Bull. Aust. Math. Soc. (First published online 2024), page 1 of 6*
doi:10.1017/S0004972724000510
*Provisional—final page numbers to be inserted when paper edition is published

MONOGENIC EVEN QUARTIC TRINOMIALS

LENNY JONES

(Received 3 May 2024; accepted 18 May 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 $\{1, \theta, \theta^2, \ldots, \theta^{N-1}\}$ is a basis for the ring of integers of $\mathbb{Q}(\theta)$, where $f(\theta) = 0$. We prove that there exist exactly three distinct monogenic trinomials of the form $x^4 + bx^2 + d$ whose Galois group is the cyclic group of order 4. We also show that the situation is quite different when the Galois group is not cyclic.

2020 *Mathematics subject classification*: primary 11R16; secondary 11R32.

Keywords and phrases: monogenic, cyclic, quartic, 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 $\{1, \theta, \theta^2, \ldots, \theta^{\deg f - 1}\}$ is a basis for the ring of integers $\mathbb{Z}_K$ of $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. From [1], when $f(x)$ is irreducible over $\mathbb{Q}$,

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

where $\Delta(f)$ and $\Delta(K)$ denote the discriminants over $\mathbb{Q}$, respectively, of $f(x)$ and the number field K. Thus, for irreducible $f(x)$, the polynomial $f(x)$ is monogenic if and only if $\Delta(f) = \Delta(K)$. We also say that any number field K is *monogenic* if there exists a power basis for $\mathbb{Z}_K$. We caution the reader 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. A simple example is $f(x) = x^2 - 5$ and $K = \mathbb{Q}(\theta)$, where $\theta = \sqrt{5}$. Then, $\Delta(f) = 20$ 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 $\mathbb{Z}_K$. Observe then that $g(x) = x^2 - x - 1$, the minimal polynomial for $(\theta + 1)/2$ over $\mathbb{Q}$, is monogenic.

This note was motivated by a recent question of Tristan Phillips (private communication) asking if it is possible to determine all distinct monogenic quartic trinomials that have Galois group C_4, the cyclic group of order 4. We consider two monogenic C_4-quartic trinomials $f(x)$ and $g(x)$ to be *distinct* if $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$, where $f(\alpha) = 0 = g(\beta)$. In this note, we provide a partial answer to Phillips's question by proving the following theorem.

THEOREM 1.1. *The three trinomials*

$$x^4 - 4x^2 + 2, \quad x^4 + 4x^2 + 2 \quad \text{and} \quad x^4 - 5x^2 + 5,$$

are the only distinct trinomials of the form $f(x) = x^4 + bx^2 + d \in \mathbb{Z}[x]$ *with* $\mathrm{Gal}(f) \simeq C_4$.

In Section 4, we show that the situation is quite different when $\mathrm{Gal}(f) \not\simeq C_4$, where $f(x) = x^4 + bx^2 + d$.

2. Preliminaries

The following theorem follows from results due to Kappe and Warren.

THEOREM 2.1 [4]. *Let* $f(x) = x^4 + bx^2 + d \in \mathbb{Z}[x]$. *Then* $f(x)$ *is irreducible over* $\mathbb{Q}$ *with* $\mathrm{Gal}(f) \simeq C_4$ *if and only if*

$$d \text{ and } b^2 - 4d \text{ are not squares in } \mathbb{Z}, \text{ but } d(b^2 - 4d) \text{ is a square in } \mathbb{Z}. \tag{2.1}$$

The next result is the specific case for our quartic situation of a 'streamlined' version of Dedekind's index criterion for trinomials that is due to Jakhar, Khanduja and Sangwan. We have used Swan's formula [5] for the discriminant of an arbitrary trinomial $f(x)$ to calculate $\Delta(f)$.

THEOREM 2.2 [3]. *Let* $K = \mathbb{Q}(\theta)$ *be an algebraic number field with* $\theta \in \mathbb{Z}_K$, *the ring of integers of* K, *having minimal polynomial* $f(x) = x^4 + bx^2 + d$ *over* $\mathbb{Q}$. *A prime factor* q *of* $\Delta(f) = 2^4 d(b^2 - 4d)^2$ *does not divide* $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ *if and only if* q *satisfies one of the following conditions:*

(1) *when* $q \mid b$ *and* $q \mid d$, *then* $q^2 \nmid d$;
(2) *when* $q \mid b$ *and* $q \nmid d$, *then*

$$\text{either} \quad q \mid b_2 \text{ and } q \nmid d_1 \quad \text{or} \quad q \nmid b_2(-db_2^2 - d_1^2),$$

where $b_2 = b/q$ *and* $d_1 = (d + (-d)^{q^j})/q$ *with* $q^j \parallel 4$;
(3) *when* $q \nmid b$ *and* $q \mid d$, *then*

$$\text{either} \quad q \mid b_1 \text{ and } q \nmid d_2 \quad \text{or} \quad q \nmid b_1 d_2(-bb_1 + d_2),$$

where $b_1 = (b + (-b)^{q^e})/q$ *with* $q^e \parallel 2$ *and* $d_2 = d/q$;
(4) *when* $q = 2$ *and* $2 \nmid bd$, *then the polynomials*

$$H_1(x) := x^2 + bx + d \quad \text{and} \quad H_2(x) := \frac{bx^2 + d + (-bx - d)^2}{2}$$

are coprime modulo 2;
(5) *when* $q \nmid 2bd$, *then* $q^2 \nmid (b^2 - 4d)$.

https://doi.org/10.1017/S0004972724000510 Published online by Cambridge University Press

3. The proof of Theorem 1.1

Following Theorem 2.1, we assume conditions (2.1) so that $f(x)$ is irreducible over $\mathbb{Q}$ with $\mathrm{Gal}(f) \simeq C_4$. Observe that if $d < 0$, then $d(b^2 - 4d) < 0$, which contradicts the fact that $d(b^2 - 4d)$ is a square. Hence, $d > 0$ and $b^2 - 4d > 0$. Furthermore, since d and $b^2 - 4d$ are not squares, but $d(b^2 - 4d)$ is a square, we deduce that $d \geq 2$ and $b^2 - 4d \geq 2$.

We use Theorem 2.2 to 'force' the monogenicity of $f(x)$. Let q be a prime divisor of d. If $q \nmid (b^2 - 4d)$, then $q \nmid b$, and $q^2 \mid d$ since $d(b^2 - 4d)$ is a square. But then condition (3) of Theorem 2.2 is not satisfied since $q \mid d_2$. Therefore, $q \mid (b^2 - 4d)$ and so $q \mid b$. Note then that if $q^2 \mid d$, then condition (1) is not satisfied. Hence, $q \parallel d$ and therefore, d is squarefree, $d \mid (b^2 - 4d)$ and $d \mid b$.

Suppose next that q is a prime divisor of $b^2 - 4d$, such that $q \nmid d$. If $q \mid b$, then $q = 2$ and

$$A := d(b^2 - 4d)/4 \quad \text{is a square in } \mathbb{Z}. \tag{3.1}$$

We examine condition (2) of Theorem 2.2 to see that

$$d_1 = \frac{d + (-d)^4}{2} \equiv \begin{cases} 1 \pmod 4 & \text{if } d \equiv 1 \pmod 4 \\ 2 \pmod 4 & \text{if } d \equiv 3 \pmod 4). \end{cases}$$

Thus, the first statement under condition (2) is satisfied if and only if

$$(b \bmod 4, d \bmod 4) = (0, 1), \tag{3.2}$$

while the second statement under condition (2) is satisfied if and only if

$$(b \bmod 4,\ d \bmod 4) = (2, 3). \tag{3.3}$$

In scenario (3.2) we have $A \equiv 3 \pmod 4$, while in scenario (3.3) we have $A \equiv 2 \pmod 4$, contradicting (3.1) in each scenario. Hence, $q \nmid b$ and $q \geq 3$. Since $q \nmid d$ and $d(b^2 - 4d)$ is a square, we must have $q^2 \mid (b^2 - 4d)$. But then condition (5) of Theorem 2.2 is not satisfied. Therefore, every prime divisor of $b^2 - 4d$ divides d.

Thus, to summarise, d is squarefree and d and $b^2 - 4d$ have exactly the same prime divisors $p_1 < p_2 < \cdots < p_k$. Hence, since $d(b^2 - 4d)$ is a square, we can write

$$d(b^2 - 4d) = \Big(\prod_{i=1}^{k} p_i\Big)\Big(b^2 - 4\Big(\prod_{i=1}^{k} p_i\Big)\Big) = \prod_{i=1}^{k} p_i^{2e_i}, \tag{3.4}$$

for some integers $e_i \geq 1$. Then, from (3.4),

$$b^2 = \Big(\prod_{i=1}^{k} p_i\Big)\Big(\Big(\prod_{i=1}^{k} p_i^{2e_i-2}\Big) + 4\Big),$$

https://doi.org/10.1017/S0004972724000510 Published online by Cambridge University Press

which implies that

$$\prod_{i=1}^{k} p_i \quad \text{divides} \quad \left(\prod_{i=1}^{k} p_i^{2e_i-2}\right) + 4. \tag{3.5}$$

We see from (3.5) that if some $e_i > 1$, then $p_i \mid 4$ so that $i = 1$ and $p_1 = 2$. In this case,

$$b^2 = 2\left(\prod_{i=2}^{k} p_i\right)(4^{e_1-1} + 4) = \begin{cases} 2^4 \displaystyle\prod_{i=2}^{k} p_i & \text{if } e_1 = 2 \\ 2^3\left(\displaystyle\prod_{i=2}^{k} p_i\right)(4^{e_1-2} + 1) & \text{if } e_1 \geq 3. \end{cases} \tag{3.6}$$

The second case of (3.6) is impossible since $b^2/8 \equiv 1 \pmod 2$. The first case of (3.6) is viable provided $k = 1$, so that $b^2 = 16$ and $d = 2$. This gives the two trinomials

$$x^4 - 4x^2 + 2 \quad \text{and} \quad x^4 + 4x^2 + 2,$$

which are both easily confirmed to be monogenic using Theorem 2.2.

The remaining possibility in (3.5) when $e_i = 1$ for all i yields $k = 1$ and $p_1 = 5$, so that $b^2 = 25$ and $d = 5$. The two resulting trinomials are then

$$x^4 + 5x^2 + 5 \quad \text{and} \quad x^4 - 5x^2 + 5.$$

Again, using Theorem 2.2, it is straightforward to verify that $x^4 + 5x^2 + 5$ is not monogenic (condition (4) fails), while $x^4 - 5x^2 + 5$ is monogenic.

Thus, we have found exactly three monogenic cyclic trinomials

$$x^4 - 4x^2 + 2, \quad x^4 + 4x^2 + 2 \quad \text{and} \quad x^4 - 5x^2 + 5.$$

Note that

$$\Delta(x^4 - 4x^2 + 2) = \Delta(x^4 + 4x^2 + 2) = 2^{11} \quad \text{and} \quad \Delta(x^5 - 5x^2 + 5) = 2^4 5^3. \tag{3.7}$$

If any two of these three trinomials generate the same quartic field, then their discriminants must be equal since they are monogenic. Hence, we see immediately from (3.7) that the quartic field generated by $x^5 - 5x^2 + 5$ is distinct from the other two quartic fields. However, equality of two discriminants is not sufficient to conclude that those trinomials generate isomorphic quartic fields. Indeed, since the field generated by $x^4 - 4x^2 + 2$ is real, while the field generated by $x^4 + 4x^2 + 2$ is nonreal, we deduce that these two fields are in fact distinct. Alternatively, we can verify that these two fields are not isomorphic using MAGMA.

4. The noncyclic monogenic even quartic trinomials

With $f(x) = x^4 + bx^2 + d \in \mathbb{Z}[x]$, we end by showing that the situation when $\mathrm{Gal}(f) \not\simeq C_4$ is quite different from the cyclic case. From [4, Theorem 3], $\mathrm{Gal}(f) \in \{C_4, V, D_4\}$, where V is the Klein 4-group and D_4 is the dihedral group of order 8. Moreover, from [4] and Theorem 2.2, conditions can be formulated to determine when

https://doi.org/10.1017/S0004972724000510 Published online by Cambridge University Press

$f(x)$ is monogenic with $\mathrm{Gal}(f) \in \{V, D_4\}$, and even distinguish between V and D_4. However, unlike the cyclic case, these conditions are not as restrictive and, in fact, lead to the construction of infinite families of distinct monogenic trinomials. For example, in [2], the infinite family

$$\mathcal{F}_2 := \{f_t(x) = x^4 + 4tx^2 + 1 : t \in \mathbb{Z} \text{ and } 4t^2 - 1 \text{ is squarefree}\}$$

of distinct monogenic even V-quartic trinomials is given. Although, to the best of our knowledge, no infinite families of distinct monogenic even D_4-quartic trinomials exist in the literature, we can easily rectify that situation. We claim that the set

$$\mathcal{F}_3 := \{f_t(x) = x^4 + 2x^2 + 4t + 2 : t \in \mathbb{Z} \text{ and } (2t+1)(4t+1) \text{ is squarefree}\}$$

is just such a family. To establish the claim, we use the following theorem that follows from [4].

THEOREM 4.1. *Let $f(x) = x^4 + bx^2 + d \in \mathbb{Z}[x]$. Then $f(x)$ is irreducible over $\mathbb{Q}$ with* $\mathrm{Gal}(f) \simeq D_4$ *if and only if d, $b^2 - 4d$ and $d(b^2 - 4d)$ are all not squares in $\mathbb{Z}$.*

PROOF OF THE CLAIM. Suppose that $f_t(x) \in \mathcal{F}_3$. Clearly, $d = 4t + 2 \equiv 2 \pmod 4$ is not a square in $\mathbb{Z}$. We also see that $b^2 - 4d = -4(4t+1)$ is not a square in $\mathbb{Z}$ since $4t + 1$ is squarefree, and $d(b^2 - 4d) = -8(2t+1)(4t+1)$ is not a square in $\mathbb{Z}$ since $2^3 \parallel -8(2t+1)(4t+1)$. Thus, $f_t(x)$ is irreducible over $\mathbb{Q}$ with $\mathrm{Gal}(f_t) \simeq D_4$, by Theorem 4.1. Noting that $\Delta(f_t) = 2^9(2t+1)(4t+1)^2$, it is then straightforward to verify that $f_t(x)$ is monogenic using Theorem 2.2, and we omit the details.

Finally, suppose that $f_s(x), f_t(x) \in \mathcal{F}_3$ are such that $\mathbb{Q}(\alpha) \simeq \mathbb{Q}(\beta)$, where $f_s(\alpha) = 0 = f_t(\beta)$. Then, since both $f_s(x)$ and $f_t(x)$ are monogenic, we must have that $\Delta(f_s) = \Delta(f_t)$ from (1.1). Using Maple to solve this discriminant equation yields the three solutions

$$\{t = t, s = t\}, \quad \left\{t = t, s = -\frac{t}{2} - \frac{1}{2} + \frac{(-12t^2 - 8t - 1)^{1/2}}{4}\right\},$$
$$\text{and} \quad \left\{t = t, s = -\frac{t}{2} - \frac{1}{2} - \frac{(-12t^2 - 8t - 1)^{1/2}}{4}\right\}.$$

Since $-12t^2 - 8t - 1 \geq 0$ only when $-1/2 \leq t \leq -1/6$, we can conclude that $s = t$, so that the trinomials in $\mathcal{F}_3$ do indeed generate distinct quartic fields, and the claim is established. □

Acknowledgement

The author thanks the referee for valuable suggestions.

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, 138 (Springer-Verlag, Berlin, 2000).

[2] J. Harrington and L. Jones, 'Monogenic quartic polynomials and their Galois groups', Preprint, 2024, arXiv:2404.05487v3.

[3] A. Jakhar, S. Khanduja and N. Sangwan, 'Characterization of primes dividing the index of a trinomial', *Int. J. Number Theory* **13**(10) (2017), 2505–2514.

[4] 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.

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

LENNY JONES, Department of Mathematics,
Shippensburg University, Shippensburg, PA 17257, USA
e-mail: doctorlennyjones@gmail.com