ACTA ARITHMETICA
Online First version

Monogenic sextic trinomials $x^6 + Ax^3 + B$ and their Galois groups

by

Joshua Harrington and Lenny Jones

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

For each 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 investigate when these trinomials generate distinct sextic fields.

1. Introduction.

Let

$$f(x) = x^6 + Ax^3 + B \in \mathbb{Z}[x], \quad \text{where } AB \neq 0. \tag{1.1}$$

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 Galois group G are *distinct* if $K_1 \neq K_2$, where $K_i = \mathbb{Q}(\theta_i)$ with $f_i(\theta_i) = 0$.

The purpose of this article is to characterize the monogenic sextic trinomials $f(x)$ described in (1.1) in terms of their Galois groups. That is, for each possible Galois group $\mathrm{Gal}(f)$ of $f(x)$ over $\mathbb{Q}$, we use a theorem of Jakhar, Khanduja and Sangwan [13] to derive conditions that allow us to provide an explicit description of all such monogenic sextic trinomials $f(x)$ having Galois group $\mathrm{Gal}(f)$. We also investigate when these trinomials are distinct.

We point out that similar research involving the monogenicity and/or Galois groups of trinomials of various degrees has been conducted by many

2020 *Mathematics Subject Classification*: Primary 11R09; Secondary 11R04, 11R32, 11R21.
Key words and phrases: monogenic, power-compositional, sextic, trinomial, Galois.
Received 22 July 2025.
Published online 1 April 2026.

DOI: 10.4064/aa250722-26-8

authors [1, 2, 4–6, 11, 12, 16–24, 28]. In particular, the results in this article extend previous work of the second author on sextic trinomials [16, 17, 22].

We make some notational remarks. Throughout this paper, for integers m and n with $m \geq 2$, we let $n \bmod m$ denote the unique integer $z \in \{0, 1, \ldots, m-1\}$ such that $n \equiv z \pmod{m}$. That is, $n \bmod m = z$. We let C_n denote the cyclic group of order n, and S_3 denote the symmetric group of order 6. At certain times, it will be convenient to let $\delta = A^2 - 4B$. We also let $\nu_p(n)$ denote the p-adic valuation of the integer n for any prime p.

Using the groups C_n and S_3, the familiar names of the possible Galois groups $\mathrm{Gal}(f)$ [1, 8, 10] are provided in Table 1. For the convenience of the reader, we also include the "T"-notation [7] for these groups, which is given in Maple when computing the Galois group.

Table 1. Possible Galois groups for $f(x) = x^6 + Ax^3 + B$

$\mathrm{Gal}(f)$	C_6	S_3	$C_2 \times S_3$	$C_3 \times S_3$	$S_3 \times S_3$
T-notation	6T1	6T2	6T3	6T5	6T9

Our main theorem is:

THEOREM 1.1. *Let $f(x) = x^6 + Ax^3 + B \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Q}$, with $AB \neq 0$. Then $f(x)$ is monogenic with $\mathrm{Gal}(f)$ isomorphic to*

(1) *C_6 if and only if $f(x) \in \mathcal{F}_1 := \{x^6 - x^3 + 1, x^6 + x^3 + 1\}$;*
(2) *S_3 never occurs;*
(3) *$C_2 \times S_3$ if and only if $f(x) \in \mathcal{F}_i$ for some $i \in \{2, 3, 4\}$, where*
   (a) $\mathcal{F}_2 := \{x^6 - 2x^3 + 2,\ x^6 + 2x^3 + 2\}$,
   (b) $\mathcal{F}_3 := \{x^6 + Ax^3 + 1 : A \bmod 9 \neq 0,\ A \neq \pm 1,$ *with $A-2$ and $A+2$ squarefree*$\}$,
   (c) $\mathcal{F}_4 := \{x^6 + Ax^3 - 1 : A \bmod 4 \neq 0,\ A \bmod 9 \notin \{0, 4, 5\},$ *with $(A^2+4)/\gcd(A^2+4, 4)$ squarefree*$\}$;
(4) *$C_3 \times S_3$ if and only if $f(x) \in \mathcal{F}_5$, where*
   $\mathcal{F}_5 := \{x^6 + Ax^3 + (A^2+3)/4 : A \bmod 2 = 1,\ A \neq \pm 1,$ *with $(A^2+3)/4$ squarefree*$\}$;
(5) *$S_3 \times S_3$ if and only if $f(x)$ is contained in one of 144 infinite pairwise-disjoint 2-parameter monogenic families.*

Moreover, $\mathcal{F}_i \cap \mathcal{F}_j = \varnothing$ for $i \neq j$, and choosing all trinomials with positive coefficient on x^3 in each $\mathcal{F}_i$ yields a complete set of distinct monogenic trinomials for the corresponding Galois groups.

2. Basic peliminaries. We begin with a theorem that provides conditions under which the possible Galois groups of $f(x) = x^6 + Ax^3 + B$ from Table 1 can occur.

THEOREM 2.1 ([8, 10]). *Let $f(x) = x^6 + Ax^3 + B \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Q}$, and let $R(x) = x^3 - 3Bx + AB$. Let $\delta = A^2 - 4B$. Then*

$$\mathrm{Gal}(f) \simeq \begin{cases} C_6 & \text{if and only if } -3\delta \text{ is a square, } R(x) \text{ is irreducible and} \\ & B = c^3 \text{ for some } c \in \mathbb{Z}, \\ S_3 & \text{if and only if } -3\delta \text{ is a square, } R(x) \text{ is reducible and} \\ & B \neq c^3 \text{ for any } c \in \mathbb{Z}, \\ C_2 \times S_3 & \text{if and only if } -3\delta \text{ is not a square and} \\ & \text{either } R(x) \text{ is reducible or } B = c^3 \text{ for some } c \in \mathbb{Z}, \\ C_3 \times S_3 & \text{if and only if } -3\delta \text{ is a square, } R(x) \text{ is irreducible and} \\ & B \neq c^3 \text{ for any } c \in \mathbb{Z}, \\ S_3 \times S_3 & \text{if and only if } -3\delta \text{ is not a square, } R(x) \text{ is irreducible} \\ & \text{and } B \neq c^3 \text{ for any } c \in \mathbb{Z}. \end{cases}$$

The next theorem is due to the authors [10, Theorem 3.1].

THEOREM 2.2. *Let $g(x) = x^2 + Ax + B \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Q}$. Then*

$$f(x) := g(x^3) = x^6 + Ax^3 + B$$

is reducible over $\mathbb{Q}$ if and only if $B = n^3$ and $A = m^3 - 3mn$ for some $m, n \in \mathbb{Z}$.

The following immediate corollary of Theorem 2.2 will be useful in the proof of Theorem 1.1.

COROLLARY 2.3. *Let $g(x) = x^2 + Ax + B \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Q}$, such that B is squarefree with $|B| \neq 1$. Then*

$$f(x) := g(x^3) = x^6 + Ax^3 + B$$

is irreducible over $\mathbb{Q}$.

The formula for the discriminant of an arbitrary trinomial is given in the next theorem.

THEOREM 2.4 ([27]). *Let $f(x) = x^n + Ax^m + B \in \mathbb{Z}[x]$, where $0 < m < n$, and let $d = \gcd(n, m)$. Then $\Delta(f)$ equals*

$$(-1)^{n(n-1)/2} B^{m-1} \big(n^{n/d} B^{(n-m)/d} - (-1)^{n/d} (n-m)^{(n-m)/d} m^{m/d} A^{n/d} \big)^d.$$

We now present some basic information concerning the monogenicity of a polynomial. Suppose that $f(x) \in \mathbb{Z}[x]$ is monic and irreducible over $\mathbb{Q}$. Let $K = \mathbb{Q}(\theta)$ with ring of integers $\mathbb{Z}_K$, where $f(\theta) = 0$. Then we have [9]

$$\Delta(f) = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 \Delta(K), \tag{2.1}$$

where $\Delta(f)$ and $\Delta(K)$ denote the discriminants over $\mathbb{Q}$, respectively, of $f(x)$ and the number field K. Thus, we have the following theorem from (2.1).

THEOREM 2.5. *The polynomial $f(x)$ is monogenic if and only if $\Delta(f) = \Delta(K)$, or equivalently, $\mathbb{Z}_K = \mathbb{Z}[\theta]$.*

We then have the following immediate corollary.

COROLLARY 2.6. *Let $f_1(x) \neq f_2(x)$ be two monogenic polynomials such that $\deg(f_1) = \deg(f_2)$. Let $K_i = \mathbb{Q}(\theta_i)$, where $f_i(\theta_i) = 0$. If $\Delta(f_1) \neq \Delta(f_2)$, then $f_1(x)$ and $f_2(x)$ are distinct.*

The next theorem, due to Jakhar, Khanduja and Sangwan [13], gives necessary and sufficient conditions for an irreducible trinomial $f(x) = x^n + Ax^m + B \in \mathbb{Z}[x]$, where $m \geq 1$ is a proper divisor of n, to be monogenic. Although the same authors have also proven a version of this theorem that addresses arbitrary irreducible trinomials [14], we do not require that more general version here.

THEOREM 2.7. *Let $n \geq 2$ be an integer. 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 $f(x) = x^n + Ax^m + B$ over $\mathbb{Q}$, where $m \geq 1$ is a proper divisor of n. Let $t = n/m$. 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*

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

where $a_2 = A/p$ and $b_1 = \frac{B+(-B)^{p^j}}{p}$ with $p^j \parallel tm$;
(3) *when $p \nmid A$ and $p \mid B$, then*

$$\text{either} \quad p \mid a_1 \text{ and } p \nmid b_2 \quad \text{or} \quad p \nmid a_1 b_2^{m-1}(Aa_1^{t-1} + (-b_2)^{t-1}),$$

where $a_1 = \frac{A+(-A)^{p^l}}{p}$ with $p^l \parallel (t-1)m$, and $b_2 = B/p$;
(4) *when $p \nmid AB$ and $p \mid m$ with $n = s'p^k$, $m = sp^k$, $p \nmid \gcd(s', s)$, then*

$$H_1(x) := x^{s'} + Ax^s + B \quad \text{and} \quad H_2(x) := \frac{Ax^{sp^k} + B + (-Ax^s - B)^{p^k}}{p}$$

are coprime modulo p;
(5) *when $p \nmid ABm$, then $p^2 \nmid (t^t B^{t-1} - (-1)^t (t-1)^{t-1} A^t)$.*

3. The proof of Theorem 1.1. Before we begin the proof of Theorem 1.1, we present an adaptation of Theorem 2.7 to the specific trinomial $f(x) = x^6 + Ax^3 + B$.

THEOREM 3.1. *Suppose that $f(x) = x^6 + Ax^3 + B \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$. Note that*

$$\Delta(f) = 3^6 B^2 (A^2 - 4B)^3 \tag{3.1}$$

by Theorem 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* $p \in \{2, 3\}$ *with*

$$(A \bmod 4,\ B \bmod 4) \in \{(0,1),(2,3)\} \quad \text{if } p = 2,$$

$$\begin{aligned} \text{and} \quad (A \bmod 9,\ B \bmod 9) \in \{&(0,2),(0,4),(0,5),(0,7),\\ &(3,1),(3,4),(3,7),(3,8),\\ &(6,1),(6,4),(6,7),(6,8)\} \quad \text{if } p = 3; \end{aligned}$$

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

$$\begin{aligned} (A \bmod 9,\ B \bmod 9) \in \{&(1,3),(1,6),(2,3),(4,6),\\ &(5,6),(7,3),(8,3),(8,6)\} \quad \text{if } p = 3; \end{aligned}$$

(4) *when* $3 \nmid AB$, *then*

$$\begin{aligned} (A \bmod 9,\ B \bmod 9) \in \{&(1,1),(1,2),(1,4),(1,5),(1,8),(2,2),(2,4),\\ &(2,5),(2,7),(2,8),(4,1),(4,2),(4,5),(4,7),\\ &(5,1),(5,2),(5,5),(5,7),(7,2),(7,4),(7,5),\\ &(7,7),(7,8),(8,1),(8,2),(8,4),(8,5),(8,8)\}; \end{aligned}$$

(5) *when* $p \nmid 3AB$, *then* $p^2 \nmid (A^2 - 4B)$.

Proof. Since the methods used for the adaptation of Theorem 2.7 to the specific trinomial $f(x) = x^6 + Ax^3 + B$ are straightforward and mainly computational, we provide details only for condition (2). Suppose that $p \mid A$ and $p \nmid B$. Then, from condition (2) of Theorem 2.7, we have $n = 6$, $m = 3$, $t = 2$ and $p^j \parallel 6$. Hence, $p \in \{2, 3\}$ with $a_2 = A/p$ and

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

Then it is easy to calculate the congruence classes of A and B modulo p^2 for which either $p \mid a_2$ and $p \nmid b_1$, or $p \nmid a_2(a_2^2 B + b_1^2)$. ∎

We observe that further refinements of Theorem 3.1 are possible. In particular, if $f(x)$ is monogenic, then B must be squarefree from conditions (1) and (3). Consequently,

$$\Gamma := (A^2 - 4B)/(2^{\nu_2(A^2-4B)} 3^{\nu_3(A^2-4B)}) \tag{3.2}$$

must also be squarefree from condition (5) of Theorem 3.1. These observations will be useful in establishing the converse of each part of Theorem 3.1. More precisely, for a given Galois group G and a monogenic trinomial $f(x) = x^6 + Ax^3 + B$ with $\mathrm{Gal}(f) \simeq G$, the fact that both B and Γ

are squarefree will be especially helpful in showing that $f(x) \in \mathcal{F}_i$ for the appropriate value of i.

Proof of Theorem 1.1. Considering, one at a time, each of the possible Galois groups

$$C_6,\ S_3,\ C_2 \times S_3,\ C_3 \times S_3,$$

we use (3.1), Theorem 2.1 and Theorem 3.1 to show that each $f(x) \in \mathcal{F}_i$ is monogenic with the prescribed Galois group. We then establish the claim concerning when the trinomials in $\mathcal{F}_i$ are distinct, and show that each $\mathcal{F}_i$, with $i \geq 3$, contains infinitely many distinct trinomials. Finally, we prove the converse for each of these groups. For the special case $\mathrm{Gal}(f) \simeq S_3 \times S_3$, we use Theorem 3.1 to illustrate how to construct infinite 2-parameter families to "capture" all monogenic trinomials $f(x)$.

We recall that

$$R(x) = x^3 - 3Bx + AB. \tag{3.3}$$

The case C_6

Trinomials in $\mathcal{F}_1$. Let $f^-(x) = x^6 - x^3 + 1$ and $f^+(x) = x^6 + x^3 + 1$. Straightforward calculations (using Maple, (3.1), Theorem 2.1 and Theorem 3.1) confirm that $f^-(x)$ and $f^+(x)$ are irreducible and monogenic with

$$\Delta(f^-) = \Delta(f^+) = -3^9 \quad \text{and} \quad \mathrm{Gal}(f^-) = \mathrm{Gal}(f^+) \simeq C_6.$$

Furthermore, if $f^+(\theta) = 0$, then since $f^-(-\theta) = 0$, it follows that $f^-(x)$ and $f^+(x)$ are not distinct.

For the converse, suppose that $f(x) = x^6 + Ax^3 + B$ is monogenic with $\mathrm{Gal}(f) \simeq C_6$. Then $B = c^3$ for some nonzero integer c, by Theorem 2.1. But B is squarefree, since $f(x)$ is monogenic. Hence, $B = \pm 1$. Also, by Theorem 2.1, we find that $-3(A^2 - 4B)$ is a square, which is impossible if $B = -1$. Thus, $B = 1$ so that

$$-3(A^2 - 4B) = -3(A^2 - 4) = 12 - 3A^2$$

is a square. Note that $12 - 3A^2 \neq 0$ since $f(x)$ is irreducible. Therefore, $A = \pm 1$, which completes the proof of (1).

The case S_3. Suppose that $f(x) = x^6 + Ax^3 + B \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$ with $\mathrm{Gal}(f) \simeq S_3$. Observe that if $2 \nmid AB$, then

$$R(x) \equiv x^3 + x + 1 \pmod 2 \tag{3.4}$$

is irreducible in $\mathbb{F}_2[x]$, and consequently, $R(x)$ is irreducible over $\mathbb{Q}$, which contradicts Theorem 2.1. Therefore, $2 \mid AB$. Note that if $2 \nmid A$ and $2 \mid B$, then

$$-3(A^2 - 4B) \equiv 5 \pmod 8,$$

which contradicts the fact that $-3(A^2-4B)$ is a square from Theorem 2.1. To rule out the final two possibilities

$$(A \bmod 2,\ B \bmod 2) \in \{(0,0),\ (0,1)\},$$

we assume that $f(x)$ is monogenic, and proceed by way of contradiction invoking Theorem 3.1.

If $2 \mid A$ and $2 \mid B$, then $B \bmod 4 = 2$ by condition (1) of Theorem 3.1, and $4 \mid (A^2-4B)$. Thus,

$$\frac{-3(A^2-4B)}{4} = -3\left((A/2)^2 - B\right) \equiv \begin{cases} 2 \pmod 4 & \text{if } 4 \mid A, \\ 3 \pmod 4 & \text{if } 4 \nmid A, \end{cases}$$

which contradicts the fact that $-3(A^2-4B)$ is a square from Theorem 2.1.

The final situation to consider is when $2 \mid A$ and $2 \nmid B$. Since $f(x)$ is monogenic and $4 \mid (A^2-4B)$, we deduce from condition (2) of Theorem 3.1 with $p=2$ that

$$(A \bmod 4, B \bmod 4) \in \{(0,1),(2,3)\}.$$

But it is then easy to verify that

$$\frac{-3(A^2-4B)}{4} \equiv \begin{cases} 3 \pmod 4 & \text{if } (A \bmod 4,\ B \bmod 4) = (0,1), \\ 2 \pmod 4 & \text{if } (A \bmod 4,\ B \bmod 4) = (2,3), \end{cases}$$

which again contradicts the fact that $-3(A^2-4B)$ is a square from Theorem 2.1. This final contradiction completes the proof of (2).

The case $C_2 \times S_3$

Trinomials in $\mathcal{F}_2$. Since the arguments here for the monogenicity of the two elements of $\mathcal{F}_2$, and the fact that they are not distinct, are similar to the case $\mathcal{F}_1$, we omit the details.

Trinomials in $\mathcal{F}_3$. Let $f(x) = x^6 + Ax^3 + 1$ such that

$$A \bmod 9 \neq 0, \quad A \neq \pm 1, \quad \text{with } A-2 \text{ and } A+2 \text{ squarefree.}$$

The restriction $A \bmod 9 \neq 0$ is to avoid the reducibility of $f(x)$ when $A=0$, and the nonmonogenicity of $f(x)$ otherwise. The restriction that $A \neq \pm 1$ is to avoid overlap with $\mathcal{F}_1$. The restriction that $A-2$ and $A+2$ be squarefree is required for the irreducibility and monogenicity of $f(x)$, as we shall see below.

We show first that $f(x)$ is irreducible over $\mathbb{Q}$. Let $h(x) = x^2+Ax+1$. It is easy to see that the only solutions to the Diophantine equation $A^2-4=y^2$ are $(A,y) \in \{(-2,0),(2,0)\}$. Hence, $h(x)$ is irreducible over $\mathbb{Q}$ since $A-2$ and $A+2$ are squarefree. Thus, if $f(x) = h(x^3)$ is reducible over $\mathbb{Q}$, we see by Theorem 2.2 that $A = m^3 - 3m$ for some $m \in \mathbb{Z}$. But then

$$A-2 = (m-2)(m+1)^2 \quad \text{and} \quad A+2 = (m+2)(m-1)^2,$$

which is impossible since $A-2$ and $A+2$ are squarefree, and $A \neq 0$. Therefore, $f(x)$ is irreducible over $\mathbb{Q}$.

Observe that

$$\Delta(f) = 3^6(A-2)^3(A+2)^3 \tag{3.5}$$

from (3.1). For the monogenicity of $f(x)$, we first consider the prime divisor $p = 3$ of $\Delta(f)$. If $3 \mid A$, then

$$(A \bmod 9,\ B \bmod 9) \in \{(3,1),(6,1)\},$$

so that condition (2) of Theorem 3.1 is satisfied. If $3 \nmid A$, then $A \not\equiv \pm 2 \pmod 9$ since $A \mp 2$ is squarefree. Hence,

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

so that condition (3) of Theorem 3.1 is satisfied.

Next, suppose that $p \mid (A-2)$ with $p \neq 3$. If $p \mid A$, then $p = 2$. It follows that $A \bmod 4 = 0$ since $A-2$ and $A+2$ are squarefree. Hence, $(A \bmod 4,\ B \bmod 4) = (0,1)$ so that condition (2) of Theorem 3.1 is satisfied. If $p \nmid A$, then $p \neq 2$ and $p \nmid (A+2)$ so that $p^2 \nmid (A^2-4)$ since $A-2$ and $A+2$ are squarefree. A similar argument shows that $p^2 \nmid (A^2-4)$ if $p \mid (A+2)$ with $p \neq 3$. Hence, condition (5) of Theorem 3.1 is satisfied, and we conclude from Theorem 3.1 that $f(x)$ is monogenic.

Note that $A^2 - 4 > 0$ from the restrictions on A. Thus, $-3(A^2-4B)$ is not a square. Since $B = c^3$ with $c = 1$, we conclude from Theorem 2.1 that $\mathrm{Gal}(f) \simeq C_2 \times S_3$.

Suppose that

$$f_1(x) = x^6 + A_1x^3 + 1 \in \mathcal{F}_3 \quad \text{and} \quad f_2(x) = x^6 + A_2x^3 + 1 \in \mathcal{F}_3,$$

such that $f_1(x) \neq f_2(x)$ and $f_i(\theta_i) = 0$. Since $A_1 \neq A_2$ and $A_i^2 - 4 > 0$, we see from (3.5) that if $\Delta(f_1) = \Delta(f_2)$, then

$$(A_1 - A_2)(A_1 + A_2)\left((A_1^2-4)^2 + (A_1^2-4)(A_2^2-4) + (A_2^2-4)^2\right) = 0,$$

which implies that $A_1 = -A_2$. Consequently, trinomials in $\mathcal{F}_3$ with positive coefficient on x^3 are distinct by Corollary 2.6.

Since $9 \nmid A$, suppose that $A = 9k + r$ for some fixed integer r with $9 \nmid r$. Then, there exist infinitely many integers $k > 0$ such that

$$(A-2)(A+2) = (9k-r-2)(9k+r+2)$$

is squarefree [3]. Hence, we conclude that there exist infinitely many distinct trinomials in $\mathcal{F}_3$.

Trinomials in $\mathcal{F}_4$. Let $f(x) = x^6 + Ax^3 - 1$ such that

$$A \bmod 4 \neq 0,\ A \bmod 9 \notin \{0,4,5\},$$
$$\text{with } (A^2+4)/\gcd(A^2+4,4) \text{ squarefree.}$$

The argument for the irreducibility of $f(x)$ here is similar to the situation of $\mathcal{F}_3$, and we omit the details.

From (3.1), we have

$$\Delta(f) = 3^6(A^2+4)^3.$$

To establish monogenicity, we proceed as before, starting with $p = 3$. If $3 \mid A$, then

$$(A \bmod 9,\ B \bmod 9) \in \{(3,8),(6,8)\},$$

so that condition (2) of Theorem 3.1 is satisfied. If $3 \nmid A$, then

$$(A \bmod 9,\ B \bmod 9) \in \{(1,8),(2,8),(7,8),(8,8)\},$$

so that condition (4) of Theorem 3.1 is satisfied.

Next, suppose that $p \mid (A^2+4)$ with $p \neq 3$. If $p = 2$, then $2 \mid A$ so that $(A \bmod 4,\ B \bmod 4) = (2,3)$ since $4 \nmid A$. Hence, condition (2) of Theorem 3.1 is satisfied. Assume then that $p \neq 2$. Note that $p \nmid A$. Thus, $p^2 \nmid (A^2+4)$ since $(A^2+4)/\gcd(A^2+4,4) = A^2+4$ is squarefree. Therefore, condition (5) of Theorem 3.1 is satisfied, and $f(x)$ is monogenic.

Arguments similar to the situation of $\mathcal{F}_3$ verify here that $\mathrm{Gal}(f) \simeq C_2 \times S_3$ and that trinomials in $\mathcal{F}_4$ with positive coefficient on x^3 are distinct. Moreover, if $A = 36k+1$, then there exist infinitely many positive integers k such that

$$\frac{A^2+4}{\gcd(A^2+4,4)} = \frac{(36k+1)^2+4}{\gcd((36k+1)^2+4,4)} = 1296k^2+72k+5$$

is squarefree [25], which implies that $\mathcal{F}_4$ contains infinitely many distinct trinomials.

We turn now to the converse. That is, we assume that $f(x) = x^6+Ax^3+B$ is monogenic with $\mathrm{Gal}(f) \simeq C_2 \times S_3$, and we show that $f(x) \in \mathcal{F}_2 \cup \mathcal{F}_3 \cup \mathcal{F}_4$. Since $f(x)$ is monogenic, we recall that B and Γ (from (3.2)) are squarefree from conditions (1), (3) and (5) of Theorem 3.1.

Suppose first that $|B| \geq 2$. Then, since B is squarefree, it follows that $B \neq c^3$ for any $c \in \mathbb{Z}$. Hence, $R(x)$ must be reducible by Theorem 2.1 since $\mathrm{Gal}(f) \simeq C_2 \times S_3$. Consequently, $2 \mid AB$ since otherwise $R(x)$ is irreducible over $\mathbb{Q}$, as in the case of S_3 in (3.4). Furthermore, if p is a prime such that $p \mid B$ and $p \nmid A$, then $R(x)$ is p-Eisenstein since B is squarefree, which implies the contradiction that $R(x)$ is irreducible over $\mathbb{Q}$. We deduce therefore that all primes dividing B must also divide A. Hence, since B is squarefree, it follows that

$$B \mid A \quad \text{and} \quad 2 \mid A. \tag{3.6}$$

Since $R(x)$ is reducible over $\mathbb{Q}$, we have

$$R(x) = (x-r)(x^2+rx+r^2-3B), \tag{3.7}$$

for some $r \in \mathbb{Z}$. Calculating $\Delta(R)$ in two ways, using Theorem 2.4 for (3.3) and [15] for (3.7), yields

$$\Delta(R) = -27(A^2 - 4B)B^2 = -27(r^2 - 4B)(r^2 - B)^2. \tag{3.8}$$

Since B is squarefree, it follows from (3.8) that $B \mid r$, so that

$$A^2 - 4B = (r^2 - 4B)\left(\frac{r^2}{B} - 1\right)^2. \tag{3.9}$$

Hence,

$$\Gamma = \frac{A^2 - 4B}{2^{\nu_2(A^2-4B)}3^{\nu_3(A^2-4B)}} = \frac{(r^2 - 4B)\left(\frac{r^2}{B} - 1\right)^2}{2^{\nu_2(A^2-4B)}3^{\nu_3(A^2-4B)}}$$

is squarefree, and consequently

$$\left|\frac{r^2}{B} - 1\right| = 2^a 3^b \tag{3.10}$$

for some nonnegative integers a and b.

We claim that $b = 0$ in (3.10). Suppose, by way of contradiction, that $b \geq 1$. Then

$$r^2/B - 1 \equiv 0 \pmod 3, \tag{3.11}$$

so that $9 \,|\, (r^2/B - 1)^2$, which implies that

$$9 \,|\, (A^2 - 4B) \tag{3.12}$$

from (3.9). Hence, since B is squarefree and $B \mid r$, we have $3 \,|\, (r^2/B)$, which contradicts (3.11). Thus, $B \equiv r^2 \equiv 1 \pmod 3$, so that $3 \nmid A$ from (3.12). Consequently, we have

$$A \bmod 9 \in \{1, 2, 4, 5, 7, 8\} \quad \text{and} \quad B \bmod 9 \in \{1, 4, 7\}.$$

Thus, in light of (3.12), straightforward calculations reveal that

$$(A \bmod 9,\ B \bmod 9) \in \{(1, 7), (2, 1), (4, 4), (5, 4), (7, 1), (8, 7)\},$$

which contradicts condition (4) of Theorem 3.1 since $f(x)$ is monogenic. Thus, the claim that $b = 0$ is established and

$$\left|\frac{r^2}{B} - 1\right| = 2^a \tag{3.13}$$

for some nonnegative integer a.

We claim next that $a \leq 1$ in (3.13). Assume, by way of contradiction, that $a \geq 2$. Then $16 \mid (r^2/B - 1)^2$ from (3.13), so that

$$16 \mid (A^2 - 4B) \tag{3.14}$$

from (3.9). If $2 \,|\, B$, then $r^2/B - 1 \equiv 1 \pmod 2$ since B is squarefree, which

contradicts (3.13). Hence, $2 \nmid B$. Thus, since $2 \mid A$ from (3.6), we see that

$$A \bmod 16 \in \{0, 2, 4, 6, 8, 10, 12, 14\},$$
$$B \bmod 16 \in \{1, 3, 5, 7, 9, 11, 13, 15\}.$$

Checking these values with the added restriction of (3.14) produces

$$(A \bmod 16,\ B \bmod 16) \in S = \{(2,1),(2,5),(2,9),(2,13),(6,1),(6,5),(6,9),$$
$$(6,13),(10,1),(10,5),(10,9),(10,13),(14,1),(14,5),(14,9),(14,13)\}.$$

Observe that the reduction modulo 4 of every pair in S results in the same pair $(A \bmod 4, B \bmod 4) = (2,1)$, which contradicts condition (2) of Theorem 3.1 since $f(x)$ is monogenic. Thus, we have established the claim that $a \leq 1$ in (3.13).

Suppose then that $a = 0$ in (3.13). If $r^2/B - 1 < 0$, then $r = 0$, which yields the contradiction that $AB = 0$ from (3.3) since $R(r) = 0$. If $r^2/B - 1 > 0$, then, since B is squarefree, we get the two solutions

$$(A, B, r) \in \{(2,2,2), (-2,2,-2)\}$$

from (3.3) since $R(r) = 0$, which correspond precisely to the elements of $\mathcal{F}_2$.

Suppose next that $a = 1$ in (3.13). Then

$$\frac{r^2}{B} - 1 = \pm 2,$$

from which we deduce that

$$(r, B) \in \{(-1,-1),(1,-1),(-3,3),(3,3)\}. \tag{3.15}$$

The first two pairs in (3.15) are impossible since $|B| \geq 2$, while the last two pairs both produce the contradiction that $A = 0$ by (3.3) since $R(r) = 0$. Therefore, we may assume that $|B| = 1$.

We first consider $B = 1$, so $f(x) = x^6 + Ax^3 + 1$. Note that if $|A| = 1$, then

$$-3\delta = -3(A^2 - 4B) = 9,$$

which contradicts the fact that -3δ is not a square from Theorem 2.1. Hence, $|A| \neq 1$. If $9 \mid A$, then

$$(A \bmod 9,\ B \bmod 9) = (0,1),$$

which contradicts condition (2) of Theorem 3.1 since $f(x)$ is monogenic. Thus, $9 \nmid A$. Next, we prove that $A - 2$ is squarefree. Assume, by way of contradiction, that $A - 2$ is not squarefree, and let p be a prime divisor of $A - 2$ such that $p^2 \mid (A - 2)$. Then $p^2 \mid (A^2 - 4)$, and $p \mid 3A$ by condition (5) of Theorem 3.1. Suppose that $p \mid A$. Then $p^2 \mid A^2$, so that $p^2 \mid 4$. Hence, $p = 2$ and $2 \mid A$. Thus, since $B \equiv 1 \pmod 4$, we must have $(A \bmod 4, B \bmod 4) = (0,1)$ from condition (2). But then $A - 2 \equiv 2 \pmod 4$, contradicting the assumption that $2^2 \mid (A-2)$. Therefore, $p = 3$ and $p \nmid A$. Since $3^2 \mid (A-2)$, it follows that $A \equiv 2 \pmod 9$, which implies that $(A \bmod 9, B \bmod 9) = (2,1)$,

contradicting condition (4) of Theorem 3.1. Hence, $A-2$ is squarefree. The proof that $A+2$ is squarefree is similar, and so we omit the details. Thus, $f(x) \in \mathcal{F}_3$, and the proof for $B=1$ is complete.

Suppose now that $B=-1$, so that $f(x)=x^6+Ax^3-1$. If $4 \mid A$, then $(A \bmod 4, B \bmod 4) = (0,3)$ which contradicts condition (2) of Theorem 3.1. Thus, $4 \nmid A$. Similarly, if $9 \mid A$, then $(A \bmod 9, B \bmod 9) = (0,8)$ which contradicts condition (2) of Theorem 3.1; and if $3 \nmid A$ with $(A \bmod 9, B \bmod 9) \in \{(4,8),(5,8)\}$, we have a contradiction with (4) of Theorem 3.1. Consequently, $A \bmod 9 \notin \{0,4,5\}$. Next, we claim that $\Omega := (A^2+4)/\gcd(A^2+4,4)$ is squarefree. Note that

$$\Omega = \begin{cases} (A^2+4)/4 & \text{if } 2 \mid A, \\ A^2+4 & \text{if } 2 \nmid A. \end{cases}$$

By way of contradiction, assume that $p^2 \mid \Omega$ for some prime p. If $2 \mid A$, then $2 \| \Omega$ since $4 \nmid A$. Thus, $p \geq 3$ regardless of the parity of A. Since $f(x)$ is monogenic, we see by condition (5) of Theorem 3.1 that $p \mid 3A$. Observe that $3 \nmid \Omega$ since -1 is not a square modulo 3; and if $p \mid A$, we arrive at the contradiction that $p=2$. Hence, the claim that Ω is squarefree has been established, which verifies that $f(x) \in \mathcal{F}_4$, and completes the proof of (3).

The case $C_3 \times S_3$

Trinomials in $\mathcal{F}_5$. Let $f(x)=x^6+Ax^3+(A^2+3)/4$ such that

$$A \bmod 2 = 1, \ A \neq \pm 1, \quad \text{with } B=(A^2+3)/4 \text{ squarefree.}$$

Let $h(x)=x^2+Ax+(A^2+3)/4$, which is irreducible over $\mathbb{Q}$ since $\Delta(h)=-3$. Then, if $f(x)=h(x^3)$ is reducible, it follows from Theorem 2.2 that the Diophantine equation

$$\mathcal{D}: \quad (A^2+3)/4 = n^3 \tag{3.16}$$

has a solution. Hence, $n=\pm 1$ since $(A^2+3)/4$ is squarefree. If $n=-1$, then $\mathcal{D}$ in (3.16) has no integer solutions, and if $n=1$, we see that $A=\pm 1$, which contradicts the restriction on A. Hence, $f(x)$ is irreducible over $\mathbb{Q}$.

From (3.1), we have

$$\Delta(f) = -3^9 \left(\frac{A^2+3}{4} \right)^2.$$

For the monogenicity of $f(x)$, we consider first the prime divisor $p=3$ of $\Delta(f)$. If $3 \mid A$, then $3 \mid (A^2+3)/4$. Thus, condition (1) of Theorem 3.1 is satisfied since $(A^2+3)/4$ is squarefree. If $3 \nmid A$, then $3 \nmid (A^2+3)/4$ and, with the restrictions on A, we have

$$(A \bmod 9, \ B \bmod 9) \in \{(1,1),(2,4),(4,7),(5,7),(7,4),(8,1)\}.$$

Thus, condition (4) of Theorem 3.1 is satisfied.

Suppose next that $p \neq 3$ is a prime divisor of $(A^2+3)/4$. Observe that $p \neq 2$ since $2 \nmid A$, and that $p \nmid A$. Thus, condition (3) of Theorem 3.1 is satisfied since $(A^2+3)/4$ is squarefree. Hence, $f(x)$ is monogenic.

To show that $\mathrm{Gal}(f) \simeq C_3 \times S_3$, we use Theorem 2.1. We have already shown that the equation $\mathcal{D}$ in (3.16) has no integer solutions. An easy calculation reveals that $-3\delta = 3^2$. Finally, we must show that

$$R(x) = x^3 - 3\left(\frac{A^2+3}{4}\right)x + A\left(\frac{A^2+3}{4}\right)$$

is irreducible over $\mathbb{Q}$. From the previous discussion, we see that

$$d := \gcd(A, (A^2+3)/4) \in \{1, 3\}.$$

If $d = 1$, then there exists a prime divisor $p \neq 3$ of $(A^2+3)/4$ such that $p \nmid A$. Since $(A^2+3)/4$ is squarefree, it follows that $R(x)$ is p-Eisenstein, and therefore irreducible over $\mathbb{Q}$. If $d = 3$, then we can let $A = 3k$ for some $k \in \mathbb{Z}$. Then

$$A\left(\frac{A^2+3}{4}\right) = 3^2 k\left(\frac{3k^2+1}{4}\right).$$

If $|k| > 1$, then $(3k^2+1)/4 > 1$ and there exists a prime divisor p of $(3k^2+1)/4$ such that $p \nmid 3^2k$. Since $(3k^2+1)/4$ is squarefree, it follows that $R(x)$ is p-Eisenstein and irreducible over $\mathbb{Q}$. If $|k| = 1$, then

$$R(x) = x^3 - 9x - 9 \quad \text{or} \quad R(x) = x^3 - 9x + 9,$$

both of which are irreducible in $\mathbb{F}_2[x]$, and hence irreducible over $\mathbb{Q}$. Thus, $\mathrm{Gal}(f) \simeq C_3 \times S_3$.

Using arguments similar to previous situations show that trinomials in $\mathcal{F}_5$ with positive coefficient on x^3 are all distinct, and that there exist infinitely many such trinomials in $\mathcal{F}_5$.

For the converse, we assume that $f(x) = x^6 + Ax^3 + B$ is monogenic with $\mathrm{Gal}(f) \simeq C_3 \times S_3$, and we show that $f(x) \in \mathcal{F}_5$. We first note that $2 \nmid A$, and since the proof is identical to the proof given in the last two paragraphs of "The case S_3", we omit the details here. Then, $2 \nmid (A^2 - 4B)$ so that

$$\Gamma = \frac{A^2 - 4B}{3^{\nu_3(A^2-4B)}}.$$

Since Γ is squarefree, and $-3(A^2-4B)$ is a square by Theorem 2.1, it follows that

$$-3(A^2 - 4B) = 3^{2b}$$

for some integer $b \geq 1$, which implies that

$$B = \frac{A^2 + 3^{2b-1}}{4}. \tag{3.17}$$

Next, we claim that $A \neq \pm 1$. Assume, by way of contradiction, that $A = \pm 1$. If $B = 1$, then $f(x) \in \mathcal{F}_1$, and if $B = -1$, then $f(x) \in \mathcal{F}_4$. Thus, $|B| \geq 2$. Observe that if $b = 1$ in (3.17), then $B = 1$, which contradicts the fact that $|B| \geq 2$. Hence, $b \geq 2$, so that $B \equiv 7 \pmod 9$. Therefore, ($A \bmod 9$, $B \bmod 9$) $\in \{(1,7),(8,7)\}$, which contradicts condition (4) of Theorem 3.1. Thus, $A \neq \pm 1$.

Suppose that $b \geq 2$ in (3.17). If $3 \,|\, A$, then $9 \,|\, B$, which contradicts the fact that B is squarefree. Hence, $3 \nmid A$ and $B \equiv 7A^2 \pmod 9$ from (3.17), so that $3 \nmid B$. Consequently,

$$(A \bmod 9,\ B \bmod 9) \in \{(1,7),(2,1),(4,4),(5,4),(7,1),(8,7)\},$$

which contradicts condition (4) of Theorem 3.1. Thus, $b = 1$ and $B = (A^2+3)/4$ from (3.17). Since $f(x)$ is monogenic, we deduce that B is squarefree, which completes the proof of (4).

The case $S_3 \times S_3$. Aside from B and Γ being squarefree, the main focus in Theorem 3.1 is on primes $p \in \{2,3\}$ for the monogenicity of $f(x)$. An examination of Theorem 3.1 reveals that

- condition (2) addresses $p = 2$ in the cases $A \bmod 4 \in \{0,2\}$ when $2 \,|\, A$, while $p = 3$ is handled in 12 separate cases when $3 \,|\, A$;
- condition (3) addresses $p = 3$ in exactly 8 separate cases;
- condition (4) addresses $p = 3$ in exactly 28 separate cases.

Certainly, $p = 2$ does not necessarily divide $\Delta(f)$, but $p = 3$ always divides $\Delta(f)$. Thus, we must also consider the third possibility for $p = 2$, that $2 \nmid A$, together with the possibilities for $p = 3$ found in Theorem 3.1. This analysis leads to a total of 3(12+8+28)=144 mutually exclusive cases. In each of these cases, an infinite 2-parameter family of monogenic trinomials $f(x)$ can be constructed, and with suitable additional restrictions if necessary, there exist infinitely many trinomials in each of these families with $\mathrm{Gal}(f) \simeq S_3 \times S_3$. We point out that such an approach could have been used for the other Galois groups, but it does not seem to lend itself so readily to yield single-parameter families.

Since the methods are similar in each of the 144 cases, we provide details in only two cases. The first case is

$$2 \nmid A \quad \text{and} \quad 3 \,|\, A \quad \text{with } (A \bmod 9,\ B \bmod 9) = (0,2). \tag{3.18}$$

By the Chinese Remainder Theorem, we have $A \equiv 9 \pmod{18}$, and so we can let $A = 18s + 9$, where s is an integer parameter. Letting $B = 9t + 2$, where t is an integer parameter, we then have

$$f(x) = x^6 + Ax^3 + B = x^6 + (18s+9)x^3 + 9t + 2, \tag{3.19}$$

with

$$\Gamma = \delta = A^2 - 4B = 324s^2 + 324s - 36t + 73$$

and

$$\Delta(f) = 3^6(9t+2)^2(324s^2+324s-36t+73)^3.$$

There exist infinitely many integers t such that $B = 9t+2$ is squarefree [26], and for each such value of t, there exist infinitely many integers s such that Γ is squarefree [25]. Let s and t be such integers with $\Gamma \neq 1$. Then $f(x)$ is irreducible over $\mathbb{Q}$ by Corollary 2.3, and is therefore monogenic by construction.

Since $3 \nmid (A^2-4B)$, we see that -3δ is not a square. If $B = 9t+2 = c^3$ for some $c \in \mathbb{Z}$, then $9t+2 = \pm 1$ since $9t+2$ is squarefree, which yields the contradiction that $t \in \{-1/3, -1/9\}$. Thus, $9t+2 \neq c^3$ for any $c \in \mathbb{Z}$. Finally, if $2 \nmid (9t+2)$, then $R(x)$ is irreducible in $\mathbb{F}_2[x]$, and if $2 \mid (9t+2)$, then $R(x)$ is 2-Eisenstein since B is squarefree. Hence, $R(x)$ is irreducible over $\mathbb{Q}$ and $\mathrm{Gal}(f) \simeq S_3 \times S_3$ by Theorem 2.1. We note that no additional restrictions on the parameters s and t are required in this case to achieve $\mathrm{Gal}(f) \simeq S_3 \times S_3$.

Thus, with $f(x)$ from (3.19), we have shown that

$$\mathcal{F}_6 := \{f(x) : B \text{ and } \Gamma \text{ are squarefree}\}$$

is the infinite set of all monogenic trinomials $f(x)$ satisfying (3.18) such that $\mathrm{Gal}(f) \simeq S_3 \times S_3$. Let

$$\widehat{\mathcal{F}_6} := \{f(x) \in \mathcal{F}_6 : A > 0 \text{ and } B = 2\}.$$

Observe that since

$$A = 18s+9 = 9(2s+1) > 0,$$

we have $A \geq 9$. We claim next that $f_1(x), f_2(x) \in \widehat{\mathcal{F}_6}$, where

$$f_1(x) = x^6 + A_1x^3 + 2 \quad \text{and} \quad f_2(x) = x^6 + A_2x^3 + 2 \in \widehat{\mathcal{F}_6},$$

with $A_1 \neq A_2$, are distinct. By way of contradiction, assume that $f_1(x)$ and $f_2(x)$ are not distinct. Then, by Corollary 2.6, we have $\Delta(f_1) = \Delta(f_2)$, or equivalently,

$$2^2 3^6 (A_1+A_2)(A_1-A_2)(A_2^4 + (A_1^2-24)A_2^2 + A_1^2(A_1^2-24)+192) = 0, \tag{3.20}$$

since

$$\Delta(f_i) = 2^2 3^6 (A_i^2-8)^3.$$

Since $A_i \geq 9$, it follows that

$$A_1 + A_2 > 0 \quad \text{and} \quad A_2^4 + (A_1^2-24)A_2^2 + A_1^2(A_1^2-24) + 192 > 0,$$

which yields the contradiction that $A_1 = A_2$ in (3.20). Thus, since there exist infinitely many positive integers A such that A^2-8 is squarefree [25], we have shown that $\mathcal{F}_6$ contains infinitely many distinct monogenic trinomials.

The second case we consider is

$$\begin{aligned} &2 \mid A \quad \text{and} \quad 3 \nmid AB \quad \text{with} \\ &(A \bmod 4,\, B \bmod 4) = (0,1), \qquad (A \bmod 9,\, B \bmod 9) = (1,1). \end{aligned} \tag{3.21}$$

Then, by the Chinese Remainder Theorem, we have

$$(A \bmod 36,\ B \bmod 36) = (28,1).$$

Hence, we can write

$$A = 36s + 28 \quad \text{and} \quad B = 36t + 1,$$

where s and t are integer parameters. Thus,

$$f(x) = x^6 + Ax^3 + B = x^6 + (36s+28)x^3 + 36t + 1 \tag{3.22}$$

and

$$\begin{aligned} A^2 - 4B &= (36s+28)^2 - 4(36t+1) \\ &= 1296s^2 + 2016s - 144t + 780 \\ &= 2^2 3(108s^2 + 168s - 12t + 65), \end{aligned}$$

where

$$\Gamma = 108s^2 + 168s - 12t + 65. \tag{3.23}$$

Therefore,

$$\begin{aligned} \Delta(f) &= 3^6 B^2 (A^2 - 4B)^3 \\ &= 3^6 (36t+1)^2 ((36s+28)^2 - 4(36t+1))^3 \\ &= 2^6 3^9 (36t+1)^2 \Gamma^3. \end{aligned}$$

There exist infinitely many integers t such that $36t+1$ is squarefree [26], and for each such value of t, there exist infinitely many integers s for which Γ is squarefree [25]. Let s and t be such integers. Since Γ is squarefree, then $A^2 - 4B$ is a square if and only if $\Gamma = 3$, which is impossible since $\Gamma \equiv 2 \pmod 3$ from (3.23). Thus, $g(x) = x^2 + Ax + B$ is irreducible over $\mathbb{Q}$, so that $f(x)$ is irreducible over $\mathbb{Q}$ by Corollary 2.3, and is therefore monogenic by construction.

If $-3\delta = -2^2 3^2 \Gamma$ is a square, then $\Gamma = -1$ since Γ is squarefree. Then, $\Gamma + 1 = 0$ and $4 \mid (\Gamma + 1)$. However, we see from (3.23) that $\Gamma + 1 \equiv 2 \pmod 4$, and this contradiction establishes the fact that -3δ is not a square. If $B = 36t+1 = c^3$ for some $c \in \mathbb{Z}$, then $36t+1 = \pm 1$ since B is squarefree. If $36t+1 = -1$, then $t = -1/18$, which is impossible. However, if $36t + 1 = 1$, then $t = 0$, and we must exclude the value $t = 0$ from the set of possible values of t. Finally, since $2 \nmid B$, then $R(x)$ is irreducible in $\mathbb{F}_2[x]$, and therefore $R(x)$ is irreducible over $\mathbb{Q}$. Hence, $\mathrm{Gal}(f) \simeq S_3 \times S_3$ by Theorem 2.1.

Thus, with $f(x)$ from (3.22), we have shown that

$$\mathcal{F}_7 := \{f(x) : t \neq 0;\ B \text{ and } \Gamma \text{ are squarefree}\}$$

is the infinite set of all monogenic trinomials $f(x)$ satisfying (3.21) such that $\mathrm{Gal}(f) \simeq S_3 \times S_3$. Let

$$\widehat{\mathcal{F}_7} := \{f(x) \in \mathcal{F}_7 : A > 0 \text{ and } B = 37\}.$$

Observe that since

$$A = 36s + 28 = 4(9s + 7) > 0,$$

we have $A \geq 28$. We claim next that $f_1(x), f_2(x) \in \widehat{\mathcal{F}_7}$, where

$$f_1(x) = x^6 + A_1x^3 + 37 \quad \text{and} \quad f_2(x) = x^6 + A_2x^3 + 37 \in \widehat{\mathcal{F}_7},$$

with $A_1 \neq A_2$, are distinct. By way of contradiction, assume that $f_1(x)$ and $f_2(x)$ are not distinct. Recall from (3.1) that

$$\Delta(f_i) = 3^6 37^2 (A_i^2 - 148)^3.$$

Then, by Corollary 2.6, we have $\Delta(f_1) = \Delta(f_2)$, or equivalently,

$$3^6 37^2 (A_1 + A_2)(A_1 - A_2)\Lambda = 0, \tag{3.24}$$

where

$$\Lambda = A_2^4 + (A_1^2 - 144)A_2^2 + A_1^2(A_1^2 - 144) + 65712.$$

Since $A_i \geq 28$, it follows that

$$A_1 + A_2 > 0 \quad \text{and} \quad \Lambda > 0,$$

which yields the contradiction that $A_1 = A_2$ in (3.24). Thus, since there exist infinitely many positive integers A such that $A^2 - 148$ is squarefree [25], we have shown that $\mathcal{F}_7$ contains infinitely many distinct monogenic trinomials, and the proof of the theorem is complete. ∎

Acknowledgements. The authors thank the anonymous referee for a thorough reading of the paper.

References

[1] C. Awtrey and P. Jakes, *Galois groups of even sextic polynomials*, Canad. Math. Bull. 63 (2020), 670–676.

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

[3] A. Booker and T. D. Browning, *Square-free values of reducible polynomials*, Discrete Anal. 2016, art. 8, 16 pp.

[4] A. Bremner and B. Spearman, *Cyclic sextic trinomials* $x^6 + Ax + B$, Int. J. Number Theory 6 (2010), 161–167.

[5] S. Brown, B. Spearman and Q. Yang, *On sextic trinomials with Galois group* C_6, S_3 *or* $C_3 \times S_3$, J. Algebra Appl. 12 (2013), art. 1250128, 9 pp.

[6] S. Brown, B. Spearman and Q. Yang, *On the Galois groups of sextic trinomials*, JP J. Algebra Number Theory Appl. 18 (2010), 67–77.

[7] G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra 11 (1983), 863–911.

[8] A. Cavallo, *An elementary computation of the Galois groups of symmetric sextic trinomials*, arXiv:1902.00965v2 (2021).
[9] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 2000.
[10] J. Harrington and L. Jones, *The irreducibility of power compositional sextic polynomials and their Galois groups*, Math. Scand. 120 (2017), 181–194.
[11] J. Harrington and L. Jones, *Monogenic quartic polynomials and their Galois groups*, Bull. Austral. Math. Soc. 111 (2025), 244–259.
[12] J. Harrington and L. Jones, *Monogenic trinomials of the form $x^4 + ax^3 + d$ and their Galois groups*, J. Algebra Appl. (online, 2026).
[13] A. Jakhar, S. Khanduja and N. Sangwan, *On prime divisors of the index of an algebraic integer*, J. Number Theory 166 (2016), 47–61.
[14] A. Jakhar, S. Khanduja and N. Sangwan, *Characterization of primes dividing the index of a trinomial*, Int. J. Number Theory 13 (2017), 2505–2514.
[15] S. Janson, *Resultant and discriminant of polynomials*, https://www2.math.uu.se/~svantejs/papers/sjN5.pdf.
[16] L. Jones, *Sextic reciprocal monogenic dihedral polynomials*, Ramanujan J. 56 (2021), 1099–1110.
[17] L. Jones, *Infinite families of reciprocal monogenic polynomials and their Galois groups*, New York J. Math. 27 (2021), 1465–1493.
[18] L. Jones, *Monogenic reciprocal trinomials and their Galois groups*, J. Algebra Appl. 21 (2022), art. 2250026, 11 pp.
[19] L. Jones, *Monogenic even quartic trinomials*, Bull. Austral. Math. Soc. 111 (2025), 238–243.
[20] L. Jones, *Monogenic cyclic trinomials of the form $x^4 + cx + d$*, Acta Arith. 218 (2025), 385–394.
[21] L. Jones, *Monogenic reciprocal quartic polynomials and their Galois groups*, arXiv: 2502.17691v1 (2025).
[22] L. Jones, *Monogenic even cyclic sextic polynomials*, Math. Slovaca 75 (2025), 1021–1034.
[23] L. Jones and D. White, *Monogenic trinomials with non-squarefree discriminant*, Internat. J. Math. 32 (2021), art. 2150089, 21 pp.
[24] Y. Motoda, T. Nakahara, A. S. I. Shah and T. Uehara, *On a problem of Hasse*, in: Algebraic Number Theory and Related Topics 2007, RIMS Kôkyûroku Bessatsu B12, Res. Inst. Math. Sci., Kyoto, 2009, 209–221.
[25] T. Nagel, *Zur Arithmetik der Polynome*, Abh. Math. Sem. Univ. Hamburg 1 (1922), 179–194.
[26] K. Prachar, *Über die kleinste quadratfreie Zahl einer arithmetischen Reihe*, Monatsh. Math. 62 (1958), 173–176.
[27] R. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. 12 (1962), 1099–1106.
[28] P. M. Voutier, *Families of cyclic quartic monogenic polynomials*, Acta Arith. 219 (2025), 365–377.

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

Lenny Jones
Professor Emeritus
Department of Mathematics
Shippensburg University
Shippensburg, PA 17257, USA
E-mail: doctorlennyjones@gmail.com