Palestine Journal of Mathematics

Vol 14(4)(2025) , 215–224

On common index divisors and monogenity of certain number fields defined by trinomials of type $x^{2^r} + ax^m + b$

Hamid Ben Yakkou

Communicated by: Ayman Badawi

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

Keywords and phrases: Monogenity, power integral basis, index of a number field, common index divisor, trinomial, Theorem of Ore, prime ideal factorization, Newton polygon.

The author would like to thank the referee and the editor for their advice, which improved this paper.

Corresponding Author: H. Ben Yakkou

Abstract. Let $K = \mathbb{Q}(\theta)$ be a number field, where θ is a root of an irreducible trinomial of type $F(x) = x^{2^r} + ax^m + b \in \mathbb{Z}[x]$. In this paper, using p-adic Newton polygon techniques applied to the decomposition of primes in number fields and the classical index theorem of Ore [20, 21, 37], we study the monogenity of K. More precisely, we prove that if a and $b+1$ are both divisible by 32, then K cannot be monogenic. For $m = 1$, we provide explicit conditions on a, b, and r for which K is not monogenic. We also construct families of irreducible trinomials which are not monogenic, but their roots generate monogenic number fields. To illustrate our results, we give some computational examples.

1 Introduction and statements of results

Let K be a number field generated by a root θ of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$ of degree n, and let $\mathbb{Z}_K$ denote the ring of integers of K. The field K is called monogenic if there exists a primitive element $\eta \in \mathbb{Z}_K$ such that $\mathbb{Z}_K = \mathbb{Z}[\eta]$, that is $(1, \eta, \ldots, \eta^{n-1})$ is an integral basis (called a power integral basis) in K. The problem of studying the monogenity of number fields and constructing power integral bases is one of the most important problems in algebraic number theory. This problem is intensively studied by several researchers in the last four decades (cf. [1, 11, 12, 14, 17, 18, 22, 23, 30, 32, 38]).

In a series of his papers [22, 23, 25], Győry provided the first general algorithms for deciding whether K is monogenic or not and for determining all power integral bases in $\mathbb{Z}_K$. He also studied in [24] and [26] the question of monogenity in relative extensions. Further, he succeeded to reduce index form equations to system of unit equations (see [27]).

For any element η of $\mathbb{Z}_K$, let $\mathrm{ind}(\eta)$ denote the index of the subgroup $\mathbb{Z}[\eta]$ in $\mathbb{Z}_K$. The index of K is defined as follows:

$$i(K) = \gcd\{\mathrm{ind}(\eta) \,|\, \eta \in \mathbb{Z}_K \text{ and } K = \mathbb{Q}(\eta)\}.$$

A prime p dividing $i(K)$ is called a prime common index divisor of K. Remark that if K is monogenic, then $i(K) = 1$. Thus, a field possessing a prime common index divisor is not monogenic.

The existence of common index divisors was first established by Dedekind. He showed that the cubic number field $K = \mathbb{Q}(\theta)$, where θ is a root of $x^3 + x^2 - 2x + 8$, cannot be monogenic, since the prime 2 splits completely in $\mathbb{Z}_K$ (see e.g., [34, Page 64]). There is an extensive literature on indices of number fields; see, for example, [14] by Dedekind, [15] by Engstrom, and [35] by Nart.

In [32], Llorente and Nart studied the index of cubic number fields defined by $x^3 + ax + b$. In [13], Davis and Spearman calculated the index of the quartic number field defined by $x^4 + ax + b$. In [2], Arnóczki and Nyul studied minimal indices of pure quartic number fields. In

[40], Taljaoui and Bouhamza determined integral bases for quartic number fields of the form $\mathbb{Q}(\sqrt[4]{p})$, where p is a prime number. In [31], Kchit studied integral bases and the monogenity of pure number fields of degree p^r. In [39], Pethő and Ziegler gave an efficient criterion to decide whether the maximal order of a biquadratic field has a unit power integral basis or not. See also [36] by Odjoumani, Togbé and Ziegler. In [38], Pethő and Pohst studied indices in multiquadratic number fields.

Combining a refined version [27] of the general approach of [22, 23] with efficient reduction and enumeration algorithms, Gaál and Győry [19], Bilu, Gaál and Győry [11] described algorithms to solve index form equations in quintic and, respectively, sextic fields. In [12], Bérczes, Evertse and Győry studied multiply monogenic orders. The books [16, 17] by Evertse and Győry give detailed surveys on the discriminant form and index form theory and its applications, including related Diophantine equations and monogenity of number fields. See also the book by Gaál [18].

In [29], Jones gave infinite families of non-monogenic trinomials. In [30], Jones and Phillips identify classes of monogenic trinomilas. For various results regarding the indices and monogenity of certain families of number fields defined by trinomials of fixed degree, or of pure number fields with variable exponents, see [3, 5, 6, 7, 8, 10] by Ben Yakkou *et al.*

The purpose of this paper is to study the monogenity of the number field $K = \mathbb{Q}(\theta)$, where θ is a root of an irreducible trinomial of type $F(x) = x^{2^r} + ax^m + b \in \mathbb{Z}[x]$. Recall that in [9] Ben Yakkou and El Fadil studied the non-monogenity of number fields defined by $x^n + ax + b$. More precisely, they gave sufficient conditions on a, b, and n for which K admits an odd prime common index divisor. These results were generalized in [4] by Ben Yakkou for number fields defined by $x^n + ax^m + b$. Also, in [28], Jakhar, Khanduja and Sangwan studied the problem of the integral closedness of $\mathbb{Z}[\theta]$: they gave necessary and sufficient conditions for a prime p to be a divisor of the index $\mathrm{ind}(\theta)$. However, the divisibility of $\mathrm{ind}(\theta)$ by p is not sufficient to decide if p is a common index divisor of K or not. Therefore, their results do not characterize the prime divisors of indices of these number fields. Therefore, the results obtained in [4, 9, 28] cannot give a complete answer about the monogenity and common index divisors of number fields defined by $x^{2^r} + ax^m + b$. For this reason, we have chosen to study this special case separately.

Throughout this paper, for any prime p and any $t \in \mathbb{Z}$, $\nu_p(t)$ stands for the p-adic valuation of t, and we set $t_p = \frac{t}{p^{\nu_p(t)}}$. We also recall that the discriminant of the trinomial $F(x) = x^n + ax^m + b$ is

$$\Delta(F) = (-1)^{\frac{n(n-1)}{2}} b^{m-1} \left(n^{n_1} b^{n_1-m_1} - (-1)^{m_1} m^{m_1} (m-n)^{n_1-m_1} a^{n_1}\right)^{d_0}, \tag{1.1}$$

where $d_0 = \gcd(n, m)$, $n_1 = \frac{n}{d_0}$ and $m_1 = \frac{m}{d_0}$. Recall also that the polynomial $F(x)$ is called monogenic if $\mathbb{Z}_K = \mathbb{Z}[\theta]$, where $K = \mathbb{Q}(\theta)$ and $F(\theta) = 0$. It is important to note that the monogenity of the polynomial $F(x)$ implies the monogenity of the field K, but the converse is not true.

Let us start with the following theorem, which is in a more general case. It gives families of irreducible non-monogenic trinomials with non-squarefree discriminant, but their roots generate monogenic number fields.

Theorem 1.1.
Let $F(x) = x^n + ax^m + b \in \mathbb{Z}[x]$ be a monic polynomial with discriminant Δ. Suppose that there exists a prime p dividing both a and b such that $\nu_p(b) \geq 2$, $\gcd(n, \nu_p(b)) = 1$, $n\nu_p(a) > (n-m)\nu_p(b)$, and Δ_p is square free. Then $F(x)$ is irreducible over $\mathbb{Q}$. Let $K = \mathbb{Q}(\theta)$ be a number field with θ a root of $F(x)$. Then $F(x)$ is not monogenic ($\mathbb{Z}_K \neq \mathbb{Z}[\theta]$), but K is monogenic. Moreover, in this case, $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, with $\alpha = \frac{\theta^s}{p^t}$, where $(s, t) \in \mathbb{N}^2$ is the unique positive solution of the Diophantine equation $\nu_p(b)s - nt = 1$ with $0 \leq s < n$.

Remark 1.2. Theorem 1.1 implies [9, Theorem 2.1], where the special case $n = p^r$ and $m = 1$ was previously considered.

Corollary 1.3.
Let $K = \mathbb{Q}(\theta)$ be a number field with θ a root of a monic irreducible polynomial $F(x) =$

$x^{2^r} + ax^m + b \in \mathbb{Z}[x]$. *Assume that there exists a prime p such that $\nu_p(a) \geq \nu_p(b) \geq 3$, $\nu_p(b)$ is odd, and Δ_p is square free. Then $F(x)$ is irreducible over $\mathbb{Q}$, and not monogenic, but K is monogenic.*

Example 1.4.
The polynomial $F(x) = x^8 + 8x + 8 \in \mathbb{Z}[x]$ has discriminant $\Delta = 2^{24} \times 1273609$. Note that 1273609 is a prime. Then $F(x)$ satisfies the conditions of Corollary 1.3 for $p = 2$. Hence, it is irreducible over $\mathbb{Q}$. Let $K = \mathbb{Q}(\theta)$ with θ is a root of $F(x)$. Then $\mathbb{Z}_K \neq \mathbb{Z}[\theta]$. But, K is monogenic and $\alpha = \frac{\theta^3}{2}$ generates a power integral basis of $\mathbb{Z}_K$.

The following result gives infinite families of number fields defined by $x^{2^r} + ax^m + b$, their indices are divisible by 2, which implies the non-monogenity of these fields.

Theorem 1.5.
Let $F(x) = x^{2^r} + ax^m + b$ be a monic irreducible trinomial, and let $K = \mathbb{Q}(\theta)$ be the number field generated by a root θ of $F(x)$. If $r \geq 3$ and a and $b + 1$ are both divisible by 32, then 2 is a common index divisor of K. In particular, K is not monogenic.

Now, we focus on the case $m = 1$. The following Theorem gives sufficient conditions which guarantee the non-monogenity of infinite families of number fields defined by trinomials of the form $x^{2^r} + ax + b$.

Theorem 1.6.
Let $K = \mathbb{Q}(\theta)$ be a number field with θ root of a monic irreducible trinomial $F(x) = x^{2^r} + ax + b \in \mathbb{Z}[x]$. If one of the following conditions holds

(i) $r \geq 3$, $a \equiv 4 \pmod 8$ *and* $b \equiv 3 \pmod 8$.

(ii) $r \geq 4$, $a \equiv 8 \pmod{16}$ *and* $b \equiv 7 \pmod{16}$.

(iii) $r \geq 3$ *and* $(a, b) \in \{(0, -1), (16, 15)\} \pmod{32}$,

then 2 is a common index divisor of K. In particular, if one of these conditions holds, then K is not monogenic.

Remark 1.7. Theorem 1.6 (i) and (iii) respectively extend Theorem 2.3 (1) and (2) of [3], where the special case $r = 3$ was previously investigated by Ben Yakkou.

When $a = 0$, the following result is an immediate consequence of the above theorem.

Corollary 1.8. *If $b \equiv 1 \pmod{32}$, then the pure number field $\mathbb{Q}(\sqrt[2^r]{b})$ is not monogenic for every natural integer $r \geq 3$.*

Remark 1.9. Note that the above corollary is exactly the result Theorem 2.6 (2) of [8] by Ben Yakkou and El Fadil.

Remark 1.10.
Note that [4, Corollary 2.4] is about trinomials of type $x^{2^r \cdot 3^k} + ax^m + b$. It gives sufficient conditions for the prime 3 to be a common index divisor of K. Although formally it includes $x^{2^r} + ax^m + b$, all statements of Corollary 2.4 of [4] concerns the cases $k \geq 1$. Hence do not overlap with Theorems 1.5 and 1.6. Here, we gave sufficient conditions for which the prime 2 is a common index divisor of K.

2 Newton polygons and the index theorem of Ore

To prove our main results, we need some preliminaries that can be found in details in [3, 4]. For any $\eta \in \mathbb{Z}_K$, it is well known from [34, Proposition 2.13] that

$$D(\eta) = (\mathbb{Z}_K : \mathbb{Z}[\eta])^2 \cdot D_K, \tag{2.1}$$

where $D(\eta)$ is the discriminant of the minimal polynomial of η and D_K is the discriminant of K. Let p be a prime. In 1878, Dedekind gave the explicit factorization of $p\mathbb{Z}_K$ when p does

not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\eta])$ (see [14] and [34, Theorem 4.33]). In 1928, Ø. Ore [37] gave a method for factoring $F(x)$ in $\mathbb{Q}_p(x)$, and so, for factoring $p\mathbb{Z}_K$ when $F(x)$ is p-regular (see [37]). This method is based on Newton polygon techniques. His method was deeply developed by Guàrdia, Montes and Nart in [20, 21], see also [33] by Montes and Nart.

We follow the presentation in [20, 21] by Guàrdia, Montes, and Nart to recall some fundamental facts about this algorithm. Let ν_p be the discrete valuation of $\mathbb{Q}_p(x)$ defined on $\mathbb{Z}_p[x]$ by

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

Let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial whose reduction modulo p is irreducible. Upon the euclidean division by successive powers of $\phi(x)$, the polynomial $F(x) \in \mathbb{Z}[x]$ admits a unique ϕ-adic development

$$F(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_n(x)\phi(x)^n,$$

with $\deg(a_i(x)) < \deg(\phi(x))$. For every $0 \le i \le n$, let $u_i = \nu_p(a_i(x))$. The ϕ-Newton polygon of $F(x)$ with respect to ν_p (or to p, briefly) is the lower convex hull of the points $\{(i, u_i) \,|\, 0 \le i \le n, a_i(x) \ne 0\}$ in the euclidean plane, which we denote by $N_\phi(F)$. The polygon $N_\phi(F)$ is the union of different adjacent sides $S_1, S_2, \ldots, S_g$ with increasing slopes $\lambda_1, \lambda_2, \ldots, \lambda_g$. We shall write $N_\phi(F) = S_1 + S_2 + \cdots + S_g$. The polygon determined by the sides of negative slopes of $N_\phi(F)$ is called the ϕ-principal Newton polygon of $F(x)$ with respect to ν_p, and will be denoted by $N_\phi^+(F)$. Note that the length of $N_\phi^+(F)$ is $l(N_\phi^+(F)) = \nu_{\overline{\phi}}(\overline{F(x)})$; the highest power of $\phi(x)$ dividing $F(x)$ modulo p.

Let S be a side of $N_\phi^+(F)$. Then the length of S, denoted $l(S)$ is the length of its projection to the horizontal axis and its height, denoted $h(S)$ is the length of its projection to the vertical axis. Let $\lambda = -\frac{h(S)}{l(S)} = -\frac{h}{e}$ its slope, where e and h are two positive coprime integers. The degree of S is $d(S) = \gcd(h(S), l(S)) = \frac{l(S)}{e}$; it is equal to the the number of segments into which the integral lattice divides S. More precisely, if (s, u_s) is the initial point of S, then the points with integer coordinates lying in S are exactly

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

The natural integer $e = \frac{l(S)}{d(S)}$ is called the ramification index of the side S and denoted by $e(S)$.

Let $\mathbb{F}_\phi$ be the finite field $\mathbb{Z}[x]/(p, \phi(x)) \simeq \mathbb{F}_p[x]/(\overline{\phi(x)})$ (note that the ideal $(p, \phi(x))$ is maximal in the ring of polynomials $\mathbb{Z}[x]$). For any abscissa $s \le i \le s + de$, we define the following residue coefficient $c_i \in \mathbb{F}_\phi$:

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

Further, we attach to S the residual polynomial:

$$R_\lambda(F)(y) = c_s + c_{s+e}y + \cdots + c_{s+(d-1)e}y^{d-1} + c_{s+de}y^d \in \mathbb{F}_\phi[y].$$

Now, we recall some related definitions to Ore's program.

Definitions 2.1. Let $F(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial. Let $\overline{F(x)} = \prod_{i=1}^{t} \overline{\phi_i(x)}^{l_i}$ be the factorization of $\overline{F(x)}$ into a product of powers of distinct monic irreducible polynomials in $\mathbb{F}_p[x]$. For every $i = 1, \ldots, t$, let $N_{\phi_i}^+(F) = S_{i1} + \cdots + S_{ir_i}$, and for every $j = 1, \ldots, r_i$, let $R_{\lambda_{ij}}(F)(y) = \prod_{s=1}^{s_{ij}} \psi_{ijs}^{n_{ijs}}(y)$ be the factorization of $R_{\lambda_{ij}}(F)(y)$ in $\mathbb{F}_{\phi_i}[y]$.

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

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

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

Now, we recall Ore's theorem which will be often used in the proof of our results (see [21, Theorem 1.19], [33] and [37]):

Theorem 2.2. *(Ore's Theorem)*
Let K be a number field generated by θ, a root of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$. Under the above notation, we have:

(i)

$$\nu_p((\mathbb{Z}_K : \mathbb{Z}[\theta])) \geq \sum_{i=1}^{t} ind_{\phi_i}(F).$$

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

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

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

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

3 proofs of the main results

Proof of Theorem 1.1. Reducing modulo p, one has $F(x) \equiv \phi(x)^n \pmod p$, where $\phi(x) = x$, because p divides both a and b. Further, we have $N_\phi^+(F) = S$ has only one side of degree 1 (because $\gcd(n, \nu_p(b)) = 1$) with slope $\lambda = -\frac{\nu_p(b)}{n}$. Its attached residual polynomial $R_\lambda(F)(y)$ is irreducible over $\mathbb{F}_\phi \simeq \mathbb{F}_p$ as it is of degree 1. By Theorem of the residual polynomial ([21, Theorem 1.19]), $F(x)$ is irreducible over $\mathbb{Q}_p$. Hence, it is irreducible over $\mathbb{Q}$. On the other hand, by using Theorem 2.2, we see that

$$\nu_p(\mathbb{Z}_K : \mathbb{Z}[\theta]) \geq ind_\phi(F) = \frac{(n-1)(\nu_p(b)-1)}{2} \geq 1.$$

Thus, p divides $(\mathbb{Z}_K : \mathbb{Z}[\theta])$. So, the polynomial $F(x)$ is not monogenic.
Let $L = \mathbb{Q}_p(\theta)$ and ω the unique valuation of L extending ν_p (note that $\mathbb{Q}_p$ is a Henselian field). Let $(s,t) \in \mathbb{N}^2$ be the unique solution in positive integers of the Diophantine equation $\nu_p(b)s - nt = 1$ with $0 \leq s < n$ and let $\alpha = \frac{\theta^s}{p^t}$. Note that $\alpha \in \mathbb{Z}_K$ if and only if $\omega(\alpha) \geq 0$. Since $N_\phi^+(F) = S$ has a single side of slope $\lambda = -\frac{\nu_p(b)}{n}$, by [33] we conclude that $\omega(\theta) = \frac{\nu_p(b)}{n}$. So,

$$\omega(\alpha) = \omega\left(\frac{\theta^s}{p^t}\right) = s\omega(\theta) - t = \frac{s\nu_p(b) - tn}{n} = \frac{1}{n}.$$

Since s and n are coprime, $K = \mathbb{Q}(\alpha)$. Let $H(x)$ be the minimal polynomial of α over $\mathbb{Q}$. By the formula relating roots and coefficients of a monic polynomial, we conclude that

$$H(x) = x^n + \sum_{i=1}^{n}(-1)^i s_i x^{n-i},$$

where $s_i = \sum_{k_1<\cdots<k_i} \alpha_{k_1}\cdots\alpha_{k_i}$, and $\alpha_1, \ldots, \alpha_n$ are the $\overline{\mathbb{Q}_p}$-conjugates of α. Since there is a unique valuation extending ν_p to any algebraic extension of $\mathbb{Q}_p$, we conclude that $\omega(\alpha_i) = 1/n$ for every $i = 1, \ldots, n$ (recall that the valuation ω is invariant under the K-embedding actions). Thus, $\nu_p(s_n) = \omega(\alpha_1\cdots\alpha_n) = 1$ and $\nu_p(s_i) \geq i/n$ for every $i = 1, \ldots, n-1$. That means that $H(x)$ is a p-Eisenstein polynomial. Hence, p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. On the other hand, every prime $q \neq p$ does not divide $(\mathbb{Z}_K : \mathbb{Z}[\theta])$, because Δ_p is square free (see [34, Proposition 2.13]). By definition of α, p is the unique positive prime integer candidate to divide $(\mathbb{Z}[\alpha] : \mathbb{Z}[\theta])$. Consequently, $\mathbb{Z}_K = \mathbb{Z}[\alpha]$.

□

To prove Theorems 1.5 and 1.6, we will use the following lemma which gives a sufficient condition for a prime p to be a common index divisor of a given field K (see [14, 15] and [34, Theorems 4.33 and 4.34]).

Lemma 3.1.
Let p be a prime and K a number field. For every positive integer f, let $L_p(f)$ be the number of distinct prime ideals of $\mathbb{Z}_K$ lying above p with residue degree f and $N_p(f)$ be the number of monic irreducible polynomials of $\mathbb{F}_p[x]$ of degree f. If $L_p(f) > N_p(f)$ for some positive integer f, then p is a common index divisor of K.

Remark 3.2.
Note that the condition $i(K) = 1$ is not sufficient for the monogenity of K. The index of the pure cubic number field $K = \mathbb{Q}(\sqrt[3]{175})$ equals 1, but K is not monogenic as its index form equation $5x^3 - 7y^3 = \pm 1$ has no integral solutions.

Proof of Theorem 1.5. By hypothesis, 2 divides a and does not divide b. Thus, $\overline{F(x)} = \overline{\phi_1(x)}^{2^r}$ in $\mathbb{F}_2[x]$, where $\phi_1(x) = x - 1$. Write

$$\begin{aligned} F(x) &= (x-1+1)^{2^r} + ax^m + b \\ &= \sum_{j=1}^{2^r} \binom{2^r}{j} \phi_1(x)^j + ax^m + 1 + b. \end{aligned} \tag{3.1}$$

Since a and $b+1$ are both divisible by 32, we have $\nu_2(a) \geq 5$ and $\nu_2(1+b) \geq 5$. So,

$$\nu_2\left(ax^m + 1 + b)\right) \geq 5.$$

Let $ax^m + 1 + b = \sum_{j=0}^{m} b_j \phi_1(x)^j$ be the ϕ-adic development of $ax^m + 1 + b$, where $b_j \in \mathbb{Z}$. Note that $\nu_2(b_j) \geq 5$ for all $j = 0, \ldots, m$. It follows that $F(x) = \sum_{j=0}^{2^r} a_j \phi_1(x)^j$, where $a_0 = b_0$ and

$$a_j = \begin{cases} b_j + \binom{2^r}{j}, & \text{if } 1 \leq j \leq m, \\ \binom{2^r}{j}, & \text{if } m < j \leq 2^r. \end{cases}$$

Recall that $\nu_2\left(\binom{2^r}{j}\right) = r - \nu_2(j))$ for every $j = 1, \ldots, 2^r$ (see [4, Lemma 3.4]). It follows that $\mu_0 = \nu_2(a_0) \geq 5$ and

$$\begin{cases} \mu_j = \nu_2\left(a_j\right) \geq \min\{5, r - \nu_2(j)\}, & \text{if } 1 \leq j \leq m, \\ \mu_j = \nu_2\left(a_j\right) = r - \nu_2(j), & \text{if } m < j \leq 2^r. \end{cases}$$

Since $r \geq 3$, $N_{\phi_1}^+ = S_{1,1} + \cdots + S_{1,t-2} + S_{1,t-1} + S_{1,t}$ has t distinct sides with $t \geq 4$, joining the points $\{(j, \mu_j),\ j = 0, \ldots, 2^r\}$ in the euclidean plane. The last three sides have degree 1 each and ramification index 2^{r-1} each. More precisely, the part $S_{1,t-2} + S_{1,t-1} + S_{1,t}$ is the polygon joining the points $(2^{r-3}, 3)$, $(2^{r-2}, 2), (2^{r-1}, 1)$ and $(2^r, 0)$ (see Figure 1).Thus, the residual polynomials $R_{1,\ t-k}(F)(y)$ are irreducible in $\mathbb{F}_{\phi_2}[y]$, since each is of degree 1, for $k = 0, 1, 2$. Applying Theorem 2.2, one has:

$$2\mathbb{Z}_K = \mathfrak{p}_{1,t-2,1}^{2^{r-1}} \cdot \mathfrak{p}_{1,t-1,1}^{2^{r-1}} \cdot \mathfrak{p}_{1,t,1}^{2^{r-1}} \mathfrak{a},$$

where $\mathfrak{p}_{1,t-2,1}, \mathfrak{p}_{1,t-1,1}$ and $\mathfrak{p}_{1,t,1}$ are three distinct prime ideals of $\mathbb{Z}_K$ of residue degree 1 each, and $\mathfrak{a}$ is a non-zero ideal of $\mathbb{Z}_K$ provided by the other segments of $N_{\phi_1}^+(F)$. So, the monic irreducible factor $\phi_1(x)$ of $F(x)$ modulo 2 provides at least three distinct prime ideals of residue degree 1 each lying above 2 in $\mathbb{Z}_K$. So, $L_2(1) \geq 3 > 2 = N_2(1)$. By Lemma 3.1, 2 divides $i(K)$. Hence, K is not monogenic.

□

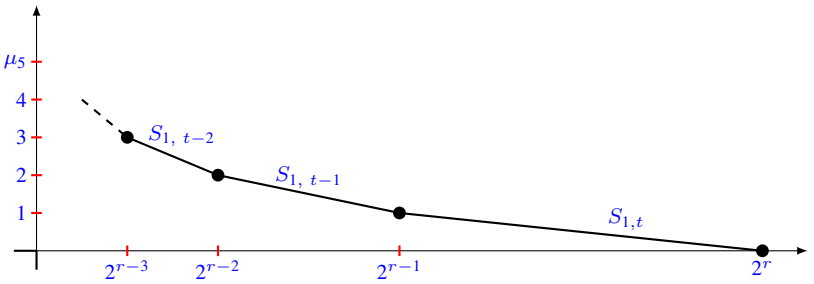

Figure 1. $N^+_{\phi_1}(F)$, where $r\geq 3$, $a\equiv 0 \pmod{32}$, and $1+b\equiv 0 \pmod{32}$

Proof of Theorem 1.6. In all cases, we prove that K is not monogenic by showing that 2 divides $i(K)$. Since in all cases, 2 divides a and does not divide b, $\overline{F(x)}=\overline{(x-1)}^{2^r}$ in $\mathbb{F}_2[x]$. Write

$$\begin{aligned} F(x) &= (x-1+1)^{2^r}+a(x-1+1)+b \\ &= (x-1)^{2^r}+\sum_{j=2}^{2^r-1}\binom{2^r}{j}(x-1)^j+(2^r+a)(x-1)+1+a+b. \end{aligned} \tag{3.2}$$

Let $\phi_1(x)=x-1$, $\mu=\nu_2(2^r+a)$, and $\nu=\nu_2(1+a+b)$. It follows that by the above ϕ_1- adic development (3.2) of $F(x)$ that the principal Newton polygon $N^+_{\phi_1}(F)$ with respect to ν_2 is the Newton polygon joining the points $\{(0,\nu),(1,\mu)\}\cup\{(2^j,r-\nu_2(j)),j=1,\dots,r\}$.

(i) If $r\geq 3$, $a\equiv 4 \pmod 8$ and $b\equiv 3 \pmod 8$, then $\mu=2$ and $\nu\geq 3$. It follows that $N^+_{\phi_1}(F)=S_{11}+S_{12}+S_{13}$ has three distinct sides of degree 1 each joining the points $(0,\nu),(1,2),(2^{r-1},1)$ and $(2^r,0)$ in the euclidean plane (see Figure 2 for an example with $r=5$). Thus, $R_{\lambda_{1k}}(F)(y)=1+y$, for $k=1,2,3$, is irreducible in $\mathbb{F}_{\phi_1}[y]\simeq\mathbb{F}_2[y]$ as it is of degree 1.- So, $F(x)$ is 2-regular. Applying Theorem 2.2, one gets:

$$2\mathbb{Z}_K=\mathfrak{p}_{111}\cdot\mathfrak{p}_{121}^{2^{r-1}-1}\cdot\mathfrak{p}_{131}^{2^{r-1}},$$

where p_{1k1} is a prime ideal of $\mathbb{Z}_K$ of residue degree $f(\mathfrak{p}_{1k1}/2)=1$, for $k=1,2,3$. So, there are three distinct prime ideals of $\mathbb{Z}_K$ of residue degree 1 each lying above 2. Applying Lemma 3.1 for $p=2$ and $f=1$, we see that 2 divides $i(K)$. Consequently, K cannot be monogenic.

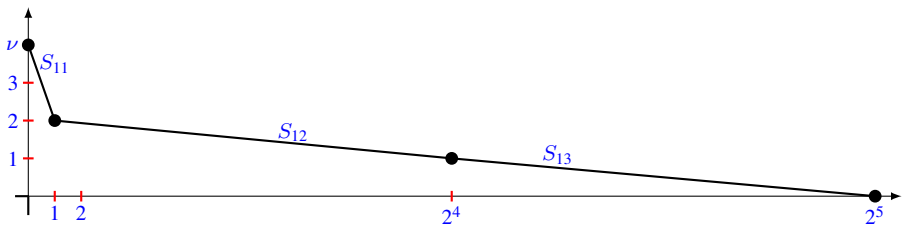

Figure 2. $N^+_{\phi_1}(F)$ with respect to ν_2, where $r=5$, $a\equiv 4 \pmod 8$ and $b\equiv 3 \pmod 8$.

(ii) If $r\geq 4$, $a\equiv 8 \pmod{16}$ and $b\equiv 7 \pmod{16}$, then $\mu=3$ and $\nu\geq 4$. It follows that $N^+_{\phi_1}(F)=S_{11}+S_{12}+S_{13}+S_{14}$ has four distinct sides of degree 1 each joining the points $(0,\nu),(1,3),(2^{r-2},2),(2^{r-1},1)$, and $(2^r,0)$ in the euclidean plane with respective slopes $\lambda_{11}\leq -1,\lambda_{12}=\frac{-1}{2^{r-1}-1},\lambda_{13}=\frac{-1}{2^{r-2}}$, and $\lambda_{14}=\frac{-1}{2^{r-1}}$ (as an example, see Figure 3 for $r=6$). Thus, $R_{\lambda_{1k}}(F)(y)$, for $k=1,2,3,4$ is irreducible over $\mathbb{F}_{\phi_1}\simeq\mathbb{F}_2$ as it is of degree 1. It follows that $F(x)$ is 2-regular. By using Theorem 2.2, we see that

$$2\mathbb{Z}_K=\mathfrak{p}_{111}\cdot\mathfrak{p}_{121}^{2^{r-2}-1}\cdot\mathfrak{p}_{131}^{2^{r-2}}\cdot\mathfrak{p}_{141}^{2^{r-1}},$$

where $\mathfrak{p}_{1k1}, k = 1, 2, 3, 4$, are four distinct prime ideals of $\mathbb{Z}_K$ of residue degree $f(\mathfrak{p}_{1k1}/2) = 1$. Thus, for $p = 2$, we have $L_2(1) = 4 > N_2(1) = 2$. By using Lemma 3.1, 2 divides $i(K)$. Hence, K cannot be monogenic.

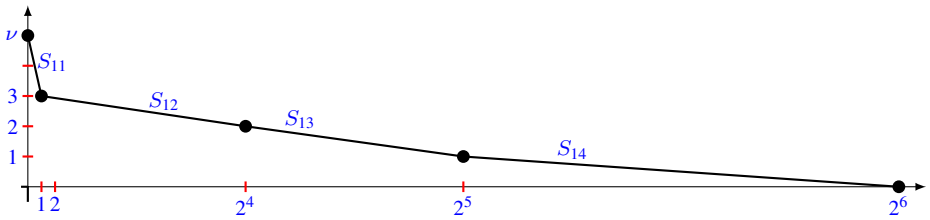

Figure 3. $N_{\phi_1}^+(F)$ with respect to ν_2, where $r = 6$, $a \equiv 8 \pmod{16}$, and $b \equiv 7 \pmod{16}$.

(iii) The case $r = 3$ was previously studied in [3, Theorem 2.3 (2)]; we have shown that 2 divides $i(K)$. Moreover, by Theorem 1.5, if $r \geq 3$, $a \equiv 0 \pmod{32}$, and $b \equiv -1 \pmod{32}$, then K is not monogenic. Assume now that $r \geq 4, a \equiv 16 \pmod{32}$, and $b \equiv 15 \pmod{32}$. Then $\mu \geq 4$ and $\nu \geq 5$. Thus,

$$N_{\phi_1}^+(F) = S_{11} + \cdots + S_{1,\,t-2} + S_{1,\,t-1} + S_{1,t}$$

has t distinct sides with $t \geq 4$. The last three sides have degree 1 each. More precisely, for $k = 0, 1, 2$, $S_{1,\,t-k}$ is the side joining the points $(2^{r-k-1}, k+1)$ and $(2^{r-k}, k)$. Their respective slopes are: $\lambda_{1,\,t-2} = \dfrac{-1}{2^{r-3}}$, $\lambda_{1,\,t-1} = \dfrac{-1}{2^{r-2}}$, and $\lambda_{1,t} = \dfrac{-1}{2^{r-1}}$. It follows that $R_{\lambda_{1,\,t-k}}(F)(y)$ is irreducible in $\mathbb{F}_{\phi_1}[y]$ as it is of degree 1 for $k = 0, 1, 2$. Hence, $F(x)$ is 2-regular. By applying Theorem 2.2, one has:

$$2\mathbb{Z}_K = \mathfrak{p}_{1,t-2,1}^{2^{r-1}} \cdot \mathfrak{p}_{1,t-1,1}^{2^{r-2}} \cdot \mathfrak{p}_{1,t,1}^{2^{r-3}} \cdot \mathfrak{a},$$

where $\mathfrak{a}$ is a proper ideal of $\mathbb{Z}_K$ provided by the other sides of $N_\phi^+(F)$, and $\mathfrak{p}_{1,t-k,1}$ is a prime ideal of $\mathbb{Z}_K$ of residue degree $f(\mathfrak{p}_{1,t-k,1}/2) = 1$ for $k = 1, 2, 3$. Hence, there exist at least three distinct prime ideals of $\mathbb{Z}_K$ lying above 2, each having residue degree 1. By Lemma 3.1, 2 divides $i(K)$. Consequently, K cannot be monogenic.

□

To illustrate our results, we give some numerical examples.

Examples 3.3.
Let $K = \mathbb{Q}(\theta)$ be a number field generated by a root of a monic irreducible polynomial $F(x) = x^{2^r} + ax^m + b$.

(i) If $F(x) = x^8 + 12x + 3$, then $F(x)$ is irreducible as it is a 3-Eisenstein polynomial. By Theorem 1.6 (1), the field K cannot be monogenic. Further, since the polynomial $F(x)$ is 2-regular, by [21], a 2-integral basis of K is given by $(1, \theta, \theta^2, \theta^3, \frac{35+\theta^4}{2}, \frac{21+15\theta+3\theta^4+\theta^5}{2}, \frac{7+5\theta^2+3\theta^4+2\theta^5+\theta^6}{2}, \frac{13+\theta+\theta^2+\theta^3+\theta^4+\theta^5+\theta^6+\theta^7}{4})$. Let $I_2(x_2, x_3, \ldots, x_8) = \pm 1$ be the 2-index form equation associated to the above 2-integral basis of K which is a Diophantine equation of degree 28 in 7 variables, where the coefficients are in $\mathbb{Z}_{(2)}$; the localization of $\mathbb{Z}$ at $p = 2$ (see [13, 17, 18]). This equation has no solution due to K being non-monogenic.

(ii) If $F(x) = x^{16}+24x^{15}+8$, then $\Delta(F) = 2^{90}\times 7\times 43\times 29778017378311761855723790106195659$. By Corollary 1.3, $F(x)$ is not monogenic, but K is monogenic and $\alpha = \frac{\theta^{11}}{4}$ generates a power integral basis of $\mathbb{Z}_K$.

(iii) The pure number field $\mathbb{Q}(\sqrt[64]{65})$ is not monogenic.

References

[1] S. Ahmad, T. Nakahara and A. Hameed, *On certain pure sextic fields related to a problem of Hasse*, Int. J. Algebra Comput., **26**, 577–583, (2016).

[2] T. Arnóczki and G. Nyul, *On a conjecture concerning the minimal index of pure quartic fields*, Publ. Math. Debrecen, **104**, 471–478, (2024).

[3] H. Ben Yakkou, *On monogenity of certain number fields defined by* $x^8 + ax + b$, Acta Math. Hungar., **166**, 614–623, (2022).

[4] H. Ben Yakkou, *On non-monogenic number fields defined by trinomials of type* $x^n + ax^m + b$, Rocky Mt. J. Math., **53**, 685–699, (2023).

[5] H. Ben Yakkou, *On common index divisors and monogenity of septic number fields defined by trinomials of type* $x^7 + ax^2 + b$, Acta Math. Hungar., **172**, 378–399, (2024).

[6] H. Ben Yakkou, *On common index divisors and monogenity of septic number fields defined by trinomials of type* $x^7 + ax^5 + b$, Math. Bohem., **150**, 245–262, (2025).

[7] H. Ben Yakkou and J. Didi, *On monogenity of certain pure number fields of degrees* $2^r \cdot 3^k \cdot 7^s$, Math. Bohem., **149**, 167–183, (2024).

[8] H. Ben Yakkou and L. El Fadil, *On monogenity of certain pure number fields defined by* $x^{p^r} - m$, Int. J. Number Theory, **17**, 2235–2242, (2021).

[9] H. Ben Yakkou and L. E. Fadil, *On monogenity of certain number fields defined by trinomials*, Funct. Approx. Comment. Math., **67**, 199–221, (2022).

[10] H. Ben Yakkou and Tiebekabe, *On common index divisors and not monogenity of nonic number fields defined by trinomials of type* $x^9 + ax + b$, Bol. Soc. Mat. Mex., **30, 44**, (2024).

[11] Y. Bilu, I. Gaál and K. Győry, *Index form equations in sextic fields: a hard computation*, Acta Arith., **115**, 85–96, (2004).

[12] A. Bérczes, J. H. Evertse and K. Győry, *Multiply monogenic orders*, Ann. Sc. Norm. Super. Pisa Cl. Sci., **(5), 12(2)**, 467–497, (2013).

[13] C. T. Davis and B. K. Spearman, *The index of quartic field defined by a trinomial* $x^4 + ax + b$, J. Algebra Appl., **17**, Article ID 1850197, 18 pp, (2018).

[14] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Göttingen Abhandlungen, **23**, 1–23, (1878).

[15] H. T. Engstrom, *On the common index divisors of an algebraic number field*, Trans. Amer. Math. Soc., **32**, 223–237, (1930).

[16] J. H. Evertse and K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge Univ. Press (2015).

[17] J. H. Evertse and K. Győry, *Discriminant Equations in Diophantine Number Theory*, Cambridge Univ. Press (2017).

[18] I. Gaál, *Diophantine Equations and Power Integral Bases, Theory and Algorithm*, 2nd ed., Birkhäuser, Boston, (2019).

[19] I. Gaál and K. Győry, *Index form equations in quintic fields*, Acta Arith., **89**, 379–396, (1999).

[20] J. Guàrdia, J. Montes and E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, J. Théor. Nombres Bordeaux, **23**, 667–696, (2011).

[21] J. Guàrdia, J. Montes and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc., **364**, 361–416, (2012).

[22] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith., **23**, 419–426, (1973).

[23] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donne III*, Publ. Math. Debrecen, **23**, 141–165, (1976).

[24] K. Győry, *On polynomials with integer coefficients and given discriminant, IV*, Publ. Math. Debrecen, **25**, 155–167, (1978).

[25] K. Győry, *Corps de nombres algébriques d'anneau d'entiers monogène*, In: "Séminaire Delange-Pisot-Poitou", 20e année: 1978/1979. Théorie des nombres, Fasc. 2 (French), Secrétariat Math., Paris, 1980, pp. Exp. No. 26, 7.

[26] K. Győry, *On discriminants and indices of integers of an algebraic number field*, J. Reine Angew. Math., **324**, 114–126, (1981).

[27] K. Győry, *Bounds for the solutions of decomposable form equations*, Publ. Math. Debrecen, **52**, 1–31, (1998).

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

[29] L. Jones, *Infinite families of non-monogenic trinomials*, Acta Sci. Math., 95–105, (2021).

[30] L. Jones and T. Phillips, *Infinite families of monogenic trinomials and their Galois groups*, Int. J. Math., **29**, Article ID 1850039, 11pp, (2018).

[31] O. Kchit, *On integral bases and monogenity of certain pure number fields defined by* $x^{p^r} - a$, Palest. J. Math., **13**, 18–29, (2024).

[32] P. Llorente and E. Nart, *Effective determination of the rational primes in a cubic field*, Proc. Amer. Math. Soc., **87**, 579–585, (1983).

[33] J. Montes and E. Nart, *On a theorem of Ore*, J. Algebra, **146**, 318–334, (1992).

[34] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, (2004).

[35] E. Nart, *On the index of a number field*, Trans. Amer. Math. Soc., **289**, 171–183, (1985).

[36] J. Odjoumani, A. Togbé and V. Ziegler, *On a family of biquadratic fields that do not admit a unit power integral basis*, Publ. Math. Debrecen, **94**, 1–19, (2019).

[37] Ø. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann., **99**, 84–117, (1928).

[38] A. Pethő and M. Pohst, *On the indices of multiquadratic number fields*, Acta Arith., **153**, 393–414, (2012).

[39] A. Pethő and V. Ziegler, *On biquadratic fields that admit unit power integral basis*, Acta Math. Hungar., **133**, 221–241, (2011).

[40] M. Taljaoui and M. Bouhamza, *Integral bases of some families of quartic number fields*, Palest. J. Math., **12**, 475–486, (2023).

Author information

Hamid Ben Yakkou, Polydisciplinary Faculty of Béni-Mellal, University Sultan Moulay Slimane, Morocco.
E-mail: beyakouhamid@gmail.com

Received: 2024-11-26
Accepted: 2025-06-25