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

(3s.) **v. 2024 (42)** : 1–9.
ISSN-0037-8712 IN PRESS
doi:10.5269/bspm.63930

# On Common Index Divisors and Monogenity of Certain Number Fields Defined by $x^5 + ax + b$

Omar Boughaleb and Karim Saber

ABSTRACT: Let $K = \mathbb{Q}(\alpha)$ be a number field, where $\alpha$ is a root of a monic irreducible polynomial $F(x) = x^5 + ax + b$ belonging to $\mathbb{Z}[x]$. The purpose of this paper is to characterize when a prime p is a common index divisor of K. More precisely, we give explicitly a sufficient conditions on $a$ and $b$ which guarantee the non-monogenity of $K$. Some useful examples are also given.

Key Words: Common index divisor, prime ideal factorization, power integral bases.

## Contents



## 1. Introduction

The problems of existence and construction of power integral bases of algebraic number fields have been intensively studied by many number theorists (c.f. [15],[21], [22], [33], [1], [16], [37]). It is called a problem of Hasse to characterize whether the ring of integers in an algebraic number field has a power integral basis. Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a complex root $\alpha$ of a monic irreducible polynomial $F(x)$ over $\mathbb{Q}$. We say that $K$ is *monogenic* if $K$ possess a power integral basis (PIB for short), or equivalently, $\{1, \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}\}$ is an integral basis of $K$ for some $\alpha \in \mathbb{Z}_K$ the ring of integer of $K$, in other words $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. The monogenity problem is a line of research within the larger theme of computing the integral closures of ring extensions, which in turn is of great interest in number theory, algebraic geometry, and commutative algebra (see [5], [38], [39]). Based on the arithmetic of the index form equations Gaál, Győry, Pohst, and Pethö with their research teams studied monogenity of several algebraic number fields (see [4], [15],[16], [17], [18]). For monogenity of pure number fields, based on prime ideal factorization, El Fadil studied the pure sextic field $\mathbb{Q}(\sqrt[6]{m})$ with $m \neq \pm 1$ (see [9], [10]). Many authors were also attracted by this problem (see [1], [17], [2]). For monogenity of number fields defined by trinomials, Jones with research team studied monogenity of some irreducible trinomials (see [28], [29], [30], [31]). According to Jones definition, if a polynomial $F(x)$ is monogenic, then $\mathbb{Q}(\alpha)$ is monogenic, but the converse is not true because a number field generated by a root of a non monogenic polynomial can be monogenic. The authors of( [25], [27], [26]) also studied the integral closedness of some number fields defined by trinomials. Their results are refined by Ibarra et al. (see [24]). It may pointed out that the results given in ( [25], [27]) can only decide on the integral closedness of $\mathbb{Z}[\alpha]$, but cannot test whether the field is monogenic or not. Therefore Jones' and Khanduja's results cover partially the study of monogenity of number fields defined by trinomials. In [19]' for a sextic number field $K$ defined by a trinomial $F(x) = x^6 + ax^3 + b \in \mathbb{Z}[x]$, Gaaál calculated all possible generators of power integral bases of K. In [11], El Fadil extended Gaál's studied some cases where $K$ is not monogenic.

2010 *Mathematics Subject Classification:* 1R21, 11R04, 11Y40.
Submitted June 10, 2022. Published December 10, 2022

In [12], for every prime integer $p$, El Fadil gave necessary and sufficient conditions on a and b which characterize when $p$ is a common index divisor of K, where K is a number field defined by an irreducible trinomial $F(x) = x^5 + ax^2 + b \in \mathbb{Z}[x]$. Also in [3], Ben Yakkou and El Fadil gave sufficient conditions on coefficients of a trinomial which guarantee the non-monogenity of the number field defined by such a trinomial. In this paper, for every prime integer p and any number field K defined by an irreducible trinomial $F(x) = x^5 + ax + b \in \mathbb{Z}[x]$, we characterize when does p is a common index divisor of $K$. In particular, under any of the mentioned conditions $K$ is not monogenic. We provide a series of examples illustrating our results.

## 2. Main results

Throughout this section, $K$ is a number field generated by a complex root $\alpha$ of an irreducible trinomial $F(x) = x^5 + ax + b \in \mathbb{Z}[X]$. It is well known that for every prime integer $p$, we can assume that $v_p(a) \leqslant 3$ or $v_p(b) \leqslant 4$. For every prime integer $p$, we give sufficient conditions, on $a$ and $b$ so that $p$ is a common index divisor of $K$. In particular, under any of these conditions, the number field $K$ is not monogenic. By Engston's results, it is well known that the unique candidate prime ideals divide $i(K)$ (see Definition 3.1) are 2 and 3 (see [8]). The next theorems allows to characterize when 2 and 3 divides $i(K)$.

**Theorem 2.1.** *The prime integer 2 is a common index divisor of $K$ if and only if one of the following conditions holds:*

1. *If $a \equiv 1 \pmod 4, v_2(b) = 4k + 2$ for some positive integer $k$.*
2. *If $a \equiv 7 \pmod 8, b \equiv 0 \pmod 8$ and $v_2(b - (a + 1)) > 3$*
3. *$a \equiv 3 \pmod 8, v_2(b) \equiv 4 \pmod 8$, $2v_2(a + 5) < 1 + v_2(b - a - 1)$.*
4. *$a \equiv 3 \pmod 8, v_2(b) = 8k + 4$ for some positive integer $k$, $v_2(b - a - 1)$ is even and $2v_2(a + 5) > 1 + v_2(b - a - 1)$.*
5. *$a \equiv 3 \pmod 8, v_2(b) \equiv 4 \pmod 8$, $v_2(r_0) > 2v_2(r_1)$ and $v_2(b - a - 1) = 2k + 1$ for some positive integer $k$ such that $F(x)$ is $x - k$-regular with respect to $p = 2$.*
6. *$a \equiv 3 \pmod 8, v_2(b) \equiv 4 \pmod 8$, $v_2(r_0) < 2v_2(r_1)$ and $v_2(r_0) = 2l$ for some positive integer $l$ and $v_2(b - a - 1) = 2k + 1$ for some positive integer $k$ such that $F(x)$ is $x - k$-regular with respect to $p = 2$.*

**Theorem 2.2.** *For e every value of $(a, b) \in \mathbb{Z}^2$ such that $x^5 + ax + b$ is irreducible over $\mathbb{Q}$, 3 does not divide the index $i(K)$, where $K$ is the number field defined by $x^5 + ax + b$.*

## 3. Preliminaries

Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field with $\alpha$ an algebraic integer and $F(x)$ its minimal polynomial over $\mathbb{Q}$. Let $\mathbb{Z}_K$ be the ring of algebraic integers of $K$. It is well known that the ring $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$ and so the abelien group $\mathbb{Z}_K/\mathbb{Z}[\alpha]$ is finite. Its cardinal order is called the index of $\mathbb{Z}[\alpha]$ and denoted by $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. The determination of the prime ideal decomposition in $\mathbb{Z}_K$ of any rational prime $p$ is one of the major problems in Algebraic Number Theory. In 1878 Dedekind proved the following result in this direction (see [35]).

**Theorem 3.1.** *Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field with $\alpha$ a root of an irreducible polynomial $F(x) \in \mathbb{Z}[x]$. Let $p$ be a rational prime. Let $\overline{F} = \overline{\phi_1}^{l_1} ... \overline{\phi_r}^{l_r}$ be the factorization of $\overline{F}$ as a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$, with $\phi_i$ monic polynomials belonging to $\mathbb{Z}[X]$. Suppose that $p$ does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, then $p\mathbb{Z}_K = \prod_{i=1}^{r} \mathcal{P}_i^{l_i}$, where $\mathcal{P}_1 ... \mathcal{P}_r$ are the distinct prime ideals of $\mathbb{Z}_K$ lying above $p$, $\mathcal{P}_i = p\mathbb{Z}_K + \phi_i(\alpha)\mathbb{Z}_K$ with residual degree $f(\mathcal{P}_i/p) = \deg \overline{\phi_i}$ for all $i$.*

Dedekind also gave a criterion which allows to test weither $p$ does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ (see [6]).

**Theorem 3.2.** *Let $K=\mathbb{Q}(\alpha)$, $F(x)$ and $\mathcal{P}_1...\mathcal{P}_r$ be as in the Theorem 3.1. Let $G$ be the polynomial $\frac{1}{p}\left(F(x)-\phi_1^{l_1}...\phi_r^{l_r}\right)$ with coefficients in $\mathbb{Z}$. Then $p$ does not divide $(\mathbb{Z}_K:\mathbb{Z}[\alpha])$ if and only if for each $i=1,...,r$, we have either $l_i=1$ or $\overline{\phi_i}$ does not divide $\overline{G}$.*

In 1894, Hensel developed a powerful approach by showing that the prime ideals of $\mathbb{Z}_K$ lying above $p$ are in one-to-one correspondence with the monic irreducible factors of $F(x)$ over the field $\mathbb{Q}_p$ of p-adic numbers and that the ramification index together with the residue degree of a prime ideal of $\mathbb{Z}_K$ lying over $p$ are same as those of the simple extension of $\mathbb{Q}$ obtained by adjoining a root of the corresponding irreducible factor of $F(x)$ belonging to $\mathbb{Q}_p[x]$. The first steep of the factorization is given by Hensel's Lemma. Unfortunately, the factors provided by Hensel's Lemma are not necessarily irreducible over $\mathbb{Q}_p$. 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. Now, we recall some fundamental techniques on Newton polygon, for more details, we refer to ( [13], [14], [32]).

We use Dedekind's theorem (see Theorem 3.1) relating the prime ideal factorization of $p\mathbb{Z}_K$ and the factorization of $F(x)$ modulo $p$, when $p$ does not divide the index $(\mathbb{Z}_K:\mathbb{Z}[\alpha])$. Also, we need to use the Dedekind's criterion (see Theorem 3.2) for testing the divisibility of $(\mathbb{Z}_K:\mathbb{Z}[\alpha])$ by $p$.

For any prime integer $p$, let $\nu_p$ be the $p$-adic valuation of $\mathbb{Q}$, $\mathbb{Q}_p$ its $p$-adic completion, and $\mathbb{Z}_p$ the ring of $p$-adic integers. Let $\nu_p$ be the Gauss's extension of $\nu_p$ to $\mathbb{Q}_p(x)$. For any polynomial $F(x)=\sum_{i=0}^{n}a_ix^i\in\mathbb{Q}_p[x]$ we set $\nu_p(F)=\min(\nu_p(a_i),\ i=0,\dots,n)$. For any nonzero polynomials $F,G\in\mathbb{Q}_p[x]$, we extend this valuation to $\mathbb{Q}_p(x)$ as follows $\nu_p(F/G)=\nu_p(F)-\nu_p(G)$. Let $\phi\in\mathbb{Z}_p[x]$ be a monic polynomial whose reduction is irreducible in $\mathbb{F}_p[x]$ and $\mathbb{F}_\phi$ the field $\frac{\mathbb{F}_p[x]}{(\overline{\phi})}$. For any monic polynomial $F(x)\in\mathbb{Z}_p[x]$, upon the Euclidean division by successive powers of $\phi$, we expand $F(x)$ as $F(x)=\sum_{i=0}^{l}a_i(x)\phi(x)^i$, called the *$\phi$-expansion* of $F(x)$ (for every $i$, $\deg(a_i(x))<\deg(\phi)$). The $\phi$-Newton polygon $N_\phi(F)$ of $F(x)$ with respect to $p$ is the lower boundary convex envelope of the set of points $\{(i,\nu_p(a_i(x))),\ a_i(x)\neq 0\}$. For every side $S$ of $N_\phi(F)$, the length $l$ of $S$ is the length of its projection to the $x$-axis and its height $h$ is the length of its projection to the $y$-axis. We call $d=\gcd(l,h)$ the degree of $S$. The *principal $\phi$-Newton polygon* $N_\phi^-(F)$ of $F$ is the part of the polygon $N_\phi(F)$, which is determined by joining all sides of negative slopes. To every side $S$ of $N_\phi^-(F)$, with initial point $(s,u_s)$ and length $l$, and to every $0\leq i\leq l$, we attach the following residue coefficient $c_i\in\mathbb{F}_\phi$:

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

where $(p,\phi(x))$ is the maximal ideal of $\mathbb{Z}_p[x]$ generated by $p$ and $\phi(x)$. 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 $S$. Notice that, the points with integer coordinates lying on $S$ are exactly $(s,u_s),(s+e,u_s-h),\cdots,(s+de,u_s-dh)$. Thus, if $i$ is not a multiple of $e$, then $(s+i,u_{s+i})$ does not lie in $S$, and so $c_i=0$. The polynomial $F_S(y)=t_dy^d+t_{d-1}y^{d-1}+\cdots+t_1y+t_0\in\mathbb{F}_\phi[y]$, is called the *residual polynomial* of $F(x)$ associated to the side $S$, where for every $i=0,\dots,d$, $t_i=c_{ie}$. Let $N_\phi^-(F)=S_1+\cdots+S_r$ be the principal $\phi$-Newton polygon of $F(x)$ with respect to $p$. We say that $F(x)$ is a *$\phi$-regular polynomial* with respect to $p$, if $F_{S_i}(y)$ is square free in $\mathbb{F}_\phi[y]$ for every $i=1,\dots,r$. The polynomial $F(x)$ is said to be *$p$-regular* if $\overline{F(x)}=\prod_{i=1}^{r}\overline{\phi_i}^{l_i}$ for some monic polynomials $\phi_1,\dots,\phi_r$ of $\mathbb{Z}[x]$ such that $\overline{\phi_1},\dots,\overline{\phi_r}$ are irreducible coprime polynomials over $\mathbb{F}_p$ and $F(x)$ is a $\phi_i$-regular polynomial with respect to $p$ for every $i=1,\dots,r$. Let $\phi\in\mathbb{Z}_p[x]$ be a monic polynomial, with $\overline{\phi(x)}$ irreducible in $\mathbb{F}_p[x]$. the *$\phi$-index* of $F(x)$, denoted by $ind_\phi(F)$, is $\deg(\phi)$ times the number of points with natural integer coordinates that lie below or on the polygon $N_\phi^-(F)$, strictly above the horizontal axis, and strictly beyond the vertical axis. Let $\overline{F(x)}=\prod_{i=1}^{r}\overline{\phi_i}^{l_i}$ is the factorization of $\overline{F(x)}$ in $\mathbb{F}_p[x]$, where every $\phi_i\in\mathbb{Z}[x]$ is monic polynomial, with $\overline{\phi_i(x)}$ is irreducible in $\mathbb{F}_p[x]$, $\overline{\phi_i(x)}$ and $\overline{\phi_j(x)}$ are coprime when $i\neq j$ and $i,j=1,\dots,r$. For every $i=1,\dots,r$, let $N_{\phi_i}^-(F)=S_{i1}+\cdots+S_{ir_i}$ be the principal $\phi_i$-Newton polygon of $F(x)$ with respect to $p$. For every $j=1,\dots,r_i$, let $F_{S_{ij}}(y)=\prod_{k=1}^{s_{ij}}\psi_{ijk}^{a_{ijk}}(y)$ be the factorization of $F_{S_{ij}}(y)$ in $\mathbb{F}_{\phi_i}[y]$. Then we have the following theorem of index of Ore:

**Theorem 3.3.** *If $F(x)$ is p-regular, then*

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

*is the factorization of $p\mathbb{Z}_K$ into powers of prime ideals of $\mathbb{Z}_K$ lying above p, where $e_{ij} = l_{ij}/d_{ij}$, $l_{ij}$ is the length of $S_{ij}$, $d_{ij}$ is the ramification degree of $S_{ij}$, and $f_{ijk} = deg(\phi_i) \times deg(\psi_{ijk})$ is the residue degree of the prime ideal $\mathfrak{p}_{ijk}$ over p.*

Now we describe how to compute a regular integer $s \in \mathbb{Z}_p$ such that $F(x)$ is $x-s$-regular with respect to $p$. Let $p$ be a prime integer and $K$ a number field defined by a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$ with $F(x) = \phi^5 + a_4\phi^4 + a_3\phi^3 + a_2\phi^2 + a_1\phi^1 + a_0$ for some $\phi = x - a \in \mathbb{Z}[x]$ and $(a_0, \ldots, a_4) \in \mathbb{Z}^5$. Assume that $N_\phi^-(F)$ has a non-trivial $k$-component for some $k \in \mathbb{N}$; a side of slope $-k$ and length $l \neq 0$. Assume also that $l \geq 2$ and $R_1(F)(y) = \pm(y-u)^2$ is the residual polynomial of $F(x)$ associated to this side for some integer $u$. Then we can construct an element $s \in \mathbb{Z}_p$ such that $F(x)$ is $x - s$-regular. Such an element $s$ is called a regular element of $F(x)$ with respect to $\phi$. How to construct such a regular element $s$? By theorem of the polygon, $F(x) = F_1(x)F_2(x)$ in $\mathbb{Z}_p[x]$ such that $F_2$ is monic, $N_\phi(F_2)$ has a single side of slope $-k$, and $R_1(F_2)(y) = \pm(y-u)^2$ is the residual polynomial of $F_2$ associated to this side. Let $u_0 = u$, $s_1 = s_0 + p^k u_0$, and $\phi = x - s_1$. Then $F_2(x) = a_1\phi^2 + b_1\phi + c_1$ for some $(a_1, b_1, c_1) \in \mathbb{Z}_p^3$ such that $\nu_p(a_1) = 0$, $\nu_p(b_1) \geq k+1$ and $\nu_p(c_1) \geq 2k+1$. If $2\nu_p(b_1) \geq \nu_p(c_1)$, $\nu_p(c_1) = 2h$ for some integer $k \geq k$ and $R_1(F)(y) = \pm(y-u_1)^2$ for some integer $u_1 \in \mathbb{Z}$, then we can repeat the same process. In this case $ind_{\phi_1}(F) \geq ind_{\phi_0}(F) + 1$. Thus $[\mathbb{Z}_K : \mathbb{Z}[\alpha]] \geq ind_{\phi_1}(F) \geq ind_{\phi_0}(F) + 1$. Since $[\mathbb{Z}_K : \mathbb{Z}[\alpha]]$ is finite, this process cannot continue infinitely. Thus after a finite number of iterations, this process will provide a regular element.

When the polynomial $F(x)$ is not $p$-regular, then the factors of certain residual polynomials $R_{\lambda_{ij}}(F)(y)$ are not irreducible in $\mathbb{Q}_p(x)$, Montes, Nart and Guárdia introduced an efficient algorithm to factorize completely the principal ideal $p\mathbb{Z}_K$ (see [20,32]). They defined the Newton polygon of order $r$ and they proved an extension of the theorem of the product, theorem of the polygon, theorem of the residual polynomial and theorem of index in arbitrary order $r$. As we will use this algorithm in second order, we shortly recall those concepts that we use throughout. Let $\phi$ be a monic irreducible factor of $F(x)$ modulo $p$. Let $S$ be a side of $N_\phi^-(F)$, of slope $\lambda = \frac{-h}{e}$ with $h$ and $e$ are two positive coprime integers such that the associated residual polynomial $R_\lambda(F)(y)$ is not separable in $\mathbb{F}_\phi$. A type of order 2 is a chain: $(\phi(x), \lambda, \phi_2(x), \lambda_2, \psi_2(y))$, where $\phi_2(x)$ is a monic irreducible polynomial in $\mathbb{Z}_p[x]$ of degree $m_2 = e\mathring{u}f\mathring{u}\deg(\phi)$, $\lambda_2$ is a negative rational number and $\psi_2(y) \in \mathbb{F} = \mathbb{F}_\phi[y]/(\psi_1(y))$ such that

(1) $N_\phi^-(\phi_2)$ is one-sided of slope $\lambda$.

(2) The residual polynomial in order 1 of $\phi_2$ is $R_\lambda(\phi_2)(y) = c\psi_1(y)$ in $\mathbb{F}_\phi[y]$, with $c \in \mathbb{F}_\phi$.

(3) $\lambda_2$ is a slope of certain side of the $\phi_2$-Newton polygon of second order and $\psi_2(y) = R^2_{\lambda_2}(F)(y)$ is the associated residual polynomial of second order.

The key polynomial $\phi_2$ induces a valuation $w_2$ in $\mathbb{Q}_p(x)$, called the augmented valuation of $v_p$ of second order with respect to $\phi$ and $\lambda$. By [[20], Proposition 2.7], If $P(x) \in \mathbb{Z}_p[x]$ such that $P(x) = a_0(x) + a_1(x)\phi(x) + ... + a_l(x)\phi(x)^l$, then

$$w_2(P(x)) = e.\min_{0\leqslant j\leqslant l}\left\{v_p(a_i(x)) + i(v_p(\phi)(x) + |\lambda|)\right\},$$

in particular $w_2(\phi_2(x)) = e.f.v_p(\phi(x))$. Let $F(x) = a_0(x) + a_1(x)\phi_2(x) + ... + a_t(x)\phi_2(x)^t$ be the $\phi_2$-adic development of $F(x)$ and let $\mu_i = w_2(a_i(x)\phi_2(x)^i)$ for every $0 \leqslant i \leqslant t$. The $\phi_2$-Newton polygon of $F(x)$ of second order with respect to $w_2$ is the lower boundary of the convex envelope of the set of points $\{(i, \mu_i), 0 \leqslant i \leqslant t\}$ in the Euclidean plane.

**Definition 3.1.** The index of a field $K$ is defined by $i(K) = gcd\{(\mathbb{Z}_K : \mathbb{Z}[\alpha]) \mid K = \mathbb{Q}(\alpha) \text{ and } \alpha \in \mathbb{Z}_K\}$. A rational prime $p$ dividing $i(K)$ is called a prime common index divisor of $K$.

**Remark 3.1.** Observe 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.

The following lemma characterizes the prime common index divisors of $K$ is needed for proving Theorem 2.1 and Theorem 2.2, its proof is an immediate consequence of Dedekind's theorem.

**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 $\mathbb{Z}_K$ 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 $F(x)$.*

## 4. Proofs of our main results

### 4.1. Proof of Theorem 2.1

Since $\Delta(F)=2^8a^5+5^5b^4$ is the discriminant of $F(x)$, if 2 is a common index divisor of $K$, then 2 divides $b$. Now assume that 2 divides $b$.

1) If 2 does not divides $a$. Then $\overline{F(x)}=x(x+1)^4$ in $\mathbb{F}_2[x]$. Let $\phi=x+1$. In this case, 2 is a common index divisor of $K$ if and only if $\phi$ provides two prime ideals of $\mathbb{Z}_K$ with residue degree 1 each. Consider the $\phi$-expansion of $F(x)=\phi^5+5\phi^4+10\phi^3-10\phi^2+(5+a)\phi+(b-(a+1))$.

   i) If $v_2(b-(a+1))=1$, then $N_\phi^-(F)=S$ has a single side joining $(0,1)$ and $(4,0)$, with degree of $S$ is 1, thus $\phi$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree one, and $2\mathbb{Z}_K=\mathcal{P}_1\mathcal{P}_2^4$. Thus by Lemma 3.1, 2 is not a common index divisor of $K$. Now assume that $v_2(b-(a+1))\geqslant 2$, ($a\equiv 1 \pmod 4$ and $b\equiv 0 \pmod 4$) or ($a\equiv 3 \pmod 4$ and $b\equiv 2 \pmod 4$).

   ii) If $a\equiv 1 \pmod 4$, then $v_2(a+5)=1$. As $v=v_2(b-(a+1))\geqslant 2$, then $N_\phi^-(F)=S_1+S_2$ has two sides joining $(0,v),(1,1)$ and $(4,0)$ with $v\geqslant 2$, thus $\phi$ provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree one each, and $2\mathbb{Z}_K=\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3^3$. Thus so 2 is a common index divisor of $K$.

   iii) If ($a\equiv 3 \pmod 8$ and $b\equiv 0 \pmod 8$) or ($a\equiv 7 \pmod 8$ and $b\equiv 4 \pmod 8$) then $v_2(a+5)\geqslant 2$ and $v_2(b-(a+1))=2$ and thus $N_\phi^-(F)=S$ has a single side joining $(0,2)$ and $(4,0)$, of degree of 2, as $R_F(y)=y^2+y+1$ is irreducible over $\mathbb{F}_2$, $\phi$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2, and $2\mathbb{Z}_K=\mathcal{P}_1\mathcal{P}_2^2$. Thus so 2 is not a common index divisor of $K$.

   iv) If $a\equiv 7 \pmod 8$ and $b\equiv 0 \pmod 8$ then $v_2(a+5)=2$ and $v_2(b-(a+1))\geqslant 3$. If $v_2(b-(a+1))=3$, then $N_\phi^-(F)=S_1+S_2$ has two sides with $\deg(S_1)=2$ and $\deg(S_2)=1$. As $R_{S_1}(y)=y^2+y+1$ is irreducible over $\mathbb{F}_2$, $\phi$ provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree one each, and $2\mathbb{Z}_K=\mathcal{P}_1\mathcal{P}_2^2\mathcal{P}_3^2$. Thus so 2 is not a common index divisor of $K$. If $v_2(b-(a+1))>3$, then $N_\phi^-(F)=S_1+S_2+S_3$, thus $\phi$ provides three prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree one each, and $2\mathbb{Z}_K=\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4^2$. Thus so 2 is a common index divisor of $K$.

   v) If $a\equiv 3 \pmod 8$ and $b\equiv 4 \pmod 8$ then $v_2(a+5)\geqslant 3$ and $v_2(b-(a+1))\geqslant 3$. Set $v_*=v_2(b-(a+1))$, then

      a) If $2v_2(a+5)>1+v_*$, then $N_\phi^-(F)=S_1+S_2$ has two sides $S_1,S_2$ with $\deg(S_2)=2$ and $S_1$ is of degree $d\in\{1,2\}$. If $v_*=2k$ for some positive integer $k$, then thus $\phi$ provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree one each. Thus so 2 is a common index divisor of $K$.
      If $v_*=2k+1$ for some positive integer $k$, then $N_\phi^-(F)=S_1+S_2$ has two sides with $\deg(S_1)=2,\lambda_{S_1}=-k$ and $\deg(S_2)=1$. Consider the regular element $k$ such that $\phi_2=x+1+2^k$, then the $\phi_2$-expansion of $F(x)$ is given by $F(x)=\phi^5+(-5-5.2_k)\phi^4+(10.2^{2k}+20.2^k+10)\phi^3+(10.2^{3k}-30.2^{2K}-30.2^k-10)\phi^2+(5.2^{4k}+20.2^{3k}+30.2^{2k}+20.2^k+$

$a+5)\phi+(-(2)^{5k}-5.2^{4k}-10.2^{3k}-10.2^{2k}-2^k a-5.2^k-a+b-1)$. Set $r_0=(-(2)^{5k}-5.2^{4k}-10.2^{3k}-10.2^{2k}-2^k a-5.2^k-a+b-1)$ and $r_1=5.2^{4k}+20.2^{3k}+30.2^{2k}+20.2^k+a+5$. Now since there are two prime ideals lying above 2 with residue degree 1 each, then 2 is a common index divisor of $K$ if and only if $v_2(r_0)>2v_2(r_1)$ or $v_2(r_0)>2v_2(r_1)$ and $v_2(r_0)=2l$ for some positive integer $l$.

b) If $2v_2(a+5)<1+v_*$, then $N_\phi^-(F)=S_1+S_2+S_3$, thus $\phi$ provides three prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree one each, and $2\mathbb{Z}_K=\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4^2$. Thus so 2 is a common index divisor of $K$.

c) If $2v_2(a+5)=1+v_*$, then $N_\phi^-(F)=S_1+S_2$ has two sides with $\deg(S_1)=2$ and $\deg(S_2)=1$. As $R_{S_1}(y)=y^2+y+1$ is irreducible over $\mathbb{F}_2$, $\phi$ provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 and 1 respectively, hence $2\mathbb{Z}_K=\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3^2$. Thus so 2 is not a common index divisor of $K$.

2) If 2 divides $a$. Then $\overline{F(x)}=\phi^5$ in $\mathbb{F}_2[x]$, where $\phi=x$. Considering the $\phi$-expansion of $F(x)$. By assumption $v_2(a)\leqslant 3$ or $v_2(b)\leqslant 4$, we conclude that if $5v_2(a)>4v_2(b)$, then $N_\phi^-(F)=S$ has a single side joining $(0,v_2(b))$ and $(5,0)$, with degree of $S$ is 1, thus $\phi$ provides a unique prime ideal $\mathcal{P}$ of $\mathbb{Z}_K$ lying above 2 with residue degree one, and $2\mathbb{Z}_K=\mathcal{P}^5$. Thus so 2 is not a common index divisor of $K$. If $5v_2(a)<4v_2(b)$, then $v_2(a)\leqslant 3$ and $N_\phi^-(F)=S_1+S_2$ has two sides joining $(0,v_2(b)),(1,v_2(a))$ and $(5,0)$ such that $S_1$ is of degree 1 and $S_2$ is of degree $d\in\{1,2\}$.

i) If $v_2(a)\in\{1,3\}$ then $d=1$, thus $\phi$ provides two prime ideals $\mathcal{P}_1,\mathcal{P}_2$ of $\mathbb{Z}_K$ lying above 2 with residue degree one, and $2\mathbb{Z}_K=\mathcal{P}_1\mathcal{P}_2^4$. Thus so 2 is not a common index divisor of $K$.

ii) If $v_2(a)=2$, then the degree of $S_1$ is 1, $d=2$ and the ramification degree of $S_2$ is $e_2=2$ with slope $\lambda=\frac{-1}{2}$. Since $R_2(F)(y)=(y+1)^2$ and $e_2=2>1$, considering the Newton polygon of higher order. Set $\phi_2=x^2-2$, consider now the $\phi_2$-expansion of $F(x)=x\phi_2^2+4x\phi_2+(a+4)x+b$ and let $w_2$ the valuation defined by $w_2(P)=2\min_{i\geqslant 0}\left\{v_2(a_i+i(v_2(\phi_1)+\frac{1}{2}))\right\}$ where $P=\sum_{i\geqslant 0}a_i\phi^i$, then we see immediately that $w_2(\phi_2)=2$, $w_2(4x)=5$ and $w_2((a+4)x+b)\in\{6,7,8\}$ as $w_2(a+4)+1\geqslant 7$ and $w_2(b)\leqslant 8$. Set $c=(a+4)x+b$, then we have two following cases:

a) If $w_2(c)\in\{6,8\}$, then $N_{\phi_2}^-(F)=S$ has a single side of degree 1, thus $\phi_2$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2, and hence $2\mathbb{Z}_K=\mathcal{P}_1\mathcal{P}_2^2$. Thus so 2 is not a common index divisor of $K$.

b) If $w_2(c)=7$, then we have $v_2(a+4)=3$ and $v_2(b)=4$. Set $\phi_3=x^2-2x-2$ and consider the $\phi_3$-expansion of $F(x)=(x+4)\phi_3^2+(16x+24)\phi_3+(a+44)x+b+32$, now using the fact that $w_2(\phi_3)=2$, $w_2(x+4)=1, w_2(16x+24)=6$ and $w_2((a+44)x+b+32)=8$ as $w_2(a+44)\geqslant 4$ and $w_2(b+32)=4$, we see that $N_{\phi_2}^-(F)=S$ has a single side of degree 1 thus $\phi_3$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with residue degree 2, and hence $2\mathbb{Z}_K=\mathcal{P}_1\mathcal{P}_2^2$. Thus so 2 is not a common index divisor of $K$.

### 4.2. Proof of Theorem 2.2

Since $\Delta(F)=2^8a^5+5^5b^4$ is the discriminant of $F(x)$, if 3 is a common index divisor of $K$, then 3 divides both $a$ and $b$ or 3 does not divides both $a$ and $b$.

1) If 3 divides $a$ and divides $b$. Then $\overline{F(x)}=\phi^5$ in $\mathbb{F}_3[x]$, where $\phi=x$. Consider the $\phi$-expansion of $F(x)$. By assumption $v_3(a)\leqslant 3$ or $v_3(b)\leqslant 4$, we conclude that if $5v_3(a)>4v_3(b)$, then $N_\phi^-(F)=S$ has a single side joining $(0,v_3(b))$ and $(5,0)$, with degree of $S$ is 1, thus $\phi$ provides a unique prime

ideal of $\mathbb{Z}_K$ lying above 3 with residue degree one, and $3\mathbb{Z}_K = \mathcal{P}^5$. Thus so 3 is not a common index divisor of $K$. If $5v_3(a) < 4v_3(b)$, then $v_3(a) \leqslant 3$ and $N_\phi^-(F) = S_1 + S_2$ has two sides joining $(0, v_3(b)), (1, v_3(a))$ and $(5, 0)$ such that $S_1$ is of degree 1 and $S_2$ is of degree $d \in \{1, 2\}$. If $v_2(a) \in \{1, 3\}$ then $d = 1$, If $v_3(a) = 2$, then the degree of $S_1$ is 1 and $d = 2$, thus $S_1$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree one and $S_2$ provides a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 2. Thus so 3 is not a common index divisor of $K$ in this case .

2) If 3 does not divide both $a$ and $b$. Then ($a \equiv \pmod 3$ and $b \equiv 2 \pmod 3$) or ($a \equiv 2 \pmod 3$ and $b \equiv 2 \pmod 3$). Hence $\overline{F(x)} = (x+2)^2(x^3+2x^2+1)$ or $\overline{F(x)} = (x+2)^2(x^3+2x^2+2)$ in $\mathbb{F}_3[x]$, set $\phi = x + 2$, thus $\phi$ provides at most two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree one each or a unique prime ideal of $\mathbb{Z}_K$ lying above 3 with residue degree 2. Thus so 3 is not a common index divisor of $K$.

## 5. Examples

Let $K = \mathbb{Q}(\alpha)$ be a number field, let $\alpha$ be a complex root of a monic irreducible polynomial $F(x) = x^5 + ax + b \in \mathbb{Z}[x]$.

1) For $F(x) = x^5 + 5x^2 + 10$, as $F(x)$ is 5-Eisenstein polynomial, it is irreducible over $\mathbb{Q}$. Then by Theorem 2.1, 2 is a common index divisor of $K$ and hence $K$ is not monogenic.

2) For $F(x) = x^5 + 7x^2 + 56d$, such that 7 does not divide $d$. Then by Theorem 2.1, 2 is a common index divisor of $K$ if and only if $d$ is odd, thus $K$ is not monogenic.

3) For $F(x) = x^5 + 11x^2 + 1100$, as $F(x)$ is 11-Eisenstein polynomial, it is irreducible over $\mathbb{Q}$, we have $2v_2(a + 5) > v_2(b - a - 1)$, then by Theorem 2.1, 2 is a common index divisor, hence $K$ is not monogenic.

4) For $F(x) = x^5 + 3x^2 + 12$, as $F(x)$ is 3-Eisenstein polynomial, it is irreducible over $\mathbb{Q}$, since $v_2(b-a-1) = 3$, then $k = 1$ hence $v_2(r_0) = 4$ is even and $v_2(r_1) = 3$, consequently $v_2(r_0) < 2v_2(r_1)$, then by Theorem 2.1, 2 is a common index divisor, hence $K$ is not monogenic.

## Acknowledgments

The author is very grateful to the anonymous referee for his careful checking.

## References

1. S. Ahmad, T. Nakahara, A. Hameed, *On certain pure sextic fields related to a problem of Hasse*. Int. J. Alg. Comput., 26(3) (2016), 577–583 .
2. H. B. Yakkou, A. Chillai, L. E. Fadil, (2021) *On power integral bases for certain pure number field defined by* $x^{2^r.5^r-m}$. Commun Algebra 49(7):2916-2926.
3. H. Ben Yakkou and L. El Fadil, *On monogenity of certain number fields defined by trinomials*. (arXiv:2109.08765).
4. Y. Bilu, I. Gaál, K. Györy, *Index form equations in sextic fields: a hard computation*. Acta Arithmetica 115(1), (2004), 85–96.
5. P . Cassou-Nogués, M. J. Taylor, *A Note on elliptic curves and the monogeneity of rings of integers*. J. Lond. Math. Soc. 37 (2)(1988) 63–72.
6. Cohen. H., *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag Berlin Heidelberg, (1993).
7. Dedekind. R., *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, Göttingen Abhandlungen*, 23, (1878), 1–23.
8. H.T. Engstrom,*On the common index divisors of an algebraic field*. Ã Trans. Amer. Math. Soc. 32(2) (1930), 223–237.
9. L. El Fadil, *On integral bases and monogeneity of pure sextic number fields with non-squarefree coefficients*. J. Number Theory 228:375–389. DOI: 10.1016/j.jnt.2021.03.025.
10. L. El Fadil,*On power integral bases for certain pure sextic fields*. Bol. Soc. Paran. Math. (2022) (8 pages). DOI: 10.5269/bspm.42373.

11. 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.

12. 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.

13. L. El Fadil, *On Newton polygon's techniques and factorization of polynomial over henselian valued fields*. J. of Algebra and its Appl, (2020), doi: S0219498820501881.

14. L. El Fadil, J. Montes, E. Nart , *Newton polygons and p-integral bases of quartic number fields*. J. Algebra and Appl, 11(4), (2012), 1250073.

15. I. Gaál, *Diophantine equations and power integral bases*. Theory and algorithm, Second edition,Boston, Birkhäuser, (2019).

16. I. Gaál and K. Györy, *Index form equations in quintic fields*. Acta Arith. 89 (1999), 379–396.

17. I. Gaál, L. Remete, *Non-monogenity in a family of octic fields*. Rocky Mountain J. Math, 47(3), (2017), 817–824.

18. I. Gaál, L. Remete, *Power integral bases and monogenity of pure fields*. J. of Number Theory,173, (2017), 129–146.

19. I. Gaál, *An experiment on the monogenity of a family of trinomials*. JP Journal of Algebra Number Theory Appl. 51(1) (2021) 97–111

20. J. Guaàrdia, J. Montes, E. Nart, *Newton polygons of higher order in algebraic number theory*. Tran. Math. Soc. American 364(1), ( 2012), 361–416.

21. Hasse. H., *Zahlentheorie*, Akademie-Verlag, Berlin, (1963).

22. K. Hensel, *Arithemetishe untersuchungen uber die gemeinsamen ausserwesentliche Discrimi-nantentheiler einer Gattung*. J. Reine Angew Math, 113, (1894), 128–160.

23. Hensel. K., *Theorie der algebraischen Zahlen*, Teubner Verlag, Leipzig, Berlin, 1908.

24. R. Ibarra, H. Lembeck, M. Ozaslan, H. Smith, K. E. Stange, *Monogenic fields arising from trinomials*. arXiv:1908.09793v2.

25. A. Jakhar, S. K. Khanduja, N. Sangwan, *Characterization of primes dividing the index of a trinomial*. Int. J. Number Theory 13(10) (2017), 2505–2514.

26. A. Jakhar and S. Kumar, *On non-monogenic number fields defined by x6 + ax + b*. Canadian Mathematical Bulletin (2021), doi: 10.4153/S0008439521000825.

27. B. Jhorar, S. K. Khanduja, *On power basis of a class of algebraic number fields*. I. J. Number Theory, 12(8)(2016), 2317–2321.

28. L. Jones, *Infinite families of non-monogenic trinomials*. Acta Sci. Math.87 (1-2), (2021) 95–105.

29. L. Jones, *Some new infinite families of monogenic polynomials with non-squarefree discriminant*. Acta Arith. 197(2), (2021) 213–219.

30. L. Jones, P. Tristan, *Infinite families of monogenic trinomials and their Galois groups*. Int.J. Math. 29(5), (2018) (11 pages).

31. L. Jones, D. White, *Monogenic trinomials withnon-square free discriminant*. (arXiv:1908.0794).

32. J. Montes, E. Nart, *On theorem of Ore, Journal of Algebra*. 146(2), (1992), 318–334.

33. Y. Motoda, T. Nakahara, S.I.A. Shah,*On a problem of Hasse*. J. Number Theory 96(2):326–334.DOI: 10.1006/jnth.2002.2805.

34. Narkiewicz. W., *Elementary and Analytic Theory of Algebraic Numbers*, Third Edition, Springer, (2004).

35. Neukirch. J., *Algebraic Number Theory*, Springer-Verlag, Berlin (1999).

36. Ore. O., *Newtonsche Polygone in der Theorie der algebraischen Korper*, Math. Ann 99, (1928), 84–117.

37. A. Pethö, M. Pohst, *On the indices of multiquadratic number fields*. Acta Arith. 153(4) (2012) 393–414.

38. L. Spriano, *On ramification theory of monogenic extensions*. Geom. Topol. Monogr. 3 (2000) 151–164.

39. S.-L. Tan, D.-Q. Zhang, *The determination of integral closures and geometric applications*, Adv. Math. 185 (2004) 215–245.

40. E. Zylinski, *Zur Theorie der ausserwesentlicher discriminamtenteiler algebraischer korper*. Math. Ann, (73), (1913), 273–274.

*Omar Boughaleb,*
*Department of Mathematics,*
*Sidi Mohamed Ben Abdellah University,*
*Morocco.*
*E-mail address:* boughaleb01omar@gmail.com

*and*

*Karim Saber,*
*Department of Mathematics,*
*Sidi Mohamed Ben Abdellah University,*
*Morocco.*
*E-mail address:* saber.fsdm@gmail.com