Article

Not peer-reviewed version

On Index Divisors and Monogenity of Certain Number Fields Defined by Trinomials x^7+ax+b

Lhoussain El Fadil [*]

Posted Date: 7 September 2023

doi: 10.20944/preprints202309.0481.v1

Keywords: Power integral bases; theorem of Ore; prime ideal factorization; common index divisor

Article

On Index Divisors and Monogenity of Certain Number Fields Defined by Trinomials $x^7 + ax + b$

Lhoussain El Fadil

Department of Mathematics, Faculty of Sciences Dhar El Mahraz-Fes, Sidi Mohamed Ben Abdellah University, Fez-Morocco; lhoussain.elfadil@usmba.ac.ma

Abstract: In this paper for every number field K generated by a root α of a trinomial $x^7 + ax + b \in \mathbb{Z}[x]$ and for every prime integer p, we calculate $\nu_p(i(K))$, the highest power of p dividing the index $i(K)$ of the field K. In particular, we calculate the index $i(K)$. As application, when the index of K is not trivial, then K is not monogenic.

Key words and phrases: power integral bases; theorem of Ore; prime ideal factorization; common index divisor

2010 Mathematics Subject Classification: 11R04; 11Y40; 11R21

1. Introduction

Let K be a number field of degree n, $\mathbb{Z}_K$ its ring of integers, and d_K its absolute discriminant. It is well known that $\mathbb{Z}_K$ is a free abelian group of rank n and by the fundamental theorem of finite abelian groups, $(\mathbb{Z}_K : \mathbb{Z}[\theta])$ is a finite group for every primitive element $\theta \in \mathbb{Z}_K$ of K. Let $ind(\theta) = (\mathbb{Z}_K : \mathbb{Z}[\theta])$. $ind(\theta)$ is called the index of θ. The index of the number field K is defined by $i(K) = GCD((\mathbb{Z}_K : \mathbb{Z}[\theta]) \mid K = \mathbb{Q}(\theta) \text{ and } \theta \in \mathbb{Z}_K)$. A rational prime integer p dividing $i(K)$ is called a prime common index divisor of K. The number field K is called monogenic if it admits a $\mathbb{Z}$ basis of type $(1, \theta, \dots, \theta^{n-1})$ for some $\theta \in \mathbb{Z}_K$. Remark that if $\mathbb{Z}_K$ has a power integral basis, then $i(K) = 1$. Therefore a field having a prime common index divisor is not monogenic. Monogenity of number fields is a classical problem of algebraic number theory, going back to Dedekind, Hasse and Hensel, see for instance [19,25,26] for the present state of this area. It is called a problem of Hasse to give an arithmetic characterization of those number fields which are monogenic [23,25,26]. For any primitive element $\theta \in \mathbb{Z}_K$ of K, it is well-known that

$$|\triangle(\theta)| = ind(\theta)^2 \cdot |d_K|$$

where $\triangle(\theta)$ is the discriminant of the minimal polynomial of θ over $\mathbb{Q}$ [19].

Clearly, $ind(\theta) = 1$ for some primitive element $\theta \in \mathbb{Z}_K$ of K if and only if $(1, \theta, \dots, \theta^{n-1})$ is a power integral basis of $\mathbb{Z}_K$.

The problem of testing the monogenity of number fields and constructing power integral bases have been intensively studied during the last four decades mainly by Gaál, Győry, Nakahara, Pohst and their collaborators (see for instance [1,16,32]). In 1871, Dedekind was the firstone who gave an example of a number field with non trivial index, he considered the cubic field K generated by a root of $x^3 - x^2 - 2x - 8$ and showed that the rational prime 2 splits completely in K ([5, § 5, page 30]). According to a well known theorem of Dedekind ([24, Chapter I, Proposition 8.3]), if we suppose that K is monogenic, then we would be able to find a cubic polynomial defining K, that splits completely into distinct polynomials of degree 1 in $\mathbb{F}_2[x]$. Since there is only two distinct polynomials of degree 1 in $\mathbb{F}_2[x]$, this is impossible. In 1930, Engstrom was the first one who related the prime ideal factorization and the index of a number field of degree less than 8 [13]. For any number field K of degree $n \le 7$, he showed that $\nu_p(i(K))$ is explicitly determined by the factorization of $p\mathbb{Z}_K$ into powers of prime ideals of K for every positive rational prime integer $p \le n$. This motivated Narkiewicz to ask a very important question, stated as problem 22 in Narkiewicz's book ([31, Problem 22]), which asks for an explicit formula of the highest power $\nu_p(i(K))$ for a given rational prime p dividing $i(K)$. In [30], Nakahara studied the index of non-cyclic but abelian biquadratic number fields. He showed that the field index of such fields is in the set $\{1,2,3,4,6,12\}$. In [17] Gaál et al. characterized the field indices of biquadratic number fields having Galois group V_4 and they proved that $i(K) \in \{1,2,3,4,6,12\}$. Recently, many authors are interested on monogenity of number fields defined by trinomials. Davis and Spearman [6] studied the index of quartic number fields K generated by a root of such a quartic trinomial $F(x) = x^4 + ax + b \in \mathbb{Z}[x]$. They gave necessary and sufficient conditions on a and b so that a prime p is a common index divisor of K for $p = 2,3$. Their method is based on the calculation of the p-index form of K, using p-integral bases of K. El Fadil and Gaál [11] studied the index of quartic number fields K generated by a root of a quadratic trinomial of the form $F(x) = x^4 + ax^2 + b \in \mathbb{Z}[x]$. They gave necessary and sufficient conditions on a and b so that a prime p is a common index divisor of K for every prime integer p. In [15], for a sextic number field K defined by a trinomial $F(x) = x^6 + ax^3 + b \in \mathbb{Z}[x]$, Gaál studied the multi-monegenity of K; he calculated all possible power integral bases of K. In [9], we extended Gaál's studies by providing some cases where K is not monogenic. Also in [10], for every prime integer p, we gave necessary and sufficient conditions on a and b so that p is a common index divisor of K, where K is a number field defined by an irreducible trinomial $F(x) = x^5 + ax^2 + b \in \mathbb{Z}[x]$. In [8], we provided some sufficient conditions which guarantee that $i(K)$ is not trivial, and so K is not mongenic. In this paper, for a septic number field generated by a root of a trinomial $F(x) = x^7 + ax + b \in \mathbb{Z}[x]$ and for every prime integer p, we calculate $\nu_p(i(K))$, the highest power of p dividing the index $i(K)$ of the field K. Our method is based on Newton's polygon techniques applied in prime ideal factorization, which is performed in [21,22] and in Montes' thesis defended in 1999. The author is very thankful to Professor Enric Nart who provided him a copy of Montes' thesis.

2. Main Results

Throughout this section K is a number field generated by a root α of an irreducible trinomial $F(x) = x^7 + ax + b \in \mathbb{Z}[x]$ and we assume that for every rational prime integer p, $\nu_p(a) \le 5$ or $\nu_p(b) \le 6$. Along this paper, for every integer $a \in \mathbb{Z}$ and a prime integer p, let $a_p = \dfrac{a}{p^{\nu_p(a)}}$.

We start with the following theorem, which characterizes when is $\mathbb{Z}[\alpha]$ integrally closed?

Theorem 2.1. *The ring $\mathbb{Z}[\alpha]$ is integrally closed if and only if every prime integer p satisfies one of these conditions:*

1. *If $p|a$ and $p|b$, then $\nu_p(b) = 1$.*
2. *If $p = 2$, p divides b and does not a, then $(a,b) \in \{(1,0),(3,2)\} \pmod 4$.*
3. *If $p = 3$, p divides b and $a \equiv -1 \pmod 3$, then $(a,b) \in \{(2,0),(8,3),(8,6)\} \pmod 9$.*
4. *If $p = 3$, p divides b and $a \equiv 1 \pmod 3$, then $(a,b) \not\equiv (1,0) \pmod 9$.*
5. *If $p = 7$, p divides a and does not divide b, then $\nu_7(1 - a - b^6) = 1$.*
6. *If $p \notin \{2,3,7\}$, p does not divide both a and b, then $\nu_p(7^7b^6 + 6^6a^7) \le 1$.*

The following example gives an infinite family of monogenic septic number fields defined by non monogenic trinomials.

Proposition 2.2. *Let K be the number field generated by a root α of $F(x) = x^7 + 2^u ax + 2^v b \in \mathbb{Z}[x]$, with $u \ge v - 1$, $2 \le v \le 6$, $GCD(6,b) = 1$, 7 does not divide a, and for every odd prime integer p, if p does not divide b, then p^2 does not divide $7^7b^6 + 6^6a^7$. Then $F(x)$ is a non monogenic polynomial and K is a monogenic number field.*

In the remainder of this section, for every prime integer p and for every values of a and b, we calculate $\nu_p(i(K))$. For every integers a and b, let $\triangle = -(6^6a^7 + 7^7b^6)$ be the discriminant of $F(x)$ and for every prime integer p, let $\triangle_p = \dfrac{\triangle}{p^{\nu_p(\triangle)}}$.

Theorem 2.3. *The following table provides the value of* $\nu_2(i(K))$.

conditions	$\nu_2(i(K))$
$a \equiv 28 \pmod{32}$ *and* $b \equiv 0 \pmod{32}$	1
$a \equiv 112 \pmod{128}$ *and* $b \equiv 0 \pmod{128}$	1
$a \equiv 1 \pmod 8$ *and* $b \equiv 2 \pmod 4$ $\nu_2(\triangle)$ *even and* $\triangle_2 \equiv 3 \pmod 4$	1
$a \equiv 3 \pmod 8$ *and* $b \equiv 4 \pmod 8$	1
$a \equiv 3 \pmod 4$ *and* $b \equiv 0 \pmod 8$	3
$(a,b) \in \{(5,2),(5,6),(13,2),(13,14)\} \pmod{16}$	1
Otherwise	0

Theorem 2.4. *The following table provides the value of* $\nu_3(i(K))$.

conditions	$\nu_3(i(K))$
$a \equiv 5 \pmod 9$ *and* $b \in \{3,6\} \pmod 9$	1
$a \equiv 8 \pmod 9$ *and* $b \equiv 0 \pmod 9$	2
$a \equiv 2 \pmod 9$ *and* $b \in \{3,6\} \pmod 9$ $\nu_3(\triangle) = 2k$ *and* $k \geq 5$	1
$a \equiv 2 \pmod 9$ *and* $b \in \{3,6\} \pmod 9$ $\nu_3(\triangle) = 2k+1$, $k \geq 5$ *and* $\triangle_3 \equiv 1 \pmod 3$	2
Otherwise	0

Theorem 2.5. *For every prime integer $p \geq 5$ and for every integers a and b such that $F(x) = x^7 + ax + b$ is irreducible over $\mathbb{Q}$, p does not divide $i(K)$, where K is the number field defined by $F(x)$.*

Corollary 2.6. *For every integers a and b such that $F(x) = x^7 + ax + b$ is irreducible over $\mathbb{Q}$, $i(K) \in \{1,2,3,6,8,9,18,24,72\}$.*

Remark 1.
1. *The field K can be non monogenic even if the index $i(K) = 1$.*
2. *The unique method which allows to test whether K is monogenic is to calculate the solutions of the index form equation of the field K (see for instance [18,19]).*

3. A short introduction to prime ideal factorization based on Newton polygons

In 1894, Hensel developed a powerful approach by showing that for every prime integer p, the prime ideals of $\mathbb{Z}_K$ lying above p are in one–one correspondence with monic irreducible factors of $F(x)$ in $\mathbb{Q}_p[x]$. For every prime ideal corresponding to any irreducible factor in $\mathbb{Q}_p[x]$, the ramification index and the residue degree together are the same as those of the local field defined by the associated irreducible factor [28]. Since then, to factorize $p\mathbb{Z}_K$, we need to factorize $F(x)$ in $\mathbb{Q}_p[x]$. Newton's polygon techniques can be used to refine the factorization. This is a standard method which is rather technical but very efficient to apply. We have introduced the corresponding concepts in several former papers. Here we only give a brief introduction which makes our proofs understandable. For a detailed description, we refer to Ore's Paper [34] and Guardia, Montes and Nart's paper [20]. For every prime integer p, let ν_p be the p-adic valuation of $\mathbb{Q}_p$ and $\mathbb{Z}_p$ the ring of p-adic integers. Let $F(x) \in \mathbb{Z}_p[x]$ be a monic polynomial and $\phi \in \mathbb{Z}_p[x]$ a monic lift of an irreducible factor of $\overline{F(x)}$ modulo p. Let $F(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_n(x)\phi(x)^l$ be the ϕ-expansion of $F(x)$, $N_\phi(F)$ the ϕ-Newton polygon of $F(x)$ and $N_{\phi}^{+}(F)$ its principal part. Let $\mathbb{F}_{\phi}$ be the field $\mathbb{F}_p[x]/(\overline{\phi})$. For every side S of $N_{\phi}^{+}(F)$ with length l and initial point (s, u_s), for every $i = 0, \ldots, l$, let $c_i \in \mathbb{F}_{\phi}$ be the residue coefficient, defined as follows:

$$c_i = \begin{cases} 0, & \text{if } (s+i, u_{s+i}) \text{ lies strictly above } S, \\ \left(\dfrac{a_{s+i}(x)}{p^{u_{s+i}}}\right) \mod (p, \phi(x)), & \text{if } (s+i, u_{s+i}) \text{ lies on } S. \end{cases}$$

Let $-\lambda = -h/e$ be the slope of S, where h and e are two positive coprime integers. Then $d = l/e$ is the degree of S. Let $R_1(F)(y) = t_d y^d + t_{d-1} y^{d-1} + \cdots + t_1 y + t_0 \in \mathbb{F}_{\phi}[y]$, called the residual polynomial of $F(x)$ associated to the side S, where for every $i = 0, \ldots, d$, $t_i = c_{ie}$. If $R_1(F)(y)$ is square free for each side of the polygon $N_{\phi}^{+}(F)$, then we say that $F(x)$ is ϕ-regular.

Let $\overline{F(x)} = \prod_{i=1}^{r} \overline{\phi_i}^{l_i}$ be the factorization of $F(x)$ into powers of monic irreducible coprime polynomials over $\mathbb{F}_p$, we say that the polynomial $F(x)$ is p-regular if $F(x)$ is a ϕ_i-regular polynomial with respect to p for every $i = 1, \ldots, r$. Let $N_{\phi_i}^{+}(F) = S_{i1} + \cdots + S_{ir_i}$ be the ϕ_i-principal Newton polygon of $F(x)$ with respect to p. For every $j = 1, \ldots, r_i$, let $R_{1_{ij}}(F)(y) = \prod_{s=1}^{s_{ij}} \psi_{ijs}^{a_{ijs}}(y)$ be the factorization of $R_{1_{ij}}(F)(y)$ in $\mathbb{F}_{\phi_i}[y]$, where $R_{1_{ij}}(F)(y)$ is the residual polynomial of $F(x)$ attached to the side S_{ij}. Then we have the following theorem of index of Ore:

Theorem 3.1. *([12, Theorems 1.7 and 1.9])*
Under the above hypothesis, we have the following:

1. $$\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) \geq \sum_{i=1}^{r} ind_{\phi_i}(F).$$
   The equality holds if $F(x)$ is p-regular.
2. *If $F(x)$ is p-regular, then*
   $$p\mathbb{Z}_K = \prod_{i=1}^{r} \prod_{j=1}^{t_i} \prod_{s=1}^{s_{ij}} \mathfrak{p}_{ijs}^{e_{ij}}$$
   is the factorization of $p\mathbb{Z}_K$ into powers of prime ideals of $\mathbb{Z}_K$, where e_{ij} is the smallest positive integer satisfying $e_{ij}\lambda_{ij} \in \mathbb{Z}$ and the residue degree of $\mathfrak{p}_{ijs}$ over p is given by $f_{ijs} = \deg(\phi_i) \times \deg(\psi_{ijs})$ for every (i, j, s).

The Dedekind criterion can be reformulated as follows:

Theorem 3.2. *([7, Theorem 1.1])*
Under the above hypothesis, let $R_i(x)$ be the remainder of the Euclidean division of $F(x)$ by $\phi_i(x)$. Then $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$ if and only if $l_i = 1$ or $\nu_p(R_i(x)) = 1$ for every $i = 1, \ldots, r$.

When the theorem of Ore fails, that is $F(x)$ is not p-regular, then in order to complete the factorization of $F(x)$, Guardia, Montes, and Nart introduced the notion of *high order Newton polygon*. By analogous to the first order, for each order r, the authors of [20] introduced the valuation ω_2 of order r, the key polynomial $\phi_2(x)$ of such a valuation, $N_r(F)$ the Newton polygon of any polynomial $F(x)$ with respect to ω_2 and $\phi_2(x)$, and for every side of $N_r(F)$ the residual polynomial $R_r(F)$, and the index of $F(x)$ in order r. For more details, we refer to [20].

doi:10.20944/preprints202309.0481.v1

4. Proofs of our main results

Proof of Theorem 2.1.

1. If p divides a and b, then by Theorem 3.2, p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_p(b) = 1$.
2. For $p = 2$, 2 divides b and does not a, we have $\overline{F(x)} = x(x-1)^2(x^2+x+1)^2$. Let $\phi_1 = x-1$ and $\phi_2 = x^2+x+1$. Since $F(x) = \cdots - (4x-2)\phi_2 + (a+1)x + b$ and $F(x) = \cdots + (a+7)\phi_1 + (a+1+b)$, by Theorem 3.2, 2 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_2(b+a+1) = 1$ and $\nu_2((a+1)x+b) = 1$, which means $b \equiv 1-a \pmod 4$ and $a \equiv 1 \pmod 4$ or $b \equiv 2 \pmod 4$. That is $(a,b) \in \{(1,0),(3,2)\} \pmod 4$.
3. For $p = 3$, 3 divides b and $a \equiv 1 \pmod 3$, we have $\overline{F(x)} = x(x^2+1)^3$. Let $\phi = x^2+1$. Since $F(x) = x\phi^3 - 3x\phi^2 + 3x\phi + (a-1)x + b$, by Theorem 3.2, 3 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_3((a-1)x+b) = 1$, which means that $a \not\equiv 1 \pmod 9$ or $b \not\equiv 0 \pmod 9$. That is $(a,b) \not\equiv (1,0) \pmod 9$.
4. For $p = 3$, 3 divides b and $a \equiv -1 \pmod 3$, we have $\overline{F(x)} = x(x-1)^3(x+1)^2$. Let $\phi_1 = x-1$ and $\phi_2 = x+1$. Since $F(x) = \phi_1^7 + 7\phi_1^6 + 21\phi_1^5 + 35\phi_1^4 + 35\phi_1^3 + 21\phi_1^2 + (a+7)\phi_1 + (a+1+b)$ and $F(x) = \phi_1^7 - 7\phi_2^6 + 21\phi_2^5 - 35\phi_2^4 + 35\phi_2^3 - 21\phi_2^2 + (a+7)\phi_2 + (b-a-1)$, by Theorem 3.2, 3 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_2(a+1+b) = 1$ and $\nu_3(b-a-1) = 1$. That is $(a,b) \in \{(2,0),(8,3),(8,6)\} \pmod 9$.
5. For $p = 7$, if 7 divides a and 7 does not divide b, then $\overline{F(x)} = (x+b)^7$. Let $\phi = x+b$. Then $F(x) = \phi^7 - 7b\phi^6 + 21b^2\phi^5 - 35b^3\phi^4 + 35b^4\phi^3 - 21b^5\phi^2 + (a+7b^6)\phi + (b-ab-b^7)$, by Theorem 3.2, 7 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_7(1-a-b^6) = 1$.
6. For $p \notin \{2,3,7\}$ such that p does not divide both a and b, if p^2 does not divide $6^6a^7 + 7^7b^6$, then by the formula $\triangle = (\mathbb{Z}_K : \mathbb{Z}[\alpha])^2 d_K$, p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. If p^2 divides $6^6a^7 + 7^7b^6$, then let t be an integer such that $6at \equiv -7b \pmod{p^2}$. Then $(6a)^6F'(t) = 7(-7b)^6 + 6^6a^7 \equiv 0 \pmod{p^2}$ and $(6a)^7F(t) \equiv 0 \pmod{p^2}$. Thus $(x-t)^2$ divides $\overline{F(x)}$ in $\mathbb{F}_p[x]$. As $F(t)$ is the remainder of the Euclidean division of $F(x)$ by $x-t$, by Theorem 3.2, p divides the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$.

For the proofs of Theorems 2.3 and 2.4, we need the following lemma, which characterizes the prime common index divisors of K.

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

Proof of Theorem 2.3.
By virtue of Engstrom's results [14], the proof is done if we provide the factorization of $2\mathbb{Z}_K$ into powers of prime ideals of $\mathbb{Z}_K$. Based on Theorem 2.1, we deal with the cases: $2|a$ and $4|b$ or $(a,b) \in \{(1,2),(3,0)\} \pmod 4$.

1. If 2 divides a and 4 divides b, then for $\phi = x$, we have $\overline{F(x)} = \phi^7$ in $\mathbb{F}_2[x]$.
   (a) If $N_\phi(F) = S$ has a single side, that is $\nu_2(a) \geq \nu_2(b)$, then the side S is of degree 1. Thus there is a unique prime ideal of $\mathbb{Z}_K$ lying above 2.
   (b) If $N_\phi(F) = S_1 + S_2$ has two sides joining $(0,\nu_2(b))$, $(1,\nu_2(a))$, and $(7,0)$, that is $\nu_2(a) + 1 \leq \nu_2(b)$, then S_1 is of degree 1, and so it provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1. Let d be the degree of S_2.
      i. If $\nu_2(a) \notin \{2,3,4\}$, then S_2 is of degree 1, and so there are exactly two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each.
      ii. If $\nu_2(a) = 2$, then the slope of S_2 is $\frac{-1}{3}$ and $R_1(F)(y) = (y+1)^2$ is the residual polynomial of $F(x)$ attached to S_2. Thus we have to use second order Newton polygon

techniques. Let ω_2 be the valuation of second order Newton polygon; defined by $\omega_2(P(x)) = \min\{3\nu_2(p_i) + ih, ß = 0, \dots, n\}$ for every non-zero polynomial $P = \sum_{i=0}^{n} p_i x^i$. Let ϕ_2 be the key polynomial of ω_2 and let $N_2(F)$ the ϕ_2-Newton polygon of $F(x)$ with respect to the valuation ω_2. It follows that:
If $\nu_2(b) = 3$, then for $\phi_2 = x^3 + 2x + 2$, we have $F(x) = x\phi_2^2 + (4 - 4x - 4x^2)\phi_2 + 8x^2 + (a-4)x + b - 8$. It follows that if $\nu_2(a-4) = 3$, then $N_2(F) = T$ has a single side joining $(0, 10)$ and $(2, 7)$. Thus T is of degree 1, and so S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2. If $\nu_2(a-4) \geq 4$ and $\nu_2(b-8) \geq 4$, then $N_2(F) = T$ has a single side joining $(0, 11)$, $(1, 9)$ and $(2, 7)$, with $R_2(F)(y) = y^2 + y + 1$, which is irreducible over $\mathbb{F}_2 = \mathbb{F}_0$. Thus S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2. Hence 2 is not a common index divisor of K.
If $\nu_2(b) \geq 4$ and $\nu_2(a+4) = 3$, then for $\phi_2 = x^3 + 2$, we have $F(x) = x\phi_2^2 - 4x\phi_2 + (a+4)x + b$ is the ϕ_2-expansion of $F(x)$, and so $N_2(F) = T$ has a single side joining $(0, 10)$ and $(2, 7)$. In this case the side T is of degree 1 and S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2. If $\nu_2(b) = 4$ and $\nu_2(a+4) \geq 4$, then for $\phi_2 = x^3 + 2$, $N_2(F) = T$ has a single side joining $(0, 12)$ and $(2, 7)$. Thus T is of degree 1, and so S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2.
If $\nu_2(b) \geq 5$ and $\nu_2(a+4) = 4$, then for $\phi_2 = x^3 + 2$, we have $F(x) = x\phi_2^2 - 4x\phi_2 + (a+4)x + b$ is the ϕ_2-expansion of $F(x)$ and $N_2(F) = T$ has a single side joining $(0, 13)$, $(1, 10)$ and $(2, 7)$. So T is of degree 2 with attached residual polynomial $R_2(F) = y^2 + y + 1$ irreducible over $\mathbb{F}_2 = \mathbb{F}_0$. Thus S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2.
If $\nu_2(b) \geq 5$ and $\nu_2(a+4) \geq 5$, then for $\phi_2 = x^3 + 2$, $N_2(F) = T_1 + T_2$ has two sides joining $(0, v)$, $(1, 10)$ and $(2, 7)$ with $v \geq 15$. So each T_i has degree 1, and so S_2 provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each. As S_1 provides a prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1, we conclude that there are three prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each, and so 2 is a common index divisor of K. In this last case, $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}^3\mathfrak{p}_{131}^3$ with residue degree 1 each prime ideal factor. Based on Engstrom's result, we conclude that $\nu_2(i(K)) = 1$.

iii. For $\nu_2(a) = 3$, we have $R_1(F)(y) = y^3 + 1 = (y^2 + y + 1)(y + 1)$ is the residual polynomial of $F(x)$ attached to T_1. Thus T_1 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2, with residue degree 1 and a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2. Thus $\nu_2(i(K)) = 0$.

iv. The case $\nu_2(a) = 4$ is similar to the case $\nu_2(a) = 2$. In this case $\nu_2(i(K)) \geq 1$ if and only if $\nu_2(b) \geq 7$ and $\nu_2(a+16) \geq 7$. In this case, $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}^3\mathfrak{p}_{131}^3$ with residue degree 1 each factor. Based on Engstrom's result, we conclude that $\nu_2(i(K)) = 1$.

2. $(a, b) \in \{(1, 2), (3, 0)\} \pmod 4$. In this case $\overline{F(x)} = x(x-1)^2(x^2 + x + 1)^2$ modulo 2. Let $\phi = x - 1$, $g(x) = x^2 + x + 1$, $F(x) = \cdots - 21\phi^2 + (7 + a)\phi + (b + a + 1)$, and $F(x) = (x-3)g^3 + (5 + 3x)g^2 - (4x + 2)g + (a + 1)x + b$. Since x provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2, we conclude that 2 is a common index divisor of K if and only if ϕ provides two prime ideals of $\mathbb{Z}_K$ lying above 2 of degree 1 each or ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 of degree 2 and g provides at least one prime ideal of $\mathbb{Z}_K$ lying above 2 of degree 2 or also g provides two prime ideals of $\mathbb{Z}_K$ lying above 2 of degree 2 each. That is if and only if one of the following conditions holds:

   (a) If $a \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$, then $\nu_2(\triangle) \geq 7$ and $N_g^+(F)$ has a single side of height 1, and so g provides a unique prime ideal $\mathfrak{p}_{311}$ of $\mathbb{Z}_K$ lying above 2 with residue degree 2. For $N_\phi^+(F)$, let $u = \dfrac{-7b_2}{3a}$. Then $u \in \mathbb{Z}_2$. Let $F(x + u) = x^7 + \cdots + 21u^5x^2 + Ax + B$, where $A = 7u^6 + a = \dfrac{-\triangle}{6^6a^6}$ and $B = u^7 + au + b = \dfrac{b\triangle}{6^7a^7}$. It follows that $\nu_2(A) = \nu_2(B) = \nu_2(\triangle) - 6$,

doi:10.20944/preprints202309.0481.v1

and so $N_{\phi}^{+}(F) = S_1$ has a single side joining $(0, \nu_2(\triangle) - 6)$ and $(2, 0)$. Thus, if $\nu_2(\triangle)$ is odd, then ϕ provides a unique prime ideal $\mathfrak{p}_{211}$ of $\mathbb{Z}_K$ lying above 2 with residue degree 1. If $\nu_2(\triangle) = 2(k+3)$ for some positive integer k, then let $F(x + u + 2^k) = x^7 + \cdots + 21(u + 2^k)^5 x^2 + A_1 x + B_1$, where $A_1 = 7u^6 + a + 3 \cdot 2^{k+1} u^5 + 2^{2k} D = A + 3 \cdot 2^{k+1} u^5 + 2^{2k} D$ and $B_1 = B + A \cdot 2^k + 2^{2k} \cdot 21 u^5 + 2^{3k} H = 2^{2k}(\frac{b_2 \triangle_2}{3^7 a^7} + 21 u^5) + 2^{3k} H$ for some $D \in \mathbb{Z}_2$ and $H \in \mathbb{Z}_2$. Thus, $B_1 = 2^{2k}(3 \cdot a \cdot b_2 \triangle_2 + 3 \cdot a \cdot b_2) + 2^{2k+3} L$ for some $L \in \mathbb{Z}_2$. Hence if $k \geq 2$, then $\nu_2(A_1) = k + 1$ and $\nu_2(B_1) \geq 2k + 1$. More precisely, if $\triangle_2 \equiv 1 \pmod 4$, then $\nu_2(B_1) = 2k + 1$, and so ϕ provides a unique prime ideal $\mathfrak{p}_{211}$ of $\mathbb{Z}_K$ lying above 2 with residue degree 1. If $\triangle_2 \equiv 3 \pmod 4$, then $\nu_2(B_1) \geq 2k + 2$. It follows that if $\nu_2(B_1) = 2k + 2$, and so ϕ provides a unique prime ideal $\mathfrak{p}_{211}$ of $\mathbb{Z}_K$ lying above 2 with residue degree 2. If $\nu_2(B_1) \geq 2k + 3$, then $\nu_2(B_1) \geq 2k + 3$, and so ϕ provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each. In these last two cases, we have 2 divides $i(K)$ and $\nu_2(\underline{i(K)}) = 1$.
For $k = 1$, we have $\nu_2(\triangle) = 8$ and $a \equiv 5 \pmod 8$. In this case $\overline{F(x)} = x(x-1)^2(x^2 + x + 1)^2$ modulo 2. Let $\phi = x - 1$, $g(x) = x^2 + x + 1$, $F(x) = \cdots - 21\phi^2 + (7 + a)\phi + (b + a + 1)$, and $F(x) = (x - 3)g^3 + (5 + 3x)g^2 - (4x + 2)g + (a + 1)x + b$. Since x provides a unique prime ideal of of $\mathbb{Z}_K$ lying above 2 with residue degree 1 and g provides a unique prime ideal of of $\mathbb{Z}_K$ lying above 2 with residue degree 2, we conclude that $\nu_2(i(K)) \geq 1$ if and only if ϕ provides a unique prime ideal of of $\mathbb{Z}_K$ lying above 2 with residue degree 2 or ϕ provides two distinct prime ideals of of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each. If $(a, b) \in \{(5, 10), (13, 2)\} \pmod{16}$, then ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2 and so $\nu_2(i(K)) = 1$. If $(a, b) \in \{(5, 10), (13, 10)\} \pmod{16}$, then ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1 and so $\nu_2(i(K)) = 0$. For $(a, b) \in \{(5, 6), (5, 14), (13, 6), (13, 14)\} \pmod{16}$, let us replace ϕ by $\phi' = x - 3$ and consider the ϕ'-Newton polygon of $F(x)$ with respect to ν_2. It follows that If $(a, b) \in \{(5, 6), (13, 14)\} \pmod{16}$, then ϕ' provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each and so $\nu_2(i(K)) = 1$. If $(a, b) \in \{(5, 14), (13, 6)\} \pmod{16}$, then ϕ' provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1 and so $\nu_2(i(K)) = 0$.

(b) $a \equiv 3 \pmod 4$ and $b \equiv -(a + 1) \pmod 8$ because $N_{\phi}^{+}(F)$ has two sides.

(c) If $a \equiv 3 \pmod 8$ and $b \equiv 0 \pmod 8$, then ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2 and g provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each because $N_{g}^{+}(F)$ has a single side of degree 2 with $(1 + x)y^2 + y + x = (x + 1)(y - 1)(y - x)$ its attached residual polynomial of $F(x)$. In this case $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{211}\mathfrak{p}_{311}\mathfrak{p}_{312}$ with residue degrees $f_{111} = 1$ and $f_{211} = f_{311} = f_{312} = 2$, and so $\nu_2(i(K)) = 3$.

(d) $a \equiv 7 \pmod 8$ and $b \equiv 0 \pmod 8$. In this case ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2 and $N_{g}^{+}(F)$ has two sides. More precisely, $2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{211}\mathfrak{p}_{311}\mathfrak{p}_{321}$ with residue degrees $f_{111} = 1$ and $f_{211} = f_{311} = f_{312} = 2$, and so $\nu_2(i(K)) = 3$.

(e) If $a \equiv 5 \pmod 8$ and $b \equiv -(a + 1) \pmod{16}$ because if $b \equiv -(a + 1) \pmod{32}$, then $N_{\phi}^{+}(F)$ has two sides and if $b \equiv -(a + 1) + 16 \pmod{32}$, then $N_{\phi}^{+}(F)$ has a single side of degree 2, which provides a single prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2 and $N_{g}^{+}(F)$ has a single side of degree 1. Thus there are 2 prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each.

(f) If $a \equiv 5 \pmod 8$ and $\nu_2(b + (a + 1)) = 2$, then $\nu_2(b - (a + 1)) \geq 3$. If $\nu_2(b - (a + 1)) = 3$, then for $\phi = x + 1$, we have $N_{\phi}^{+}(F)$ has a single side of degree 1. Since $\nu_2(a + 1) = 1$, then $N_{g}^{+}(F)$ has a single side of height 1. Thus there are two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each and one prime ideal with residue degree 2. If $\nu_2(b - (a + 1)) = 4$, then for $\phi = x + 1$, we have $N_{\phi}^{+}(F)$ has a single side of degree 2 and its attached residual polynomial of F is $R_1(F)(y) = y^2 + y + 1$. Since $b \equiv 6 \pmod 8$, we conclude that $N_{g}^{+}(F)$ has a single side of degree 1, then there are 2 prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each, and so 2 divides $i(K)$. If $\nu_2(b - (a + 1)) \geq 5$, then for $\phi = x + 1$, we have

$N_\phi^+(F)$ has two sides of degree 1 each, and so there are 3 prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each, and so 2 divides $i(K)$.

Proof of Theorem 2.4.
By virtue of Engstrom's results [14], the proof is done if we provide the factorization of $3\mathbb{Z}_K$ into powers of prime ideals of $\mathbb{Z}_K$. Based on Theorem 2.1, we deal with the cases:

1. $3|a$ and $9|b$.
2. $(a,b) \notin \{(2,0),(8,3),(8,6)\} \pmod 9$.
3. $(a,b) \equiv (1,0) \pmod 9$.

1. $3|a$ and $9|b$, then for $\phi = x$, $\overline{F(x)} = \phi^7$ in $\mathbb{F}_3[x]$. It follows that:

   (a) If $\nu_3(a) \geq \nu_3(b)$, then $N_\phi(F)$ has a single side of degree 1, and so there is a unique prime ideal of $\mathbb{Z}_K$ lying above 3.

   (b) If $\nu_3(a) + 1 \leq \nu_3(b)$, then $N_\phi(F) = S_1 + S_2$ has two sides joining $(0, \nu_3(b))$, $(1, \nu_3(a))$, and $(7,0)$. Since S_1 is of degree 1, S_1 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1. Thus $\nu_3(i(K)) \geq 1$ if and only if S_2 provides at least three prime ideals of $\mathbb{Z}_K$ lying above 3, with residue degree 1 each. If $\nu_3(a) \notin \{2,3,4\}$, then S_2 is of degree 1, and so S_2 provides exactly one prime ideal of $\mathbb{Z}_K$ lying above 3, with residue degree 1 each. If $\nu_3(a) \in \{2,4\}$, then S_2 is of degree 2, and so S_2 provides at most two prime ideal of $\mathbb{Z}_K$ lying above 3. Hence 3 is not a common index divisor of K. If $\nu_3(a) = 3$, then S_2 is of degree 3 and its attached residual polynomial of $F(x)$ is $R_1(F)(y) = y^3 + a_3 = (y + a_3)^3$. So, we have to use second order Newton polygon. Let ω_2 be the valuation of second order Newton polygon. ω_2 is defined by $\omega_2(P) = \min\{2\nu_3(p_i) + i, i = 0, \ldots, n\}$ for every non zero polynomial $p = \sum_{i=0}^{n} p_i x^i$ of $\mathbb{Q}_3[x]$. Let $\phi_2 = x^2 + 3a_3$ be a key polynomial of ω_2 and $N_2(F)$ the ϕ_2-Newton polygon of $F(x)$ with respect to ω_2. It follows that: If $a_3 \equiv 1 \pmod 3$, then for $\phi_2 = x^2 + 3$, we have $F(x) = x\phi_2^3 - 9x\phi_2^2 + 27x\phi_2 + (a-27)x + b$ is the ϕ_2-expansion of $F(x)$. We have the following cases:

      i. If $\nu_3(b) = 4$, then $N_2(F) = T$ has a single side joining $(0,8)$ and $(3,7)$. Thus T is of degree 1 and S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1.

      ii. If $\nu_3(b) \geq 5$ and $\nu_3(a-27) = 4$, then $N_2(F) = T$ has a single side joining $(0,9)$ and $(3,7)$. Thus T is of degree 1 and S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1.

      iii. If $\nu_3(b) = 5$ and $\nu_3(a-27) \geq 5$, then $N_2(F) = T$ has a single side joining $(0,10)$ and $(3,7)$ and its attached residual polynomial of F is $R_2(F)(y) = xy^3 + xy + b_3$, which is irreducible over $\mathbb{F}_2 = \mathbb{F}_\phi$ because ϕ is of degree 1. Thus S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 3.

      iv. If $\nu_3(b) \geq 6$ and $\nu_3(a-27) \geq 5$, then $N_2(F) = T_1 + T_2$ has two sides joining $(0,v)$, $(2,9)$ and $(3,7)$ with $v \geq 11$. Thus T_1 is of degree 1, T_2 of degree 2 and $R_2(F)(y) = xy^2 + x$ is its attached residual polynomial of $F(x)$, which is irreducible over $\mathbb{F}_2 = \mathbb{F}_\phi$. Thus S_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3, with residue degree 1 and a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 2.

   Similarly, for $a_3 \equiv -1 \pmod 3$, let $\phi_2 = x^2 - 3$. Then $F(x) = x\phi_2^3 + 9x\phi_2^2 + 27x\phi_2 + (a + 27)x + b$ is the ϕ_2-expansion of $F(x)$. By analogous to the case $a_3 \equiv 1 \pmod 3$, in every case 3 does not divide $i(K)$. If $a \equiv 1 \pmod 3$, then $\overline{F(x)} = x(x^2+1)^3$ in $\mathbb{F}_3[x]$. So, there are exactly a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1 and the other prime ideals of $\mathbb{Z}_K$ lying above 3 are of residue degrees at least 2 each prime ideal factor. Hence $\nu_3(i(K)) = 0$.

   (c) If $a \equiv -1 \pmod 3$, then $\overline{F(x)} = x(x-1)^3(x+1)^3$ in $\mathbb{F}_3[x]$. Let $\phi_1 = x - 1$, $\phi_2 = x + 1$, $F(x) = \phi_1^7 + 7\phi_1^6 + 21\phi_1^5 + 35\phi_1^4 + 35\phi_1^3 + 21\phi_1^2 + (7+a)\phi_1 + (b + a + 1)$, and $F(x) = \phi_2^7 - 7\phi_2^6 + 21\phi_2^5 - 35\phi_2^4 + 35\phi_2^3 - 21\phi_2^2 + (7+a)\phi_2 + (b - (a+1))$. It follows that:

i. If $a \equiv 8 \pmod 9$ and $b \equiv 0 \pmod 9$, then $\nu_3(b+(1+a)) \geq 2$ and $\nu_3(b-(1+a)) \geq 2$. Thus x a provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1, and each ϕ_i provides two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each prime ideal factor. In this two cases $\nu_3(i(K)) = 2$.

ii. If $a \equiv 5 \pmod 9$ and $b \equiv 3 \pmod 9$, then $\nu_3(b+(1+a)) \geq 2$ and $\nu_3(b-(1+a)) = 1$. Thus each of x and ϕ_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1, and ϕ_1 provides two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. Similarly, if $a \equiv 5 \pmod 9$ and $b \equiv 6 \pmod 9$, then $\nu_3(b-(1+a)) \geq 2$ and $\nu_3(b+(1+a)) = 1$. Thus each of x and ϕ_1 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1, ϕ_2 provides two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. In these two cases $\nu_3(i(K)) = 1$.

iii. If $a \equiv 2 \pmod 9$ and $b \equiv (1+a) \pm 9 \pmod{27}$, then $N_{\phi_2}^{+}(F)$ has a single side joining $(0,2)$ and $(3,0)$ and $N_{\phi_1}^{+}(F)$ has a single side joining $(0,1)$ and $(3,0)$. Thus there are 3 prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each, and so $\nu_3(i(K)) = 0$.

iv. Similarly, if $a \equiv 2 \pmod 9$ and $b \equiv -(1+a) \pm 9 \pmod{27}$, then there are 3 prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each, and so $\nu_3(i(K)) = 0$.

v. If $a \equiv 2 \pmod 9$ and $\nu_3(b) = 1$, then $\nu_3(\triangle) \geq 8$. Let $u = \frac{-7b_3}{2a}$. Then $u \in \mathbb{Z}_3$. Let $\phi = x - u$ and $F(x+u) = x^7 + \cdots + 35u^4x^3 + 21u^5x^2 + Ax + B$, where $A = 7u^6 + a = \frac{-\triangle}{6^6a^6}$ and $B = u^7 + au + b = \frac{b\triangle}{6^7a^7}$. It follows that $\nu_3(A) = \nu_3(B) = \nu_3(\triangle) - 6$, and so $N_{\phi}^{+}(F) = S_1$ has a single side joining $(0, \nu_3(\triangle) - 6)$ and $(3,0)$. Remark that since $\nu_3(b) = 1$ and $\nu_3(B) \geq 2$, $\nu_3(-u^7 - au + b) = 1$, and so $(x+u)$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1. Thus $\nu_3(i(K)) \geq 1$ if and only if ϕ provides at least two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each prime ideal factor.

A. If $\nu_3(\triangle) = 8$, then $N_{\phi}^{+}(F)$ has a single side of degree one, and so ϕ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1.

B. If $\nu_3(\triangle) = 9$, then $N_{\phi}^{+}(F) = S$ has a single side joining $(0,3)$ and $(3,0)$ with $R_1(F)(y) = -u^4y^3 + u^5y^2 + B_3$ its attached residual polynomial of $F(x)$. Since $a \equiv -1 \pmod 3$ and $B = \frac{b\triangle}{6^7a^7}$, we have $u \equiv -b_3 \pmod 3$ and $B_3 \equiv b_3\triangle_3 \pmod 3$. Thus $R_1(F)(y) = -y^3 - b_3y^2 + b_3\triangle_3$. Since $R_1(F)(y)$ is square free and $R_1(F)(0) \neq 0$, then $R_1(F)(y)$ has at most one root in $\mathbb{F}_{\phi}$. Thus S provides at most a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1. Therefore, $\nu_3(i(K)) = 0$.

C. If $\nu_3(\triangle) \geq 10$, then $N_{\phi}^{+}(F) = S_1 + S_2$ has two sides joining $(0, v-6)$ and $(3,1)$. It follows that Since S_2 is of degree 1, it provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 1. Moreover, if $\nu_3(\triangle)$ is even then S_1 is of degree 1, and so ϕ provides two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. In this case $\nu_3(i(K)) = 1$. If $\nu_3(\triangle) = 2(k+3)+1$, then S_1 is of degree 2 with residual polynomial $R_1(F)(y) = uy^2 + b_3\triangle_3$. Since $a \equiv -1 \pmod 3$, we have $2a \equiv 1 \pmod 3$ and $u \equiv -b_3 \pmod 3$. Thus $R_1(F)(y) = -b_3(y^2 - \triangle_3)$. It follows that if $(\frac{\triangle_3}{3}) = 1$, then $R_1(F)(y)$ has two different factors of degree 1 each, and so S_1 provides two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. In this case there are exactly five prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each and according to Engstrom's results $\nu_3(i(K)) = 2$. But if $(\frac{\triangle_3}{3}) = -1$, then $R_1(F)(y)$ is irreducible over $\mathbb{F}_{\phi} = \mathbb{F}_3$, and so S_1 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 2. In this last case there are exactly three prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each, and so $\nu_3(i(K)) = 0$.

Proof of Theorem 2.5.

We start by showing that 5 does not divide $i(K)$ for every integers of a and b such that $x^7 + ax + b$ is irreducible. By virtue of Engstrom's results [14], the proof is done if we provide the factorization of $5\mathbb{Z}_K$ into powers of prime ideals of $\mathbb{Z}_K$. By by the index formula $\triangle = (\mathbb{Z}_K : \mathbb{Z}[\alpha])^2 d_K$, if 5^2 does not divide $\triangle$, then $\nu_5(i(K)) = 0$. So, we assume that 5^2 divides $\triangle$.

1. So, $6^6a^7 + 7^7b^6 \equiv 0 \pmod{5}$. Since $a^5 \equiv a \pmod{5}$ and $b^5 \equiv b \pmod{5}$, then $a^3 \equiv 2b^2 \pmod{5}$, which means $(a,b) \in \{(0,0),(3,1),(2,2),(2,3),(3,4)\} \pmod{5}$. In order to show that $\nu_5(i(K)) = 0$ it suffices to show that for every value $(a,b) \in \mathbb{Z}^2$ such that $x^7 + ax + b$ is irreducible and $(a,b) \in \{(0,0),(2,1),(3,2),(3,3),(2,34\} \pmod{5}$ there are at most four prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 1, where K is the number field generated by a complex root of $x^7 + ax + b$.
    (a) For $(a,b) \equiv (0,0) \pmod{5}$, if $\nu_5(a) \geq \nu_5(b)$, then $N_\phi(F) = S$ has a single side and it is of degree 1. Thus there is a unique prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$ lying above 5 with residue degree 1. More precisely $5\mathbb{Z}_K = \mathfrak{p}^7$.
    If $\nu_5(a) + 1 \leq \nu_5(b)$, then $N_\phi(F) = S_1 + S_2$ has two sides. More precisely, S_1 is of degree 1. Let d be degree of S_2. Since 6 is the length of S_2, then $d \in \{1,2,3\}$. Thus S_1 provides a unique prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$ lying above 5 with residue degree 1 and S_2 provides at most three prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each.
    (b) For $(a,b) \equiv (3,1) \pmod{5}$, since $\overline{F(x)} = (x+4)^2(x+3)(x^4+4x^3+x^2+x+2)$ in $\mathbb{F}_5[x]$, there are at most three prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each.
    (c) For $(a,b) \equiv (2,2) \pmod{5}$, since $\overline{F(x)} = (x^4+2x^3+4x^2+2x+2)(x+4)(x+2)^2$ in $\mathbb{F}_5[x]$, there are at most three prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each.
    (d) For $(a,b) \equiv (2,3) \pmod{5}$, since $\overline{F(x)} = (x+1)(x+3)^2(x^4+3x^3+4x^2+3x+2)$ in $\mathbb{F}_5[x]$, there are at most three prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each.
    (e) For $(a,b) \equiv (3,4) \pmod{5}$, since $\overline{F(x)} = (x^4+x^3+x^2+4x+2)(x+1)^2(x+2)$ in $\mathbb{F}_5[x]$, there are at most three prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each.

We conclude that in all cases $\nu_5(i(K)) = 0$.
For $p \geq 7$, since the field K is of degree 7, there are at most 7 prime ideals of $\mathbb{Z}_K$ lying above p. The fact that there at least $p \geq 7$ monic irreducible polynomial of degree f in $\mathbb{F}_p[x]$ for every positive integer $f \in \{1,2,3\}$, we conclude that p does not divide $i(K)$.

Proof of Proposition 2.2.
First according to Theorem 2.1 and the hypotheses of Example 2.2, 2 is the unique prime integer candidate to divide $ind(\alpha)$. Let $\phi = x$. Then $\overline{F(x)} = \phi^7$ in $\mathbb{F}_2[x]$ and $N_\phi(F) = S$ has a single side of degree GCD$(7,v) = 1$. Thus $F(x)$ is irreducible over $\mathbb{Q}_2$. Let K be the number field generated by a root α of $F(x)$. Since $F(x)$ is irreducible over $\mathbb{Q}_2$, there is a unique valuation ω of K extending ν_2. By Theorem 3.1, we have $\nu_2(\mathbb{Z}_K : \mathbb{Z}[\alpha]) \geq ind_\phi(F) \geq 1$, and so $F(x)$ is not a monogenic polynomial. Let $\theta = \dfrac{\alpha^x}{2^y}$, where (x,y) is the unique solution of integers of the Diophantine equation $vx - 7y = 1$ and $0 \leq x \leq 6$. Then $\theta \in K$. Since v and 7 are coprime, we conclude that $K = \mathbb{Q}(\theta)$. Let us show that $\mathbb{Z}_K = \mathbb{Z}[\theta]$, and so K is monogenic. By [13, Corollary 3.1.4], in order to show that $\theta \in \mathbb{Z}_K$, we need to show that $\omega(\theta) \geq 0$, where ω is the unique valuation of K extending ν_2. Since $N_\phi(F) = S$ has a single side of slope $-v/7$, we conclude that $\omega(\alpha) = v/7$, and so $\omega(\theta) = \dfrac{xv}{7} - y = \dfrac{1}{7}$. Let $g(x)$ be the minimal polynomial of θ over $\mathbb{Q}$. By the formula relating roots and coefficients of a monic polynomial, we conclude that $g(x) = x^7 + \displaystyle\sum_{i=1}^{7}(-1)^i s_i x^{7-i}$, where $s_i = \displaystyle\sum_{k_1<\cdots<k_i} \theta_{k_1}\cdots\theta_{k_i}$ and $\theta_1,\ldots,\theta_7$ are the $\mathbb{Q}_p$-conjugates of θ. Since there is a unique valuation extending ν_2 to any algebraic extension of $\mathbb{Q}_2$, we conclude that $\omega(\theta_i) = 1/7$ for every $i = 1,\ldots,7$. Thus $\nu_2(s_7) = \omega(\theta_1\cdots\theta_7) = 7 \times 1/7 = 1$ and $\nu_2(s_i) \geq i/7$ for every $i = 1,\ldots,6$, which means that $g(x)$ is a 2-Eisenstein polynomial. Hence 2 does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\theta])$. As 2 is the unique positive prime integer candidate to divide

$(\mathbb{Z}[\alpha]:\mathbb{Z}[\theta])$, we conclude that for every prime integer p, p does not divide $(\mathbb{Z}_K:\mathbb{Z}[\theta])$, which means that $\mathbb{Z}_K=\mathbb{Z}[\theta]$.

5. Examples

Let $F=x^7+ax+b\in\mathbb{Z}[x]$ be a monic irreducible polynomial and K a number field generated by a root α of $F(x)$. In the following examples, we calculate the index of the field K. First based on Theorem 2.5, $\nu_p(i(K))=0$ for every prime integer $p\geq 5$. Thus we need only to calculate $\nu_p(i(K))$ for $p=2,3$.

1. For $a=6$ and $b=6$, since $F(x)$ is p-Eisenstein for every $p=2,3$, we conclude that $F(x)$ is irreducible over $\mathbb{Q}$, 2 (resp. 3) does not divide $(\mathbb{Z}_K:\mathbb{Z}[\alpha])$. Thus 2 (resp. 3) does not divide $i(K)$), and so $i(K)=1$.
2. For $a=28$ and $b=32$, since $\overline{F(x)}$ is irreducible over $\mathbb{F}_5$, $F(x)$ is irreducible over $\mathbb{Q}$. By the first item of Theorem 2.3, we have $\nu_2(i(K))=1$. By Theorem 2.4, $\nu_3(i(K))=0$. Thus $i(K)=2$.
3. For $a=3$ and $b=8$, $\overline{F(x)}$ is irreducible over $\mathbb{F}_5$, $F(x)$ is irreducible over $\mathbb{Q}$. Again since $a\equiv 3 \pmod 4$ and $b\equiv 0 \pmod 8$, by Theorem 2.3, $\nu_2(i(K))=3$. By Theorem 2.4, $\nu_3(i(K))=0$. Thus $i(K)=8$.
4. For $a=-1$ and $b=9$, since $\overline{F(x)}$ is irreducible over $\mathbb{F}_2$, $F(x)$ is irreducible over $\mathbb{Q}$. Since $2\mathbb{Z}_K$ is a prime ideal of $\mathbb{Z}_K$, $\nu_2(i(K))=0$. Also since $a\equiv 8 \pmod 9$ and $b\equiv 0 \pmod 9$, by Theorem 2.4, $\nu_3(i(K))=2$. Thus $i(K)=9$.
5. For $a=803$ and $b=2112$, since $\overline{F(x)}$ is irreducible over $\mathbb{F}_5$, $F(x)$ is irreducible over $\mathbb{Q}$. Since $a\equiv 3 \pmod 4$ and $b\equiv 0 \pmod 8$, by Theorem 2.3, $\nu_2(i(K))=3$. Similarly since $a\equiv 5 \pmod 9$ and $b\equiv 6 \pmod 9$, by Theorem 2.4, $\nu_3(i(K))=1$. Thus $i(K)=24$.
6. For $a=35$ and $b=72$, since $\overline{F(x)}$ is irreducible over $\mathbb{F}_{11}$, $F(x)$ is irreducible over $\mathbb{Q}$. Since $a\equiv 3 \pmod 4$ and $b\equiv 0 \pmod 8$, by Theorem 2.3, $\nu_2(i(K))=3$. Similarly since $a\equiv 8 \pmod 9$ and $b\equiv 0 \pmod 9$, by Theorem 2.4, $\nu_3(i(K))=2$. Thus $i(K)=72$.

Conflicts of Interest: There are non-financial competing interests to report.

Data Availability Statement: Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

1. S. Ahmad, T. Nakahara, and A. Hameed, *On certain pure sextic fields related to a problem of Hasse*, Int. J. Alg. Comput., 26(3) (2016), 577–583 .
2. H. Ben Yakkou and L. El Fadil, On monogenity of certain number fields defined by trinomials (arXiv:2109.08765)
3. Y. Bilu, I. Gaál and K. Győry, Index form equations in sextic fields: a hard computation, *Acta Arithmetica* **115(1)**, (2004), 85–96.
4. L. Carlitz , A note on common index divisors, Proc. Amer. Math. Soc. 3 (1952) 688–692
5. R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, *Göttingen Abhandlungen*, **23**, (1878), 1–23.
6. , C. T. Davis and B. K. Spearman, *The index of a quartic field defined by a trinomial x^4+ax+b*, J. of Alg. and Its Applications, **17(10)** (2018) 1850197
7. A. Deajim and L. El Fadil, On the integral closednessof $R[\alpha]$, Math. Reports **24(74)(3)** (2022) 571–581
8. L. El Fadil, On index and monogenity of certain number fields defined by trinomials, Math. Slovaca **73(4)**, (2023), 861–870
9. L. El Fadil, *On non monogenity of certain number fields defined by a trinomial x^6+ax^3+b*, J. Number Theory, available online Junary 24, 2022, doi: 10.1016/j.jnt.2021.10.017
10. L. El Fadil, *On common index divisor and monogenity of certain number fields defined by a trinomial x^5+ax^2+b*, Commun. Algebra, available online Junary 23, 2022,doi 10.1080/00927872.2022.2025820
11. L. El Fadil and I. Gaál, *On non-monogenity of certain number fields defined by trinomials x^4+ax^2+b* (Submitted)
12. L. El Fadil, J. Montes and E. Nart , Newton polygons and p-integral bases of quartic number fields *J. Algebra and Appl*, **11(4)**, (2012), 1250073.

13. O. Endler, *Valuation Theory*, Springer-Verlag, Berlin, 1972
14. H. T. Engstrom, *On the common index divisors of an algebraic field*, Trans. Amer. Math. Soc. **32(2)** (1930) 223–237.
15. I. Gaál, *An experiment on the monogenity of a family of trinomials*, JP Journal of Algebra Number Theory Appl. 51(1) (2021) 97–111
16. I. Gaál and K. Györy, *Index form equations in quintic fields*, Acta Arith. 89 (1999), 379–396
17. I. Gaál, A. Pethö, and M. Pohst, *On the indices of biquadratic number fields having Galois group V_4*, Arch. Math. 57 (1991), 357 – 361.
18. I. Gaál and L. Remete, Power integral bases and monogenity of pure fields, *J. of Number Theory*, **173**, (2017) 129–146
19. I. Gaál, Diophantine equations and power integral bases, Theory and algorithm, *Second edition, Boston, Birkhäuser*, (2019)
20. J. Guardia, J. Montes, and E. Nart, Newton polygons of higher order in algebraic number theory, Trans. Amer. Math. Soc. **364** (1) (2012), 361–416.
21. J. Guardia, J. Montes, and E. Nart, Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields, Journal de Théorie des Nombres de Bordeaux, **23** (3) (2011), 3667–696.
22. P. LlOrente, E. Nart and N. Vila, Decomposition of primes in number fields defined by trinomials, Séminaire de Théorie des Nombres de Bordeaux, 3 (1991), 27–41.
23. Y. Motoda, T. Nakahara and S. I. A. Shah, *On a problem of Hasse*, J. Number Theory, 96 (2002), 326–334
24. J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin (1999)
25. H. Hasse, Zahlentheorie, *Akademie-Verlag, Berlin*, (1963)
26. K. Hensel, Theorie der algebraischen Zahlen, *Teubner Verlag, Leipzig, Berlin*, (1908)
27. K. Hensel, Arithemetishe untersuchungen uber die gemeinsamen ausserwesentliche Discriminantentheiler einer Gattung, *J. Reine Angew Math*, **113**, (1894) 128–160
28. K. Hensel, Untersuchung der Fundamentalgleichung einer Gattung fr̈ eine reelle Primzahl als Modul und Bestimmung der Theiler ihrer Discriminante, **(113)**, (1894) 61–83
29. S. MacLane, A construction for absolute values in polynomial rings, Trans. Amer. Math. Soc. 40 (1936) 363–395
30. T. Nakahara, *On the indices and integral bases of non-cyclic but abelian biquadratic fields*, Archiv der Mathematik 41(6), 504-508.
31. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer Verlag, 3. Auflage, 2004.
32. A. Pethö and M. Pohst, *On the indices of multiquadratic number fields*, Acta Arith. 153(4) (2012) 393–414
33. H. Smith, The monogenity of radical extension, *Acta Arithmitica*, **198**, (2021) 313–327
34. O. Ore, Newtonsche Polygone in der Theorie der algebraischen Korper, *Math. Ann* **99**, (1928) 84–117

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.