New York Journal of Mathematics

New York J. Math. **31** (2025) 91–125.

Monogenic even octic polynomials and their Galois groups

Lenny Jones

ABSTRACT. A monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree N is called *monogenic* if $f(x)$ is irreducible over $\mathbb{Q}$ and $\{1, \theta, \theta^2, \ldots, \theta^{N-1}\}$ is a basis for the ring of integers of $\mathbb{Q}(\theta)$, where $f(\theta) = 0$. In a series of recent articles, complete classifications of the Galois groups were given for irreducible polynomials

$$\mathcal{F}(x) := x^8 + ax^4 + b \in \mathbb{Z}[x]$$

and

$$\mathcal{G}(x) := x^8 + ax^6 + bx^4 + ax^2 + 1 \in \mathbb{Z}[x], \quad a \neq 0.$$

In this article, for each Galois group G arising in these classifications, we either construct an infinite family of monogenic octic polynomials $\mathcal{F}(x)$ or $\mathcal{G}(x)$ having Galois group G, or we prove that at most a finite such family exists. In the finite family situations, we determine all such polynomials. Here, a "family" means that no two polynomials in the family generate isomorphic octic fields.

CONTENTS

1. Introduction

Unless stated otherwise, when we say that $f(x) \in \mathbb{Z}[x]$ is "irreducible", we mean irreducible over $\mathbb{Q}$. We let $\Delta(f)$ and $\Delta(K)$ denote the discriminants over $\mathbb{Q}$, respectively, of $f(x)$ and a number field K. If $f(x)$ is irreducible, with $f(\theta) = 0$ and $K = \mathbb{Q}(\theta)$, then [7]

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

where $\mathbb{Z}_K$ is the ring of integers of K. We define a monic polynomial $f(x) \in \mathbb{Z}[x]$ to be *monogenic* if $f(x)$ is irreducible and $\mathbb{Z}_K = \mathbb{Z}[\theta]$, or equivalently from (1.1), that $\Delta(f) = \Delta(K)$. When $f(x)$ is monogenic, $\{1, \theta, \theta^2, \ldots, \theta^{\deg(f)-1}\}$

Received May 30, 2024.
2020 *Mathematics Subject Classification.* Primary 11R21, 11R32.
Key words and phrases. monogenic, octic, Galois.

ISSN 1076-9803/2025

is a basis for $\mathbb{Z}_K$, commonly referred to as a *power basis*. The existence of a power basis facilitates computations in $\mathbb{Z}_K$, as in the case of the cyclotomic polynomials $\Phi_n(x)$ [45]. A number field K is defined to be *mongenic* if there exists a power basis for $\mathbb{Z}_K$.

We caution the reader concerning two items. Certainly, the monogenicity of $f(x)$ implies the monogenicity of $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. However, the converse is not necessarily true. For example, let $f(x) = x^2 - 5$ and $K = \mathbb{Q}(\theta)$, where $\theta = \sqrt{5}$. Then, easy calculations show that $\Delta(f) = 20$ and $\Delta(K) = 5$. Thus, $f(x)$ is not monogenic, but K is monogenic since $\{1, (\theta+1)/2\}$ is a power basis for $\mathbb{Z}_K$. A second item of concern is the following. We see from (1.1) that if $\Delta(f)$ is squarefree, then $f(x)$ is monogenic. However, the converse is false in general, and when $\Delta(f)$ is not squarefree, it can be quite difficult to determine whether $f(x)$ is monogenic.

In a series of recent articles [1–3, 6], complete classifications of the Galois groups were given for irreducible polynomials

$$\mathcal{F}(x) := x^8 + ax^4 + b \in \mathbb{Z}[x], \tag{1.2}$$

and

$$\mathcal{G}(x) := x^8 + ax^6 + bx^4 + ax^2 + 1 \in \mathbb{Z}[x], \quad a \neq 0. \tag{1.3}$$

These classifications provide $\mathrm{Gal}(\mathcal{F})$ and $\mathrm{Gal}(\mathcal{G})$, the Galois groups over $\mathbb{Q}$ of $\mathcal{F}(x)$ and $\mathcal{G}(x)$, respectively, by determining whether certain expressions involving only the coefficients of $\mathcal{F}(x)$ and $\mathcal{G}(x)$ are, or are not, squares in $\mathbb{Z}$. We point out that some of the results in [1–3, 6] were given over $\mathbb{Q}$ or an arbitrary field of characteristic zero. However, in this article, we are only concerned with polynomials with coefficients in $\mathbb{Z}$.

Using the standard "8TX"-notation for transitive groups of degree 8 as given in Magma and [5,8,36], the values of X that arise in the classifications in [1–3,6] for $\mathcal{F}(x)$ and $\mathcal{G}(x)$ are, respectively,

$$X_{\mathcal{F}} := \{2, 3, 4, 6, 8, 9, 11, 15, 16, 17, 22, 26\} \text{ and } X_{\mathcal{G}} := \{2, 3, 4, 9, 10, 18\}. \tag{1.4}$$

Using C_n to denote the cyclic group of order n, D_n to denote the dihedral group of order $2n$, Q_8 to denote the quaterion group, $\times$ to denote a direct product, $\rtimes$ to denote a semi-direct product, . to denote a non-split extension, $\circ$ to denote a central product, $\wr$ to denote a wreath product and Hol to denote the holomorph, we provide in Table 1 some more-familiar names for the groups in (1.4).

X	2	3	4	6	8	9	10
8TX	$C_2 \times C_4$	C_2^3	D_4	D_8	$Q_8 \rtimes C_2$	$C_2 \times D_4$	$C_2^2 \rtimes C_4$
X	11	15	16	17	18	22	26
8TX	$C_4 \circ D_4$	$C_8 \rtimes C_2^2$	$C_4.D_4$	$C_4 \wr C_2$	$C_2^2 \wr C_2$	$D_4 \circ D_4$	$\mathrm{Hol}(D_4)$

TABLE 1. Familiar names for the groups 8TX in (1.4)

In this article, for each value of X in (1.4), we either construct an infinite family of monogenic polynomials $\mathcal{F}(x)$ or $\mathcal{G}(x)$ in $\mathbb{Z}[x]$ having Galois group 8TX, or we prove that at most a finite such family exists. In the finite family situations, we determine all such polynomials. In certain cases, there are no such polynomials. By a "family", we mean that all polynomials in the family are distinct in the sense that no two polynomials in the family generate isomorphic octic fields.

More precisely, we prove the following:

Theorem 1.1. *Let $\mathcal{F}(x) \in \mathbb{Z}[x]$ and $\mathcal{G}(x) \in \mathbb{Z}[x]$ be as defined in (1.2) and (1.3). Let $X_{\mathcal{F}}$ and $X_{\mathcal{G}}$ be as defined in (1.4).*

(1) For each $\mathrm{X} \in \{9, 15, 17, 26\}$, there exists at least one infinite family of monogenic polynomials $\mathcal{F}(x)$ having Galois group 8TX. For all other values of $\mathrm{X} \in X_{\mathcal{F}}$, there exist at most finitely many monogenic polynomials $\mathcal{F}(x)$ having Galois group 8TX.

(2) For each $\mathrm{X} \in \{9, 18\}$, there exists at least one infinite family of monogenic polynomials $\mathcal{G}(x)$ having Galois group 8TX. For all other values of $\mathrm{X} \in X_{\mathcal{G}}$, there exist at most finitely many monogenic polynomials $\mathcal{G}(x)$ having Galois group 8TX.

The literature involving the construction of monogenic or non-monogenic polynomials is fairly extensive [9, 11, 16–21, 23–30, 32, 33, 35, 41–43]. However, the approach used in the proof of Theorem 1.1 differs from most previously-addressed situations in that each monogenic family is constructed with the specific goal that every polynomial in the family has the same Galois group. We do point out that a similar approach was carried out in [11, 30] for monogenic quartic polynomials and their Galois groups. Of course, in the quartic case, a complete classification of the Galois groups is known [34].

Another distinction of Theorem 1.1 is the fact that, for certain groups G, we also establish the nonexistence of a monogenic polynomial $\mathcal{F}(x)$ or $\mathcal{G}(x)$ having Galois group G. Consequently, Theorem 1.1 is somewhat more in line with the following theorem of Gras [10]:

Theorem 1.2. [10] *Let ℓ be a prime, and let K be a degree-ℓ cyclic extension of $\mathbb{Q}$. If $\ell \geq 5$, then $\mathbb{Z}_K$ does not have a power basis except in the case when $2\ell + 1$ is prime and $K = \mathbb{Q}(\zeta_{2\ell+1} + \zeta_{2\ell+1}^{-1})$, the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{2\ell+1})$, where $\Phi_{2\ell+1}(\zeta_{2\ell+1}) = 0$.*

By providing two examples, we illustrate how Theorem 1.2 fits into the framework of Theorem 1.1. Suppose first that $\ell = 7$. Then, since $2 \cdot 7 + 1 = 15$ is not prime, Theorem 1.2 tells us that no monogenic polynomial of degree 7 exists having Galois group $7\mathrm{T}1 = C_7$. However, if $\ell = 5$, then $2 \cdot 5 + 1 = 11$ is prime, and we conclude from Theorem 1.2 that there exists a degree-5 monogenic polynomial $f(x)$ having Galois group $5\mathrm{T}1 = C_5$. For example, if $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$, which is the minimal polynomial over $\mathbb{Q}$ of $\alpha = \zeta_{11} + \zeta_{11}^{-1}$, where ζ_{11} is a primitive 11th root of unity, then $f(x)$ is monogenic and $\mathrm{Gal}(f) \simeq 5\mathrm{T}1$. Moreover, Theorem 1.2 says that $f(x)$ is essentially the

only such polynomial, in the sense that if $g(x)$ is a degree-5 monogenic polynomial with $g(x) \neq f(x)$ and $\mathrm{Gal}(g) \simeq 5\mathrm{T}1$, then $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$, where $g(\beta) = 0$.

Computer computations in this article were done using either Magma [4], Maple [38] or Sage [40].

2. Preliminaries

When we refer to an expression as being a square, we mean a square in $\mathbb{Z}$. The next theorem follows from [37].

Theorem 2.1. *Let $N \geq 0$ be an integer. Then $2^N - 1$ is a square if and only if $N \in \{0, 1\}$.*

The formula for the discriminant of an arbitrary monic trinomial, due to Swan [44, Theorem 2], is given in the following theorem.

Theorem 2.2. *Let $f(x) = x^n + Ax^m + B \in \mathbb{Q}[x]$, where $0 < m < n$, and let $d = \gcd(n, m)$. Then*

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

The next two theorems are transcriptions due to Awtrey and Patane [3] of the more-algorithmic classifications of $\mathcal{F}(x)$ given in [6].

Theorem 2.3. *Let $\mathcal{F}(x)$ be as defined in (1.2). Suppose that b and $\sqrt{b}$ are squares. Then $\mathrm{Gal}(\mathcal{F})$ is isomorphic to*

(1) 8T2 *if and only if $-a^2 + 4b$ is a square,*
(2) 8T3 *if and only if $a + 2\sqrt{b}$ is a square,*
(3) 8T4 *if and only if $a - 2\sqrt{b}$ is a square,*
(4) 8T9 *if and only if none of $-a^2 + 4b$, $a + 2\sqrt{b}$ and $a - 2\sqrt{b}$ is a square.*

Theorem 2.4. *Let $\mathcal{F}(x)$ be as defined in (1.2). Suppose that b is a square and $\sqrt{b}$ is not a square. Then $\mathrm{Gal}(\mathcal{F})$ is isomorphic to*

(1) 8T2 *if and only if $a + 2\sqrt{b}$ and $a\sqrt{b} - 2b$ are both squares,*
(2) 8T4 *if and only if both quantities in one of the following pairs are squares:*

$$(a + 2\sqrt{b}, -a\sqrt{b} + 2b), \quad (a - 2\sqrt{b}, a\sqrt{b} + 2b), \quad (-a\sqrt{b} + 2b, a\sqrt{b} + 2b).$$

(3) 8T9 *if and only if $(a - 4b)\sqrt{b}$ is a not a square, and exactly one of*

$$a + 2\sqrt{b}, \quad a - 2\sqrt{b}, \quad -a\sqrt{b} + 2b, \quad a\sqrt{b} + 2b$$

is a square.

(4) 8T11 *if and only if neither $-a\sqrt{b} + 2b$ nor $a\sqrt{b} + 2b$ is a square, and exactly one of*

$$-a^2 + 4b, \quad -a\sqrt{b} - 2b, \quad (a^2 - 4b)\sqrt{b}, \quad a\sqrt{b} - 2b, \quad (4b - a^2)\sqrt{b}$$

is a square,

(5) 8T22 *if and only if none of*

$$a+2\sqrt{b},\quad a-2\sqrt{b},\quad -a\sqrt{b}+2b,\quad a\sqrt{b}+2b,$$
$$-a^2+4b,\quad -a\sqrt{b}-2b,\quad (a^2-4b)\sqrt{b},\quad a\sqrt{b}-2b,\quad (4b-a^2)\sqrt{b}$$

is a square.

The next theorem is a compilation of the classifications given in [1] and [3].

Theorem 2.5. *Let $\mathcal{F}(x)$ be as defined in (1.2). Suppose that b is not a square.*

(1) *Then $Gal(\mathcal{F}) \simeq$ 8T16 if and only if $b(a^2-4b)$ is a square.*
(2) *Then $Gal(\mathcal{F}) \simeq$ 8T17 if and only if $b(a^2-4b)$ is not a square and $4b-a^2$ is a square.*
(3) *Suppose further that neither $b(a^2-4b)$ nor $4b-a^2$ is a square.*
   (a) *Then $Gal(\mathcal{F}) \simeq$ 8T6 if and only if one of*
   $$2\sqrt{-b},\quad 4b+2\sqrt{-b(a^2-4b)},\quad 4b-2\sqrt{-b(a^2-4b)}$$
   is a nonzero square.
   (b) *Then $Gal(\mathcal{F}) \simeq$ 8T8 if and only if*
   $$2(a^2-4b)\sqrt{-b}\quad \text{or}\quad -4b+2\sqrt{-b(a^2-4b)}$$
   is a nonzero square.
   (c) *Then $Gal(\mathcal{F}) \simeq$ 8T15 if and only if $-b$ or $-b(a^2-4b)$ is a square, and none of*
   $$2\sqrt{-b},\quad 2(a^2-4b)\sqrt{-b},\quad 4b+2\sqrt{-b(a^2-4b)},$$
   $$4b-2\sqrt{-b(a^2-4b)},\quad -4b+2\sqrt{-b(a^2-4b)}$$
   is a nonzero square.
   (d) *Then $Gal(\mathcal{F}) \simeq$ 8T26 if and only if neither $-b$ nor $-b(a^2-4b)$ is a square.*

The next two theorems present the classification of the Galois groups given in [2] for $\mathcal{G}(x)$, as defined in (1.3). We let

$$W_1 := b+2-2a,\quad W_2 := b+2+2a\quad \text{and}\quad W_3 := a^2-4b+8. \tag{2.1}$$

Theorem 2.6. *Let $\mathcal{G}(x)$ be as defined in (1.3). Then $Gal(\mathcal{G}) \simeq$*

(1) 8T2 *if and only if exactly two of*
$$W_1W_3,\quad W_2W_3\quad \text{and}\quad W_1W_2W_3\quad \text{are squares,}$$
(2) 8T3 *if and only if all of*
$$W_1,\quad W_2\quad \text{and}\quad W_1W_2\quad \text{are squares,}$$
(3) 8T10 *if and only if exactly one of*
$$W_1W_3,\quad W_2W_3\quad \text{and}\quad W_1W_2W_3\quad \text{is a square,}$$
(4) 8T18 *if and only if none of*
$$W_1,\ W_2,\ W_1W_2,\ W_1W_3,\ W_2W_3\ \text{and}\ W_1W_2W_3\ \text{is a square.}$$

Theorem 2.7. *Gal*$(\mathcal{G}) \simeq$ 8T4 *or* 8T9 *if and only if exactly one of*

$$W_1, \quad W_2 \quad \text{and} \quad W_1W_2 \quad \text{is a square,}$$

and none of

$$W_1W_3, \quad W_2W_3 \quad \text{and} \quad W_1W_2W_3 \quad \text{is a square.}$$

Furthermore, if Gal$(\mathcal{G}) \simeq$ 8T4 *or* 8T9*, then Gal*$(\mathcal{G}) \simeq$ 8T4 *if and only if either exactly one of*

$$W_2\left(-a+4-2\sqrt{W_1}\right) \quad \text{and} \quad W_2\left(-a+4+2\sqrt{W_1}\right) \quad \text{is a square}$$
$$\text{when } W_1 \text{ is a square,}$$

or exactly one of

$$W_1\left(-a-4-2\sqrt{W_2}\right) \quad \text{and} \quad W_1\left(-a-4+2\sqrt{W_2}\right) \quad \text{is a square}$$
$$\text{when } W_2 \text{ is a square,}$$

or exactly one of

$$W_2\left((12-2b-W_3)^2-4W_1W_2\right), \quad W_2\left(2b+W_3-12+2\sqrt{W_1W_2}\right)$$
$$\text{and} \quad W_2\left(2b+W_3-12-2\sqrt{W_1W_2}\right) \quad \text{is a square}$$
$$\text{when } W_1W_2 \text{ is a square;}$$

otherwise, Gal$(\mathcal{G}) \simeq$ 8T9.

The following theorem, which is known as *Dedekind's Index Criterion*, or simply *Dedekind's Criterion* if the context is clear, is a standard tool used in determining the monogenicity of a polynomial.

Theorem 2.8 (Dedekind [7])**.** *Let $K = \mathbb{Q}(\theta)$ be a number field, $T(x) \in \mathbb{Z}[x]$ the monic minimal polynomial of θ, and $\mathbb{Z}_K$ the ring of integers of K. Let q be a prime number and let $\overline{*}$ denote reduction of $*$ modulo q (in $\mathbb{Z}$, $\mathbb{Z}[x]$ or $\mathbb{Z}[\theta]$). Let*

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

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

$$h_1(x) = \prod_{i=1}^{k} \tau_i(x),$$

where the $\tau_i(x) \in \mathbb{Z}[x]$ are arbitrary monic lifts of the $\overline{\tau_i}(x)$. Let $h_2(x) \in \mathbb{Z}[x]$ be a monic lift of $\overline{T}(x)/\overline{h_1}(x)$ and set

$$F(x) = \frac{h_1(x)h_2(x) - T(x)}{q} \in \mathbb{Z}[x].$$

Then

$$[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q} \iff \gcd\left(\overline{F}, \overline{h_1}, \overline{h_2}\right) = 1 \text{ in } \mathbb{F}_q[x].$$

The next result is the specific case for our octic situation of a "streamlined" version of Dedekind's index criterion for trinomials that is due to Jakhar, Khanduja and Sangwan [15].

Theorem 2.9. [15] *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 $\mathcal{F}(x) = x^8 + ax^4 + b$ over $\mathbb{Q}$. A prime factor q of $\Delta(\mathcal{F}) = 2^{16}b^3(a^2-4b)^4$ does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if q satisfies on 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*

$$\text{either} \quad q \mid a_2 \text{ and } q \nmid b_1 \quad \text{or} \quad q \nmid a_2\left(-ba_2^2 - b_1^2\right),$$

where $a_2 = a/q$ and $b_1 = \frac{b+(-b)^{q^j}}{q}$ with $q^j \mid\mid 8$;
(3) *when $q \nmid a$ and $q \mid b$, then*

$$\text{either} \quad q \mid a_1 \text{ and } q \nmid b_2 \quad \text{or} \quad q \nmid a_1 b_2^3\left(-aa_1 + b_2\right),$$

where $a_1 = \frac{a+(-a)^{q^e}}{q}$ with $q^e \mid\mid 4$, and $b_2 = b/q$;
(4) *when $q = 2$ and $2 \nmid ab$, then the polynomials*

$$H_1(x) := x^2 + ax + b \quad \text{and} \quad H_2(x) := \frac{ax^4 + b + (-ax - b)^4}{2}$$

are coprime modulo 2;
(5) *when $q \nmid 2ab$, then $q^2 \nmid \left(a^2 - 4b\right)$.*

Remark 2.10. We will find both Theorem 2.8 and Theorem 2.9 useful in our investigations.

The remaining discussion and results in this section are crucial for the construction of the infinite families described in the proof of Theoem 1.1. In particular, Corollary 2.14 and Lemma 2.15 provide guidelines as to how to guarantee the existence of infinitely many values of the coefficients of $\mathcal{F}(x)$ and $\mathcal{G}(x)$ in order to ensure the monogenicity of $\mathcal{F}(x)$ and $\mathcal{G}(x)$.

Theorem 2.11. *Let $G(t) \in \mathbb{Z}[t]$, and suppose that $G(t)$ factors into a product of distinct non-constant polynomials $\gamma_i(t) \in \mathbb{Z}[t]$ that are irreducible over $\mathbb{Z}$, such that the degree of each $\gamma_i(t)$ is at most 3. Define*

$$N_G(X) = \left|\{p \le X : p \text{ is prime and } G(p) \text{ is squarefree}\}\right|.$$

Then,

$$N_G(X) \sim C_G \frac{X}{\log(X)}, \tag{2.2}$$

where

$$C_G = \prod_{\ell \text{ prime}} \left(1 - \frac{\rho_G\left(\ell^2\right)}{\ell(\ell-1)}\right) \tag{2.3}$$

and $\rho_G\left(\ell^2\right)$ is the number of $z \in \left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^*$ such that $G(z) \equiv 0 \pmod{\ell^2}$.

Remark 2.12. Theorem 2.11 follows from work of Helfgott, Hooley and Pasten [13, 14, 39]. For more details, see the discussion following [20, Theorem 2.11].

Definition 2.13. In the context of Theorem 2.11, for $G(t) \in \mathbb{Z}[t]$ and a prime ℓ, if $G(z) \equiv 0 \pmod{\ell^2}$ for all $z \in \left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^*$, we say that $G(t)$ has a *local obstruction at* ℓ. A polynomial $G(t) \in \mathbb{Z}[t]$ is said to have *no local obstructions*, if for every prime ℓ there exists some $z \in \left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^*$ such that $G(z) \not\equiv 0 \pmod{\ell^2}$.

Note that $C_G > 0$ in (2.3) if and only if $G(t)$ has no local obstructions. Consequently, it follows that $N_G(X) \to \infty$ as $X \to \infty$ in (2.2), when $G(t)$ has no local obstructions. Hence, we have the following immediate corollary of Theorem 2.11.

Corollary 2.14. *Let $G(t) \in \mathbb{Z}[t]$, and suppose that $G(t)$ factors into a product of distinct non-constant polynomials $\gamma_i(t) \in \mathbb{Z}[x]$ that are irreducible over $\mathbb{Z}$, such that the degree of each $\gamma_i(t)$ is at most 3. To avoid the situation when $C_G = 0$ (in (2.3)), we suppose further that $G(t)$ has no local obstructions. Then there exist infinitely many primes p such that $G(p)$ is squarefree.*

The following lemma, which generalizes a discussion found in [27], will be useful in the proof of Theorem 1.1.

Lemma 2.15. *Let $G(t) \in \mathbb{Z}[t]$ with $\deg(G) = N$, and suppose that $G(t)$ factors into a product of distinct non-constant polynomials that are irreducible over $\mathbb{Z}$, such that the degree of each factor is at most 3. If $G(t)$ has an obstruction at the prime ℓ, then $\ell \leq (N_\ell + 2)/2$, where N_ℓ is the number of not-necessarily distinct non-constant linear factors of $G(t)$ in $\mathbb{F}_\ell[t]$.*

Proof. Since no factors of $G(t)$ in $\mathbb{Z}[t]$ are constant, we can assume that the content of every factor of $G(t)$ is 1. Furthermore, since a nonlinear factor of $G(t) \pmod{\ell}$ never has a zero in $\left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^*$, we can also assume, without loss of generality, that $G(t)$ factors completely into N, not-necessarily distinct, non-constant linear factors in $\mathbb{Z}[t]$. Thus,

$$G(t) \equiv c \prod_{j=0}^{\ell-1} (t-j)^{e_j} \pmod{\ell}, \tag{2.4}$$

where $c \not\equiv 0 \pmod{\ell}$, $e_j \geq 0$ for each j and $N = \sum_{j=0}^{\ell-1} e_j$. Observe that if $e_j = 0$ for some $j \neq 0$ in (2.4), then $G(j) \not\equiv 0 \pmod{\ell^2}$, contradicting the fact that $G(t)$ has an obstruction at the prime ℓ. If $e_j = 1$ for some $j \neq 0$ in (2.4), then the zero j of $x - j \pmod{\ell}$ lifts to the unique zero j of $x - j \pmod{\ell^2}$. Thus, $G(j + \ell) \not\equiv 0 \pmod{\ell^2}$, again contradicting the fact that $G(t)$ has an obstruction at the prime ℓ. Hence, $e_j \geq 2$ for all $j \in \{1, 2, \dots, \ell - 1\}$. Assume, by way of contradiction, that $\ell > (N+2)/2$. Then

$$2(\ell - 1) > N = \sum_{j=0}^{\ell-1} e_j = e_0 + \sum_{j=1}^{\ell-1} e_j \geq e_0 + 2(\ell - 1),$$

which is impossible, and the proof is complete. □

3. The Proof of Theorem 1.1

In certain situations of the proof of item (2) of Theorem 1.1, it will be convenient to examine the monogenicity of

$$g(x) := x^4 + ax^3 + bx^2 + ax + 1, \tag{3.1}$$

in light of the fact that

$$\text{if } g(x) \text{ is not monogenic, then } \mathcal{G}(x) = g(x^2) \text{ is not monogenic.} \tag{3.2}$$

Throughout this section, we let $\mathcal{G}(x)$ be as defined in (1.3), and we let W_1, W_2 and W_3 be as defined in (2.1). Straightforward computations reveal that

$$\Delta(g) = (b+2-2a)(b+2+2a)(a^2-4b+8)^2 = W_1W_2W_3^2 \quad \text{and} \quad \Delta(\mathcal{G}) = 2^8\Delta(g)^2.$$

Before we present the proof of Theorem 1.1, we prove some lemmas that will be useful for the proof of item (2) of Theorem 1.1. The first lemma follows from [27, Theorem 1.1].

Lemma 3.1. *If*

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

and $W_1W_2W_3$ is squarefree, then $\mathcal{G}(x)$ is monogenic.

Lemma 3.2.

(1) If there exists a prime q, such that $q^2 \mid W_1$ or $q^2 \mid W_2$, then $\mathcal{G}(x)$ is not monogenic.
(2) If W_1 and W_2 are squarefree and there exists a prime $q \geq 3$ such that $q^2 \mid W_3$, then $\mathcal{G}(x)$ is not monogenic.
(3) Suppose that W_1 and W_2 are squarefree, and that W_3 is not divisible by the square of an odd prime. If $(a \bmod 4,\ b \bmod 4) \in \{(0,1),(2,3)\}$, then $\mathcal{G}(x)$ is not monogenic.

Proof. For all items of the lemma, it is enough, by (3.2), to show that $g(x)$, as defined in (3.1), is not monogenic.

We begin with item (1), and we assume that $q^2 \mid W_1$. We present details only in this case since the case $q^2 \mid W_2$ is similar. Because $q^2 \mid W_1$, it follows that $b \equiv 2a - 2 \pmod q$ and

$$g(x) \equiv x^4 + ax^3 + (2a-2)x^2 + ax + 1 \equiv (x+1)^2 g_1(x) \pmod q,$$

where $g_1(x) = x^2 + (a-2)x + 1$ with $\Delta(g_1) = a(a-4)$. The three possibilities for the quadratic polynomial $g_1(x)$ over $\mathbb{F}_q$ are:

$$g_1(x) \text{ is irreducible,} \tag{3.3}$$
$$g_1(x) \text{ has a double zero,} \tag{3.4}$$
$$g_1(x) \text{ has two distinct zeros.} \tag{3.5}$$

We use Theorem 2.8 with the prime q and $T(x) := g(x)$ to show in each of these possibilities that $x+1$ divides $\gcd(\overline{F}, \overline{h_1}, \overline{h_2})$.

For possibility (3.3), we can let

$$h_1(x) = (x+1)g_1(x) \quad \text{and} \quad h_2(x) = x+1.$$

Then

$$\begin{aligned} qF(x) &= h_1(x)h_2(x) - T(x) = (x+1)^2 g_1(x) - g(x) \\ &= -(b+2-2a)x^2 \equiv 0 \pmod{q^2}, \end{aligned}$$

from which we conclude that $g(x)$ is not monogenic.

For possibility (3.4), we have that

$$g_1(x) \equiv \begin{cases} (x+1)^2 \pmod{q} & \text{if and only if } q \mid (a-4) \\ (x-1)^2 \pmod{q} & \text{if and only if } q \mid a. \end{cases}$$

Thus, we can choose $h_1(x)$ and $h_2(x)$ so that

$$h_1(x)h_2(x) = \begin{cases} (x+1)^4 & \text{if and only if } q \mid (a-4), \\ (x+1)^2(x-1)^2 & \text{if and only if } q \mid a, \end{cases}$$

and

$$qF(x) = \begin{cases} -((a-4)x^2 + (b-6)x + a - 4) & \text{if and only if } q \mid (a-4) \\ -(ax^2 + (b+2)x + a) & \text{if and only if } q \mid a. \end{cases}$$

Since, for both of these cases, we have that

$$qF(-1) = b + 2 - 2a \equiv 0 \pmod{q^2},$$

it follows that $g(x)$ is not monogenic for this possibility.

Finally, for possibility (3.5), suppose that $g_1(x) \equiv (x-c)(x-d) \pmod{q}$, with $c \not\equiv d \pmod{q}$. Note that

$$g_1(-1) = (-1)^2 + (a-2)(-1) + 1 = -(a-4) \not\equiv 0 \pmod{q},$$

so that $c \not\equiv -1 \pmod{q}$ and $d \not\equiv -1 \pmod{q}$. Then, we can let

$$h_1(x) = (x+1)(x-c)(x-d) \quad \text{and} \quad h_2(x) = x+1.$$

Then,

$$h_1(x)h_2(x) = (x+1)^2(x-c)(x-d),$$

so that

$$\begin{aligned} qF(x) &= (x+1)^2(x-c)(x-d) - g(x) \\ &= (-c+2-a-d)x^3 + (-2c+1+dc-2d-b)x^2 \\ &\quad + (-d+2dc-a-c)x + dc - 1. \end{aligned}$$

Observe then that

$$qF(-1) = -(b+2-2a) \equiv 0 \pmod{q^2}.$$

Hence, $g(x)$ is not monogenic in this possibility as well, and the proof of item (1) is complete.

We turn next to item (2), and we let $q \geq 3$ be a prime divisor of $W_3 = a^2 - 4b + 8$ such that $q^2 \mid W_3$. Then $b \equiv (a^2+8)/4 \pmod{q}$ and

$$g(x) \equiv (x^2 + (a/2)x + 1)^2 \pmod{q}.$$

We consider the three possibilities for the polynomial

$$g_1(x) := x^2 + (a/2)x + 1 \in \mathbb{F}_q[x] : \tag{3.6}$$

(1) $g_1(x)$ is irreducible,
(2) $g_1(x)$ has a double zero,
(3) $g_1(x)$ has two distinct zeros.

We use Theorem 2.8 with the prime q and $T(x) := g(x)$ to examine each of these possibilities.

If $g_1(x)$ is irreducible in $\mathbb{F}_q[x]$, then we can let

$$h_1(x) = h_2(x) = x^2 + \left(\frac{q^2+1}{2}\right)ax + 1 \in \mathbb{Z}[x],$$

so that

$$\begin{aligned} qF(x) &= h_1(x)h_2(x) - T(x) \\ &= \left(x^2 + \left(\frac{q^2+1}{2}\right)ax + 1\right)^2 - g(x) \\ &= -x\left(-aq^2x^2 + \left(b - 2 - \frac{(q+1)^2}{4}a^2\right)x - aq^2\right) \\ &\equiv \left(\frac{a^2 - 4b + 8}{4}\right)x^2 \pmod{q^2} \\ &\equiv 0 \pmod{q^2}. \end{aligned}$$

Hence, $g(x)$ is not monogenic.

Suppose next that $g_1(x)$ has a double zero in $\mathbb{F}_q[x]$. Then $q \mid (a^2 - 16)$, since $\Delta(g_1) = (a^2-16)/4$. Thus, $q \mid (b-6)$ since $a^2 - 16 - (a^2 - 4b + 8) = 4(b-6)$ and $q \geq 3$. Consequently,

$$W_1W_2 = (b+2)^2 - 4a^2 \equiv (b+2)^2 - 4(4b-b) \equiv (b-6)^2 \equiv 0 \pmod{q^2}.$$

Hence, since W_1 and W_2 are squarefree, it follows that $q \mid \gcd(W_1, W_2)$. Then $q \mid a$, since q divides $W_1 - W_2 = -4a$, and $q \geq 3$. Thus, q divides $a^2 - (a^2-16) = 16$, which contradicts the fact that $q \geq 3$. Therefore, $g_1(x)$ never has a double zero in $\mathbb{F}_q[x]$ when $q \geq 3$.

Next, with $g_1(x)$ as defined in (3.6), suppose that $g_1(x) \equiv (x-c)(x-d) \pmod{q}$, where $c \not\equiv d \pmod{q}$. Then

$$x^2 + \left(\frac{q^2+1}{2}\right)ax + 1 = (x-c)(x-d) - qr(x),$$

for some linear polynomial $r(x) \in \mathbb{Z}[x]$. Thus, with $T(x) = g(x)$ and

$$h_1(x) = h_2(x) = (x-c)(x-d) = x^2 + \left(\frac{q^2+1}{2}\right)ax + 1 + qr(x),$$

a straightforward computation reveals that

$$\begin{aligned} F(x) &= \frac{h_1(x)h_2(x) - T(x)}{q} \\ &= aqx^3 + \left(\frac{a^2-4b+8}{q} + \frac{a^2(q^3+2q)}{4} + 2r(x)\right)x^2 \\ &\qquad + (aq^2r(x) + aq + ar(x))x + qr(x)^2 + 2r(x) \\ &\equiv 2r(x)\left(x^2 + \left(\frac{a}{2}\right)x + 1\right) \pmod{q} \\ &\equiv 2r(x)(x-c)(x-d) \pmod{q}, \end{aligned}$$

which implies that $\gcd(\overline{F}, \overline{h_1}) \neq 1$. Hence, again, $g(x)$ is not monogenic, and the proof of item (2) is complete.

Finally, we consider item (3). Since $2 \mid a$, it follows that $2 \mid W_3$, so that $2 \mid \Delta(g)$. Then, we apply Theorem 2.8 with $T(x) := g(x)$ and $q = 2$. Since $(a \bmod 4,\ b \bmod 4) \in \{(0,1),(2,3)\}$, we have that $\overline{T}(x) = (x^2+x+1)^2$. Therefore, we can let $h_1(x) = h_2(x) = x^2 + x + 1$ since $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. Hence,

$$\begin{aligned} F(x) &= \frac{h_1(x)h_2(x) - T(x)}{q} \\ &= \frac{(x^2+x+1)^2 - g(x)}{2} \\ &= -x\left(\left(\frac{a}{2}\right)x^2 + \left(\frac{b-1}{2}\right)x + \frac{a}{2}\right) \\ &\equiv \begin{cases} 0 \pmod 2 & \text{if } (a \bmod 4,\ b \bmod 4) = (0,1) \\ x(x^2+x+1) \pmod 2 & \text{if } (a \bmod 4,\ b \bmod 4) = (2,3). \end{cases} \end{aligned}$$

Thus, we see in either case, that $\gcd(\overline{F}, \overline{h_1}) \neq 1$ so that $g(x)$ is not monogenic, and the proof of the lemma is complete. □

Proof of Theorem 1.1. We follow closely the classifications given in Theorems 2.3, 2.4, 2.5, 2.6 and 2.7. To determine the monogenic polynomials, we use Theorem 2.9 for the proof of item (1), and Theorem 2.8 for the proof of item (2).

We begin with the proof of item (1). From Theorem 2.2, we have that

$$\Delta(\mathcal{F}) = 2^{16}b^3(a^2-4b)^4. \tag{3.7}$$

We see from the classification for $\mathcal{F}(x)$ given in Theorem 2.3, Theorem 2.4 and Theorem 2.5 that $X_{\mathcal{F}}$ in (1.4) can be partitioned into the two sets

$$X_{\mathcal{F}}^{\square} = \{2,3,4,9,11,22\} \quad \text{and} \quad X_{\mathcal{F}}^{\not\square} = \{6,8,15,16,17,26\}, \tag{3.8}$$

where each element in $X_{\mathcal{F}}^{\square}$ arises from polynomials $\mathcal{F}(x)$ with b a square, while each element in $X_{\mathcal{F}}^{\not\square}$ arises from polynomials $\mathcal{F}(x)$ with b not a square. This partitioning is useful for the following reason. Suppose that b is a square, and q is a prime that divides b. We see then that condition (1) of Theorem 2.9 is false if $q \mid a$, while condition (3) of Theorem 2.9 is false if $q \nmid a$. Thus, the only possible monogenic polynomials in these cases must have $b = 1$. Consequently, we have immediately that the situations in the classification where b is a square and $\sqrt{b}$ is not a square (see Theorem 2.4) have no monogenic polynomials $\mathcal{F}(x)$. In particular, there are no monogenic polynomials $\mathcal{F}(x)$ having Galois group 8T11 or 8T22.

We systematically proceed through the values of X in $X_{\mathcal{F}} \setminus \{11, 22\}$, beginning with the values of X in $X_{\mathcal{F}}^{\square} \setminus \{11, 22\}$ given in (3.8).

3.1. Values of X in $X_{\mathcal{F}}^{\square} \setminus \{11, 22\}$. We assume that $b = 1$, and we use Theorem 2.3.

X=2. We assume that $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T2. Then, from Theorem 2.3, we have that $-a^2 + 4$ is a square. If q is an odd prime prime dividing $-a^2 + 4$, we have that $q \nmid 2a$, and we conclude that condition (5) of Theorem 2.9 is false since $-a^2 + 4$ is a square. Thus, we must have that $-a^2 + 4 = 2^{2m}$, for some integer $m \geq 0$. Therefore,

$$4 - 2^{2m} = a^2 \geq 0,$$

which implies that $m = 1$ and $a = 0$. Hence, the only monogenic polynomial is this case is the cyclotomic polynomial $\Phi_{16}(x) = x^8 + 1$.

X=3. We assume that $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T3. By Theorem 2.3, we have that $a + 2$ is a square. Suppose that q is an odd prime dividing $a + 2$. Then $q \nmid 2a$, and since $a + 2$ is a square, we deduce that $q^2 \mid (a^2 - 4)$, making condition (5) of Theorem 2.9 false.

Hence, $a + 2 = 2^{2m}$, for some integer $m \geq 0$. If $m \geq 1$, then $2 \mid a$, but $4 \nmid a$. Thus, $2 \nmid a_2$ and $b_1 = 1$. Since

$$a_2 \left(a_2^2 - (-1)^2\right) \equiv 0 \pmod 2,$$

we conclude that condition (2) of Theorem 2.9 is false. If $m = 0$, then $a = -1$, and it is easy to check that $\mathcal{F}(x) = x^8 - x^4 + 1$ is indeed monogenic. Therefore, there is exactly one monogenic polynomial in this situation.

X=4. We assume that $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T4. Using Theorem 2.3, the approach is similar to X=3, and so we omit the details. The only monogenic in this case is $\mathcal{F}(x) = x^8 + 3x^4 + 1$.

X=9. We employ a slightly different strategy here. Let $G(t) = (4t+1)(4t+5)$. We claim that $G(t)$ has no obstructions. By Lemma 2.15, we only have to check for obstructions at the prime $\ell = 2$, which is easily confirmed since $G(1) \not\equiv 0 \pmod 4$. Hence, by Corollary 2.14, there exist infinitely many primes p such that $G(p)$ is squarefree. Let p be such a prime. We claim that $\mathcal{F}(x) = x^8 + (4p+3)x^4 + 1$ is monogenic with $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T9. We see from [27, Lemma 3.1] that $\mathcal{F}(x)$ is irreducible. Since $(4p+1)(4p+5)$ is squarefree, it follows from Theorem 2.3 that $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T9. We use Theorem 2.9 to verify that $\mathcal{F}(x)$ is monogenic. Note that

$$\Delta(\mathcal{F}) = 2^{16}(4p+1)^4(4p+5)^4$$

from (3.7). If q is an odd prime dividing $\Delta(\mathcal{F})$, then $q \nmid 2(4p+3)$; and every condition of Theorem 2.9 is true, including condition (5) since $(4p+1)(4p+5)$ is squarefree. If $q = 2$, then $2 \nmid (4p+3)$ and we need to check condition (4) of Theorem 2.9. An easy calculation reveals that

$$H_2(x) = \frac{(4p+3)x^4 + 1 + (-(4p+3)x - 1)^4}{2} \equiv (x+1)^2 \pmod 2.$$

Since $H_1(x) = x^2 + (4p+3)x + 1 \equiv x^2 + x + 1 \pmod 2$ is irreducible in $\mathbb{F}_2[x]$, we deduce that condition (4) of Theorem 2.9 is true. Thus, $\mathcal{F}(x)$ is monogenic. By equating discriminants, Maple confirms that there does not exist a prime p' such that the octic field generated by $x^8 + (4p'+3)x^4 + 1$ is isomorphic to the octic field generated by $\mathcal{F}(x) = x^8 + (4p+3)x^4 + 1$. Thus, the set of all such $\mathcal{F}(x)$, where $(4p+1)(4p+5)$ is squarefree does indeed represent an infinite family of distinct monogenic 8T9-octic trinomials.

Remark 3.3. We point out to the reader that the family of monogenic polynomials described above does not constitute all monogenic polynomials $\mathcal{F}(x) = x^8 + ax^4 + b$ with $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T9. Indeed, if $t \neq 0$ and $4t^2 - 1$ is squarefree, it can be shown via the techniques used here that the polynomial $f_t(x) = x^8 + 4tx^4 + 1$ is monogenic with $\mathrm{Gal}(f_t) \simeq$ 8T9, yielding another such infinite family.

3.2. Values of X in $X_{\mathcal{F}}^{\square}$.

We turn now to values of X in $X_{\mathcal{F}}^{\square}$ given in (3.8). We assume that b is not a square, and we use Theorem 2.5.

X=6. Following Theorem 2.5, we suppose that neither $b(a^2 - 4b)$ nor $4b - a^2$ is a square, and that $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T6. Then one of

$$2\sqrt{-b}, \quad 4b + 2\sqrt{-b(a^2-4b)}, \quad 4b - 2\sqrt{-b(a^2-4b)} \tag{3.9}$$

is a nonzero square.

We consider the three possibilities in (3.9) one at a time, but first we make the following useful observation. Suppose that q is a prime such that $q^2 \mid b$. If $q \mid a$, then condition (1) of Theorem 2.9 is false. If $q \nmid a$, then $b_2 = b/q \equiv 0 \pmod q$, which implies that condition (3) of Theorem 2.9 is false. Hence, if $\mathcal{F}(x)$ is monogenic, then b must be squarefree. Thus, since $-b$ is squarefree, we see easily that the first possibility in (3.9) is impossible.

Suppose next that $4b + 2\sqrt{-b(a^2-4b)}$ is a nonzero square, which implies that $-b(a^2-4b)$ is a square. Let

$$d := \gcd(-b, a^2-4b).$$

Consider first the case when $-b > 0$. If $d = 1$, then a^2-4b is a square, since $-b(a^2-4b)$ is a square, which yields the contradiction that $\mathcal{F}(x) = (x^4)^2 + a(x^4) + b$ is reducible. Thus, $d > 1$. Suppose that d has exactly $n \geq 1$ distinct prime divisors $r_1 < r_2 < \cdots < r_n$. Then $d = \prod_{i=1}^{n} r_i$ since b is squarefree. Futhermore, since $-b(a^2-4b)$ is a square and $\gcd(-b/d, (a^2-4b)/d) = 1$, it follows that

$$-b = d \quad \text{and} \quad a^2 - 4b = Sd,$$

where S is a square. Thus,

$$a^2 = (S-4)d, \tag{3.10}$$

which implies that $S \geq 4$. Let q be a prime divisor of S, so that $q^2 \mid (a^2-4b)$ since S is a square. Suppose that $q \geq 3$. Observe that if $q \mid a$ or $q \mid b$, then $q^2 \mid b$, which contradicts the fact that b is squarefree. Therefore, it must be that $q = 2$, and we can assume that $S = 2^{2k}$, for some integer $k \geq 1$. Thus, $2 \mid a$, and we have from (3.10) that

$$(a/2)^2 = d(4^{k-1} - 1). \tag{3.11}$$

Suppose that $2 \mid b$. Then $r_1 = 2$ and

$$(a/2)^2 = 2\left(\prod_{i=2}^{n} r_i\right)\left(4^{k-1}-1\right). \tag{3.12}$$

If $k > 1$, then $4^{k-1} - 1 \not\equiv 0 \pmod 2$ which implies that (3.12) is impossible, since the right-hand side of (3.12) is not a square. If $k = 1$, then $a = 0$, $-b(a^2-4b) = 4d^2$ and

$$4b + 2\sqrt{-b(a^2-4b)} = -4d + 2(2d) = 0, \tag{3.13}$$

contradicting the fact that $4b + 2\sqrt{-b(a^2-4b)}$ is a nonzero square.

We conclude therefore that $2 \nmid b$. It $k > 1$, then we see from (3.34) that $2 \,||\, a$ and $(a/2)^2 \equiv b \equiv 1 \pmod 4$. Thus, condition (3) of Theorem 2.9 is false since

$$\frac{a}{2} \equiv 1 \pmod 2 \quad \text{and} \quad -b\left(\frac{a}{2}\right)^2 - \left(-\frac{b+b^8}{2}\right)^2 \equiv 0 \pmod 2.$$

It follows that there are no monogenic polynomials $\mathcal{F}(x)$ in the case when $-b > 0$.

Consider next the case that $b > 0$. Then $4b - a^2 > 0$, and since $-b(a^2-4b) = b(4b-a^2)$ is a square, we get the contradiction that b is a square if $d = 1$. Hence, $d > 1$. Arguing as in the case $-b > 0$, we arrive at

$$(a/2)^2 = (1 - 4^{k-1})d. \tag{3.14}$$

Thus, $k = 1$ and $a = 0$. Then

$$4b + 2\sqrt{b(4b - a^2)} = 8b,$$

which implies that $b = 2$ since $8b$ is a nonzero square and b is squarefree. It is straightforward to verify that $\mathcal{F}(x) = x^8 + 2$ is monogenic and $\mathrm{Gal}(\mathcal{F}) \simeq$8T6. Thus, there is only one mongenic polynomial $\mathcal{F}(x)$ in this case.

The arguments for the final possibility from (3.9) are similar to the previous possibility, and so we omit the details. No further monogenic polynomials exist for this possibility.

X=8. Following Theorem 2.5, we assume that none of b, $b(a^2-4b)$ and $4b-a^2$ is a square, that either $-b$ or $-b(a^2-4b)$ is a square, and that $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T8. Then either

$$2(a^2-4b)\sqrt{-b} \quad \text{or} \quad -4b + 2\sqrt{-b(a^2-4b)}$$

is a nonzero square.

We assume first that $2(a^2-4b)\sqrt{-b}$ is a nonzero square. Then $-b$ is a square. Suppose that q is a prime dividing b. Then $q^2 \mid b$. Thus, condition (1) of Theorem 2.9 is false if $q \mid a$, while condition (3) of Theorem 2.9 is false if $q \nmid a$. Hence, $b = -1$, and $2(a^2+4)$ is a square. Suppose that $q \geq 3$ is a prime divisor of a^2+4. Then $q^2 \mid (a^2+4)$ and $q \nmid 2a$, which implies that condition (5) of Theorem 2.9 is false. Therefore, we may assume that $a^2+4 = 2^k$, for some odd integer $k \geq 3$. Then, if $k > 3$, we have that

$$(a/2)^2 = 2^{k-2} - 1 \equiv 3 \pmod 4,$$

which is impossible. Hence, $k = 3$ and $a = \pm 2$. It is easy to verify that the two trinomials $\mathcal{F}(x) = x^8 \pm 2x^4 - 1$ are indeed monogenic and $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T8. However, Magma confirms that they generate isomorphic octic fields, distinct from the octic field generated by $\mathcal{F}(x) = x^8 - 2$.

Next, we assume that $-4b + 2\sqrt{-b(a^2-4b)}$ is a nonzero square. It follows that $-b(a^2-4b)$ is a square. Suppose that q is a prime divisor of b. If $q^2 \mid b$, then condition (1) of Theorem 2.9 is false if $q \mid a$, while condition (3) of Theorem 2.9 is false if $q \nmid a$. Hence, we assume that b is squarefree. Thus, if $2 \mid b$, then $2 \mid (a^2-4b)$ since $-b(a^2-4b)$ is a square. Hence, $2 \mid a$. Suppose that $2 \nmid b$. If $2 \nmid a$, then $-b(a^2-4b) \equiv 1 \pmod 4$, so that

$$-4b + 2\sqrt{-b(a^2-4b)} \equiv 2 \pmod 4,$$

which is impossible since $-4b + 2\sqrt{-b(a^2-4b)}$ is a square. Hence, $2 \mid a$ for any value of b. Also, if $b > 0$, then $4b^2 - a^2b < 4b^2$, so that

$$-4b + 2\sqrt{-b(a^2-4b)} < -4b + 2\sqrt{4b^2} = 0,$$

which is impossible since $-4b + 2\sqrt{-b(a^2-4b)}$ is a square. Thus, $b < 0$.

Next, let $q \geq 3$ be a prime divisor of a^2-4b, and suppose that $q^2 \mid (a^2-4b)$. Observe that if $q \mid a$ or $q \mid b$, then $q^2 \mid b$, which contradicts the fact that b is

squarefree. Hence, since $2 \mid a$, we have that

$$a^2 - 4b = 2^k \quad \text{or} \quad a^2 - 4b = 2^k \prod_{i=1}^{n} r_i,$$

where $k \geq 2$, $n \geq 1$ and the r_i are distinct odd primes. Note that if $a^2 - 4b = 2^k$ with $2 \mid k$, then $-b = 1$ since b is squarefree and $-b(a^2 - 4b)$ is a square, which contradicts the fact that $-b$ is not a square. Therefore, we have that $2 \nmid k$ for the possibility $a^2 - 4b = 2^k$. Hence, since

$$-b(a^2 - 4b) = -b\left(2^k \prod_{i=1}^{n} r_i\right),$$

is a square, it follows that the possibilities for $-b$ are

$$-b \in \left\{2, \quad 2\prod_{i=1}^{n} r_i, \quad \prod_{i=1}^{n} r_i\right\}.$$

The possibility $-b = 2$ occurs if $a^2 - 4b = 2^k$, where $2 \nmid k$. That is, we have $a^2 = 2^3(2^{k-3} - 1)$, which implies that $k = 3$, $a = 0$ and $\mathcal{F}(x) = x^8 - 2$. It is easily verified that $\mathcal{F}(x)$ is monogenic with $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}8$.

The next possibility is $-b = 2\prod_{i=1}^{n} r_i$ yields

$$a^2 = 2^2(-2b)\left(2^{k-3} - 1\right),$$

which implies that $k = 3$ and $a = 0$. But then,

$$-4b + 2\sqrt{-b(a^2 - 4b)} = 2^3(-2b),$$

which contradicts the fact that $-4b + 2\sqrt{-b(a^2 - 4b)}$ is a square. Hence, there are no monogenic polynomials for this possibility.

The last possibility is $-b = \prod_{i=1}^{n} r_i$. In this case, we have that

$$a^2 = 2^2(-b)\left(2^{k-2} - 1\right)$$

and

$$-4b + 2\sqrt{-b(a^2 - 4b)} = 2^2(-b)\left(2^{(k-2)/2} + 1\right).$$

Hence,

$$A := (-b)\left(2^{k-2} - 1\right) \quad \text{and} \quad B := (-b)\left(2^{(k-2)/2} + 1\right),$$

are squares. Thus, AB is a square, which implies that

$$\left(2^{k-2} - 1\right)\left(2^{(k-2)/2} + 1\right) = \left(2^{(k-2)/2} - 1\right)\left(2^{(k-2)/2} + 1\right)^2,$$

is a square, which in turn implies that $2^{(k-2)/2} - 1$ is a square. By Theorem 2.1, it follows that $k \in \{2, 4\}$. When $k = 2$, we get that $B = -2b$, which contradicts the fact that B is a square. When $k = 4$, we get that $b = -3$, $a = \pm 6$ and $\mathcal{F}(x) = x^8 \pm 6x^4 - 3$. Although $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}8$ for both of these polynomials,

neither one is monogenic, which can be seen in the following way. Observe that $2 \mid a$ and $2 \nmid b$. Hence, since

$$a_2 = a/2 \equiv 1 \pmod 2 \quad \text{and} \quad b_1 = \frac{-b + (-b)^8}{2} = \frac{-3 + (-3)^8}{2} \equiv 1 \pmod 2,$$

we see that $-ba_2^2 - b_1^2 \equiv 0 \pmod 2$, and therefore, condition (2) of Theorem 2.9 is false with $q = 2$.

In conclusion, there are exactly two monogenic polynomials

$$\mathcal{F}(x) \in \{x^8 - 2x^4 - 1, \quad x^8 - 2\}$$

with $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}8$.

X=15. Following Theorem 2.5, we assume that none of b, $b(a^2-4b)$ and $4b-a^2$ is a square, and that $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}15$. Then, either $-b$ or $-b(a^2-4b)$ is a square, and none of

$$2\sqrt{-b}, \quad 2(a^2-4b)\sqrt{-b}, \quad 4b + 2\sqrt{-b(a^2-4b)},$$
$$4b - 2\sqrt{-b(a^2-4b)}, \quad -4b + 2\sqrt{-b(a^2-4b)}$$

is a nonzero square.

We assume first that $-b$ is a square. Suppose that q is a prime dividing b. Then $q^2 \mid b$. Thus, condition (1) of Theorem 2.9 is false if $q \mid a$, while condition (3) of Theorem 2.9 is false if $q \nmid a$. Hence, $b = -1$. Let $D := a^2 + 4$, and let $q \geq 3$ be a prime divisor of D. Note that $q \nmid 2a$. If $q^2 \mid D$, then condition (5) of Theorem 2.9 is false. Thus, we may assume that $D/2^{\nu_2(D)}$ is squarefree. If $4 \mid a$, then $a_2 \equiv 0 \pmod 2$, and since $b_1 = 0$, we see that condition (2) of Theorem 2.9 is false with $q = 2$. Hence, we can also assume that $4 \nmid a$. Thus,

$$D = \begin{cases} \prod_{i=1}^n r_i & \text{if } a \equiv 1 \pmod 2 \\ 2^3 \prod_{i=1}^n r_i & \text{if } a \equiv 2 \pmod 4, \end{cases} \tag{3.15}$$

where $n \geq 1$ and the r_i are distinct odd primes. Define

$$G(t) := \begin{cases} t^2 + 4 & \text{if } a \equiv 1 \pmod 2 \\ t^2 + 1 & \text{if } a \equiv 2 \pmod 4. \end{cases} \tag{3.16}$$

By Lemma 2.15, we only have to check for obstructions at the prime $\ell = 2$. Since $G(1) \not\equiv 0 \pmod 4$ in each case of $G(t)$ in (3.16), we deduce that $G(t)$ has no obstructions. Hence, from Corollary 2.14, it follows that there exist infinitely many values of a, in each case of a in (3.15), for which such a value of D exists.

We claim if $4 \nmid a$, $b = -1$ and D is as defined in (3.15), together with the restrictions set forth above from Theorem 2.5, then $\mathcal{F}(x) = x^8 + ax^4 - 1$ is monogenic with $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}15$. From (3.7), we have that $\Delta(\mathcal{F}) = -2^{16}D^4$. To establish the claim, suppose first that q is a prime divisor of D. If $q \geq 3$, then $q \nmid 2ab$, and it is easy to see that condition (5) and, consequently, all other conditions of Theorem 2.9 are true for q. If $q = 2$, then $2 \mid a$ and we see that

$2 \nmid a_2$ and $2 \nmid (a_2^2 - b_1^2)$ since $b_1 = 0$. Hence, in particular, condition (2) of Theorem 2.9 is true, and so all conditions of Theorem 2.9 are true. Finally, suppose that $q = 2$ and $2 \nmid D$. Then $2 \nmid a$ and we examine condition (4) of Theorem 2.9, where

$$H_1(x) := x^2 + ax - 1 \quad \text{and} \quad H_2(x) := \frac{ax^4 - 1 + (-ax + 1)^4}{2}.$$

Since $H_1(x) \equiv x^2 + x + 1 \pmod 2$ is irreducible in $\mathbb{F}_2[x]$ and

$$H_2(x) \equiv \begin{cases} x^2(x+1)^2 \pmod 2 & \text{if } a \equiv 1 \pmod 4 \\ x^2 \pmod 2 & \text{if } a \equiv 3 \pmod 4, \end{cases}$$

it follows that $H_1(x)$ and $H_2(x)$ are coprime in $\mathbb{F}_2[x]$, which establishes the claim. Moreover, this argument proves that these polynomials account for all monogenics $\mathcal{F}(x)$ with $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T15.

Finally, with $a > 0$, together with the restrictions on a set forth above, we claim that the set $\mathcal{S} := \{\mathcal{F}(x) = x^8 + ax^4 - 1\}$ is an infinite family of monogenic 8T15-octic trinomials. The additional restriction of $a > 0$ is due to the fact that the octic field generated by $x^8 - ax^4 - 1$ is isomorphic to the octic field generated by $x^8 + ax^4 - 1$. Then, comparing discriminants using Maple, it is easy to confirm that the trinomials in $\mathcal{S}$ generate distinct octic fields.

X=16. Following Theorem 2.5, we assume that b is not a square and $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T16, so that $b(a^2 - 4b)$ is a square. Let $d = \gcd(b, a^2 - 4b)$, and let q be a prime divisor of d. Then $q \mid a$. If $q^2 \mid b$, then condition (1) of Theorem 2.9 is false. Hence, we can assume that $q \,||\, b$ so that d is squarefree. Next, suppose that $q \geq 3$ is a prime dividing $\widehat{b} := b/d$, so that $q \nmid a$. If $q^2 \mid b$, then we see that condition (3) of Theorem 2.9 is false since $a_1 = 0$ and $b_2 = b/q \equiv 0 \pmod q$. Thus, we may assume that $\widehat{b}/2^{\nu_2(\widehat{b})}$ is squarefree. Next, suppose that $q \geq 3$ is a prime divisor of $\widehat{d} := (a^2 - 4b)/d$. Then $q \nmid a$ and so $q \nmid 2ab$. Hence, if $q^2 \mid \widehat{d}$, then condition (5) of Theorem 2.9 is false. Therefore, we can assume that $\widehat{d}/2^{\nu_2(\widehat{d})}$ is squarefree. Thus, since $b(a^2 - 4b)$ is a square, it follows that

$$b = d\widehat{b} = 2^c d \quad \text{and} \quad a^2 - 4b = d\widehat{d} = 2^e d \tag{3.17}$$

for some nonegative integers c and e with $c \equiv e \pmod 2$.

If $2 \mid d$, then $2 \mid a$ so that $2^2 \mid (a^2 - 4b)$. Note then that $2^2 \nmid b$, since d is squarefree. Thus, $2 \,||\, b$ and $b = d$. Hence, since $b(a^2 - 4b)$ is a square, we have that $2^3 \mid (a^2 - 4b)$, which implies that $2^4 \mid a^2$. However, $2^4 \nmid (a^2 - 4b)$ since $2 \,||\, b$. Thus, $2^3 \,||\, (a^2 - 4b)$. Therefore, in this case, we have that $c = 0$, $e = 2$ and $a^2 = 8d$, which implies that $b = d = 2$ and $a = \pm 4$. It is straightforward to verify that the two polynomials $\mathcal{F}(x) = x^8 \pm 4x^4 + 2$ are both monogenic with $\mathrm{Gal}(\mathcal{F}) \simeq$ 8T16.

Suppose next that $2 \nmid d$. There are three cases to consider:

(1) $2 \mid a$ and $2 \nmid b$,

(2) $2 \nmid a$ and $2 \mid b$,
(3) $2 \nmid a$ and $2 \nmid b$.

For case (1), we have from (3.17) that $b = d$ and

$$a^2 = 2^2(2^{e-2} + 1)d, \tag{3.18}$$

where $e \geq 2$. Observe that the right-hand side of (3.18) is not a square if $e = 2$. If $e = 3$ in (3.18), then $d = 3 = b$, $a = \pm 6$, and $b(a^2 - 4b) = 72$, contradicting the fact that $b(a^2 - 4b)$ is a square. If $e \geq 4$ in (3.18), then $4 \nmid a$ and $b \equiv 1 \pmod 4$. An examination of condition (2) of Theorem 2.9 reveals then that $2 \nmid a_2$ and $2 \nmid b_1$, so that $2 \mid (a_2((-b)a_2^2 - b_1^2)$, which implies that condition (2) is false. Thus, there are no monogenic polynomials in this case.

For case (2), we see that $2 \nmid (a^2 - 4b)$. Hence, from (3.17), we have that $b = 2^c d$, for some $c \geq 1$, and $a^2 - 4b = d$. Then, since $2 \nmid d$ and $b(a^2 - 4b) = 2^c d^2$ is a square, we deduce that $c \equiv 0 \pmod 2$ with $c \geq 2$. Thus, $2 \mid b/2$, which implies that condition (3) of Theorem 2.9 is false, and there are no monogenic polynomials in this case.

Finally, for case (3), we see from (3.17) that $b = d = a^2 - 4b$. Hence, $a^2 = 5d$, which implies that $d = b = 5$, since d is squarefree, and $a = \pm 5$. Since $2 \nmid ab$, we examine condition (4) of Theorem 2.9 with $q = 2$ for each of the two polynomials $\mathcal{F}(x) = x^8 \pm 5x^4 + 5$. For $\mathcal{F}(x) = x^8 + 5x^4 + 5$, we get

$$H_1(x) \equiv x^2 + x + 1 \pmod 2 \quad \text{and} \quad H_2(x) \equiv (x^2 + x + 1)^2 \pmod 2,$$

so that $H_1(x)$ and $H_2(x)$ are not coprime in $\mathbb{F}_2[x]$. Hence, $\mathcal{F}(x) = x^8 + 5x^4 + 5$ is not monogenic. For $\mathcal{F}(x) = x^8 - 5x^4 + 5$, we get

$$H_1(x) \equiv x^2 + x + 1 \pmod 2 \quad \text{and} \quad H_2(x) \equiv (x + 1)^2 \pmod 2,$$

so that $H_1(x)$ and $H_2(x)$ are coprime in $\mathbb{F}_2[x]$. Hence, $\mathcal{F}(x) = x^8 - 5x^4 + 5$ is monogenic with $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}16$.

Note that

$$\Delta(x^8 - 4x^4 + 2) = 2^{31} = \Delta(x^8 + 4x^4 + 2),$$

and $\Delta(x^8 - 5x^4 + 5) = 2^{16}5^7$, so that the octic field generated by $x^8 - 5x^4 + 5$ is distinct from the other two. All zeros of $x^8 - 4x^4 + 2$ are real, while all zeros of $x^8 + 4x^4 + 2$ are non-real, and Magma confirms that the respective octic fields are not isomorphic. Therefore, in summary, there are exactly three monogenic polynomials

$$\mathcal{F}(x) \in \{x^8 - 4x^4 + 2, \quad x^8 + 4x^4 + 2, \quad x^8 - 5x^4 + 5\}$$

with $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}16$.

X=17. Following Theorem 2.5, we assume that b is not a square and $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}17$, so that $b(a^2 - 4b)$ is not a square and $4b - a^2$ is a square. Note then that $a \neq 0$ since b is not a square. Let $d = \gcd(b, 4b - a^2)$. Suppose that $d > 1$ and let q be a prime divisor of d. Then $q \mid a$. If $q^2 \mid b$, then condition (1) of Theorem 2.9 is false. Hence, we can assume that $q \,||\, b$, so that d is squarefree. Furthermore, if $q \geq 3$, then since $q^2 \mid a^2$ and $q \,||\, b$, it follows that $q^2 \nmid (4b - a^2)$, contradicting the fact that $4b - a^2$ is a square. Thus, $d \in \{1, 2\}$.

Since

$$4b - a^2 \equiv -a^2 \pmod 4,$$

and $4b - a^2$ is a square, it follows that $2 \mid a$ and $b - (a/2)^2$ is a square. Suppose that $2 \mid (b - (a/2)^2)$. If $2 \mid (a/2)$, then $2^2 \mid (a/2)^2$. But $2^2 \nmid b$ so that $2^2 \nmid (b - (a/2)^2)$, contradicting the fact that $b - (a/2)^2$ is a square. Thus, $2 \nmid (a/2)$ and $2 \nmid b$. Then, $(a/2)^2 \equiv 1 \pmod 4$, and since $2 \mid (b - (a/2)^2)$ and $b - (a/2)^2$ is a square, we deduce that $2^2 \mid (b - (a/2)^2)$ so that $b \equiv 1 \pmod 4$. Then,

$$b_1 = \frac{b + (-b)^8}{2} \equiv 1 \pmod 4$$

and

$$(-b)(a/2)^2 - b_1^2 \equiv 0 \pmod 2,$$

which implies that condition (2) of Theorem 2.9 is false. Hence, we can assume that $2 \nmid (b - (a/2)^2)$, and therefore, $2^2 \,||\, (4b - a^2)$.

Next, suppose that $q \geq 3$ is a prime divisor of $4b - a^2$. We have shown above that $q \nmid b$, and therefore $q \nmid a$. Thus $q \nmid 2ab$. However, since $4b - a^2$ is a square, we have that $q^2 \mid (4b - a^2)$. Thus, condition (5) of Theorem 2.9 is false. Hence, for the monogenicity of $\mathcal{F}(x)$, we must have that $4b - a^2 = 4$.

Consequently, we have shown that if $\mathcal{F}(x) = x^8 + ax^4 + b$ is monogenic with $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}17$, then $a = 2t$ and $b = t^2 + 1$, for some integer $t \neq 0$. In fact, with $t \neq 0$, we claim that

$$\mathcal{F}(x) = x^8 + 2tx^4 + t^2 + 1 \text{ is monogenic if and only if } t^2 + 1 \text{ is squarefree.} \tag{3.19}$$

To establish (3.19), we begin by noting that $\mathcal{F}(x) = x^8 + 2tx^4 + t^2 + 1$ is irreducible by [12, Lemma 3.4] if $t^2 + 1$ is squarefree, since

$$(2t \bmod 4,\ t^2 + 1 \bmod 4) \in \{(0, 1), (2, 2)\}$$

and $t^2 + 1 \geq 2$. Note, by (3.7), that

$$\Delta(\mathcal{F}) = 2^{24}(t^2 + 1)^3. \tag{3.20}$$

Observe that if $q = 2$ is a divisor of $t^2 + 1$, then, since $q \mid 2t$, condition (1) of Theorem 2.9 is false if and only if $4 \mid (t^2 + 1)$. If $q = 2$ does not divide $t^2 + 1$, then $t^2 \equiv 0 \pmod 4$, and in this case, we examine condition (2) of Theorem 2.9. We see that

$$a_2 = t \equiv 0 \pmod 2 \quad \text{and} \quad b_1 = \frac{t^2 + 1 + (-(t^2 + 1))^8}{2} \equiv 1 \pmod 2.$$

Thus, condition (2) of Theorem 2.9 is true. Suppose next that $q \geq 3$ is a prime divisor of $t^2 + 1$. Then $q \nmid 2t$. Thus, we examine condition (3) of Theorem 2.9. Since q is odd, we see that $a_1 = 0$ and therefore, the second statement under condition (3) is false. So, to determine whether condition (3) of Theorem 2.9 is true or false, we need to examine the first statement under condition (3). Thus, since $b_2 = (t^2 + 1)/q$, we see that condition (3) of Theorem 2.9 is false if and only if $q^2 \mid (t^2 + 1)$, which establishes the claim (3.19).

Since, $G(1) \not\equiv 0 \pmod 4$ for $G(t) = t^2 + 1$, we conclude from Lemma 2.15 that $G(t)$ has no local obstructions, and therefore, from Corollary 2.14, we have that there exist infinitely many values of t such that $G(t)$ is squarefree. Thus, we have shown that there exist infinitely many monogenic trinomials $\mathcal{F}(x) = x^8 + 2tx^4 + t^2 + 1$ with $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}17$. Moreover, comparing discriminants (3.20) for all such $t > 0$, we see that the octic fields they generate are distinct.

X=26. Computer evidence suggests that there is an abundance of monogenic polynomials $\mathcal{F}(x)$ with $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}26$. We use a strategy similar to the case of 8T9 to construct one infinite family. Let $\mathcal{F}(x) = x^8 + tx^4 + 3$. By (3.7), we have that

$$\Delta(\mathcal{F}) = 2^{16}3^3(t^2 - 12)^4. \tag{3.21}$$

Let $G(t) = t^2 - 12$. Since $G(1) \equiv 1 \pmod 4$, we see from Lemma 2.15 that $G(t)$ has no local obstructions. Hence, by Corollary 2.14, there exist infinitely many primes p such that $G(p)$ is squarefree. Let $p \geq 5$ be such a prime. We claim that

$$\mathcal{F}(x) = x^8 + px^4 + 3 \text{ is monogenic with } \mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}26. \tag{3.22}$$

Since

$$(p \pmod 4,\ 3 \pmod 4) \in \{(1,3),(3,3)\},$$

we have that $\mathcal{F}(x)$ is irreducible by [12, Lemma 3.4]. With $a = p$ and $b = 3$, we have that

$$\begin{aligned} b &= 3, \\ b(a^2 - 4b) &= 3(p^2 - 12) \not\equiv 0 \pmod 9, \\ 4b - a^2 &= -(p^2 - 12) < 0, \\ -b &= -3 < 0 \quad \text{and} \\ -b(a^2 - 4b) &= -3(p^2 - 12) < 0. \end{aligned}$$

Hence, it follows from Theorem 2.5 that $\mathrm{Gal}(\mathcal{F}) \simeq 8\mathrm{T}26$.

To see that $\mathcal{F}(x)$ is monogenic, first let $q = 2$. Since $2 \nmid p$, we examine condition (4) of Theorem 2.9. Then

$$\begin{aligned} H_1(x) &\equiv x^2 + x + 1 \pmod 2 \quad \text{and} \\ H_2(x) &= p(p^2 - p + 1)\left(\frac{p+1}{2}\right)x^4 + 6p^3x^3 + 27p^2x^2 + 54px + 42 \\ &\equiv x^2\left(\left(\overline{\frac{p+1}{2}}\right)x + 1\right)^2 \pmod 2. \end{aligned}$$

Hence, $H_1(x)$ and $H_2(x)$ are coprime in $\mathbb{F}_2[x]$.

Next, let $q = 3$. We examine condition (3) of Theorem 2.9. Since $a_1 = 0$ and $b_2 = 1$, we see that the first statement under condition (3) is true.

Finally, let q be a prime divisor of $p^2 - 12$. Then, $q \nmid 6p$, and we see that condition (5) of Theorem 2.9 is true since $p^2 - 12$ is squarefree. Therefore, the claim (3.22) is established.

Suppose now that p_1 and p_2 are primes with $5 \le p_1 < p_2$ such that $G(p_1)$ and $G(p_2)$ are squarefree, and that $\mathcal{F}_{p_1}(x)$ and $\mathcal{F}_{p_2}(x)$ generate isomorphic octic fields. Then, since $\mathcal{F}_{p_1}(x)$ and $\mathcal{F}_{p_2}(x)$ are both monogenic, we must have that

$$2^{16}3^3(p_1^2-12)^4 = \Delta(\mathcal{F}_{p_1}) = \Delta(\mathcal{F}_{p_2}) = 2^{16}3^3(p_2^2-12)^4, \tag{3.23}$$

which contradicts the fact that $5 \le p_1 < p_2$. We deduce that the set

$$\{\mathcal{F}(x) = x^8 + px^4 + 3 \,:\, p \ge 5 \text{ is prime with } p^2-12 \text{ squarefree}\},$$

is an infinite family of monogenic 8T26-octic trinomials $\mathcal{F}(x)$, which completes the proof of item (1).

We turn now to the proof of item (2). We recall the definition of W_1, W_2 and W_3 given in (2.1). Straightforward computations reveal that

$$\Delta(g) = (b+2-2a)(b+2+2a)(a^2-4b+8)^2 = W_1W_2W_3^2 \quad \text{and} \quad \Delta(\mathcal{G}) = 2^8\Delta(g)^2.$$

X=2. We assume that $\mathrm{Gal}(\mathcal{G}) \simeq$ 8T2. Following Theorem 2.6, we see that there are three possibilities.

Suppose first that W_1W_3 and W_2W_3 are squares, while $W_1W_2W_3$ is not a square. Then $W_1W_3W_2W_3 = W_1W_2W_3^2$ is a square, which implies that W_1W_2 is a square. Note that $W_1W_2 \neq 0$ since $\mathcal{G}(x)$ is irreducible. Furthermore, $W_1 \neq W_2$, since if $W_1 = W_2$, then $a = 0$, which contradicts our assumption that $a \neq 0$ from (1.3). Hence, since W_1W_2 is a square, we conclude that $W_1W_2 > 1$ and that there exists a prime divisor q of W_1W_2, such that $q^2 \mid W_1$ or $q^2 \mid W_2$. Hence, by Lemma 3.2, it follows that $\mathcal{G}(x)$ is not monogenic.

The second possibility in Theorem 2.6 is that W_1W_3 and $W_1W_2W_3$ are squares, while W_2W_3 is not a square. Then $W_1W_3W_1W_2W_3 = W_1^2W_2W_3^2$ is a square, which implies that W_2 is a square. If $W_2 > 1$, then $q^2 \mid W_2$ for some prime q, and $\mathcal{G}(x)$ is not monogenic by Lemma 3.2. Therefore, suppose then that $W_2 = 1$. Hence, $b = -2a - 1$ and

$$W_1W_3 = -4a^3 - 31a^2 - 40a + 12.$$

Since W_1W_3 is a square, say m^2, we consider the elliptic curve

$$y^2 = x^3 - 32x^2 + 160x + 192, \tag{3.24}$$

where $x := -4a$ and $y := 4m$. Using Sage to find all integral points (x, y), with $y \ge 0$, on (3.24) yields

$$(x, y) \in \{(-1, 0), (4, 20), (8, 0), (24, 0), (44, 180)\}.$$

Checking the points (x, y) where $x \equiv 0 \pmod 4$ reveals that all such points, with the exception of $(x, y) = (4, 20)$, produce values (a, b) such that $\mathcal{G}(x)$ is reducible. The lone point $(4, 20)$ implies that $(a, b) = (-1, 1)$, and it is straightforward to verify that $\mathcal{G}(x) = x^8 - x^6 + x^4 - x^2 + 1$ is indeed monogenic.

The third and final possibility in Theorem 2.6 is that W_2W_3 and $W_1W_2W_3$ are squares, while W_1W_3 is not a square. Arguing as before, we see that W_1 is a square, and if $W_1 > 1$, we achieve no monogenic polynomials by Lemma 3.2. If $W_1 = 1$, then we arrive at the same elliptic curve (3.24), where $x := 4a$ and $y := 4m$. In this case, the integral points with $x \equiv 0 \pmod 4$ produce

reducible polynomials $\mathcal{G}(x)$, except when $(x, y) = (44, 180)$. For this particular point, we get that $(a, b) = (11, 21)$. However, is is easy to verify that, while the polynomial

$$\mathcal{G}(x) = x^8 + 11x^6 + 21x^4 + 11x^2 + 1$$

is irreducible with $\mathrm{Gal}(\mathcal{G}) \simeq 8\mathrm{T}2$, it is not monogenic.

In conclusion, there is exactly one monogenic polynomial

$$\mathcal{G}(x) = \Phi_{10}(x^2) = x^8 - x^6 + x^4 - x^2 + 1,$$

where $\mathrm{Gal}(\mathcal{G}) \simeq 8\mathrm{T}2$.

X=3. We assume that $\mathrm{Gal}(\mathcal{G}) \simeq 8\mathrm{T}3$. Then, W_1, W_2 and W_1W_2 are all squares from Theorem 2.6. If $W_1 = W_2$, then $a = 0$, which contradicts the fact that $a \neq 0$ from (1.3). Hence, without loss of generality, suppose that $W_1 > 1$. Then there exists a prime q with $q^2 \mid W_1$, and we can argue as in the case X=2 to deduce that no monogenic polynomials $\mathcal{G}(x)$ exist in this case.

X=4. We assume that $\mathrm{Gal}(\mathcal{G}) \simeq 8\mathrm{T}4$. From Theorem 2.7, we have that exactly one of

$$W_1, \quad W_2 \quad \text{and} \quad W_1W_2 \quad \text{is a square,}$$

and none of

$$W_1W_3, \quad W_2W_3 \quad \text{and} \quad W_1W_2W_3 \quad \text{is a square.}$$

Suppose first that W_1 is a square. We deduce from Lemma 3.2 that $W_1 = 1$, so that $b = 2a - 1$. Then, it is easy to see that

$$W_2\left(-a + 4 - 2\sqrt{W_1}\right) = (4a + 1)(-a + 2) = -4a^2 + 7a + 2$$

is a square if and only if $a = 2$. But then $W_3 = a^2 - 4b + 8 = a^2 - 4 = 0$, which contradicts the fact that $W_1W_3 = W_3$ is not a square. Also, it is easy to see that

$$W_2\left(-a + 4 + 2\sqrt{W_1}\right) = (4a + 1)(-a + 6)$$

is a square if and only if $a \in \{1, 2, 6\}$. With the corresponding values of b, we observe that $W_3 = 0$ when $a \in \{2, 6\}$, which again contradicts the fact that W_1W_3 is not a square. For $a = 1$, we have that $\mathcal{G}(x) = x^8 + x^6 + x^4 + x^2 + 1$, which is reducible. Hence, there are no monogenics when W_1 is a square.

The case when W_2 is a square is similar. We can assume that $W_2 = 1$ by Lemma 3.2, so that $b = -2a - 1$. Then, using Maple (the **isolve** command), we see that

$$W_1\left(-a - 4 - 2\sqrt{W_2}\right) = (4a - 1)(a + 6)$$

is a square if and only if $a \in \{-42, -11, -6\}$, while

$$W_1\left(-a - 4 + 2\sqrt{W_2}\right) = (4a - 1)(a + 2)$$

is a square if and only if $a \in \{-6, -2, 1\}$. Checking these values yields the contradictions that W_3 is a square when $a \in \{-6, -2\}$, while $\mathcal{G}(x)$ is reducible when $a \in \{-42, -11\}$. Although, $\mathcal{G}(x)$ is irreducible when $a = 1$, it is not monogenic. Thus, there are no monogenics arising in this situation.

Finally, suppose that W_1W_2 is a square, and neither W_1 nor W_2 is a square. By Lemma 3.2, we deduce that W_1 and W_2 are squarefree. Since W_1W_2 is a square, it follows that $W_1 = W_2$, contradicting our assumption that $a \neq 0$ in (1.3). Hence, there are no monogenic polynomials $\mathcal{G}(x)$ when X=4.

X=9. Let

$$\mathcal{G}_t(x) := x^8 + (4t+3)x^6 + (8t+5)x^4 + (4t+3)x^2 + 1.$$

Then $\Delta(\mathcal{G}) = 256(16t+13)^2(4t+1)^4(4t-3)^4$. Let $G(t) := (16t+13)(4t+1)(4t-3)$. Since $G(1) \equiv 1 \pmod 4$, we deduce from Lemma 2.15 that $G(t)$ has no local obstructions. Hence, from Corollary 2.14, there exist infinitely many primes p such that $G(p)$ is squarefree. Let p be such a prime. Note, for $\mathcal{G}_p(x)$, with $a := 4p+3$, $b := 8p+5$ and W_i as defined in (2.1), we have

$$W_1 = 1, \quad W_2 = 16p+13 \quad \text{and} \quad W_3 = (4p+1)(4p-3),$$

so that

$$W_1W_2W_3 = (16p+13)(4p+1)(4p-3) = G(p).$$

Since $W_1W_2W_3$ is squarefree and

$$(a \bmod 4,\ b \bmod 4) = (3,1),$$

it follows from Proposition 3.1 that $\mathcal{G}_p(x)$ is monogenic. Moreover, since $W_1 = 1$ is a square and $G(p)$ is squarefree, it is easy to see that none of

$$W_2,\ W_1W_2,\ W_1W_3,\ W_2W_3,\ W_1W_2W_3,$$

$$W_2\left(-a+4-2\sqrt{W_1}\right) = -(16p+3)(4p+1) \quad \text{and}$$
$$W_2\left(-a+4+2\sqrt{W_1}\right) = -(16p+3)(4p-3)$$

is a square. Hence, we deduce from Theorem 2.7 that $\mathrm{Gal}(\mathcal{G}_p) \simeq$ 8T9.

Suppose that, for some primes $p < q$, with $G(p)$ and $G(q)$ both squarefree, we have that $\mathcal{G}_p(x)$ and $\mathcal{G}_q(x)$ generate the same octic field. Then, since $\mathcal{G}_p(x)$ and $\mathcal{G}_q(x)$ are both monogenic, it must be that $\Delta(\mathcal{G}_p) = \Delta(\mathcal{G}_q)$, which implies that

$$256(16p+13)^2(4p+1)^4(4p-3)^8 = 256(16q+13)^2(4q+1)^4(4q-3)^4,$$

contradicting the fact that $p < q$. Thus, $\{\mathcal{G}_p(x) : G(p) \text{ is squarefree}\}$ is an infinite family of monogenic even octic 8T9-polynomials.

X=10. We assume that $\mathrm{Gal}(\mathcal{G}) \simeq$ 8T10. Then, following Theorem 2.6, we have that exactly one of

$$W_1W_3, \quad W_2W_3 \quad \text{and} \quad W_1W_2W_3 \quad \text{is a square.}$$

Note then that $W_1 \neq 1$, $W_2 \neq 1$ and $W_1 \neq W_2$. Since we are searching for monogenic polynomials, we can also assume that W_1 and W_2 are squarefree, by Lemma 3.2.

Suppose first that

$$\begin{aligned} & W_1W_3 \quad \text{is a square} \\ \text{while neither} \quad & W_2W_3 \quad \text{nor} \quad W_1W_2W_3 \quad \text{is a square.} \end{aligned} \tag{3.25}$$

Note that $W_1 \mid W_3$ since W_1 is squarefree and W_1W_3 is a square. If $W_1 = W_3 = -1$, then $a = 4 \pm \sqrt{-5}$, while if $W_1 = W_3 = 1$, then $a = 4 \pm \sqrt{5}$. Hence, $W_1W_3 > 1$. Suppose that q is a prime divisor of W_3 such that $q \nmid W_1$. Since W_1W_3 is a square, and W_1 is squarefree, it follows that $q^2 \mid W_3$. Thus, by Lemma 3.2, we can assume that $q = 2$. Then, since $2 \mid W_3$ and $2 \nmid W_1$, it follows that $2 \mid a$ and $2 \nmid b$. Thus,

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

A closer examination reveals that $2^3 \mid\mid W_3$ when $(a \bmod 4,\ b \bmod 4) = (2,1)$, which contradicts the fact that W_1W_3 is a square. Invoking Lemma 3.2 once again narrows it down to $(a \bmod 4,\ b \bmod 4) = (0,3)$. However, in this case, it is easy to see that $W_1 \equiv 1 \pmod 4$ and $W_3/4 \equiv 3 \pmod 4$ so that $W_1W_3/4 \equiv 3 \pmod 4$, which contradicts the fact that $W_1W_3/4$ is a square. Consequently, we have shown that the prime divisors of W_3 are exactly the prime divisors of W_1, and furthermore,

$$\text{either} \quad W_3 = W_1 \quad \text{or} \quad W_3 = 2^{2k}W_1 \quad \text{for some integer } k \geq 1.$$

If $W_3 = W_1$, then $b = ((a+1)^2+5)/5$ so that $W_1 = (a-4)^2/5$. Since W_1 is squarefree, it follows that $a \in \{-1, 9\}$. If $a = -1$, then $W_2 = 1$, which contradicts the fact that W_2 is squarefree. Thus, $a = 9$, $b = 21$ and $\mathcal{G}(x) = x^8 + 9x^6 + 21x^4 + 9x^2 + 1$. We use Theorem 2.8 with $T(x) := \mathcal{G}(x)$ and $q = 2$ to investigate the monogenicity of $\mathcal{G}(x)$. Since $\overline{T}(x) = (x^4+x^3+x^2+x+1)^2$, we can let $h_1(x) = h_2(x) = x^4+x^3+x^2+x+1$. Then

$$\begin{aligned} F(x) &= \frac{(x^4+x^3+x^2+x+1)^2 - (x^8+9x^6+21x^4+9x^2+1)}{2} \\ &= x^7 - 3x^6 + 2x^5 - 8x^4 + 2x^3 - 3x^2 + x \\ &\equiv x^7 + x^6 + x^2 + x \pmod 2 \\ &\equiv x(x+1)^2(x^4+x^3+x^2+x+1). \end{aligned}$$

Hence, $\gcd(\overline{F}, \overline{h_1}) = x^4+x^3+x^2+x+1$ and $\mathcal{G}(x)$ is not monogenic by Theorem 2.8. Thus, there are no monogenic 8T10-polynomials $\mathcal{G}(x)$ when conditions (3.25) hold with $W_1 = W_3$.

Suppose then that $W_3 = 2^{2k}W_1$ for some integer $k \geq 1$. Then

$$b = \frac{a^2 + 2^{2k+1}a - 2^{2k+1} + 8}{2^{2k}+4},$$

and since b is an integer, we see that $2 \mid a$. Suppose that $k \geq 2$. Since $2^2 \,||\, (2^{2k}+4)$, it follows that

$$b \equiv \begin{cases} 1 \pmod 2 & \text{if } a \equiv 2 \pmod 4 \\ 0 \pmod 2 & \text{if } a \equiv 0 \pmod 4. \end{cases} \tag{3.26}$$

We use Theorem 2.8 with $T(x) := \mathcal{G}(x)$ and $q = 2$ to examine the monogenicity of $\mathcal{G}(x)$. From (3.26), we get that

$$\mathcal{G}(x) \equiv \begin{cases} (x^2+x+1)^4 \pmod 2 & \text{if } a \equiv 2 \pmod 4 \\ (x+1)^8 \pmod 2 & \text{if } a \equiv 0 \pmod 4. \end{cases}$$

Hence, if $a \equiv 2 \pmod 4$, then $a^2 + 2^{2k+1}a - 21 \cdot 2^{2k} - 68 \equiv 0 \pmod{16}$, and therefore

$$F(x) = 2x^7 + \left(\frac{10-a}{2}\right)x^6 + 8x^5 - \left(\frac{a^2 + 2^{2k+1}a - 21\cdot 2^{2k} - 68}{2(2^{2k}+4)}\right)x^4 + 8x^3 + \left(\frac{10-a}{2}\right)x^2 + 2x \equiv 0 \pmod 2.$$

Thus, $\gcd(\overline{F}, x^2+x+1) \neq 1$ and $\mathcal{G}(x)$ is not monogenic.

If $a \equiv 0 \pmod 4$, then $a^2 + 2^{2k+1}a - 72 \cdot 2^{2k} - 272 \equiv 0 \pmod{16}$, and hence

$$F(x) = \left(\frac{4^{k+1}+16}{2^{2k}+4}\right)x^7 + \left(\frac{28-a}{2}\right)x^6 + 28x^5 - \left(\frac{a^2 + 2^{2k+1}a - 72\cdot 2^{2k} - 272}{2(2^{2k}+4)}\right)x^4 + 28x^3 + \left(\frac{28-a}{2}\right)x^2 + \left(\frac{4^{k+1}+16}{2^{2k}+4}\right)x \equiv 0 \pmod 2.$$

Thus, $\gcd(\overline{F}, x+1) \neq 1$ and $\mathcal{G}(x)$ is not monogenic.

Therefore, $\mathcal{G}(x)$ is not monogenic when $k \geq 2$. So, suppose now that $k = 1$. Then $b = a^2/8 + a$ so that $4 \mid a$. Then

$$\mathcal{G}(x) = x^8 + ax^6 + (a^2/8 + a)x^4 + ax^2 + 1 \equiv (x+1)^8 \pmod 2.$$

Hence, applying Theorem 2.8 with $T(x) := \mathcal{G}(x)$ and $q = 2$, we get that

$$F(x) = 4x^7 + (14 - a/2)\,x^6 + 28x^5 - \left(a^2/16 + a/2 - 35\right)x^4 + 28x^3 + (14 - a/2)\,x^2 + 4x \equiv 0 \pmod 2$$

if $2^2 \,||\, a$. Thus, suppose that $a = 8m$, for some integer $m \neq 0$. Then $\overline{F}(x) = x^4$ and $\gcd(\overline{F}, x+1) = 1$. Since $W_1 = (a-4)^2/8 = 2(2m-1)^2$ is squarefree, it follows that $m = 1$ so that $a = 8$ and $b = 16$. It is straightforward to confirm that

$$\mathcal{G}(x) = x^8 + 8x^6 + 16x^4 + 8x^2 + 1 \quad \text{with} \quad \Delta(\mathcal{G}) = 2^{24}27^2$$

is indeed monogenic with $\mathrm{Gal}(\mathcal{G}) \simeq 8\mathrm{T}10$.

The second case to examine is

$$\begin{aligned} &W_2W_3 \quad \text{is a square} \\ \text{while neither} \quad &W_1W_3 \quad \text{nor} \quad W_1W_2W_3 \quad \text{is a square.} \end{aligned} \tag{3.27}$$

Since this case is similar to the first case, we give only a summary of the results. In this case, we found exactly two monogenic 8T10-polynomials:

$$\begin{aligned} &\mathcal{G}(x) = x^8 - 9x^6 + 21x^4 - 9x^2 + 1 \quad \text{with} \quad \Delta(\mathcal{G}) = 2^8 5^6 41^2 \quad \text{and} \\ &\mathcal{G}(x) = x^8 - 8x^6 + 16x^4 - 8x^2 + 1 \quad \text{with} \quad \Delta(\mathcal{G}) = 2^{24} 17^2. \end{aligned}$$

The third, and final, case to examine is

$$\begin{aligned} &W_1W_2W_3 \quad \text{is a square} \\ \text{while neither} \quad &W_1W_3 \quad \text{nor} \quad W_2W_3 \quad \text{is a square.} \end{aligned} \tag{3.28}$$

If $W_1W_2W_3 = 1$, then using Maple to solve this equation yields four solutions, all of which require

$$b^4 - 24b^3 + 216b^2 - 864b + 1280 = (b-8)(b-4)(b^2 - 12b + 40)$$

to be a square.

Using Magma (**IntegralQuarticPoints**([1,-24,216,-864,1280],[4,0]);), we see that the only integral points on the curve $y^2 = b^4 - 24b^3 + 216b^2 - 864b + 1280$ are $(b, y) \in \{(4, 0), (8, 0)\}$. However, each of these values of b produces only irrational values for a. Hence, $W_1W_2W_3 > 1$ since $W_1W_2W_3$ is a square.

If $2 \mid W_3$ then $2 \mid a$, and so $4 \mid W_3$. We claim that $2 \nmid b$. Assume, by way of contradiction, that $2 \mid b$. Note that if $b \equiv 2 \pmod 4$, then $4 \mid W_1$, contradicting the fact that W_1 is squarefree. Hence, $4 \mid b$, $2 \mid W_1$ and $2 \mid W_2$. Thus, $16 \mid W_1W_2W_3$, so that $M := W_1W_2W_3/16$ is a square and

$$\begin{aligned} M &= ((b/2) + 1 - a)((b/2) + 1 + a)((a/2)^2 + b - 2) \\ &\equiv \begin{cases} (1)(1)(3) \equiv 3 \pmod 4 & \text{if } a \equiv 2 \pmod 4 \text{ and } b \equiv 4 \pmod 8, \\ (3)(3)(3) \equiv 3 \pmod 4 & \text{if } a \equiv 2 \pmod 4 \text{ and } b \equiv 0 \pmod 8, \\ (3)(3)(2) \equiv 2 \pmod 4 & \text{if } a \equiv 0 \pmod 4 \text{ and } b \equiv 4 \pmod 8, \\ (1)(1)(2) \equiv 2 \pmod 4 & \text{if } a \equiv 0 \pmod 4 \text{ and } b \equiv 0 \pmod 8, \end{cases} \end{aligned}$$

which is impossible in any case. Thus, the claim that $2 \nmid b$ is established, and therefore,

$$g(x) \equiv (x^2 + x + 1)^2 \pmod 2.$$

Note that $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. Then, applying Theorem 2.8 with $T(x) := g(x)$ and $q = 2$, we can let

$$h_1(x) = h_2(x) = x^2 + x + 1, \tag{3.29}$$

so that

$$F(x) = -x\left(\left(\frac{a-2}{2}\right)x^2 + \left(\frac{b-3}{2}\right)x + \left(\frac{a-2}{2}\right)\right). \tag{3.30}$$

Next, we determine the possible values of ($a \bmod 4$, $b \bmod 4$). Since $4 \mid W_1W_2W_3$, then $N := W_1W_2W_3/4$ is a square with

$$\begin{aligned} N &= \frac{(b+2-2a)(b+2+2a)(b^2-4b+8)}{4} \\ &= (b+2-2a)(b+2-2a)((a/2)^2-b+2). \end{aligned} \tag{3.31}$$

Hence, since $2 \mid a$ and $2 \nmid b$, we see that $(b+2-2a)(b+2+2a) \equiv 1 \pmod 4$ and

$$N \equiv (a/2)^2 - b - 2 \equiv \begin{cases} -b-1 \pmod 4 & \text{if } a \equiv 2 \pmod 4 \\ -b-2 \pmod 4 & \text{if } a \equiv 0 \pmod 4. \end{cases}$$

Thus, it follows that

$$b \equiv \begin{cases} 3 \pmod 4 & \text{if } a \equiv 2 \pmod 4 \\ 1 \pmod 4 & \text{if } a \equiv 0 \pmod 4. \end{cases}$$

Hence, $g(x)$ and $\mathcal{G}(x)$ are not monogenic by Lemma 3.2.

Thus, we can assume additionally that $2 \nmid a$ and W_3 is squarefree. We claim that $2 \nmid b$. To see this, we proceed by way of contradiction and consider the two cases: $b \equiv 0 \pmod 4$ and $b \equiv 2 \pmod 4$. If $b \equiv 0 \pmod 4$, then $W_1 \equiv 0 \pmod 4$, contradicting the fact that W_1 is squarefee. If $b \equiv 2 \pmod 4$, then $4 \mid W_1W_2W_3$ and N, as given in (3.31), is a square with

$$\begin{aligned} N &= ((b/2)+1-a)((b/2)+1+a)(a^2-4b+8) \\ &\equiv (2-a)(2+a)(1) \equiv -a^2 \equiv 3 \pmod 4, \end{aligned}$$

which is impossible. Hence, $2 \nmid b$ and $W_1W_2W_3 \not\equiv 0 \pmod 2$.

Note that W_1W_2 and W_3 are either both positive or both negative since $W_1W_2W_3$ is a square. If

$$W_1W_2 = (b+2)^2 - 4a^2 < 0 \quad \text{and} \quad W_3 = a^2 - 4b + 8 < 0,$$

then

$$(b+2)^2 < 4a^2 < 16b - 32,$$

which yields the contradiction

$$(b+2)^2 - 16b + 32 = (b-6)^2 < 0.$$

Hence,

$$W_1W_2 > 0 \quad \text{and} \quad W_3 > 0. \tag{3.32}$$

Let

$$P = \gcd(W_1, W_3), \quad Q = \gcd(W_1, W_2) \quad \text{and} \quad R = \gcd(W_2, W_3).$$

Then,

$$\begin{aligned} |W_1| &= |b+2-2a| = PQ \\ |W_2| &= |b+2+2a| = QR \\ W_3 &= a^2 - 4b + 8 = PR, \end{aligned} \tag{3.33}$$

where PQR is squarefree. Thus, either $PQR = 1$ or PQR is the product of distinct odd primes.

We claim that $Q \neq 1$. To see this, we assume that $Q = 1$ and proceed by way of contradiction. Then, we deduce from (3.32) and (3.33) that

$$(b+2)^2 - 4a^2 = a^2 - 4b + 8,$$

so that

$$a^2 = \frac{b^2 + 8b - 4}{5}. \tag{3.34}$$

Thus,

$$W_1 W_2 = (b+2)^2 - 4a^2 = (b+2)^2 - 4\left(\frac{b^2+8b-4}{5}\right) = \frac{(b-6)^2}{5}. \tag{3.35}$$

Since $Q = 1$, it follows that $W_1 W_2$ is squarefree. Hence, from (3.35), we conclude that $b \in \{1, 11\}$. If $b = 1$, then $a = \pm 1$ from (3.34). However, if $a = 1$, we arrive at the contradiction that $W_1 = 1$, while if $a = -1$, we get the contradiction that $W_2 = 1$. If $b = 11$, then $a^2 = 41$ from (3.34). Therefore, the claim is established, and $Q \geq 3$, since Q is odd.

Note that if $P = R \neq 1$, then $W_3 = R^2 > 1$, which contradicts the fact that W_3 is squarefree. If $P = R = 1$, then $W_1 W_2 = |W_1 W_2| = Q^2$, which contradicts the fact that $W_1 W_2$ is not a square. Therefore, $P \neq R$. Similar arguments show that $P \neq Q$ and $Q \neq R$.

We proceed by providing details in the situation when $W_1 > 0$ and $W_2 > 0$. We omit details when $W_1 < 0$ and $W_2 < 0$ since the arguments are similar, and no new solutions arise (see [31, p.10]). Invoking Maple to solve the system (3.33), we get that

$$P^2Q^2 - 2PQ^2R + Q^2R^2 - 32PQ - 32QR - 16PR + 256 = 0. \tag{3.36}$$

It follows from (3.36) that

$$P \mid (QR - 16), \quad Q \mid (PR - 16) \quad \text{and} \quad R \mid (PQ - 16). \tag{3.37}$$

Thus, since PQR is squarefree, we deduce from (3.37) that PQR divides

$$\begin{aligned} Z :&= \frac{(QR-16)(PR-16)(PQ-16) - PQR(PQR - 16P - 16Q - 16R)}{256} \\ &= PQ + QR + PR - 16. \end{aligned}$$

It is easy to see that $Z \geq 7$ since P, Q and R are distinct odd positive integers. Hence, since PQR divides Z, we have that $H := PQR - Z \leq 0$. On the other hand, using Maple, we see that the minimum value of H, subject to the constraints $\{P \geq 3, Q \geq 3, R \geq 3\}$, is 16. Thus, we deduce that $P = 1$ or $R = 1$. Letting $P = 1$ in (3.36), and solving for Q yields

$$Q = \frac{4(4R + 4 \pm \sqrt{R^3 - 2R^2 + 65R})}{(R-1)^2}, \tag{3.38}$$

while solving for R produces

$$R = \frac{Q^2 + 16Q + 8 \pm 4\sqrt{4Q^3 + Q^2 + 16Q + 4}}{Q^2}. \tag{3.39}$$

For Q to be a viable solution, we conclude from (3.38) that

$$y^2 = R^3 - 2R^2 + 65R, \tag{3.40}$$

for some integer y. Using Sage to find all integral points (with $y \geq 0$) on the elliptic curve (3.40) we get

$$(R, y) \in \{(0,0), (1,8), (5,20), (13,52), (16,68), (45,300), (65,520), (1573,62348)\}.$$

In (3.38), we cannot have $R = 1$, and since $R \geq 1$ is odd and squarefree, we have that $R \in \{5, 13, 65\}$. Plugging these values back into (3.38) reveals only the two valid solution triples $(P, Q, R) \in \{(1,11,5), (1,3,13)\}$. Although the triple $(1,1,5)$ arises here, it is not legitimate since we know that $P \neq Q$. Because (3.36) is symmetric in P and R, we can also derive the two additional solutions $(5,11,1)$ and $(13,3,1)$. Using the same approach on (3.39) yields no additional solutions. Also, the substitution of $R = 1$ into (3.36) produces no additional solutions as well. In summary, the only solutions are given by

$$(P, Q, R) \in \{(1,11,5), (1,3,13), (5,11,1), (13,3,1)\}. \tag{3.41}$$

The corresponding values of (a, b) can be found by using the values of P, Q and R in (3.41), and solving the resulting systems in (3.33). These pairs are

$$(a, b) \in \{(11,31), (9,19), (-11,31), (-9,19)\},$$

and the corresponding polynomials are

$$\begin{aligned}
\mathcal{G}(x) &= x^8 + 11x^6 + 31x^4 + 11x^2 + 1 \quad \text{with } \Delta(\mathcal{G}) = 2^8 5^6 11^4,\\
\mathcal{G}(x) &= x^8 + 9x^6 + 19x^4 + 9x^2 + 1 \quad \text{with } \Delta(\mathcal{G}) = 2^8 3^4 13^6,\\
\mathcal{G}(x) &= x^8 - 11x^6 + 31x^4 - 11x^2 + 1 \quad \text{with } \Delta(\mathcal{G}) = 2^8 5^6 11^4,\\
\mathcal{G}(x) &= x^8 - 9x^6 + 31x^4 - 9x^2 + 1 \quad \text{with } \Delta(\mathcal{G}) = 2^8 3^4 13^6.
\end{aligned}$$

In summary, we have shown that there exist exactly seven distinct monogenic polynomials $\mathcal{G}(x)$ with $\mathrm{Gal}(\mathcal{G}) \simeq 8\mathrm{T}10$ (see Table 2), and Magma confirms that these polynomials generate distinct octic fields.

X=18. Let

$$\mathcal{G}_t(x) := x^8 + 3x^6 + (2t+1)x^4 + 3x^2 + 1.$$

Then $\Delta(\mathcal{G}_t) = 256(2t+9)^2(2t-3)^2(8t-13)^4$. Let $G(t) := (2t+9)(2t-3)(8t-13)$. Since $G(1) \equiv 3 \pmod 4$, we deduce from Lemma 2.15 that $G(t)$ has no local obstructions. Hence, from Corollary 2.14, there exist infinitely many primes p such that $G(p)$ is squarefree. Let $p \geq 3$ be such a prime. Observe then for $\mathcal{G}_p(x)$ we have

$$W_1 = 2p - 3, \quad W_2 = 2p + 9 \quad \text{and} \quad W_3 = -8p + 13. \tag{3.42}$$

Since $G(p)$ is squarefree, it follows that $\mathrm{Gal}(\mathcal{G}) \simeq 8\mathrm{T}18$ from Theorem 2.6, and that $\mathcal{G}(x)$ is monogenic from Lemma 3.1.

Suppose that, for some primes $3 \le p < q$, with $G(p)$ and $G(q)$ both squarefree, we have that $\mathcal{G}_p(x)$ and $\mathcal{G}_q(x)$ generate the same octic field. Then, it must be that $\Delta(\mathcal{G}_p) = \Delta(\mathcal{G}_q)$, which implies that

$$256(2p+9)^2(2p-3)^2(8p-13)^4 = 256(2q+9)^2(2q-3)^2(8q-13)^4,$$

contradicting the fact that $p < q$. Thus, $\{\mathcal{G}_p(x) : G(p) \text{ is squarefree}\}$ is an infinite family of monogenic even octic 8T18-polynomials, which completes the proof of the theorem. □

We have summarized the results of Theorem 1.1 below in Tables 2 and 3.

X	Distinct Monogenic 8TX-Trinomials $\mathcal{F}(x)$	#
2	x^8+1	1
3	x^8-x^4+1	1
4	x^8+3x^4+1	1
6	x^8+2	1
8	$x^8-2x^4-1, \quad x^8-2$	2
9	$x^8+(4p+3)x^4+1$	∞
	where p is prime with $(4p+1)(4p+5)$ squarefree	
11	none	0
15	x^8-ax^4-1	∞
	where $a>0$, $4 \nmid a$ with $(a^2+4)/\gcd(a^2,4)$ squarefree	
16	$x^8-4x^4+2,\ x^8+4x^4+2,\ x^8-5x^4+5$	3
17	$x^8+2tx^4+t^2+1$	∞
	where $t>0$ with t^2+1 squarefree	
22	none	0
26	x^8+px^4+3	∞
	where $p \ge 5$ is prime with p^2-12 squarefree	

TABLE 2. Monogenic 8TX-even-trinomials with X$\in X_{\mathcal{F}}$

X	Distinct Monogenic 8TX-Polynomials $\mathcal{G}(x)$	#
2	$x^8 - x^6 + x^4 - x^2 + 1$	1
3	none	0
4	none	0
9	$x^8 + (4p+3)x^6 + (8p+5)x^4 + (4p+3)x^2 + 1$	∞
	where p is prime with $(16p+13)(4p+1)(4p-3)$ squarefree	
10	$x^8 + 8x^6 + 16x^4 + 8x^2$,	7
	$x^8 - 9x^6 + 21x^4 - 9x^2 + 1$, $x^8 - 8x^6 + 16x^4 - 8x^2$	
	$x^8 + 11x^6 + 31x^4 + 11x^2 + 1$, $x^8 + 9x^6 + 19x^4 + 9x^2 + 1$	
	$x^8 - 11x^6 + 31x^4 - 11x^2 + 1$, $x^8 - 9x^6 + 19x^4 - 9x^2 + 1$	
18	$x^8 + 3x^6 + (2p+1)x^4 + 3x^2 + 1$	∞
	where p is prime with $(2p+9)(2p-3)(8p-13)$ squarefree	

TABLE 3. Monogenic 8TX-even-reciprocal polynomials with X$\in X_{\mathcal{G}}$

4. Acknowledgments

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

References

[1] ALTMANN, ANNA; AWTREY, CHAD; CRYAN, SAM; SHANNON, KILEY; TOUCHETTE, MADELEINE. Galois groups of doubly even octic polynomials. *J. Algebra Appl.* **19** (2020), 2050014, 15 pp. MR4065005, Zbl 1467.11126, doi: 10.1142/S0219498820500140. 92, 95

[2] AWTREY, CHAD; PATANE, FRANK. On the Galois group of a reciprocal even octic polynomial. *Comm. Algebra* **52** (2024), no. 7, 3018–3026. MR4735436, Zbl 1542.12001, doi: 10.1080/00927872.2024.2312461. 92, 95

[3] AWTREY, CHAD; PATANE, FRANK. An elementary characterization of the Galois group of a doubly even octic polynomial. *J. Algebra Appl.* (to appear). doi: 10.1142/S0219498825502482. 92, 94, 95

[4] BOSMA, WIEB.; CANNON, JOHN; PLAYOUST, CATHERINE. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24** (1997), no. 3-4, 235–265. MR1484478, Zbl 0898.68039, doi: 10.1006/jsco.1996.0125. 94

[5] BUTLER, GREGORY; MCKAY, JOHN. The transitive groups of degree up to eleven. *Comm. Algebra* **11** (1983), no. 8, 863–911. MR0695893 (84f:20005), Zbl 0518.20003, doi: 10.1080/00927878308822884. 92

[6] CHEN, MALCOLM H. W.; CHIN, ANGELINA Y. M.; TAN, TA SHENG. Galois groups of certain even octic polynomials. *J. Algebra Appl.* **22** (2023), no. 12, Paper No. 2350263. MR4663913, Zbl 07766206, arXiv:2210.10257, doi: 10.1142/S0219498823502638. 92, 94

[7] COHEN, HENRI. A course in computational algebraic number theory. Graduate Texts in Mathematics, 138. *Springer-Verlag, Berlin*, 1993. xii+534 pp. ISBN:3-540-55640-0 MR1228206 (94i:11105), Zbl 0786.11071, doi: 10.1007/978-3-662-02945-9. 91, 96

[8] DOKCHITSER, TIM. Transitive groups of degree up to 31. https://people.maths.bris.ac.uk/ matyd/GroupNames/T31.html. 92

[9] GASSERT, T. ALDEN; SMITH, HANSON; STANGE, KATHERINE E. A family of monogenic S_4 quartic fields arising from elliptic curves. *J. Number Theory* **197** (2019), 361–382. MR3906505, Zbl 1410.11050, arXiv:1708.03953, doi: 10.1016/j.jnt.2018.09.026. 93

[10] GRAS, MARIE-NICOLE. Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $\ell \geq 5$. [Nonmonogeneity of the ring of integers of cyclic extensions of $\mathbb{Q}$ of prime degree $\ell \geq 5$] *J. Number Theory* **23** (1986), no. 3, 347–353. MR0846964, Zbl 0564.12008, doi: 10.1016/0022-314X(86)90079-X. 93

[11] HARRINGTON, JOSHUA; JONES, LENNY. Monogenic quartic polynomials and their Galois groups. *Bull. Aust. Math. Soc.*, 2024, 1–16. arXiv:2404.05487v3. doi: 10.1017/S000497272400073X. 93

[12] HARRINGTON, JOSHUA; JONES, LENNY. The irreducibility and monogenicity of power-compostional trinomials. *Math. J. Okayama Univ.* (to appear). arXiv:2204.07784. 111, 112

[13] HELFGOTT, HARALD A. Square-free values of $f(p)$, f cubic. *Acta Math.* **213** (2014), no. 1, 107–135. MR3261012, Zbl 1316.11084, arXiv:1112.3820, doi: 10.1007/s11511-014-0117-2. 98

[14] HOOLEY, CHRISTOPHER. Applications of sieve methods to the theory of numbers. Cambridge Tracts in Mathematics, 70. *Cambridge University Press, Cambridge-New York-Melbourne*, (1976). xiv+122 pp. MR0404173 (53 #7976), Zbl 0624.10037. 98

[15] JAKHAR, ANUJ; KHANDUJA, SUDESH K.; SANGWAN, NEERAJ. 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. 97

[16] JONES, LENNY. A brief note on some infinite families of monogenic polynomials. *Bull. Aust. Math. Soc.* **100** (2019), no. 2, 239–244. MR4001541, Zbl 1461.11138, doi: 10.1017/S0004972719000182. 93

[17] JONES, LENNY. Monogenic polynomials with non-squarefree discriminant. *Proc. Amer. Math. Soc.* **148** (2020), no. 4, 1527–1533. MR4069191, Zbl 1436.11125, doi: 10.1090/proc/14858. 93

[18] JONES, LENNY. Generating infinite families of monogenic polynomials using a new discriminant formula. *Albanian J. Math.* **14** (2020), 37–45. MR4086717, Zbl 1441.11268. 93

[19] JONES, LENNY. Infinite families of non-monogenic trinomials. *Acta Sci. Math. (Szeged)* **87** (2021), no. 1–2, 95–105. MR4276748, Zbl 1488.11163, doi: 10.14232/actasm-021-463-3. 93

[20] JONES, LENNY Infinite families of reciprocal monogenic polynomials and their Galois groups. *New York J. Math.* **27** (2021), 1465–1493. MR4334375, Zbl 1487.11096, 93, 98

[21] 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. 93

[22] JONES, LENNY. Some new infinite families of monogenic polynomials with non-squarefree discriminant. *Acta Arith.* **197** (2021), no. 2, 213–219. MR4189721, Zbl 1465.11204, doi: 10.4064/aa200211-21-7.

[23] JONES, LENNY. Infinite families of monogenic quadrinomials, quintinomials and sextinomials. *Colloq. Math.* **169** (2022), no. 1, 1–10. MR4425002, Zbl 1498.11214, doi: 10.4064/cm8552-4-2021. 93

[24] 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. 93

[25] JONES, LENNY. The monogenity of power-compositional Eisenstein polynomials. *Ann. Math. Inform.* **55** (2022), 93–113. MR4535607, Zbl 1524.11192, doi: 10.33039/ami.2022.09.001. 93

[26] JONES, LENNY. On necessary and sufficient conditions for the monogeneity of a certain class of polynomials. *Math. Slovaca* **72** (2022), no. 3, 591–600. MR4437487, Zbl 1487.11097, doi: 10.1515/ms-2022-0039. 93

[27] JONES, LENNY. Reciprocal monogenic quintinomials of degree 2^n. *Bull. Aust. Math. Soc.* **106** (2022), no. 3, 437–447. MR4510135, Zbl 1521.11068, doi: 10.1017/S0004972722000193. 93, 98, 99, 104

[28] JONES, LENNY. Generalized Wall–Sun–Sun primes and monogenic power-compositional trinomials. *Albanian J. Math.* **17** (2023), no. 2, 3–17. MR4613607, Zbl 1532.11147, doi: 10.51286/albjm/1678110273. 93

[29] JONES, LENNY. On the monogenicity of power-compositional Shanks polynomials. *Funct. Approx. Comment. Math.* **69** (2023), no. 1, 93–103. MR4642608, Zbl 1536.11035, arXiv:2303.11872, doi: 10.7169/facm/2104. 93

[30] JONES, LENNY. Monogenic even quartic trinomials. *Bull. Aust. Math. Soc.* (to appear). doi: 10.1017/S0004972724000510. 93

[31] JONES, LENNY. The monogenicity and Galois groups of certain quintinomials. *Funct. Approx. Comment. Math.* (to appear). 120

[32] JONES, LENNY; PHILLIPS, TRISTAN. Infinite families of monogenic trinomials and their Galois groups. *Internat. J. Math.* **29** (2018), no. 5, 1850039, 11 pp. MR3808054, Zbl 1423.11181, doi: 10.1142/S0129167X18500398. 93

[33] 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. 93

[34] 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 (90i:12006), Zbl 0702.11075, doi: 10.2307/2323198. 93

[35] KEDLAYA, KIRAN S. A construction of polynomials with squarefree discriminants. *Proc. Amer. Math. Soc.* **140** (2012), no. 9, 3025–3033. MR2917075, Zbl 1301.11072, arXiv:1103.5728, doi: 10.1090/S0002-9939-2012-11231-6. 93

[36] KLÜNERS, JÜRGEN.; MALLE, GUNTER. A database for number fields. http://galoisdb.math.upb.de/home. 92

[37] LJUNGGREN, WILHELM. Some theorems on indeterminate equations of the form $\frac{x^n-1}{x-1} = y^q$. *Norsk. Mat. Tidsskr.* **25** (1943), 17–20. MR0018674, Zbl 0028.00901. 94

[38] MAPLE (2019). Maplesoft, a division of Waterloo Maple Inc. Waterloo, Ontario. Retrieved from https://hadoop.apache.org. 94

[39] PASTEN, HECTOR. The ABC conjecture, arithmetic progressions of primes and squarefree values of polynomials at prime arguments. *Int. J. Number Theory* **11** (2015), no. 3, 721–737. MR3327840, Zbl 1337.11065, doi: 10.1142/S1793042115500396. 98

[40] THE SAGE DEVELOPERS. SageMath, the Sage Mathematics Software System (Version 8.1), 2017. https://www.sagemath.org. 94

[41] SMITH, HANSON. Two families of monogenic S_4 quartic number fields. *Acta Arith.* **186** (2018), no. 3, 257–271. MR3879393, Zbl 1417.11150, doi: 10.4064/aa180423-24-8. 93

[42] SPEARMAN, BLAIR K. Monogenic A_4 quartic fields. *Int. Math. Forum* **1** (2006), no. 37–40, 1969–1974. MR2277489, Zbl 1190.11057, doi: 10.12988/imf.2006.06174. 93

[43] SPEARMAN, BLAIR K.; WATANABE, AYA; WILLIAMS, KENNETH S. $PSL(2,5)$ sextic fields with a power basis. *Kodai Math. J.* **29** (2006), no. 1, 5–12. MR2222162, Zbl 1096.11038, doi: 10.2996/kmj/1143122382. 93

[44] 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. 94

[45] 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 (97h:11130), Zbl 0966.11047, doi: 10.1112/blms/15.6.612. 92

(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/2025/31-5.html.