New York Journal of Mathematics

New York J. Math. **32** (2026) 1199–1216.

Characterizing monogenic trinomials $x^{12} + ax^6 + b$ according to their Galois groups

Lenny Jones

Abstract. Let $f(x) = x^{12} + ax^6 + b \in \mathbb{Z}[x]$, with $ab \neq 0$. We say that $f(x)$ is *monogenic* if $f(x)$ is irreducible over $\mathbb{Q}$ and $\{1, \theta, \theta^2, \ldots, \theta^{11}\}$ 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 give explicit descriptions of all monogenic trinomials $f(x)$ having Galois group G. These results extend recent work on monogenic power-compositional quartic and sextic trinomials.

Contents

1. Introduction

We say that a monic polynomial $F(x) \in \mathbb{Z}[x]$ is *monogenic* if $F(x)$ is irreducible over $\mathbb{Q}$ and $\{1, \theta, \theta^2, \ldots, \theta^{\deg(F)-1}\}$ is a basis for the ring of integers, $\mathbb{Z}_K$, of $K = \mathbb{Q}(\theta)$, where $F(\theta) = 0$. It is well known [9] that

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

where $\Delta(F)$ and $\Delta(K)$ denote the discriminants over $\mathbb{Q}$, respectively, of $F(x)$ and the number field K. We refer to $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ as the *index* of $F(x)$, and we denote it index(F). Thus, from (1.1),

$$F(x) \text{ is monogenic if and only if } \Delta(F) = \Delta(K), \text{ or equivalently, } \mathbb{Z}_K = \mathbb{Z}[\theta]. \tag{1.2}$$

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

ISSN 1076-9803/2026

Throughout this article, for $a, b \in \mathbb{Z}$ with $ab \neq 0$ and $j \in \{1, 2, 3\}$, we let

$$\begin{aligned} f(x) &:= x^{12} + ax^6 + b, \quad g_{2j}(x) := x^{2j} + ax^j + b, \\ r(x) &:= x^3 - 3bx + ab, \quad \alpha := a + 2\sqrt{b}, \quad \beta := a - 2\sqrt{b}, \\ \delta &:= a^2 - 4b, \quad \mathcal{W} := \delta / \gcd(2, a)^2. \end{aligned} \tag{1.3}$$

Observe that if $f(x)$ is irreducible over $\mathbb{Q}$, then the trinomials $g_{2j}(x)$ are irreducible over $\mathbb{Q}$ as well. Note also that $r(x)$ is a cubic resolvent for $g_6(x)$.

We use the notation 4Tn, 6Tn and 12Tn [6], to denote the possible Galois groups G_4, G_6 and Gal(f), for respectively, the trinomials $g_4(x)$, $g_6(x)$ and $f(x)$. These possible groups [26, 14, 8] are given in Table 1.

	n															
4Tn	1	2	3													
6Tn	1	2	3	5	9											
12Tn	2	3	10	11	12	13	14	15	16	18	28	37	38	39	42	81

TABLE 1. Possible Galois groups for $g_4(x)$, $g_6(x)$ and $f(x)$

For integers r and N, with $N > 1$, we let the notation "$r \bmod N$" denote the unique integer $z \in \{0, 1, 2, \ldots, N-1\}$ such that $r \equiv z \pmod N$. That is, $r \bmod N = z$.

In this article, we provide a complete characterization of the monogenic trinomials $f(x)$ according to Gal$(f) \simeq$ 12Tn for each value of n given in Table 1. More precisely, we prove the following:

Theorem 1.1. *Suppose that $f(x)$ is irreducible over $\mathbb{Q}$, so that* Gal$(f) \simeq$ 12Tn, *for some n in Table 1. If $n \in \{3, 11, 12, 13, 14, 15, 16, 18, 37\}$, then $f(x)$ is not monogenic. If $n \in \{2, 10, 28, 38, 39, 42, 81\}$, then $f(x)$ is monogenic with* Gal$(f) \simeq$

(1) 12T2 *if and only if $f(x) = x^{12} - x^6 + 1$;*

(2) 12T10 *if and only if $f(x) = x^{12} + ax^6 + 1$, where a satisfies the conditions*

$$\mathcal{C}_{10} := \{a \neq -1,\ a \bmod 4 \in \{0, 3\},\ a \bmod 9 \neq 0,\ \mathcal{W} \text{ is squarefree}\};$$

(3) 12T28 *if and only if either $f(x) \in \{x^{12} + 2x^6 + 2,\ x^{12} - 2x^6 + 2\}$ or $f(x) = x^{12} + ax^6 - 1$, where a satisfies the conditions*

$$\mathcal{C}_{28} := \{a \bmod 4 \neq 0,\ a \bmod 9 \notin \{0, 4, 5\},\ \mathcal{W} \text{ is squarefree}\};$$

(4) 12T38 *if and only if*

$$f(x) \in \{x^{12} \pm 4x^6 - 2,\ x^{12} \pm 4x^6 + 6\}$$

or $f(x) = x^{12} + ax^6 - 3$, where a satisfies the conditions

$$\mathcal{C}_{38} := \{a \bmod 4 \in \{0, 3\},\ a \bmod 9 \notin \{2, 7\},\ \mathcal{W} \text{ is squarefree}\};$$

(5) 12T39 *if and only if $f(x) \in \{x^{12} \pm 4x^6 + 2,\ x^{12} - 5x^6 + 5\}$.*

(6) 12T42 *if and only if* $f(x)=x^{12}+ax^6+(a^2+3)/4$, *where a satisfies the conditions*

$$\mathcal{C}_{42} := \{a \bmod 8 \in \{3,5,7\},\ a \neq -1,\ (a^2+3)/4 \textit{ is squarefree}\};$$

(7) 12T81 *if and only if a and b satisfy the conditions*

$$\begin{aligned}\mathcal{C}_{81} := \{&b \textit{ and } \mathcal{W} \textit{ are squarefree with } b \textit{ not a cube},\\ &-3b,\ -3b\delta \textit{ and } b\delta \textit{ are not squares}\},\end{aligned}$$

such that $(a \bmod 4,\ b \bmod 4) \in \mathcal{R}$ *and* $(a \bmod 9,\ b \bmod 9) \in \mathcal{S}$, *where*

$$\mathcal{R} = \{(0,1),(0,2),(2,2),(2,3),(1,3),(3,2),(3,1),(3,3)\} \textit{ and}$$

$$\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3 \cup \mathcal{S}_4, \textit{ with } \mathcal{S}_1 = \{(0,3),(0,6),(3,3),(3,6),(6,3),(6,6)\},$$

$$\begin{aligned}\mathcal{S}_2 = \{&(0,2),(0,4),(0,5),(0,7),(3,1),(3,4),\\ &(3,7),(3,8),(6,1),(6,4),(6,7),(6,8)\},\end{aligned}$$

$$\mathcal{S}_3 = \{(1,3),(1,6),(2,3),(4,6),(5,6),(7,3),(8,3),(8,6)\}$$

and

$$\begin{aligned}\mathcal{S}_4 = \{&(1,1),(1,2),(1,4),(1,5),(1,8),(2,2),(2,4),(2,5),(2,7),(2,8),\\ &(4,1),(4,2),(4,5),(4,7),(5,1),(5,2),(5,5),(5,7),(7,2),(7,4),\\ &(7,5),(7,7),(7,8),(8,1),(8,2),(8,4),(8,5),(8,8)\}.\end{aligned}$$

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, 3, 13, 11, 14, 12, 15, 20, 18, 19, 21, 17, 25, 22, 23, 24, 28, 5, 4, 30].

The proof of Theorem 1.1 entails two main steps: the characterization of the Galois groups of $f(x)$, and an investigation of the monogenicity of $f(x)$. Typically, the monogenicity of $f(x)$ would be determined using either Dedekind's Index Criterion [9] or an algorithmic version of Dedekind's theorem that has been engineered specifically for trinomials, due to Jakhar, Khanduja and Sangwan [16]. Each of these methods gives necessary and sufficient conditions to decide when a prime divisor of the discriminant $\Delta(f)$ divides the index(f). Both steps in this procedure can be lengthy and computationally tedious. However, we are able to streamline this process here in the following ways. First, Chen [8] has provided a characterization of the Galois groups of $f(x)$ in terms of the Galois groups G_4 and G_6 of respectively, $g_4(x)$ [26] and $g_6(x)$ [7, 10], along with some additional restrictions on the coefficients a and b of $f(x)$. Second, a recent theorem due to Kaur, Kumar and Remete [27], designed specifically for determining the monogenicity of power-compositional polynomials, allows us to utilize the characterizations of the monogenic trinomials $g_{2j}(x)$. Some, but not all, of these characterizations have already been established. The characterization of the monogenic trinomials $g_6(x)$ has been given recently in [14]. However, only a partial characterization of the monogenic trinomials $g_4(x)$ has been given in [11, 20], and so we complete this characterization here. For the sake of completeness, we also provide the characterization of the monogenic trinomials $g_2(x)$. In many cases, the possibilities for monogenic trinomials $f(x)$ are narrowed down considerably during this stage. Finally, we check the monogenicity of the trinomials $f(x)$ that have survived up to this point, and we use a special case of the theorem of Jakhar, Khanduja and Sangwan [16] tailored for our specific situation to accomplish this task. Another component of the theorem of Kaur, Kumar and Remete also helps to expedite the entire process by allowing us to focus solely on the primes $q \in \{2, 3\}$ when invoking the tailor-made version of the theorem of Jakhar, Khanduja and Sangwan.

2. Preliminaries

Let $m \geq 1$ be an integer, and let $\mathfrak{F}(x) = x^{2m} + Ax^m + B \in \mathbb{Z}[x]$. Then, from a theorem due to Swan [29], we have that

$$\Delta(\mathfrak{F}) = B^{m-1}m^{2m}(A^2 - 4B)^m. \tag{2.1}$$

Note that since $\Delta(g_2) = a^2 - 4b = \delta$, we have from (2.1), that

$$\Delta(g_4) = 2^4\delta^2 b, \quad \Delta(g_6) = 3^6\delta^3 b^2 \quad \text{and } \Delta(f) = 2^{12}3^{12}\delta^6 b^5.$$

The following theorem is a special case of a theorem due to Jakhar, Khanduja and Sangwan [16] that will be used to determine the monogenicity of $f(x)$.

Theorem 2.1. *Let $m \geq 1$ be an integer, and let $\mathfrak{F}(x) = x^{2m} + Ax^m + B \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Q}$. Let $\mathbb{Z}_K$ denote the ring of integers of $K = \mathbb{Q}(\theta)$, where $\mathfrak{F}(\theta) = 0$. A prime factor q of $\Delta(\mathfrak{F})$ does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if q satisfies one of the following conditions:*

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

(2) when $q \mid A$ and $q \nmid B$, then

$$\text{either} \quad q \mid a_2 \text{ and } q \nmid b_1 \quad \text{or} \quad q \nmid a_2\left(a_2^2 B + b_1^2\right),$$

where $a_2 = A/q$ and $b_1 = \frac{B+(-B)^{q^j}}{q}$, such that $q^j \mid\mid 2m$ with $j \geq 1$;

(3) when $q \nmid A$ and $q \mid B$, then

$$\text{either} \quad q \mid a_1 \text{ and } q \nmid b_2 \quad \text{or} \quad q \nmid a_1 b_2^{m-1}\left(Aa_1 - b_2\right),$$

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

(4) when $q \nmid AB$ and $q \mid m$ with $m = sq^k$, $q \nmid s$, then the polynomials

$$H_1(x) := x^{2s} + Ax^s + B \quad \text{and} \quad H_2(x) := \frac{Ax^{sq^k} + B + \left(-Ax^s - B\right)^{q^k}}{q}$$

are coprime in $\mathbb{F}_q[x]$;

(5) when $q \nmid ABm$, then $q^2 \nmid \left(A^2 - 4B\right)$.

We now use Theorem 2.1 to present a complete description of the monogenic trinomials $g_2(x)$. Of course, in this situation, we have that $\mathrm{Gal}(g_2) \simeq 2T1$, the cyclic group of order 2, for all irreducible trinomials $g_2(x)$.

Theorem 2.2. *The trinomial $g_2(x)$ is monogenic if and only if $\mathcal{W}$ is squarefree and*

$$(a \bmod 4,\ b \bmod 4) \in \{(0,1),(0,2),(2,2),(2,3)\} \quad \textit{if } 2 \mid a.$$

Proof. Let q be a prime divisor of $\Delta(g_2) = a^2 - 4b = \delta$. Observe that conditions (3) and (4) of Theorem 2.1 are not possible. Suppose first that $2 \nmid a$, so that $q \geq 3$ and $\mathcal{W} = \delta$. Note then that condition (2) of Theorem 2.1 is not applicable since $q \geq 3$. Finally, we see that conditions (1) and (5) of Theorem 2.1 are satisfied if and only if $\mathcal{W}$ is squarefree. Suppose next that $2 \mid a$, and let $q = 2$. If $2 \mid a$ and $2 \mid b$, then condition (1) is satisfied if and only if

$$(a \bmod 4,\ b \bmod 4) \in \{(0,2),(2,2)\}.$$

Suppose then that $2 \mid a$ and $2 \nmid b$. Then, we have from condition (2) of Theorem 2.1 that $j = 1$, and

$$b_1 = (b + b^2)/2 \equiv \begin{cases} 1 \pmod 2 & \text{if } b \equiv 1 \pmod 4, \\ 0 \pmod 2 & \text{if } b \equiv 3 \pmod 4. \end{cases}$$

If $2 \mid a_2$, then $2 \nmid \operatorname{index}(g_2)$ if and only if $b \equiv 1 \pmod 4$. That is, in this case we have $(a \bmod 4,\ b \bmod 4) = (0,1)$. If $2 \nmid a_2$, then

$$a_2^2 b + b_1^2 \equiv \begin{cases} 0 \pmod 2 & \text{if } b \equiv 1 \pmod 4, \\ 1 \pmod 2 & \text{if } b \equiv 3 \pmod 4. \end{cases}$$

Thus, in this case, $2 \nmid \operatorname{index}(g_2)$ if and only if $b \equiv 3 \pmod 4$. Consequently, $(a \bmod 4,\ b \bmod 4) = (2,3)$. Finally, as in the case when $2 \nmid a$, we deduce from conditions (1) and (5) of Theorem 2.1 that $q \nmid \operatorname{index}(g_2)$ if and only if $\mathcal{W}$ is squarefree when $q \geq 3$. □

The next theorem targets power-compositional situations and is due to Kaur, Kumar and Remete [27].

Theorem 2.3. *Let $\mathfrak{g}(x)$ be a monic polynomial with integer coefficients. Let $k \geq 2$ be an integer such that $\mathfrak{f}(x) := \mathfrak{g}(x^k)$ is irreducible over $\mathbb{Q}$. Then $\mathfrak{f}(x)$ is monogenic if and only if all of the following conditions are satisfied:*

(1) $\mathfrak{g}(0)$ is squarefree,
(2) q does not divide the index of $\mathfrak{f}(x)$ for all primes $q \mid k$,
(3) $\mathfrak{g}(x)$ is monogenic.

We then have the following immediate corollary of Theorem 2.3.

Corollary 2.4. *Suppose that $\mathfrak{F}(x) = x^{2m} + Ax^m + B \in \mathbb{Z}[x]$ is monogenic, where $AB \neq 0$ and $m \geq 2$. Then B and $(A^2 - 4B)/\gcd(2, A)^2$ are squarefree. Moreover, $\mathfrak{F}_d(x) := x^{2d} + Ax^d + B$ is monogenic for every divisor $d \geq 1$ of m.*

The special cases $m \in \{2, 3, 6\}$ of Corollary 2.4 will be useful to us in this article.

We turn now to $g_4(x)$. The following theorem follows from [26], and gives the characterization of the possible Galois groups G_4 of $g_4(x)$, using the notation 4Tn [6], in terms of conditions on the coefficients a and b.

Theorem 2.5. *If $g_4(x)$ is irreducible over $\mathbb{Q}$, then $G_4 \simeq$*

(1) 4T1 *if and only if $b\delta$ is a square,*
(2) 4T2 *if and only if b is a square,*
(3) 4T3 *if and only if neither b nor $b\delta$ is a square.*

The complete characterization of the 4T1-monogenic trinomials $g_4(x)$ and a partial characterization of the 4T3-monogenic trinomials $g_4(x)$ were given in [20], while a partial characterization of the 4T2-monogenic trinomials $g_4(x)$ was given in [11]. By completing the characterizations for the cases 4T2 and 4T3, we present in the following theorem the comprehensive characterization of the monogenic trinomials $g_4(x)$, according to their Galois groups.

Theorem 2.6. *Suppose that $g_4(x)$ is irreducible over $\mathbb{Q}$. Then $g_4(x)$ is monogenic with $G_4 \simeq$*

(1) 4T1 *if and only if $g_4(x) \in \{x^4 \pm 4x^2 + 2,\ x^4 - 5x^2 + 5\}$;*
(2) 4T2 *if and only if $\mathcal{W}$ is squarefree and*

$$g_4(x) \in \mathcal{F}_0 = \{x^4 + ax^2 + 1 : a \bmod 4 \in \{0, 3\}\};$$

(3) 4T3 *if and only if $\mathcal{W}$ and $b \neq 1$ are squarefree, $b\delta$ is not a square and*

$$g_4(x) \in \mathcal{F}_1 = \{x^4 + ax^2 + b : (a \bmod 4,\ b \bmod 4) \in \mathcal{R}\},$$

where $\mathcal{R} = \{(0,1), (0,2), (2,2), (2,3), (1,3), (3,2), (3,1), (3,3)\}$.

Proof. The proof of item (1) can be found in [20].

For item (2), suppose that $G_4 \simeq$ 4T2. If $g_4(x)$ is monogenic, it follows from Corollary 2.4 that $g_2(x)$ is monogenic, and both b and $\mathcal{W}$ are squarefree. Since $g_2(x)$ is monogenic, we see from Theorem 2.2 that

$$(a \bmod 4,\ b \bmod 4) \in \{(0,1), (0,2), (2,2), (2,3)\} \quad \text{if } 2 \mid a. \tag{2.2}$$

From Theorem 2.5 we have that b is a square, while from Theorem 2.3, we have that $g_2(0) = b$ is squarefree. Hence, $b = 1$. Thus, if $2 \mid a$, we conclude from (2.2) that $a \equiv 0 \pmod 4$. So, suppose that $2 \nmid a$. From Theorem 2.3, we only have to check divisibility of the index(g_4) by $q = 2$. Since $g_4(x)$ is monogenic, we have by condition (4) of Theorem 2.1 with $\mathfrak{F}(x) = g_4(x)$ and $q = 2$, that

$$H_1(x) = x^2 + ax + 1 \text{ and } H_2(x) = \frac{ax^2 + 1 + (-ax - 1)^2}{2} = \left(\frac{a^2 + a}{2}\right)x^2 + ax + 1$$

are coprime in $\mathbb{F}_2[x]$. Since $2 \nmid a$, $H_1(x)$ is irreducible in $\mathbb{F}_2[x]$, which implies that $a \equiv 3 \pmod 4$.

Conversely, suppose that $g_4(x) \in \mathcal{F}_0$, where $\mathcal{W}$ is squarefree. Then $g_2(x)$ is monogenic from Theorem 2.2, and we deduce that $g_4(x)$ is monogenic from Theorem 2.3.

For item (3), suppose that $G_4 \simeq$ 4T3. If $g_4(x)$ is monogenic, then we have that b and $\mathcal{W}$ are both squarefree, and $g_2(x)$ is monogenic, from Corollary 2.4. From Theorem 2.5, we have that $b\delta$ and b are not squares, so that $b \neq 1$. Moreover, we have from Theorem 2.2 that conditions (2.2) hold. Suppose then that $2 \nmid a$. From condition (4) of Theorem 2.1 with $q=2$, we get that

$$\begin{aligned} H_1(x) &= x^2+ax+b \ \text{ and} \\ H_2(x) &= \frac{ax^2+b+(-ax-b)^2}{2} = \left(\frac{a^2+a}{2}\right)x^2+abx+\frac{b^2+b}{2} \end{aligned} \tag{2.3}$$

are coprime in $\mathbb{F}_2[x]$. If $2 \mid b$, then $b \equiv 2 \pmod 4$ since b is squarefree. Then

$$H_1(x) \equiv x(x+a) \pmod 2 \quad \text{and} \quad H_2(x) \equiv \left(\frac{a^2+a}{2}\right)x^2+1 \pmod 2$$

from (2.3), which implies that $a \equiv 3 \pmod 4$. If $2 \nmid b$, then we have from (2.3) that $H_1(x) \equiv x^2+x+1 \pmod 2$ is irreducible in $\mathbb{F}_2[x]$. Thus, the only way that $H_1(x)$ and $H_2(x)$ would not be coprime in $\mathbb{F}_2[x]$ is if $H_2(x) \equiv H_1(x) \pmod 2$, which implies that $(a \bmod 4,\ b \bmod 4)=(1,1)$. Hence, we must have

$$(a \bmod 4,\ b \bmod 4) \in \{(1,3),(3,1),(3,3)\}.$$

The converse is similar to the previous case 4T2, and we omit the details. □

We turn next to $g_6(x)$. The characterization of the monogenic trinomials $g_6(x)$ according to their Galois groups is given below [14].

Theorem 2.7. *If $g_6(x)$ is irreducible over $\mathbb{Q}$, then $g_6(x)$ is monogenic with $G_6 \simeq$*

(1) 6T1 *if and only if* $g_6(x) \in \{x^6-x^3+1,\ x^6+x^3+1\}$*;*
(2) 6T2 *never occurs;*
(3) 6T3 *if and only if* $g_6(x) \in \mathcal{F}_i$ *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) 6T5 *if and only if* $g_6(x) \in \mathcal{F}_5$*, where*

$$\mathcal{F}_5 := \{x^6+ax^3+(a^2+3)/4 : a \bmod 2 = 1,\ a \neq \pm 1, \text{ with } (a^2+3)/4 \text{ squarefree}\};$$

(5) 6T9 *if and only if* $g_6(x)$ *is contained in one of* 144 *infinite pairwise-disjoint 2-parameter monogenic families, where* -3δ *is not a square,* $r(x)$ *is irreducible and* $b \neq c^3$ *for any* $c \in \mathbb{Z}$*.*

Let P, Q, R and S denote the following statements:

$$\begin{aligned} P:&\quad -3b\delta \text{ is a square,}\\ Q:&\quad -3b \text{ is a square,}\\ R:&\quad r(x) \text{ is reducible,}\\ S:&\quad b \text{ is a cube.} \end{aligned} \tag{2.4}$$

Making use of (2.4), the next theorem uses the possible pairs (G_4, G_6) and conditions on the coefficients a and b of $f(x)$ to determine $\mathrm{Gal}(f)$.

Theorem 2.8. [8] *Recall the definitions as given in* (1.3) *and* (2.4)*. The pairs* $(G_4, G_6) \in \{(4T1, 6T1), (4T1, 6T2), (4T1, 6T5)\}$ *are not possible. Table 2 indicates how the pair* (G_4, G_6) *determines the possibilities for* $\mathrm{Gal}(f)$.

(G_4, G_6)	$\mathrm{Gal}(f)$		
(4T1, 6T3)	12T11		
(4T1, 6T9)	12T39		
(4T2, 6T1)	12T2		
(4T2, 6T2)	12T3		
(4T2, 6T5)	12T18		
(4T2, 6T3)	12T3 *if* 3α *or* 3β *is a square*	12T10 *otherwise*	
(4T2, 6T9)	12T16 *if* 3α *or* 3β *is a square*	12T37 *otherwise*	
(4T3, 6T1)	12T14		
(4T3, 6T2)	12T15		
(4T3, 6T5)	12T42		
(4T3, 6T3)	12T12 *if* P *and* R *are true or* Q *and* S *are true*	12T13 *if* Q *and* R *are true or* P *and* S *are true*	12T28 *otherwise*
(4T3, 6T9)	12T38 *if* $-3b$ *or* $-3b\delta$ *is a square*	12T81 *otherwise*	

TABLE 2. $\mathrm{Gal}(f)$ from possible pairs (G_4, G_6)

3. Proof of Theorem 1.1

Proof. For each possible pair (G_4, G_6) yielding 12Tn from Theorem 2.8, we use Theorem 2.6, Theorem 2.7 and Theorem 2.3 to determine the 12Tn-monogenic trinomials $f(x)$. More precisely, if $f(x) = x^{12} + ax^6 + b$ with $\mathrm{Gal}(f) \simeq 12\mathrm{T}n$, which arises from (G_4, G_6) in Theorem 2.8, then it follows from Theorem 2.3 that $f(x)$ is monogenic if and only if both $g_4(x)$ and $g_6(x)$ are monogenic, b is squarefree and $\gcd(\mathrm{index}(f), 6) = 1$. Consequently, we need to determine the pairs (a, b) that occur for both $g_4(x)$ and $g_6(x)$ in, respectively, Theorem 2.6 and Theorem 2.7 for the specific pair (G_4, G_6). Recall, from Corollary 2.4, that b and $\mathcal{W}$ are squarefree for every possible monogenic $g_4(x)$ and $g_6(x)$. Therefore, once we have determined the viable monogenic candidates $f(x)$ from this process, we only need to check that $\gcd(\mathrm{index}(f), 6) = 1$, and we can do so using Theorem 2.1. One important item that follows from Theorem 2.3 is that if both $g_4(x)$ and $g_6(x)$ are known to be monogenic, then we can determine the monogenicity of $f(x)$ by examining either $q = 2$ (since $f(x) = g_6(x^2)$) or $q = 3$ (since $f(x) = g_4(x^3)$) in Theorem 2.1. That is, Theorem 2.3 does not require the examination of both $q = 2$ and $q = 3$ in Theorem 2.1 to determine the monogenicity of $f(x)$. Therefore, we can choose to examine $q = 2$ or $q = 3$, depending on which situation requires fewer calculations.

The Case 12T2. If $\mathrm{Gal}(f) \simeq 12\mathrm{T}2$, then we have from Theorem 2.8 that $(G_4, G_6) = (4\mathrm{T}2, 6\mathrm{T}1)$. Observe that $(a, b) = (-1, 1)$ is the only pair for which $g_4(x)$ and $g_6(x)$ are both monogenic with the appropriate (G_4, G_6) from Theorem 2.6 and Theorem 2.7. Thus, $f(x) = x^{12} - x^6 + 1 = \Phi_{36}(x)$ (the cyclotomic polynomial of index 36), which is well known to be monogenic [31], is the only monogenic trinomial $f(x)$ with $\mathrm{Gal}(f) \simeq 12\mathrm{T}2$. Knowing that $f(x) = \Phi_{36}(x)$ is irreducible, we can verify independently the fact that $f(x) = g_6(x^2)$ is monogenic by appealing to Theorem 2.3 and examining condition (4) of Theorem 2.1 with $q = 2$. We get

$$H_1(x) = x^6 - x^3 + 1 \equiv x^6 + x^3 + 1 \pmod 2 \quad \text{and}$$

$$H_2(x) = \frac{-x^6 + 1 + (x^3 - 1)^2}{2} \equiv (x + 1)(x^2 + x + 1) \pmod 2,$$

from which it is easily seen that $H_1(x)$ and $H_2(x)$ are coprime in $\mathcal{F}_2[x]$. It follows that $2 \nmid \mathrm{index}(f)$, and we conclude that $f(x)$ is monogenic by Theorem 2.3.

The Case 12T3. If $\mathrm{Gal}(f) \simeq 12\mathrm{T}3$, then we see from Theorem 2.8 that there are two possibilities in this case. However, the possibility $(G_4, G_6) = (4\mathrm{T}2, 6\mathrm{T}2)$ cannot yield any monogenic trinomials $f(x)$ since there are no 6T2-monogenic trinomials $g_6(x)$ by Theorem 2.7. So, suppose that $(G_4, G_6) = (4\mathrm{T}2, 6\mathrm{T}3)$, where

$$3\alpha \quad \text{or} \quad 3\beta \quad \text{is a square.} \tag{3.1}$$

If $f(x)$ is monogenic, then, since $g_4(x)$ must be monogenic by Theorem 2.3, we see from Theorem 2.6 that $b = 1$. Hence,

$$3\alpha = 3(a + 2) \quad \text{and} \quad 3\beta = 3(a - 2). \tag{3.2}$$

Furthermore, since $b = 1$, and $g_6(x)$ must be monogenic by Theorem 2.3, we see from Theorem 2.7 that $g_6(x) \in \mathcal{F}_3$ with both $a + 2$ and $a - 2$ squarefree.

It follows from (3.1) and (3.2) that $a \in \{1, 5\}$, which contradicts the fact that $a \bmod 4 \in \{0, 3\}$ by Theorem 2.6. Thus, there are no 12T3-monogenic trinomials $f(x)$.

The Case 12T10. Suppose that $\mathrm{Gal}(f) \simeq$ 12T10. Then we have from Theorem 2.8 that $(G_4, G_6) = (\text{4T2}, \text{6T3})$, such that neither 3α nor 3β is a square.

Suppose that $f(x)$ is monogenic. We see from the analysis given in Case 12T3 that $b = 1$, $a \notin \{1, 5\}$ and $a \bmod 4 \in \{0, 3\}$. Furthermore, by Theorem 2.7, we have that $a \neq \pm 1$ and $a \bmod 9 \neq 0$, with $a+2$ and $a-2$ both squarefree, which is equivalent to $\mathcal{W}$ being squarefree. Thus, $f(x)$ satisfies conditions $\mathcal{C}_{10}$.

Conversely, suppose that $f(x) = x^{12} + ax^6 + 1$ satisfies conditions $\mathcal{C}_{10}$. Then, from Theorem 2.7, we see that $g_6(x)$ is monogenic. Since $f(x) = g_6(x^2)$, it follows from Theorem 2.3 that we can determine the monogenicity of $f(x)$ by examining the prime $q = 2$ in Theorem 2.1. If $2 \mid a$, then $4 \mid a$ from conditions $\mathcal{C}_{10}$, and in this case we see that $q = 2$ satisfies condition (2) of Theorem 2.1 since $2 \mid a_2$ and $b_1 = 1$. Thus, $2 \nmid \mathrm{index}(f)$ and $f(x)$ is monogenic. If $2 \nmid a$, then we must examine condition (4) of Theorem 2.1. Note that $a \bmod 4 = 3$ from conditions $\mathcal{C}_{10}$. We get

$$H_1(x) = x^6 + ax^3 + 1 \equiv x^6 + x^3 + 1 \pmod 2,$$

which is irreducible in $\mathbb{F}_2[x]$, and

$$\begin{aligned} H_2(x) &= \frac{ax^6 + 1 + (-ax^3 - 1)^2}{2} \\ &= \left(\frac{a^2 + a}{2}\right) x^6 + ax^3 + 1 \\ &\equiv (x+1)(x^2 + x + 1) \pmod 2. \end{aligned}$$

It is then easy to see that $H_1(x)$ and $H_2(x)$ are coprime in $\mathbb{F}_2[x]$, so that $2 \nmid \mathrm{index}(f)$ by Theorem 2.1, and $f(x)$ is monogenic.

The Case 12T11. We see from Theorem 2.8 that $(G_4, G_6) = (\text{4T1}, \text{6T3})$. By inspection of Theorem 2.6 and Theorem 2.7, we conclude that there do not exist any monogenic trinomials $f(x)$ with $\mathrm{Gal}(f) \simeq$ 12T11.

The Case 12T12. Suppose that $\mathrm{Gal}(f) \simeq$ 12T12. Then, from Theorem 2.8, we have that $(G_4, G_6) = (\text{4T3}, \text{6T3})$, such that either $-3b\delta$ is a square and $r(x)$ is reducible, or $-3b$ is a square and b is a cube.

Suppose that $f(x)$ is monogenic. Then, from Corollary 2.4, we have that b and $\mathcal{W}$ are squarefree, and $g_2(x)$, $g_4(x)$ and $g_6(x)$ are all monogenic.

Assume first that $-3b\delta$ is a square and $r(x)$ is reducible over $\mathbb{Q}$. Then $3 \mid\mid b\delta$, and $-b(a^2 - 4b)/3$ is a square. Suppose that $2 \nmid a$. If $3 \mid b$, then since $b/3$ and $a^2 - 4b$ are squarefree, it follows that $-b/3 = a^2 - 4b$, or equivalently, $a^2 = 11b/3$. Hence, $(a, b) \in \{(\pm 11, 33)\}$, which contradicts Theorem 2.7. If $3 \mid \delta$, then $-b = \delta/3$, or equivalently, $a^2 = b$. Thus, $(a, b) \in \{(\pm 1, 1)\}$. It is easy to see that the pair $(a,b)=(1,1)$ contradicts Theorem 2.6, while a straightforward check reveals that the pair $(a,b)=(-1,1)$ yields the monogenic trinomial $f(x)=x^{12}-x^6+1$. However, in this case,

$$r(x)=x^3-3bx+ab=x^3-3x-1$$

is irreducible over $\mathbb{Q}$, which contradicts the fact that $\mathrm{Gal}(f)\simeq 12\mathrm{T}12$. (Indeed, we have already shown that $\mathrm{Gal}(f)\simeq 12\mathrm{T}2$ in this case.) Suppose then that $2\mid a$. If $3\mid b$, then $(-b/3)((a/2)^2-b)$ is a square. Since $-b/3$ and $(a/2)^2-b$ are squarfree, we have that $-b/3=(a/2)^2-b$, or equivalently, $(a/2)^2=2(b/3)$. Therefore, $(a,b)\in\{(\pm 4,6)\}$, which contradicts Theorem 2.7. If $3\mid\delta$, then $-b=((a/2)^2-b)/3$, or equivalently, $(a/2)^2=-2b$. Hence, $(a,b)\in\{(\pm 4,-2)\}$, which again contradicts Theorem 2.7.

Assume next that $-3b$ is a square and b is a cube. Since b is squarefree and b is a cube, we have that $b=\pm 1$, which contradicts the fact that $-3b$ is a square. Hence, this final contradiction confirms that there do not exist any monogenic trinomials $f(x)$ with $\mathrm{Gal}(f)\simeq 12\mathrm{T}12$.

The Case 12T13. Suppose that $\mathrm{Gal}(f)\simeq 12\mathrm{T}13$. From Theorem 2.8, we have that $(G_4,G_6)=(4\mathrm{T}3,6\mathrm{T}3)$, such that either $-3b$ is a square and $r(x)$ is reducible, or $-3b\delta$ is a square and b is a cube.

Suppose that $f(x)$ is monogenic. From Corollary 2.4, we have that $g_2(x)$, $g_4(x)$ and $g_6(x)$ are all monogenic, with b and $\mathcal{W}$ squarefree.

Assume first that $-3b$ is a square and $r(x)$ is reducible over $\mathbb{Q}$. Since b is squarefree, it follows that $b=-3$, which contradicts Theorem 2.7.

Assume next that $-3b\delta$ is a square and b is a cube. The same arguments used in the case 12T12 yield a contradiction in every possible situation, and we omit the details. Thus, there exist no 12T13-monogenic trinomials $f(x)$.

The Case 12T14. Suppose that $\mathrm{Gal}(f)\simeq 12\mathrm{T}14$. From Theorem 2.8, we have that $(G_4,G_6)=(4\mathrm{T}3,6\mathrm{T}1)$. By inspection, we deduce from Theorem 2.6 and Theorem 2.7 that $(a,b)=(-1,1)$, so that $f(x)=x^{12}-x+1$. However, we have already shown that $\mathrm{Gal}(f)=12\mathrm{T}2$. Hence, there are no monogenic trinomials $f(x)$ in this case.

The Case 12T15. Suppose that $\mathrm{Gal}(f)\simeq 12\mathrm{T}15$. From Theorem 2.8, we have that $(G_4,G_6)=(4\mathrm{T}3,6\mathrm{T}2)$. However, there are no 6T2-monogenic trinomials $g_6(x)$ by Theorem 2.7, and therefore, there are no 12T15-monogenic trinomials $f(x)$ by Theorem 2.3.

The Case 12T16. Suppose that $\mathrm{Gal}(f)\simeq 12\mathrm{T}16$. From Theorem 2.8, we have that $(G_4,G_6)=(4\mathrm{T}2,6\mathrm{T}9)$, such that either 3α or 3β is a square.

If $f(x)$ is monogenic, $g_4(x)$ is monogenic by Corollary 2.4. Then, from Theorem 2.6, we have that $a \bmod 4\in\{0,3\}$ and $b=1$. Hence,

$$3\alpha \bmod 4=3(a+2)\bmod 4\in\{2,3\}\quad\text{and}\quad 3\beta \bmod 4=3(a-2)\bmod 4\in\{2,3\},$$

so that neither 3α nor 3β is a square. This contradiction shows that no 12T16-monogenic trinomials $f(x)$ exist.

The Case 12T18. Suppose that $\mathrm{Gal}(f) \simeq 12\mathrm{T}18$. From Theorem 2.8, we have that $(G_4, G_6) = (4\mathrm{T}2, 6\mathrm{T}5)$.

If $f(x)$ is monogenic, then $g_4(x)$ and $g_6(x)$ are monogenic by Corollary 2.4. Hence, $b = 1 = (a^2+3)/4$ from Theorems 2.6 and 2.7. Thus, $a = \pm 1$, which contradicts Theorem 2.7. Hence, there exist no 12T18-monogenic trinomials $f(x)$.

The Case 12T28. From Theorem 2.8, we have that $(G_4, G_6) = (4\mathrm{T}3, 6\mathrm{T}3)$. Furthermore, to ensure that $\mathrm{Gal}(f) \simeq 12\mathrm{T}28$, we must have from Theorem 2.8 that the negation of the statement

$$Y := [(P \wedge R) \vee (Q \wedge S)] \vee [(Q \wedge R) \vee (P \wedge S)]$$

is true, where P, Q, R and S are the statements as given in (2.4). The seven possibilities for the truth values of the statements P, Q, R and S for which $\neg Y$ is true are given in Table 3.

P	T	T	F	F	F	F	F
Q	T	F	T	F	F	F	F
R	F	F	F	T	T	F	F
S	F	F	F	T	F	T	F

TABLE 3. Truth values of P, Q, R and S for which $\neg Y$ is true

Suppose that $f(x)$ is monogenic. Then $g_2(x)$, $g_4(x)$ and $g_6(x)$ are all monogenic, with b and $\mathcal{W}$ squarefree, from Corollary 2.4. We use Theorem 2.6 and Theorem 2.7 with $(G_4, G_6) = (4\mathrm{T}3, 6\mathrm{T}3)$ to impose further restrictions on statements P, Q, R and S to determine the possibilities in Table 3 that could actually yield monogenic trinomials $f(x)$, and to derive necessary conditions for the monogenicity of $f(x)$.

Observe that $b \neq 1$ from Theorem 2.6 and $b \in \{\pm 1, 2\}$ from Theorem 2.7. Thus, $b \in \{-1, 2\}$, and

$$-3b\delta = \begin{cases} 3(a^2+4) & \text{if } b = -1, \\ -6(a^2-8) & \text{if } b = 2. \end{cases}$$

If $3(a^2+4)$ is a square, then $3 \mid (a^2+4)$ and we arrive at the contradiction that $a^2 \equiv 2 \pmod 3$. The same contradiction is reached if we assume that $-6(a^2-8)$ is a square. Hence, statement P is false, which eliminates the first two possibilities in Table 3. A similar argument, which we omit, shows that statement Q is false, eliminating the third possibility in Table 3.

If $b = 2$, then statement S is false, and $a = \pm 2$ from Theorem 2.7. Note also that

$$r(x) = x^3 - 6x \pm 4 = (x \mp 2)(x^2 \pm 2x - 2),$$

so that statement R is true. Thus, we get that $f(x) = x^{12} \pm 2x^6 + 2$.

If $b=-1$, then statement S is true. Moreover, for $a\neq 0$, it is easy to see that $r(x)$ is reducible if and only if $a=n^3+3n$ for $n\in\mathbb{Z}$, and in this case we have

$$r(x)=(x-n)(x^2+nx+n^2+3),$$

which implies that

$$\begin{aligned} f(x)&=x^{12}+(n^3+n)x^6-1\\ &=(x^4+nx^2-1)(x^8-nx^6+n^2x^4+x^4+nx^2n+1). \end{aligned}$$

Thus, we can assume that $r(x)$ is irreducible so that statement R is false. In this situation, we have that $g_4(x)\in\mathcal{F}_1$ from Theorem 2.6 and $g_6(x)\in\mathcal{F}_4$ from Theorem 2.7, such that $a \bmod 4\neq 0$ and $a \bmod 9\notin\{0,4,5\}$. That is, we have shown that if $f(x)$ is monogenic, then

$$f(x)\in\{x^{12}+2x^6+2,\ x^{12}-2x^6+2\}$$

or $f(x)=x^{12}+ax^6-1$, where a satisfies the conditions $\mathcal{C}_{28}$. We have also established that the last possibility in Table 3 cannot occur when $f(x)$ is monogenic.

Conversely, suppose that $f(x)=x^{12}\pm 2x^6+2$ or $f(x)=x^{12}+ax^6-1$, where a satisfies the conditions $\mathcal{C}_{28}$. It is easy to see that each of the irreducible (2-Eisenstein) trinomials $f(x)=x^{12}+2x^6+2$ and $f(x)=x^{12}-2x^6+2$ satisfies condition (1) of Theorem 2.1 with $q=2$, which implies that they are both monogenic by Theorem 2.3 since $g_6(x)$ is monogenic in each case by Theorem 2.7, and $f(x)=g_6(x^2)$.

Suppose then that $f(x)=x^{12}+ax^6-1$, where a satisfies the conditions $\mathcal{C}_{28}$. We use Theorem 2.1 to examine the monogenicity of $f(x)=x^{12}+ax^6-1$. Suppose first that $q=2$ divides a. Then, by condition (2) of Theorem 2.1, $2\nmid \operatorname{index}(f)$ since $4\nmid a$. If $2\nmid a$, then in condition (4) of Theorem 2.1, we have that

$$H_1(x)=x^6+ax^3+1 \quad\text{and}\quad H_2(x)=x^3\left(\left(\frac{a^2+a}{2}\right)x^3-a\right).$$

Since $2\nmid a$, we have that $H_1(x)$ is irreducible in $\mathbb{F}_2[x]$, which implies that $H_1(x)$ and $H_2(x)$ are coprime in $\mathbb{F}_2[x]$. Thus, $2\nmid\operatorname{index}(f)$. Suppose next that $q=3$ is a divisor of a. Then, we see from condition (2) of Theorem 2.1 that $3\nmid\operatorname{index}(f)$ since $a\not\equiv 0 \pmod 9$. If $3\nmid a$, then we see by inspection of Table 4, generated from condition (4) of Theorem 2.1 with $a \bmod 9\in\{1,2,7,8\}$, that $3\nmid\operatorname{index}(f)$, which verifies that $f(x)$ is monogenic.

The Case 12T37. Suppose that $\operatorname{Gal}(f)\simeq$ 12T37. From Theorem 2.8, we have that $(G_4,G_6)=(4T2,6T9)$, where neither 3α nor 3β is a square.

Suppose that $f(x)$ is monogenic. Then we have from Corollary 2.4 that $g_2(x)$, $g_4(x)$ and $g_6(x)$ are all monogenic, with b and $\mathcal{W}$ squarefree. From Theorem 2.6, we see that $a \bmod 4\in\{0,3\}$ and $b=1$. Consequently, both $a-2$ and $a+2$ are squarefree since $\mathcal{W}$ is squarefree. Note also that if $a=-1$, then

$a \bmod 9$	$H_1(x) \bmod 3$	$H_2(x) \bmod 3$
1	$x^4 + x^2 + 2$	$x^2(x+1)(x+2)$
2	$x^4 + 2x^2 + 2$	$x^2(x+1)^2(x+2)^2$
7	$x^4 + x^2 + 2$	$2x^2(x^2+1)^2$
8	$x^4 + 2x^2 + 2$	$x^2(x^2+1)$.

TABLE 4. Factorization of $H_i(x)$ into irreducibles in $\mathbb{F}_3[x]$

$f(x) = x^{12} - x^6 + 1$ so that $\mathrm{Gal}(f) \simeq$ 12T2. Hence, $a \neq \pm 1$. Furthermore, $a \bmod 9 = 0$, otherwise we would have $g_6(x) \in \mathcal{F}_3$, so that $G_6 =$ 6T3 by Theorem 2.7, contradicting the fact that $G_6 =$ 6T9.

Since 3 divides $\Delta(f) = 2^{12}3^{12}(a-2)^6(a+2)^6$, $a \bmod 9 = 0$ and $b = 1$, we know that condition (2) of Theorem 2.1 must be satisfied with $q = 3$. However, $3 \mid a_2$ and $b_1 = 0$ in condition (2) of Theorem 2.1, which implies that $3 \mid \mathrm{index}(f)$, and contradicts the assumption that $f(x)$ is monogenic. Hence, there do not exist any 12T37-monogenic trinomials $f(x)$.

The Case 12T38. Suppose that $\mathrm{Gal}(f) \simeq$ 12T38. From Theorem 2.8, we have that $(G_4, G_6) =$ (4T3, 6T9), where $-3b$ or $-3b\delta$ is a square. If $-3b$ and $-3b\delta$ are both squares, then δ is a square, which contradicts the fact that $f(x)$ is irreducible. Hence, $-3b$ and $-3b\delta$ cannot both be squares.

Suppose that $f(x)$ is monogenic. Then we have from Corollary 2.4 that $g_2(x)$, $g_4(x)$ and $g_6(x)$ are all monogenic, with b and $\mathcal{W}$ squarefree.

Assume first that $-3b$ is a square. Since b is squarefree, it follows that $b = -3$, so that $a \bmod 4 \in \{0, 3\}$ from Theorem 2.6. Note then that

$$b\delta = -3(a^2 + 12)$$

is not a square. We need to determine the precise conditions under which $g_6(x) = x^6 + ax^3 - 3$ is monogenic. To do this, we only need to examine the prime $q = 3$ in Theorem 2.1 by Theorem 2.3, since $g_2(x) = x^2 + ax - 3$ is monogenic and $g_6(x) = g_2(x^3)$. Furthermore, since $g_6(0) = -3$ is squarefree, we only have to analyze condition (3) of Theorem 2.1, where we have

$$a_1 = \frac{a - a^3}{3} \quad \text{and} \quad b_2 = -1.$$

We see that $3 \mid a_1$ if and only if $a \bmod 9 \in \{0, 1, 8\}$, and that

$$3 \nmid a_1(aa_1 + 1) \quad \text{if and only if} \quad a \bmod 9 \in \{3, 4, 5, 6\}.$$

Thus, it follows that $g_6(x)$ and, consequently, $f(x)$ are monogenic if and only if $a \bmod 9 \notin \{2, 7\}$.

Assume next that $-3b\delta$ is a square. From the arguments used in the case 12T12, we have that

$$(a, b) \in \{(\pm 1, 1),\ (\pm 4, -2),\ (\pm 4, 6),\ (\pm 11, 33)\}. \tag{3.3}$$

It is easy to verify that $(a,b)=(1,1)$ is impossible since $f(x)$ is reducible in this situation, while $(a,b)=(-1,1)$ gives $f(x)$ with $\mathrm{Gal}(f)\simeq$ 12T2. With $(a,b)=(\pm 11,33)$, we see that condition (3) of Theorem 2.1 fails for $g_6(x)$ with $q=3$. Thus, neither one of the two trinomials $f(x)=x^{12}\pm 11x^6+33=g_6(x^2)$ is monogenic by Theorem 2.3. Straightforward calculations using Theorem 2.1, or a computer algebra system, verify that the remaining four possibilities in (3.3) yield 12T38-monogenic trinomials $f(x)$.

Conversely, suppose that $f(x)=x^{12}+ax^6-3$, such that a satisfies the conditions in $\mathcal{C}_{38}$. Then,

$$(a \bmod 4,\ b \bmod 4)\in\{(0,1),\ (3,1)\}$$

and $b\delta=-3(a^2+12)<0$ is not a square. With the calculations done in the other direction of this proof, it follows that $g_4(x)$ is monogenic with $G_4=$ 6T3 and $g_6(x)$ is monogenic with $G_6=$ 6T9, so that $f(x)$ is monogenic by Theorem 2.3.

The Case 12T39. Suppose that $\mathrm{Gal}(f)\simeq$ 12T39. From Theorem 2.8, we have that $(G_4,G_6)=$ (4T1, 6T9). If $f(x)$ is monogenic, then $g_4(x)$ is monogenic from Corollary 2.4. Hence,

$$f(x)\in S:=\{x^{12}\pm 4x^6+2,\ x^{12}-5x^6+5\}$$

from Theorem 2.6. Then, using Theorem 2.1 or a computer algebra system, it is straightforward to confirm that each $f(x)\in S$ is monogenic with $\mathrm{Gal}(f)\simeq$ 12T39.

The Case 12T42. Suppose that $\mathrm{Gal}(f)\simeq$ 12T42. Then, from Theorem 2.8, we have that $(G_4,G_6)=$ (4T3, 6T5).

Suppose that $f(x)$ is monogenic. Then $g_2(x)$, $g_4(x)$ and $g_6(x)$ are all monogenic, with b and $\mathcal{W}$ squarefree, from Corollary 2.4. We deduce then from Theorem 2.6 and Theorem 2.7 that $b=(a^2+3)/4$ is squarefree and

$$(a \bmod 4,\ b \bmod 4)\in\{(1,3),(3,1),(3,3)\},$$

with $a\neq\pm 1$. By Theorem 2.3, since $f(x)=g_6(x^2)$, we only need to focus on $q=2$ in Theorem 2.1 to ascertain further restrictions on a to guarantee that $f(x)$ is monogenic. From condition (4) of Theorem 2.1 we get

$$H_1(x):=x^6+ax^3+(a^2+3)/4 \quad \text{and}$$
$$H_2(x):=\left(\frac{a(a+1)}{2}\right)x^6+\left(\frac{a(a^2+3)}{4}\right)x^3+\frac{(a^2+3)(a^2+7)}{32}.$$

Since $2\nmid a$ and $2^2 \mid\mid (a^2+3)$, we have that $H_1(x)\equiv x^6+x^3+1 \bmod 2$ is irreducible in $\mathbb{F}_2[x]$. Thus, $2\mid \mathrm{index}(f)$ if and only if $H_2(x)\equiv H_1(x) \bmod 2$. Note that the coefficient on x^3 in both $H_2(x)$ and $H_1(x)$ modulo 2 is always 1, while equating the coefficients on x^6 and the constant terms modulo 2 yields

$$\frac{a^2+a}{2}\equiv 1 \bmod 2 \quad \text{and} \quad \frac{a^2+7}{8}\equiv 1 \bmod 2. \tag{3.4}$$

The first congruence in (3.4) is true if and only if $a \bmod 4 = 1$, while the second congruence is true if and only if $a \bmod 16 \in \{1, 7, 9, 15\}$. Hence, for both congruences in (3.4) to hold simultaneously, we must have $a \bmod 8 = 1$. We conclude that $2 \nmid \operatorname{index}(f)$ if and only if $a \bmod 8 \in \{3, 5, 7\}$. Hence, a satisfies the conditions in $\mathcal{C}_{42}$.

Conversely, suppose that $f(x) = x^{12} + ax^6 + (a^2+3)/4$, where a satisfies the conditions in $\mathcal{C}_{42}$. Observe also that $\mathcal{W} = -3$ is squarefree, and $a \neq 1$, since otherwise $f(x)$ is reducible over $\mathbb{Q}$. Furthermore, $b\delta = -3(a^2+3)/4 < 0$ is not a square. Thus, $g_4(x)$ is monogenic with $G_4 = 4\text{T}3$ and $g_6(x)$ is monogenic with $G_6 = 6\text{T}5$. Since $f(x) = g_6(x^2)$, it follows from Theorem 2.3 that $f(x)$ is monogenic form the calculations done in the previous direction of the proof for condition 4 of Theorem 2.1 with $q = 2$.

The Case 12T81. Suppose that $\operatorname{Gal}(f) \simeq 12\text{T}81$. From Theorem 2.8, we have that $(G_4, G_6) = (4\text{T}3, 6\text{T}9)$, where neither $-3b$ nor $-3b\delta$ is a square.

Suppose that $f(x)$ is monogenic. Then, from Corollary 2.4, $g_2(x)$, $g_4(x)$ and $g_6(x)$ are all monogenic, with b and $\mathcal{W}$ squarefree. From Theorem 2.6, we have that $b\delta$ is not a square and $(a \bmod 4,\ b \bmod 4) \in \mathcal{R}$. From Theorem 2.7, we have that b is not a cube, which precludes overlap with $\mathcal{C}_{28}$. By Theorem 2.3, since $g_6(x) = g_2(x^3)$, and $g_2(x)$ is monogenic from Theorem 2.2, we can use Theorem 2.1 with $q = 3$ to determine precise conditions under which $g_6(x)$ is monogenic. Observe that condition (5) of Theorem 2.1 is satisfied since $\mathcal{W}$ is squarefree. If $3 \mid a$ and $3 \mid b$, then condition (1) of Theorem 2.1 is satisfied if and only if $(a \bmod 9,\ b \bmod 9)$ is an element of $\mathcal{S}_1$, since b is squarefree. If $3 \mid a$ and $3 \nmid b$, then straightforward calculations show that condition (2) of Theorem 2.1 is satisfied if and only if $(a \bmod 9,\ b \bmod 9) \in \mathcal{S}_2$. Similarly, if $3 \nmid a$ and $3 \mid b$, then it is easy to see that condition (3) of Theorem 2.1 is satisfied if and only if $(a \bmod 9,\ b \bmod 9) \in \mathcal{S}_3$. Finally, we examine condition (4) of Theorem 2.1 to get that

$$H_1(x) = x^2 + ax + b$$

and

$$H_2(x) = \left(\frac{a - a^3}{3}\right)x^3 - a^2bx^2 - ab^2x + \frac{b - b^3}{3}$$

are coprime in $\mathbb{F}_3[x]$ if and only if $(a \bmod 9,\ b \bmod 9) \in \mathcal{S}_4$.

The converse is straightforward and follows by utilizing the calculations done previously in the other direction of the proof of this case. $\square$

4. Acknowledgments

The author thanks the anonymous referee for a careful reading of this article, and for all the excellent suggestions.

References

[1] AWTREY, CHAD; JAKES, PETER. Galois groups of even sextic polynomials. *Canad. Math. Bull.* **63** (2020), no. 3, 670–676. MR4148127, Zbl 1458.11173, doi: 10.4153/S0008439519000754. 1201

[2] AWTREY, CHAD; LEE, ALLY. Galois groups of reciprocal sextic polynomials. *Bull. Aust. Math. Soc.* **109** (2024), no. 1, 37–44. MR4695455, Zbl 1527.12002, doi: 10.1017/S0004972723000163. 1201

[3] BREMNER, ANDREW; SPEARMAN, BLAIR K. Cyclic sextic trinomials $x^6 + Ax + B$. *Int. J. Number Theory* **6** (2010), no. 1, 161–167. MR2641719, Zbl 1245.12001, doi: 10.1142/S1793042110002843. 1201

[4] BROWN, STEPHEN C.; SPEARMAN, BLAIR K.; YANG, QIDUAN. On the Galois groups of sextic trinomials. *JP J. Algebra Number Theory Appl.* **18** (2010), no. 1, 67–77. MR2766535, Zbl 1218.11101. 1201

[5] BROWN, STEPHEN C.; SPEARMAN, BLAIR K.; YANG, QIDUAN. 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. MR3005580, Zbl 1290.12005, doi: 10.1142/S0219498812501289. 1201

[6] BUTLER, GREGORY; MCKAY, JOHN. The transitive groups of degree up to eleven. *Comm. Algebra* **11** (1983), no. 8, 863–911. MR0695893, Zbl 0518.20003, doi: 10.1080/00927878308822884. 1200, 1204

[7] CAVALLO, ALBERTO. An elementary computation of the Galois groups of symmetric sextic trinomials. arXiv:1902.00965v2. 1201

[8] CHEN, MALCOM H. W. Elementary characterization for Galois groups of $x^{12} + ax^6 + b$. arXiv:2410.00870v2. 1200, 1201, 1206

[9] COHEN, H. A course in computational algebraic number theory. Graduate Texts in Mathematics, 138. *Springer-Verlag, New York*, 2000. MR1228206, Zbl 0786.11071, doi: 10.1007/978-3-662-02945-9. 1199, 1201

[10] HARRINGTON, JOSHUA; JONES, LENNY. The irreducibility of power compositional sextic polynomials and their Galois groups. *Math. Scand.* **120** (2017), no. 2, 181–194. MR3657411, Zbl 1414.12001, doi: 10.7146/math.scand.a-25850. 1201

[11] HARRINGTON, JOSHUA; JONES, LENNY. Monogenic quartic polynomials and their Galois groups. *Bull. Aust. Math. Soc.* **111** (2025), no. 2, 244–259. MR4879768, Zbl 1579.11174, arXiv:2404.05487. doi: 10.1017/S000497272400073X. 1201, 1204

[12] HARRINGTON, JOSHUA; JONES, LENNY. The irreducibility and monogenicity of power-compositional trinomials. *Math. J. Okayama Univ.* **67** (2025), 53–65. MR4855654, Zbl 1562.11173, arXiv:2204.07784. 1201

[13] HARRINGTON, JOSHUA; JONES, LENNY. Monogenic trinomials of the form $x^4 + ax^3 + d$ and their Galois groups. *J. Algebra Appl.* **25** (2026), no. 10, Paper No. 2650096, 8pp. MR5063013, Zbl 08196870, arXiv:2407.00413 doi: 10.1142/S0219498826500969. 1201

[14] HARRINGTON, JOSHUA; JONES, LENNY. Monogenic sextic trinomials $x^6 + Ax^3 + B$ and their Galois groups. *Acta Arith.* **223** (2026), no. 2, 167–184. MR5068940, Zbl 08200798, arXiv:2507.17021, doi: 10.4064/aa250722-26-8. 1200, 1201, 1205

[15] HARRINGTON, JOSHUA; JONES, LENNY. On the monogenicity and Galois groups of $x^{2p} + ax^p + b^p$. *Bull. Aust. Math. Soc.* (to appear) arXiv:2603.06432. 1201

[16] 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. MR3713088, Zbl 1431.11116, doi: 10.1142/S1793042117501391. 1201, 1202

[17] JONES, LENNY. Sextic reciprocal monogenic dihedral polynomials. *Ramanujan J.* **56** (2021), no. 3, 1099–1110. MR4341112, Zbl 1487.11095, doi: 10.1007/s11139-020-00310-w. 1201

[18] JONES, LENNY. Infinite families of reciprocal monogenic polynomials and their Galois groups. *New York J. Math.* **27** (2021), 1465–1493. MR4334375, Zbl 1487.11096, 1201

[19] JONES, LENNY. Monogenic reciprocal trinomials and their Galois groups. *J. Algebra Appl.* **21** (2022), no. 2, Paper No. 2250026, 11 pp. MR4381284, Zbl 1500.11075, doi: 10.1142/S0219498822500268. 1201

[20] JONES, LENNY. Monogenic even quartic trinomials. *Bull. Aust. Math. Soc.* **111** (2025), no. 2, 238–243. MR4879767, Zbl 1580.11100, doi: 10.1017/S0004972724000510. 1201, 1204

[21] JONES, LENNY. Monogenic cyclic trinomials of the form $x^4 + cx + d$. *Acta Arith.* **218** (2025), no. 4, 385–394. MR4898516, Zbl 8044224, arXiv:2411.10572, doi: 10.4064/aa241127-1-1. 1201

[22] JONES, LENNY Monogenic even cyclic sextic polynomials. *Math. Slovaca* **75**, No. 5, (2025), 1021–1034. MR4976593, Zbl 1573.11333, arXiv:2502.04120v2, doi: 10.1515/ms-2025-0075. 1201

[23] JONES, LENNY. Monogenic cyclic cubic trinomials. *Bol. Soc. Mat. Mex.* (3) **31** (2025), no. 1, Paper No. 28, 9 pp. MR4847743, Zbl 1580.11099, arXiv:2412.13075 doi: 10.1007/s40590-024-00708-2. 1201

[24] JONES, LENNY. Monogenic even octic polynomials and their Galois groups. *New York J. Math.* **31** (2025), 91–125. MR4853788, Zbl 1557.11140, arXiv:2404.17921. 1201

[25] JONES, LENNY; WHITE, DANIEL. Monogenic trinomials with non-squarefree discriminant. *Internat. J. Math.* **32** (2021), no. 13, Paper No. 2150089, 21 pp. MR4361991, Zbl 1478.11125, arXiv:1908.07947, doi: 10.1142/S0129167X21500890. 1201

[26] KAPPE, LUISE-CHARLOTTE.; WARREN, BETTE. An elementary test for the Galois group of a quartic polynomial. *Amer. Math. Monthly* **96** (1989), no. 2, 133–137. MR0992075, Zbl 0702.11075, doi: 10.2307/2323198. 1200, 1201, 1204

[27] KAUR, SUMANDEEP; KUMAR, SURRENDER; REMETE, LÁSZLÓ. On the index of power compositional polynomials. *Finite Fields Appl.* **107** (2025), Paper No. 102642, 20 pp. MR4902688, Zbl 1577.11172, arXiv:2404.17351, doi: 10.1016/j.ffa.2025.102642. 1201, 1203

[28] MOTODA, YASUO; NAKAHARA, TORU; SHAH, SYED INAYAT ALI; UEHARA, TSUYOSHI. On a problem of Hasse. *Algebraic number theory and related topics 2007*, 209–221. RIMS Kôkyûroku Bessatsu, B12. *Research Institute for Mathematical Sciences (RIMS), Kyoto*, 2009. MR2605782, Zbl 1251.11073. 1201

[29] SWAN, RICHARD G. Factorization of polynomials over finite fields. *Pacific J. Math.* **12** (1962), 1099–1106. MR0144891, Zbl 0113.01701, doi: 10.2140/pjm.1962.12.1099. 1202

[30] VOUTIER, PAUL M. Families of cyclic quartic monogenic polynomials. *Acta Arith.* **219** (2025), no. 4, 365–377. MR4929829, Zbl 8087062, arXiv:2405.20288v2. doi: 10.4064/aa240919-10-3. 1201

[31] WASHINGTON, LAWRENCE C. Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. *Springer-Verlag, New York*, 1997.xiv+487 pp. ISBN:0-387-94762-0. MR1421575, Zbl 0966.11047, doi: 10.1007/978-1-4612-1934-7. 1207

(Lenny Jones) PROFESSOR EMERITUS, DEPARTMENT OF MATHEMATICS, SHIPPENSBURG UNIVERSITY, SHIPPENSBURG, PENNSYLVANIA 17257, USA
doctorlennyjones@gmail.com

This paper is available via http://nyjm.albany.edu/j/2026/32-48.html.