MONOGENIC QUARTIC POLYNOMIALS AND THEIR GALOIS GROUPS

JOSHUA HARRINGTON^[®] and LENNY JONES^[®]

(Received 10 April 2024; accepted 15 June 2024)

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 $\{1, \theta, \theta^2, \dots, \theta^{N-1}\}$ is a basis for the ring of integers of $\mathbb{Q}(\theta)$, where $f(\theta) = 0$. We use the classification of the Galois groups of quartic polynomials, due to Kappe and Warren ['An elementary test for the Galois group of a quartic polynomial', *Amer. Math. Monthly* **96**(2) (1989), 133–137], to investigate the existence of infinite collections of monogenic quartic polynomials having a prescribed Galois group, such that each member of the collection generates a distinct quartic field. With the exception of the cyclic case, we provide such an infinite single-parameter collection for each possible Galois group. We believe these examples are new and we provide evidence to support this belief by showing that they are distinct from other infinite collections in the literature. Finally, we devote a separate section to the cyclic case.

2020 *Mathematics subject classification*: primary 11R16; secondary 11R32. *Keywords and phrases*: monogenic, quartic polynomial, Galois group.

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 $\{1, \theta, \theta^2, \dots, \theta^{\deg f - 1}\}$ is an integral basis for the ring of integers \mathbb{Z}_K of $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$; that is, $\mathbb{Z}_K = \mathbb{Z}[\theta]$. We let $\Delta(f)$ and $\Delta(K)$ denote the discriminants over \mathbb{Q} respectively of f(x) and the number field *K*. From [3], when f(x) is irreducible over \mathbb{Q} ,

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

so that, in this situation, f(x) is monogenic if and only if $\Delta(f) = \Delta(K)$. We also say that a number field *K* is *monogenic* if there exists a power basis for \mathbb{Z}_K . We point out that, while the monogenicity of f(x) implies the monogenicity of $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$, 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 nevertheless, *K* is monogenic since $\{1, (\theta + 1)/2\}$ is a power basis for \mathbb{Z}_K . In fact, $g(x) = x^2 - x - 1$, the minimal polynomial for $(\theta + 1)/2$, is monogenic.

[©] The Author(s), 2024. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.

It is the goal of this article to determine new families of monogenic quartic polynomials that have a prescribed Galois group over \mathbb{Q} . A 'family' here means an infinite collection of polynomials, such that for any two polynomials f(x) and g(x) in the family, we have $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$, where $f(\alpha) = g(\beta) = 0$. For quartic polynomials f(x) that are irreducible over \mathbb{Q} , there are five possibilities for the Galois group Gal(f) over \mathbb{Q} , namely

$$C_4, C_2 \times C_2, D_4, A_4 \text{ and } S_4,$$
 (1.1)

where C_n denotes the cyclic group of order n, D_n denotes the dihedral group of order 2n, A_n denotes the alternating group on n letters of order n!/2 and S_n denotes the symmetric group on n letters of order n!. With the exception of the cyclic case C_4 , we provide a single-parameter family of monogenic quartic polynomials for each group in (1.1), while also providing evidence in a separate section (see Section 4) to support our belief that these families are actually new. Finally, we devote a separate section to a discussion concerning the cyclic case (see Section 5).

The new results are presented in the following main theorem.

THEOREM 1.1.

- (1) $C_2 \times C_2$. Let $t \in \mathbb{Z}$ and let $f_t(x) := x^4 + 4tx^2 + 1$. Then:
 - (a) $f_t(x)$ is irreducible and $\operatorname{Gal}(f_t) \simeq C_2 \times C_2$;
 - (b) $f_t(x)$ is monogenic if and only if (2t 1)(2t + 1) is squarefree;
 - (c) $\mathcal{F}_2 := \{f_t(x) : 4t^2 1 \text{ is squarefree}\}$ is an infinite family of monogenic $C_2 \times C_2$ -quartics.
- (2) **D**₄. Let $t \in \mathbb{Z}$ and let $f_t(x) := x^4 + 24tx^3 + (12t+4)x^2 + 4x + 1$. Then:
 - (a) $f_t(x)$ is irreducible and $\operatorname{Gal}(f_t) \simeq D_4$;
 - (b) $f_t(x)$ is monogenic if and only if (6t 1)(6t + 1) is squarefree;
 - (c) $\mathcal{F}_3 := \{f_t(x) : 36t^2 1 \text{ is squarefree}\}\$ is an infinite family of monogenic D_4 -quartics.
- (3) **A**₄. Let $t \in \mathbb{Z}$ and let $f_t(x) := x^4 + 2x^3 + 2x^2 + 4tx + 36t^2 16t + 2$. Then:
 - (a) $f_t(x)$ is irreducible and $Gal(f_t) \simeq A_4$;
 - (b) $f_t(x)$ is monogenic if and only if $(4t 1)(108t^2 54t + 7)$ is squarefree;
 - (c) $\mathcal{F}_4 := \{f_t(x) : (4t-1)(108t^2 54t + 7) \text{ is squarefree}\}\$ is an infinite family of monogenic A_4 -quartics.

(4) **S**₄. Let $t \in \mathbb{Z}$ and let $f_t(x) := x^4 - 2x^3 - 2x^2 + 6x + 4t - 2$. Then:

- (a) $f_t(x)$ is irreducible and $Gal(f_t) \simeq S_4$;
- (b) $f_t(x)$ is monogenic if and only if 4t + 1, 4t 7 and 64t + 13 are squarefree;
- (c) $\mathcal{F}_5 := \{f_t(x) : 4t + 1, 4t 7 \text{ and } 64t + 13 \text{ are squarefree}\}\$ is an infinite family of monogenic S_4 -quartics.

To the best of our knowledge, the families given in Theorem 1.1 are new and in Section 4, we show that these families contain no overlap with all explicit families that we found in the literature.

REMARK 1.2. Gaál [4] has recently given a description of the generators of power integral bases in the number fields generated by a root of the monogenic polynomials in Theorem 1.1.

2. Preliminaries

The following theorem is due to Kappe and Warren [11].

THEOREM 2.1 [11]. Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$ be irreducible over \mathbb{Q} . Let $r(x) := x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2)$ with splitting field L. Then $\operatorname{Gal}(f) \simeq$

(1) C_4 if and only if r(x) has exactly one root $s \in \mathbb{Q}$ and

$$g(x) := (x^2 - sx + d)(x^2 + ax + (b - s))$$
(2.1)

splits over L;

- (2) $C_2 \times C_2$ if and only if r(x) splits into linear factors over \mathbb{Q} ;
- (3) D_4 if and only if r(x) has exactly one root $s \in \mathbb{Q}$ and g(x), as defined in (2.1), does not split over L;
- (4) A_4 if and only if r(x) is irreducible over \mathbb{Q} and $\Delta(f)$ is a square in \mathbb{Q} ;
- (5) S_4 if and only if r(x) is irreducible over \mathbb{Q} and $\Delta(f)$ is not a square in \mathbb{Q} .

REMARK 2.2. The polynomial r(x) in Theorem 2.1 is known as the cubic resolvent of f(x).

The following theorem, 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 an irreducible polynomial.

THEOREM 2.3 (Dedekind, see [3]). 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 factorisation 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,

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

3. The proof of Theorem 1.1

PROOF. For each case, we let $K = \mathbb{Q}(\theta)$, where $f_t(\theta) = 0$, and we let \mathbb{Z}_K denote the ring of integers of *K*.

3.1. C₂ × C₂. Since $f_t(x-1) = x^4 - 4x^3 + (4t+6)x^2 - (8t+4)x + 4t + 2$ is 2-Eisenstein, we conclude that $f_t(x) = x^4 + 4tx^2 + 1$ is irreducible over \mathbb{Q} . The cubic resolvent of $f_t(x)$ is

$$r_t(x) = x^3 - 4tx^2 - 4x + 16t = (x - 2)(x + 2)(x - 4t).$$

By Theorem 2.1, it follows that $Gal(f_t) \simeq C_2 \times C_2$, which proves item (1a).

For item (1b), a straightforward calculation reveals that

$$\Delta(f_t) = 2^8 (4t^2 - 1)^2. \tag{3.1}$$

To establish the monogenicity of $f_t(x)$, we use Theorem 2.3 with $T(x) := f_t(x)$ and we examine the prime divisors q of $\Delta(f_t)$.

First, let q = 2. Then $\overline{T}(x) = (x+1)^4$ and we can let $h_1(x) = x+1$ and $h_2(x) = (x+1)^3$. Then,

$$F(x) = \frac{(x+1)^4 - f_t(x)}{2} = 2x^3 - (2t-3)x^2 + 2x \equiv x^2 \pmod{2}.$$

Thus, $gcd(\overline{h_1}, \overline{h_2}, \overline{F}) = 1$ and $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ is not divisible by q = 2.

Next, we give details only for the case when a prime q divides 2t - 1 since the case when q divides 2t + 1 is similar. Since $t \equiv 1/2 \pmod{q}$, it follows that

$$\overline{T}(x) = \begin{cases} (x^2 + 1)^2 & \text{if } q \equiv 3 \pmod{4}, \\ (x - y)^2 (x + y)^2 & \text{if } q \equiv 1 \pmod{4}, \end{cases}$$

where $y \in \mathbb{Z}$ such that $y^2 \equiv -1 \pmod{q}$. If $q \equiv 3 \pmod{4}$, we can let $h_1(x) = h_2(x) = x^2 + 1$. Then,

$$\overline{F}(x) = \overline{-2\left(\frac{2t-1}{q}\right)}x^2$$

so that $gcd(\overline{h_1}, \overline{h_2}, \overline{F}) = 1$ if and only if $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ is not divisible by q if and only if $q^2 \nmid (2t-1)$. If $q \equiv 1 \pmod{4}$, then $y^2 = zq - 2t$ for some integer z since $-2t \equiv -1 \pmod{q}$. Then,

$$\overline{F}(x) = \overline{-2z}(x^2 + 1) + \overline{\left(\frac{4t^2 - 1}{q}\right)},$$

from which we see that

$$\overline{F}(\pm y) = \left(\frac{4t^2 - 1}{q}\right) \neq 0 \quad \text{if and only if} \quad q^2 \notin (2t - 1).$$

Thus, we conclude that $f_t(x)$ is monogenic if and only if $4t^2 - 1$ is squarefree, completing the proof of item (1b).

For item (1c), we note first that \mathcal{F}_2 is an infinite set since there exist infinitely many integers *t* such that $4t^2 - 1$ is squarefree [1]. To see that the fields generated by the elements $f_t(x)$ of \mathcal{F}_2 are all distinct, we proceed by way of contradiction. We assume for integers $t_1 \neq t_2$, that $K_1 = K_2$, where $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$ with $f_{t_1}(\alpha_1) = 0 = f_{t_2}(\alpha_2)$. Since both $f_{t_1}(x)$ and $f_{t_2}(x)$ are monogenic by item (1b), it follows that $\Delta(f_{t_1}) = \Delta(f_{t_2})$. Consequently, from (3.1),

$$8(t_1 - t_2)(t_1 + t_2)(2t_1^2 + 2t_2^2 - 1) = 0.$$

Hence, $t_1 = -t_2$. Without loss of generality, we may assume that $t_1 > 0$ so that $t_2 < 0$. Since the zeros of $f_t(x)$ are

$$\sqrt{-2t + \sqrt{4t^2 - 1}}, \quad \sqrt{-2t - \sqrt{4t^2 - 1}}, \quad -\sqrt{-2t + \sqrt{4t^2 - 1}}, \quad -\sqrt{-2t - \sqrt{4t^2 - 1}},$$

it follows that all zeros of $f_t(x)$ are real if t < 0, while all zeros of $f_t(x)$ are nonreal if $t \ge 0$, which contradicts the assumption that $K_1 = K_2$.

3.2. D₄. Note that $f_0(x - 1) = x^4 - 4x^3 + 10x^2 - 8x + 2$ is 2-Eisenstein. Hence, $f_0(x)$ is irreducible over \mathbb{Q} . Suppose next that $t \neq 0$. Then, |t| > 10/12, from which we deduce that

$$|24t| = |12t| + 12|t| > |12t| + 10 \ge |12t + 4| + 6.$$

Thus, $f_t(x) = x^4 + 24tx^3 + (12t + 4)x^2 + 4x + 1$ is irreducible over \mathbb{Q} when $t \neq 0$ by Perron's irreducibility criterion [16].

To determine $Gal(f_t)$, we use Theorem 2.1. The cubic resolvent of $f_t(x)$ is

$$r_t(x) = x^3 - (12t+4)x^2 + (96t-4)x - (576t^2 - 48t)$$
$$= (x - 12t)(x^2 - 4x + (48t - 4)).$$

Since

$$\Delta(x^2 - 4x + (48t - 4)) = -192t + 32 = 16(-12t + 2),$$

and $-12t + 2 \equiv 2 \pmod{4}$, we conclude that $r_t(x)$ has exactly the one rational zero x = 12t. Consequently, the splitting field of $r_t(x)$ is $L = \mathbb{Q}(\sqrt{-2(6t-1)})$. Then, in Theorem 2.1, we have $g(x) = g_1(x)g_2(x)$, where

$$g_1(x) = x^2 - 12tx + 1$$
 and $g_2(x) = x^2 + 24tx + 4$.

Since $\Delta(g_1) = 4(6t - 1)(6t + 1)$ and $\Delta(g_2) = 16(6t - 1)(6t + 1)$, it follows that both $g_1(x)$ and $g_2(x)$ are irreducible over *L*. Hence, $\operatorname{Gal}(f_t) \simeq D_4$ by Theorem 2.1, which proves item (2a).

To establish item (2b), we use Theorem 2.3 with $T(x) := f_t(x)$. A straightforward calculation yields

$$\Delta(f_t) = -2^9 (6t - 1)^3 (6t + 1)^2.$$

First let q = 2. Then, $\overline{T}(x) = (x + 1)^4$, and we can select

$$h_1(x) = x + 1$$
 and $h_2 = (x + 1)^3$. (3.2)

Thus,

$$F(x) = \frac{(x+1)^4 - f_t(x)}{2} = (2 - 12t)x^3 + (1 - 6t)x^2 \equiv x^2 \pmod{2}.$$

Therefore, $gcd(\overline{h_1}, \overline{F}) = 1$ so that $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ is not divisible by q = 2.

When q is a prime divisor of 6t - 1, we also get

$$\overline{T}(x) = x^4 + 4x^3 + 6x^2 + 4x + 1 = (x+1)^4,$$

with $h_i(x)$ as in (3.2). Then,

$$F(x) = \frac{(x+1)^4 - f_t(x)}{2} = \frac{-2(6t-1)}{q}(2x+1)x^2,$$

and it follows that

$$gcd(\overline{h_1}, \overline{F}) = 1$$
 if and only if $q^2 \nmid (6t - 1)$.

Thus, $q \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if $q^2 \nmid (6t - 1)$.

Suppose next that q is a prime divisor of 6t + 1. Then, $t \equiv -1/6 \pmod{q}$ and

$$T(x) \equiv (x^2 - 2x - 1)^2 \pmod{q}.$$

If $x^2 - 2x - 1$ is irreducible over \mathbb{F}_q , then we can let $h_1(x) = h_2(x) = x^2 - 2x - 1$. In this case, we get

$$F(x) = \frac{(x^2 - 2x - 1)^2 - f_t(x)}{2} = -2\left(\frac{6t + 1}{q}\right)x^2(2x + 1),$$

so that

 $gcd(\overline{h_1}, \overline{F}) = 1$ if and only if $q^2 \nmid (6t + 1)$.

If $x^2 - 2x - 1$ is reducible over \mathbb{F}_q , then

 $x^{2} - 2x - 1 = (x - (1 + y))(x - (1 - y)),$

where $y \in \mathbb{Z}$ with $y^2 \equiv 2 \pmod{q}$. Then, we can select

$$h_1(x) = h_2(x) = (x - (1 + y))(x - (1 - y)),$$

so that

[7]

$$F(x) = -4\left(\frac{6t+1}{q}\right)x^3 - 2\left(\frac{6t+1}{q} + \frac{y^2 - 2}{q}\right)x^2 + 4\left(\frac{y^2 - 2}{q}\right)x + y^2\left(\frac{y^2 - 2}{q}\right).$$

Then, computer calculations reveal that

$$\overline{F}(1 \pm y) = 2\left(\frac{6t+1}{q}\right)(\mp 12y - 17).$$

If $\mp 12y - 17 \equiv 0 \pmod{q}$, then, since $y^2 \equiv 2 \pmod{q}$,

$$288 \equiv 144y^2 \equiv (\mp 12y)^2 \equiv 17^2 \equiv 289 \pmod{q},$$

which yields the contradiction that $0 \equiv 1 \pmod{q}$. Hence,

$$gcd(\overline{h_1}, \overline{F}) = 1$$
 if and only if $q^2 \nmid (6t + 1)$,

completing the proof that $f_t(x)$ is monogenic if and only if $36t^2 - 1$ is squarefree.

For item (2c), we proceed as in the case of $C_2 \times C_2$. The set \mathcal{F}_3 is infinite since there exist infinitely many values of t such that $36t^2 - 1$ is squarefree [1]. We assume for integers $t_1 \neq t_2$ that $K_1 = K_2$, where $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$ with $f_{t_1}(\alpha_1) =$ $0 = f_{t_2}(\alpha_2)$. Since both $f_{t_1}(x)$ and $f_{t_2}(x)$ are monogenic by item (2b), it follows that $\Delta(f_{t_1}) = \Delta(f_{t_2})$. Solving this discriminant equation using Maple shows that $6t_1$ must be a zero of the polynomial

$$\mathcal{G}(X) := X^4 + (6t_2 - 1)X^3 + (36t_2^2 - 6t_2 - 2)X^2 + (216t_2^3 - 36t_2^2 - 12t_2 + 2)X + 1296t_2^4 - 216t_2^3 + 12t_2 - 72t_2^2 + 1,$$

which is impossible since $\mathcal{G}(0) \neq 0 \pmod{6}$. This contradiction completes the proof of item (2c) for the case of D_4 .

3.3. A₄. Since $f_t(x)$ is 2-Eisenstein, $f_t(x)$ is irreducible over \mathbb{Q} . Straightforward calculations using Maple give

$$\Delta(f_t) = 2^6 (4t - 1)^2 (108t^2 - 54t + 7)^2$$

and the cubic resolvent of $f_t(x)$ as

$$r_t(x) = x^3 - 2x^2 - (144t^2 - 72t + 8)x + 128t^2 - 64t + 8.$$

If $r_t(x)$ is reducible over \mathbb{Q} , then

$$r_t(x) = (x+z)(x^2 + Ax + B) = x^3 + (A+z)x^2 + (Az+B)x + Bz,$$

for some integers A, B, z. Hence, by equating coefficients, we see that

$$A + z = -2$$

$$Az + B = -(144t^{2} - 72t + 8)$$

$$Bz = 128t^{2} - 64t + 8.$$

Solving this system in Maple yields

$$B = (8z^2 + 16z + 8)/(9z + 8).$$

Let $d := \gcd(8z^2 + 16z + 8, 9z + 8)$. Then, easy greatest common divisor (gcd) calculations show that $d \mid 8$. Since *B* is an integer, d = 9z + 8. Hence, the only possibilities for *z* are z = 0 and z = -1. However, checking the values of -z in $r_t(x)$ gives $r(0) = 8(4t - 1)^2 \neq 0$ and $r(1) = -(4t - 1)^2 \neq 0$, since $t \in \mathbb{Z}$. Hence, $r_t(x)$ is irreducible over \mathbb{Q} , and it follows from Theorem 2.1 that $\operatorname{Gal}(f_t) \simeq A_4$, which proves item (3a).

For item (3b), we use Theorem 2.3 with $T(x) := f_t(x)$ to check the prime divisors q of $\Delta(f_t)$. Suppose first that q = 2. Then, $\overline{T}(x) = x^4$, so that we can let $h_1(x) = x$ and $h_2(x) = x^3$, and we get

$$F(x) = -x^3 - x^2 - 2tx - 18t^2 + 8t - 1 \equiv x^3 + x^2 + 1 \pmod{2}.$$

Hence, we see quite easily that $gcd(\overline{h_1}, \overline{F}) = 1$, from which we conclude that $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ is not divisible by q = 2.

Next, let q be a prime divisor of 4t - 1. Then, $t \equiv 1/4 \pmod{q}$ and

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

Suppose first that $x^2 + x + 1/2$ is irreducible over \mathbb{F}_q . Note that in this situation, we must have $q \equiv 3 \pmod{4}$ since -1 is not a square. Then we can let

$$h_1(x) = h_2(x) = x^2 + x + (q+1)/2,$$

which yields

$$\overline{F}(x) = x^2 - \overline{\left(\frac{4t-1}{q}-1\right)}x - \overline{\left(\frac{(4t-1)(36t-7)-q^2-2q}{4q}\right)}$$
$$= x^2 - \overline{\left(\frac{4t-1}{q}-1\right)}x - \overline{\left(\frac{(4t-1)(36t-7)}{4q}\right)} + \overline{\frac{1}{2}}.$$

Note that $36t - 7 \equiv 2 \pmod{q}$ so that $q \nmid (36t - 7)$. Hence, it follows that $gcd(\overline{h_1}, \overline{F}) \neq 1$ if and only if $\overline{F}(x) = \overline{h_1}(x)$, which is true if and only if $q^2 \mid (4t - 1)$.

Suppose next that $x^2 + x + 1/2$ is reducible over \mathbb{F}_q . Then, $q \equiv 1 \pmod{4}$ and

$$x^{2} + x + 1/2 \equiv \left(x - \left(\frac{-1 + y}{2}\right)\right) \left(x - \left(\frac{-1 - y}{2}\right)\right) \pmod{q},$$

where $y^2 \equiv -1 \pmod{q}$. Choosing $y \equiv 1 \pmod{2}$, we can let

$$h_1(x) = h_2(x) = \left(x - \left(\frac{-1 + y}{2}\right)\right)\left(x - \left(\frac{-1 - y}{2}\right)\right).$$

Then, computer calculations produce

$$\overline{F}(x) = \overline{\left(\frac{-y^2 - 1}{2q}\right)}x^2 + \overline{\left(\frac{1 - y^2 - 8t}{2q}\right)}x + \overline{\left(\frac{y^4 - 2y^2 - 576t^2 + 256t - 31}{16q}\right)},$$

so that

[9]

$$\overline{F}((-1\pm y)/2) = \frac{-(4t-1)(9(4t-1)\pm 2y)}{q} + \frac{(y^2+1)^2}{4q} = \overline{\mp 2y}\Big(\frac{4t-1}{q}\Big).$$

Hence, we see that $\overline{F}((-1 \pm y)/2) = 0$ if and only if $q^2 \mid (4t - 1)$, which completes the proof when $q \mid (4t - 1)$.

Now, suppose that q is a prime divisor of $108t^2 - 54t + 7$. Note that $q \notin \{2, 3\}$. Then, it follows that

$$\overline{T}(x) = (x - (18t - 5))(x - (1 - 6t))^3,$$

and therefore, we can let

$$h_1(x) = (x - (18t - 5))(x - (1 - 6t))$$
 and $h_2(x) = (x - (1 - 6t))^2$. (3.3)

Observe from (3.3) that we only need to check $\overline{F}(1-6t)$ to determine $gcd(\overline{h_1}, \overline{h_2}, \overline{F})$. More precisely,

$$[\mathbb{Z}_K : \mathbb{Z}[\theta]] \equiv 0 \mod q \quad \text{if and only if} \quad \overline{F}(1 - 6t) = 0. \tag{3.4}$$

Straightforward calculations yield

$$F(x) = \left(\frac{108t^2 - 54t + 7}{q}\right)(-2x^2 - 2(8t - 1)x - (36t^2 - 10t + 1)),$$

so that

$$\overline{F}(1-6t) = -\overline{\left(\frac{108t^2 - 54t + 7}{q}\right)}(12t^2 - 6t + 1) = -\frac{2}{9}\left(\frac{108t^2 - 54t + 7}{q}\right),$$

since

$$9(12t^2 - 6t + 1) - 2 = 108^2 - 54t + 7 \equiv 0 \pmod{q}.$$

Hence,

$$\overline{F}(1-6t) = 0 \quad \text{if and only if} \quad 108t^2 - 54t + 7 \equiv 0 \mod q^2.$$

Consequently, from (3.4),

 $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \equiv 0 \mod q \quad \text{if and only if} \quad 108t^2 - 54t + 7 \equiv 0 \mod q^2.$

Since $gcd(4t - 1, 108t^2 - 54t + 7) = 1$, the proof of item (3b) for A_4 is complete.

For item (3c), we proceed as in the previous cases. The set \mathcal{F}_4 is infinite since there exist infinitely many values of t such that $(4t - 1)(108t^2 - 54t + 7)$ is squarefree [1]. We assume for integers $t_1 \neq t_2$ that $K_1 = K_2$, where $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$ with $f_{t_1}(\alpha_1) = 0 = f_{t_2}(\alpha_2)$. Since both $f_{t_1}(x)$ and $f_{t_2}(x)$ are monogenic by item (3b), it follows that $\Delta(f_{t_1}) = \Delta(f_{t_2})$. Using Maple to solve this equation, we get six possible solutions. One solution has $t_1 = t_2$, which we are not considering. A second solution has $t_1 = 1/2 - t_2$, which is impossible in integers t_1 and t_2 . The remaining four solutions contain the expression $\sqrt{-255 + 1944t_2 - 3888t_2^2}$. Thus, for one of these solutions to be viable, $-255 + 1944t_2 - 3888t_2^2$ must be a perfect square. However, it is easy to see that $-3888x^2 + 1944x - 255 < 0$ for all $x \in \mathbb{R}$, and this fact completes the proof of item (3c) for the case of A_4 .

3.4. S₄. For item (4a), $f_t(x)$ is irreducible over \mathbb{Q} for all $t \in \mathbb{Z}$ since $f_t(x)$ is 2-Eisenstein. Using Maple, we calculate

$$\Delta(f_t) = 16(4t+1)(4t-7)(64t+13).$$

Since gcd(4t + 1, 4t - 7) = 1 with 4t + 1 and 4t - 7 squarefree, it follows that (4t + 1)(4t - 7) divides 64t + 13 if $\Delta(f_t)$ is a square. Observe then that 64t + 13 = 16(4t + 1) - 3 implies that 4t + 1 divides 3, from which we conclude that $t \in \{-1, 0\}$. However, $64t + 13 = 16(4t - 7) + 5^3$ implies that 4t - 7 divides 5, which in turn implies that $t \in \{2, 3\}$. This impossibility shows that $\Delta(f_t)$ is not a square. The cubic resolvent of $f_t(x)$ is

$$r_t(x) = x^3 + 2x^2 - 4(4t+1)x - 12(4t+1).$$

If $r_t(x)$ is reducible over \mathbb{Q} , then

$$r_t(x) = (x+z)(x^2 + Ax + B) = x^3 + (A+z)x^2 + (Az+B)x + Bz$$

for some integers A, B, z. Equating coefficients,

$$A + z = 2$$
, $Az + B = -16t - 4$ and $Bz = -48t - 12$.

Thus,

$$B := -\frac{3z(z-2)}{z-3} = -3(z+1) - \frac{9}{z-3} \in \mathbb{Z},$$

which implies that z - 3 divides 9, and hence, $-z \in \{-12, -6, -4, -2, 0, 6\}$. However, solving $r_t(-z) = 0$ for *t* for each of these values of -z yields

$$t \in \{39/4, 11/4, 7/4, -1/4\},\$$

which contradicts the fact that $t \in \mathbb{Z}$. Therefore, $r_t(x)$ is irreducible for all $t \in \mathbb{Z}$, and we deduce from Theorem 2.1 that $Gal(f_t) \simeq S_4$.

To establish item (4b), we use Theorem 2.3 with $T(x) := f_t(x)$ to check the prime divisors q of $\Delta(f_t)$. Since the details are similar for any prime divisor q of $\Delta(f_t)$, we only give details in the case when q divides 4t - 7. Then, $t \equiv 7/4 \pmod{q}$ and

$$T(x) \equiv (x^2 - 4x + 5)(x + 1)^2 \pmod{q}.$$

Since x = -1 is a zero of $x^2 - 4x + 5$ if and only if q = 5, we have three cases to consider:

$$\overline{T}(x) = \begin{cases} x(x+1)^3 & \text{if } q = 5, \\ (x^2 - 4x + 5)(x+1)^2 & \text{if } x^2 - 4x + 5 \text{ is irreducible over } \mathbb{F}_q, \\ (x - A)(x - B)(x+1)^2 & \text{if } x^2 - 4x + 5 \text{ is reducible over } \mathbb{F}_q, \end{cases}$$
(3.5)

11

where A and B are integers with $A, B \not\equiv -1 \pmod{q}$. We see in all of these cases that $h_2(x) = x + 1$ so that $gcd(\overline{h_1}, \overline{h_2}, \overline{F})$ can be determined by calculating $\overline{F}(-1)$. Thus, more precisely,

 $gcd(\overline{h_1}, \overline{h_2}, \overline{F}) = 1 \iff \overline{F}(-1) \neq 0 \iff [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ is not divisible by q.

Straightforward calculations reveal in all cases of (3.5) that

$$\overline{F}(-1) = \overline{-\left(\frac{4t-7}{q}\right)}.$$

Consequently, we deduce that

 $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q}$ if and only if 4t - 7 is squarefree.

For item (4c), we first note that there exist infinitely many integers t such that

$$(4t+1)(4t-7)(64t+13)$$

is squarefree [1]. Hence, there are infinitely many integers *t* such that 4t + 1, 4t - 7 and 65t + 13 are simultaneously squarefree. Thus, the set \mathcal{F}_5 is infinite. To see that each such value of *t* generates a distinct field, we proceed as in previous cases, and let Maple solve the equation $\Delta(f_{t_1}) = \Delta(f_{t_2})$. In all solutions given by Maple, other than $t_1 = t_2$, we see that $W(t_2) := -12288t_2^2 + 10624t_2 + 19049$ must be a perfect square. It is easy to verify that $W(t_2) < 0$ for all integers $t_2 \notin \{0, 1\}$. Since neither W(0) = 19049 nor W(1) = 17385 is a square, the proofs of item (4c) and the theorem are complete.

4. Comparing the families in Theorem 1.1 to known families

4.1. $C_2 \times C_2$. The literature on quartic polynomials with Galois group $C_2 \times C_2$ is fairly extensive, with some authors addressing the issue of monogenicity [2, 7, 9, 14, 20]. However, we found only one explicit two-parameter family of monogenic $C_2 \times C_2$ -quartic polynomials [9], given by

$$\mathcal{F}(x) = x^4 + (36rp - 1)x^2 + 1,$$

where $r \ge 3$ and p are primes, such that r is a primitive root modulo 9 and

$$(12rp - 1)(12rp + 1)(36rp - 1)(36rp + 1)$$

is squarefree. Suppose that $\mathcal{F}(\alpha) = 0$ and $f_t(\theta) = 0$. To see that $K \neq L$, where $K := \mathbb{Q}(\alpha)$ and $L := \mathbb{Q}(\theta)$, suppose to the contrary that K = L. Since both $\mathcal{F}(x)$ and $f_t(x)$ are monogenic, it follows that

$$144(36rp+1)^2(12rp-1)^2 = \Delta(\mathcal{F}) = \Delta(K) = \Delta(f_t) = 256(2t-1)^2(2t+1)^2,$$

which is clearly seen to be impossible by examining the power of 2 dividing each side. Hence, $K \neq L$.

4.2. D₄. Several authors have investigated integral bases for D_4 -quartic number fields [8–10, 12], but we found only two (two-parameter) families of monogenic quartic D_4 -polynomials [9], given by

$$\mathcal{F}^+(x) = x^4 + x^3 + (100rp + 1)x^2 + x + 1$$
 and
 $\mathcal{F}^-(x) = x^4 - x^3 + (100rp + 1)x^2 - x + 1,$

where $r \ge 3$ and p are primes, such that r is a primitive root modulo 25 and

(20rp + 1)(100rp + 1)(80rp - 1)

is squarefree. Note that, for fixed values of *r* and *p*, $\mathcal{F}^+(x)$ and $\mathcal{F}^-(x)$ generate the same field. Since

$$\Delta(\mathcal{F}^{\pm}) = 5^3 (20rp + 1)(100rp + 1)(80rp - 1)^2 \quad \text{and} \quad \Delta(f_t) = -2^9 (6t - 1)^3 (6t + 1)^2,$$

an argument similar to that given for $C_2 \times C_2$ easily shows that the family $\mathcal{F}^+(x)$ differs from the family given in Theorem 1.1 for D_4 .

4.3. A₄. The only monogenic A_4 -quartic family of polynomials we could find in the literature is the single-parameter family

$$\mathcal{F}_m(x) = x^4 + 18x^2 - 4mx + m^2 + 81,$$

where $m(m^2 + 108)$ is squarefree [18]. Note that *m* is odd. To see that the family $\mathcal{F}_m(x)$ has no overlap with the family presented in this article, we assume for some integers *m* and *t* for which $\mathcal{F}_m(x)$ and $f_t(x)$ are respectively monogenic, that K = L, where $K := \mathbb{Q}(\alpha)$ and $L := \mathbb{Q}(\theta)$ with $\mathcal{F}_m(\alpha) = 0$ and $f_t(\theta) = 0$. Then,

$$2^8 m^2 (m^2 + 108)^2 = \Delta(\mathcal{F}) = \Delta(K) = \Delta(f_t) = 2^6 (4t - 1)^2 (108t^2 - 54t + 7)^2.$$

Using Maple to solve this equation, we find that any solution must have

$$z^{2} = 11664m^{6} + 2519424m^{4} + 136048896m^{2} + 1$$
(4.1)

for some integer z. Multiplying both sides of (4.1) by 4 shows that $(x, y) = (36m^2, 2z)$ is an integral point on the elliptic curve

$$y^2 = x^3 + 7776x^2 + 15116544x + 4.$$
(4.2)

Using Sage to find all integral points (x, y) (with $y \ge 0$) on (4.2), we find

$$(x, y) \in \{(0, 2), (-3888, 2), (14281868898720, 53973124902433105922)\}.$$

Since $x = 36m^2$ with *m* odd, it is easy to see that none of these points yields a valid solution to (4.1). That is, there is no overlap with these two families.

4.4. S₄. We found two families of monogenic S_4 -quartic trinomials in [17] and one family in [5]. The first family in [17] is

$$\mathcal{F}_b(x) = x^4 + bx + b \in \mathbb{Z}[x] \quad \text{with } \Delta(\mathcal{F}_b) = (256 - 27b)b^3, \tag{4.3}$$

where $b \notin \{3, 5\}$, and both b and 256 - 27b are squarefree, and the second is

$$\mathcal{G}_d(x) = x^4 + x^3 + d \in \mathbb{Z}[x] \quad \text{with } \Delta(\mathcal{G}_d) = (256d - 27)d^2,$$
(4.4)

where $d \neq -2$, and both d and 256d - 27 are squarefree. The family in [5] is

$$\mathcal{H}_m(x) = x^4 - 6x^2 - mx - 3 \in \mathbb{Z}[x] \quad \text{with } \Delta(\mathcal{H}_m) = -27(m-8)^2(m+8)^2.$$
(4.5)

Recall that $f_t(x) := x^4 - 2x^3 - 2x^2 + 6x + 4t - 2$, with

$$\Delta(f_t) = 16(4t+1)(4t-7)(64t+13).$$

The question is whether $f_t(x)$ and $\mathcal{F}_b(x)$ (or $\mathcal{G}_d(x)$ or $\mathcal{H}_m(x)$) generate the same quartic field for some integers *t* and *b* (or *d* or *m*). If so, then K = L, where $K = \mathbb{Q}(\alpha)$, $L = \mathbb{Q}(\theta)$, $f_t(\theta) = 0$ and $\mathcal{F}_b(\alpha) = 0$ (or $\mathcal{G}_d(\alpha) = 0$ or $\mathcal{H}_m(\alpha) = 0$). More importantly in this situation, since all of these polynomials are monogenic, their respective discriminants must be equal. In each case, we assume that these polynomial discriminants are equal and proceed towards a contradiction.

We begin with $\mathcal{F}_b(x)$ in (4.3). Here we are assuming that

$$(256 - 27b)b^3 = 16(4t + 1)(4t - 7)(64t + 13)$$

for some integers *b* and *t*. Since 4t + 1, 4t - 7 and 64t + 13 are all odd and squarefree, it follows that b = 2. Then, Maple tells us that P(t) = 0, where

$$P(x) := 128x^3 - 166x^2 - 95x - 24.$$

Since $\Delta(P) < 0$, we know that P(x) has exactly one real zero, and since P(1) < 0 while P(2) > 0, it follows that P(t) has no integer zero, which contradicts the fact that $t \in \mathbb{Z}$.

For $\mathcal{G}_d(x)$ in (4.4), a similar argument shows that d = 4 and P(t) = 0, where

$$P(x) := 128x^3 - 166x^2 - 95x - 136.$$

As before, P(x) has exactly one real noninteger zero between 1 and 2, which contradicts the fact that $t \in \mathbb{Z}$.

Finally, we address $\mathcal{H}_m(x)$ in (4.5). We assume that

$$-27(m-8)^2(m+8)^2 = 16(4t+1)(4t-7)(64t+13)$$
(4.6)

for some integers *m* and *t*. An examination of each of the factors A := 4t + 1, B := 4t - 7 and C := 64t + 13 modulo 3 produces

$$[A \mod 3, B \mod 3, C \mod 3] = \begin{cases} [1, 2, 1] & \text{if } t \equiv 0 \mod 3, \\ [2, 0, 2] & \text{if } t \equiv 1 \mod 3, \\ [0, 1, 0] & \text{if } t \equiv 2 \mod 3. \end{cases}$$

Thus, since A, B and C are squarefree, it follows that $ABC \not\equiv 0 \pmod{27}$, and so there are no solutions to (4.6).

5. The cyclic case C_4

The case of monogenic quartic polynomials f(x) such that $Gal(f) \simeq C_4$ seems to be quite different from the other possible quartic Galois groups. Gras [6] showed that there are only two distinct imaginary monogenic cyclic quartic fields

$$\mathbb{Q}(\zeta_5)$$
 and $\mathbb{Q}(\zeta_{16} - \zeta_{16}^{-1})$,

where ζ_n is a primitive *n*th root of unity. Respective corresponding monogenic polynomials are $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ and $x^4 + 4x^2 + 2$. Gras [6] also found twelve real monogenic cyclic quartic fields, but she did not provide explicit corresponding monogenic polynomials generating these fields.

Olajos [15] proved for the simplest quartics

$$\mathcal{F}_k(x) = x^4 - kx^3 - 6x^2 + kx + 1, \quad k \notin \{\pm 3, 0\},\$$

there are only two values of k, namely $k \in \{2, 4\}$, for which there exists a power integral basis for the field $\mathbb{Q}(\alpha)$, where $\mathcal{F}_t(\alpha) = 0$. Since these fields are real, they represent fields distinct from the two imaginary monogenic cyclic quartic fields found by Gras. Note, however, that $\mathcal{F}_2(x)$ and $\mathcal{F}_4(x)$ are not monogenic. Nevertheless, from [15], we can easily construct two monogenic quartic polynomials $f_2(x)$ and $f_4(x)$ corresponding respectively to the two real monogenic cyclic quartic fields of Olajos:

$$f_2(x) = x^4 - 10x^3 + 25x^2 - 20x + 5$$
 and $f_4(x) = x^4 - 8x^3 + 16x^2 - 8x - 2$

Straightforward calculations show that

$$\Delta(f_2) = 2^4 \cdot 5^3$$
 and $\Delta(f_4) = 2^{11}$.

While we could not find a family of real monogenic C_4 -quartic polynomials, a computer search revealed four additional distinct real monogenic quartics:

$$g_1(x) = x^4 + 9x^3 + 19x^2 + 9x + 1 \qquad \text{with } \Delta(g_1) = 3^2 \cdot 13^3, \\ g_2(x) = x^4 + 5x^3 + 5x^2 - 5x - 5 \qquad \text{with } \Delta(g_2) = 3^2 \cdot 5^3, \\ g_3(x) = x^4 + 11x^3 + 31x^2 + 11x + 1 \qquad \text{with } \Delta(g_3) = 5^3 \cdot 11^2 \quad \text{and} \\ g_4(x) = x^4 + 7x^3 + 9x^2 - 7x + 1 \qquad \text{with } \Delta(g_4) = 5^3 \cdot 7^2.$$

Using Maple and Theorem 2.3, it is straightforward to verify that the polynomials $f_2(x)$, $f_4(x)$, $g_1(x)$, $g_2(x)$, $g_3(x)$ and $g_4(x)$ are all monogenic. By comparing discriminants and using Maple, it is also easy to see that these polynomials generate distinct real fields. It was brought to our attention by Paul Voutier (private communication) that these six polynomials actually generate six of the twelve real monogenic cyclic quartic fields given by Gras in [6].

The authors of [13] have outlined two approaches to generate distinct monogenic cyclic quartic fields, and they claim to prove that the number of such fields is infinite by providing an argument to show that the set of these fields from their second approach has positive density. However, we believe their density argument is incorrect. This has been corroborated by analytic number theorists, Daniel White and Stanley Xiao, in independent private communications. Thus, it appears that the existence of an infinite family of monogenic cyclic quartic polynomials is still unresolved, at least

unconditionally. Very recently, while this article was still under review, Paul Voutier informed us that he has been able to construct a family of totally real cyclic quartic monogenic polynomials, under the assumption of the *abc*-conjecture for number fields [19].

Acknowledgement

The authors thank the anonymous referee for helpful comments.

References

- A. R. Booker and T. D. Browning, 'Square-free values of reducible polynomials', *Discrete Anal.* 2016 (2016), Article no. 8, 16 pages.
- [2] M.-L. Chang, 'Monogeneity in biquadratic fields', Int. J. Pure Appl. Math. 31(4) (2006), 481–490.
- H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics, 138 (Springer-Verlag, Berlin–Heidelberg, 2000).
- [4] I. Gaál, 'Calculating power integral bases in some quartic fields corresponding to monogenic families of polynomials', Preprint, 2024, arXiv:2405.13429v1.
- [5] T. Gassert, H. Smith and K. Stange, 'A family of monogenic S₄ quartic fields arising from elliptic curves', J. Number Theory 197 (2019), 361–382.
- [6] M.-N. Gras, "Z-bases d'entiers 1, θ, θ², θ³ dans les extensions cycliques de degré 4 de Q', in: Number Theory, 1979–1980 and 1980–1981 (Publications Mathématiques de la Faculté des Sciences de Besançon, Université de Franche-Comté, Besançon, 1981), exp. no. 6, 14 pages.
- [7] M.-N. Gras and F. Tanoé, 'Corps biquadratiques monogènes', *Manuscripta Math.* 86(1) (1995), 63–79.
- [8] J. Huard, B. Spearman and K. Williams, 'Integral bases for quartic fields with quadratic subfields', J. Number Theory 51(1) (1995), 87–102.
- [9] L. Jones, 'Infinite families of reciprocal monogenic polynomials and their Galois groups', *New York J. Math.* 27 (2021), 1465–1493.
- [10] A. Kable, 'Power bases in dihedral quartic fields', J. Number Theory **76**(1) (1999), 120–129.
- [11] L.-C. Kappe and B. Warren, 'An elementary test for the Galois group of a quartic polynomial', *Amer. Math. Monthly* 96(2) (1989), 133–137.
- [12] W. Ledermann and C. van der Ploeg, 'Integral bases of dihedral number fields I', J. Aust. Math. Soc. Ser. A 38(3) (1985), 351–371.
- [13] Y. Motoda, T. Nakahara, A. S. I. Shah and T. Uehara, 'On a problem of Hasse', in: *Algebraic Number Theory and Related Topics 2007*, RIMS Kôkyûroku Bessatsu, B12 (eds. M. Asada, H. Nakamura and H. Takahashi) (Research Institute for Mathematical Sciences (RIMS), Kyoto, 2009), 209–221.
- [14] G. Nyul, 'Power integral bases in mixed biquadratic number fields', Acta Acad. Paedagog. Agriensis Sect. Math. (N.S.) 28 (2001), 79–86.
- [15] P. Olajos, 'Power integral bases in the family of simplest quartic fields', *Exp. Math.* 14(2) (2005), 129–132.
- [16] O. Perron, 'Neue Kriterien f
 ür die Irreduzibilit
 ät algebraischer Gleichungen', J. reine angew. Math. 132 (1907), 288–307.
- [17] H. Smith, 'Two families of monogenic S_4 quartic number fields', Acta Arith. 186(3) (2018), 257–271.
- [18] B. Spearman, 'Monogenic A₄ quartic fields', Int. Math. Forum 1(37–40) (2006), 1969–1974.
- [19] P. Voutier, 'A family of cyclic quartic monogenic polynomials', Preprint, 2024, arXiv:2405.20288v1.
- [20] K. Williams, 'Integers of biquadratic fields', Canad. Math. Bull. 13 (1970), 519–526.

JOSHUA HARRINGTON, Department of Mathematics, Cedar Crest College, Allentown, Pennsylvania, USA e-mail: Joshua.Harrington@cedarcrest.edu

LENNY JONES, Department of Mathematics, Shippensburg University, Shippensburg, Pennsylvania, USA e-mail: doctorlennyjones@gmail.com