DOI: 10.3842/umzh.v76i7.7536

UDC 511

Omar Kchit[1] (Faculty of Sciences Dhar El Mahraz, Atlas-Fes, Sidi Mohamed ben Abdellah University, Morocco)

ON INDEX DIVISORS AND MONOGENITY OF CERTAIN OCTIC NUMBER FIELDS DEFINED BY $x^8 + ax^3 + b$

ПРО ІНДЕКСНІ ДІЛЬНИКИ ТА МОНОГЕННІСТЬ ДЕЯКИХ ПОЛІВ ОКТИЧНИХ ЧИСЕЛ, ЩО ЗАДАНІ ФОРМУЛОЮ $x^8 + ax^3 + b$

For any octic number field K generated by a root α of a monic irreducible trinomial $F(x) = x^8 + ax^3 + b \in \mathbb{Z}[x]$ and for every rational prime p, we show when p divides the index of K. We also describe the prime power decomposition of the index $i(K)$. In this way, we give a partial answer to Problem 22 of Narkiewicz [*Elementary and analytic theory of algebraic numbers*, Springer-Verlag, Auflage (2004)] for this family of number fields. As an application of our results, we conclude that if $i(K) \neq 1$, then K is not monogenic. We illustrate our results by some computational examples.

Для довільного октичного числового поля K, породженого коренем α монічного незвідного тричлена $F(x) = x^8 + ax^3 + b \in \mathbb{Z}[x]$, і для кожного раціонального простого p показано, коли p ділить індекс K. Також описано розклад індексу $i(K)$ за простими степенями. Таким чином, дано часткову відповідь на проблему 22 Наркевича [*Elementary and analytical theory of algebraic numbers*, Springer-Verlag, Auflage (2004)] для цієї сім'ї числових полів. Як застосування одержаних результатів, зроблено висновок, що якщо $i(K) \neq 1$, то K не є моногенним. Отримані результати проілюстровано деякими обчислювальними прикладами.

1. Introduction. Let K be a number field of degree n and $\mathbb{Z}_K$ its ring of integers. For any primitive element $\alpha \in \mathbb{Z}_K$ of K, it is well-known that $\mathbb{Z}[\alpha]$ is a free $\mathbb{Z}$-module of rank n. In what follows that $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, the index of $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_K$ is finite. A known formula linking $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, $\Delta(\alpha)$, and d_K is given by

$$\Delta(\alpha) = \pm(\mathbb{Z}_K : \mathbb{Z}[\alpha])^2 \cdot d_K, \tag{1.1}$$

where d_K is the absolute discriminant of K and $\Delta(\alpha)$ is the discriminant of the minimal polynomial of α over $\mathbb{Q}$. The index of K, denoted by $i(K)$, is the greatest common divisor of the indices of all integral primitive elements of K. Say $i(K) = \gcd\{(\mathbb{Z}_K : \mathbb{Z}[\theta]) \mid K = \mathbb{Q}(\theta) \text{ and } \theta \in \mathbb{Z}_K\}$. A rational prime p dividing $i(K)$ is called a prime common index divisor of K. If K is monogenic, then $\mathbb{Z}_K$ has a power integral basis, i.e., a $\mathbb{Z}$-basis of the form $(1, \theta, \ldots, \theta^{n-1})$, and the index of K is trivial, say $i(K) = 1$. Therefore, a field having a prime common index divisor is not monogenic. Two of the well-known examples of monogenic number fields are quadratic fields $\mathbb{Q}(\sqrt{d})$ and cyclotomic fields $\mathbb{Q}(\zeta_n)$. Their rings of integers can be written as $\mathbb{Z}[\theta]$, where θ is $\sqrt{d}$ or $\dfrac{1+\sqrt{d}}{2}$ in the quadratic case, and ζ_n in the cyclotomic case. In 1871, Dedekind was the first who gave an example of a nonmonogenic number field with nontrivial index [3, p. 30, § 5]. Based on Dedekind's ideas and using Kronecker's theory of algebraic number fields, Hensel gave necessary and sufficient condition on the so-called "index divisors of K" for any rational prime p to be a prime common index divisor [14]. In 1930, Engstrom [11] was the first one who studied the prime power decomposition of the index of a number field. He showed that, for number fields of degree $n \leq 7$, $\nu_p(i(K))$ is determined by the form of the factorization of $p\mathbb{Z}_K$, where ν_p is the p-adic valuation of $\mathbb{Q}$. This motivated a

[1] E-mail: omar.kchit@usmba.ac.ma.

very important question, stated as Problem 22 in Narkiewicz's book [16], which asks for an explicit formula of the highest power $\nu_p(i(K))$ for a given rational prime p dividing $i(K)$. In [19], Śliwa showed that, if p is a nonramified ideal in K, then $\nu_p(i(K))$ is determined by the factorization of $p\mathbb{Z}_K$. These results were generalized by Nart [17], who developed a p-adic characterization of the index of a number field. In [15], Nakahara studied the index of noncyclic but Abelian biquadratic number fields. In [12], Gaál et al. characterized the field indices of biquadratic number fields having Galois group V_4. Recently many authors have been interested on index divisors and monogenity of number fields defined by trinomials. In [2], for any quartic number field K defined by a trinomial $x^4 + ax + b$, Davis and Spearman characterized when $p = 2, 3$ divides $i(K)$. In [6], for any quartic number field K defined by a trinomial $x^4 + ax^2 + b$, El Fadil and Gaál gave necessary and sufficient conditions on a and b to characterize when a rational prime p divides $i(K)$. In [4], for any rational prime p, El Fadil characterized when p divides the index $i(K)$ for any quintic number field K defined by a trinomial $x^5 + ax^2 + b$. In [7], El Fadil and Kchit characterized the index and studied the monogenity of any sextic number field defined by $x^6 + ax^5 + b$. In [8], for every rational prime p, they characterized $\nu_p(i(K))$ for any septic number field defined by a trinomial $x^7 + ax^3 + b$. In [5], El Fadil characterized the index of any quintic number field defined by $x^5 + ax^3 + b$. In this paper, for any octic number field K defined by a monic irreducible trinomial $x^8 + ax^3 + b \in \mathbb{Z}[x]$ and for every rational prime p, we characterize when p divides the index $i(K)$. Based on Engstrom's results given in [11], we evaluate $\nu_p(i(K))$ in some cases. In particular, we show that $i(K) = 2^{\nu_2} \cdot 3^{\nu_3}$, where $\nu_2 \geq 0$ and $0 \leq \nu_3 \leq 1$.

2. Main results. Throughout this section, K is a number field generated by a complex root α of a monic irreducible trinomial $F(x) = x^8 + ax^3 + b \in \mathbb{Z}[x]$. Without loss of generality, we assume that, for every rational prime p, $\nu_p(a) \leq 4$ or $\nu_p(b) \leq 7$.

Along this paper, $\Delta = \Delta(F)$ denote the discriminant of $F(x)$. For every integer $m \in \mathbb{Z}$ and a rational prime p, let $m_p = \dfrac{m}{p^{\nu_p(m)}}$.

In the next theorems, for every rational prime p, we characterize when p divides $i(K)$. The following theorem characterizes when 2 divides $i(K)$.

Theorem 2.1. *The following table gives some information on* $\nu_2(i(K))$:

Table 1

Conditions		$\nu_2(i(K))$
$(a,b) \equiv (4,3) \pmod 8$		≥ 1
$(a,b) \in \{(16,15),(0,31)\} \pmod{32}$		
$(a,b) \equiv (8,7) \pmod{16}$	$\nu_2(\Delta)$ is odd	2
	$\nu_2(\Delta) = 28$ and $\Delta_2 \equiv 3 \pmod 4$	
	$\nu_2(\Delta) = 28$ and $\Delta_2 \equiv 1 \pmod 8$	≥ 1
	$\nu_2(\Delta) = 2k \geq 30$ and $\Delta_2 \equiv 1 \pmod 4$	2
	$\nu_2(\Delta) = 2k \geq 30$ and $\Delta_2 \equiv 7 \pmod 8$	≥ 1
$a \equiv 64 \pmod{128}$ and $b \equiv 368 \pmod{512}$		
$a \equiv 64 \pmod{128}$ and $b \equiv 240 \pmod{256}$		2
$a \equiv 0 \pmod{128}$ and $b \equiv 496 \pmod{512}$		≥ 1
Otherwise		0

The following theorem characterizes when 3 divides $i(K)$.

Theorem 2.2. *The rational prime* 3 *divides* $i(K)$ *if and only if* $a \equiv \pm 81 \pmod{3^5}$, $b \equiv 4374 \pmod{3^8}$, $\nu_3(\Delta) = 2k \geq 54$, *and* $\Delta_3 \equiv -1 \pmod 3$. *More precisely, if the above conditions hold, then* $\nu_3(i(K)) = 1$.

Theorem 2.3. *For every rational prime* $p \geq 5$ *and for every* $(a, b) \in \mathbb{Z}^2$ *such that* $F(x) = x^8 + ax^3 + b$ *is irreducible,* p *does not divide the index* $i(K)$, *where* K *is the number field defined by* $F(x)$.

***Corollary* 2.1.** *For every integers* a *and* b *such that* $F(x) = x^8 + ax^3 + b$ *is irreducible over* $\mathbb{Q}$, $i(K) = 2^{\nu_2} \cdot 3^{\nu_3}$, *where* $\nu_2 \geq 0$, $0 \leq \nu_3 \leq 1$, *and* K *is the number field generated by a root of* $F(x)$.

In the next theorems, we provide some cases when the index $i(K) = 1$ and K is monogenic. The following theorem characterizes when the ring $\mathbb{Z}[\alpha]$ is integrally closed.

Theorem 2.4. *The ring* $\mathbb{Z}[\alpha]$ *is integrally closed if and only if the following conditions hold*:

(1) b *is square free.*

(2) *If* 2 *divides* a *and does not divide* b, *then* $(a, b) \in \{(0, 1), (2, 3)\} \pmod 4$.

(3) *If* 5 *divides* b *and does not divide* a, *then* $\nu_5(b - a^4 + a^8) = 1$.

(4) *For every rational prime* $p \notin \{2, 3, 5\}$ *dividing* Δ, *if* $\nu_p(ab) = 0$, *then* $\nu_p(\Delta) = 1$.

If all these conditions hold, then K *is monogenic and* $i(K) = 1$.

The following theorem gives sufficient conditions on a and b so that K is monogenic even thought $\mathbb{Z}[\alpha]$ is not integrally closed.

Theorem 2.5. *Let* p *be any rational prime and* $K = \mathbb{Q}(\alpha)$ *a number field generated by a root* α *of a monic irreducible trinomial* $F(x) = x^8 + ax^3 + b$ *such that* $\nu_5(a) \geq 1$, b_p *is square free, and* $\nu_q(3^3 \cdot 5^5 a^8 - 2^{24} b^5) \leq 1$ *for any rational prime* $q \notin \{3, 5, p\}$. *Then we have the following:*

(1) *If* $\nu_p(b) = 3$, $\nu_p(a) \geq 2$, *then* $\mathbb{Z}_K = \mathbb{Z}[\alpha^3/p]$.

(2) *If* $\nu_p(b) = 5$, $\nu_p(a) \geq 4$, *then* $\mathbb{Z}_K = \mathbb{Z}[\alpha^5/p^3]$.

(3) *If* $\nu_p(b) = 7$, $\nu_p(a) \geq 5$, *then* $\mathbb{Z}_K = \mathbb{Z}[\alpha^7/p^6]$.

In particular, if one of the above conditions holds, then K *is monogenic and* $i(K) = 1$.

3. Preliminaries. Our proofs are based on Newton polygon techniques applied on prime ideal factorization, which is a standard method that is rather technical but very efficient to apply. We have introduced the corresponding concepts in several former papers. Here we only give the theorem of index of Ore which plays a key role for proving our main results.

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a complex root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$. We shall use Dedekind's theorem [18, Chapter I, Proposition 8.3] and Dedekind's criterion [1, Theorem 6.1.4]. Let $\phi \in \mathbb{Z}_p[x]$ be a monic lift to an irreducible factor of $F(x)$ modulo p, $F(x) = a_0(x) + a_1(x)\phi(x) + \ldots + a_l(x)\phi(x)^l$ the ϕ-expansion of $F(x)$, and $N_\phi^+(F)$ the principal ϕ-Newton polygon of $F(x)$. Let $\mathbb{F}_\phi$ be the field $\mathbb{F}_p[x]/(\overline{\phi})$. Then to every side S of $N_\phi^+(F)$ with initial point (i, u_i), and every $i = 0, \ldots, l$, let the residue coefficient $c_i \in \mathbb{F}_\phi$ defined as follows:

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

Let $-\lambda = -h/e$ be the slope of S, where h and e are two positive coprime integers and $l = l(S)$ its length. Then $d = l/e$ is the degree of S. Hence, if i is not a multiple of e, then $(s + i, u_{s+i})$ does

not lie on S, and so $c_i = 0$. Let $R_1(F)(y) = t_d y^d + t_{d-1}y^{d-1} + \ldots + t_1 y + t_0 \in \mathbb{F}_\phi[y]$, called the residual polynomial of $F(x)$ associated to the side S, where, for every $i = 0, \ldots, d$, $t_i = c_{s+ie}$. 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 $N_{\phi_i}^+(F) = S_{i1} + \ldots + S_{ir_i}$ 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 $\mathbb{F}_{\phi_i}[y]$. Then we have the following theorem of index of Ore.

Theorem 3.1 [9, Theorems 1.7 and 1.9]**.** *Under the above hypotheses, we have the following*:

(1) $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) \geq \sum_{i=1}^{r} \operatorname{ind}_{\phi_i}(F)$. *The equality holds if $F(x)$ is p-regular.*

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

$$p\mathbb{Z}_K = \prod_{i=1}^{r} \prod_{j=1}^{r_i} \prod_{s=1}^{s_{ij}} \mathfrak{p}_{ijs}^{e_{ij}}$$

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 $f_{ijs} = \deg(\phi_i)\deg(\psi_{ijs})$ for every (i, j, s).

If the theorem of Ore fails, that is, $F(x)$ is not p-regular, then in order to complete the factorization of $F(x)$, Guàrdia, Montes, and Nart introduced the notion of high order Newton polygon [13]. Similar to first order, for each order r, they introduced the valuation ω_r, the key polynomial $\phi_r(x)$ for this valuation, the Newton polygon $N_r(F)$ of any polynomial $F(x)$ with respect to ω_r and $\phi_r(x)$, and for each side T_i of $N_r(F)$, the residual polynomial $R_r(F)(y)$, and the index of $F(x)$ in order r. For more details, we refer to [13].

For the proof of results, we need the following lemma, which characterizes the prime common index divisors of K.

Lemma 3.1 [11]**.** *Let p be a rational prime and K 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 divides the index $i(K)$ if and only if $\mathcal{P}_f > \mathcal{N}_f$ for some positive integer f.*

4. Proofs of main results. Throughout this section, if $p\mathbb{Z}_K = \prod_{i=1}^{r} \prod_{j=1}^{t_i} \prod_{s=1}^{s_{ij}} \mathfrak{p}_{ijs}^{e_{ij}}$, then e_{ij} denotes the ramification index of $\mathfrak{p}_{ijs}$ and f_{ijs} denotes its residue degree for every (i, j, s).

***Proof of Theorem* 2.1**. Since $\Delta = -b^2(3^3 \cdot 5^5 a^8 - 2^{24} b^5)$ is the discriminant of $F(x)$, thanks to the index formula (1.1), if 2 does not divide ab, then $\nu_2((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$, and so $\nu_2(i(K)) = 0$. Assume that 2 divides ab. Then we have the following cases:

(1) If $\nu_2(a) = 0$ and $\nu_2(b) \geq 1$, then $F(x) \equiv x^3(x-1)(x^4 + x^3 + x^2 + x + 1) \pmod 2$. Obviously, $x - 1$ (resp., $x^4 + x^3 + x^2 + x + 1$) provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 1 (resp., 4). Let $\phi = x$. Then $N_\phi^+(F) = S_1$ has a single side joining $(0, \nu_2(b))$ and $(3, 0)$.

(i) If $\nu_2(b) \not\equiv 0 \pmod 3$, then $d(S_1) = 1$, and so $2\mathbb{Z}_K = \mathfrak{p}_1^3\mathfrak{p}_2\mathfrak{p}_3$ with $f_1 = f_2 = 1$ and $f_3 = 4$. Hence, $\nu_2(i(K)) = 0$.

(ii) If $\nu_2(b) \equiv 0 \pmod 3$, then $d(S_1) = 3$ with $R_1(F)(y) = y^3 + 1 = (y+1)(y^2+y+1) \in \mathbb{F}_\phi[y]$. Thus, $2\mathbb{Z}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}\mathfrak{p}_{21}\mathfrak{p}_{31}$ with $f_{11} = f_{21} = 1$, $f_{21} = 2$, and $f_{31} = 4$. Hence, $\nu_2(i(K)) = 0$.

(2) If $\nu_2(a) \geq 1$ and $\nu_2(b) = 0$, then $F(x) \equiv (x-1)^8 \pmod 2$. Let $\phi = x - 1$. Then

$$F(x) = \phi^8 + 8\phi^7 + 28\phi^6 + 56\phi^5 + 70\phi^4 + (a+56)\phi^3 + (3a+28)\phi^2 + (3a+8)\phi + a + b + 1.$$

(i) If $(a,b) \in \{(0,1),(2,3)\} \pmod 4$, then $N_\phi(F) = S_1$ has a single side of height 1. Thus, $2\mathbb{Z}_K = \mathfrak{p}_1^8$ with residue degree 1. Hence, $\nu_2(i(K)) = 0$.

(ii) If $(a,b) \equiv (2,1) \pmod 4$, then $N_\phi(F) = S_1 + S_2$ has two sides joining $(0,w)$, $(1,1)$, and $(8,0)$ with $w \geq 2$. Thus, the degree of each side is 1, and so $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2^7$ with residue degree 1 each ideal factor. Hence, $\nu_2(i(K)) = 0$.

(iii) If $(a,b) \in \{(0,3),(4,7)\} \pmod 8$, then $N_\phi(F) = S_1$ has a single side joining $(0,2)$ and $(8,0)$ with $R_1(F)(y) = y^2 + y + 1$, which is irreducible over $\mathbb{F}_\phi$. Thus, $2\mathbb{Z}_K = \mathfrak{p}_1^4$ with residue degree 2. Hence, $\nu_2(i(K)) = 0$.

(iv) If $(a,b) \equiv (4,3) \pmod 8$, then $N_\phi(F) = S_1 + S_2 + S_3$ has three sides joining $(0,w)$, $(1,2)$, $(4,1)$, and $(8,0)$ with $w \geq 3$. Thus, the degree of each side is 1, and so $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2^3\mathfrak{p}_3^4$ with residue degree 1 each ideal factor. Hence, 2 divides $i(K)$.

(v) If $(a,b) \equiv (0,7) \pmod 8$, then we have the following subcases:

(a) If $(a,b) \in \{(0,7),(8,15)\} \pmod{16}$, then $N_\phi(F) = S_1 + S_2$ has two sides joining $(0,3)$, $(4,1)$, and $(8,0)$ with $d(S_2) = 1$ and $R_{1_1}(F)(y) = y^2 + y + 1$, which is irreducible over $\mathbb{F}_\phi$. Thus, $2\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2^4$ with $f_1 = 2$ and $f_2 = 1$. Hence, $\nu_2(i(K)) = 0$.

(b) If $(a,b) \equiv (0,15) \pmod{16}$, then we have two cases:

(b_1) If $(a,b) \in \{(0,15),(16,31)\} \pmod{32}$, then $N_\phi(F) = S_1 + S_2 + S_3$ has three sides joining $(0,4)$, $(2,2)$, $(4,1)$, and $(8,0)$ with $d(S_2) = d(S_3) = 1$ and $R_{1_1}(F)(y) = y^2 + y + 1$, which is irreducible over $\mathbb{F}_\phi$. Thus, $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^4$ with $f_1 = 2$ and $f_2 = f_3 = 1$. Hence, $\nu_2(i(K)) = 0$.

(b_2) If $(a,b) \in \{(16,15),(0,31)\} \pmod{32}$, then $N_\phi(F) = S_1 + S_2 + S_3 + S_4$ has four sides joining $(0,w)$, $(1,3)$, $(2,2)$, $(4,1)$, and $(8,0)$ wit $w \geq 5$. Thus, the degree of each side is 1, and so $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_4^4$ with residue degree 1 each ideal factor. Hence, 2 divides $i(K)$.

(c) If $(a,b) \equiv (8,7) \pmod{16}$, then $\nu_2(\Delta) \geq 28$. Let $a_2 = \dfrac{a}{8}$ and $u = \dfrac{-b^2}{75a_2^3} \in \mathbb{Q}$. Since $\nu_2(75a_2^3) = 0$, then $u \in \mathbb{Z}_2$. Let $\phi = x - u$. Then $F(x) = \phi^8 + 8u\phi^7 + 28u^2\phi^6 + 56u^3\phi^5 + 70u^4\phi^4 + (56u^5 + a)\phi^3 + (28u^6 + 3au)\phi^2 + A\phi + B$ with

$$A = 8u^7 + 3au^2 = \frac{\Delta^2}{2^{45} \cdot 3^7 \cdot 5^{14} a_2^{21}} - \frac{b^7\Delta}{2^{20} \cdot 3^7 \cdot 5^{14} a_2^{21}}$$

and

$$B = u^8 + au^3 + b = \frac{-\Delta^3}{2^{72} \cdot 3^9 \cdot 5^{15} a_2^{24} b^5} + \frac{7b^2\Delta^2}{2^{48} \cdot 3^9 \cdot 5^{16} a_2^{24}} + \frac{b^9\Delta}{2^{24} \cdot 3^9 \cdot 5^{16} a_2^{24}}.$$

Thus, $\nu_2(A) = \nu_2(\Delta) - 20$ and $\nu_2(B) = \nu_2(\Delta) - 24$. Hence, $N_\phi(F) = S_1 + S_2 + S_3$ has three sides joining $(0, \nu_2(\Delta) - 24)$, $(2,2)$, $(4,1)$, and $(8,0)$ with $d(S_2) = d(S_3) = 1$. It follows that if $\nu_2(\Delta)$ is odd, then $d(S_1) = 1$, and so $2\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^4$ with residue degree 1 each ideal factor. Hence, 2 divides $i(K)$. Applying [11, Theorem 6], we get $\nu_2(i(K)) = 2$. If $\nu_2(\Delta) = 2k + 26$ $(k \geq 1)$ is even, then $d(S_1) = 2$ with $R_{1_1}(F)(y) = (y+1)^2 \in \mathbb{F}_\phi[y]$. Let us replace ϕ by $x - (u + 2^k)$. Then $F(x) = (x - (u+2^k))^8 + \sum_{l=0}^{7} A_l(x - (u+2^k))^l$ with $\nu_2(A_4) = 1$, $\nu_2(A_3) \geq 3$, $\nu_2(A_2) = 2$,

$$A_1 = A + 2^k(6au^2 + 56u^6) + 2^{2k}(3a + 168u^5) + 280u^4(2^{3k}) + 280u^3(2^{4k}) + 168u^2(2^{5k}) + 56u(2^{6k}) + 8(2^{7k}),$$

and

$$A_0 = B + 2^k A + (3au + 28u^6)(2^{2k}) + (a + 56u^5)(2^{3k}) + 70u^4(2^{4k}) + 56u^3(2^{5k}) + 28u^2(2^{6k}) + 8u(2^{7k}) + 2^{8k}.$$

Obviously, $\nu_2(A_1) = k + 3$.

For $\nu_2(\Delta) = 28,\ k = 1$, we have

$$A_0 \equiv 2^4\left(\frac{b^9\Delta_2}{35a_2^{24}} + 6a_2u + 7u^6 + 70u^4\right) \pmod{128},$$

$$\equiv \frac{2^4}{a_2^{24}}(11b^9\Delta_2 - 10a_2^{22}b^2 + 95a_2^6b^{12} + 102a_2^{12}b^8) \pmod{128}.$$

Since $11b^9\Delta_2 - 10a_2^{22}b^2 + 95a_2^6b^{12} + 102a_2^{12}b^8 \equiv 5\Delta_2 + 3 \pmod 8$, three cases arise: If $\Delta_2 \equiv$ 3,7 (mod 8), then $\nu_2(A_0) = 5$. Thus, $N_{x-(u+2)}(F) = S_1 + S_2 + S_3$ has three sides joining (0,5), (2,2), (4,1), and (8,0). It follows that $2\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^4$ with residue degree 1 each ideal factor. Hence, 2 divides $i(K)$. Applying [11, Theorem 6], we get $\nu_2(i(K)) = 2$.

If $\Delta_2 \equiv 5 \pmod 8$, then $\nu_2(A_0) = 6$. Thus, $N_{x-(u+2)}(F) = S_1 + S_2 + S_3$ has three sides joining (0,6), (2,2), (4,1), and (8,0) with $d(S_2) = d(S_3) = 1$ and $R_{1_1}(F)(y) = y^2 + y + 1$, which is irreducible over $\mathbb{F}_{x-(u+2)}$. It follows that $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^4$ with $f_1 = 2$ and $f_2 = f_3 = 1$. Hence, $\nu_2(i(K)) = 0$.

If $\Delta_2 \equiv 1 \pmod 8$, then $\nu_2(A_0) \geq 7$. Thus, $N_{x-(u+2)}(F) = S_1 + S_2 + S_3 + S_4$ has four sides joining $(0, w)$, $(1, 4)$, $(2, 2)$, $(4, 1)$, and $(8, 0)$ with $w \geq 7$. It follows that $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_4^4$ with residue degree 1 each ideal factor. Hence, 2 divides $i(K)$.

For $\nu_2(\Delta) \geq 30,\ k \geq 2$, we have

$$A_0 \equiv \frac{2^{2k+2}b^9\Delta_2}{3^9 \cdot 5^{16}a^{24_2}} + (3au + 28u^6)(2^{2k}) \pmod{2^{2k+5}},$$

$$\equiv \frac{2^{2k+2}}{3^9 \cdot 5^{16}a_2^{24}}(b^9\Delta_2 - 2 \cdot 3^9 \cdot 5^{16}a_2^{22}b^2 + 3^3 \cdot 5^4 \cdot 7a_2^6b^{12}) \pmod{2^{2k+5}}.$$

Since $b^9\Delta_2 - 2 \cdot 3^9 \cdot 5^{16}a_2^{22}b^2 + 3^3 \cdot 5^4 \cdot 7a_2^6b^{12} \equiv 7\Delta_2 + 7 \pmod 8$, three cases arise:

If $\Delta_2 \equiv 1, 5 \pmod 8$, then $\nu_2(A_0) = 2k + 3$. Thus, $N_{x-(u+2)}(F) = S_1 + S_2 + S_3$ has three sides joining $(0, 2k+3)$, $(2, 2)$, $(4, 1)$, and $(8, 0)$. It follows that $2\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^4$ with residue degree 1 each ideal factor. Hence, 2 divides $i(K)$. Applying [11, Theorem 6], we get $\nu_2(i(K)) = 2$.

If $\Delta_2 \equiv 3 \pmod 8$, then $\nu_2(A_0) = 2k + 4$. Thus, $N_{x-(u+2)}(F) = S_1 + S_2 + S_3$ has three sides joining $(0, 6)$, $(2, 2)$, $(4, 1)$, and $(8, 0)$ with $d(S_2) = d(S_3) = 1$ and $R_{1_1}(F)(y) = y^2 + y + 1$, which is irreducible over $\mathbb{F}_{x-(u+2)}$. It follows that $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^4$ with $f_1 = 2$ and $f_2 = f_3 = 1$. Hence, $\nu_2(i(K)) = 0$.

If $\Delta_2 \equiv 7 \pmod 8$, then $\nu_2(A_0) \geq 2k + 5$. Thus, $N_{x-(u+2)}(F) = S_1 + S_2 + S_3 + S_4$ has four sides joining $(0, w)$, $(1, k + 3)$, $(2, 2)$, $(4, 1)$, and $(8, 0)$ with $w \geq 2k + 5$. It follows that $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_4^4$ with residue degree 1 each ideal factor. Hence, 2 divides $i(K)$.

(3) If $\nu_2(a) \geq 1$ and $\nu_2(b) \geq 1$, then $F(x) \equiv x^8 \pmod 2$. Let $\phi = x$. By assumption, $\nu_2(a) \leq 4$ or $\nu_2(b) \leq 7$.

If $\nu_2(b) > \dfrac{8}{5}\nu_2(a)$, then $N_\phi(F) = S_1 + S_2$ has two sides joining $(0, \nu_2(b))$, $(3, \nu_2(a))$, and $(8, 0)$ with $d(S_2) = 1$ since $\nu_2(a) \leq 4$ by assumption.

(i) If $\nu_2(b) \not\equiv \nu_2(a) \pmod 3$, then $d(S_1) = 1$, and so $2\mathbb{Z}_K = \mathfrak{p}_1^3\mathfrak{p}_2^5$ with residue degree 1 each ideal factor. Hence, $\nu_2(i(K)) = 0$.

(ii) If $\nu_2(b) \equiv \nu_2(a) \pmod 3$, then $d(S_1) = 3$ with $R_{1_1}(F)(y) = y^3+1 = (y+1)(y^2+y+1) \in \mathbb{F}_\phi[y]$. Thus, $2\mathbb{Z}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}\mathfrak{p}_{21}^5$ with $f_{11} = f_{21} = 1$ and $f_{12} = 2$. Hence, $\nu_2(i(K)) = 0$.

If $\nu_2(b) < \dfrac{8}{5}\nu_2(a)$, then $N_\phi(F) = S_1$ has a single side joining $(0, \nu_2(b))$ and $(8, 0)$ with $d(S_1) \in \{1, 2, 4\}$ since $\nu_2(b) \leq 7$ by assumption. Let $d = d(S_1)$, then we have the following cases:

(i) If $d = 1$, $\nu_2(b) \in \{1, 3, 5, 7\}$, then $R_1(F)(y)$ is irreducible as it is of degree 1. Thus, $2\mathbb{Z}_K = \mathfrak{p}_1^8$ with residue degree 1. Hence, $\nu_2(i(K)) = 0$.

(ii) If $d = 2$, $\nu_2(b) \in \{2, 6\}$, then $R_1(F)(y) = (y+1)^2 \in \mathbb{F}_\phi[y]$. Since $-\lambda_1 \in \{-1/4, -3/4\}$ is the slope of S_1, then $e_1 = 4$ divides the ramification index of any prime ideal of $\mathbb{Z}_K$ lying above 2. Thus, the possible decompositions of $2\mathbb{Z}_K$ are: $\mathfrak{p}_1^8$ with $f_1 = 1$ or $\mathfrak{p}_1^4$ with $f_1 = 2$ or $\mathfrak{p}_1^4\mathfrak{p}_2^4$ with $f_1 = f_2 = 1$. In each case, $\nu_2(i(K)) = 0$.

(iii) If $d = 4$, $b \equiv 16 \pmod{32}$ and $a \equiv 0 \pmod 8$, then $R_1(F)(y) = (y+1)^4 \in \mathbb{F}_\phi[y]$. In this case, we have to use second order Newton polygon. Let $\omega_2 = 2[\nu_2, \phi, 1/2]$ be the valuation of second order Newton polygon and $g_2 = x^2 - 2$ the key polynomial of ω_2, where $[\nu_2, \phi, 1/2]$ is the augmented valuation of ν_2 with respect to ϕ and $\lambda_1 = 1/2$. Let $F(x) = g_2^4 + 8g_2^3 + 24g_2^2 + (x + a + 32)g_2 + (2ax + b + 16)$. Then $\omega_2(x) = 1$, $\omega_2(g_2) = 2$, and $\omega_2(m) = 2 \cdot \nu_2(m)$ for every $m \in \mathbb{Q}_2$.

(a) If $a \equiv 8 \pmod{16}$, then $N_2(F) = T_1$ has a single side joining $(0, 9)$ and $(4, 8)$. Thus, the degree of T_1 is 1, and so $2\mathbb{Z}_K = \mathfrak{p}_1^8$ with residue degree 1. Hence, $\nu_2(i(K)) = 0$.

(b) If $b \equiv 16 \pmod{64}$, then $N_2(F) = T_1$ has a single side joining $(0, 10)$ and $(4, 8)$ with $R_2(F)(y) = (y+1)^2 \in \mathbb{F}_2[y]$. Since $-\lambda_1' = -1/2$ is the slope of T_1 and $-\lambda_1 = -1/2$ is the slope of S_1, then $e_1e_1' = 4$ divides the ramification index of any prime ideal $\mathbb{Z}_K$ lying above 2. Thus, the possible decompositions of $2\mathbb{Z}_K$ are: $\mathfrak{p}_1^8$ with $f_1 = 1$ or $\mathfrak{p}_1^4$ with $f_1 = 2$ or $\mathfrak{p}_1^4\mathfrak{p}_2^4$ with $f_1 = f_2 = 1$. In each case, $\nu_2(i(K)) = 0$.

(c) If $a \equiv 16 \pmod{32}$ and $b \equiv 48 \pmod{64}$, then $N_2(F) = T_1$ has a single side joining $(0, 11)$ and $(4, 8)$. Thus, $2\mathbb{Z}_K = \mathfrak{p}_1^8$ with residue degree 1. Hence, $\nu_2(i(K)) = 0$.

(d) If $a \equiv 0 \pmod{32}$ and $b \equiv 48 \pmod{128}$, then $N_2(F) = T_1$ has a single side joining $(0, 12)$ and $(4, 8)$ with $R_2(F)(y) = y^4+y^2+1 = (y^2+y+1)^2 \in \mathbb{F}_2[y]$. In this case, we have to use third order Newton polygon. Let $\omega_3 = 1[\omega_2, g_2, 1]$ be the valuation of third order Newton polygon and $g_3 = x^4 - 2x^3 - 4x^2 + 4x - 4$ the key polynomial of ω_3, where $[\omega_2, g_2, 1]$ is the augmented valuation of ω_2 with respect to g_2 and $\lambda_1' = 1$. Let $F(x) = g_3^2 + ((4x + 12)g_2 + 96 + 24x)g_3 + ((a + 192)x + 224)g_2 + (192 + 2a)x + b + 720$. Then $\omega_3(x) = 1$, $\omega_3(g_2) = 3$, $\omega_3(g_3) = 6$, and $\omega_3(m) = 2 \cdot \nu_2(m)$ for every $m \in \mathbb{Q}_2$. It follows that $N_3(F) = T_1$ has a single side joining $(0, 13)$ and $(2, 12)$, and so $2\mathbb{Z}_K = \mathfrak{p}_1^4$ with residue degree 2. Hence, $\nu_2(i(K)) = 0$.

(e) If $a \equiv 32 \pmod{64}$ and $b \equiv 112 \pmod{128}$, then $N_2(F) = T_1 + T_2$ has two sides joining $(0, 13)$, $(2, 10)$, and $(4, 8)$ with $d(T_1) = 1$ and $R_{2_2}(F)(y) = (y+1)^2 \in \mathbb{F}_2[y]$. In this case, we have to use third order Newton polygon. Let $\omega_3 = 1[\omega_2, g_2, 1]$ be the valuation of third order Newton polygon and $g_3 = x^2 - 2x - 2$ the key polynomial of ω_3, where $[\omega_2, g_2, 1]$ is the augmented valuation of ω_2 with respect to g_2 and $\lambda_2' = 1$. Let $F(x) = g_3^4 + (32 + 8x)g_3^3 + (248 + 128x)g_3^2 + ((a + 608)x +$

$704+2a)g_3+(6a+896)x+b+656+4a$. Then $\omega_3(x)=1$, $\omega_3(g_3)=3$, and $\omega_3(m)=2\cdot\nu_2(m)$ for every $m\in\mathbb{Q}_2$. It follows that $N_3^+(F)=T_1$ has a single side joining $(0,13)$ and $(2,12)$, and so $2\mathbb{Z}_K=\mathfrak{p}_1^4\mathfrak{p}_2^4$ with residue degree 1 each ideal factor. Hence, $\nu_2(i(K))=0$.

(f) If $a\equiv 0\pmod{64}$ and $b\equiv 112\pmod{256}$, then $N_2(F)=T_1+T_2$ has two sides joining $(0,14)$, $(2,10)$, and $(4,8)$ with $R_{2_1}(F)(y)=y^2+y+1$, which is irreducible over $\mathbb{F}_2$. On the other hand, $R_{2_2}(F)(y)=(y+1)^2\in\mathbb{F}_2[y]$. In this case, we have to use third order Newton polygon. Let $\omega_3=1[\omega_2,g_2,1]$ be the valuation of third order Newton polygon and $g_3=x^2-2x-2$ the key polynomial of ω_3, where $[\omega_2,g_2,1]$ is the augmented valuation of ω_2 with respect to g_2 and $\lambda_2'=1$. Let $F(x)=g_3^4+(32+8x)g_3^3+(248+128x)g_3^2+((a+608)x+704+2a)g_3+(6a+896)x+b+656+4a$. Then $\omega_3(x)=1$, $\omega_3(g_3)=3$, and $\omega_3(m)=2\cdot\nu_2(m)$ for every $m\in\mathbb{Q}_2$.

(f_1) If $a\equiv 0\pmod{128}$, then $N_3^+(F)=T_1'$ has a single side joining $(0,15)$ and $(2,12)$. It follows that $2\mathbb{Z}_K=\mathfrak{p}_1^2\mathfrak{p}_2^4$ with $f_1=2$ and $f_2=1$. Hence, $\nu_2(i(K))=0$.

(f_2) If $a\equiv 64\pmod{128}$ and $b\equiv 112\pmod{512}$, then $N_3^+(F)=T_1'+T_2'$ has two sides joining $(0,w)$, $(1,14)$, and $(2,12)$ with $w\geq 18$. It follows that $2\mathbb{Z}_K=\mathfrak{p}_{11}^2\mathfrak{p}_{21}^2\mathfrak{p}_{22}^2$ with $f_{11}=2$ and $f_{21}=f_{22}=1$. Hence, $\nu_2(i(K))=0$.

(f_3) If $a\equiv 64\pmod{128}$ and $b\equiv 368\pmod{512}$, then $N_3^+(F)=T_1'$ has a single side joining $(0,16)$ and $(2,12)$ with $R_3(F)(y)=y^2+y+1$, which is irreducible over $\mathbb{F}_3$. It follows that $2\mathbb{Z}_K=\mathfrak{p}_1^2\mathfrak{p}_2^2$ with residue degree 2 each ideal factor. Hence, 2 divides $i(K)$.

(g) If $a\equiv 0\pmod{64}$ and $b\equiv 240\pmod{256}$, then $N_2(F)=T_1+T_2+T_3$ has three sides joining $(0,w)$, $(1,12)$, $(2,10)$, and $(4,8)$ with $w\geq 15$, $d(T_1)=d(T_2)=1$ and $R_{2_3}(F)(y)=(y+1)^2\in\mathbb{F}_2[y]$. In this case, we have to use third order Newton polygon. Let $\omega_3=1[\omega_2,g_2,1]$ be the valuation of third order Newton polygon and $g_3=x^2-2x-6$ the key polynomial of ω_3, where $[\omega_2,g_2,1]$ is the augmented valuation of ω_2 with respect to g_2 and $\lambda_2'=1$. Let $F(x)=g_3^4+(48+8x)g_3^3+(728+224x)g_3^2+((a+2016)x+4480+2a)g_3+(10a+5888)x+b+9744+12a$. Then $\omega_3(x)=1$, $\omega_3(g_3)=3$, and $\omega_3(m)=2\cdot\nu_2(m)$ for every $m\in\mathbb{Q}_2$.

(g_1) If $a\equiv 64\pmod{128}$, then $N_3^+(F)=T_1'$ has a single side joining $(0,15)$ and $(2,12)$. It follows that $2\mathbb{Z}_K=\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^4$ with residue degree 1 each ideal factor. Hence 2 divides $i(K)$. Applying [11, Theorem 6], we get $\nu_2(i(K))=2$.

(g_2) If $a\equiv 0\pmod{128}$ and $b\equiv 240\pmod{512}$, then $N_3^+(F)=T_1'$ has a single side joining $(0,16)$ and $(2,14)$ with $R_3(F)(y)=y^2+y+1$ which is irreducible over $\mathbb{F}_3$. It follows that $2\mathbb{Z}_K=\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$ with $f_1=f_2=1$ and $f_2=2$. Hence, $\nu_2(i(K))=0$.

(g_3) If $a\equiv 0\pmod{128}$ and $b\equiv 496\pmod{512}$, then $N_3^+(F)=T_1'+T_2'$ has two sides joining $(0,w)$, $(1,1)$, and $(2,14)$ with $w\geq 18$. It follows that $2\mathbb{Z}_K=\mathfrak{p}_{11}^2\mathfrak{p}_{21}^2\mathfrak{p}_{31}^2\mathfrak{p}_{32}^2$ with residue degree 1 each ideal factor. Hence, 2 divides $i(K)$.

Theorem 2.1 is proved.

***Proof of Theorem* 2.2.** If $\nu_3(b)=0$, then since $\Delta=-b^2(3^3\cdot 5^5a^8-2^{24}b^5)$ is the discriminant of $F(x)$, thanks to the index formula (1.1), $\nu_3((\mathbb{Z}_K:\mathbb{Z}[\alpha]))=0$, and so $\nu_3(i(K))=0$. Now assume that 3 divides b. Then we have the following cases:

(1) If $a\equiv -1\pmod 3$, then $F(x)\equiv x^3(x-1)(x^4+x^3+x^2+x+1)\pmod 3$. Thus, there are two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 and 4 provided by $x-1$ and $x^4+x^3+x^2+x+1$, respectively. On the other hand, let $\phi=x$. Then $N_\phi^+(F)=S_1$ has a single side joining $(0,\nu_3(b))$ and $(3,0)$.

(i) If $\nu_3(b)\not\equiv 0\pmod 3$, then $d(S_1)=1$, and so its attached residual polynomial is irreducible. It follows that $3\mathbb{Z}_K=\mathfrak{p}_1^3\mathfrak{p}_2\mathfrak{p}_3$ with $f_1=f_2=1$ and $f_3=4$. Hence, $\nu_3(i(K))=0$.

(ii) If $\nu_3(b) = 3k$ for some positive integer k, then $d(S_3) = 3$ with $R_1(F)(y) = -y^3 + b_3 = -(y - b_3)^3 \in \mathbb{F}_\phi[y]$. Let us replace ϕ by $x - 3^k b_3$. Then $F(x) = \ldots + A_3(x - 3^k b_3)^3 + A_2(x - 3^k b_3)^2 + A_1(x - 3^k b_3) + A_0$ with $\nu_3(A_3) = 0$,

$$A_0 = b + 3^{3k} a b_3^3 + 3^{8k} b_3^8,$$

$$A_1 = 3^{2k+1} a b_3^2 + 8 \cdot 3^{7k} b_3^7,$$

and

$$A_2 = 28 \cdot 3^{6k} b_3^6 + 3^{k+1} a b_3.$$

Obviously, $\nu_3(A_2) = k + 1$, $\nu_3(A_1) = 2k + 1$, and $\nu_3(A_0) \geq 3k + 1$.

(a) If $\nu_3(A_0) = 3k + 1$, then $N^+_{x-3^k b_3}(F) = S_1$ has a single side joining $(0, 3k + 1)$ and $(3, 0)$. Thus, $3\mathbb{Z}_K = \mathfrak{p}_1^3 \mathfrak{p}_2 \mathfrak{p}_3$ with $f_1 = f_2 = 1$ and $f_3 = 4$. Hence, $\nu_3(i(K)) = 0$.

(b) If $\nu_3(A_0) \geq 3k+2$, then $N^+_{x-3^k b_3}(F) = S_1 + S_2$ has two sides joining $(0, w)$, $(1, 2k+1)$, and $(3, 0)$. Thus, $3\mathbb{Z}_K = \mathfrak{p}_{11} \mathfrak{p}_{12}^2 \mathfrak{p}_{21} \mathfrak{p}_{31}$ with $f_{11} = f_{12} = f_{21} = 1$ and $f_{31} = 4$. Hence, $\nu_3(i(K)) = 0$.

(2) If $a \equiv 1 \pmod 3$, then $F(x) \equiv x^3(x + 1)(x^4 + 2x^3 + x^2 + 2x + 1) \pmod 3$. The treatment of this case is similar to the case $a \equiv -1 \pmod 3$ above, and we get $\nu_3(i(K)) = 0$.

(3) If $\nu_3(a) \geq 1$, then $F(x) \equiv x^8 \pmod 3$. Let $\phi = x$. By assumption, $\nu_3(a) \leq 4$ or $\nu_3(b) \leq 7$. If $\nu_3(b) > \dfrac{8}{5}\nu_3(a)$, then $N_\phi(F) = S_1 + S_2$ has two sides joining $(0, \nu_3(b))$, $(3, \nu_3(a))$, and $(8, 0)$ with $d(S_2) = 1$ since $\nu_3(a) \leq 4$ by assumption.

(i) If $\nu_3(b) \not\equiv \nu_3(a) \pmod 3$, then $d(S_1) = 1$, and so $3\mathbb{Z}_K = \mathfrak{p}_1^3 \mathfrak{p}_2^5$ with residue degree 1 each ideal factor. Hence, $\nu_3(i(K)) = 0$.

(ii) If $\nu_3(b) = 3k + \nu_3(a)$, then $d(S_1) = 3$ with $R_{1_1}(F)(y) = a_3 y^3 + b_3 = (y + a_3 b_3)^3 \in \mathbb{F}_\phi[y]$. Let us replace ϕ by $x + 3^k u$, where $u = a_3 b_3$. Then $F(x) = (x + 3^k u)^8 + \sum_{l=1}^{7} A_0 (x + 3^k u)^l$ with $\nu_3(A_7) = k$, $\nu_3(A_6) = 2k$, $\nu_3(A_5) = 3k$, $\nu_3(A_4) = 4k$, $\nu_3(A_3) = \nu_3(a)$,

$$A_2 = 28 \cdot 3^{6k} u^6 - 3^{k+1} a u,$$

$$A_1 = 3^{2k+1} a u^2 - 8 \cdot 3^{7k} u^7,$$

and

$$A_0 = b - 3^{3k} a u^3 + 3^{8k} u^8.$$

(a) If $k \geq 1$ or $\nu_3(a) \leq 3$, then $\nu_3(A_2) = k + \nu_3(a) + 1$, $\nu_3(A_1) = 2k + \nu_3(a) + 1$, and $\nu_3(A_0) \geq 3k + \nu_3(a) + 1$. It follows that:

(a$_1$) If $\nu_3(A_0) = 3k + \nu_3(a) + 1$, then $N_{x+3^k u}(F) = S_1 + S_2$ has two sides joining $(0, 3k + \nu_3(a)+1)$, $(3, \nu_3(a))$, and $(8, 0)$. It follows that $3\mathbb{Z}_K = \mathfrak{p}_1^3 \mathfrak{p}_2^5$ with residue degree 1 each ideal factor. Hence, $\nu_3(i(K)) = 0$.

(a$_2$) If $\nu_3(A_0) \geq 3k + \nu_3(a) + 2$, then $N_{x+3^k u}(F) = S_1 + S_2 + S_3$ has three sides joining $(0, \nu_3(A_0))$, $(1, 2k + \nu_3(a) + 1)$ $(3, \nu_3(a))$, and $(8, 0)$. It follows that $3\mathbb{Z}_K = \mathfrak{p}_1 \mathfrak{p}_2^2 \mathfrak{p}_3^5$ with residue degree 1 each ideal factor. Hence, $\nu_3(i(K)) = 0$.

(b) If $k = 1$ and $\nu_3(a) = 4$, then $\nu_3(b) = 7$, $\nu_3(A_3) = 4$,

$$A_2 = 28 \cdot 3^6 u^6 - 3^2 au = 3^6(28u^6 + a_3 u),$$
$$A_1 = 3^3 au^2 - 8 \cdot 3^7 u^7 = 3^7(a_3 u^2 - 8u^7),$$

and

$$A_0 = b - 3^3 au^3 + 3^8 u^8 = 3^7(b_3 - a_3 u^3 + 3u^8).$$

Obviously, $\nu_3(A_0) \geq 8$, $\nu_3(A_1) \geq 7$, and $\nu_3(A_2) \geq 6$. If $b_3 \equiv 1 \pmod 3$; $b \equiv 3^7 \pmod{3^8}$, then

$$A_2/3^6 \equiv 28a_3^6 b_3^6 + a_3^2 b_3 \pmod 3 \equiv 2 \pmod 3,$$
$$A_1/3^7 \equiv a_3^3 - 8a_3^7 b_3^7 \equiv 2 \pmod 3.$$

Hence, $\nu_3(A_1) = 7$ and $\nu_3(A_2) = 6$. If $\nu_3(A_0) = 8$, then $N_{x+3u}(F) = S_1 + S_2$ has two sides joining $(0, 8)$, $(3, 4)$, and $(8, 0)$. Thus, $3\mathbb{Z}_K = \mathfrak{p}_1^3 \mathfrak{p}_2^5$ with residue degree 1 each ideal factor. Hence, $\nu_3(i(K)) = 0$. If $\nu_3(A_0) \geq 9$, then $N_{x+3u}(F) = S_1 + S_2 + S_3$ has three sides joining $(0, \nu_3(A_0))$, $(1, 7)$, $(3, 4)$, and $(8, 0)$. Thus, $3\mathbb{Z}_K = \mathfrak{p}_1 \mathfrak{p}_2^2 \mathfrak{p}_3^5$ with residue degree 1 each ideal factor. Hence, $\nu_3(i(K)) = 0$. If $b_3 \equiv 1 \pmod 3$, $b \equiv 4374 \pmod{3^8}$, then $\nu_3(\Delta) \geq 50$. Let $v = \dfrac{-2^9 \cdot 3b_3^2}{5^2 a_3^3}$. Since $\nu_3(5^2 a_3^3)$, then $v \in \mathbb{Z}_3$. Let us replace $x - 3u$ by $g = x - v$. Then $F(x) = g^8 + 8vg^7 + 28v^2 g^6 + 56v^3 g^5 + 70v^4 g^4 + (56v^5 + a)g^3 + A'g^2 + B'g + C'$ with

$$A' = 28v^6 + 3av = \frac{-2^9 \Delta^2}{3^{92} \cdot 5^{12} a_3^{18} b_3^2} + \frac{2^{34} b_3^5 \Delta}{3^{43} \cdot 5^{12} a_3^{18}} + \frac{2^{56} \cdot 3^6 \cdot 5 b_3^{12}}{5^{12} a_3^{18}},$$

$$B' = 8v^7 + 3av^2 = \frac{2^{18} \Delta^2}{3^{91} \cdot 5^{14} a_3^{21}} - \frac{2^{43} b_3^7 \Delta}{3^{42} \cdot 5^{14} a_3^{21}},$$

and

$$C' = v^8 + av^3 + b = \frac{-\Delta^3}{3^{140} \cdot 5^{15} a_3^{24} b_3^5} + \frac{2^{24} \cdot 7 b_3^2 \Delta^2}{3^{91} \cdot 5^{16} a_3^{24}} + \frac{2^{48} b_3^9 \Delta}{3^{42} \cdot 5^{16} a_3^{24}}.$$

Thus, $\nu_3(C') = \nu_3(B') = \nu_3(\Delta) - 42$ and $\nu_3(A') = 6$. Then we have the following cases:

(b_1) If $\nu_3(\Delta) = 50$ (resp., $\nu_3(\Delta) = 51$), then $N_g(F) = S_1 + S_2$ has two sides joining $(0, 8)$ (resp., $(0, 9)$), $(3, 4)$, and $(8, 0)$. Thus, the degree of each side is 1, and so $3\mathbb{Z}_K = \mathfrak{p}_1^3 \mathfrak{p}_2^5$ with residue degree 1 each ideal factor. Hence, $\nu_3(i(K)) = 0$.

(b_2) If $\nu_3(\Delta) = 52$, then $N_g(F) = S_1 + S_2$ has two sides joining $(0, 10)$, $(3, 4)$, and $(8, 0)$ with $d(S_2) = 1$ and $R_{\lambda_{1_1}}(F)(y) = a_3 y^3 - y^2 + C_3'$ (since $A_3' \equiv -1 \pmod 3$), which is separable but does not split completely over $\mathbb{F}_g$. Thus, the possible decompositions of $3\mathbb{Z}_K$ are $\mathfrak{p}_1 \mathfrak{p}_2^5$ with $f_1 = 3$ and $f_2 = 1$, or $\mathfrak{p}_{11} \mathfrak{p}_{12} \mathfrak{p}_{21}^5$ with $f_{11} = f_{21} = 1$ and $f_{12} = 2$. In both cases, $\nu_3(i(K)) = 0$.

(b_3) If $\nu_3(\Delta) \geq 53$ and $\nu_3(\Delta)$ is odd, then $N_g(F) = S_1 + S_2 + S_3$ has three sides joining $(0, \nu_3(\Delta) - 42)$, $(2, 6)$, $(3, 4)$, and $(8, 0)$. Thus, the degree of each side is 1, and so $3\mathbb{Z}_K = \mathfrak{p}_1^2 \mathfrak{p}_2 \mathfrak{p}_3^5$ with residue degree 1 each ideal factor. Hence, $\nu_3(i(K)) = 0$.

(b_4) If $\nu_3(\Delta) \geq 53$ and $\nu_3(\Delta)$ is even, then $N_g(F) = S_1 + S_2 + S_3$ has three sides joining $(0, \nu_3(\Delta) - 42)$, $(2, 6)$, $(3, 4)$, and $(8, 0)$ with $d(S_2) = d(S_3) = 1$ and $R_{1_1}(F)(y) = -y^2 + C_3' \in \mathbb{F}_g[y]$. Since $C_3' \equiv -\Delta_3 \pmod 3$, then two cases arises:

If $\Delta_3 \equiv 1 \pmod 3$, then $R_{1_1}(F)(y) = -y^2 - 1$, which is irreducible over $\mathbb{F}_g$. Thus, $3\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^5$ with $f_1 = 2$ and $f_2 = f_3 = 1$. Hence, $\nu_3(i(K)) = 0$.

If $\Delta_3 \equiv -1 \pmod 3$, then $R_{1_1}(F)(y) = -y^2 + 1 = -(y-1)(y+1) \in \mathbb{F}_g[y]$. Thus, $3\mathbb{Z}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}\mathfrak{p}_{21}\mathfrak{p}_{31}^5$ with residue degree 1 each ideal factor. Hence, 3 divides $i(K)$. Applying [11, p. 230, Corollary], we get $\nu_3(i(K)) = 1$.

If $\nu_3(b) < \frac{8}{5}\nu_3(a)$, then $N_\phi(F) = S_1$ has a single side joining $(0, \nu_3(b))$ and $(8, 0)$ with $d(S_1) \in \{1, 2, 4\}$ since $\nu_3(b) \le 7$ by assumption. Let $d = d(S_1)$, then we have the following cases:

(i) If $d = 1$, $\nu_3(b) \in \{1, 3, 5, 7\}$, then $R_1(F)(y)$ is irreducible as it is of degree 1. Thus, $3\mathbb{Z}_K = \mathfrak{p}_1^8$ with residue degree 1. Hence, $\nu_3(i(K)) = 0$.

(ii) If $d = 2$, $\nu_3(b) \in \{2, 6\}$, then $R_1(F)(y) = y^2 + b_3 \in \mathbb{F}_\phi[y]$. If $b_3 \equiv 1 \pmod 3$, then $R_1(F)(y)$ is irreducible over $\mathbb{F}_\phi$, and so $3\mathbb{Z}_K = \mathfrak{p}_1^4$ with residue degree 2. Hence, $\nu_3(i(K)) = 0$. If $b_3 \equiv -1 \pmod 3$, then $R_1(F)(y) = (y-1)(y+1) \in \mathbb{F}_\phi[y]$. Thus, $3\mathbb{Z}_K = \mathfrak{p}_{11}^4\mathfrak{p}_{12}^4$ with residue degree 1 each ideal factor. Hence, $\nu_3(i(K)) = 0$.

(iii) If $d = 4$, $\nu_3(b) = 4$, then $R_1(F)(y) = y^4 + b_3 \in \mathbb{F}_\phi[y]$. If $b_3 \equiv 1 \pmod 3$, then $R_1(F)(y) = (y^2 - y - 1)(y^2 + y - 1) \in \mathbb{F}_\phi[y]$, and so $3\mathbb{Z}_K = \mathfrak{p}_{11}^2\mathfrak{p}_{12}^2$ with residue degree 2 each ideal factor. Hence, $\nu_3(i(K)) = 0$. If $b_3 \equiv -1 \pmod 3$, then $R_1(F)(y) = (y-1)(y+1)(y^2+1) \in \mathbb{F}_\phi[y]$. Thus, $3\mathbb{Z}_K = \mathfrak{p}_{11}^2\mathfrak{p}_{12}^2\mathfrak{p}_{13}^2$ with $f_{11} = f_{12} = 1$ and $f_{13} = 2$. Hence, $\nu_3(i(K)) = 0$.

Theorem 2.2 is proved.

***Proof of Theorem* 2.3.** For $p = 5$. Since $\Delta = -b^2(3^3 \cdot 5^5 a^8 - 2^{24} b^5)$, if $\nu_5(b) = 0$, then $\nu_5((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$, and so $\nu_5(i(K)) = 0$. Now assume that 5 divides b. Then we have the following cases:

(1) If $\nu_5(a) = 0$, then $F(x) = x^3(x+a)^5 \pmod 5$. Let $\phi_1 = x$ and $\phi_2 = x + a$. Then

$$\begin{aligned} F(x) &= \phi_1^8 + a\phi_1^3 + b, \\ &= \cdots - 56a^3\phi_2^5 + (-56a^5 + a)\phi_2^4 + (28a^6 - 3a^2)\phi_2^3 + (3a^3 - 8a^7)\phi_2^2 + \phi_2 + b - a^4 + a^8. \end{aligned}$$

For ϕ_1, $N_{\phi_1}^+(F) = S_1$ has a single side joining $(0, \nu_5(b))$ and $(3, 0)$. If $\nu_5(b) \not\equiv 0 \pmod 3$, then $d(S_1) = 1$, and so ϕ_1 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 5 with residue degree 1. If $\nu_5(b) \equiv 0 \pmod 3$, then $d(S_1) = 3$ with $R_{1_1}(F)(y) = ay^3 + b_5 \in \mathbb{F}_{\phi_1}[y]$. One can check easily that, for every values of a and b_5 in $\mathbb{F}_{\phi_1}^*$, $ay^3 + b_5 \equiv \psi_1 \cdot \psi_2 \pmod{(5, \phi_1)}$ with $\deg(\psi_1) = 1$, $\deg(\psi_2) = 2$, ψ_1 and ψ_2 are coprime irreducible polynomials over $\mathbb{F}_{\phi_1}$. Thus, ϕ_1 provides two prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degrees 1 and 2, respectively. For ϕ_2, we have the following cases:

(i) If $\nu_5(b - a^4 + a^8) = 1$, then $N_{\phi_2}^+(F) = S_2$ has a single side of height 1. Thus, ϕ_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 5 with residue degree 1.

(ii) If $\nu_5(b - a^4 + a^8) \ge 2$ and $\nu_5(3a^3 - 8a^7) = 1$, then $N_{\phi_2}^+(F) = S_{21} + S_{22}$ has two sides of degree 1 each side. Thus, ϕ_2 provides two prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each ideal factor.

(iii) If $\nu_5(b - a^4 + a^8) \ge 2$ and $\nu_5(3a^3 - 8a^7) \ge 2$, then one can check easily that $\nu_5(3a^3 - 8a^7) \ge 2$ if and only if $a \in \{2, 11, 14, 23\} \pmod{25}$. But for these values, we have $\nu_5(3a^3 - 8a^7) = 1$. It follows that $N_{\phi_2}^+(F) = \ldots + S'$ such that the side S' join the points $(2, 1)$ and $(5, 0)$ with slope $-\lambda' = -1/3$. In this case, ϕ_2 can provide at most three prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each ideal factor.

We conclude that there are at most four prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each ideal factor. Hence, $\nu_5(i(K)) = 0$.

(2) If $\nu_5(a) \geq 1$, then $F(x) \equiv x^8 \pmod 5$. Let $\phi = x$. By assumption, $\nu_5(a) \leq 4$ or $\nu_5(b) \leq 7$. If $\nu_5(b) > \dfrac{8}{5}\nu_5(a)$, then $N_\phi(F) = S_1 + S_2$ has two sides joining $(0, \nu_5(b))$, $(3, \nu_5(a))$, and $(8, 0)$ with $d(S_2) = 1$ since $\nu_5(a) \leq 4$ by assumption.

(i) If $\nu_5(b) \not\equiv \nu_5(a) \pmod 3$, then $d(S_1) = 1$, and so $5\mathbb{Z}_K = \mathfrak{p}_1^3\mathfrak{p}_2^5$ with residue degree 1 each ideal factor. Hence, $\nu_5(i(K)) = 0$.

(ii) If $\nu_5(b) \equiv \nu_5(a) \pmod 3$, then $d(S_1) = 3$ with $R_{1_1}(F)(y) = a_5y^3 + b_5 = \psi_1 \cdot \psi_2 \in \mathbb{F}_\phi[y]$ with, for every values of a_5 and b_5 in $\mathbb{F}_{\phi_1}^*$, $\deg(\psi_1) = 1$, $\deg(\psi_2) = 2$, ψ_1 and ψ_2 are coprime irreducible polynomials over $\mathbb{F}_{\phi_1}$. Thus, $5\mathbb{Z}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}\mathfrak{p}_{21}^5$ with $f_{11} = f_{21} = 1$ and $f_{12} = 2$. Hence, $\nu_5(i(K)) = 0$.

If $\nu_5(b) < \dfrac{8}{5}\nu_5(a)$, then $N_\phi(F) = S_1$ has a single side $(0, \nu_5(b))$ and $(8, 0)$ with $d(S_1) \in \{1, 2, 4\}$ since $\nu_5(b) \leq 7$ by assumption. Thus, there are at most four prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each ideal factor. Hence, $\nu_5(i(K)) = 0$.

For $p = 7$. Since $\Delta = -b^2(3^3 \cdot 5^5a^8 - 2^{24}b^5)$, $\nu_7(\Delta) \geq 1$ if and only if $\nu_7(b) \geq 1$ or $(a, b) \in \{(1, 2), (2, 4), (3, 1), (4, 1), (5, 4), (6, 2)\} \pmod 7$. Then we have the following cases:

(1) For $(a, b) \in \{(1, 2), (2, 4), (3, 1), (4, 1), (5, 4), (6, 2)\} \pmod 7$, one can easily check that $F(x) \equiv \phi_{i1}^2 \cdot \phi_{i2} \pmod 7$ with $\deg(\phi_{i1}) = 1$, $\deg(\phi_{i2}) = 6$, and ϕ_{ij} is irreducible over $\mathbb{F}_7$ for every $i = 1, \ldots, 6$ and $j = 1, 2$. Thus, there is at most two prime ideals of $\mathbb{Z}_K$ lying above 7 with residue degree 1 each ideal factor. Hence, $\nu_7(i(K)) = 0$.

(2) If $\nu_7(b) \geq 1$ and $\nu_7(a) = 0$, then $F(x) \equiv x^3 \cdot \phi_1 \cdot \phi_2 \pmod 7$ with, for every value of a, $\deg(\phi_1) = 1$, $\deg(\phi_2) = 4$, and ϕ_i is irreducible over $\mathbb{F}_7$ for every $i = 1, 2$. Thus, there are at most four prime ideals of $\mathbb{Z}_K$ lying above 7 with residue degree 1 each ideal factor. Hence, $\nu_7(i(K)) = 0$.

(3) If $\nu_7(b) \geq 1$ and $\nu_7(a) \geq 1$, then $F(x) \equiv x^8 \pmod 7$. Let $\phi = x$. By assumption, $\nu_7(a) \leq 4$ or $\nu_7(b) \leq 7$.

If $\nu_7(b) > \dfrac{8}{5}\nu_7(a)$, then $N_\phi(F) = S_1 + S_2$ has two sides joining $(0, \nu_7(b))$, $(3, \nu_7(a))$, and $(8, 0)$ with $d(S_2) = 1$ since $\nu_7(a) \leq 4$ by assumption.

(i) If $\nu_7(b) \not\equiv \nu_7(a) \pmod 3$, then $d(S_1) = 1$, and so $7\mathbb{Z}_K = \mathfrak{p}_1^3\mathfrak{p}_2^5$ with residue degree 1 each ideal factor. Hence, $\nu_7(i(K)) = 0$.

(ii) If $\nu_7(b) \equiv \nu_7(a) \pmod 3$, then $d(S_1) = 3$ with $R_{1_1}(F)(y) = a_7y^3 + b_7 \in \mathbb{F}_\phi[y]$. Thus, there are at most four prime ideals of $\mathbb{Z}_K$ lying above 7 with residue degree 1 each ideal factor. Hence, $\nu_7(i(K)) = 0$.

If $\nu_7(b) < \dfrac{8}{5}\nu_7(a)$, then $N_\phi(F) = S_1$ has a single side $(0, \nu_7(b))$, $(3, \nu_7(a))$, and $(8, 0)$ with $d(S_1) \in \{1, 2, 4\}$ since $\nu_7(b) \leq 7$ by assumption. Thus, there are at most four prime ideals of $\mathbb{Z}_K$ lying above 7 with residue degree 1 each ideal factor. Hence, $\nu_7(i(K)) = 0$.

For $p \geq 11$, since there is at most 8 prime ideals of $\mathbb{Z}_K$ lying above p with residue degree 1 each ideal factor, and there is at least $p \geq 11$ monic irreducible polynomial of degree f in $\mathbb{F}_p[x]$ for every positive integer f, we conclude that p does not divide $i(K)$.

Theorem 2.3 is proved.

***Proof of Theorem* 2.4.** Let $K = \mathbb{Q}(\alpha)$ be a number field defined by a monic irreducible trinomial $F(x) = x^8 + ax^3 + b \in \mathbb{Z}[x]$. Since $\Delta = -b^2(3^3 \cdot 5^5a^8 - 2^{24}b^5)$ is the discriminant of $F(x)$, thanks to the index formula (1.1), we have the following:

(1) If p divides both a and b, then p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_p(b) = 1$.

(2) If $p = 2$ and 2 does not divide ab, then 2 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$.

(3) If $p = 2$, 2 divides a and does not divide b, then $F(x) \equiv (x-1)^8 \pmod 2$. Let $\phi = x - 1$. Then $F(x) = \cdots + (3a + 8)\phi + a + b + 1$. Hence, 2 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_2(a + b + 1) = 1$; that is $(a, b) \in \{(0, 1), (2, 3)\} \pmod 4$.

(4) If $p \neq 5$ divides b and does not divide a, then $F(x) \equiv x^3(x^5 + a) \pmod p$. Since $x^5 + a$ is square free over $\mathbb{F}_p$. p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_p(b) = 1$.

(5) If $p = 5$ divides b and does not divide a, then $F(x) \equiv x^3(x + a)^5 \pmod 5$. Let $\phi = x + a$. Then $F(x) = \ldots + (3a^3 - 8a^7)\phi + b - a^4 + a^8$. Hence, 5 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ if and only if $\nu_5(b) = \nu_5(b - a^4 + a^8) = 1$.

(6) If $p \notin \{2, 3, 5\}$, p^2 divides $3^3 \cdot 5^5 a^8 - 2^{24} b^5$, and $\nu_p(ab) = 0$, then $F(x)$ admits a multiple root $\overline{u}$ modulo p if and only if $F(u) = u^8 + au^3 + b \equiv 0 \pmod p$ and $F'(u) = 8u^7 + 3au^2 \equiv 0 \pmod p$. Let $u = \dfrac{-2^9 b^2}{75a^3} \in \mathbb{Q}$. Since $\nu_p(75a^3) = 0$, then $u \in \mathbb{Z}_p$. Let $\phi = x - u$. Then $F(x) = \ldots + A\phi^2 + B\phi + C$, with

$$A = 28u^6 + 3au = \frac{-2^9\Delta^2}{3^6 \cdot 5^{12} a^{18} b^2} + \frac{2^{34} b^5 \Delta}{3^6 \cdot 5^{12} a^{18}} + \frac{2^{56} \cdot 5 b^{12}}{3^6 \cdot 5^{12} a^{18}},$$

$$B = 8u^7 + 3au^2 = \frac{2^{18}\Delta^2 - 2^{43} b^7 \Delta}{3^7 \cdot 5^{14} a^{21}},$$

and

$$C = u^8 + au^3 + b = \frac{-\Delta^3}{3^9 \cdot 5^{15} a^{24} b^5} + \frac{2^{24} \cdot 7 b^2 \Delta^2}{3^9 \cdot 5^{16} a^{24}} + \frac{2^{48} b^9 \Delta}{3^9 \cdot 5^{16} a^{24}}.$$

Since $\nu_p(C) = \nu_p(B) = \nu_p(\Delta)$ and $\nu_p(A) = 0$, then $N_\phi^+(F) = S_1$ has a single side joining $(0, \nu_p(\Delta))$ and $(2, 0)$. Since $\nu_p(\Delta) \geq 2$, by Theorem 3.1, $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) \geq \lfloor \nu_p(\Delta)/2 \rfloor \geq 1$. Hence, p divides the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$.

Theorem 2.4 is proved.

***Proof of Theorem* 2.5.** Under the hypotheses, thanks to the index formula, the unique prime candidate to divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ are the rational primes dividing b. Let $q \neq p$ be a rational prime dividing b. If q divides a, then $\nu_q((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$ since b_p is square free. If q does not divide a, then $F(x) \equiv x^3(x^5 + a) \pmod q$ (the case of $q = 5$ is not in this case since $\nu_5(a) \geq 1$). Since $x^5 + a$ is square free modulo q and b_p is square free, then $\nu_q((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$. Now consider the case $q = p$. We have $F(x) \equiv x^8 \pmod p$. Let $\phi = x$.

(1) If $\nu_p(b) = 3$ and $\nu_p(a) \geq 2$, then $N_\phi(F) = S_1$ has a single side joining $(0, 3)$ and $(8, 0)$. Hence, $d(S_1) = 1$ and its attached residual polynomial $R_1(F)(y)$ is irreducible as it is of degree 1. By Theorem 3.1, $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 7$; $(\mathbb{Z}_K : \mathbb{Z}[\alpha]) = p^7$, and so $\mathbb{Z}[\alpha]$ is not integrally closed. On the other hand, let $L = \mathbb{Q}_p(\alpha)$. Since $\mathbb{Q}_p$ is Henselian, there is a unique valuation ω of L extending ν_p. Let $\theta = \alpha^3/p$, then $\theta \in K$, and since 3 and 8 are coprime, we conclude that $K = \mathbb{Q}(\theta)$. Furthermore, $N_\phi(F) = S_1$ has a single side of slope $-\lambda_1 = -3/8$. Hence, $\omega(\alpha) = 3/8$, and so $\omega(\theta) = 1/8$. By [10, Corollary 3.1.4], we conclude that $\theta \in \mathbb{Z}_K$. Let $G(x)$ be the minimal polynomial of θ over $\mathbb{Q}$. Using the formula relating roots and coefficients of a monic polynomial, we get $G(x) = x^8 + \sum_{i=1}^{8} (-1)^i s_i x^{8-i}$, where $s_i = \sum_{k_1 < \cdots < k_i} \theta_{k_1} \ldots \theta_{k_i}$, with $\theta_1 = \theta$ and $\theta_2, \ldots, \theta_8$ are the $\mathbb{Q}_p$-conjugates of θ. Then $\omega(\theta_i) = 1/8$ for every $i = 1, \ldots, 8$. Thus, $\nu_p(s_8) = \omega(s_8) = \omega(\theta_1 \cdots \theta_8) = 8 \cdot 1/8 = 1$ and $\omega(s_i) \geq i/8 > 0$. We conclude that $\nu_p(s_i) \geq 1$

for every $i = 1, \ldots, 7$, and so $G(x)$ is a p-Eisenstein polynomial. Hence, $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\theta])) = 0$. Since p is the unique rational prime candidate to divide $(\mathbb{Z}[\alpha] : \mathbb{Z}[\theta])$, we conclude that $\nu_q((\mathbb{Z}_K : \mathbb{Z}[\theta])) = 0$ for every rational prime q (including p), which means that $\mathbb{Z}_K = \mathbb{Z}[\theta]$. Hence, K is monogenic.

(2) The treatment of the cases (2) ($\nu_p(b) = 5$ and $\nu_p(a) \geq 4$) and (3) ($\nu_p(b) = 7$ and $\nu_p(a) \geq 5$) is similar to the case (1) above.

Theorem 2.5 is proved.

5. Examples. Let $F(x) = x^8 + ax^3 + b \in \mathbb{Z}[x]$ be a monic irreducible polynomial and K the octic number field generated by a complex root of $F(x)$.

(1) For $a = 14$ and $b = 247$, we have b is square free, $(a, b) \equiv (2, 3) \pmod 4$, and for every rational prime $p \notin \{2, 13, 19\}$, $\nu_p(\Delta) \leq 1$. By Theorem 2.4, $\mathbb{Z}[\alpha]$ is integrally closed and so K is monogenic. Hence, $i(K) = 1$.

(2) For $a = 875$ and $b = 750$, we have $\nu_5(a) = 3$, $\nu_5(b) = 3$, $b_5 = 6$ is square free, and $\nu_q(3^3 \cdot 5^5 a^8 - 2^{24} b^5) \leq 1$ for every rational prime $q \notin \{3, 5\}$. By Theorem 2.5 (1), $\mathbb{Z}_K = \mathbb{Z}[\alpha^3/5]$. Hence, K is monogenic and so $i(K) = 1$.

(3) For $a = 84$ and $b = 43$, we have $(a, b) \equiv (4, 3) \pmod 8$, then, by Theorem 2.1, $i(K)$ is even. Hence, K is not monogenic.

(4) For $a = 81$ and $b = 20717451$, we have $\nu_2(ab) = 0$, then, by Theorem 2.1, $\nu_2(i(K)) = 0$. On the other hand, $a \equiv 81 \pmod{243}$, $b \equiv 4374 \pmod{3^8}$, $\nu_3(\Delta) = 54$, and $\Delta_3 \equiv -1 \pmod 3$, by Theorem 2.2, $\nu_3(i(K)) = 1$. Hence, $i(K) = 3$ and so K is not monogenic.

(5) For $a = 40$ and $b = 183$, we have $(a, b) \equiv (8, 7) \pmod{16}$ and $\nu_3(\Delta) = 29$, then, by Theorem 2.1, $\nu_2(i(K)) = 2$. On the other hand, $\nu_3(b) = 0$, by Theorem 2.2, $\nu_3(i(K)) = 0$. We conclude that $i(K) = 4$. Hence, K is not monogenic.

(6) For $a = 3240$ and $b = 989094807$, we have $(a, b) \equiv (8, 7) \pmod{16}$, $\nu_2(\Delta) = 30$, and $\Delta_2 \equiv 1 \pmod 4$, then by Theorem 2.1, $\nu_2(i(K)) = 2$. On the other hand, $a \equiv 81 \pmod{243}$, $b \equiv 4374 \pmod{3^8}$, $\nu_3(\Delta) = 56$, and $\Delta_3 \equiv -1 \pmod 3$, by Theorem 2.2, $\nu_3(i(K)) = 1$. We conclude that $i(K) = 12$. Hence, K is not monogenic.

(7) For $a = 384$ and $b = 1008$, we have $a \equiv 0 \pmod{128}$ and $b \equiv 496 \pmod{512}$, then by Theorem 2.1, $\nu_2(i(K)) = 5$. On the other hand, $F(x)$ is 3-Eisenstein, then $\nu_3(i(K)) = 0$. We conclude that $i(K) = 2^{\nu_2}$ with $\nu_2 \geq 1$. Hence, K is not monogenic.

(8) For $a = 41472$ and $b = 222724080$, we have $a \equiv 0 \pmod{128}$ and $b \equiv 496 \pmod{512}$, then by Theorem 2.1, 2 divides $i(k)$. On the other hand, $a \equiv 162 \pmod{243}$, $b \equiv 4374 \pmod{3^8}$, $\nu_3(\Delta) = 54$, and $\Delta_3 \equiv -1 \pmod 3$, by Theorem 2.2, $\nu_3(i(K)) = 1$. We conclude that $i(k) = 2^{\nu_2} \cdot 3$ with $\nu_2 \geq 1$. Hence, K is not monogenic.

Acknowledgements. The author is deeply grateful to the anonymous referee whose valuable comments and suggestions have tremendously improved the quality of this paper. Also, he is deeply grateful to Professor Lhoussain El Fadil for his help and encouragement.

Conflict of interest. The author declares that he has no potential conflict of interest in relation to the study in this paper.

Funding. The author declares that no funds, grants, or other support were received during the preparation of this manuscript.

References

1. H. Cohen, *A course in computational algebraic number theory*, GTM, **138**, Springer-Verlag, Berlin, Heidelberg (1993).
2. C. T. Davis, B. K. Spearman, *The index of a quartic field defined by a trinomial* $x^4 + ax + b$, J. Algebra and Appl., **17**, № 10, 185 – 197 (2018).
3. R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Göttingen Abhandlungen, **23**, 1 – 23 (1878).
4. L. El Fadil, *On common index divisors and monogenity of certain number fields defined by* $x^5 + ax^2 + b$, Comm. Algebra, **50**, № 7, 3102 – 3112 (2022).
5. L. El Fadil, *On the index divisors and monogenity of number fields defined* $x^5 + ax^3 + b$, Quaest., 1 – 11 (2023); DOI: 10.2989/16073606.2022.2156000.
6. L. El Fadil, I. Gaál, *On non-monogenity of certain number fields defined by trinomials* $x^4 + ax^2 + b$ (2022); arXiv:2204.03226.
7. L. El Fadil, O. Kchit, *On index divisors and monogenity of certain sextic number fields defined by* $x^6 + ax^5 + b$, Vietnam J. Math. (2024); https://doi.org/10.1007/s10013-023-00679-3.
8. L. El Fadil, O. Kchit, *On index divisors and monogenity of certain septic number fields defined by* $x^7 + ax^3 + b$, Comm. Algebra, 1 – 15 (2022); DOI: 10.1080/00927872.2022.2159035.
9. L. El Fadil, J. Montes, E. Nart, *Newton polygons and p-integral bases of quartic number fields*, J. Algebra and Appl., **11**, № 4, Article 1250073 (2012).
10. A. J. Engler, Prestel, *Valued fields*, Springer-Verlag, Berlin, Heidelberg (2005).
11. H. T. Engstrom, *On the common index divisor of an algebraic number field*, Trans. Amer. Math. Soc., **32**, 223 – 237 (1930).
12. I. Gaál, A. Pethö, M. Pohst, *On the indices of biquadratic number fields having Galois group* V_4, Arch. Math., **57**, 357 – 361 (1991).
13. J. Guàrdia, J. Montes, E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc., **364**, № 1, 361 – 416 (2012).
14. K. Hensel, *Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung*, J. reine und angew. Math., **113**, 128 – 160 (1894); DOI: 10.1515/crll.1894.113.128.
15. T. Nakahara, *On the indices and integral bases of non-cyclic but Abelian biquadratic fields*, Arch. Math., **41**, № 6, 504 – 508 (1983).
16. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer-Verlag, Auflage (2004).
17. E. Nart, *On the index of a number field*, Trans. Amer. Math. Soc., **289**, 171 – 183 (1985).
18. J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin (1999).
19. J. Śliwa, *On the nonessential discriminant divisor of an algebraic number field*, Acta Arith., **42**, 57 – 72 (1982).

Received 19.03.23