Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 6** : 1–8.
ISSN-0037-8712
doi:10.5269/bspm.81161

On the Indices of Certain Number Fields Defined by Polynomials $x^6 + ax + b$

Lhoussain El Fadil and Mohamed Faris

ABSTRACT: Let K be a sextic number field defined by a trinomial $F(x) = x^6 + ax + b \in \mathbb{Z}[x]$. In this paper, for any prime integer p, we compute the p-adic valuation of the field index $i(K)$. In what follows, we explicitly compute the full index $i(K)$. In particular, if $i(K)$ is nontrivial, then K is not monogenic. The study of the monogenicity of K can be performed in some cases, when $i(K) = 1$.

Keywords: Newton Polygons, index of number fields, p-adic valuation, prime ideal factorization, Ore's theorem.

Contents

1. Introduction

Let K be a number field of degree n with ring of integers $\mathcal{O}_K$. Let $\alpha \in \mathcal{O}_K$ be a primitive integral element of K. The index of α, denoted by $ind(\alpha) = (\mathcal{O}_K : \mathbb{Z}[\alpha])$, is the index the Abelian group $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$. We have the following formula linking $(\mathcal{O}_K : \mathbb{Z}[\alpha])\,, \Delta(\alpha)$ and d_K is given by :

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

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 primitive integeral elements of K. Say $i(K) = \gcd\{(\mathcal{O}_K : \mathbb{Z}[\theta])\,;\ \theta \in \mathcal{O} \text{ and } K = \mathbb{Q}(\theta)\}$. A rational prime p dividing $i(K)$ is called a prime common index divisor of K. If K is monogenic, then $\mathcal{O}_K$ has a power integral basis, i.e., a $\mathbb{Z}$-basis of the form $\left(1, \theta, \ldots, \theta^{n-1}\right)$, and the index of K is trivial. Say $i(K) = 1$. Therefore, a field having a prime common index divisor is not monogenic. The first number field with non trivial index was given by Dedekind in 1871, who exhibited the example of the cubic number field K defined by $x^3 - x^2 - 2x - 8$ and showed that the index of any primitive integer of K is even. In 1930, Engstrom [7] was the first one who studied the prime power decomposition of the index of a number field. He showed that, $v_p(i(K))$ is completely determined by the form of the factorization of $p\mathcal{O}_K$ for every number field of degree $n \le 7$ and any positive prime integer $p < n$. This motivated a very important question, stated as problem 22 in Narkiewicz's book [9], which asks for an explicit formula of the highest power $v_p(i(K))$ for a given rational prime p dividing $i(K)$. In [12], Śliwa showed that, if p is a non-ramified ideal in K, then $v_p(i(K))$ is determined by the factorization of $p\mathcal{O}_K$. These results were generalized by Nart [10], who developed a p-adic characterization of the index of a number field. In [8], Nakahara studied the index of non-cyclic but abelian biquadratic number fields. In [?]

2020 *Mathematics Subject Classification:* 11R04, 11R21, 12J10.
Submitted January 01, 2026. Published February 17, 2026

Gaál et al. characterized the field indices of biquadratic number fields having Galois group V_4. In [4], El Fadil and Kchit gave a characterization of the index and studied the monogenity of any sextic number field defined by x^6+ax^5+b. In [5], for every rational prime p, they calculated $v_p(i(K))$ for any septic number field defined by a trinomial x^7+ax^3+b. In [2], El Fadil characterized the index of any quintic number field defined by x^5+ax^3+b. In [3], Kchit studied the index of any number field defined by x^9+ax+b. In this paper, we calculate $v_p(i(K))$ for any number field K defined by a monic irreducible trinomial $x^6+ax+b\in\mathbb{Z}[x]$, we calculate $v_p(i(K))$ for every rational prime p. In particular, we show that $i(K)\in\{1,2,3,6,12\}$.

2. Main Results

Throughout this section, K is a number field generated by a complex root α of a monic irreducible trinomial $F(x)=x^6+ax+b\in\mathbb{Z}[x]$. Without loss of generality, we assume that $v_p(a)\le 4$ or $v_p(b)\le 5$ for every rational prime integer p. Along this paper, we denote $\Delta=6^6b^5-5^5a^6$ the discriminant of F, and $k_p=\frac{k}{p^{v_p(k)}}$ for every integer $k\in\mathbb{Z}$ and a rational prime integer p.

The following theorems provide the value of $\nu_p(i(K))$ for every prime integer $p:=2,3$.

Theorem 2.1 *The following table provides* $v_2(i(K))$: $a\equiv 2(\mod 8)$ *and* $\Delta_2\equiv b(\mod 8)$ *or* $a\equiv 6(\mod 8)$ *and* $\Delta_2\equiv 4+b(\mod 8)$

Table 1: $v_2(i(K))$

Conditions			$v_2(i(K))$
$\nu_2(a)=1$	$\nu_2(\Delta)=8$	$a\equiv 2(\text{mod } 8)$ and $\Delta_2\equiv b(\text{mod } 8)$ or $a\equiv 2(\text{mod } 8)$ and $\Delta_2\equiv b(\text{mod } 8)$	1
	$\nu_2(\Delta)\ge 10$ and $\nu_2(\Delta)$ even	$\Delta_2\equiv 7(\text{mod}8)$	
$\nu_2(a)\ge 2$		$(a,b)\equiv(0,7)$or $(0,3)(\text{mod}8)$	2
Otherwise			0

Theorem 2.2 *The following table provides* $v_3(i(K))$ *:*

Table 2: $v_3(i(K))$

Conditions		$v_3(i(K))$
$(a,b)\equiv(0,8)(\text{mod}9)$		1
$(a,b)\equiv(3,5)(\text{mod}9)$	$\Delta_3\equiv 2(\text{mod}3)$	
$(a,b)\equiv(6,5)(\text{mod}9)$	$\Delta_3\equiv 1(\text{mod}3)$	
Otherwise		0

Theorem 2.3 *For every rational prime* $p\ge 5$ *and for every* $(a,b)\in\mathbb{Z}^2$ *such that* $F(x)=x^6+ax+b$ *is irreducible over* $\mathbb{Q}$, $\nu_p(i(K))=0$, *where* K *is the number field defined by* $F(x)$.

3. Preliminaries

Our proofs are based on Newton polygon techniques applied on prime ideal factorization, which is necessary to prove our main results. In several former papers, El Fadil et al. have introduced the corresponding concepts. 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 [11, Chapter I, Proposition 8.3] and Dedekind's criterion [1, Theorem 6.1.4]. Let p be a prime integer, $\phi\in\mathbb{Z}[x]$ be a monic lift to an irreducible factor of $F(x)$ modulo p, $F(x)=a_0(x)+a_1(x)\phi(x)+\cdots+a_l(x)\phi(x)^l$ the ϕ-expansion of $F(x)$, and $N_\phi^+(F)$ the principal ϕ-Newton polygon of $F(x)$ with respect to p. Let $\mathbb{F}_\phi$ be the field $\mathbb{F}_p[x]/(\bar{\phi})$. Let S be a side of $N_\phi^+(F)$ with initial point (s,u_s). For every $i=0,\dots,l$, let $c_i\in\mathbb{F}_\phi$ be the residue coefficient defined as follows:

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

Let $\lambda=-h/e$ be the slope of S, where h and e are two positive coprime integers. Since $\lambda=-H/l$, where is the height of the side S, then e divides l. Let $d=l/e$ be the degree of S. Hence, if i is not a multiple of e, then ($s+i,u_{s+i}$) does not lie on the side S, and so $c_i=0$. Let $R_\lambda(F)(y)=t_dy^d+t_{d-1}y^{d-1}+\cdots+t_1y+t_0\in\mathbb{F}_\phi[y]$, called the residual polynomial of $F(x)$ associated to the side S, where for every $i=0,\dots,d, t_i=c_{ie}$. If $R_\lambda(F)(y)$ is square free for each side of the polygon $N_\phi^+(F)$, then we say that $F(x)$ is ϕ-regular. Let $\overline{F(x)}=\prod_{i=1}^r\bar{\phi}_i{}^{l_i}$ 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 $i=1,\dots,r$. 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 $j=1,\dots,r_i$, let $R_{\lambda_{ij}}(F)(y)=\prod_{s=1}^{s_{ij}}\psi_{ijs}^{a_{ijs}}(y)$ be the factorization of $R_{\lambda_{ij}}(F)(y)$ in $\mathbb{F}_{\phi_i}[y]$. Then we have the following theorem of index of Ore:

Theorem 3.1 *[6, Theorem 1.7 and Theorem 1.9]*
Under the above hypothesis, we have the following:

1.
$$\nu_p\left((\mathcal{O}_K:\mathbb{Z}[\alpha])\right)\geq\sum_{i=1}^r \mathrm{ind}_{\phi_i}(F)$$

   The equality holds if $F(x)$ is p-regular.

2. *If $F(x)$ is p-regular, then*
$$p\mathcal{O}_K=\prod_{i=1}^r\prod_{j=1}^{t_i}\prod_{s=1}^{s_{ij}}\mathfrak{p}_{ijs}^{e_{ij}}$$
   is the factorization of $p\mathcal{O}_K$ into powers of prime ideals of $\mathcal{O}_K$, 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 $f_{ijs}=\deg(\phi_i)\cdot\deg(\psi_{ijs})$ 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 [?]. 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 [?].

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

The index of a field K is defined by $i(K)=\gcd\{(\mathcal{O}_K:\mathbb{Z}[\alpha])\mid K=\mathbb{Q}(\alpha)\text{ and }\alpha\in\mathcal{O}_K\}$. A rational prime p dividing $i(K)$ is called a prime common index divisor of K. If $\mathcal{O}_K$ has a power integral basis, then $i(K) = 1$. Therefore a field having a prime common index divisor is not monogenic. The existence of prime common index divisors was first established in 1871 by Dedekind who exhibited examples in cubic and quartic number fields. For example, he considered the cubic field K generated by a complex root of $x^3 - x^2 - 2x - 8$ and showed that the prime 2 splits completely in K. So, if we suppose that K is monogenic, then we would be able to find a cubic polynomial generating K, that splits completely into distinct polynomials of degree 1 in $\mathbb{F}_2[x]$. Since there are only 2 distinct polynomials of degree 1 in $\mathbb{F}_2[x]$, this is impossible.

Remark 3.1 It is well known that for any number field K and a prime integer p, if p is a common index divisor of K, then $p \leq n$, where n is the degree of K (see [7]). It follows that the unique prime candidates to be a prime common index divisor of K are $2, 3$, and 5.

For the proof of Theorems 2.1, we need the following lemma, which characterizes the prime common index divisors of K.

Lemma 3.1 *Let p be a rational prime integer and K be a number field. For every positive integer $F(x)$, let $\mathcal{P}_f$ be the number of distinct prime ideals of $\mathcal{O}_K$ lying above p with residue degree $F(x)$ and $\mathcal{N}_f$ the number of monic irreducible polynomials of $\mathbb{F}_p[x]$ of degree $F(x)$. Then p is a prime common index divisor of K if and only if $\mathcal{P}_f > \mathcal{N}_f$ for some positive integer $F(x)$.*

Based on the Engstrom theorem [7, Theorem 8], the unique prime integers which can divide $i(K)$ are $2, 3$, and 5. More precisely, $i(K) = 2^u \cdot 3^v \cdot 5^t$ for some integers 4u,v,4 and t. In this paper, we show that $0 \leq u \leq 2$, $0 \leq v \leq 1$, and $t = 0$.

4. Proofs of our Main Results

4.1. Proof of Theorem 2.1

Since $\triangle = 6^6 b^5 - 5^5 a^6$, we conclude that if 2 divides $(\mathcal{O}_K : \mathbb{Z}[\alpha])$, then 2 divides a. So, assume that 2 divides a. Then

1. If 2 does not divide b, then $\overline{F(x)} = (\phi_1 \cdot \phi_2)^2$ in $\mathbb{F}_2[x]$, where $\phi_1 = x - 1$ and $\phi_2 = x^2 + x + 1$. Consider the following expansions of $F(x)$:

$$\begin{aligned} F(x) &= \phi_1^6 + 6\phi_1^5 + 15\phi_1^4 + 20\phi_1^3 + 15\phi_1^2 + (6+a)\phi_1 + 1 + a + b && (1) \\ &= \phi_2^3 - 3x\phi_2^2 + (2x-2)\phi_2 + ax + 1 + b && (2) \end{aligned}$$

(a) If $\nu_2(a) \geq 2$, then the results are summarized in Table 3.

Table 3: $v_2(a) \geq 2$

Conditions	**Principal Newton polygons**	**Associated residual polynomials**	**Prime ideal factorization**	$i_2(K)$
$(a,b) \equiv (0,7)(\text{mod}8)$	$N_{\phi_i}(F) = S_{i1} + S_{i2}$	$d_{ij} = 1$	$(2) = \mathfrak{p}_{11}\mathfrak{p}_{12}\mathfrak{p}_{21}\mathfrak{p}_{22}$	2
$(a,b) \equiv (0,3)(\text{mod}8)$	$N_{\phi_i}(F) = S_{i1}$	$R_{11}(F)(y) = y^2 + y + 1$ $R_{21}(F)(y) = x(y-1)(y-x^2)$	$(2) = \mathfrak{p}_{11}\mathfrak{p}_{21}\mathfrak{p}_{22}$	
$(a,b) \equiv (0,1)(\text{mod}4)$	$N_{\phi_i}(F) = S_{i1}$	$d_{i1} = 1$	$(2) = \mathfrak{p}_{11}^2\mathfrak{p}_{21}^4$	0
$(a,b) \equiv (4,7)(\text{mod}8)$		$R_{11}(F)(y) = y^2 + y + 1$ $R_{21}(F)(y) = xy^2 + (x-1)y + x$	$(2) = \mathfrak{p}_{11}\mathfrak{p}_{21}$	
$(a,b) \equiv (4,3)(\text{mod}8)$	$N_{\phi_1}(F) = S_{11} + S_{12}$ $N_{\phi_2}(F) = S_{21}$	$d_{11} = d_{12} = 1$ $R_{21}(F)(y) = xy^2 + (x-1)y + x + 1$	$(2) = \mathfrak{p}_{11}\mathfrak{p}_{12}\mathfrak{p}_{21}$	

(b) If $\nu_2(a) = 1$, then we get the followings results:
We have $\nu_2(\Delta) \geq 7$. Let $s = \frac{-3b}{5a_2} \in \mathbb{Z}_2$ and $\phi = x - s$. The ϕ-expansion of the polynomial $F(x)$ is :

$$F(x) = A + B\phi + C\phi^2 + \dots$$

Where

$$A=F(s)=\frac{-b\Delta}{5^6a^6},\quad \text{with } \nu_2(A)=\nu_2(\Delta)-6$$
$$B=F'(s)=\frac{\Delta}{5^5a^5},\quad \text{with } \nu_2(B)=\nu_2(\Delta)-5$$
$$C=\frac{F''(s)}{2!}=\frac{3^5b^4}{5^3a_2^4}=5s^4,\quad \text{with } \nu_2(C)=0.$$

Hence $N_\phi^+(F)=S$ has a single side of slope $\frac{-\nu_2(\Delta)+6}{2}$.

- If $\nu_2(\Delta)$ is odd, then ϕ provides a unique prime ideal of residue degree 1. Hence $\nu_2(i(K))=0$.
- If $\nu_2(\Delta)$ is even, then $\nu_2(\Delta)=2k+6$ for some integer $k\geq 1$. Then S is of degree 2 and its associated residual polynomial $R_1(F)(y)=(y+1)^2$. Replace ϕ by $x-(s+2^k)$. The ϕ-expansion of $F(x)$ is :

  $$F(x)=A_1+B_1\phi+C_1\phi^2+\dots$$

  Where

  $$A_1=A+2^ka+3s^52^{k+1}+15s^42^{2k}+5s^32^{3k+2}+15s^22^{4k}+3s2^{5k+1}+2^{6k}$$
  $$B_1=B+15s^42^{k+1}+15s^32^{2k+2}+15s^22^{3k+2}+15s2^{4k+2}+3\cdot 2^{5k+1}$$
  $$C_1=C+5s^32^{k+2}+15s^22^{2k+1}+5s2^{3k+2}+5\cdot 2^{4k}.$$

  Then $\nu_2(B_1)=k+1$, and $\nu_2(C_1)=0$. Also $A_1\equiv A+2^ka+3s^52^{k+1}+15s^42^{2k}(\bmod 2^{3k+1})$, then $A_1\equiv A+2^kB+15s^42^{2k}(\mod 2^{3k+1})$. It follows that:

  (a') If $k=1$, then $A_1\equiv 4\left(-(10a+b)\frac{\Delta_2}{5^6a_2^6}+15s^4+15s^24\right)(\bmod 2^5)$. Thus $\nu_2(A_1)\geq 3$. 3 cases are following:
  - If $(2a+b)\Delta_2\equiv 3(\bmod 4)$; that is $\Delta_2\not\equiv b(\bmod 4)$, then $\nu_2(A_1)=3$, thus $N_\phi^+(F)$ has a single side of degree 1. Then $2\mathcal{O}_K=\mathfrak{p}_{11}^2\mathfrak{p}_{21}^2$ with residual degrees $f_{11}=1$ and $f_{21}=2$. Therefore $\nu_2(i(K))=0$.
  - $(2a+b)\Delta_2\equiv 1(\bmod 8)$; that is $a\equiv 2(\mod 8)$ and $\Delta_2\equiv b(\mod 8)$ or $a\equiv 6(\mod 8)$ and $\Delta_2\equiv 4+b(\mod 8)$. Then $\nu_2(A_1)=4$, thus $N_\phi^+(F)$ has a single side of degree 2 and its associated residual polynomial is $R_1(F)=y^2+y+1\in\mathbb{F}_\phi[y]$ which is irreducible. Then $2\mathcal{O}_K=\mathfrak{p}_{11}^2\mathfrak{p}_{21}^2$ with residual degrees $f_{11}=f_{21}=2$. Therefore $\nu_2(i(K))=1$.
  - $(2a+b)\Delta_2\equiv 5(\bmod 8)$; that is $\Delta_2\equiv b(\mod 8)$. Then $\nu_2(A_1)\geq 2k+3$, thus $N_\phi^+(F)$ has two sides of degree 1 each. Then $2\mathcal{O}_K=\mathfrak{p}_{11}\mathfrak{p}_{12}\mathfrak{p}_{21}^2$ with residual degrees $f_{11}=f_{12}=1$ and $f_{21}=2$. Therefore $\nu_2(i(K))=0$.

  (b') If $k\geq 2$, then $\nu_2(A_1)\geq 2k+1$. Since $\nu_2(B_1)=k+1$, then 2 divides $i(K)$ if and only if $\nu_2(A_1)=2k+2$. Based on the formula of A_1 that is $\Delta_2\equiv 7(\mod 8)$. Indeed, $N_\phi^+(F)$ has a single side of degree 2 and its associated residual polynomial is $R_1(F)=y^2+y+1\in\mathbb{F}_\phi[y]$ which is irreducible. Then $2\mathcal{O}_K=\mathfrak{p}_{11}^2\mathfrak{p}_{21}^2$ with residual degrees $f_{11}=f_{21}=2$. In this case, $\nu_2(i(K))=1$.

2. If 2 divides b, then $\overline{F(x)}=\phi^6$ in $\mathbb{F}_2[x]$, with $\phi=x$. It follows that:

   (a) If $6\nu_2(a)<5\nu_2(b)$, then $N_\phi^+(F)=S_1+S_2$ has two sides joining the points $(0,\nu_2(b)),(0,\nu_2(a))$, and $(6,0)$. Since by assumption, $\nu_2(b)\leq 5$ or $\nu_2(a)\leq 4$, we conclude that $\nu_2(a)\leq 4$, and each side of $N_\phi^+(F)$ is of degree 1. Thus $2\mathcal{O}_K=\mathfrak{p}_{11}^5\mathfrak{p}_{21}$ with $f_{11}=f_{21}=1$. By Lemma 3.1, 2 is not a common index divisor. Hence $\nu_2(i(K))=0$.

   (b) If $6\nu_2(a)\geq 5\nu_2(b)$, then $N_\phi^+(F)=S_1$ has a single side joining the points $(0,\nu_2(b))$ and $(6,0)$. Let d_1 be the degree of S_1. Then $d_1\in\{1,2,3\}$.

   If $d_1=1$, then $2\mathcal{O}_K=\mathfrak{p}^6$ with residue degree $f_1=1$. By Lemma 3.1, 2 is not a common index divisor. Hence $\nu_2(i(K))=0$.

If $d_1 = 2$; $\nu_2(b) \in \{2, 4\}$, then $e_1 = 3$ is the ramification degree of S_1. Since $R_1(F)(y) = (y+1)^2$ is the residual polynomial of $F(x)$ attached to S_1, the Newton polygon of $F(x)$ of second order $N_2(F)$ has length 2. Thus $N_2(F)$ has two sides of degree 1 each or $N_2(F)$ has a single side and its attached residual polynomial has at most degree 2, and so there at most two prime ideals of $\mathcal{O}_K$ lying above 2. Hence $\nu_2(i(K)) = 0$.

If $d_1 = 3$, then $e_1 = 2$ and $R_1(F)(y) = y^3 - 1 = (y-1)\left(y^2 + y + 1\right)$ is the residual polynomial of $F(x)$ attached to S_1. Thus $2\mathcal{O}_K = \mathfrak{p}_{21}^2\mathfrak{p}_{22}^2$ with $f_{21} = 1$ and $f_{22} = 2$. Hence $\nu_2(i(K)) = 0$.

4.2. Proof of Theorem 2.2

For $p = 3$, since $\triangle = 6^6b^5 - 5^5a^6$, we conclude that 3 is a candidate to divide $(\mathcal{O}_K : \mathbb{Z}[\alpha])$ if and only if 3 divides a. Assume that 3 divides a. Then we have the following cases :

1. If $b \equiv 1(\text{mod}3)$, then $\overline{F}(x) = \overline{\phi}^3$ in $\mathbb{F}_3[x]$, with $\phi = x^2 + 1$. The ϕ-expansion of $F(x) =$ is $F(x) = \phi^3 - 3\phi^2 + 3\phi + (ax + b - 1)$. The principal ϕ-Newton polygon of $F(x)$. Since the length of $N_\phi^+(F)$ equals 3, we conclude that ϕ can provide at most tree prime ideals of $\mathcal{O}_K$ lying above 3. Thus 3 is not a common index divisor of K. Hence $\nu_3(i(K)) = 0$.

2. If $b \equiv -1(\text{mod}3)$, then $\overline{F(x)} = \overline{(\phi_1\phi_2)}^3$ in $\mathbb{F}_3[x]$, with $\phi_1 = x - 1$ and $\phi_2 = x + 1$. Let

$$F(x) = \phi_1^6 + 6\phi_1^5 + 15\phi_1^4 + 20\phi_1^3 + 15\phi_1^2 + (6+a)\phi_1 + 1 + a + b, \tag{3}$$
$$= \phi_2^6 - 6\phi_2^5 + 15\phi_2^4 - 20\phi_2^3 + 15\phi_2^2 + (6-a)\phi_2 + 1 + b - a. \tag{4}$$

It follows that :

(a) If $(a, b) \equiv (0, -1)$ mod 9, then $N_{\phi_i}^+(F) = S_{i1} + S_{i2}$ has two sides joining $(0, v)$, $(1, 1)$, and $(3, 0)$, where $v \geq 2$. Thus $3\mathcal{O}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}^2\mathfrak{p}_{21}\mathfrak{p}_{22}^2$, with residue degree 1 each. Therefore $\nu_3(i(K)) = 1$.

(b) If $a \equiv 0(\text{mod}9)$ and $b \not\equiv -1(\text{mod}9)$ or $a \not\equiv 0(\text{mod}9)$ and $b \equiv -1(\text{mod}9)$, then $N_{\phi_i}^+(F) = S_{i1}$ has a single side of height 1 for every $i = 1, 2$. By Lemma 3.1, 3 is not a common index divisor. Hence $\nu_3(i(K)) = 0$.

(c) If $(a, b) \equiv (3, 7)(\text{mod}9)$, then $N_{\phi_1}^+(F) = S_{11}$ has a single side of height 1 and $N_{\phi_2}^+(F) = S_{21} + S_{22}$ has two sides joining $(0, v)$, $(1, 1)$, and $(3, 0)$ with $v \geq 2$. Thus $3\mathcal{O}_K = \mathfrak{p}_{11}^3\mathfrak{p}_{21}^2\mathfrak{p}_{22}$, with residue degree 1 each. By Lemma 3.1, 3 is not a common index divisor. Hence $\nu_3(i(K)) = 0$.

(d) If $(a, b) \equiv (3, 5)(\text{mod}9)$, then $N_{\phi_2}^+(F) = S_{21}$ has a single side of height 1 and of length 3. For $N_{\phi_1}^+(F) = S_{11}$. We have $\nu_3(\Delta) \geq 8$. Let $s = \frac{-2b}{5a_3} \in \mathbb{Z}_3$ and $\phi_2 = x - s$. The ϕ-expansion of the polynomial $F(x)$ is :
$F(x) = A + B\phi + C\phi^2 + D\phi^3 + \dots$
Where

$$A = F(s) = \frac{-b\Delta}{5^6a^6}, \quad \text{with } \nu_3(A) = \nu_3(\Delta) - 6$$
$$B = F'(s) = \frac{\Delta}{5^5a^5}, \quad \text{with } \nu_3(B) = \nu_3(\Delta) - 5$$
$$C = \frac{F''(s)}{2!} = \frac{2^4 3^5 b^4}{5^3a^4} = 15s^4, \quad \text{with } \nu_3(C) = 1$$
$$D = \frac{F^{(3)}(s)}{3!} = 20s^3, \quad \text{with } \nu_3(D) = 0.$$

Hence $N_{\phi_2}^+(F) = S_{21} + S_{22}$ has 2 sides joining the points $(0, v)$, $(2, 1)$, and $(3, 0)$ with $v = \nu_2(A)$. The S_{22} is of degree 1 and the side S_{21} is of slope $\frac{-\nu_3(\Delta)+7}{2}$.

- If $\nu_2(\Delta)$ is even, then S_{21} provides a unique prime ideal of residue degree 1. Thus $3\mathcal{O}_K = \mathfrak{p}_{11}^3\mathfrak{p}_{21}^2\mathfrak{p}_{22}$, with residue degree 1 each. Hence $\nu_3(i(K)) = 0$.

- If $\nu_2(\Delta)$ is odd, that is, i.e.; $\nu_3(\Delta) \geq 9$. Hence $\nu_3(\Delta) = 2k + 7$ for some integer $k \geq 1$. Then S_{21} is of degree 2 and its associated polynomial $R_1(F)(y) = \overline{A_3} - y^2$ over $\mathbb{F}_{\phi_2} \simeq \mathbb{F}_3$. Since $A_3 \equiv -\Delta_3 \bmod 3$
  If $\Delta_3 \equiv 2(\mod 3)$, then $R_1(F)(y) = -(y-1)(y+1)$, thus S_{21} provides 2 prime ideals of residual degree 1 each. Then $3\mathcal{O}_K = \mathfrak{p}_{11}^3 \mathfrak{p}_{211} \mathfrak{p}_{212} \mathfrak{p}_{22}$ with residual degrees 1. Therefore $\nu_3(i(K)) = 1$.
  If $\Delta_3 \equiv 1(\mod 3)$, then $R_1(F)(y) = -y^2 - 1$ is irreducible over $\mathbb{F}_3$, thus S_{21} provides a unique prime ideal of residual degree 2 each. Then $3\mathcal{O}_K = \mathfrak{p}_{11}^3 \mathfrak{p}_{21} \mathfrak{p}_{22}$ with residual degrees $f_{11} = f_{22} = 1$ and $f_{21} = 2$. By Lemma 3.1, 3 is not a common index divisor. Hence $\nu_3(i(K)) = 0$.

(*e*) If $(a,b) \equiv (6,2) (\text{mod} 9)$, then $N_{\phi_2}^+(F) = S_{21}$ has a single side of height 1 and $N_{\phi_1}^+(F) = S_{11} + S_{12}$ has two sides joining the points $(0,v)$, $(1,1)$, and $(3,0)$ with $v \geq 2$. Thus each side is of degree 1. Thus there are exactly three prime ideals of $\mathcal{O}_K$ lying above 3, and so 3 is not a common index divisor of K. Hence $\nu_3(i(K)) = 0$.

(*f*) If $(a,b) \equiv (6,5) (\text{mod} 9)$, then $N_{\phi_1}^+(F) = S_{11}$ has a single side of height 1 and length 3. For $N_{\phi_1}^+(F) = S_{11}$. We have $\nu_3(\Delta) \geq 8$. Let $s = \frac{-2b}{5a_3} \in \mathbb{Z}_3$ and $\phi_2 = x - s$. The ϕ-expansion of the polynomial $F(x)$ is :

$$F(x) = A + B\phi + C\phi^2 + D\phi^3 + \dots$$

Where

$$\begin{aligned}
A = F(s) &= \frac{-b\Delta}{5^6 a^6}, && \text{with } \nu_3(A) = \nu_3(\Delta) - 6 \\
B = F'(s) &= \frac{\Delta}{5^5 a^5}, && \text{with } \nu_3(B) = \nu_3(\Delta) - 5 \\
C = \frac{F''(s)}{2!} = \frac{2^4 3^5 b^4}{5^3 a^4} &= 15 s^4, && \text{with } \nu_3(C) = 1 \\
D = \frac{F^{(3)}(s)}{3!} &= 20 s^3, && \text{with } \nu_3(D) = 0.
\end{aligned}$$

Hence $N_{\phi_2}^+(F) = S_{21} + S_{22}$ has 2 sides joining the points $(0,v)$, $(2,1)$, and $(3,0)$ with $v = \nu_2(A)$. The S_{22} is of degree 1 and the side S_{21} is of slope $\frac{-\nu_3(\Delta)+7}{2}$.

- If $\nu_2(\Delta)$ is even, then S_{21} provides a unique prime ideal of residue degree 1. Thus $3\mathcal{O}_K = \mathfrak{p}_{11}^3 \mathfrak{p}_{21}^2 \mathfrak{p}_{22}$, with residue degree 1 each. Hence $\nu_3(i(K)) = 0$.
- If $\nu_2(\Delta)$ is odd, that is, i.e.; $\nu_3(\Delta) \geq 9$. Hence $\nu_3(\Delta) = 2k + 7$ for some integer $k \geq 1$. Then S_{21} is of degree 2 and its associated polynomial $R_1(F)(y) = \overline{A_3} - y^2$ over $\mathbb{F}_{\phi_2} \simeq \mathbb{F}_3$. Since $A_3 \equiv \Delta_3 \bmod 3$, there are 2 cases :
  If $\Delta_3 \equiv 1(\mod 3)$, then $R_1(F)(y) = -(y-1)(y+1)$, thus S_{21} provides 2 prime ideals of residual degree 1 each. Then $3\mathcal{O}_K = \mathfrak{p}_{11}^3 \mathfrak{p}_{211} \mathfrak{p}_{212} \mathfrak{p}_{22}$ with residual degrees 1. Therefore $\nu_3(i(K)) = 1$.
  If $\Delta_3 \equiv 2(\mod 3)$, then $R_1(F)(y) = -y^2 - 1$ is irreducible over $\mathbb{F}_3$, thus S_{21} provides a unique prime ideal of residual degree 2 each. Then $3\mathcal{O}_K = \mathfrak{p}_{11}^3 \mathfrak{p}_{21} \mathfrak{p}_{22}$ with residual degrees $f_{11} = f_{22} = 1$ and $f_{21} = 2$. By Lemma 3.1, 3 is not a common index divisor. Hence $\nu_3(i(K)) = 0$.

4.3. Proof of Theorem 2.3

Since the candidate prime integers to divide $i(K)$ are $2, 3$, and 5, we have to show that 5 is not a common index divisor of K. As $\triangle = 5^5 a^6 - 6^6 b^5$, if 5 divides $i(K)$, then 5 divides b.

1. If $a \not\equiv 0(\mod 5)$, $\overline{F(x)} = (x+a)^5 x$ in $\mathbb{F}_5[x]$. Let $\phi = x + a$ and $F(x) = \phi^6 - 6a\phi^5 + 15a^2\phi^4 - 20a^3\phi^3 + 15a^4\phi^2 + a\left(1 - 6a^4\right)\phi + \left(b - a^2\left(1 - a^4\right)\right)$ be the ϕ-expansion of $F(x)$. Since $\nu_5\left(15a^4\right) = 1$, $N_\phi^+(F)$ has at most 3 sides and ϕ can provide at most 3 prime ideals of $\mathcal{O}_K$ lying above 5. Thus there are at most 4 prime ideals of $\mathcal{O}_K$ lying above 5, and so 5 is not a common index divisor of K. Hence $\nu_5(i(K)) = 0$.

2. If 5 divides a and $\nu_5(a) < \nu_5(b)$, then there are exactly 2 prime ideals of $\mathcal{O}_K$ lying above 5. Hence $\nu_5(i(K)) = 0$.
3. If 5 divides a and $\nu_5(a) \geq \nu_5(b)$, then $\nu_5(b) \leq 5$, and so $N_\phi^+(F)$ has a single side of degree 1. Thus there is a unique prime ideal of $\mathcal{O}_K$ lying above 5. Hence $\nu_5(i(K)) = 0$.

5. Examples

Let K be a number field generated by a complex root α of an irreducible trinomial $F(x) \in \mathbb{Z}[x]$. Based on Theorems 2.1 and 2.1, we evaluate $i(K)$.

1. For $F(x) = x^6 + 18x^5 + 33$, we have $F(x)$ is 3-Eisenstein. Thus $F(x)$ is irreducible over $\mathbb{Q}$ and 3 does not divide $(\mathcal{O}_K : \mathbb{Z}[\alpha])$, and so $\nu_3(i(K)) = 0$. Since $\nu_2(18) = 1$, $\nu_2(\Delta) = 8$, and $(2a + b)\Delta_2 \equiv 1 (\text{mod} 8)$, then by Theorem 2.1, $\nu_2(i(K)) = 1$. Hence $i(K) = 2$.
2. For $F(x) = x^6 + 72x - 1$. Since $\nu_2(72) \geq 2$, $(a, b) \equiv (0, 7)(\text{mod} 8)$, and $(a, b) \equiv (0, 8)(\text{mod} 9)$, then by Theorems 2.1 and 2.2, $\nu_2(i(K)) = 2$ and $\nu_3(i(K)) = 1$. Thus $i(K) = 12$.
3. For $F(x) = x^6 + 22x - 3$, since $\nu_2(22) = 1$ and $\nu_2(\Delta_2) = 9$, then by Theorem 2.1, $\nu_2(i(K)) = 0$. Also, since $(a, b) \equiv (4, 6)(\text{mod} 9)$, then by Theorem 2.2 we get $\nu_3(i(K)) = 0$. Hence $i(K) = 1$.

References

1. H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag Berlin Heidelberg, (1993).
2. L. El Fadil, *On the index divisors and monogenity of number fields defined* $x^5 + ax^3 + b$, Quaest., (2023), 1-11. doi: 10.2989/16073606.2022.2156000.
3. L. El Fadil, *On the index divisors and monogenity of number fields defined* $x^9 + ax + b$
4. L. El Fadil and O. Kchit, *On index divisors and monogenity of certain sextic number fields defined by* $x^6 + ax^5 + b$, Vietnam J. Math., (2023).
5. El Fadil and Omar Kchit , *On index divisors and monogenity of certain septic number fields defined by* $x^7 + ax^3 + b$, Commun. Algebra, (2022), 1-15. doi: 10.1080/00927872.2022.2159035.
6. J. GuÀrdia, J. Montes, and E. Nart, *Newton polygons and p-integral bases of quartic number fields*, J. Algebra Appl., 11(4) (2012), 1250073.
7. H. T. Engstrom, *On the common index divisor of an algebraic number field*, Trans. Amer. Math. Soc., 32 (1930), 223-237.
8. T. Nakahara, *On the indices and integral bases of non-cyclic but abelian biquadratic fields*, Arch. Math., 41(6) (1983), 504-508.
9. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer Verlag, 3. Auflage, (2004).
10. E. Nart, *On the index of a number field*, Trans. Amer. Math. Soc., 289 (1985), 171-183.
11. J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, (1999).
12. J. Śliwa, *On the nonessential discriminant divisor of an algebraic number field.* Acta Arith., 42 (1982), 57-72.

Lhoussain EL FADIL,
Department of Mathematics,
Faculty of Sciences Dhar-El Mahraz, University of Sidi Mohamed Ben Abdellah P.O.B. 1796, Fes
MOROCCO.
E-mail address: `lhoussain.elfadil@usmba.ac.ma`

and

Mohamed FARIS,
Department of Mathematics,
Faculty of Sciences Dhar-El Mahraz, University of Sidi Mohamed Ben Abdellah P.O.B. 1796, Fes
MOROCCO.
E-mail address: `mohamed.faris3@usmba.ac.ma`