Mathematica Bohemica

Hamid Ben Yakkou; Jalal Didi

On monogenity of certain pure number fields of degrees $2^r \cdot 3^k \cdot 7^s$

Mathematica Bohemica, Vol. 149 (2024), No. 2, 167–183

Persistent URL: http://dml.cz/dmlcz/152466

ON MONOGENITY OF CERTAIN PURE NUMBER FIELDS OF DEGREES $2^r \cdot 3^k \cdot 7^s$

Hamid Ben Yakkou, Jalal Didi, Fez

Received May 29, 2022. Published online March 27, 2023.
Communicated by Clemens Fuchs

Abstract. Let $K = \mathbb{Q}(\alpha)$ be a pure number field generated by a complex root α of a monic irreducible polynomial $F(x) = x^{2^r \cdot 3^k \cdot 7^s} - m \in \mathbb{Z}[x]$, where r, k, s are three positive natural integers. The purpose of this paper is to study the monogenity of K. Our results are illustrated by some examples.

Keywords: power integral basis; theorem of Ore; prime ideal factorization; common index divisor

MSC 2020: 11R04, 11R16, 11R21

1. Introduction

Let K be a number field generated by a complex root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$ of degree n and $\mathbb{Z}_K$ its ring of integers which is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$. If $\mathbb{Z}_K$ has a power integral basis $(1, \theta, \dots, \theta^{n-1})$ for some $\theta \in \mathbb{Z}_K$; $\mathbb{Z}_K = \mathbb{Z}[\theta]$, then the field K is said to be monogenic. Otherwise, K is called not monogenic. Recall that for any $\theta \in \mathbb{Z}_K$, the abelian quotient group $\mathbb{Z}_K/\mathbb{Z}[\theta]$ is finite. Its cardinal order is called the index of $\mathbb{Z}[\theta]$, which we denote by $(\mathbb{Z}_K : \mathbb{Z}[\theta])$. The index of the field K is

$$i(K) = \gcd\{(\mathbb{Z}_K : Z[\theta]),\ \theta \in \mathbb{Z}_K \text{ and } K = \mathbb{Q}(\theta)\}.$$

A rational prime integer p dividing $i(K)$ is called a prime common index divisor of K. If $\mathbb{Z}_K$ has a power integral basis, then $i(K) = 1$. Thus, if there is a prime common index divisor of K, then K is not monogenic. The problem of studying the monogenity of number fields is called the problem of Hasse (see [11], [19]). It

DOI: 10.21136/MB.2023.0071-22

is one of the most important problems in algebraic number theory. This problem is the subject of many studies and is of interest to several researchers. Let us recall some previous works regarding this problem. In [13], Gaál and Remete calculated the elements of index 1 in pure quartic number fields $\mathbb{Q}(\sqrt[4]{m})$ for $1 < m < 10^7$ and $m \equiv 2, 3 \pmod 4$. In [12], Gaál and Győry described an algorithm to solve index form equations in quintic number fields and they computed all generators of power integral bases in some totally real quintic fields with the Galois group S_5. In [4], Bilu, Gaál and Győry studied the monogenity of some totally real sextic number fields with the Galois group S_6. In [2], Ahmad, Nakahara and Husnine proved that if $m \equiv 2, 3 \pmod 4$ and $m \neq \pm 1 \pmod 9$, then the pure sextic number field $\mathbb{Q}(\sqrt[6]{m})$ is monogenic.

On the other hand, if $m \equiv 1 \pmod 4$ and $m \not\equiv \pm 1 \pmod 9$, then it is not monogenic (see [1]). Also, Hameed and Nakahara proved that if $m \equiv 1 \pmod 4$, then the octic number field $\mathbb{Q}(\sqrt[8]{m})$ is not monogenic, but if $m \equiv 2, 3 \pmod 4$, then it is monogenic (see [18]). In [14], Gaál and Remete obtained, by applying the explicit form of the index equation, new deep results on monogenity of number fields $\mathbb{Q}(\sqrt[n]{m})$, where $3 \leqslant n \leqslant 9$ and m is a square-free rational integer. They also showed in [15] that if $m \equiv 2$ or $3 \pmod 4$ is a square-free rational integer, then the octic number field $K = \mathbb{Q}(i, \sqrt[4]{m})$ is not monogenic. Also in [23], Pethő and Pohst studied indices in multiquadratic number fields.

The aim of this paper is to study the monogenity of a pure number field K generated by a complex root α of a monic irreducible polynomial $F(x) = x^{2^r \cdot 3^k \cdot 7^s} - m$ with $m \neq \pm 1$ being a rational integer. Recall that in [7], [10], El Fadil et al. studied the cases $r = 0$ and $s = 0$, respectively. Also in [8], El Fadil, Ben Yakkou and Didi studied the special case $r = k = s = 1$. We also note that we based our method on Newton polygon techniques applied on prime ideal factorization.

2. Main results

Let K be a pure number field generated by a complex root α of a monic irreducible polynomial $F(x) = x^{2^r \cdot 3^k \cdot 7^s} - m \in \mathbb{Z}[x]$, where $m \neq \pm 1$ is a rational integer, and r, k and s are three positive natural integers. The following theorem gives necessary and sufficient conditions for $\mathbb{Z}_K = \mathbb{Z}[\alpha]$.

Theorem 2.1. *The ring $\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if m is square-free, $m \not\equiv 1 \pmod 4$, $m \not\equiv \pm 1 \pmod 9$ and $\overline{m} \notin \{\pm 1, \pm 18, \pm 19\} \pmod{49}$. In this case, K is monogenic and α generates a power integral of $\mathbb{Z}_K$.*

R e m a r k 2.2. Note that significant Gassert's result (see [16], Theorem 1.1) yields only one way and cannot guarantee the equivalence. However, Theorem 2.1 above gives the wanted equivalence in the context of pure number fields of degrees $2^r \cdot 3^k \cdot 7^s$. The reader can also see Corollary 1.3 of [20]. In this paper, we prove the above theorem since its proof is useful for the proof of Theorem 2.3.

According to Theorem 2.1, if m is not square-free, $m \equiv 1 \pmod 4$, $m \equiv \pm 1 \pmod 9$ or $\overline{m} \notin \{\pm 1, \pm 18, \pm 19\} \pmod{49}$, then α does not generate a power integral basis of $\mathbb{Z}_K$. Henceforth, Theorem 2.1 cannot decide on the monogenity of K. The following theorem gives a partial answer. It produces infinite families of non-monogenic pure number fields defined by $x^{2^r \cdot 3^k \cdot 7^s} - m$, i.e., $\mathbb{Z}_K$ has no power integral basis.

Theorem 2.3. *Under the above hypothesis, if one of the conditions*
(1) $m \equiv 1 \pmod 4$,
(2) (a) $m \equiv 1 \pmod 9$,
    (b) $r \geqslant 2$ *and* $m \equiv -1 \pmod 9$,
    (c) $r = 1$ *and* $m \equiv -1 \pmod{81}$,
(3) (a) $m \equiv 1 \pmod{49}$,
    (b) $r = 1$, $s \geqslant 7$ *and* $m \equiv -1 \pmod{7^8}$,
    (c) $r \geqslant 2$, $s \geqslant 3$ *and* $m \equiv -1 \pmod{7^4}$
holds, then K is not monogenic.

As a consequence of the two previous theorems, the following result gives an important characterization of the monogenity of some special pure number fields of degrees $2^r \cdot 3^k \cdot 7^s$.

Corollary 2.4. *Let K be a pure number field generated by a complex root of a monic irreducible polynomial $x^{2^r \cdot 3^k \cdot 7^s} - m^t$, where $m \neq \pm 1$ is a square-free rational integer and t a positive integer which is coprime to 42. Then the following hold.*
(1) *If $m \not\equiv 1 \pmod 4$, $m \not\equiv \pm 1 \pmod 9$ and $\overline{m} \notin \{\pm 1, \pm 18, \pm 19\} \pmod{49}$, then K is monogenic.*
(2) *If $m \equiv 1 \pmod 4$, then K is not monogenic.*
(3) *If* (a) $m \equiv 1 \pmod 9$,
    (b) $r \geqslant 2$ *and* $m \equiv -1 \pmod 9$,
    (c) $r = 1$ *and* $m \equiv -1 \pmod{81}$
    then K is not monogenic.
(4) *If* (a) $m \equiv 1 \pmod{49}$,
    (b) $r = 1$, $s \geqslant 7$ *and* $m \equiv -1 \pmod{7^8}$,
    (c) $r \geqslant 2$, $s \geqslant 3$ *and* $m \equiv -1 \pmod{7^4}$
    then K is not monogenic.

3. Preliminaries

To prove our results, we based our method on prime ideal factorization. Let p be a rational prime integer. In 1878, Dedekind gave the explicit factorization of the principal ideal $p\mathbb{Z}_K$ when p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\theta])$ for some $\theta \in \mathbb{Z}_K$ (see [6] and [21], Theorem 4.33). He also gave a criterion known as Dedekind's criterion to test the divisibility of the index $(\mathbb{Z}_K : \mathbb{Z}[\theta])$ by p (see [5], Theorem 6.14, [6] and [21]). When p divides $i(K)$, then Dedekind's theorem cannot give the prime ideal factorization of $p\mathbb{Z}_K$. In 1928, Ore developed an algorithm to factorize $p\mathbb{Z}_K$. His method is based on Newton polygon techniques. The papers [9], [17] and [22] give a detailed survey on the theory and applications of Newton polygon techniques, including prime ideal factorization in number fields. Now, let us recall some fundamental notions on Newton polygon techniques. Let ν_p be the discrete valuation of $\mathbb{Q}_p(x)$ defined on $\mathbb{Z}_p[x]$ by

$$\nu_p\Big(\sum_{i=0}^{r} a_i x^i\Big) = \min\{\nu_p(a_i)\colon\ 0 \leqslant i \leqslant r\}.$$

Let $\varphi(x) \in \mathbb{Z}[x]$ be a monic polynomial whose reduction modulo p is irreducible. By successive Euclidean divisions, any monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$ admits a unique φ-adic development

$$F(x) = a_0(x) + a_1(x)\varphi(x) + \ldots + a_n(x)\varphi(x)^n$$

with $\deg(a_i(x)) < \deg(\varphi(x))$. For every $0 \leqslant i \leqslant n$, let $u_i = \nu_p(a_i(x))$. The φ-Newton polygon of $F(x)$ is the lower boundary convex envelope of the set of points

$$\{(i, u_i)\colon\ 0 \leqslant i \leqslant n,\ a_i(x) \neq 0\}$$

in the Euclidean plane, which we denote by $N_\varphi(F)$. The polygon $N_\varphi(F)$ 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 write $N_\varphi(F) = S_1 + S_2 + \ldots + S_g$. The polygon determined by the sides of negative slopes of $N_\varphi(F)$ is called the φ-principal Newton polygon of $F(x)$ and is denoted by $N_\varphi^+(F)$. Recall that the length of $N_\varphi^+(F)$ is $l(N_\varphi^+(F)) = \nu_{\overline{\varphi}}(\overline{F(x)})$, the highest power of $\varphi(x)$ dividing $F(x)$ modulo p. Let $\mathbb{F}_\varphi$ be the finite residue field $\mathbb{Z}[x]/(p, \varphi(x)) \simeq \mathbb{F}_p[x]/(\overline{\varphi(x)})$. We attach to any abscissa $0 \leqslant i \leqslant l(N_\varphi^+(F))$, the residue coefficient

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

Let S be one of the sides of $N_\varphi^+(F)$ and $\lambda = -h/e$ be its slope, where e and h are two positive coprime integers. The length of S, denoted $l(S)$, is the length of its projection to the horizontal axis. The degree of S is $d = d(S) = l(S)/e$; it is equal to the number of segments into which the integral lattices divide S. More precisely, if (s, u_s) is the initial point of S, then the points with integer coordinates lying in S are exactly

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

We attach to S the residual polynomial defined by

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

The φ-index of $F(x)$, denoted $\mathrm{ind}_\varphi(F)$, is $\deg(\varphi)$ times the number of points with natural integer coordinates that lie below or on the polygon $N_\varphi^+(F)$, strictly above the horizontal axis and strictly beyond the vertical axis (see Figure 1). We say that the polynomial $F(x)$ is φ-regular with respect to p if for each side S of $N_\varphi^+(F)$ of slope λ, its associated residual polynomial $R_\lambda(F)(y)$ is separable in $\mathbb{F}_\varphi[y]$. The polynomial $F(x)$ is said to be p-regular if $F(x)$ is φ_i-regular for every $1 \leqslant i \leqslant t$, where $\overline{F(x)} = \prod_{i=1}^{t} \overline{\varphi_i(x)}^{l_i}$ is 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 $N_{\varphi_i}^+(F) = S_{i1} + \ldots + S_{ir_i}$ 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 $\mathbb{F}_{\varphi_i}[y]$.

Now, we state the theorem of Ore, which plays a significant role in the proof of our results (see [9], Theorem 1.7 and Theorem 1.9; [17] and [22]).

Theorem 3.1 (Ore's theorem)**.** *Under the above notations, we have*

(1)
$$\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) \geqslant \sum_{i=1}^{t} \mathrm{ind}_{\varphi_i}(F).$$

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

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

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

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

Corollary 3.2. *Under the hypothesis of the above theorem, if for every* $i = 1, \dots, t$, $l_i = 1$ *or* $N^+_{\varphi_i}(F) = S_i$ *has a single side of height* 1, *then* p *does not divide* $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$.

Example 3.3. Consider the monic irreducible polynomial $F(x) = x^6 + 153x + 17$, which factors in $\mathbb{F}_3[x]$ into $\overline{F(x)} = (\overline{\varphi_1(x)\varphi_2(x)})^3$, where $\varphi_1(x) = x - 1$ and $\varphi_2(x) = x + 1$. The φ_1-development of $F(x)$ is

$$f(x) = 171 + 159\varphi_1(x) + 15\varphi_1(x)^2 + 20\varphi_1(x)^3 + 15\varphi_1(x)^4 + 6\varphi_1(x)^5 + \varphi_1(x)^6,$$

and the $\varphi_2(x)$-adic development of $F(x)$ is

$$F(x) = -135 + 129\varphi_2(x) + 15\varphi_2(x)^2 - 20\varphi_2(x)^3 + 15\varphi_2(x)^4 - 6\varphi_2(x)^5 + \varphi_2(x)^6.$$

It follows that $N^+_{\varphi_i}(F) = S_{i1} + S_{i2}$ with respect to ν_3 has two sides with $d(S_{i1}) = d(S_{i2}) = 1$ (see Figure 1). Thus, the residual polynomials $R_{\lambda_{it}}(F)(y)$ attached to the sides of $N^+_{\varphi_i}(F)$ are irreducible in $\mathbb{F}_{\varphi_i}[y] \simeq \mathbb{F}_3[y]$ as they are of degree 1 for every $i = 1, 2$ and $t = 1, 2$. Thus $F(x)$ is φ_i-regular for $i = 1, 2$, hence it is 3-regular. By Theorem 3.1,

$$\nu_3((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \mathrm{ind}_{\varphi_1}(F) + \mathrm{ind}_{\varphi_2}(F) = 1 + 1 = 2$$

and

$$3\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}^2\mathfrak{p}_{211}\mathfrak{p}_{221}^2$$

with the residue degree $f(\mathfrak{p}_{ij1}/3) = 1$ for every $i = 1, 2$ and $j = 1, 2$.

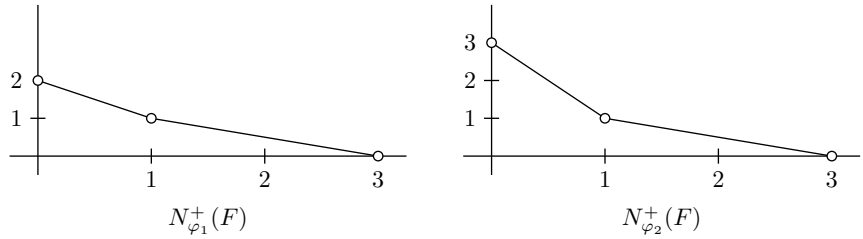

Figure 1. $N^+_{\varphi_i}(F)$, $i = 1, 2$.

In order to prove theorem of the product, Guàrdia, Montes and Nart introduced in [17] the notion of φ-admissible development. In this paper we use this technique in order to treat some special cases when the φ-adic development of a given polynomial $F(x)$ is not obvious. Let

$$F(x) = \sum_{j=0}^{n} A_j(x)\varphi(x)^j, \quad A_j(x) \in \mathbb{Z}_p[x] \tag{3.1}$$

be a φ-development of $F(x)$, not necessarily the φ-adic one. Take $\omega_j = \nu_p(A_j(x))$ for all $0 \leqslant j \leqslant n$. Let N be the principal Newton polygon of the set of points $\{(j, \omega_j)\colon\ 0 \leqslant j \leqslant n,\ \omega_j \neq \infty\}$. To any $0 \leqslant j \leqslant n$, we attach a residual coefficient

$$c'_j = \begin{cases} 0 & \text{if } (j, \omega_j) \text{ lies strictly above } N, \\ \dfrac{A_j(x)}{p^{\omega_j}} \pmod{(p, \varphi(x))} & \text{if } (j, \omega_j) \text{ lies on } N. \end{cases}$$

Moreover, for any side S of N with slope λ, we define the residual polynomial associated to S and denoted $R'_\lambda(F)(y)$ (similar to the residual polynomial $R_\lambda(F)(y)$ defined from the φ-adic development). We say that a φ-development (3.1) of $F(x)$ is admissible if $c'_j \neq 0$ for each abscissa j of a vertex of N. Note that $c'_j \neq 0$ if and only if $\overline{\varphi(x)}$ does not divide $\overline{(A_j(x)/p^{\omega_j})}$. For more details, see [17]. The following lemma shows an important relationship between the φ-adic development and any φ-admissible development of a given polynomial $F(x)$.

Lemma 3.4 ([17], Lemma 1.12)**.** *If a φ-development of $F(x)$ is admissible, then $N^+_\varphi(F) = N$ and $c'_j = c_j$. In particular, for any segment S of N with slope λ we have $R'_\lambda(F)(y) = R_\lambda(F)(y)$ (up to the multiplication by a nonzero element of $\mathbb{F}_\varphi$).*

4. Proofs

In order to prove our theorems, we need the following lemma which gives the p-adic valuation of the binomial coefficient $\binom{p^r}{j}$. For the proof, refer to [3].

Lemma 4.1. *Let p be a rational prime integer and r a positive integer. Then*

$$\nu_p\left(\binom{p^r}{j}\right) = r - \nu_p(j)$$

for any integer $j = 1, \ldots, p^r - 1$.

P r o o f of Theorem 2.1. Let $D(\alpha)$ be the discriminant of the algebraic integer α and D_K the field discriminant of K. Since $F(x)$ is the minimal polynomial of α over $\mathbb{Q}$, by [21], Propositions 2.9 and 2.13, one has

$$\begin{aligned} (4.1)\quad D(\alpha) &= D(1, \alpha, \ldots, \alpha^{2^r \cdot 3^k \cdot 7^s - 1}) = (-1)^{2^r \cdot 3^k \cdot 7^s (2^r \cdot 3^k \cdot 7^s - 1)/2} N_{K/\mathbb{Q}}(F'(\alpha)) \\ &= \pm N_{K/\mathbb{Q}}(2^r \cdot 3^k \cdot 7^s \cdot \alpha^{2^r \cdot 3^k \cdot 7^s - 1}) \\ &= \pm (2^r \cdot 3^k \cdot 7^s)^{2^r \cdot 3^k \cdot 7^s} \cdot N_{K/\mathbb{Q}}(\alpha)^{2^r \cdot 3^k \cdot 7^s - 1} \\ &= \pm (2^r \cdot 3^k \cdot 7^s)^{2^r \cdot 3^k \cdot 7^s} \cdot m^{2^r \cdot 3^k \cdot 7^s - 1} = (\mathbb{Z}_K : \mathbb{Z}[\alpha])^2 \cdot D_K. \end{aligned}$$

Thus, $\mathbb{Z}[\alpha]$ is integrally closed if and only if p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ for every rational prime p dividing $2 \cdot 3 \cdot 7 \cdot m$. Let p be a rational prime dividing m, then $F(x) \equiv \varphi^{2^r \cdot 3^k \cdot 7^s} \pmod{p}$, where $\varphi = x$. The φ-principal Newton polygon of $F(x)$ with respect to ν_p, $N_\varphi^+(F) = S$ has a single side with slope $\lambda = -\nu_p(m)/(2^r \cdot 3^k \cdot 7^s)$; it is the side joining the points $(0, \nu_p(m))$ and $(2^r \cdot 3^k \cdot 7^s, 0)$. If $\nu_p(m) \geqslant 2$ (this means that m is not square-free), then by using Theorem 3.1, we have

$$\nu_p(\mathbb{Z}_K : \mathbb{Z}[\alpha]) \geqslant \operatorname{ind}_\varphi(F) = \frac{(2^r \cdot 3^k \cdot 7^s - 1)(\nu_p(m) - 1) + \gcd(2^r \cdot 3^k \cdot 7^s, \nu_p(m))}{2}$$

Consequently, p^2 divides the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ and α does not generate a power integral basis of $\mathbb{Z}_K$. If $\nu_p(m) = 1$ for every prime divisor of m (i.e., m is square-free), then $N_\varphi^+(F) = S$ has a single side of height 1 with slope $\lambda = -1/(2^r \cdot 3^k \cdot 7^s)$. Thus, the residual polynomial $R_\lambda(F)(y)$ is irreducible over $\mathbb{F}_\varphi \simeq \mathbb{F}_p$ as it is of degree 1. By Theorem 3.1, we get $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \operatorname{ind}_\varphi(F) = 0$, that is to say, p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. Now, we deal with the cases $p \in \{2, 3, 7\}$ when p does not divide m. Set $2^r \cdot 3^k \cdot 7^s = a \cdot p^u$, where $a = 2^r \cdot 3^k \cdot 7^s / p^u$ and p does not divide a. Since p does not divide $a \cdot m$, the polynomial $\overline{x^a - m}$ is separable in $\mathbb{F}_p[x]$. Fix a monic irreducible factor $\overline{\varphi(x)}$ of $\overline{F(x)}$ in $\mathbb{F}_p[x]$. Then $\overline{\varphi(x)}$ is a monic irreducible factor of the polynomial $\overline{x^a - m}$ in $\mathbb{F}_p[x]$. Moreover, for a suitable lifting $\varphi(x)$ of $\overline{\varphi(x)}$, there exist two polynomials $U(x)$ and $T(x) \in \mathbb{Z}[x]$ such that $x^a - m = \varphi(x)U(x) + pT(x)$, where $\overline{\varphi(x)}$ does not divide $\overline{U(x)T(x)}$. Set $\psi(x) = pT(x) + m$ and write

$$\begin{aligned} F(x) &= x^{2^r \cdot 3^k \cdot 7^s} - m = (x^a)^{p^u} - m = (\varphi(x)U(x) + \psi(x))^{p^u} - m \\ &= (\varphi(x)U(x))^{p^u} + \sum_{j=1}^{p^r - 1} \binom{p^u}{j} \psi(x)^{p^u - j} U(x)^j \varphi(x)^j + \psi(x)^{p^u} - m. \end{aligned}$$

By the binomial expansion and Lemma 4.1, we see that

$$\psi(x)^{p^u} = p^{u+1} H(x) + m^{p^u},$$

where

$$H(x) = m^{p^u - 1} T(x) + \frac{1}{p^{u+1}} \sum_{j=0}^{p^u - 2} \binom{p^u}{j} m^j (pT(x))^{p^u - j}.$$

It follows that

$$\begin{aligned} F(x) = (\varphi(x)U(x))^{p^u} &+ \sum_{j=1}^{p^u - 1} \binom{p^u}{j} \psi(x)^{p^u - j} U(x)^j \varphi(x)^j \\ &+ p^{u+1} H(x) + m^{p^u} - m. \end{aligned} \tag{4.2}$$

Let $V(x)$ and $R(x)$ be the quotient and the remainder upon the Euclidean division of $H(x)$ by $\varphi(x)$, respectively. Then, we have

$$(4.3)\quad F(x) = \sum_{j=2}^{p^u} \binom{p^u}{j} \psi(x)^{p^u-j} U(x)^j \varphi(x)^j + \left(\binom{p^u}{1} \psi(x)^{p^u-1} U(x) + p^{u+1} V(x) \right) \varphi(x) + p^{u+1} R(x) + m^{p^u} - m.$$

Thus $F(x) = \sum_{j=0}^{p^r} A_j(x) \varphi(x)^j$, where

$$\begin{cases} A_0(x) = p^{u+1} R(x) + m^{p^u} - m, \\ A_1(x) = \binom{p^u}{1} \psi(x)^{p^u-1} U(x) + p^{u+1} V(x), \\ A_j(x) = \binom{p^u}{j} \psi(x)^{p^u-j} U(x)^j \text{ for every } 2 \leqslant j \leqslant p^u. \end{cases}$$

Let $\nu = \nu_p(m^{p^u} - m)$. Note that as remarked in [3], if a rational prime integer p does not divide a nonzero rational integer m, then for every positive integer k, $\nu = \nu_p(m^{p^u} - m) = \nu_p(m^{p^{u-1}} - 1) = \nu_p(m^{p-1} - 1)$. Let $\omega_j = \nu_p(A_j(x))$ for every $j = 0, 2, \ldots, p^u$. Using Lemma 4.1, we see that $\omega_0 = \nu_p(p^{u+1} R(x) + m^{p^u} - m) \geqslant \min\{\nu, u+1\}$. Note that $\overline{\varphi(x)}$ does not divide $\overline{(A_0(x)/p^{\omega_0})}$ (because $\deg(R(x)) < \deg(\varphi(x))$). We also have $\omega_1 = u$ and $\overline{(A_1(x)/p^{\omega_1})} = \overline{\psi(x)^{p^u-1} \cdot U(x)}$. It follows that $\overline{\varphi(x)}$ does not divide $\overline{(A_1(x)/p^{\omega_1})}$. Moreover, for every $j = 2, 3, \ldots, p^u$, $\omega_j = u - \nu_p(j)$ and $\overline{(A_j(x)/p^{\omega_j})} = \left(\binom{p^u}{j}/p^{u-\nu_p(j)}\right) \cdot \overline{\psi(x)^{p^u-1} \cdot U(x)}$. So, $\overline{\varphi(x)}$ does not divide $\overline{(A_j(x)/p^{\omega_j})}$ for every $j = 0, 1, \ldots, p^r$. Thus, the φ-development (4.3) of $F(x)$ is admissible. By Lemma 3.4, $N_\varphi^+(F)$ is the Newton polygon joining the points $\{(0, \omega_0)\} \cup \{(p^j, k-j) \colon 0 \leqslant j \leqslant r\}$ in the Euclidean plane. If $\nu = 1$, then $N_\varphi^+(F)$ is the Newton polygon joining the points $(0, 1)$ and $(p^u, 0)$. In this case, by Theorem 3.1, we have

$$\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \sum_{i=0}^{t} \operatorname{ind}_{\varphi_i}(F) = 0,$$

where $\overline{\varphi_i(x)}$, $i = 1, \ldots, t$, are the monic irreducible factors of $\overline{F(x)}$ in $\mathbb{F}_p[x]$. Otherwise, if $\nu \geqslant 2$, we see that the point $(1, 1)$ with natural integer coordinates that lie below or on the polygon $N_\varphi^+(F)$, strictly above the horizontal axis and strictly beyond the vertical axis. By Theorem 3.1, we see that

$$\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) \geqslant \sum_{i=0}^{t} \operatorname{ind}_{\varphi_i}(F) \geqslant 1 \times t \geqslant 1.$$

This completes the proof. □

Recall that the field index of K is

$$i(K) = \gcd\{(Z_K : \mathbb{Z}[\theta]),\ \theta \in \mathbb{Z}_K \text{ generates } K\}.$$

A rational prime p dividing $i(K)$ is called a prime common index divisor of K. If $\mathbb{Z}_K$ has a power integral basis, then $i(K) = 1$. Thus a field possessing a prime common index divisor cannot be monogenic.

For the proof of Theorem 2.3, we use the following lemma, which gives a sufficient condition for a rational prime integer p to be a prime common index divisor of K; it is a consequence of a theorem of Dedekind (see [21], Theorems 4.33 and 4.34, and [6]).

Lemma 4.2. *Let p be a rational prime integer 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 $L_p(f) > N_p(f)$, then p is a common index divisor of K.*

R e m a r k 4.3. Note that the condition $i(K) = 1$ is not sufficient for the monogenity of K. The pure cubic number field $K = \mathbb{Q}(\sqrt[3]{175})$ is a simple example of the case $i(K) = 1$, but K is not monogenic as its index form equation equals $5x^3 - 7y^3$ and never assumes the values ± 1.

P r o o f of Theorem 2.3. In all cases, we show that K is not monogenic by showing that $i(K)$ is divisible by an adequate rational prime integer. Since p does not divide m, according to the equation (4.1) and the definition of $i(K)$, the rational prime candidates to divide $i(K)$ are $2, 3$ and 7.

(1) If $m \equiv 1 \pmod 4$, then $\overline{F(x)} = \overline{(x^{3^k\cdot 7^s} - 1)}^{2^r} = \overline{((x-1)(x^2+x+1)U(x))}^{2^r} \in \mathbb{F}_2[x]$, where $U(x) = \sum_{j=0}^{3^{k-1}\cdot 7^s - 1} (x^3)^{3^{k-1}\cdot 5^s - j}$. Set $\varphi_1(x) = x-1$ and $\varphi_2(x) = x^2+x+1$. Note that $\overline{(x^{3^k\cdot 7^s} - 1)}$ is separable in $\mathbb{F}_2[x]$ (because 2 does not divide $3^k \cdot 7^s$). It follows that $\overline{\varphi_i(x)}$ does not divide $\overline{U(x)}$ in $\mathbb{F}_2[x]$ for $i = 1, 2$. Write

$$\begin{aligned} (4.4)\ F(x) &= x^{2^r\cdot 3^k\cdot 7^s} - m = (x^{3^k\cdot 7^s} - 1 + 1)^{2^r} - m = (\varphi_1(x)\varphi_2(x)U(x) + 1)^{2^r} - m \\ &= (\varphi_1(x)\varphi_2(x)U(x))^{2^r} + \sum_{j=1}^{2^r-1} \binom{2^r}{j} (U(x)\varphi_1(x)\varphi_2(x))^j + 1 - m. \end{aligned}$$

Let $\nu = \nu_2(1-m)$, then $\nu \geqslant 2$. Since $\overline{\varphi_i(x)}$ does not divide $\overline{U(x)}$ in $\mathbb{F}_2[x]$ for $i = 1, 2$, the φ_i-development (4.4) of $F(x)$ is admissible for $i = 1, 2$. By Lemmas 3.4 and 4.1, we see that for $i = 1, 2$, the principal Newton polygon $N^+_{\varphi_i}(F)$ is the lower convex hull of the points $(0, \nu)$, $(1, r)$, $(2, r-1), \ldots$ and $(2^r, 0)$. Note also that $U(y) = 1 \pmod{(2, \varphi_2(x))}$. That is $U(y) = 1$ in the residual field $\mathbb{F}_{\varphi_2}[y]$.

Assume that $m \equiv 5 \pmod 8$, then $\nu = 2$. In this case, $N^+_{\varphi_i}(F) = S_{i1}$ has one side of degree 2 with the slope $\lambda_{i1} = -1/2^{r-1}$ and ramification index $e_{i1} = 2^{r-1}$ for $i = 1, 2$. More precisely, $N^+_{\varphi_i}(F) = S_{i1}$ is the lower convex hull of the points $(0, 2)$, $(2^{r-1}, 1)$ and $(2^r, 0)$ (see Figure 2).

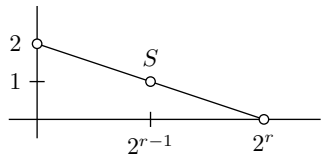

Figure 2. $N^+_{\varphi_i}(F), i = 1, 2$, when $m \equiv 5 \pmod 8$.

In this case the attached residual polynomials are $R_{\lambda_{11}}(F)(y) = 1 + y + y^2 \in \mathbb{F}_{\varphi_1}[y] \simeq \mathbb{F}_2[y]$ and

$$\begin{aligned} R_{\lambda_{21}}(F)(y) &= c_0 + c_e y + c_{2e} y^2 \\ &= 1 + (U(x)\varphi_1(x))^{2^{r-1}} y + (\varphi_1(x)U(x))^{2^r} y^2 \in \mathbb{F}_{\varphi_2}[y]. \end{aligned} \tag{4.5}$$

It follows that if r is odd, then

$$R_{\lambda_{21}}(F)(y) = 1 + (x+1)y + xy^2 = (y+1)(xy+1)$$

and, if r is even, then

$$R_{\lambda_{21}}(F)(y) = 1 + xy + (x+1)y^2 = (y+1)((1+x)y+1).$$

So, $R_{\lambda_{21}}(F)(y)$ is separable in $\mathbb{F}_{\varphi_2}[y]$. Then, $F(x)$ is φ_i-regular for $i = 1, 2$. Applying Theorem 3.1, one gets

$$2\mathbb{Z}_K = \mathfrak{p}_{111}^{2^{r-1}} \mathfrak{p}_{211}^{2^{r-1}} \mathfrak{p}_{212}^{2^{r-1}} \mathfrak{a},$$

where $\mathfrak{a}$ is a nonzero ideal of $\mathbb{Z}_K$ provided by the monic irreducible factors of $U(x)$ modulo 2 and $\mathfrak{p}_{i1k}$ is a prime ideal of $\mathbb{Z}_K$ of residue degree $f(\mathfrak{p}_{i1k}/2) = 2$ for $i = 1, 2$ and $k = 1, 2$. Thus, there are at least three prime ideals of residue degree 2 each, lying above 2 in $\mathbb{Z}_K$. As there is only one monic irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, namely $x^2 + x + 1$, by Lemma 4.2, 2 divides $i(K)$. So, K is not monogenic. Assume now that $m \equiv 9 \pmod{16}$, then $\nu = 3$. We discuss two cases: $r = 1$ and $r \geqslant 2$. If $r = 1$, then $N^+_{\varphi_i}(F) = S_{i1} + S_{i2}$ has two sides of degree 1 each, joining the points $(0, 3)$, $(1, 1)$ and $(2, 0)$ for $i = 1, 2$. Thus, the residual polynomial $R_{\lambda_{ik}}(F)(y)$ is irreducible in $\mathbb{F}_{\varphi_i}[y]$ for every $i = 1, 2$ and $k = 1, 2$. Applying Theorem 3.1, one has

$$2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}\mathfrak{p}_{211}\mathfrak{p}_{221}\mathfrak{a},$$

where $\mathfrak{a}$ is a nonzero ideal of $\mathbb{Z}_K$ provided by the monic irreducible factors of $U(x)$ modulo 2 and $\mathfrak{p}_{ikj}$ are prime ideals of $\mathbb{Z}_K$ with residue degrees

$$f(\mathfrak{p}_{111}/2) = f(\mathfrak{p}_{121}/2) = 1 \quad \text{and} \quad f(\mathfrak{p}_{211}/2) = f(\mathfrak{p}_{221}/2) = 2.$$

Thus, there are two prime ideals of $\mathbb{Z}_K$ of residue degree 2 each lying above 2. By Lemma 4.2, 2 divides $i(K)$. Consequently, K is not monogenic. Assume now that $r \geqslant 2$. In this case, $N^+_{\varphi_i}(F) = S_{i1} + S_{i2}$ has two sides with respective degrees $d(S_{i1}) = 2$ and $d(S_{i2}) = 1$ joining the points $(0, 3)$, $(2^{r-1}, 1)$ and $(2^r, 0)$ (see Figure 3).

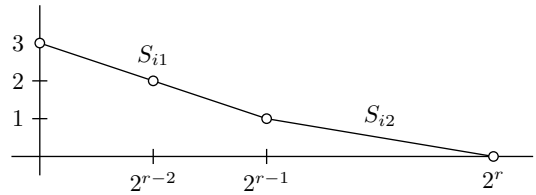

Figure 3. $N^+_{\varphi_i}(F), i = 1, 2$, when $r \geqslant 2$ and $m \equiv 9 \pmod{16}$.

In this case, we have $R_{\lambda_{11}}(F)(y) = 1+y+y^2$ which is irreducible in $\mathbb{F}_{\varphi_1}[y] \simeq \mathbb{F}_2[y]$. We also have that $R_{\lambda_{22}}(F)(y) = 1 + y$ which is irreducible in $\mathbb{F}_{\varphi_2}[y]$. Applying Theorem 3.1, we see that

$$2\mathbb{Z}_K = \mathfrak{p}_{111}^{2^{r-2}} \mathfrak{p}_{221}^{2^{r-1}} \mathfrak{a},$$

where $\mathfrak{a}$ is a nonzero ideal of $\mathbb{Z}_K$ provided by the segments S_{12} and S_{21} and the monic irreducible factors of $U(x)$ modulo 2, and $\mathfrak{p}_{111}$ and $\mathfrak{p}_{221}$ are two prime ideals of $\mathbb{Z}_K$ of residue degree 2 each. So, there are two prime ideals of $\mathbb{Z}_K$ lying above 2 of residue degree 2 each. As there is only one monic irreducible polynomial in $\mathbb{F}_2[x]$, by Lemma 4.2, 2 divides $i(K)$. Hence, K is not monogenic. Assume now that $m \equiv 1 \pmod{16}$, then $\nu \geqslant 4$. If $r = 1$, by applying Theorem 3.1, we see that

$$2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}\mathfrak{p}_{211}\mathfrak{p}_{221}\mathfrak{a},$$

where $\mathfrak{a}$ is a nonzero ideal of $\mathbb{Z}_K$ and $\mathfrak{p}_{ikj}$ are prime ideals of $\mathbb{Z}_K$ with residue degrees

$$f(\mathfrak{p}_{111}/2) = f(\mathfrak{p}_{121}/2) = 1 \quad \text{and} \quad f(\mathfrak{p}_{211}/2) = f(\mathfrak{p}_{221}/2) = 2.$$

By Lemma 4.2, 2 divides $i(K)$. If $r = 2$, we obtain that

$$2\mathbb{Z}_K = \mathfrak{p}_{111}\mathfrak{p}_{121}\mathfrak{p}_{131}^2\mathfrak{q}_{111}\mathfrak{q}_{121}\mathfrak{q}_{131}^2\mathfrak{a},$$

where $\mathfrak{a}$ is a nonzero ideal and $\mathfrak{p}_{1k1}$ is a prime ideal of $\mathbb{Z}_K$ with residue degree $f(\mathfrak{p}_{1k1}/2) = 2$ for $k = 1, 2, 3$ and $\mathfrak{q}_{1k1}$ is a prime ideal of $\mathbb{Z}_K$ with residue

degree $f(\mathfrak{q}_{1k1}/2) = 1$ for $k = 1, 2, 3$. Then, 2 divides $i(K)$. Assume now that $r \geqslant 3$. In this case, we have that

$$N^+_{\varphi_i}(F) = S_{i1} + \ldots + S_{i,t-1} + S_{it}$$

has t sides with $t \geqslant 3$. The last two sides have degree 1 each. More precisely, the part $S_{i,t-1} + S_{it}$ is the lower convex hull of the points $(2^{r-2}, 2)$, $(2^{r-1}, 1)$ and $(2^r, 0)$ (see Figure 4).

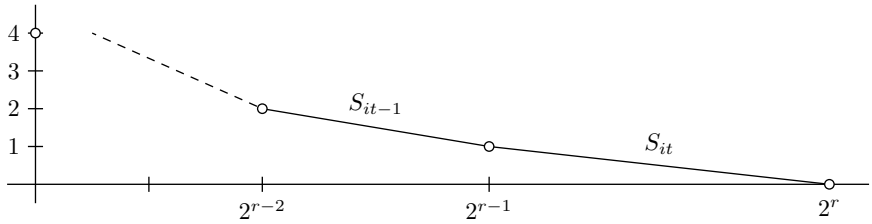

Figure 4. $N^+_{\varphi_i}(F), i = 1, 2$, when $r \geqslant 3$, and $m \equiv 1 \pmod{16}$.

It follows that the residual polynomials $R_{2,t-1}(F)(y)$ and $R_{2,t}(F)(y)$ are irreducible in $\mathbb{F}_{\varphi_2}[y]$ as they are of degree 1 each. Applying Theorem 3.1, one has

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

where $\mathfrak{a}$ is a nonzero ideal of $\mathbb{Z}_K$ provided by the other segments of $N^+_{\varphi_2}(F)$, the segments of $N^+_{\varphi_1}(F)$ and the monic irreducible factors of $U(x)$ modulo 2, and $\mathfrak{p}_{t-1}$ and $\mathfrak{p}_t$ are two prime ideals of $\mathbb{Z}_K$ of residue degree 2 each. So, the factor $\varphi_2(x)$ of $F(x)$ modulo 2 provides at least two prime ideals of residue degree 2 each, lying above 2 in $\mathbb{Z}_K$. By Lemma 4.2, 2 divides $i(K)$. Hence, K is not monogenic.

(2) If $m \equiv 1 \pmod 9$, then $\overline{F(x)} = \overline{(x^{2^r \cdot 7^s} - 1)}^{3^k} = \overline{((x-1)(x+1)V(x))}^{3^k}$, where $V(x) = \sum_{j=0}^{2^{r-1} \cdot 7^s - 1} (x^2)^{2^{r-1} \cdot 5^s - j}$. Set $\varphi_1(x) = x - 1$ and $\varphi_2(x) = x + 1$. Note also that $\overline{(x^{2^r \cdot 7^s} - 1)}$ is separable in $\mathbb{F}_3[x]$ (because 3 does not divide $2^r \cdot 7^s$). It follows that $\overline{\varphi_i(x)}$ does not divide $\overline{V(x)}$ in $\mathbb{F}_3[x]$ for $i = 1, 2$. Write

$$\begin{aligned} F(x) &= x^{2^r \cdot 3^k \cdot 7^s} - m = (\varphi_1(x)\varphi_2(x)V(x) + 1)^{3^k} - m \\ &= (\varphi_1(x)\varphi_2(x)V(x))^{3^k} + \sum_{j=1}^{3^k - 1} \binom{3^k}{j} (V(x)\varphi_1(x)\varphi_2(x))^j + 1 - m. \end{aligned} \tag{4.6}$$

Let $\omega = \nu_3(1 - m)$, then $\omega \geqslant 2$ (because $m \equiv 1 \pmod 9$). Since $\overline{\varphi_i(x)}$ does not divide $\overline{V(x)}$ in $\mathbb{F}_3[x]$ for $i = 1, 2$, the above φ_i-development of $F(x)$ is admissible for $i = 1, 2$. By Lemmas 4.1 and 3.4,

$$N^+_{\varphi_i}(F) = S_{i1} + \ldots + S_{it}$$

has t sides of degree 1 each with $t \geqslant 2$. More precisely, $N^+_{\varphi_i}(F)$ is the lower convex hull of the points $(0,\omega)$, $(1,k)$, $(3,k-1),\ldots,(3^{k-1},1)$ and $(3^k,0)$. Thus $R_{\lambda_{ik}}(F)(y)$ are separable over $\mathbb{F}_{\varphi_i}$ as they are of degree 1. By Theorem 3.1, the monic irreducible factors $\varphi_1(x)$ and $\varphi_2(x)$ provide at least four prime ideals of $\mathbb{Z}_K$ of residue degree 1 each lying above 3. As there are only three monic irreducible polynomials of degree 1 in $\mathbb{F}_3[x]$, namely, x, $x-1$ and $x-2$, by Lemma 4.2, 3 divides $i(K)$. Consequently, K is not monogenic. Assume now that $r \geqslant 2$ and $m \equiv -1 \pmod 9$. In this case,

$$\overline{F(x)} = \overline{((x^2+x-1)(x^2-x-1)W(x))}^{3^k} \quad \text{in } \mathbb{F}_3[x],$$

where $W(x) = \sum_{j=1}^{2^{r-2}\cdot 7^s-1} (-1)^j (x^4)^j$. Let $\varphi_1(x) = x^2+x-1$, $\varphi_2(x) = x^2-x-1$ and $\mu = \nu_3(-1-m)$. Write

$$\begin{aligned} F(x) &= (\varphi_1(x)\varphi_2(x)W(x)-1)^{3^k} - m \\ &= (\varphi_1(x)\varphi_2(x)W(x))^{3^k} + \sum_{j=1}^{3^k-1} (-1)^j \binom{3^k}{j} (\varphi_1(x)\varphi_2(x)W(x))^j - 1 - m. \end{aligned} \tag{4.7}$$

Since $\overline{\varphi_i(x)}$ does not divide $\overline{W(x)}$ (because 3 does not divide $2^r \cdot 7^s$), the above φ_i-development (4.7) is admissible for $i = 1, 2$. Note also that $\mu \geqslant 2$ (because $m \equiv -1 \pmod 9$). By Lemmas 4.1 and 3.4,

$$N^+_{\varphi_i}(F) = S_{i1} + \ldots + S_{it}$$

has t sides of degree 1 each with $t \geqslant 2$. More precisely, $N^+_{\varphi_i}(F)$ is the lower convex hull of the points $(0,\mu)$, $(1,k)$, $(3,k-1),\ldots,(3^{k-1},1)$ and $(3^k,0)$. Thus $R_{\lambda_{ik}}(F)(y)$ are separable over $\mathbb{F}_{\varphi_i}$ as they are of degree 1 for every $i = 1, 2$ and $k = 1,\ldots,t$. By Theorem 3.1, the monic factor $\varphi_i(x)$ provides at least two prime ideals of residue degree 2 each for $i = 1, 2$. As there are only three monic irreducible polynomials in $\mathbb{F}_3[x]$ of degree 2, namely, x^2+1, x^2+x-1 and x^2-x-1, by Lemma 4.2, 3 divides $i(K)$. Hence, K is not monogenic. Similarly, if $r = 1$ and $m \equiv -1 \pmod{81}$, we see that the monic irreducible factor x^2+1 of $F(x)$ modulo 3 provides at least four prime ideals of residue degree 1 each, lying above 3 in $\mathbb{Z}_K$. It follows that 3 divides $i(K)$. So, K cannot be monogenic.

(3) Since 7 does not divide m, $\overline{F(x)} = \overline{(x^{2^r\cdot 3^k} - m)}^{7^s}$ in $\mathbb{F}_7[x]$. Let $\varphi_i(x)$ be a monic irreducible factor of $F(x) \pmod 7$ (this means that $\varphi_i(x)$ is a monic irreducible factor of $x^{2^r\cdot 3^k} - m \pmod 7$). Let $\psi_i(x)$, $U_i(x)$, $V_i(x)$, and $R_i(x)$ be as in the proof of Theorem 2.1, where we determined the φ-principal Newton polygon of $F(x)$ in the cases $p = 7$, and p does not divide m. Let $\omega_0 = \nu_7(m^{7^s} - m) = \nu_7(m^6 - 1)$ and

$\omega_{i0} = \nu_7(7^{s+1}R_i(x) + m^{p^s} - m) \geqslant \min\{s+1, \omega_0\}$. Then, $N^+_{\varphi_i}(F)$ is the lower convex hull of the points $\{(0, \omega_{i0})\} \cup \{(7^j, s-j)\colon\ 0 \leqslant j \leqslant s\}$ in the Euclidean plane.

(a) Assume now that $m \equiv 1 \pmod{49}$; $\omega_0 \geqslant 2$, then $\overline{F(x)} = \overline{\Big(\prod_{i=1}^{6} \varphi_i(x)M(x)\Big)}^{7^s}$ in $F_7[x]$, where $\varphi_i(x) = x + i$. It follows that $N^+_{\varphi_i}(F) = S_{i1} + \ldots + S_{it}$ has t sides of degree 1 each, with $t \geqslant 2$ for every $i = 1, \ldots, 6$. By Theorem 3.1, every factor $\overline{\varphi_i(x)}$ of $\overline{F(x)}$ provides at least two prime ideals of residue degree 1 each. Hence, there are at least 12 prime ideals of residue degree 1 each, lying above 7. There are only seven monic irreducible polynomials of degree 1 in $\mathbb{F}_7[x]$, namely x, $x+1$, $x+2$, $x+3$, $x+4$, $x+5$ and $x+6$. By Lemma 4.2, 7 divides $i(K)$. Consequently, K cannot be monogenic.

(b) Suppose that $r = 1$, $s \geqslant 7$ and $m \equiv -1 \pmod{7^8}$. In this case, $\overline{F(x)} = \overline{(\varphi_1(x)\varphi_2(x)\varphi_3(x)A(x))}^{7^s}$ in $\mathbb{F}_7[x]$, where $\varphi_1(x) = x^2 + 1$, $\varphi_1(x) = x^2 + 2$, $\varphi_3(x) = x^2 + 4$ and $A(x) \in \mathbb{Z}[x]$ such that $\overline{\varphi_i(x)}$ does not divide $\overline{A(x)}$ for $i = 1, 2, 3$. According to the above description of φ_i-Newton polygons, we see that

$$N^+_{\varphi_i}(F) = S_{i1} + S_{i2} + \ldots + S_{it}$$

has t sides of degree 1 each with $t \geqslant 8$. Thus, $R_{\lambda_{ik}}(F)(y)$ is irreducible over $\mathbb{F}_{\varphi_i}$ as it is of degree 1 for every $i = 1, 2, 3$ and $k = 1, 2, \ldots, t$. By Theorem 3.1, we see that

$$7\mathbb{Z}_K = \prod_{i=1}^{3}\prod_{j=1}^{t} \mathfrak{p}_{it}^{e_{it}}\mathfrak{a},$$

where e_{it} is the ramification index of the segment S_{it}, $\mathfrak{a}$ is a nonzero ideal of $\mathbb{Z}_K$ and $\mathfrak{p}_{it}$ is a prime ideal of $\mathbb{Z}_K$ of residue degree $f(\mathfrak{p}_{it}/7) = \deg(\varphi_i) \times \deg(R_{\lambda_{it}}(F)(y)) = 2 \times 1 = 2$. So, there are at least 24 prime ideals of residue degree 2 of $\mathbb{Z}_K$ lying above 7. Recall also that the number of monic irreducible polynomials of degree g in $\mathbb{F}_p[x]$ is

$$N_p(m) = \frac{1}{g}\sum_{d|g} \mu(d)p^{g/d},$$

where μ is the Möbius function. It follows that for $p = 7$ and $g = 2$, $N_7(2) = 21$. As there are only 21 monic irreducible polynomials in $\mathbb{F}_7[x]$, by Lemma 4.2, 7 divides $i(K)$. So, K is not monogenic.

(c) If $r \geqslant 2$, $s \geqslant 3$, and $m \equiv -1 \pmod{7^4}$, then $\overline{F(x)} = \overline{\Big(\prod_{i=1}^{6} \varphi_i(x)H(x)\Big)}^{7^s}$ in $\mathbb{F}_7[x]$, where $\varphi_1 = x^2 + x + 4$, $\varphi_2(x) = x^2 + 2x + 2$, $\varphi_3(x) = x^2 + 3x + 1$, $\varphi_4(x) = x^2 + 4x + 1$, $\varphi_5(x) = x^2 + 5x + 2$, $\varphi_6(x) = x^2 + 6x + 4$, and $\overline{\varphi_i(x)}$ does

not divide $\overline{H(x)}$ for every $i = 1, \ldots, 6$, and we have also $\omega_{i0} \geqslant 4$. It follows that $N^+_{\varphi_i}(F) = S_{i1} + \ldots + S_{it}$ has t sides of degree 1 each, with $t \geqslant 4$ for every $i = 1, \ldots, 6$. By Theorem 3.1, every factor $\overline{\varphi_i(x)}$ of $\overline{F(x)}$ provides at least four prime ideals of residue degree 2 each. Hence, there are at least 24 prime ideals of residue degree 2 each of $\mathbb{Z}_K$ lying above 7. Since there are only 21 monic irreducible polynomials of degree 2 in $\mathbb{F}_7[x]$, by Lemma 4.2, 7 divides $i(K)$. So, K is not monogenic. □

P r o o f of Theorem 2.4. Since $\gcd(t, 42) = 1$, let (x, y) be the positive solution of the Diophantine equation $tx - 2^r \cdot 3^k \cdot 7^s y = 1$ with $1 \leqslant y < 2^r \cdot 3^k \cdot 7^s$ and let $\eta = \alpha^x / m^y$. Then $\eta^{2^r \cdot 3^k \cdot 7^s} = m$. Thus η is a root of the polynomial $G(x) = x^{2^r \cdot 3^k \cdot 7^s} - m$. Since m is square-free, $G(x)$ is irreducible over $\mathbb{Q}$. As $\eta \in K$ and $[K : \mathbb{Q}] = 2^r \cdot 3^k \cdot 7^s = \deg(G(x))$, K is generated by η, a root of $G(x)$. The proof is therefore a direct application of Theorems 2.1 and 2.3. □

E x a m p l e 4.4. Let $F(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial and K the number field defined by a complex root of $F(x)$.

(1) Let $F(x) = x^{504} - 22$; $m = 22$. Since m is square-free, $m \equiv 2 \pmod 4$, $m \equiv 4 \pmod 9$ and $m \equiv 22 \pmod{49}$, by Theorem 2.1, K is monogenic and α generates a power integral basis of $\mathbb{Z}_K$.

(2) Let $F(x) = x^{84} - 82$; $m = 82$. Since $m \equiv 1 \pmod 9$, by Theorem 2.3, K cannot be monogenic.

(3) Let $F(x) = x^{1764} - 66^{353}$; $m = 66$ and $t = 353$. By Corollary 2.4, K is monogenic and $\eta = \frac{1}{66}\alpha^5$ generates a power integral basis of $\mathbb{Z}_K$.

A c k n o w l e d g m e n t s. The authors are deeply grateful to Editor Clemens Fuchs for his patience and professionalism during the review process of this manuscript. We would like to profoundly thank the anonymous referees for their precious time and their efforts. Their valuable comments, important suggestions and rare remarks have tremendously improved the quality of this paper. Also, we thank Professor Lhoussain El Fadil who introduced us to work on monogenity of number fields.

References

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

[2] *S. Ahmad, T. Nakahara, S. M. Husnine*: Power integral bases for certain pure sextic fields. Int. J. Number Theory *10* (2014), 2257–2265. zbl MR doi

[3] *H. Ben Yakkou, A. Chillali, L. El Fadil*: On power integral bases for certain pure number fields defined by $x^{2^r \cdot 5^s} - m$. Commun. Algebra *49* (2021), 2916–2926. zbl MR doi

[4] *Y. Bilu, I. Gaál, K. Győry*: Index form equations in sextic fields: A hard computation. Acta Arith. *115* (2004), 85–96. zbl MR doi

[5] *H. Cohen*: A Course in Computational Algebraic Number Theory. Graduate Texts in Mathematics 138. Springer, Berlin, 1993. zbl MR doi

[6] *R. Dedekind*: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen. Abh. Akad. Wiss. Gött. *23* (1878), 3–38. (In German.)
[7] *L. El Fadil*: On power integral bases for certain pure number fields defined by $x^{3^r \cdot 7^s} - m$. Colloq. Math. *169* (2022), 307–317. zbl MR doi
[8] *L. El Fadil, H. Ben Yakkou, J. Didi*: On power integral bases for certain pure number fields defined by $x^{42} - m$. Bol. Soc. Mat. Mex., III. Ser. *27* (2021), Article ID 81, 10 pages. zbl MR doi
[9] *L. El Fadil, J. Montes, E. Nart*: Newton polygons and p-integral bases of quartic number fields. J. Algebra Appl. *11* (2012), Article ID 1250073, 33 pages. zbl MR doi
[10] *L. El Fadil, A. Najim*: On power integral bases for certain pure number fields defined by $x^{2^u \cdot 3^v} - m$. Available at `https://arxiv.org/abs/2106.01252` (2021), 12 pages.
[11] *I. Gaál*: Diophantine Equations and Power Integral Bases: Theory and Algorithms. Birkhäuser, Cham, 2019. zbl MR doi
[12] *I. Gaál, K. Győry*: Index form equations in quintic fields. Acta Arith. *89* (1999), 379–396. zbl MR doi
[13] *I. Gaál, L. Remete*: Binomial Thue equations and power integral bases in pure quartic fields. JP J. Algebra Number Theory Appl. *32* (2014), 49–61. zbl
[14] *I. Gaál, L. Remete*: Integral bases and monogenity of pure fields. J. Number Theory *173* (2017), 129–146. zbl MR doi
[15] *I. Gaál, L. Remete*: Non-monogenity in a family of octic fields. Rocky Mt. J. Math. *47* (2017), 817–824. zbl MR doi
[16] *T. A. Gassert*: A note on the monogeneity of power maps. Albanian J. Math. *11* (2017), 3–12. zbl MR
[17] *J. Guàrdia, J. Montes, E. Nart*: Newton polygons of higher order in algebraic number theory. Trans. Am. Math. Soc. *364* (2012), 361–416. zbl MR doi
[18] *A. Hameed, T. Nakahara*: Integral bases and relative monogenity of pure octic fields. Bull. Math. Soc. Sci. Math. Roum., Nouv. Sér. *58* (2015), 419–433. zbl MR
[19] *H. Hasse*: Zahlentheorie. Akademie-Verlag, Berlin, 1963. (In German.) zbl MR
[20] *A. Jakhar, S. Khanduja, N. Sangwan*: On the discriminant of pure number fields. Colloq. Math. *167* (2022), 149–157. zbl MR doi
[21] *W. Narkiewicz*: Elementary and Analytic Theory of Algebraic Numbers. Springer Monographs in Mathematics. Springer, Berlin, 2004. zbl MR doi
[22] *Ö. Ore*: Newtonsche Polygone in der Theorie der algebraischen Körper. Math. Ann. *99* (1928), 84–117. (In German.) zbl MR doi
[23] *A. Pethő, M. E. Pohst*: On the indices of multiquadratic number fields. Acta. Arith. *153* (2012), 393–414. zbl MR doi

Authors' address: *Hamid Ben Yakkou* (corresponding author), *Jalal Didi*, Faculty of Sciences Dhar El Mahraz, P.O. Box 1874, Fez, Sidi Mohamed Ben Abdellah University, Morocco, e-mail: `beyakouhamid@gmail.com`, `didimath1992@live.fr`.