Bull. Aust. Math. Soc. (First published online 2026), page 1 of 5*
doi:10.1017/S0004972726101646
*Provisional—final page numbers to be inserted when paper edition is published

A NOTE ON ABELIAN MONOGENIC TRINOMIALS

LENNY JONES

(Received 27 May 2026 UTC; accepted 2 June 2026 UTC)

Abstract

An *abelian monogenic* polynomial $f(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree $N \geq 2$ that is irreducible over $\mathbb{Q}$, such that the Galois group of $f(x)$ over $\mathbb{Q}$ is abelian, 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 determine all abelian monogenic trinomials of the form $x^{2n} + ax^n + b$, where $n, a, b \in \mathbb{Z}$ with $n \geq 1$ and $ab \neq 0$.

2020 *Mathematics subject classification*: primary 11R09; secondary 11R21, 11R32.

Keywords and phrases: Abelian, Galois, monogenic, trinomial, power-compositional.

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 the number field $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. It is well known [1] that

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

where $\Delta(f)$ and $\Delta(K)$ denote the discriminants over $\mathbb{Q}$ of $f(x)$ and the number field K, respectively. We refer to $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ as the *index* of $f(x)$ and denote it by $\text{index}(f)$. Thus, from (1.1), $f(x)$ is monogenic if and only if $\Delta(f) = \Delta(K)$ or, equivalently, $\text{index}(f)=1$. We say that $f(x)$ is *abelian monogenic* if $f(x)$ is monogenic and the Galois group of $f(x)$ over $\mathbb{Q}$, denoted by $\text{Gal}(f)$, is abelian.

The investigations in this note were motivated by the following results of Marie-Nicole Gras.

THEOREM 1.1 [2]. *Let $N \geq 5$ be an integer with $\gcd(N, 6) = 1$. There exist only finitely many abelian extensions of $\mathbb{Q}$ of degree N whose ring of algebraic integers is monogenic.*

THEOREM 1.2 [3]. *Let $\ell \geq 5$ be prime. Then, there exists at most one cyclic extension $K/\mathbb{Q}$ of degree ℓ. Moreover, if $2\ell + 1$ is prime, then K is the maximal real subfield of the cyclotomic field of index $2\ell + 1$ and if $2\ell + 1$ is not prime, then no such cyclic extension exists.*

© The Author(s), 2026. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 22:47:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101646

THEOREM 1.3 [4]. *Let $K/\mathbb{Q}$ be a cyclic extension of degree ℓ^r, where $\ell \geq 5$ is prime and $r \geq 2$. Let $\mathbb{Z}_K$ denote the ring of integers of K.*

(1) *If $2\ell^r + 1$ is not prime, then $\mathbb{Z}_K$ is not monogenic.*
(2) *If $2\ell^r + 1$ is a prime p and if there exists a prime $q \neq p$ such that q is totally ramified in K, then $\mathbb{Z}_K$ is not monogenic.*

We see that Theorems 1.1, 1.2 and 1.3 are concerned with abelian monogenic number fields whose degree over $\mathbb{Q}$ is relatively prime to 6. Our focus in this note is on the specific trinomials

$$\mathcal{F}_{n,a,b}(x) := x^{2n} + ax^n + b \in \mathbb{Z}[x], \quad \text{where } n \geq 1 \text{ and } ab \neq 0.$$

If $\mathcal{F}_{n,a,b}(x)$ is irreducible over $\mathbb{Q}$, then we make two observations: the degree of the number field $\mathbb{Q}(\alpha)$, where $\mathcal{F}_{n,a,b}(\alpha) = 0$, is not relatively prime to 6 and if d is a divisor of n with $d \geq 1$, then $\mathcal{F}_{d,a,b}(x)$ is also irreducible over $\mathbb{Q}$. It is our goal to determine all abelian monogenic trinomials of the form $\mathcal{F}_{n,a,b}(x)$.

We make some notational remarks. For $\mathcal{F}_{n,a,b}(x)$, we let

$$\mathcal{W} := (a^2 - 4b)/\gcd(2, a)^2.$$

For any integer $N \geq 1$, we let C_N denote the cyclic group of order N, and $\Phi_N(x)$ denote the cyclotomic polynomial of index N and degree $\phi(N)$. For integers r and m with $m \geq 2$, we let the notation '$r \bmod m$' denote the unique integer $z \in \{0, 1, 2, \ldots, m-1\}$ such that $r \equiv z \pmod m$, that is, $r \bmod m = z$. For any integer $n \geq 2$, we define the *radical of n*, denoted $\mathrm{rad}(n)$, to be the product of the distinct prime divisors of n.

Our main result is as follows.

THEOREM 1.4. *The trinomial $\mathcal{F}_{n,a,b}(x)$ is abelian monogenic if and only if (n, a, b) is contained in one of the following pairwise-disjoint sets.*

(1) $\{(1, a, b) : \mathcal{W}$ *is squarefree and*

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

In this case, $\mathrm{Gal}(\mathcal{F}_{1,a,b}) \simeq C_2$.
(2) $\{(2, \pm 4, 2), (2, -5, 5)\}$. *In this case,* $\mathrm{Gal}(\mathcal{F}_{2,a,b}) \simeq C_4$.
(3) $\{(2, a, 1) : \mathcal{W}$ *is squarefree and* $a \bmod 4 \in \{0, 3\}\}$. *In this case,*

$$\mathrm{Gal}(\mathcal{F}_{2,a,1}) \simeq C_2 \times C_2.$$

(4) $\{(2^r, -1, 1) :\ r \geq 2\}$. *In this case,* $\mathcal{F}_{2^r,-1,1}(x) = \Phi_{2^{r+1}\cdot 3}(x)$ *so that*

$$\mathrm{Gal}(\mathcal{F}_{2^r,-1,1}) \simeq C_2 \times C_2 \times C_{2^{r-1}}.$$

(5) $\{(3^s, 1, 1) :\ s \geq 1\}$. *In this case,* $\mathcal{F}_{3^s,1,1}(x) = \Phi_{3^{s+1}}(x)$ *so that* $\mathrm{Gal}(\mathcal{F}_{3^s,1,1}) \simeq C_{2\cdot 3^s}$.
(6) $\{(3^s, -1, 1) :\ s \geq 1\}$. *In this case,* $\mathcal{F}_{3^s,-1,1}(x) = \Phi_{2\cdot 3^{s+1}}(x)$ *so that*

$$\mathrm{Gal}(\mathcal{F}_{3^s,-1,1}) \simeq C_{2\cdot 3^s}.$$

(7) $\{(2^r 3^s, -1, 1) :\ rs \geq 1\}$. *In this case,* $\mathcal{F}_{2^r 3^s,-1,1}(x) = \Phi_{2^{r+1}3^{s+1}}(x)$ *so that*

$$\mathrm{Gal}(\mathcal{F}_{2^r 3^s,-1,1}) \simeq C_2 \times C_2 \times C_{2^{r-1}} \times C_{3^s}.$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 22:47:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101646

2. Preliminaries

The following lemma shows that there are severe restrictions on the value of n if $\mathrm{Gal}(\mathcal{F}_{n,a,b})$ is abelian.

LEMMA 2.1. *Suppose that $\mathcal{F}_{n,a,b}(x)$ is irreducible over $\mathbb{Q}$ and that $\mathrm{Gal}(\mathcal{F}_{n,a,b})$ is abelian. Then, $n = 2^r 3^s$ for some nonnegative integers r and s. Furthermore, if $d \geq 1$ is a divisor of n, then $\mathrm{Gal}(\mathcal{F}_{d,a,b})$ is abelian.*

PROOF. Note that if $n = 1$, then $\mathrm{Gal}(\mathcal{F}_{1,a,b}) \simeq C_2$ is abelian. So, suppose that $n \geq 2$ and let p be a prime divisor of n. Then, $\mathcal{F}_{p,a,b}(x)$ is irreducible over $\mathbb{Q}$ since $\mathcal{F}_{n,a,b}(x) = \mathcal{F}_{p,a,b}(x^{n/p})$ is irreducible over $\mathbb{Q}$. Observe that if α is a zero of $\mathcal{F}_{p,a,b}(x)$, then $\alpha\zeta_p$ is also a zero of $\mathcal{F}_{p,a,b}(x)$, where ζ_p is a primitive pth root of unity. Thus, since $L = \mathbb{Q}(\alpha)$ is normal over $\mathbb{Q}$, L contains the cyclotomic field $\mathbb{Q}(\zeta_p)$. Hence, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ divides $[L : \mathbb{Q}] = 2p$, which implies that $p \in \{2, 3\}$.

Suppose next that $d \geq 2$ is a divisor of n, and let K and L be the respective splitting fields of $\mathcal{F}_{n,a,b}(x)$ and the irreducible trinomial $\mathcal{F}_{d,a,b}(x)$. Then, $L \subseteq K$ and L is normal over $\mathbb{Q}$. It follows that $\mathrm{Gal}(\mathcal{F}_{d,a,b})$ is abelian since otherwise, $\mathrm{Gal}(\mathcal{F}_{n,a,b})$ would have a nonabelian quotient, which is impossible. □

The following four theorems describe the abelian monogenic trinomials $\mathcal{F}_{n,a,b}(x)$ for respectively $n \in \{1, 2, 3, 6\}$. The proofs can be found in [6].

THEOREM 2.2. *Suppose that $\mathcal{F}_{1,a,b}(x)$ is irreducible over $\mathbb{Q}$. Then, $\mathcal{F}_{1,a,b}(x)$ is abelian monogenic if and only if $\mathcal{W}$ is squarefree and*

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

THEOREM 2.3. *Suppose that $\mathcal{F}_{2,a,b}(x)$ is irreducible over $\mathbb{Q}$. Then, $\mathcal{F}_{2,a,b}(x)$ is abelian monogenic and:*

(1) $\mathrm{Gal}(\mathcal{F}_{2,a,b}) \simeq C_4$ *if and only if* $\mathcal{F}_{2,a,b}(x) \in \{x^4 \pm 4x^2 + 2,\ x^4 - 5x^2 + 5\}$;
(2) $\mathrm{Gal}(\mathcal{F}_{2,a,b}) \simeq C_2 \times C_2$ *if and only if $\mathcal{W}$ is squarefree and*

$$\mathcal{F}_{2,a,b}(x) \in \{x^4 + ax^2 + 1 : a \bmod 4 \in \{0, 3\}\}.$$

THEOREM 2.4. *Suppose that $\mathcal{F}_{3,a,b}(x)$ is irreducible over $\mathbb{Q}$. Then, $\mathcal{F}_{3,a,b}(x)$ is abelian monogenic if and only if $\mathcal{F}_{3,a,b}(x) \in \{x^6 - x^3 + 1,\ x^6 + x^3 + 1\}$, in which case,* $\mathrm{Gal}(\mathcal{F}_{3,a,b}) \simeq C_6$.

THEOREM 2.5. *Suppose that $\mathcal{F}_{6,a,b}(x)$ is irreducible over $\mathbb{Q}$. Then, $\mathcal{F}_{6,a,b}(x)$ is abelian monogenic if and only if $\mathcal{F}_{6,a,b}(x) = x^{12} - x^6 + 1$, in which case,* $\mathrm{Gal}(\mathcal{F}_{6,a,b}) \simeq C_2 \times C_6$.

The next lemma is an application to our specific situation of a theorem due to Kaur, Kumar and Remete [7, Theorem 1.1].

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 22:47:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101646

LEMMA 2.6. *Let $n, a, b, r, s \in \mathbb{Z}$ such that $n = 2^r 3^s$ with $n \notin \{1, 2, 3, 6\}$ and $ab \neq 0$. Let $k = n/\mathrm{rad}(n)$. Then, $k > 1$ and*

$$\mathcal{F}_{n,a,b}(x) = \mathcal{F}_{\mathrm{rad}(n),a,b}(x^k).$$

If $\mathcal{F}_{n,a,b}(x)$ is irreducible over $\mathbb{Q}$, then $\mathcal{F}_{n,a,b}(x)$ is monogenic if and only if all of the following conditions are satisfied:

(1) *b is squarefree;*
(2) *q does not divide* index*$(\mathcal{F}_{n,a,b})$ for all prime divisors q of k;*
(3) *$\mathcal{F}_{\mathrm{rad}(n),a,b}(x)$ is monogenic.*

3. Proof of Theorem 1.4

PROOF. Suppose first that $\mathcal{F}_{n,a,b}(x)$ is abelian monogenic. Thus, $n = 2^r 3^s$, for some nonnegative integers r and s, by Lemma 2.1. Then, using Theorems 2.2, 2.3, 2.4 and 2.5, along with Lemma 2.6, and considering the four cases

$$(r = 0, s = 0), \quad (r \geq 1, s = 0), \quad (r = 0, s \geq 1) \quad \text{and} \quad (r \geq 1, s \geq 1), \tag{3.1}$$

we arrive at the exact sets given in the statement of the theorem.

Since the methods for each of the cases in (3.1) are similar, we provide details only for the case $(r \geq 1, s = 0)$, which will yield the sets in items (2), (3) and (4) in the statement of the theorem. If $r = 1$, then $\mathcal{F}_{2,a,b}(x)$ is monogenic by assumption. If $r \geq 2$, then, since

$$\mathcal{F}_{n,a,b}(x) = \mathcal{F}_{2^r,a,b}(x) = \mathcal{F}_{2,a,b}(x^{2^{r-1}})$$

is monogenic, it follows from Lemma 2.6 that $\mathcal{F}_{2,a,b}(x)$ is monogenic. That is, in either situation, $\mathcal{F}_{2,a,b}(x)$ is monogenic. Therefore, we deduce from Theorem 2.3 the two possibilities for (a, b):

$$(a, b) \in \{(\pm 4, 2), (-5, 2)\} \quad \text{or} \quad a \bmod 4 \in \{0, 3\},\ b = 1 \text{ with } \mathcal{W} \text{ squarefree}. \tag{3.2}$$

Hence, if $r = 1$, then $(n, a, b) = (2, a, b)$ is contained in either the set of item (2) or the set of item (3). If $r \geq 2$, then it is easy to verify, using a computer algebra system, that $\mathcal{F}_{2^2,\pm 4,2}(x)$ and $\mathcal{F}_{2^2,-5,2}(x)$ are nonabelian. Consequently, $\mathcal{F}_{2^r,\pm 4,2}(x)$ and $\mathcal{F}_{2^r,-5,2}(x)$ are nonabelian for any $r \geq 2$ by Lemma 2.1. For the second possibility in (3.2), it follows from [5] that $\mathcal{F}_{2^2,a,1}(x)$ is abelian only when $a = -1$. Thus, in this situation, we get $\mathcal{F}_{2^2,-1,1}(x) = \Phi_{24}(x)$, so that $\mathcal{F}_{2^2,-1,1}(x)$ is monogenic and $\mathrm{Gal}(\mathcal{F}_{2^2,-1,1}) \simeq C_2 \times C_2 \times C_2$. Therefore, $(n, a, b) = (2^r, -1, 1)$ is contained in the set of item (4) in the theorem since, when $r \geq 3$, we have $\mathcal{F}_{2^r,-1,1}(x) = \Phi_{2^{r+1}\cdot 3}(x)$.

Conversely, if (n, a, b) is contained in one of the seven sets given in the statement of the theorem, then it is straightforward to confirm that $\mathcal{F}_{n,a,b}(x)$ is abelian monogenic. For example, if $(n, a, b) \in \{(2^r 3^s, -1, 1) : rs \geq 1\}$, then it is easy to verify that $\mathcal{F}_{2^r 3^s,-1,1}(x) = \Phi_{2^{r+1}3^{s+1}}(x)$. Hence,

$$\mathrm{Gal}(\mathcal{F}_{2^r 3^s,-1,1}) \simeq C_2 \times C_2 \times C_{2^{r-1}} \times C_{3^s},$$

and $\mathcal{F}_{2^r 3^s,-1,1}(x)$ is monogenic by [8, Theorem 2.6]. □

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 22:47:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101646

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, 138 (Springer-Verlag, Berlin, 2000).
[2] M.-N. Gras, 'Non monogénéité de l'anneau des entiers de certaines extensions abélienne de Q' (in French), *Publ. Math. de Besançon. Algèbre et théorie des nombres* **1984** (1984), Article no. 5, 25 pages.
[3] M.-N. Gras, 'Non monogénéité de l'anneau des entiers des extensions cycliques de Q de degré premier $\ell \geq 5$' (in French), *J. Number Theory* **23**(3) (1986), 347–353.
[4] M.-N. Gras, 'Condition nécessaire de monogénéité de l'anneau des entiers d'une extension abélienne de Q' (in French), in: *Séminaire de théorie des nombres, Paris 1984–85* (ed. C. Goldstein), Progress in Mathematics, 63 (Birkhäuser, Boston, MA, 1986), 97–107.
[5] L. Jones, 'Monogenic even octic polynomials and their Galois groups', *New York J. Math.* **31** (2025), 91–125.
[6] L. Jones, 'Characterizing monogenic trinomials $x^{12} + ax^6 + b$ according to their Galois groups', Preprint, 2026, arXiv:2604.18830.
[7] S. Kaur, S. Kumar and L. Remete, 'On the index of power compositional polynomials', *Finite Fields Appl.* **107** (2025), Article no. 102642, 20 pages.
[8] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edn, Graduate Texts in Mathematics, 83 (Springer-Verlag, New York, 1997).

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

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 22:47:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0004972726101646