{and } h(x) \textit{ is irreducible;} \\ S_4^- & \textit{if and only if neither } -B \textit{ nor } \Delta(g) \textit{ is a square,} \\ & -B\Delta(g) \textit{ is a square and } h(x) \textit{ is irreducible;} \\ C_2\times S_4 & \textit{if and only if neither } -B \textit{ nor } \Delta(g) \textit{ nor } -B\Delta(g) \\ & \textit{is a square and } h(x) \textit{ is irreducible.} \end{cases}$$

We now present some basic information concerning the monogenicity of a polynomial $\mathfrak{F}(x)$. Suppose that $\mathfrak{F}(x)\in\mathbb{Z}[x]$ is monic and irreducible over $\mathbb{Q}$. Let

$K = \mathbb{Q}(\theta)$ with ring of integers $\mathbb{Z}_K$, where $\mathfrak{F}(\theta) = 0$. Then, we have [8]

$$\Delta(\mathfrak{F}) = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 \, \Delta(K), \tag{2.4}$$

where $\Delta(\mathfrak{F})$ and $\Delta(K)$ denote the discriminants over $\mathbb{Q}$, respectively, of $\mathfrak{F}(x)$ and the number field K. Thus, from (2.4),

(2.5) $\mathfrak{F}(x)$ is monogenic if and only if $\Delta(\mathfrak{F}) = \Delta(K)$, or equivalently, $\mathbb{Z}_K = \mathbb{Z}[\theta]$.

We then have from (2.5) a sufficient condition for when two monogenic polynomials of the same degree are distinct.

Corollary 2.6. *Let $\mathfrak{F}_1(x) \neq \mathfrak{F}_2(x)$ be two monogenic polynomials such that $\deg(\mathfrak{F}_1) = \deg(\mathfrak{F}_2)$. Let $K_i = \mathbb{Q}(\theta_i)$, where $\mathfrak{F}_i(\theta_i) = 0$. If $\Delta(\mathfrak{F}_1) \neq \Delta(\mathfrak{F}_2)$, then $K_1 \neq K_2$ so that $\mathfrak{F}_1(x)$ and $\mathfrak{F}_2(x)$ are distinct.*

The next theorem, due to Jakhar, Khanduja and Sangwan [15], gives necessary and sufficient conditions for an arbitrary irreducible trinomial to be monogenic.

Theorem 2.7. *Let $n, m \in \mathbb{Z}$ with $n > m \geq 1$. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with $\theta \in \mathbb{Z}_K$, the ring of integers of K, having minimal polynomial $\mathfrak{F}(x) = x^n + Ax^m + B$ over $\mathbb{Q}$, where $\gcd(m, n) = d_0$, $m = m_1 d_0$ and $n = n_1 d_0$. A prime factor p of $\Delta(\mathfrak{F})$ does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if p satisfies one of the following conditions:*

(i) *when $p \mid A$ and $p \mid B$, then $p^2 \nmid B$;*

(ii) *when $p \mid A$ and $p \nmid B$, then*

$$\text{either} \quad p \mid a_2 \text{ and } p \nmid b_1 \quad \text{or} \quad p \nmid a_2 \left((-B)^{m_1} a_2^{n_1} + (-b_1)^{n_1}\right),$$

where $a_2 = A/p$ and $b_1 = \frac{B+(-B)^{p^j}}{p}$, such that $p^j \mid\mid n$ with $j \geq 1$;

(iii) *when $p \nmid A$ and $p \mid B$, then*

$$\text{either} \quad p \mid a_1 \text{ and } p \nmid b_2 \quad \text{or} \quad p \nmid a_1 b_2^{m-1} \left((-A)^{m_1} a_1^{n_1 - m_1} - (-b_2)^{n_1 - m_1}\right),$$

where $a_1 = \frac{A+(-A)^{p^l}}{p}$, such that $p^l \mid\mid (n - m)$ with $l \geq 0$, and $b_2 = B/p$;

(iv) *when $p \nmid AB$ and $p \mid m$ with $n = s'p^r$, $m = sp^r$, $p \nmid \gcd(s', s)$, then the polynomials*

$$G(x) := x^{s'} + Ax^s + B \quad \text{and} \quad H(x) := \frac{Ax^{sp^r} + B + (-Ax^s - B)^{p^r}}{p}$$

are coprime modulo p;

(v) *when $p \nmid ABm$, then*

$$p^2 \nmid \left(B^{n_1 - m_1} n_1^{n_1} - (-1)^{m_1} A^{n_1} m_1^{m_1} (m_1 - n_1)^{n_1 - m_1}\right).$$

The next theorem is an application of Theorem 2.7 to the trinomials $f(x)$ in (2.1).

Theorem 2.8. *Let $k \in \{1, 2\}$, and suppose that $f(x) = x^6 + Ax^{2k} + B$ is irreducible over $\mathbb{Q}$. Then*

$$\Delta(f) = -64B^{2k-1}\delta^2$$

by Corollary 2.4. Let $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$, and let $\mathbb{Z}_K$ denote the ring of integers of K. A prime factor p of $\Delta(f)$ does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if p satisfies one of the following conditions:

(1) when $p \mid A$ and $p \mid B$, then $p^2 \nmid B$;

(2) when $p \mid A$ and $p \nmid B$, then $p \in \{2, 3\}$ such that

$$(A \bmod 4,\ B \bmod 4) \in \{(0, 1),\ (2, 3)\} \quad \textit{if } p = 2, \textit{ and}$$
$$(A \bmod 9,\ B \bmod 9) \in \mathcal{R}_k \quad \textit{if } p = 3,$$

where $$\mathcal{R}_k = \{(0, 2),\ (0, 4),\ (0, 5),\ (0, 7),\ (3, 1),\ (3, 2),\ (3, 8),\ (3, 10 - 3k),\ (6, 1),\ (6, 5),\ (6, 8),\ (6, 3k + 1)\};$$

(3) when $p \nmid A$ and $p \mid B$, then $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if $p \neq 2$ and

$$(A \bmod 4,\ B \bmod 4) = (3,\ 2) \quad \textit{if } p = 2;$$

(4) when $2 \nmid AB$, then $2 \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$;

(5) when $p \nmid 2AB$, then $p^2 \nmid \delta$.

Proof. Let p be a prime divisor of $\Delta(f)$. Note that conditions (1) and (5) remain the same as conditions (i) and (v) of Theorem 2.7.

For condition (2), we suppose that $p \mid A$ and $p \nmid B$. Then, from condition (ii) of Theorem 2.7, we have that $p^j \mid\mid 6$ with $j \geq 1$. Hence, $p \in \{2, 3\}$ with $j = 1$ for each of these primes, $a_2 = A/p$ and

$$b_1 = \begin{cases} \frac{B+B^2}{2} & \text{if } p = 2 \\ \frac{B-B^3}{3} & \text{if } p = 3. \end{cases}$$

Observe that, in Theorem 2.7, we have for each value of $k \in \{1, 2\}$ that $n_1 = 3$ and $m_1 = k$. Then, it is easy to calculate, in each of the two cases $p \in \{2, 3\}$ with $k \in \{1, 2\}$, the congruence classes of A and B modulo p^2 for which

$$\text{either} \quad p \mid a_2 \text{ and } p \nmid b_1, \quad \text{or} \quad p \nmid a_2\left((-B)^k a_2^3 - b_1^3\right).$$

For condition (3), suppose that $p \nmid A$ and $p \mid B$. Then, from condition (iii) of Theorem 2.7, we have that $p^l \mid\mid (6 - 2k)$, which implies that either $\ell = 0$ if $p \geq 3$, in which case the first statement under condition (iii) of Theorem 2.7 must be true for monogenicity, or $p = 2$ and $p^l = 2^{3-k}$. In this latter case, we have

$$a_1 = \frac{A^{2^{3-k}} + A}{2} \equiv \begin{cases} 1 \pmod 2 & \text{if } A \equiv 1 \pmod 4, \\ 0 \pmod 2 & \text{if } A \equiv 3 \pmod 4. \end{cases}$$

Since $m = 2k > 1$, we observe that $4 \nmid B$ so that $2 \nmid b_2$; otherwise, condition (iii) of Theorem 2.7 fails. It follows that we must have $(A \bmod 4,\ B \bmod 4) = (3, 2)$.

Finally, for condition (4), suppose that $p \nmid AB$ and $p \mid m$. Thus, $p = 2$ since $p \mid 2k$ with $k \in \{1, 2\}$. Hence, the possibilities of $(A \bmod 4,\ B \bmod 4)$ are

$$(A \bmod 4,\ B \bmod 4) \in \{(1,1),\ (1,3),\ (3,1),\ (3,3)\} \tag{2.6}$$

since $2 \nmid AB$. From condition (iv) of Theorem 2.7, we see that

$$G(x) = x^3 + Ax^k + B \quad \text{and} \quad H(x) = \left(\frac{A^2 + A}{2}\right) x^{2k} + ABx^k + \left(\frac{B^2 + B}{2}\right).$$

Straightforward calculations reveal that $G(x)$ and $H(x)$ are coprime in $\mathbb{F}_2[x]$ for all possibilities of $(A \bmod 4,\ B \bmod 4)$ in (2.6). Consequently, the prime $p = 2$ satisfies condition (4) when $2 \nmid AB$. That is, $2 \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ when $2 \nmid AB$. $\square$

The following corollary, which follows immediately from conditions (1) and (3) of Theorem 2.8, will be useful in the proof of Theorem 1.1.

Corollary 2.9. *If $f(x)$ is monogenic, then B is squarefree.*

3. The Proof of Theorem 1.1

We first prove a lemma.

Lemma 3.1. *Suppose that $f(x)$ is irreducible over $\mathbb{Q}$. If $h(x)$ is reducible over $\mathbb{Q}$, then $\Delta(g) < 0$.*

Proof. Since $f(x)$ is irreducible, then $\widehat{h}(x)$ is irreducible from Lemma 2.1. Then, since $h(x)$ is reducible, it follows from Lemma 2.2 that $M(\mu) = 0$ for some $\mu \in \mathbb{Z}$. Calculating $\Delta(M)$, using [10, Theorem 3.1] when $k = 1$, and Theorem 2.3 when $k = 2$, reveals that

$$\Delta(M) = -2^{12}B^{k+1}(4A^3 + 27B^{3-k}) = 2^{12}B^2\Delta(g). \tag{3.1}$$

Note that $g(x)$ is irreducible, since $f(x)$ is irreducible, so that $\Delta(g) \neq 0$. Assume, by way of contradiction, that $\Delta(g) > 0$. Thus, $\Delta(M) > 0$, from (3.1). Consequently, $M(x)$ has four distinct real zeros since $\mu \in \mathbb{R}$. Note that since $A \neq 0$, it follows from (2.3) that $\mu \neq 0$ for either value of k, and $\mu \neq -A/2$ if $k = 2$. Observing from (2.3) that

$$\mu^3 - 2A\mu - 8B = -A^2/\mu \quad \text{if } k = 1$$

and

$$\mu^3 - 8B = \mu^3 A/(A + 2\mu) \quad \text{if } k = 2,$$

straightforward calculations show that $M(x) = (x - \mu)Q(x)$, where

$$Q(x) = \begin{cases} x^3 + \mu x^2 + (\mu^2 - 2A)x - A^2/\mu & \text{if } k = 1 \\ x^3 + \mu x^2 + \mu^2 x + \mu^3 A/(A + 2\mu) & \text{if } k = 2. \end{cases}$$

Calculating $\Delta(Q)$ using [10, Theorem 3.1], or Theorem 2.3 if $\mu^2 = 2A$ and $k = 1$, yields

$$\Delta(Q) = \begin{cases} -(3\mu^4 - 14A\mu^2 + 27A^2)(-\mu^2 + A)^2/\mu^2 & \text{if } k = 1 \\ -4\mu^6(3\mu^2 - 4A\mu + 4A^2)/(A + 2\mu)^2 & \text{if } k = 2. \end{cases} \tag{3.2}$$

Since $Q(x)$ has three distinct real zeros, then $\Delta(Q) > 0$, which implies from (3.2) that

$$-(3\mu^4 - 14A\mu^2 + 27A^2) > 0 \text{ if } k = 1, \text{ and } -(3\mu^2 - 4A\mu + 4A^2) > 0 \text{ if } k = 2.$$

However,

$$-(3\mu^4 - 14A\mu^2 + 27A^2) = -(3(\mu^2 - 7A/3)^2 + 32A^2/3) < 0$$

and

$$-(3\mu^2 - 4A\mu + 4A^2) = -(3(\mu - 2A/3)^2 + 8A^2/3) < 0.$$

These contradictions complete the proof that $\Delta(g) < 0$. □

The following corollary of Lemma 3.1 indicates that the list of possible Galois groups for $f(x)$ is slightly smaller than the list given in Table 1 for an arbitrary even sextic polynomial.

Corollary 3.2. *Suppose that $f(x)$ is irreducible over $\mathbb{Q}$. Then* $\mathrm{Gal}(f) \not\simeq C_6$.

Proof. We proceed by way of contradiction, assuming that $\mathrm{Gal}(f) \simeq C_6$. Then, from Theorem 2.5, we have that:

$$-B \text{ is not a square}, \quad \Delta(g) \text{ is a square}, \quad \text{and } h(x) \text{ is reducible.} \tag{3.3}$$

Since $h(x)$ is reducible, we have from Lemma 3.1 that $\Delta(g) < 0$, which contradicts the fact that $\Delta(g)$ is a square. □

Remark 3.3. It is easy to verify that the groups listed in Table 1, with the exception of C_6, actually do occur as Galois groups of $f(x)$.

Proof of Theorem 1.1. We address the Galois groups, one at a time, as presented in the statement of the theorem. It will sometimes be convenient to handle the cases $k = 1$ and $k = 2$ separately. Recall that

$$\begin{aligned} f(x) &= x^6 + Ax^2 + B, \\ \delta &= 4A^3 + 27B^2, \\ \Delta(f) &= -2^6 B\delta^2 \text{ and} \\ \Delta(g) &= -\delta, \end{aligned} \tag{3.4}$$

when $k = 1$, while

$$\begin{aligned} f(x) &= x^6 + Ax^4 + B, \\ \delta &= 4A^3 + 27B, \\ \Delta(f) &= -2^6 B^3\delta^2 \text{ and} \\ \Delta(g) &= -B\delta, \end{aligned} \tag{3.5}$$

when $k = 2$.

The Case $\mathbf{C_6}$. By Corollary 3.2, it follows that no monogenic trinomials $f(x)$ exist with $\mathrm{Gal}(f) \simeq C_6$.

The Case $\mathbf{S_3}$. Assume, by way of contradiction, that $f(x)$ is monogenic with $\mathrm{Gal}(f) \simeq S_3$. By Theorem 2.5, we have:

$$-B \text{ is not a square}, \quad -B\Delta(g) \text{ is a square}, \quad h(x) \text{ is reducible.} \tag{3.6}$$

We first address the case $k = 1$ in (3.4). Suppose that p is a prime divisor of B. Then $p \mid\mid B$ by Corollary 2.9, which implies that $p \mid \delta$ since $-B\Delta(g) = B\delta$ is a square. If $p \notin \{2, 3\}$, then $p^3 \mid\mid B\delta$, which contradicts the fact that $B\delta$ is a square. Hence, $p \in \{2, 3\}$. Consequently,

$$|B| \in \{1, 2, 3, 6\}, \tag{3.7}$$

since B is squarefree. Since $-B\Delta(g)$ is a square, we can write

$$y^2 = -B\Delta(g) = B(4A^3 + 27B^2),$$

for some $y \in \mathbb{Z}$, so that

$$(4By)^2 = (4AB)^3 + (16)(27)B^5. \tag{3.8}$$

It follows then from (3.8) that, for each of the eight values of B in (3.7), we need to determine the integral points (X, Y) on the elliptic curve

$$Y^2 = X^3 + 2^4 3^3 B^5,$$

such that $X = 4AB$ for some integers A and Y with $AY \neq 0$. To do this, we use Sage and we provide the results of these calculations in Table 2.

B	1	-1	2	-2	3	-3	6	-6
A	none	-3	none	-5	none	none	-3	-9

Tab. 2: Possible values for A and B

From Table 2, we get the four trinomials:

$$x^6 - 3x^2 - 1, \quad x^6 - 5x^2 - 2, \quad x^6 - 3x^2 + 6, \quad x^6 - 9x^2 - 6. \tag{3.9}$$

Observe that

$$x^6 - 5x^2 - 2 = (x^2 + 2)(x^4 - 2x^2 - 1).$$

Straightforward methods verify that the remaining three trinomials in (3.9) are irreducible over $\mathbb{Q}$. Then, a computer algebra system, such as Maple, Sage or Magma, in conjunction with Theorem 2.8, can be used to complete the proof that there exist no even monogenic trinomials $f(x)$ with $\mathrm{Gal}(f) \simeq S_3$ when $k = 1$. The results of these computations are summarized in Table 3.

$f(x)$	$x^6 - 3x^2 - 1$	$x^6 - 3x^2 + 6$	$x^6 - 9x^2 - 6$
$\mathrm{Gal}(f)$	A_4	S_3	S_4^-
Monogenic	yes	no	yes

Tab. 3: Results for trinomials when $k = 1$

Suppose next that $k = 2$ as in (3.5). Since $-B\Delta(g) = B^2\delta$ is a square, we deduce that δ must be a square. Let p be a prime divisor of δ. Then, since $f(x)$ is monogenic, it follows from condition (5) of Theorem 2.8 that $p \mid 2AB$. If $p \neq 3$, then $p^3 \mid\mid \delta$ by Corollary 2.9, which contradicts the fact that δ is a square. Hence, $p = 3$, so that $3 \mid AB$ and

$$\delta = 4A^3 + 27B = 3^{2z}, \tag{3.10}$$

for some integer $z \geq 0$.

We consider first the two cases $z \in \{0, 1\}$ in (3.10). If $z = 0$, then we see that $3 \nmid A$. Therefore, $3 \mid B$, and we get that $A^3 \equiv 61 \pmod{81}$, which is impossible since 61 is not a cube modulo 81. Suppose next that $z = 1$. If $3 \mid A$, then it follows from (3.10) that

$$3\left(4(A/3)^3 + B\right) = 1,$$

which is impossible. Thus, $3 \nmid A$ and $3 \mid B$, so that $A^3 \equiv 63 \pmod{81}$ from (3.10), which is also impossible since 63 is not a cube modulo 81.

We have shown that $z \geq 2$ in (3.10). Therefore, $2z - 3$ is a positive integer, and we can rewrite (3.10) as

$$B = 3^{2z-3} - 4(A/3)^3, \tag{3.11}$$

which implies that $A/3 \in \mathbb{Z}$. If $z \geq 3$, then we deduce from (3.11) and Corollary 2.9 that $3 \nmid (A/3)$. Thus, $3 \nmid B$ and

$$(A \bmod 9,\ B \bmod 9) \in \{(3, 5),\ (6, 4)\}.$$

Since $\{(3, 5),\ (6, 4)\} \cap \mathcal{R}_2 = \varnothing$, we conclude from condition (3) of Theorem 2.8 that $f(x)$ is not monogenic when $z \geq 3$.

Hence, we only need to examine the situation $z = 2$. Then we have

$$B = 3 - 4(A/3)^3, \tag{3.12}$$

from (3.11). Since $f(x)$ is monogenic, then $f(x)$ is irreducible over $\mathbb{Q}$, and so $\widehat{h}(x)$ is irreducible over $\mathbb{Q}$ by Lemma 2.1. Since $h(x)$ is reducible over $\mathbb{Q}$ from (3.6), we have, from Lemma 2.2, that

$$M(x) = x^4 - 8Bx - 4AB \tag{3.13}$$

is reducible over $\mathbb{Q}$. Let p be a prime divisor of B. Observe from (3.12) that $p \neq 2$. If $p \nmid A$, then, since B is squarefree, we get the contradiction that $M(x)$ in (3.13) is irreducible over $\mathbb{Q}$ because $M(x)$ is Eisenstein with respect to p. Thus, $p \mid A$, and we deduce from (3.12) that $p = 3$. Hence, we only need to address the cases $|B| \in \{1, 3\}$. From (3.12), it is easy to see that cases $B \in \{1, -3\}$ are impossible, while the case $B = 3$ yields the contradiction that $A = 0$. The only viable case is then $(A, B) = (3, -1)$. However, in this case, it is straightforward to verify that $M(x) = x^4 + 8x + 12$ is irreducible over $\mathbb{Q}$. This final contradiction completes the proof of the nonexistence of even monogenic trinomials $f(x)$ with $\mathrm{Gal}(f) \simeq S_3$.

The Case $\mathbf{C_2 \times S_3}$. Assume that $f(x)$ is monogenic with $\operatorname{Gal}(f) \simeq C_2 \times S_3$. By Theorem 2.5, we have:

(3.14) neither $-B$, nor $\Delta(g)$, nor $-B\Delta(g)$ is a square, and $h(x)$ is reducible.

Suppose first that $k = 1$. Since $h(x)$ is reducible, we have from Lemma 2.2 that

$$M(\mu) = \mu^4 - 2A\mu^2 - 8B\mu + A^2 = 0, \tag{3.15}$$

for some $\mu \in \mathbb{Z}$. Solving (3.15) for A yields

$$A = \mu^2 \pm 2\sqrt{2B\mu}, \tag{3.16}$$

which implies that $2B\mu$ is a nonzero square, since $A, B \in \mathbb{Z}$ with $AB \neq 0$. Observe from (3.15) that

$$\mu \equiv A \pmod 2. \tag{3.17}$$

We claim that $2 \mid \mu$. Suppose, by way of contradiction, that $2 \nmid \mu$. Then $2 \nmid A$ from (3.17), and $2 \mid B$ since $2B\mu$ is a nonzero square. Furthermore,

$$\mu^2 \equiv A^2 \equiv 1 \pmod 8,$$

so that $2(A-1) \equiv 0 \pmod 8$ from (3.15). Hence, $A \equiv 1 \pmod 4$, which contradicts the fact that $A \equiv 3 \pmod 4$ from condition (3) of Theorem 2.8, and the claim that $2 \mid \mu$ is established. Observe from (3.16) that if $2 \mid B$, then $(B/2) \mid \mu$ since $2B\mu$ is a nonzero square and B is squarefree. However, since $2 \mid \mu$ and $2 \nmid (B/2)$, we actually have that $2(B/2) = B$ divides μ. Clearly, if $2 \nmid B$, then $B \mid \mu$. Therefore, $B \mid \mu$, regardless of the parity of B.

Let

$$B = 2^{\varepsilon} \prod_{p_i \geq 3} p_i \qquad \text{and} \qquad 2^e \mid\mid \mu,$$

where $\varepsilon \in \{0, 1\}$, $e \geq 1$ and the p_i are the odd prime divisors of B. Thus, since $2B\mu$ is a nonzero square, we have that

$$2B\mu = 2^{e+1+\varepsilon} \prod_{p_i \geq 3} p_i^2 \left(\frac{\mu}{2^e \prod_{p_i \geq 3} p_i} \right), \tag{3.18}$$

where $2 \mid (e + 1 + \varepsilon)$ and $\mu/(2^e \prod_{p_i \geq 3} p_i) = m^2$ for some nonzero odd integer m. Hence,

$$\mu = 2^{e-\varepsilon} m^2 2^{\varepsilon} \prod_{p_i \geq 3} p_i = 2^{2r-1} m^2 B, \tag{3.19}$$

where $r = (e + 1 - \varepsilon)/2 \geq 1$. Then

$$A = 2^{r+1} mB \left(2^{3r-3} m^3 B \pm 1\right), \tag{3.20}$$

from (3.16) and (3.19). An easy calculation shows that

$$\delta = 4A^3 + 27B^2 = B^2 \left(2^{3r-1} m^3 B \pm 1\right)^2 \left(2^{6r-1} m^6 B^2 \pm 2^{3r} 5m^3 B + 27\right), \tag{3.21}$$

where the plus sign holds in (3.21) if and only if the plus sign holds in (3.20). Let $d = 2^{3r-1} m^3 B \pm 1$. Note that $|d| > 1$ since $r \geq 1$ and $mB \neq 0$. Let p be a prime divisor of d, and observe that $p \nmid 2mB$. Since $f(x)$ is monogenic and $p^2 \mid \delta$ from (3.21), it follows from condition (5) of Theorem 2.8 that $p \mid A$. Hence,

$$p \mid \left(2^{3r-3}m^3B \pm 1\right),$$

from (3.20). Consequently, p divides

$$d - \left(2^{3r-3}m^3B \pm 1\right) = 3 \cdot 2^{3r-3}m^3B,$$

so that $p = 3$. Therefore,

$$|d| = \left|2^{3r-1}m^3B \pm 1\right| = 3^z, \tag{3.22}$$

for some integer $z \geq 1$. If $z = 1$ in (3.22), we get that

$$2^{3r-1}m^3B \in \begin{cases} \{-4, 2\} & \text{when the plus sign holds in (3.22) and (3.20)} \\ \{-2, 4\} & \text{when the minus sign holds in (3.22) and (3.20).} \end{cases}$$

It follows that $r = 1$, so that $m^3B = \pm 1$. Since $-B$ is not a square from (3.14), we see that $B \neq -1$. We conclude that $(m, B) = (\pm 1, 1)$, where the plus sign (minus sign) holds if and only if the minus sign (plus sign) holds in (3.22) and (3.20). Both of these scenarios yield the contradiction that $A = 0$.

Hence, we may assume that $z \geq 2$ in (3.22). Thus,

$$B \bmod 9 = \frac{\mp 1}{2^{3r-1}m^3} \bmod 9 \in \{2, 7\},$$

which implies from (3.20), regardless of the sign, that

$$A \bmod 9 = \frac{-3}{2^{2r}m^2}. \tag{3.23}$$

Let $S = \{1, 4, 7\}$, which is the multiplicative subgroup of squares modulo 9. Since $2^{2r} \bmod 9 \in S$, $m^2 \bmod 9 \in S$ and

$$\frac{-3}{s_1} + \frac{3}{s_2} = -3\left(\frac{s_2 - s_1}{s_1 s_2}\right) \equiv 0 \pmod 9$$

for any $s_1, s_2 \in S$, it follows from (3.23) that $A \bmod 9 = 6$. Hence,

$$(A \bmod 9,\ B \bmod 9) \in \{(6, 2), (6, 7)\},$$

which yields the contradiction that $f(x)$ is not monogenic by condition (2) of Theorem 2.8 since neither $(6, 2)$ nor $(6, 7)$ is an element of $\mathcal{R}_1$. This completes the proof that there are no monogenic trinomials $f(x)$ with $\mathrm{Gal}(f) \simeq C_2 \times S_3$ in the case of $k = 1$.

Suppose next that $k = 2$. Since $h(x)$ is reducible, we have from Lemma 2.2 that

$$M(\mu) = \mu^4 - 8B\mu - 4AB = 0, \tag{3.24}$$

for some $\mu \in \mathbb{Z}$, or equivalently,

$$\mu^4 = 4B(2\mu + A). \tag{3.25}$$

Note that $\mu \neq 0$ since $AB \neq 0$. Observe from (3.25) that $B \mid \mu$ since B is squarefree. Thus, we can write $\mu = mB$, for some nonzero integer m. Then, noting that $2 \mid \mu$ from (3.25), and solving for A in (3.24), we get

$$\begin{aligned} A &= \frac{\mu(\mu^3 - 8B)}{4B} \\ &= \frac{mB(m^3B^2 - 8)}{4} \\ &= \left(\frac{mB}{2}\right)\left(\frac{m^3B^2}{2} - 4\right), \end{aligned} \tag{3.26}$$

where each factor in (3.26) is an integer. Hence,

$$\begin{aligned} \delta &= 4A^3 + 27B \\ &= \frac{B(m^6B^4 - 20m^3B^2 + 108)(m^3B^2 - 2)^2}{16} \\ &= B\left(\frac{m^6B^4}{4} - 5m^3B^2 + 27\right)\left(\frac{m^3B^2}{2} - 1\right)^2, \end{aligned} \tag{3.27}$$

where each factor in (3.27) is an integer.

Let $d = m^3B^2/2 - 1$ from (3.27). Since $f(x)$ is irreducible, we know that $d \neq 0$. We claim that $|d| = 1$. Suppose, by way of contradiction, that $|d| > 1$, and let p be a prime divisor of d. Observe that $p \nmid mB$, which also implies that $p \neq 2$ since $2 \mid mB$. Since $f(x)$ is monogenic and $p^2 \mid \delta$ from (3.27), it follows from condition (5) of Theorem 2.8 that $p \mid A$. Hence,

$$p \mid (m^3B^2/2 - 4),$$

from (3.26). Consequently, p divides

$$d - \left(\frac{m^3B^2}{2} - 4\right) = 3,$$

so that $p = 3$. Therefore,

$$|d| = \left|m^3B^2/2 - 1\right| = 3^z, \tag{3.28}$$

for some integer $z \geq 1$. If $z = 1$ in (3.28), then it is easy to see that

$$(m, B) \in \{(2, \pm 1), (-1, \pm 2)\}.$$

The solutions $(m, B) = (2, \pm 1)$ yield the contradiction that $A = 0$. The solutions $(m, B) = (-1, \pm 2)$ produce the pairs $(A, B) \in \{(-6, -2), (6, 2)\}$, so that

$$(A \bmod 9,\ B \bmod 9) \in \{(3, 7), (6, 2)\}.$$

However, neither of these pairs is contained in $\mathcal{R}_2$ from condition (2) of Theorem 2.8, which contradicts the fact that $f(x)$ is monogenic.

Hence, we may assume that $z \geq 2$ in (3.28). Then, $m^3B^2 \equiv 2 \pmod 9$, which implies that

$$(m \bmod 9,\ B \bmod 9) \in \{(2, 4), (2, 5), (5, 4), (5, 5), (8, 4), (8, 5)\}. \tag{3.29}$$

It follows from (3.29) and (3.26) that

$$(A \bmod 9,\ B \bmod 9) \in \{(3,5),(6,4)\},$$

and neither of these pairs is an element of $\mathcal{R}_2$ from condition (2) of Theorem 2.8, which again contradicts the fact that $f(x)$ is monogenic. Thus, we have established the claim that $|d| = 1$, so that $z = 0$ in (3.28).

The only solutions to $|d| = 1$ are easily found to be $(m, B) \in \{(1, \pm 2)\}$, and these solutions lead to the pairs $(A, B) \in \{(2,-2),(-2,2)\}$. Using Theorem 2.5 and Theorem 2.8 (or a computer algebra system), it is straightforward to verify that $f(x)$ is monogenic with $\mathrm{Gal}(f) \simeq C_2 \times S_3$, for each of these pairs (A, B), which completes the proof of this case.

The Case $\mathbf{A_4}$. Assume that $f(x)$ is monogenic with $\mathrm{Gal}(f) \simeq A_4$. By Theorem 2.5, we have:

$$-B \quad \text{and} \quad \Delta(g) \quad \text{are squares,} \quad \text{and} \quad h(x) \quad \text{is irreducible.}$$

Then, by Corollary 2.9, it follows that $B = -1$. Thus, since

$$\Delta(g) = -B^{k-1}\left(4A^3 + 27B^{3-k}\right) = (-1)^k\left(4A^3 + 27(-1)^{3-k}\right) = (-1)^k 4A^3 - 27$$

is a square, we need to find the integral points on the elliptic curve

$$E: \quad Y^2 = X^3 - 2^4 3^3,$$

where $X = (-1)^k 4A$. Using Sage, we get $X = 12$, which yields $A = -3$ when $k = 1$, and $A = 3$ when $k = 2$. It is easy to confirm that

$$(k, A, B) \in \{(1,-3,-1),(2,3,-1)\}$$

produce monogenic even sextic trinomials $f(x)$ with $\mathrm{Gal}(f) \simeq A_4$.

The Case $\mathbf{C_2} \times \mathbf{A_4}$. Suppose first that $f(x)$ is monogenic with $\mathrm{Gal}(f) \simeq C_2 \times A_4$. Then

$$-B \text{ is not a square,} \quad \Delta(g) \text{ is a square,} \quad \text{and} \quad h(x) \text{ is irreducible,} \tag{3.30}$$

by Theorem 2.5. Regardless of the value of k, we need to show that

$$2 \nmid AB, \quad B \neq -1 \text{ is squarefree} \quad \text{and} \quad \mathrm{rad}(|\delta|) \mid A. \tag{3.31}$$

To show that $2 \nmid AB$, we proceed by way of contradiction. Suppose first that $2 \mid A$. Since B is squarefree, we have that

$$B \bmod 32 \notin \{0,4,8,12,16,20,24,28\}.$$

Consequently,

$$\Delta(g) \bmod 32 \in \{5,13,20,21,29\},$$

regardless of the value of k, which contradicts the fact that $\Delta(g)$ is a square, since the squares modulo 32 are $\{0,1,4,9,16,17,25\}$. Hence, $2 \nmid A$. Suppose that $2 \mid B$. Then, since $f(x)$ is monogenic, we have from condition (3) of Theorem 2.8 that $(A \bmod 4, B \bmod 4) = (3,2)$. But then

$$\Delta(g) \equiv \begin{cases} 8 \pmod{16} & \text{if } k = 1; \\ 12 \pmod{16} & \text{if } k = 2. \end{cases}$$

which contradicts the fact that $\Delta(g)$ is a square. Therefore, $2 \nmid B$, and the claim that $2 \nmid AB$ is established.

Since $f(x)$ is monogenic, we have from Corollary 2.9 that B is squarefree. Since $-B$ is not a square, we deduce that $B \neq -1$.

We turn next to showing that $\operatorname{rad}(|\delta|) \mid A$. Since

$$\Delta(g) = -B^{k-1}\delta = -B^{k-1}(4A^3 + 27B^{3-k})$$

is a square, we deduce from condition (5) of Theorem 2.8 that $\operatorname{rad}(|\delta|) \mid 2AB$. Let p be a prime divisor of δ. Since $2 \nmid B$, it follows that $p \neq 2$. Therefore, $p \mid A$ or $p \mid B$, with $p \geq 3$. If $p \nmid A$, then $p \mid B$, which yields the contradiction that $p \nmid \delta$. Thus, $p \mid A$, which completes the proof that conditions (3.31) hold, regardless of the value of k.

Moving forward, we split our analysis into the two cases $k \in \{1, 2\}$, as described in (3.4) and (3.5). Consider first the case $k = 1$. Suppose that $3 \mid \Delta(f)$. If $3 \nmid A$, then $3 \mid B$, and we see from condition (3) of Theorem 2.8 that $3 \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Suppose then that $3 \mid A$. We claim that $3 \nmid B$. Assume, to the contrary, that $3 \mid B$, and let

$$Z := 4(A/3)^3 + B^2 \in \mathbb{Z}.$$

Then, since $\Delta(g) = -3^3 Z$ is a square, we have that $3 \mid Z$, which implies that $3 \mid (A/3)$. Hence, $3^2 \mid\mid Z$ since $3 \mid\mid B$, so that $3^5 \mid\mid \Delta(g)$, which contradicts the fact that $\Delta(g)$ is a square. Thus, $3 \nmid B$, and it is easy to verify that

$$(A \bmod 9,\ B \bmod 9) \in \{(6,1), (6,4), (6,5), (6,8)\},$$

from condition (2) of Theorem 2.8.

Next, suppose that p is a prime divisor of $\Delta(f)$ with $p \geq 5$. If $p \mid \delta$, then $p \mid A$ since $\operatorname{rad}(|\delta|) \mid A$, which implies that $p \mid B$. Since B is squarefree, we see that condition (1) of Theorem 2.8 is satisfied with no further restrictions on A and B. If $p \mid B$ and $p \nmid \delta$, then $p \nmid A$ so that $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ from condition (3) of Theorem 2.8, which concludes our analysis of the case $k = 1$.

Consider now the case $k = 2$. Since $\Delta(g) = -B(4A^3 + 27B)$ is a square, $2 \nmid B$ and B is squarefree, it follows that $B \mid \delta$. Thus, $B \mid A$ and

$$-\delta/B = -\left(4A^2(A/B) + 27\right) \tag{3.32}$$

is a square, since $\Delta(g) = -B\delta = B^2(-\delta/B)$ is a square. Let p be a prime divisor of δ/B. Then $p \mid A$, since $\operatorname{rad}(|\delta|) \mid A$ from (3.31). Thus, $p = 3$ from (3.32) and

$$-\delta/B = -\left(4A^2(A/B) + 27\right) = 3^{2n},$$

for some integer $n \geq 0$, or equivalently,

$$A^2(A/B) = \frac{3^{2n} + 3^3}{-4}. \tag{3.33}$$

For values of $n \in \{0, 1, 2\}$, it is then straightforward to determine all solutions of equation (3.33), which are given in Table 4.

For $n \geq 3$, we rewrite equation (3.33) as

$$A^2(A/B) = 3^3\left(\frac{3^{2n-3} + 1}{-4}\right), \tag{3.34}$$

n	0	1	2
Solutions	none	$(A,B)\in\{(-3,3),(3,-3)\}$	$(A,B)=(-3,1)$.

Tab. 4: Solutions to Equation (3.33) for $n\in\{0,1,2\}$

from which we deduce that $3 \mid\mid A$ and $3\nmid B$. Consequently, $3B\mid A$ and, rewriting equation (3.34), we get

$$(2B)^2\left(\frac{-A}{3B}\right)^3=3^{2n-3}+1\equiv 1 \pmod 9, \tag{3.35}$$

since $n\ge 3$. Since $f(x)$ is monogenic, it follows from condition (2) of Theorem 2.8 that

$$\begin{aligned}(A \bmod 9,\ B \bmod 9)\in\{&(3,1),(3,2),(3,8),(3,4),\\ &(6,1),(6,5),(6,8),(6,7)\}.\end{aligned} \tag{3.36}$$

However, a simple computation reveals that

$$(2B)^2\left(\frac{-A}{3B}\right)^3 \bmod 9\in\{4,5,7,8\},$$

for each of the pairs $(A \bmod 9,\ B \bmod 9)$ in (3.36), contradicting (3.35). This contradiction shows that no monogenic trinomials $f(x)$ with $\mathrm{Gal}(f)\simeq C_2\times A_4$ exist when $k=2$ and $n\ge 3$, which completes the proof in this direction.

Conversely, assume that conditions (3.31) hold. When $k=2$, the fact that $f(x)$, where $(A,B)\in\{(-3,1),(-3,3),(3,-3)\}$, is monogenic with $\mathrm{Gal}(f)\simeq C_2\times A_4$ can be confirmed easily from conditions (3.31) and Theorem 2.8, or simply using a computer algebra system on the three trinomials, and we omit the details.

So, suppose that $k=1$ and let $f(x)\in\mathcal{F}_1$. We show first that $\mathrm{Gal}(f)\simeq C_2\times A_4$ by verifying that conditions (3.30) hold. Observe that $-B$ cannot be a square, since B is squarefree with $B\ne -1$. Thus, the first condition of (3.30) is satisfied for $f(x)$.

We show next that the second condition in (3.30) holds; that is, that $\Delta(g)$ is a square. If $3\mid A$, then

$$(A \bmod 9,\ B \bmod 9)\in\{(6,1),(6,4),(6,5),(6,8)\}.$$

Hence, in this case we have

$$\Delta(g)/(-3^3)=\delta/3^3=4(A/3)^3+B^2\equiv\begin{cases}6 & \text{if } B \bmod 9\in\{1,8\}\\ 3 & \text{if } B \bmod 9\in\{4,5\},\end{cases}$$

so that $3^4 \mid\mid \Delta(g)$. Observe that if $3\nmid A$, then $3\nmid\Delta(g)$. Suppose next, regardless of whether $3\mid A$, that $p\ge 5$ is a prime divisor of $\Delta(g)=-\delta$. Since $\mathrm{rad}(|\delta|)\mid A$, it follows that $p\mid A$ and $p\mid B$. Then $p^2 \mid\mid B^2$ since B is squarefree, and therefore,

$$\frac{\delta}{p^2}=\frac{4A^3+27B^2}{p^2}=4A(A/p)^2+27(B/p)^2\equiv 27(B/p)^2\not\equiv 0 \pmod p.$$

Thus, $p^2 \mid\mid \Delta(g)$. Consequently,

$$|\Delta(g)| = |\delta| = \left|4A^3 + 27B^2\right| = \begin{cases} 3^4 \prod_i p_i^2 & \text{if } 3 \mid A, \\ \prod_i p_i^2 & \text{if } 3 \nmid A, \end{cases} \tag{3.37}$$

where the p_i are the distinct prime divisors of δ with $p_i \geq 5$. Since $2 \nmid B$, then we see that $\delta \equiv 3 \pmod 4$ so that δ cannot be a square, and we deduce from (3.37) that $|\delta| = -\delta$. Hence, $\Delta(g)$ is a square, which confirms that the second condition of (3.30) is satisfied for $f(x) \in \mathcal{F}_1$.

To show that $h(x) = x^6 - Ax^2 - B^2$ is irreducible, which is the third condition of (3.30), we proceed by way of contradiction and assume that $h(x)$ is reducible. Then, with $M(x)$ as defined in (2.3), we have that

$$M(\mu) = \mu^4 - 2A\mu^2 - 8B\mu + A^2 = 0 \tag{3.38}$$

for some $\mu \in \mathbb{Z}$, by Lemma 2.2. Observe from (3.38) that $2 \nmid \mu$ since $2 \nmid A$ from (3.31). Solving (3.38) for A, we get

$$A = \mu^2 \pm 2\sqrt{2B\mu} \in \mathbb{Z}.$$

Thus, $2B\mu$ is a nonzero square, which yields the contradiction that $2 \mid B\mu$. Hence, $h(x)$ is irreducible and $\mathrm{Gal}(f) \simeq C_2 \times A_4$. The fact that $f(x)$ is monogenic follows easily from conditions (3.31) and Theorem 2.8, and we omit the details.

The Case $\mathbf{S_4^+}$. Assume that $f(x)$ is monogenic with $\mathrm{Gal}(f) \simeq S_4^+$. By Theorem 2.5, we have:

$$-B \text{ is a square}, \quad \Delta(g) \text{ is not a square}, \quad \text{and} \quad h(x) \text{ is irreducible.} \tag{3.39}$$

Since $-B$ is a square and B is squarefree by Corollary 2.9, it follows that $B = -1$. If $A = (-1)^k 3$, then we see from Case A_4 that $\mathrm{Gal}(f) \simeq A_4$. Hence, $A \neq (-1)^k 3$. If $4 \mid A$, then $(A \bmod 4,\ B \bmod 4) = (0, 3)$, which contradicts condition (2) of Theorem 2.8. Similarly, if $9 \mid A$, then $(A \bmod 9,\ B \bmod 9) = (0, 8) \notin \mathcal{R}_k$, which also contradicts condition (2) of Theorem 2.8. Hence, $4 \nmid A$ and $9 \nmid A$. The fact that $\delta/3^{\nu_3(\delta)}$ is squarefree follows from condition (5) of Theorem 2.8. We conclude that $f(x) \in \mathcal{F}_2$, which proves the first direction.

Conversely, suppose that $f(x) \in \mathcal{F}_2$. We show first that $\mathrm{Gal}(f) \simeq S_4^+$ by verifying that conditions (3.39) hold. Clearly, $-B$ is a square since $B = -1$. If $\Delta(g)$ is a square, then

$$Y^2 = X^3 - 2^4 3^3, \tag{3.40}$$

where

$$(X, Y) = \left((-1)^k 4A,\ (-1)^k 16\delta\right).$$

Using Sage to find the integral points on the elliptic curve (3.40) yields $X = 12$, so that $A = (-1)^k 3$, which gives $f(x)$ with $\mathrm{Gal}(f) \simeq A_4$. Hence, we conclude that $\Delta(g)$ is not a square. To see that $h(x)$ is irreducible, we assume that $h(x)$ is reducible and proceed by way of contradiction. Exactly the same argument used in the proof of Corollary 3.2 can be used here with $B = -1$ to achieve a contradiction. Thus, $\mathrm{Gal}(f) \simeq S_4^+$. The fact that $f(x)$ is monogenic can be deduced from Theorem 2.8, and we omit the details, since they are essentially outlined in the proof of the first direction.

The Case $\mathbf{S_4^-}$. Assume that $f(x)$ is monogenic with $\mathrm{Gal}(f) \simeq S_4^-$. By Theorem 2.5, we have:

$$\begin{aligned} &\text{neither } -B \text{ nor } \Delta(g) \text{ is a square,} \quad -B\Delta(g) \text{ is a square,} \\ &\text{and} \quad h(x) \text{ is irreducible.} \end{aligned} \tag{3.41}$$

Recall that

$$-B\Delta(g) = -B(-B^{k-1}(4A^3+27B^{3-k})) = B^k(4A^3+27B^{3-k}). \tag{3.42}$$

Suppose first that $k=1$, so that

$$-B\Delta(g) = B(4A^3+27B^2). \tag{3.43}$$

Then, since B is squarefree from Corollary 2.9 and $-B\Delta(g)$ is a square from (3.41), we see from (3.43) that $B \mid (4A^3+27B^2)$. Thus,

$$A \equiv \begin{cases} 0 \pmod{B} & \text{if } 2 \nmid B \\ 0 \pmod{(B/2)} & \text{if } 2 \mid B. \end{cases} \tag{3.44}$$

If $2 \nmid B$, then we see from (3.43) and (3.44) that

$$B^3(4B(A/B)^3+27)$$

is a square. Since B is squarefree, it follows that $B \mid (4B(A/B)^3+27)$, so that $B \mid 27$, and we deduce that $B \in \{\pm1, \pm3\}$.

Similarly, if $2 \mid B$, then $B \mid 2A$ from (3.44), and

$$B^3(A(2A/B)^2+27)$$

is a square. Thus, $(B/2) \mid (A(2A/B)^2+27)$, which implies that $(B/2) \mid 27$, and consequently, $B \in \{\pm2, \pm6\}$.

To determine the possible corresponding values of A for each of these values of B, we use Sage to find all integral points on the elliptic curves:

$$\begin{aligned} E_1^{\pm}: &\quad Y^2 = X^3 \pm 2^4 3^3 \quad \text{when } B = \pm1, \text{ with } X = \pm 4A; \\ E_2^{\pm}: &\quad Y^2 = X^3 \pm 2^4 3^8 \quad \text{when } B = \pm3, \text{ with } X = \pm 12A; \\ E_3^{\pm}: &\quad Y^2 = X^3 \pm 2^3 3^3 \quad \text{when } B = \pm2, \text{ with } X = \pm 2A; \\ E_4^{\pm}: &\quad Y^2 = X^3 \pm 2^3 3^8 \quad \text{when } B = \pm6, \text{ with } X = \pm 6A. \end{aligned}$$

The curves E_1^+ and E_2^- contain no integral points. For the other curves, we provide the values of X and the corresponding viable integer pairs (A,B) in Table 5.

Curve	E_1^-	E_2^+	E_3^+	E_3^-	E_4^+	E_4^-
X	12	0	-6	6,10,33	-18	54,1942
(A,B)	$(-3,-1)$	$\varnothing$	$(-3,2)$	$(-3,-2)$,$(-5,-2)$	$(-3,6)$	$(-9,-6)$.

TAB. 5: Integral X-coordinates on $E_i^{\pm}$ and corresponding pairs (A,B)

It is straightforward to verify that $(A,B)=(-9,-6)$ is the only pair in Table 5 such that $f(x)$ is monogenic with $\mathrm{Gal}(f)\simeq S_4^-$, which completes the proof when $k=1$.

Suppose now that $k=2$. It follows from (3.41) and (3.42) that

$$\delta = 4A^3+27B \quad \text{is a square.} \tag{3.45}$$

Using the same argument as given in Case S_3 when $k=2$, we arrive at the equation

$$B=3-4(A/3)^3,$$

given in (3.12). Observe that $3\mid A$ since $B\in\mathbb{Z}$. Also, $B\neq -1$ by (3.41), B is squarefree by Corollary 2.9, and $4\nmid A$ by condition (2) of Theorem 2.8.

Conversely, it is straightforward to verify that these conditions are sufficient for $f(x)$ to be monogenic with $\mathrm{Gal}(f)\simeq S_4^-$.

The Case $\mathbf{C_2\times S_4}$. The necessity of these conditions is straightforward and we omit the details. To prove that these conditions are sufficient, we need to show that $-B\delta(g)$ is not a square and that $h(x)$ is irreducible. To see that $-B\delta(g)$ is not a square, we assume the contrary, and proceed using the arguments contained in the Case S_3. To prove that $h(x)$ is irreducible, recall from Lemma 2.2 that the reducibility of $h(x)$ implies that $M(\mu)=0$ for some unique integer μ. Then, we proceed by way of contradiction and apply the the arguments used in the Case $C_2\times S_3$ to complete the proof. ☐

4. The Proof of Corollary 1.2

Proof. We first address item (1), and we begin with the family

$$\mathcal{F}_1=\{f(x): 3\nmid A \text{ or } (A \bmod 9,\ B \bmod 9)\in\{(6,1),(6,4),(6,5),(6,8)\}\}.$$

Recall, in this scenario we have $k=1$ such that

$$2\nmid AB, \quad B\neq -1 \text{ and is squarefree}, \quad \mathrm{rad}(\delta)\mid A, \tag{4.1}$$

where $f(x)=x^6+Ax^2+B\in\mathcal{F}_1$ is monogenic with $\mathrm{Gal}(f)\simeq C_2\times A_4$. We provide two infinite single-parameter subfamilies $\mathcal{T}_1$ and $\mathcal{T}_2$ of $\mathcal{F}_1$, such that all elements of each subfamily generate distinct sextic fields. We let t denote an integer parameter for both examples.

For our first example, define

$$A:=-(27t^2+27t+7), \quad B:=(2t+1)A \quad \text{and}$$
$$\mathcal{T}_1:=\{f_t(x)=x^6+Ax^2+B : t\geq 0 \text{ and } B \text{ is squarefree}\}.$$

Let $f_t(x)\in\mathcal{T}_1$ and let $g_t(x)=x^3+Ax+B$. Note that $-A>1$ and $\gcd(2t+1,A)=1$. Then, since $B=(2t+1)A$ is squarefree, we have that A is squarefree and so $f_t(x)$ is Eisenstein with respect to every prime divisor of A. Thus, $f_t(x)$ is irreducible over $\mathbb{Q}$. An easy computation shows that

$$\Delta(g_t)=-\delta=-(4A^3+27B^2)=A^2.$$

Hence, $f_t(x)$ satisfies the conditions in (4.1), and since $3\nmid A$, we see that $\mathcal{T}_1\subset\mathcal{F}_1$. Since there exist infinitely many integers t such that $(2t+1)(27t^2+27t+7)$ is squarefree [3], it follows that $\mathcal{T}_1$ and consequently, $\mathcal{F}_1$, is infinite. We claim that the elements of $\mathcal{T}_1$ generate distinct sextic fields. For $i \in \{1, 2\}$, let $f_{t_i}(x) \in \mathcal{T}_1$ with $t_1 \neq t_2$, let $f_{t_i}(\theta_i) = 0$ and $K_i = \mathbb{Q}(\theta_i)$. Assume, by way of contradiction, that $K_1 = K_2$. Then, $\Delta(K_1) = \Delta(K_2)$, and since $f_{t_i}(x)$ is monogenic, it follows from (2.4) that $\Delta(f_{t_1}) = \Delta(f_{t_2})$. Calculating $\Delta(f_{t_i})$ using Corollary (2.4), we get

$$64(2t_1 + 1)(27t_1^2 + 27t_1 + 7)^5 - 64(2t_2 + 1)(27t_2^2 + 27t_2 + 7)^5 = 64(t_1 - t_2)T = 0,$$

where $T > 0$, which yields the contradiction that $t_1 = t_2$. Thus, if $t_1 \neq t_2$, then $\Delta(f_{t_1}) \neq \Delta(f_{t_2})$, and the claim that each element of $\mathcal{T}_1$ generates a distinct sextic field follows from Corollary 2.6. We point out that the argument used in this first example to show that the sextic fields are distinct is similar to the argument needed to establish the same claim in the examples that follow, and so we omit the details.

For our second example, we define

$$\begin{aligned} &A := -3(9t^2 - 21t + 13), \quad B := (6t - 7)A \quad \text{and} \\ &\mathcal{T}_2 := \{f_t(x) = x^6 + Ax^2 + B : t \geq 0 \text{ and } B \text{ is squarefree}\}. \end{aligned}$$

Note, as in the example $\mathcal{T}_1$, $f_t(x) \in \mathcal{T}_2$ is irreducible over $\mathbb{Q}$ since $f_t(x)$ is Eisenstein with respect to every prime divisor of A, due to the fact that A is squarefree and $\gcd(6t - 7, 3(9t^2 - 21t + 13)) = 1$. Here, with $g_t(x) = x^3 + Ax + B$, we have

$$\Delta(g_t) = -\delta = -(4A^3 + 27B^2) = 9A^2,$$

so that $\operatorname{rad}(\delta) \mid A$. Hence, $f_t(x)$ satisfies (4.1). Since $(A \bmod 9,\ B \bmod 9) = (6, 1)$, it follows that $\mathcal{T}_2 \subset \mathcal{F}_1$.

We turn next to the family

$$\mathcal{F}_2 = \{f(x) : B = -1,\ A \neq (-1)^k 3,\ 4 \nmid A,\ 9 \nmid A \text{ and } \delta/3^{\nu_3(\delta)} \text{ is squarefree}\},$$

where $f(x) \in \mathcal{F}_2$ is monogenic with $\mathrm{Gal}(f) \simeq S_4^+$. We focus on $k = 1$ since that will suffice to establish what we claim. We let s be an integer parameter, and define

$$\mathcal{S} := \{f_s(x) = x^6 + (6s + 1)x^2 - 1 : s \geq 0 \text{ and } \delta \text{ is squarefree}\},$$

where $\delta = 4(6s + 1)^3 + 27$. It is easy to see that $\mathcal{S} \subset \mathcal{F}_2$, and since there exist infinitely many positive integers s such that δ is squarefree [9], it follows that $\mathcal{S}$ is infinite.

Finally, for item (1), we consider the family

$$\mathcal{F}_3 = \{f(x) : 3 \mid A,\ 4 \nmid A,\ B \neq -1,\ B = 3 - 4(A/3)^3 \text{ is squarefree}\},$$

where $f(x) = x^6 + Ax^4 + B$ is monogenic with $\mathrm{Gal}(f) \simeq S_4^-$. We let u be an integer parameter, and define

$$\begin{aligned} &A := 6u + 3, \quad B := 3 - 4(2u + 1)^3 \quad \text{and} \\ &\mathcal{U} := \{f_u(x) = x^6 + Ax^4 + B : u \geq 1 \text{ and } B \text{ is squarefree}\}. \end{aligned}$$

Note that $B \neq -1$ since $u \neq 0$. It is clear that $\mathcal{U} \subset \mathcal{F}_3$ and that $\mathcal{U}$ is infinite since there exist infinitely many positive integers u such that B is squarefree [9].

We turn now to item (2). Let v be an integer parameter.

Suppose that $k = 1$, and define

$$A := 6v + 1, \quad B := 1 \quad \text{and}$$
$$\mathcal{V}_1 := \{f_v(x) = x^6 + Ax^2 + B : v \geq 0 \text{ and } \delta \text{ is squarefree}\},$$

where $\delta = 4(6v + 1)^3 + 27$. Note that $-\delta$ cannot be a square since $\delta > 0$. Then $f_v(x) \in \mathcal{V}_1$ is monogenic with $\mathrm{Gal}(f_v) \simeq C_2 \times S_4$, and $\mathcal{V}_1$ is infinite since there exist infinitely many positive integers v such that δ is squarefree [9].

Suppose that $k = 2$, and define

$$A := 36v + 12, \quad B := 1 \quad \text{and}$$
$$\mathcal{V}_2 := \{f_v(x) = x^6 + Ax^4 + B : v \geq 0 \text{ and } \delta / \prod_{p \mid 2AB} p^{\nu_p(\delta)} \text{ is squarefree}\},$$

where

$$\delta = 4(36v + 12)^3 + 27 = 3^3 \left(2^8(3v + 1)^3 + 1\right).$$

Thus,

$$\delta / \prod_{p \mid 2AB} p^{\nu_p(\delta)} = \delta/3^3 = 2^8(3v + 1)^3 + 1,$$

and since there exist infinitely many positive integers v such that $2^8(3v + 1)^3 + 1$ is squarefree [9], we conclude that $\mathcal{V}_2$ is infinite. Since $(A \bmod 9,\ B \bmod 9) = (3, 1)$, it follows that $f_v(x) \in \mathcal{V}_2$ is monogenic with $\mathrm{Gal}(f_v) \simeq C_2 \times S_4$. $\square$

Remark 4.1. The infinite families given in the proof of Corollary 1.2 are not exhaustive, in the sense that other such single-parameter infinite families can be constructed in a similar manner.

References

[1] Awtrey, C., Jakes, P., *Galois groups of even sextic polynomials*, Canad. Math. Bull. **63** (2020), no. 3, 670–676.

[2] Awtrey, C., Lee, A., *Galois groups of reciprocal sextic polynomials*, Bull. Aust. Math. Soc. **109** (2024), 37–44.

[3] Booker, A., Browning, T. D., *Square-free values of reducible polynomials*, Discrete Anal. (2016), Paper No. 8, 16 pp.

[4] Bremner, A., Spearman, B., *Cyclic sextic trinomials* $x^6 + ax + b$, Int. J. Number Theory **6** (2010), no. 1, 161–167.

[5] Brown, S., Spearman, B., Yang, Q., *On the galois groups of sextic trinomials*, JP J. Algebra Number Theory Appl. **18** (2010), no. 1, 67–77.

[6] Brown, S., Spearman, B., Yang, Q., *On sextic trinomials with galois group* C_6*,* S_3 *or* $C_3 \times S_3$, J. Algebra Appl. **12** (2013), no. 1, 1250128, 9 pp.

[7] Butler, G., McKay, J., *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), no. 8, 863–911.

[8] Cohen, H., *A course in computational algebraic number theory*, Springer-Verlag, 2000.

[9] Erdős, P., *Arithmetical properties of polynomials*, J. London Math. Soc. **28** (1953), 416–425.

[10] Gajdzica, K., *Discriminants of special quadrinomials*, Rocky Mountain J. Math. **52** (2022), no. 5, 1587–1603.

[11] Harrington, J., Jones, L., *Monogenic sextic trinomials $x^6 + ax^3 + b$ and their Galois groups*, Acta Arith., to appear.

[12] Harrington, J., Jones, L., *Monogenic trinomials of the form $x^4 + ax^3 + d$ and their Galois groups*, J. Algebra Appl., to appear.

[13] Harrington, J., Jones, L., *The irreducibility of power compositional sextic polynomials and their Galois groups*, Math. Scand. **120** (2017), no. 2, 181–194.

[14] Harrington, J., Jones, L., *Monogenic quartic polynomials and their Galois groups*, Bull. Aust. Math. Soc. **111** (2025), no. 2, 244–259.

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

[16] Jones, L., *Monogenic reciprocal quartic polynomials and their Galois groups*, arXiv:2502.17691v1.

[17] Jones, L., *Infinite families of reciprocal monogenic polynomials and their Galois groups*, New York J. Math. **27** (2021), 1465–1493.

[18] Jones, L., *Sextic reciprocal monogenic dihedral polynomials*, Ramanujan J. **56** (2021), no. 3, 1099–1110.

[19] Jones, L., *Monogenic reciprocal trinomials and their Galois groups*, J. Algebra Appl. **21** (2022), no. 2, 2250026, 11 pp.

[20] Jones, L., *Monogenic cyclic trinomials of the form $x^4 + cx + d$*, Acta Arith. **218** (2025), no. 4, 385–394.

[21] Jones, L., *Monogenic even cyclic sextic polynomials*, Math. Slovaca **75** (2025), no. 5, 1021–1034.

[22] Jones, L., *Monogenic even quartic trinomials*, Bull. Aust. Math. Soc. **111** (2025), no. 2, 238–243.

[23] Jones, L., White, D., *Monogenic trinomials with non-squarefree discriminant*, Internat. J. Math. **32** (2021), no. 13, 2150089, 21 pp.

[24] Motoda, Y., Nakahara, T., Shah, A. S. I., Uehara, T., *On a problem of Hasse*, RIMS Kôkyûroku Bessatsu **B12** (2009), 209–221.

[25] Swan, R., *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.

[26] Voutier, P., *A family of cyclic quartic monogenic polynomials*, arXiv:2405.20288v2.

Department of Mathematics, Shippensburg University,
Shippensburg, Pennsylvania 17257, USA
E-mail: `doctorlennyjones@gmail.com`