Mathematica Bohemica

Hamid Ben Yakkou

On common index divisors and monogenity of septic number fields defined by trinomials of type $x^7 + ax^5 + b$

Mathematica Bohemica, Vol. 150 (2025), No. 2, 245–262

Persistent URL: http://dml.cz/dmlcz/152974

ON COMMON INDEX DIVISORS AND MONOGENITY OF SEPTIC NUMBER FIELDS DEFINED BY TRINOMIALS OF TYPE $x^7 + ax^5 + b$

Hamid Ben Yakkou

Received September 28, 2023. Published online November 5, 2024.
Communicated by Clemens Fuchs

Abstract. Let K be a septic number field generated by a root θ of an irreducible polynomial $F(x) = x^7 + ax^5 + b \in \mathbb{Z}[x]$. In this paper, we explicitly characterize the index $i(K)$ of K. More precisely, for all a and b, we show that $i(K) \in \{1, 2\}$. Our results answer completely to Problem 22 of W. Narkiewicz's book (2004) for these families of number fields. In particular, we provide sufficient conditions for which K is not monogenic. We illustrate our results by some computational examples.

Keywords: monogenity; power integral basis; theorem of Ore; prime ideal factorization; common index divisor; Newton polygon

MSC 2020: 11R04, 11R16, 11R21, 11Y40

1. Introduction

Let K be a number field generated by θ, a root of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$ of degree n, and A_K its ring of integers. It is well-known that A_K is a free $\mathbb{Z}$-module of rank n. We say that the ring A_K has a power integral basis if it is generated by one element as a $\mathbb{Z}$-module, that is $A_K = \mathbb{Z}[\eta]$ for some primitive element η of A_K. In such a case, K is said to be monogenic. Otherwise, K is called not monogenic. The familiar examples of monogenic number fields are quadratic and cyclotomic fields.

Throughout this paper, for every $\eta \in A_K$ generating K, $\operatorname{ind}(\eta)$ denotes the index of $\mathbb{Z}[\eta]$ in A_K and $i(K)$ denotes the index of K as defined by Dedekind:

$$i(K) := \gcd\{\operatorname{ind}(\eta) \colon \eta \in A_K \text{ and } K = \mathbb{Q}(\eta)\}. \tag{1.1}$$

So, $i(K) = 1$ for every monogenic number field K. However, if $i(K) > 1$, then K is not monogenic. A prime p is called a common index divisor of K if p divides $i(K)$.

DOI: 10.21136/MB.2024.0148-23

Dedekind was the first one to show the existence of a common divisor of indices. He exhibited an example of a cubic number field in which 2 is a common divisor of indices. He showed that 2 divides $i(K)$, where $K = \mathbb{Q}(\theta)$ and $\theta^3 - \theta^2 - 2\theta - 8$ (cf. [30], page 64). In [11], Engstrom gave explicit formulas which compute $\nu_p(i(K))$, the highest power of p dividing $i(K)$, according to the type of splitting of p in A_K, and employed these results to compute $\nu_p(i(K))$ for all number fields of degrees less or equal 7. Nart in [31] determined $\nu_p(i(K))$ in totally ramified cases. The problem of determination of $\nu_p(i(K))$ is referred as Problem 22 of Narkiewicz (see [30]).

The problem of testing the monogenity and non-monogenity of number fields and constructing power integral bases have been the subject of extensive research. To determine whether a number field K is monogenic or not, one must solve the corresponding index form equations, see, e.g., [7], [13], [14], [17], [20], [21], [33], where the authors develop efficient algorithms for a great number of classes of number fields.

In [20], [21], [23], [24], Győry made a general breakthrough by proving in full generality that for any $I \in \mathbb{Z}$ the index form equation $I(x_2, \dots, x_n) = I$ (in $x_2, x_3, \dots, x_n \in \mathbb{Z}$) associated to an integral basis of K can have only finitely many integral solutions and gives effective bounds for the solutions. The best known bounds for the solutions can be found in [13]. He also reduced index form equations to the system of unit equations in [25] and gave effective results regarding the monogenity of relative extensions in [22] and [24]. For more details, we suggest consulting the books [12], [13] by Evertse and Győry which provide comprehensive studies regarding discriminant form and index form theory and their practical applications, including relevant Diophantine equations and monogenity of number fields.

In [17], Gaál and Schulte gave efficient algorithms for solving index form equations in cubic number fields. In [16], Gaál, Pethő and Pohst provided algorithms for solving index form equations in a quartic number field. In [34], Pethő and Ziegler gave an efficient criterion to decide whether the maximal order of a biquadratic number field has a unit power integral basis or not. For multiquadratic number fields, we refer to [33] by Pethő and Pohst.

Combining the general approach of [21] and its refined version [25] with some other technical results, Gaál and Győry [7] and Bilu et al. [15] described algorithms and used them to solve index form equations in quintic, respectively, sextic number fields.

Nakahara's research team based their method on the existence of relative power integral bases of some special sub-fields. They studied the monogenity of several number fields: for example, under the assumption that $m \not\equiv \pm 1 \pmod 9$, Ahmad, Nakahara and Husnine [2], and Ahmad, Nakahara and Hameed [1] showed that the pure sextic number field $\mathbb{Q}(\sqrt[6]{m})$ with square-free m is monogenic when $m \equiv 2, 3 \pmod 4$,

but it is not monogenic when $m \equiv 1 \pmod 4$, respectively. For some results regarding the monogenity of certain pure number fields see [5], [6] by Ben Yakkou et al. For a survey on monogenity with a focus on efficient algorithms for several classes of number fields, see the books [13] by Evertse and Győry and [14] by Gaál.

Recently, many authors have been interested in the study of indices, monogenity and non-monogenity of the number field defined by roots of trinomials of type $x^n + ax^m + b$. Llorente and Nart (see [28]) proved that for a cubic number field defined by $x^3 + ax + b$, $i(K) = 1$ or 2 and gave a necessary and sufficient condition for $i(K) = 2$. In [9], Davis and Spearman showed that the index of a quartic number field defined by $x^4 + ax + b$ is contained in the set $\{1, 2, 3, 6\}$. Ben Yakkou and Boudine [4] studied the index of the octic number field defined by $x^8 + ax + b$. In [26], Jakhar, Khanduja and Sangwan studied the problem of the integral closedness of $\mathbb{Z}[\theta]$: they gave necessary and sufficient conditions for a prime p to be a divisor of $\mathrm{ind}(\theta)$. However, by the definition (1.1) of $i(K)$, the divisibility of $\mathrm{ind}(\theta)$ by p is not sufficient to decide whether p is a common index divisor of K or not. Therefore, their results do not characterize the prime divisors of indices of these number fields. In [3], Ben Yakkou gave some sufficient conditions on coefficients of a trinomial $x^n + ax^m + b$ for which K has an odd prime common index divisor which guarantees the non-monogenity of the number field defined by such a trinomial. Also, in [27], Jones and White identify infinite parametric families of monogenic trinomials with a non square-free discriminant.

The aim of the present paper is to determine the index of any number field K generated by a root θ of an irreducible trinomial of type $F(x) = x^7 + ax^5 + b \in \mathbb{Z}[x]$. Note that all the available results cannot be applied to characterize the prime common index divisors and to answer the question of monogenity for these number fields. So, we are motivated to study separately these families of number fields. To reach our goal, we have based our method on prime ideal factorization via Newton polygon techniques.

2. Main results

In what follows, let K be a septic number field generated by θ, a root of a monic irreducible trinomial $F(x) = x^7 + ax^5 + b \in \mathbb{Z}[x]$, and A_K its ring of integers. For every prime p and any nonzero p-adic integer m, $\nu_p(m)$ denotes the p-adic valuation of m, the highest power of p dividing m, and $m_p := m/p^{\nu_p(m)}$. Scaling the coefficients if necessary, we lose no generality in assuming

$$\nu_p(a) < 2 \quad \text{or} \quad \nu_p(b) < 7. \tag{2.1}$$

For simplicity, if $pA_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ is the factorization of pA_K into a product of powers of distinct prime ideals in A_K with residue degrees $f(\mathfrak{p}_i/p) = [A_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}] = f_i$, then we write $pA_K = [f_1^{e_1}, \dots, f_g^{e_g}]$. Also, if $e_i = 1$ for some i, then we shortly write f_i instead of $f_i^{e_i}$.

In this paper, we prove the following results.

Theorem 2.1. *Let $K = \mathbb{Q}(\theta)$ be a number field with θ being a root of a monic irreducible polynomial $F(x) = x^7 + ax^5 + b \in \mathbb{Z}[x]$. Then for any odd prime p, p is not a common index divisor of K; p does not divide $i(K)$.*

From the above theorem, the only candidate prime to divide $i(K)$ is 2. Thus, either $i(K) = 1$ or $i(K) = 2^k$ for some positive integer k. The following result gives the complete answer. Precisely, we prove that $i(K)$ is either 1 or 2.

Theorem 2.2. *Let K be a number field generated by a root θ of an irreducible trinomial $F(x) = x^7 + ax^5 + b \in \mathbb{Z}[x]$. Then* Table 1 *gives the form of the factorization of the ideal $2A_K$ into a product of powers of distinct prime ideals of A_K and the exact value of the index $i(K)$ in every case. In particular, 2 is a common index divisor of K if and only if one of the conditions* C9, C10, C11, C17 *holds.*

Corollary 2.3. *Let $K = \mathbb{Q}(\theta)$ be a number field with θ being a root of a monic irreducible polynomial $F(x) = x^7 + ax^5 + b \in \mathbb{Z}[x]$. Then*

(1) *$i(K) = 2$ if and only if one of the conditions* C9, C10, C11, C17 *holds. Otherwise, $i(K) = 1$.*
(2) *If any one of the conditions* C9, C10, C11, C17 *holds, then K is not monogenic; $\mathbb{Z}_K$ has no power integral basis.*

R e m a r k 2.4. The condition $i(K) = 1$ is not sufficient for K to be monogenic. A number field K can have index 1, but A_K has no power integral basis. Thanks to the following example: $K = \mathbb{Q}(\sqrt[3]{175})$ (see [30], page 56).

3. Examples

To illustrate our results, we propose some examples. Let $K = \mathbb{Q}(\theta)$ be a septic number field with θ a root of an irreducible polynomial $F(x) = x^7 + ax^5 + b \in \mathbb{Z}[x]$.

(1) Let $F(x) = x^7 + 867x^5 + 68$. Since $F(x)$ is a 17-Eisenstein polynomial, it is irreducible over $\mathbb{Q}$. By Case C9 of Table 1 of Theorem 2.2, $i(K) = 2$. So, K is not monogenic.

(2) Let $F(x) = x^7 + 45927x^5 + 24$. The polynomial $F(x)$ is irreducible over $\mathbb{Q}$ as it is a 3-Eisenstein polynomial. In view of Case C10 of Table 1 of Theorem 2.2, $i(K) = 2$. Consequently, A_K has no power integral basis.

(3) Let $F(x) = x^7 + 33x^5 + 66$. As $F(x)$ is an 11-Eisenstein polynomial, it is irreducible over $\mathbb{Q}$. According to Case C17 of Table 1, K is not monogenic and $i(K) = 2$.

(4) Let $F(x) = x^7 + p^r x^5 + p$, where p is an odd prime and r is a positive integer. By Theorem 2.1 and Case C1 of Table 1, $i(K) = 1$.

Case	Conditions	Factorization of $2A_K$	$i(K)$
C1	$a \equiv 1 \pmod 2$ and $b \equiv 1 \pmod 2$	$[2^1, 5^1]$	1
C2	$a \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$	$[1, 3, 3]$	1
C3	$7\nu_2(a) > 2\nu_2(b)$ and $\nu_2(b) \in \{1, 2, 3, 4, 5, 6\}$	$[1^7]$	1
C4	$\nu_2(a) = 1, \nu_2(b) \geqslant 4$ and $5 \nmid \nu_2(b) - 1$	$[1^2, 1^5]$	1
C5	$\nu_2(a) = 1, \nu_2(b) \geqslant 4$ and $5 \mid \nu_2(b) - 1$	$[1, 1^2, 4]$	1
C6	$a \equiv 3 \pmod 8, b \equiv 0 \pmod 8$ and $5 \nmid \nu_2(b)$	$[1^5, 2]$	1
C7	$a \equiv 3 \pmod 8, b \equiv 0 \pmod 8$ and $5 \mid \nu_2(b)$	$[1, 2, 4]$	1
C8	$a \equiv 7 \pmod 8, b \equiv 4 \pmod 8$	$[2, 1^5]$	1
C9	$a \equiv 3 \pmod 8, b \equiv 4 \pmod 8$	$[1, 1, 1^5]$	2
C10	$a \equiv 7 \pmod 8, b \equiv 0 \pmod 8$ and $5 \nmid \nu_2(b)$	$[1, 1, 1^5]$	2
C11	$a \equiv 7 \pmod 8, b \equiv 0 \pmod 8$ and $5 \mid \nu_2(b)$	$[1, 1, 1, 4]$	2
C12	$a \equiv 3 \pmod 4$ and $b \equiv 2 \pmod 4$	$[1^2, 1^5]$	1
C13	$a \equiv 1 \pmod 4, b \equiv 0 \pmod 4$ and $5 \nmid \nu_2(b)$	$[1^2, 1^5]$	1
C14	$a \equiv 1 \pmod 4, b \equiv 0 \pmod 4$ and $5 \mid \nu_2(b)$	$[1, 1^2, 4]$	1
C15	$(a, b) \in \{(1, 10), (9, 2), (1, 6), (9, 14)\} \pmod{16}$	$[1^2, 1^5]$	1
C16	$(a, b) \in \{(1, 18), (17, 2), (1, 14), (17, 30)\} \pmod{32}$	$[2, 1^5]$	1
C17	$(a, b) \in \{(1, 2), (17, 18), (1, 30), (17, 14)\} \pmod{32}$	$[1, 1, 1^5]$	2
C18	$(a, b) \in \{(5, 2), (5, 14), (13, 6), (13, 10)\} \pmod{16}$	$[1^2, 1^5]$	1

Table 1. The factorization of $2A_K$ and the value of $i(K)$.

4. Preliminary results

Let K be a number field generated by θ, a root of a monic irreducible trinomial $F(x) = x^7 + ax^5 + b \in \mathbb{Z}[x]$, and A_K its ring of integers. Let p be a prime and $\mathbb{F}_p$ denote the finite field with the p elements. The following result is one of the most basic results on the index of a number field. It gives a necessary and sufficient condition for a prime p to be a common index divisor of K. This lemma will play an important role in the proof of our results (see [30], Theorems 4.33–4.34 and [10]).

Lemma 4.1. *Let p be a prime and K a number field. For every positive integer f, let $L_p(f)$ denote the number of distinct prime ideals of A_K lying above p with residue degree f and $N_p(f)$ denote the number of monic irreducible polynomials of $\mathbb{F}_p[x]$ of degree f. Then p is a common index divisor of K if and only if $L_p(f) > N_p(f)$ for some positive integer f.*

To apply Lemma 4.1, we need to determine the number of distinct prime ideals of A_K lying above p. We use Newton polygon techniques. So, let us shortly recall some fundamental notions and results on this method on which the proof of our results are based. For more details, we refer to [18], [19] by Guàrdia, Montes and Nart, [29] by Montes and Nart and [32] by Ore.

Let p be a prime and ν_p denote the discrete valuation of $\mathbb{Q}_p(x)$ defined on $\mathbb{Z}_p[x]$ by

$$\nu_p\left(\sum_{i=0}^{m} a_i x^i\right) = \min\{\nu_p(a_i),\ 0 \leqslant i \leqslant m\}.$$

Let $\varphi(x) \in \mathbb{Z}[x]$ be a monic polynomial whose reduction modulo p is irreducible. The polynomial $F(x) \in \mathbb{Z}[x]$ admits a unique φ-adic expansion

$$F(x) = a_0(x) + a_1(x)\varphi(x) + \ldots + a_n(x)\varphi(x)^n$$

with $\deg(a_i(x)) < \deg(\varphi(x))$. For every $0 \leqslant i \leqslant n$, let $u_i = \nu_p(a_i(x))$. The φ-Newton polygon of $F(x)$ with respect to ν_p is the lower boundary convex envelope of the set of points $\{(i, u_i), 0 \leqslant i \leqslant n, a_i(x) \neq 0\}$ in the Euclidean plane, which we denote by $N_\varphi(F)$. The polygon $N_\varphi(F)$ is the union of different adjacent sides $S_1, S_2, \ldots, S_g$ with increasing slopes $\lambda_1, \lambda_2, \ldots, \lambda_g$. We write $N_\varphi(F) = S_1 + S_2 + \ldots + S_g$. The polygon determined by the sides of negative slopes of $N_\varphi(F)$ is called the φ-principal Newton polygon of $F(x)$ with respect to ν_p (or p) and is denoted by $N_\varphi^+(F)$. The length of $N_\varphi^+(F)$ is $l(N_\varphi^+(F)) = \nu_{\overline{\varphi}}(\overline{F(x)})$, the highest power of $\varphi(x)$ dividing $F(x)$ modulo p.

Let $\mathbb{F}_\varphi$ be the finite field $\mathbb{Z}[x]/(p, \varphi(x)) \simeq \mathbb{F}_p[x]/(\overline{\varphi(x)})$. We attach to any abscissa $0 \leqslant i \leqslant l(N_\varphi^+(F))$ the following residual coefficient $c_i \in \mathbb{F}_\varphi$:

$$c_i = \begin{cases} 0 & \text{if } (i, u_i) \text{ lies strictly above } N_\varphi^+(F), \\ \dfrac{a_i(x)}{p^{u_i}} \pmod{(p, \varphi(x))} & \text{if } (i, u_i) \text{ lies on } N_\varphi^+(F). \end{cases}$$

Let S be one of the sides of $N_\varphi^+(F)$. Then the length of S, denoted by $l(S)$, is the length of its projection to the horizontal axis and its height, denoted by $h(S)$, is the length of its projection to the vertical axis. Let $\lambda = -h(S)/l(S) = -h/e$ be its slope, where e and h are two positive coprime integers. The degree of S is $d(S) := \gcd(h(S), l(S)) = l(S)/e$; it is equal to the number of segments into which

the integral lattices divide S. More precisely, if (s, u_s) is the initial point of S, then the points with integer coordinates lying in S are exactly

$$(s, u_s), (s + e, u_s - h), \ldots, (s + de, u_s - dh).$$

The positive integer $e = l(S)/d(S)$ is called the ramification index of the side S and denoted by $e(S)$. We attach to S the residual polynomial

$$R_l(F)(y) = c_s + c_{s+e}y + \ldots + c_{s+(d-1)e}y^{d-1} + c_{s+de}y^d \in \mathbb{F}_\varphi[y].$$

Now, we give some related definitions to this algorithm.

Definition 4.2. Let $F(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial. Let $F(x) \equiv \prod_{i=1}^{t} \varphi_i(x)^{l_i} \pmod p$ be the factorization of $F(x)$ into a product of powers of distinct monic irreducible polynomials in $\mathbb{F}_p[x]$. For every $i = 1, \ldots, t$, let $N^+_{\varphi_i}(F) = S_{i1} + \ldots + S_{ir_i}$, and for every $j = 1, \ldots, r_i$, let $R_{l_{ij}}(F)(y) = \prod_{s=1}^{s_{ij}} \psi_{ijs}^{n_{ijs}}(y)$ be the factorization of $R_{l_{ij}}(F)(y)$ in $\mathbb{F}_{\varphi_i}[y]$.

(1) For every $i = 1, \ldots, t$, the φ_i-index of $F(x)$, denoted by $\mathrm{ind}_{\varphi_i}(F)$, is $\deg(\varphi_i)$ multiplied by the number of points with natural integer coordinates that lie below or on the polygon $N^+_{\varphi_i}(F)$, strictly above the horizontal axis and strictly beyond the vertical axis.

(2) The polynomial $F(x)$ is said to be φ_i-regular with respect to ν_p if for every $j = 1, \ldots, r_i$, $R_{l_{ij}}(F)(y)$ is separable, that is $n_{ijs} = 1$.

(3) The polynomial $F(x)$ is said to be p-regular if it is φ_i-regular for every $1 \leqslant i \leqslant t$.

Now, we recall Ore's Theorem which will be used in the proof of Theorems 2.1 and 2.2 (see [18], Theorems 1.13, 1.15 and 1.19, [29] and [32]).

Theorem 4.3 (Ore's Theorem)**.** *Let K be a number field generated by θ, a root of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$. Under the above notations, we have*

(1)

$$\nu_p(\mathrm{ind}(\theta)) \geqslant \sum_{i=1}^{t} \mathrm{ind}_{\varphi_i}(F).$$

Moreover, the equality holds if $F(x)$ is p-regular.

(2) *If $F(x)$ is p-regular, then*

$$pA_K = \prod_{i=1}^{t} \prod_{j=1}^{r_i} \prod_{s=1}^{s_{ij}} \mathfrak{p}_{ijs}^{e_{ij}},$$

where e_{ij} is the ramification index of the side S_{ij} and $f_{ijs} = \deg(\varphi_i) \times \deg(\psi_{ijs})$ is the residue degree of $\mathfrak{p}_{ijs}$ over p.

The following result is an immediate consequence of the above theorem.

Corollary 4.4. *Under the above hypotheses, the following hold:*

(1) *If $l_i = 1$ for some $i = 1, \dots, t$, then the factor $\varphi_i(x)$ provides that a unique prime ideal of A_K lies above p of residue degree equals $\deg(\varphi_i(x))$ and of ramification index equals 1.*

(2) *If for some $i = 1, \dots, t$, $N^+_{\varphi_i}(F)$ has k distinct sides of degree 1 each, then the factor $\varphi_i(x)$ provides k distinct prime ideals of A_K lying above p with the same residue degree equals $\deg(\varphi_i(x))$ with ramification indices $e(\mathfrak{p}_{ij1}/p) = e(S_{ij})$, $j = 1, \dots, k$.*

The proof of the following example in the quartic case is based on the application of Ore's Theorem.

E x a m p l e 4.5. Consider $F(x) = x^4 + 2312x^3 + 119 \in \mathbb{Z}[x]$. Since $F(x)$ is a 17-Eisenstein polynomial, $F(x)$ is irreducible over $\mathbb{Q}$. Let θ be a root of $F(x)$ and $K := \mathbb{Q}(\theta)$. We propose to determine $i(K)$. It is known by Engstrom's work (see [11]) that $i(K) = 2^u \cdot 3^v$ with $u \leqslant 2$ and $v \leqslant 1$. For $p = 3$, we have $F(x) \equiv x^4 - x^3 - 1 \pmod 3$. By Corollary 4.4, $3A_K$ is a prime ideal of A_K. Therefore, by Lemma 4.1, $3 \nmid i(K)$, and so $v = 0$. For $p = 2$, we have $F(x) \equiv (x-1)^4 \pmod 2$. Let $\varphi_1 = x - 1$. The φ_1-adic expansion of $F(x)$ is

$$F(x) = 2432 + 6940\varphi_1(x) + 6942\varphi_1(x)^2 + 2316\varphi_1(x)^3 + \varphi_1(x)^4.$$

Computing the 2-adic valuations of the coefficients in the above expansion, we see that $\nu_2(2432) = 7$, $\nu_2(6940) = 2$, $\nu_2(6942) = 1$ and $\nu_2(2316) = 2$. Thus, $N^+_{\varphi_1}(F) = S_{11} + S_{12} + S_{13}$ has three distinct sides of degree 1, each with respective slopes $l_{11} = -5$, $l_{12} = -1$ and $l_{13} = -\frac{1}{2}$. Precisely, $N^+_{\varphi_1}(F)$ is the lower convex hull of the points $(0,7), (1,2), (2,1), (3,2)$ and $(4,0)$ (see Figure 1). Further, we have $\mathrm{ind}(\varphi_1) = 3$. The corresponding residual polynomials are the same: $R_{l_{1k}}(F)(y) = y - 1 \in \mathbb{F}_{\varphi_1}[y] \simeq \mathbb{F}_2[y]$, $k = 1, 2, 3$. So, they are separable as they have degree 1 each. Thus, $F(x)$ is φ_1-regular. So, it is 2-regular. Applying Theorem 4.3, we see that

$$\nu_2(\mathrm{ind}(\theta)) = \mathrm{ind}(\varphi_1) = 3,$$

and

$$2A_K = \mathfrak{p}_{111}\mathfrak{p}_{121}\mathfrak{p}^2_{131},$$

where $\mathfrak{p}_{111}$, $\mathfrak{p}_{121}$ and $\mathfrak{p}_{131}$ are the three distinct prime ideals of A_K of residue degree $f(\mathfrak{p}_{1k1}/2) = \deg(R_{l_{1k}}(F)) \times \deg(\varphi_1) = 1 \times 1 = 1$ for $k = 1, 2, 3$. By Engstrom's table concerning indices of number fields of degree less than 7 (see [11], page 234), we have $u = 1$. We conclude that $i(K) = 2$, and so K is not monogenic.

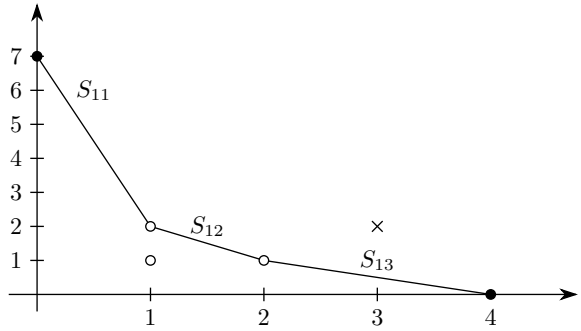

Figure 1. $N^+_{\varphi_1}(F)$ with respect to ν_2.

Recall also the following useful result which is a special case of [8], Theorem 4.8.5 in the context of septic number fields.

Lemma 4.6. *Let $K = \mathbb{Q}(\theta)$ and $F(x)$ be as in Theorems* 2.1 *and* 2.2. *Let p be a prime. If $pA_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ is the factorization of pA_K into a product of powers of distinct prime ideals in A_K with residue degrees $f(\mathfrak{p}_i/p) = f_i$, then $\sum_{i=1}^{g} e_i f_i = 7$.*

5. Proofs of the main results

After recalling necessary preliminaries and results in the previous section, we are now in the position to prove our main results. Let us begin by Theorem 2.1.

P r o o f of Theorem 2.1. Since the degree of K is 7, by the result of Żyliński (see [35]), if p divides $i(K)$, then $p < 7$, see also [11] by Engstrom. Therefore, the candidate primes to be common index divisors of K are $2, 3$ and 5. So, to prove this theorem, it is sufficient to show that $3 \nmid i(K)$ and $5 \nmid i(K)$. On the other hand, by [30], Proposition 2.13, for any $\eta \in \mathbb{Z}_K$, we have the index formula

$$\nu_p(D(\eta)) = 2\nu_p(\mathrm{ind}(\eta)) + \nu_p(D_K), \tag{5.1}$$

where $D(\eta)$ is the discriminant of the minimal polynomial of η and D_K is the discriminant of K. It follows by the definition (1.1) of $i(K)$ that if p divides $i(K)$, then p divides $\Delta(F)$. Recall also that

$$\Delta(F) = -b^4(7^7b^2 + 2^2 \times 5^5a^7). \tag{5.2}$$

Let us first show that $3 \nmid i(K)$. By the relation (5.1) and formula (5.2), if $3 \mid i(K)$, then

$$(a, b) \in \{(1, 0), (-1, 0), (1, 1), (1, -1), (0, 0)\} \pmod 3.$$

We distinguish several sub-cases. Table 2 gives the form of the factorization of the ideal $3A_K$ into a product of powers of distinct prime ideals of A_K in all possible cases. Note also that by (2.1), if 3 divides both a and b, then $\nu_3(a) < 2$ or $\nu_3(b) < 7$.

Case	Conditions	Factorization of $3A_K$
A1	$a \equiv 1 \pmod 3, b \equiv 0 \pmod 3$ and $5 \nmid \nu_3(b)$	$[1^5, 2]$
A2	$a \equiv 1 \pmod 3, b \equiv 0 \pmod 3$ and $5 \mid \nu_3(b)$	$[1, 2, 4]$
A3	$a \equiv -1 \pmod 3, b \equiv 0 \pmod 3$ and $5 \nmid \nu_3(b)$	$[1, 1, 1^5]$
A4	$a \equiv -1 \pmod 3, b \equiv 0 \pmod 3$ and $5 \mid \nu_3(b)$	$[1, 1, 1, 4]$
A5	$a \equiv 1 \pmod 3$ and $b \equiv \pm 1 \pmod 3$	$[1, 1, 2, 3]$, $[1^2, 2, 3]$ or $[2, 2, 3]$
A6	$7\nu_3(a) > 2\nu_3(b)$ and $\nu_3(b) \in \{1, 2, 3, 4, 5, 6\}$	$[1^7]$
A7	$\nu_3(a) = 1, \nu_3(b) \geqslant 4$ and $5 \nmid \nu_3(b) - 1$	$[1^2, 1^5]$
A8	$\nu_3(a) = 1, \nu_3(b) \geqslant 4$ and $5 \mid \nu_3(b) - 1$	$[1, 1^2, 4]$

Table 2. The factorization of $3A_K$.

We discuss each sub-case separately.

Sub-case A1: $a \equiv 1 \pmod 3$, $b \equiv 0 \pmod 3$ and $5 \nmid \nu_3(b)$. In this case, $F(x) \equiv \varphi_1(x)^5 \varphi_2(x) \pmod 3$, where $\varphi_1(x) = x$ and $\varphi_2(x) = x^2 + 1$. Since 5 does not divide $\nu_3(b)$, $N^+_{\varphi_1}(F) = S_{11}$ has a single side of degree 1 joining the points $(0, \nu_3(b))$ and $(5, 0)$ with ramification index $e_{11} = 5$. Also, we have $\nu_{\varphi_2}(\overline{F(x)}) = 1$. By Corollary 4.4, we see that $3A_K = \mathfrak{p}_{111}^5 \cdot \mathfrak{p}_{211}$, where $\mathfrak{p}_{111}$ and $\mathfrak{p}_{211}$ are two prime ideals of A_K with respective residue degrees $f(\mathfrak{p}_{111}/3) = 1$ and $f(\mathfrak{p}_{211}/3) = 2$. In view of Lemma 4.1, $3 \nmid i(K)$.

Sub-case A2: $a \equiv 1 \pmod 3, b \equiv 0 \pmod 3$ and $5 \mid \nu_3(b)$. Here, the factorization of $F(x)$ modulo 3 and the polygons $N^+_{\varphi_1}(F)$ and $N^+_{\varphi_2}(F)$ are the same as in the above case. Further, since $\nu_3(b)$ is divisible by 5, we have

$$R_{l_{11}}(F)(y) = b_3 + ay^5 = \begin{cases} (y+1)(y^4 - y^3 + y^2 - y + 1) & \text{if } b_3 \equiv 1 \pmod 3, \\ (y-1)(y^4 + y^3 + y^2 + y + 1) & \text{if } b_3 \equiv -1 \pmod 3. \end{cases}$$

Thus, $F(x)$ is 3-regular. By Theorem 4.3, $3A_K = [1, 2, 4]$. Therefore, by Lemma 4.1, $3 \nmid i(K)$.

Sub-case A3: $a \equiv -1 \pmod 3$, $b \equiv 0 \pmod 3$ and $5 \nmid \nu_3(b)$. In this case, $F(x) \equiv \varphi_1(x)^5\varphi_2(x)\varphi_3(x) \pmod 3$, where $\varphi_1(x) = x$, $\varphi_2(x) = x - 1$ and $\varphi_3(x) = x + 1$. Also, $N^+_{\varphi_1}(F) = S_{11}$ and $R_{l_{11}}(F)(y)$ are the same as in Case A1. Using Corollary 4.3, $3A_K = [1, 1, 1^5]$. Hence, by Lemma 4.1, $3 \nmid i(K)$.

Sub-case A4: $a \equiv -1 \pmod 3$, $b \equiv 0 \pmod 3$ and $5 \mid \nu_3(b)$. Here, the factorization of $F(x)$ modulo 3 is the same as in the above case. Further, $N^+_{\varphi_1}(F) = S_{11}$ and $R_{l_{11}}(F)(y)$ are the same as in Case A2. Therefore, by Corollary 4.4, $3A_K = [1, 1, 1, 4]$. Consequently, by Lemma 4.1, $3 \nmid i(K)$.

Sub-case A5: $a \equiv 1 \pmod 3$ and $b \equiv \pm 1 \pmod 3$. If $b \equiv 1 \pmod 3$, then $F(x) \equiv \varphi_1(x)^2\varphi_2(x)\varphi_3(x) \pmod 3$, where $\varphi_1(x) = x - 1$, $\varphi_2(x) = x^2 - x - 1$ and $\varphi_3(x) = x^3 - x - 1$. By Corollary 4.4 (1), the factor $\varphi_2(x)$ provides a unique prime ideal $\mathfrak{p}_{211}$ of A_K of residue degree 2 and of ramification index 1. Also, the factor $\varphi_3(x)$ provides a unique prime ideal $\mathfrak{p}_{311}$ of A_K of residue degree 3 and of ramification index 1. It follows that $3A_K = \mathfrak{p}_{211} \cdot \mathfrak{p}_{311} \cdot \mathfrak{a}$, where $\mathfrak{a}$ is a proper ideal of A_K. By Lemma 4.6, the form of the factorization of $\mathfrak{a}$ is either $[1, 1], [1^2]$ or $[2]$. Therefore, the form of the factorization of $3A_K$ is either $[1, 1, 2, 3], [1^2, 2, 3]$ or $[2, 2, 3]$. Hence, by Lemma 4.1, $3 \nmid i(K)$. If $b \equiv -1 \pmod 3$, then $F(x) \equiv (x + 1)^2(x^2 + x - 1)(x^3 - x + 1) \pmod 3$. Similarly to the case $b \equiv 1 \pmod 3$, we see that $3 \nmid i(K)$.

Note that by (2.1), if 3 divides both a and b, then $\nu_3(a) < 2$ or $\nu_3(b) < 7$. So, the conditions A6–A8 cover all possible cases when a and b are both divisible by 3. On the other hand, $F(x) \equiv \varphi_1(x)^7 \pmod 3$, where $\varphi_1(x) = x$. Thus, $N^+_{\varphi_1}(F)$ is the lower convex hull of the points $(0, \nu_3(b)), (5, \nu_3(a))$ and $(7, 0)$.

Sub-case A6: $7\nu_3(a) > 2\nu_3(b)$ and $\nu_3(b) \in \{1, 2, 3, 4, 5, 6\}$. In this case, $N^+_{\varphi_1}(F) = S_{11}$ has a single side of degree 1 and of ramification index 7. By Corollary 4.4, $3A_K = [1^7]$. By Lemma 4.1, $3 \nmid i(K)$.

Sub-case A7: $\nu_3(a) = 1$, $\nu_3(b) \geqslant 4$ and $5 \nmid \nu_3(b) - 1$. Here, $N^+_{\varphi_1}(F) = S_{11} + S_{12}$ has two distinct sides of degree 1, each joining the points $(0, \nu_3(b)), (5, 1)$ and $(7, 0)$. Their respective ramification indices are $e_{11} = 5$ and $e_{12} = 2$. Therefore, by Corollary 4.4 (2), $3A_K = [1^2, 1^5]$. Thus, $3 \nmid i(K)$.

Sub-case A8: $\nu_3(a) = 1$, $\nu_3(b) \geqslant 4$ and $5 \mid \nu_3(b) - 1$. In this case, $N^+_{\varphi_1}(F) = S_{11} + S_{12}$ has two distinct sides joining the points $(0, \nu_3(b)), (5, 1)$ and $(7, 0)$. Further, we have $d(S_{12}) = 5$, $e_{12} = 1$ and $R_{l_{11}}(F)(y)$ is the same as in Case A2. So, $F(x)$ is 3-regular. Using Theorem 4.3, we get $3A_K = [1, 1^2, 4]$. So, by Lemma 4.1, $3 \nmid i(K)$.

We conclude that in every case, 3 is not a common index divisor of K.

Now, we prove that 5 does not divide $i(K)$. By (5.1) and (5.2), if 5 divides $i(K)$, then 5 divides b. We distinguish seven cases which cover all the possibilities. Table 3 gives the form of the factorization of $5A_K$ in A_K.

Case	Conditions	Factorization of $5A_K$
B1	$7\nu_5(a) > 2\nu_5(b)$ and $\nu_5(b) \in \{1,2,3,4,5,6\}$	$[1^7]$
B2	$\nu_5(a) = 1, \nu_5(b) \geqslant 4$ and $5 \nmid \nu_5(b) - 1$	$[1^2, 1^5]$
B3	$\nu_5(a) = 1, \nu_5(b) \geqslant 4$ and $5 \mid \nu_5(b) - 1$	$[1^2, 1^5]$ or $[1, 1^4, 1^2]$
B4	$a \equiv \pm 2 \pmod 5, b \equiv 0 \pmod 5$ and $5 \nmid \nu_5(b)$	$[1^5, 2]$
B5	$a \equiv \pm 2 \pmod 5, b \equiv 0 \pmod 5$ and $5 \mid \nu_5(b)$	$[2, 1^5]$ or $[1, 1^4, 2]$
B6	$a \equiv \pm 1 \pmod 5, b \equiv 0 \pmod 5$ and $5 \nmid \nu_5(b)$	$[1, 1, 1^5]$
B7	$a \equiv \pm 1 \pmod 5, b \equiv 0 \pmod 5$ and $5 \mid \nu_5(b)$	$[1, 1, 1^5]$ or $[1, 1, 1, 1^4]$

Table 3. The factorization of $5A_K$.

Cases B1–B2: These cases are, respectively, similar to Cases A6, A7 of Table 2.

Case B3: $\nu_5(a) = 1$, $\nu_5(b) \geqslant 4$ and $5 \mid \nu_5(b) - 1$. In this case $F(x) \equiv \varphi_1(x)^7 \pmod 5$, where $\varphi_1(x) = x$. Here, $N^+_{\varphi_1}(F) = S_{11} + S_{12}$ has two distinct sides joining the points $(0, \nu_5(b)), (5, 1)$ and $(7, 0)$. Further, we have $d(S_{11}) = 5$ and $R_{l_{11}}(F)(y) = b_5 + a_5 y^5 = a_5(y + b_5/a_5)^5$ which is not separable in $\mathbb{F}_{\varphi_1}[y]$. Set $\nu_5(b) = 5k + 1$ for some positive integer k. In order to apply Ore's Theorem (Theorem 4.3), we replace the lifting $\varphi_1(x) = x$ of $\overline{\varphi_1(x)} = \overline{x} \in \mathbb{F}_5[x]$ by $\psi_1(x) = x - 5^k c$ with $c \equiv -b_5 a_5^{-1} \pmod 5$ which allows to the polynomial $F(x)$ to be ψ_1-regular. For any prime p, it is important to note that Theorem 4.3 does not depend on the monic irreducible liftings of the monic irreducible factors of $F(x)$ modulo p. The ψ_1-adic expansion of $F(x)$ is

$$\begin{aligned}(5.3)\quad F(x) = {} & 5^{7k}c^7 + 5^{5k}ac^5 + b + 5^{4k+1}c^4(7 \cdot 5^{2k-1}c^2 + a)\psi_1(x) \\ & + 5^{3k+1}c^3(21 \cdot 5^{k-1}c + 2a)\psi_1(x)^2 + 5^{2k+1}c^2(7 \cdot 5^{2k}c^2 + 2a)\psi_1(x)^3 \\ & + 5^{k+1}(7 \cdot 5^{2k} + a)\psi_1(x)^4 + (21 + 5^{5k}c^2 + a)\psi_1(x)^5 \\ & + 7 \cdot 5^k c\psi_1(x)^6 + \psi_1(x)^7.\end{aligned}$$

Let $A_0 = 5^{7k}c^7 + 5^{5k}ac^5 + b$, $A_1 = 5^{4k+1}c^4(7 \cdot 5^{2k-1}c^2 + a)$, $A_2 = 5^{3k+1}c^3 \times (21 \cdot 5^{2k-1}c + 2a)$, $A_3 = 5^{2k+1}c^2(7 \cdot 5^{2k}c^2 + 2a)$, $A_4 = 5^{k+1}c(7 \cdot 5^{2k}c^2 + a)$, $A_5 = 21 \cdot 5^{2k}c^2 + a$, $A_6 = 7 \cdot 5^k c$ and $\mu_i = \nu_5(A_i)$ for $i = 1, \ldots, 6$. Note that $\mu_5 = 1$, because $\nu_5(a) = 1$. We distinguish two cases according to $k \geqslant 2$ or $k = 1$.

Case 1: If $k \geqslant 2$, then $\mu_0 = \nu_5(5^{5k+1}(5^{2k-1}c^7 + a_5c^5 + b_5)) \geqslant 5k + 2$, $\mu_1 = 4k + 2$, $\mu_2 = 3k + 2$, $\mu_3 = 2k + 2$ and $\mu_4 = k + 2$. Then we have the following two sub-cases:

Sub-case 1.1: If $\nu_5(a_5c^5 + b_5) = 1$, then $\mu_0 = 5k + 2$. Thus, by (5.3), $N^+_{\psi_1}(F) = S_{11} + S_{12}$ has two distinct sides of degree 1, each joining the points $(0, 5k + 2), (5, 1)$ and $(7, 0)$ with $e_{11} = 5$ and $e_{12} = 2$. Therefore, by Corollary 4.4, $5A_K = [1^5, 1^2]$.

Sub-case 1.2: If $\nu_5(a_5c^5 + b_5) \geqslant 2$, then $\mu_0 \geqslant 5k + 3$. So, $N^+_{\psi_1}(F) = S_{11} + S_{12} + S_{13}$ has three distinct sides of degree 1, each joining the points $(0, \mu_0), (1, 4k + 2), (5, 1)$ and $(7, 0)$ with $e_{11} = 1, e_{12} = 4$ and $e_{13} = 2$. Consequently, $5A_K = [1, 1^4, 1^2]$.

Case 2: If $k = 1$ (that is $\nu_5(b) = 6$), then $\mu_0 = 6 + \nu_5(5c^7 + a_5c^5 + b_5) \geqslant 7$. Moreover, we have $\mu_1 = \nu_5(5^6c^4(7c^2 + a_5)) \geqslant 6$, $\mu_2 \geqslant 5$, $\mu_3 \geqslant 4$ and $\mu_4 \geqslant 3$. We proceed as in case when $k \geqslant 2$ and obtain that $5A_K = [1^2, 1^5]$ or $[1, 1^4, 1^2]$ according to $\nu_5(5c^7 + a_5c^5 + b_5) = 1$ or $\geqslant 2$.

Case B4: $a \equiv \pm 2 \pmod 5$, $b \equiv 0 \pmod 5$ and $5 \nmid \nu_5(b)$. Here, $F(x) \equiv \varphi_1(x)^5\varphi_2(x) \pmod 5$, where $\varphi_1(x) = x$ and $\varphi_2(x) = x^2 + a$. By Corollary 4.4 (1), $\varphi_2(x)$ provides that a unique prime ideal of A_K lies above 5 of residue degree 2 with the ramification index 1, say $\mathfrak{p}_{211}$. Since $5 \nmid \nu_5(b)$, $N^+_{\varphi_1}(F) = S_{11}$ has a single side of degree 1 joining the points $(0, \nu_5(b))$ and $(5, 0)$. By Corollary 4.4 (2), $\varphi_1(x)$ provides that a unique prime ideal of A_K lies above 5 of residue degree 1 with ramification index 5, say $\mathfrak{p}_{111}$. Therefore, $5A_K = [1^5, 2]$. Hence, $5 \nmid i(K)$.

Case B5: $a \equiv \pm 2 \pmod 5$, $b \equiv 0 \pmod 5$ and $5 \mid \nu_5(b)$. Set $\nu_5(b) = 5k$ for some positive integer k. Let $A_{a,b_5} \in \mathbb{Z}$ such that 5 divides $aA^5_{a,b_5} + b_5$. To treat this case, we use $\psi_1(x) = x - 5^kA_{a,b_5}$ as in Case B3. Write $A_0 = 5^{7k}A^7_{a,b_5} + 5^{5k}(aA^5_{a,b_5} + b_5)$. According to (5.3), we have $\mu_1 = 4k + 1$, $\mu_2 = 3k + 1$, $\mu_3 = 2k + 1$ and $\mu_4 = k + 1$. We distinguish two sub-cases.

Sub-case 1.1: If $\nu_5(aA^5_{a,b_5} + b_5) = 1$, then $\mu_0 = 5k + 1$. Thus, by (5.3), $N^+_{\psi_1}(F) = S_{11}$ has a single side of degree 1 joining the points $(0, 5k+1)$ and $(5, 0)$. Its ramification index equals 5. By Corollary 4.4 (2), the factor $\psi_1(x)$ (or $\varphi_1(x)$) provides that a unique prime ideal of A_K lies above 5 of residue degree 1 with the ramification index 5. Therefore, $5A_K = [2, 1^5]$. Hence, $5 \nmid i(K)$.

Sub-case 1.2: If $\nu_5(aA^5_{a,b_5} + b_5) \geqslant 2$, then $\mu_0 \geqslant 5k + 2$. Thus, by (5.3), $N^+_{\psi_1}(F) = S_{11} + S_{11}$ has two sides of degree 1, each joining the points $(0, \mu_0), (1, 4k + 1)$ and $(5, 0)$. Their respective ramification indices are $e_{11} = 1$ and $e_{12} = 4$. By Theorem 4.3, the factor $\psi_1(x)$ (or $\varphi_1(x)$) provides two distinct prime ideals of A_K lying above 5 of residue degree 1 each. Therefore, $5A_K = [1, 1^4, 2]$. So, $5 \nmid i(K)$.

Cases B6–B7: We proceed analogously as in Cases B4, B5.

Since the factorization of $5A_K$ does not satisfy the inequality $L_5(f) > N_5(f)$ for any positive integer f, we conclude by Lemma 4.1 that $5 \nmid i(K)$. This completes the proof of the theorem. □

From Theorem 2.1, no prime $p \geqslant 3$ can be a common index divisor of K. Therefore, $i(K) = 2^{\nu_2(i(K))}$. Now, let us prove Theorem 2.2. In every case, we give the form of the factorization of $2A_K$ and by using Egstrom's results (see [11]) we deduce the exact value of $i(K)$.

P r o o f of Theorem 2.2. *Case C1:* $a \equiv 1 \pmod 2$ and $b \equiv 1 \pmod 2$. In this case, $F(x) \equiv (x^2 + x + 1)(x^5 + x^4 + x^3 + x + 1) \pmod 2$. By Corollary 4.4 (1), $2A_K = [2, 5]$. In view of Lemma 4.1, $2 \nmid i(K)$. So, $i(K) = 1$.

Case C2: $a \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$. Here, $F(x) \equiv (x+1)(x^3+x+1) \times (x^3+x^2+1) \pmod 2$. By Corollary 4.4 (1), $2A_K = [1,3,3]$. Therefore, $\nu_2(i(K)) = 0$. Hence, $i(K) = 1$.

In Cases C3, C4, C5, 2 divides both a and b. These cases are similar to Cases A6, A7, A8, respectively, when we consider $p = 3$. Therefore we omit their proofs. In these cases, we have $i(K) = 1$.

From Case C6, 2 divides b, but does not divide a. It follows that $F(x) \equiv \varphi_1(x)^5\varphi_2(x)^2 \pmod 2$, where $\varphi_1(x) = x$ and $\varphi_2(x) = x - 1$. For $\varphi_1(x)$, the polynomial $F(x)$ is φ_1-regular. Moreover, by using Theorem 4.3, we have the following:

(1) If 5 does not divide $\nu_2(b)$, then $\varphi_1(x)$ provides that a unique prime ideal lies above $2A_K$ of residue degree 1 with the ramification index 5. So, $2A_K = \mathfrak{p}_{111}^5 \cdot \mathfrak{a}$, where $f(\mathfrak{p}_{111}/2) = 1$ and $\mathfrak{a}$ is a nonzero ideal of A_K.

(2) If 5 does divide $\nu_2(b)$, then $\varphi_1(x)$ provides two distinct prime ideals lying above $2A_K$ with the ramification index 1 each. One of them has a residue degree 1 and the other has a residue degree 4. Thus, $2A_K = \mathfrak{p}_{111} \cdot \mathfrak{p}_{121} \cdot \mathfrak{a}$, where $f(\mathfrak{p}_{111}/2) = 1$, $f(\mathfrak{p}_{112}/2) = 4$ and $\mathfrak{a}$ is a nonzero ideal of A_K.

Thus, the number of prime ideals of A_K that divide $2A_K$ which are provided by $\varphi_1(x)$ are determined with their residue degrees. On the other hand, the ideal $\mathfrak{a}$ is provided by the factor $\varphi_2(x)$. To factorize it, we analyze $N^+_{\varphi_2}(F)$, the φ_2-principal Newton polygon of $F(x)$. The φ_2-adic expansion of $F(x)$ is

$$F(x) = 1 + a + b + (7+5a)\varphi_2(x) + (21+10a)\varphi_2(x)^2 + \ldots + \varphi_2(x)^7. \tag{5.4}$$

Let $\nu = \nu_2(1+a+b)$ and $\mu = \nu_2(7+5a)$. It follows by (5.4) that $N^+_{\varphi_2}(F)$ is the lower convex hull of the points $(0,\nu), (1,\mu)$ and $(2,0)$. Note also that the finite residual field $\mathbb{F}_{\varphi_2}$ is isomorphic to $\mathbb{F}_2$.

Cases C6–C8: In all these cases, we have $\nu = 2$ and $\mu = 1$. Thus, $N^+_{\varphi_2}(F) = S_{11}$ has a single side of degree 2 joining the points $(0,2), (1,1)$ and $2,0$. Further, we have $e_{11} = 1$ and $R_{l_{11}}(F)(y) = 1 + y + y^2$ which is separable in $\mathbb{F}_{\varphi_2}[y]$. Therefore, by Theorem 4.3, the form of the factorization of $\mathfrak{a}$ is [2]. Thus, we conclude the form of the factorization of $2A_K$ in these cases is as given in Table 1.

Cases C9–C11: In all these cases, $\nu \geqslant 2$ and $\mu = 1$. Thus, $N^+_{\varphi_2}(F) = S_{11} + S_{12}$ has two sides of degree 1, each joining the points $(0,\nu), (1,1)$ and $(2,0)$. Their ramification indices equal 1. Their attached residual polynomial are separable as they are of degree 1. By Theorem 4.3, the form of factorization of $\mathfrak{a}$ is $[1,1]$. Therefore, we conclude the form of factorization of $2A_K$ in these cases is as given in Table 1. Since $L_2(1) = 3 > 2 = N_2(1)$, by Lemma 4.1, $2 \mid i(K)$. In Case C11, we have $2A_K = [1,1,1,4]$, then according to above mentioned Engstrom's table, we see that $\nu_2(i(K)) = 1$. On the other hand, in Cases C9 and C10, we have $2A_K = [1,1,1^5]$. In view of [11], Corollary on p. 230, $\nu_2(i(K)) = 1$. Consequently, $i(K) = 2$.

Cases C12–C14: In all these cases, $\nu = 1$. Thus, $N^+_{\varphi_2}(F) = S_{11}$ has a single side of degree 1 with the ramification index 2. By Corollary 4.4 (2), the form of the factorization of $\mathfrak{a}$ is $[1^2]$. Therefore, $2A_K = [1^2, 1^5]$ or $2A_K = [1, 1^2, 4]$. Hence, by Lemma 4.1, $2 \nmid i(K)$.

From Case C15, we have $\nu_2(1 + a) = \nu_2(b) = 1$. It follows that $\min\{\nu, \mu\} \geqslant 2$. Then we cannot control their values. To apply Ore's Theorem (Theorem 4.3), we replace the lifting $\varphi_2(x) = x - 1$ of $\overline{\varphi_2(x)}$ by $\psi_2(x) = x - s$ for an adequate odd rational integer s which allows the polynomial $F(x)$ to be ψ_2-regular. The ψ_2-adic expansion of $F(x)$ is

$$F(x) = s^7 + as^5 + b + (7s^6 + 5as^4)\psi_2(x) + (21s^5 + 10as^3)\psi_2(x)^2 + \ldots + \psi_2(x)^7. \tag{5.5}$$

Let $\omega = \nu_2(s^7 + as^5 + b)$ and $\delta = \nu_2(7s^6 + 5as^4)$. Thus, by (5.5), $N^+_{\psi_2}(F)$ is the lower convex hull of the points $(0, \omega), (1, \delta)$ and $(2, 0)$. In the next cases, we give s explicitly and the form of the factorization of $\mathfrak{a}$ in A_K. Remark in these cases that the factor $\varphi_1(x)$ provides a unique prime ideal of residue degree 1 with ramification index 5, because $\nu_2(b) = 1$.

Case C15: $(a, b) \in \{(1, 10), (9, 2), (1, 6), (9, 14)\} \pmod{16}$. When

$$(a, b) \in \{(1, 10), (9, 2)\} \pmod{16},$$

we choose any s such that $s \equiv 3, 7, 11,$ or $15 \pmod{16}$, and if

$$(a, b) \in \{(1, 6), (9, 14)\} \pmod{16},$$

consider any s satisfying $s \equiv 1, 5, 9,$ or $13 \pmod{16}$. Then, we get $\omega = 3$ and $\delta = 2$. It follows by (5.5) that $N^+_{\psi_2}(F) = S_{11}$ has a single side of degree 1 joining the points $(0, 3)$ and $(2, 0)$. Its ramification index equals 2. By Corollary 4.4 (2), the form of the factorization of $\mathfrak{a}$ is $[1^2]$. Therefore, $2A_K = [1^2, 1^5]$. So, $2 \nmid i(K)$.

Case C16: $(a, b) \in \{(1, 18), (17, 2), (1, 14), (17, 30)\} \pmod{32}$. For

$$(a, b) \in \{(1, 18), (17, 2)\} \pmod{16},$$

we choose $s \equiv 3, 7, 11, 15, 19, 23, 27, 31 \pmod{32}$, and for

$$(a, b) \in \{(1, 14), (17, 30)\} \pmod{32},$$

we choose any $s \equiv 1, 5, 9, 13, 17, 21, 25, 29 \pmod{32}$. Then, we have $\omega = 4$ and $\delta = 2$. It follows by (5.5) that $N^+_{\psi_2}(F) = S_{11}$ has a single side of degree 2 joining the points $(0, 4), (1, 2)$ and $(2, 0)$. Its attached residual polynomial is $R_{l_{11}}(F)(y) = y^2 + y + 1$ which is separable in $\mathbb{F}_{\psi_2}[y]$. So, $F(x)$ is ψ_2-regular. By Theorem 4.3, the form of the factorization of $\mathfrak{a}$ is $[2]$. Therefore, $2A_K = [2, 1^5]$. Hence, by Lemma 4.1, $2 \nmid i(K)$.

Case C17: $(a,b) \in \{(1,2),(17,18),(1,30),(17,14)\} \pmod{32}$. When

$$(a,b) \in \{(1,2),(17,18)\} \pmod{32},$$

let $s \equiv 3,7,11,15,19,23,27,31 \pmod{32}$, and for$(a,b) \in \{(1,30),(17,14)\} \pmod{32}$, let $s \equiv 1,5,9,13,17,21,25,29 \pmod{32}$. Under these considerations, we have $\omega \geqslant 5$ and $\delta = 2$. Thus, $N^+_{\psi_2}(F) = S_{11}+S_{12}$ has two sides of degree 1, each joining the points $(0,\omega),(1,2)$ and $(2,0)$. Their ramification indices equal 1. Using Theorem 4.3, the form of the factorization of $\mathfrak{a}$ is $[1,1]$. So, $2A_K = [1,1,1^5]$. Therefore, by using [11], Corollary p. 230, we have $\nu_2(i(K)) = 1$. So, $i(K) = 2$.

Case C18: $(a,b) \in \{(5,2),(5,14),(13,6),(13,10)\} \pmod{16}$. For

$$(a,b) \in \{(5,2),(13,10)\} \pmod{16},$$

we choose any $s \equiv 1,5,9,13 \pmod{16}$, and for $(a,b) \in \{(5,14),(13,6)\} \pmod{16}$, we consider any $s \equiv 3,7,11,15 \pmod{16}$. Then, we get $\omega = 3$ and $\delta \geqslant 3$. It follows that $N^+_{\psi_2}(F) = S_{11}$ has a single side of degree 1 joining the points $(0,3)$ and $(2,0)$. As in Case C15, $2A_K = [1^2,1^5]$. Consequently, $2 \nmid i(K)$, and so $i(K) = 1$. This completes the proof of the theorem. □

A c k n o w l e d g m e n t s. The author is deeply grateful to Editor Clemens Fuchs for his professionalism during the review process of this manuscript. He also expresses deep gratitude to the referee whose invaluable comments and suggestions significantly enhanced the quality of this paper.

References

[1] *S. Ahmad, T. Nakahara, A. Hameed*: On certain pure sextic fields related to a problem of Hasse. Int. J. Algebra Comput. *26* (2016), 577–583. zbl MR doi
[2] *S. Ahmad, T. Nakahara, S. M. Husnine*: Power integral bases for certain pure sextic fields. Int. J. Number Theory *10* (2014), 2257–2265. zbl MR doi
[3] *H. Ben Yakkou*: On nonmonogenic number fields defined by trinomials of type $x^n + ax^m + b$. Rocky Mt. J. Math. *53* (2023), 685–699. zbl MR doi
[4] *H. Ben Yakkou, B. Boudine*: On the index of the octic number field defined by x^8+ax+b. Acta Math. Hung. *170* (2023), 585–607. zbl MR doi
[5] *H. Ben Yakkou, J. Didi*: On monogenity of certain pure number fields of degrees $2^r \cdot 3^k \cdot 7^s$. Math. Bohem. *149* (2024), 167–183. zbl MR doi
[6] *H. Ben Yakkou, L. El Fadil*: On monogenity of certain pure number fields defined by $x^{p^r} - m$. Int. J. Number Theory *17* (2021), 2235–2242. zbl MR doi
[7] *Y. Bilu, I. Gaál, K. Győry*: Index form equations in sextic fields: A hard computation. Acta Arith. *115* (2004), 85–96. zbl MR doi
[8] *H. Cohen*: A Course in Computational Algebraic Number Theory. Graduate Texts in Mathematics 138. Springer, Berlin, 1993. zbl MR doi

[9] *C. T. Davis, B. K. Spearman*: The index of quartic field defined by a trinomial $X^4 + aX + b$. J. Algebra Appl. *17* (2018), Article ID 1850197, 18 pages. zbl MR doi
[10] *R. Dedekind*: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. Abh. König. Gesell. Wiss. Gött. *23* (1878), 202–232. (In German.)
[11] *H. T. Engstrom*: On the common index divisors of an algebraic field. Trans. Am. Math. Soc. *32* (1930), 223–237. zbl MR doi
[12] *J.-H. Evertse, K. Győry*: Unit Equations in Diophantine Number Theory. Cambridge Studies in Advanced Mathematics 146. Cambridge University Press, Cambridge, 2015. zbl MR doi
[13] *J.-H. Evertse, K. Győry*: Discriminant Equations in Diophantine Number Theory. New Mathematical Monographs 32. Cambridge University Press, Cambridge, 2017. zbl MR doi
[14] *I. Gaál*: Diophantine Equations and Power Integral Bases: Theory and Algorithms. Birkhäuser, Cham, 2019. zbl MR doi
[15] *I. Gaál, K. Győry*: Index form equations in quintic fields. Acta Arith. *89* (1999), 379–396. zbl MR doi
[16] *I. Gaál, A. Pethő, M. Pohst*: On the resolution of index form equations in quartic number fields. J. Symb. Comput. *16* (1993), 563–584. zbl MR doi
[17] *I. Gaál, N. Schulte*: Computing all power integral bases of cubic fields. Math. Comput. *53* (1989), 689–696. zbl MR doi
[18] *J. Guàrdia, J. Montes, E. Nart*: Newton polygons of higher order in algebraic number theory. Trans. Am. Math. Soc. *364* (2012), 361–416. zbl MR doi
[19] *J. Guàrdia, J. Montes, E. Nart*: Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields. J. Théor. Nombres Bordx. *23* (2021), 667–669. zbl MR doi
[20] *K. Győry*: Sur les polynômes á coefficients entiers et de discriminant donné. Acta Arith. *23* (1973), 419–426. (In French.) zbl MR doi
[21] *K. Győry*: Sur les polynômes á coefficients entiers et de discriminant donné. III. Publ. Math. Debr. *23* (1976), 141–165. (In French.) zbl MR doi
[22] *K. Győry*: On polynomials with integer coefficients and given discriminant. IV. Publ. Math. Debr. *25* (1978), 155–167. zbl MR doi
[23] *K. Győry*: Corps de nombres algébriques d'anneau d'entiers monogéne. Séminaire Delange-Pisot-Poitou, 20e année: 1978/1979. Théorie des nombres. Fascicule 2: Exposés 22 à 33, Index cumulatif 1re à 20e années, 1959/1960 à 1978/1979. Secrétariat Mathématique, Paris, 1980, pp. Article ID 26, 7 pages. (In French.) zbl MR
[24] *K. Győry*: On discriminants and indices of integers of an algebraic number field. J. Reine Angew. Math. *324* (1981), 114–126. zbl MR doi
[25] *K. Győry*: Bounds for the solutions of decomposable form equations. Publ. Math. Debr. *52* (1998), 1–31. zbl MR doi
[26] *A. Jakhar, S. K. Khanduja, N. Sangwan*: Characterization of primes dividing the index of a trinomial. Int. J. Number Theory *13* (2017), 2505–2514. zbl MR doi
[27] *L. Jones, D. White*: Monogenic trinomials with non-squarefree discriminant. Int. J. Math. *32* (2021), Article ID 2150089, 21 pages. zbl MR doi
[28] *P. Llorente, E. Nart*: Effective determination of the decomposition of the rational primes in a cubic field. Proc. Am. Math. Soc. *87* (1983), 579–585. zbl MR doi
[29] *J. Montes, E. Nart*: On a theorem of Ore. J. Algebra *146* (1992), 318–334. zbl MR doi
[30] *W. Narkiewicz*: Elementary and Analytic Theory of Algebraic Numbers. Springer Monographs in Mathematics. Springer, Berlin, 2004. zbl MR doi
[31] *E. Nart*: On the index of a number field. Trans. Am. Math. Soc. *289* (1985), 171–183. zbl MR doi
[32] *Ö. Ore*: Newtonsche Polygone in der Theorie der algebraischen Körper. Math. Ann. *99* (1928), 84–117. (In German.) zbl MR doi

[33] *A. Pethő, M. E. Pohst*: On the indices of multiquadratic number fields. Acta Arith. *153* (2012), 393–414. zbl MR doi
[34] *A. Pethő, V. Ziegler*: On biquadratic fields that admit unit power integral basis. Acta Math. Hung. *133* (2011), 221–241. zbl MR doi
[35] *E. von Żyliński*: Zur Theorie der außerwesentlichen Diskriminantenteiler algebraischer Körper. Math. Ann. *73* (1913), 273–274. (In German.) zbl MR doi

Author's address: *Hamid Ben Yakkou*, Sidi Mohamed Ben Abdellah University, Faculty of Sciences Dhar El Mahraz, P. O. Box 1874, 30050 Fez, Morocco, e-mail: `beyakouhamid@gmail.com`.