Khayyam J. Math. 10 (2024), no. 1, 41-50
DOI: 10.22034/KJM.2023.397983.2874

Khayyam Journal of Mathematics
emis.de/journals/KJM
kjm-math.org

ON THE MONOGENEITY OF A CERTAIN CLASS OF NUMBER FIELDS

JALAL DIDI[1], MOHAMMED SAHMOUDI[2*] AND ABDELHAKIM CHILLALI[1]

Communicated by B. Mashayekhy

Abstract. Let $K = \mathbb{Q}(\alpha)$ be a pure number field generated by α a root of a monic irreducible polynomial $F(x) = x^{3^r \cdot 5^s \cdot 7^t} - m \in \mathbb{Z}[x]$, where $m \neq \pm 1$ is a square-free rational integer, r, s, and t are three positive rational integers. The aim of this paper is to study the problem of monogeneity of the field K. More precisely, we provide explicit conditions on r, s, t, and m for which K is monogenic. We show that if $m \not\equiv \pm 1\,(mod\,9)$, $\overline{m} \notin \{\overline{\pm 1}, \overline{\pm 7}\}\,(mod\,25)$, and $\overline{m} \notin \{\overline{\pm 1}, \overline{\pm 18}, \overline{\pm 19}\}\,(mod\,49)$, then K is monogenic. In addition, we prove the existence of infinite families of nonmonogenic number fields of degree $n = 3^r \cdot 5^s \cdot 7^t$. At the conclusion of this work, a few illustrative examples are provided.

1. Introduction and preliminaries

Let K be a pure number field defined by a monic irreducible polynomial $F(x) = x^{3^r \cdot 5^s \cdot 7^t} - m \in \mathbb{Z}[x]$ and let $\mathfrak{o}_K$ be the ring of integers of K. The ring $\mathfrak{o}_K$ is said to have a power integral basis (PIB for short) if it has a $\mathbb{Z}$-basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ for some $\alpha \in \mathfrak{o}_K$. An algebraic number field K is said to be monogenic if $\mathfrak{o}_K$ has a PIB. In such a case, the field K is said to be monogenic; that is, the index $(\mathfrak{o}_K : \mathbb{Z}[\alpha]) = 1$. If K does not have any such α, then the field K is said to be nonmonogenic. Computing PIBs or relative power integral bases (RPIBs for short) has been intensively studied during the last century and this century, mainly by Gaál, Nakahara, Pethö, Sahmoudi, El Fadil, and their collaborators (see, for example, [12,14,18–21,24]). Using the explicit form of the index formula,

Date: Received: 18 May 2023; Revised: 5 November 2023; Accepted: 22 January 2024.

[*] Corresponding author.

2020 *Mathematics Subject Classification.* 11Y40, 11Y21, 11Y40.

Key words and phrases. Monogeineity, Dedekind's criterion, Newton polygon, Ore's Theorem, prime ideal factorization.

Gaál and Remete [12] obtained new results on the monogeneity of pure number fields $\mathbb{Q}(\sqrt[n]{m})$ with $3 \leq n \leq 9$ and $m \neq \pm 1$ a square-free integer. They also showed in [11] that if $m \equiv 2 \,\text{or}\, 3\,(mod\, 4)$ is a square-free rational integer, then the octic field $\mathbb{Q}(i, \sqrt[4]{m})$ is not monogenic.

Hameed et al. [14]showed that if $m \equiv 2, 3\,(mod\, 4)$, then $\mathbb{Q}(\sqrt[2^n]{m})$ is monogenic.This involves the pure quartic and pure octic fields. Moreover, they showed that if m is square free and all the prime factors of n divide m, then $\mathbb{Q}(\sqrt[n]{m})$ is monogenic. Khan, Nakahara, and Sekiguchi [15] studied the monogeneity of the family of cyclic sextic composite fields $K.L$ over the field $\mathbb{Q}$, where K is a cyclic cubic field of prime conductor p and L is a quadratic field with the field discriminant d_k such that $(p, d_L) = 1$. Yakkou, Chillali, and El Fadil [1] studied pure number fields defined by $x^{2^r \cdot 5^s} - m$. They proved that if $m \equiv 1\,(mod\, 4)$ and $\overline{m} \notin \{\overline{1}, \overline{7}, \overline{18}, \overline{24}\}\,(mod\, 25)$, then K is monogenic. In a series of papers, El fadil studied the monogenity of pure number fields of degrees 6, 12, 18, 20, 24, 36, $2^u \cdot 3^v \cdot 5^t - m$, where $m \neq \pm 1$ is a square-free rational integer and u, v, and t are three positive integers. Sahmoudi and Charkani [18] studied the relative monogeneity of number fields L defined by $x^p - m$ over an arbitrary number field K by a simple and practical version of Dedekind's criterion characterizing the existence of PIBs over an arbitrary Dedekind ring by using the Gauss valuation. Also, Sahmoudi et al. [21, 22] studied the relative monogeneity of $L = K(\alpha)$, where α satisfies the monic irreducible polynomial $F(x) = X^{p^n} - m \in \mathfrak{o}_K[x]$ with $p = 3$ and in the general case where $(p > 3)$.

In this paper, we study the monogeneity of pure number field $K = \mathbb{Q}(\alpha)$ generated by a complex root α of a monic irreducible polynomial $F(x) = x^{3^r \cdot 5^s \cdot 7^t} - m$, where $m \neq \pm 1$ is a rational integer without square and r, s, and t are positive integers. The method employed is essentially based on the Dedekind criterion, the techniques of Newton's polygons, and the factorization of prime ideals.

In view of proving our main theorems, we mention some fundamental techniques on prime ideal factorization and calculation of the index: $Ind_{\mathbb{Z}}(\alpha) = [\mathfrak{o}_K : \mathbb{Z}[\alpha]]$. Let $K = \mathbb{Q}(\alpha)$ be a number field, where $\alpha \in \mathfrak{o}_K$ is an algebraic integer over $\mathbb{Z}$. Let $F = Irrd(\alpha, \mathbb{Z}) \in \mathbb{Z}[x]$ be the monic irreducible polynomial of α. Let p be a nonzero prime integer, and let $\bar{F} = \prod_{i=1}^{r} \bar{\phi}_i^{\,l_i}$ be the primary decomposition of $\bar{F}$ in $\mathbb{F}_p[x]$ for some monic polynomial $\phi_i \in \mathbb{Z}[x]$. Let $R_i \in \mathbb{Z}[x]$ be the remainder of the Euclidean division of F by ϕ_i. Let υ_{G^p} be the Gauss valuation on $\mathbb{Q}[x]$. Dedekind's criterion allows us to test whether a prime integer p divides or not the index $[\mathfrak{o}_K : \mathbb{Z}[\alpha]]$.

Theorem 1.1 (Dedekind Criterion, [3, 18])**.** *With the assumptions and notations as above, p does not divide the index integer $Ind_{\mathbb{Z}}(\alpha)$ if and only if either $\upsilon_{G^p}(R_i) = 1$ or $l_i = 1$ for all $i = 1, \dots, r$ such that $l_i \geq 2$.*

Dedekind's criterion fails sometimes, that is to say, the prime p divides the index $\text{Ind}_{\mathbb{Z}}(\alpha)$ for every primitive element $\alpha \in \mathfrak{o}_K$. Then for such primes and number fields, we are not able to find the factorization of the prime ideal of $p\mathfrak{o}_K$. So, to resolve this problem, we start by recalling some fundamental notions about Newton's polygon. For additional information, we refer to [9, 13, 17]. Let p be a rational prime integer and let $\phi \in \mathbb{Z}[x]$ be a monic polynomial that is irreducible modulo p. Upon the Euclidean division by the successive power of ϕ, we can expand $F(x)$ as follows: $F(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_n(x)\phi(x)^n$, with $deg\ (a_i(x)) < deg\ (\phi(x))$. Any such expansion is unique, which is called the ϕ-adic expansion of $F(x)$. For every $i = 0, \ldots, n$, 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 $\{(i, u_i), 0 \leq i \leq n,\ a_i(x) \neq 0\}$ in the Euclidean plane, which is denoted 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 $\lambda_1 < \lambda_2 < \cdots < \lambda_g$. 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 $F(x)$ and denoted by $N_\phi^+(F)$. The length of $N_\phi^+(F)$ is $\nu_{\overline{\phi}}(\overline{F(x)})$; the highest power of $\overline{\phi}$ dividing $\overline{F(x)}$ in $\mathbb{F}_p[x]$.

Let $\mathbb{F}_\phi$ be the finite field $\mathbb{Z}[x]/(p, \phi(x)) \simeq \mathbb{F}_p[x]/(\overline{\phi(x)})$ (note that if $deg(\phi) = 1$, then $\mathbb{F}_\phi \simeq \mathbb{F}_p$). For every $i = 0, \ldots, n$, we attach the following residue coefficient $c_i \in \mathbb{F}_\phi$:

$$c_i = \begin{cases} 0, & \text{if } (i, u_i) \text{ lies strictly above } N_\phi^+(F), \\ \left(\dfrac{a_i(x)}{p^{u_i}}\right) \ (mod\,(p, \phi(x)), & \text{if } (i, u_i) \text{ lies on } N_\phi^+(F). \end{cases} \tag{1.1}$$

Let S be a side of $N_\phi^+(F)$ and let $\lambda = -\frac{h}{e}$ be its slope, where e and h are two positive coprime integers. The length of S, denoted by $l(S)$, is the length of its projection to the horizontal axis, and its height, denoted by $h(S)$, is the length of its projection to the vertical axis. The degree of S is $d = d(S) = \gcd(l(S), h(S))$. Remark that if (s, u_s) is the initial point of S, then the points with integer coordinates lying on 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

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

As defined in [9, Def. 1.3], the ϕ-index of $F(x)$, denoted by $ind_\phi(F)$, is $\deg(\phi)$ multiplied by 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 (see Figure 1).

The polynomial $F(x)$ is said to be ϕ-regular for p if, for each side S of $N_\phi^+(F)$, the corresponding residual polynomial $R_\lambda(F)(y)$ is separable in $\mathbb{F}_\phi[y]$.

Now, let $\overline{F(x)} = \prod_{i=1}^t \overline{\phi_i}^{l_i}$ be the factorization of $\overline{F(x)}$ into monic irreducible polynomials $\phi_1, \ldots, \phi_t$ in $\mathbb{F}_p[x]$. The polynomial $F(x)$ is said to be p-regular if $F(x)$ is ϕ_i-regular for $i = 1, \ldots, t$.

Let $N_{\phi_i}^+(F) = S_{i1} + \cdots + S_{it_i}$ be the principal ϕ_i-Newton polygon of F with regard to p for each $i = 1, \ldots, t$. For every $j = 1, \ldots, t_i$, let $-\lambda_{ij}$ be the slope of the side S_{ij}, and 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 $\mathbb{F}_{\phi_i}[y]$. Then we have the Ore index theorem, which plays a significant role in the proof of our theorems (see [9, Theorems 1.7 and 1.9], [13, Theorem 3.9], and [17]):

Theorem 1.2 (Ore's Theorem). *With the notation above, we have*

(1) $\nu_p((\mathfrak{o}_K : \mathbb{Z}[\alpha])) \geq \sum_{i=1}^t ind_{\phi_i}(F)$, *with equality if $F(x)$ is p-regular.*

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

$$p\mathfrak{o}_K = \prod_{i=1}^{t}\prod_{j=1}^{r_i}\prod_{s=1}^{s_{ij}} \mathfrak{p}_{ijs}^{e_{ij}}, \tag{1.2}$$

where e_{ij} is the ramification index of the side S_{ij}, that is, the smallest positive integer satisfying $e_{ij}\lambda_{ij} \in \mathbb{Z}$ and $f_{ijs} = deg(\phi_i) \times deg(\psi_{ijs})$ is the residue degree of $\mathfrak{p}_{ijs}$ over p.

Corollary 1.3 ([10, Corollary 3.3.]). *Under the assumptions of Theorem 1.2, p does not divide the index $(\mathfrak{o}_K : \mathbb{Z}[\alpha])$ if and only if $l_i = 1$ or $N_{\phi_i}^{+}(F) = S_i$ has a single side of height 1 for every $i = 1, \dots, r$. Then, $F(x)$ is p-regular and $\nu_p((\mathfrak{o}_K : \mathbb{Z}[\alpha])) = 0$.*

Lemma 1.4 ([8]). *Let m and n be two positive integers, and let p be a prime number that divides n and does not divide m. Let $n = u \cdot p^r$ be in $\mathbb{Z}$ with p not divide u and let $v = \nu_p(m^{p-1} - 1)$. Let $\phi \in \mathbb{Z}[x]$ be a monic polynomial whose reduction modulo p divides $\overline{F(x)}$, where $F(x) = x^n - m \in \mathbb{Z}[x]$ is an irreducible polynomial.*

(1) *If $v \leq r$, then $N_{\phi}^{+}(F)$ is the lower boundary of the convex envelope of the set of the points $\{(0, v)\} \cup \{(p^j, r - j), j = 0, \dots, r\}$.*
(2) *If $v \geq r + 1$, then $N_{\phi}^{+}(F)$ is the lower boundary of the convex envelope of the set of the points $\{(0, V)\} \cup \{(p^j, r - j), j = 0, \dots, r\}$ for some integer $V \geq r + 1$.*

Example 1.5. We consider the monic irreducible polynomial $F(x) = x^8 + 3x^2 + 30 \in \mathbb{Z}[x]$. As $F(x)$ is 3-Eisenstein polynomial, then it is irreducible over $\mathbb{Q}$ which factors in $\mathbb{F}_2[x]$ as follows: $\overline{F(x)} = \overline{\phi}^2 \cdot \overline{\psi}^2 \cdot \overline{\psi_1}^2$, where $\phi = x + 1$, $\psi = x$ and $\psi_1 = x^2 + x + 1$. The ϕ-development of $F(x)$ is

$$F(x) = 34 - 14\phi + 31\phi^2 - 56\phi^3 + 70\phi^4 - 56\phi^5 + 28\phi^6 - 8\phi^7 + \phi^8.$$

The ψ-development of $F(x)$ is

$$F(x) = \psi^8 + 3\psi^2 + 30 \in \mathbb{Z}[x].$$

Thus, $N_{\phi}^{+}(F) = S$ and $N_{\psi}^{+}(F) = S^{'}$ with respect to ν_2 have one side with respective degrees $d(S) = d(S^{'}) = 1$ and slopes $=^{'} = \frac{-1}{2}$ (see Figure 1).

The residual polynomials attached to the sides of $N_{\phi}^{+}(F)$ and $N_{\psi}^{+}(F)$ are $R(F)(y) = R_{'}(F)(y) = 1 + y$, which are irreducible polynomials in $\mathbb{F}_{\phi}[y] \simeq \mathbb{F}_2[y]$. Thus, $F(x)$ is ϕ and ψ-regular. Moreover, since $\nu_{\overline{\psi_1(x)}}(\overline{F(x)}) = 2$ and $v_2(-4x + 26) = 1$, where $-4x + 26$ is the remainder of division Euclidean of $F(x)$ by ψ_1, then $F(x)$ is ψ_1-regular. Hence, it is 2-regular. By Theorem 1.2, $\nu_2((\mathfrak{o}_K : \mathbb{Z}[\alpha])) = ind_{\phi}(F) + ind_{\psi}(F) + ind_{\psi_1}(F) = 0+0+0 = 0$, and $2\mathfrak{o}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$ with residue degrees $f(\mathfrak{p}_i/2) = 1$ for $i = 1, 2$ and $f(\mathfrak{p}_3/2) = 2$, (see Figure 1).

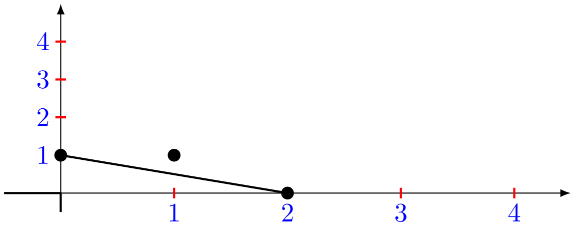

Figure 1. The ϕ and ψ-principal Newton polygon $N_\phi^+ F$ and $N_\psi^+(F)$ with respect to ν_2.

2. Main results

Through this section, K is a pure number field that is generated by a root α of a monic irreducible polynomial $F(x) = x^n - m$, where $n = 3^r \cdot 5^s \cdot 7^t$, $m \neq \pm 1$ is a rational integer, r, s, and t are three positive integers. For any monic irreducible polynomial F, we put

$$S_F \;=\; \{\, p,\, prime\, integer\, ;\, p^2\, divides\, disc_{\mathbb{Z}}(F)\},$$

where $disc_{\mathbb{Z}}(F)$ is the discriminant of the polynomial F.
The following theorem gives necessary and sufficient conditions for $\mathbb{Z}[\alpha]$ to be integrally closed in K.

Theorem 2.1. *Let p be a prime integer in S_F. Then, $p \nmid (\mathfrak{o}_K : \mathbb{Z}[\alpha])$ if and only if the following conditions hold:*

1. $m \not\equiv \pm 1\,(mod\, 9)$, $\overline{m} \notin \{\overline{\pm 1}, \overline{\pm 7}\}\,(mod\, 25)$ *and* $\overline{m} \notin \{\overline{\pm 1}, \overline{\pm 18}, \overline{\pm 19}\}\,(mod\, 49)$ *if* $p \in \{3, 5, 7\}$ *and* $\nu_p(m) = 0$,
2. m *square-free,* *if* $\nu_p(m) \geq 1$.

In particular, in these cases K is monogenic.

Remark 2.2. Theorem 2.1 cannot decide about monogeneity of K, if $m \equiv \pm 1\,(mod\, 9)$, or $\overline{m} \in \{\overline{\pm 1}, \overline{\pm 7}\}\,(mod\, 25)$ or $\overline{m} \in \{\overline{\pm 1}, \overline{\pm 18}, \overline{\pm 19}\}\,(mod\, 49)$. In this case, $\mathbb{Z}[\alpha]$ is not the ring of integers in K but K may happen to be monogenic. The next theorem gives a partial response.

Theorem 2.3. *K is not monogenic if one of the following statements holds:*

1. $r \geq 3$ *and* $m \equiv \pm 1\;(mod\, 81)$.
2. $s \geq 5$ *and* $m \equiv \pm 1\;(mod\, 5^6)$.
3. $s \geq 5$, r *even, and* t *odd, or* r *odd and* t *even, and* $m \equiv \pm 7\;(mod\, 5^6)$,
4. $s \geq 5$, r *even and* t *odd, or* r *odd and* t *even, and* $m^2 \equiv -1\;(mod\, 5^6)$,
5. $t \geq 7$ *and* $m \equiv \pm 1\;(mod\, 7^8)$.

Theorem 2.4. *Let $K = \mathbb{Q}(\alpha)$ be a pure number field, where α is a root of a monic irreducible polynomial $F(x) = x^{3^r \cdot 5^s \cdot 7^t} - a^u \in \mathbb{Z}[x]$, with a is a square-free, $\neq \pm 1$ and $u < 3^r \cdot 5^s \cdot 7^t$ a positive rational integer coprime to 105. Then,*

1. *K is monogenic if* $a \not\equiv \pm 1\,(mod\, 9))$, $\overline{a} \notin \{\overline{\pm 1}, \overline{\pm 7}\}\,(mod\, 25)$ *and* $\overline{a} \notin \{\overline{\pm 1},\ \overline{\pm 18},\ \overline{\pm 19}\}\,(mod\, 49)$.
2. *K is not monogenic if*
   - $r \geq 3$ *and* $a \equiv \pm 1\,(mod\, 81)$.

- $s \geq 5$ *and* $a \equiv \pm 1\,(mod\, 5^6)$.
- $s \geq 5$*,* r *even and* t *odd, or* r *odd and* t *even and* $a \equiv \pm 7\ (mod\, 5^6)$.
- $s \geq 5$*,* r *even and* t *odd, or* r *odd and* t *even and* $a^2 \equiv -1\ (mod\, 5^6)$.
- $t \geq 7$ *and* $a \equiv \pm 1\,(mod\, 7^8)$.

3. Proofs

Proof of Theorem 2.1. Since $F(x)$ is the minimal polynomial of the algebraic integer α over $\mathbb{Q}$, by [16, Propositions 2.9 and 2.13], one has the following index formula:

$$\begin{aligned} disc_{\mathbb{Z}}(\alpha) &= \pm N_{K/\mathbb{Q}}(F^{'}(\alpha)) = \pm N_{K/\mathbb{Q}}(3^r \cdot 3^s \cdot 7^t \cdot \alpha^{3^r \cdot 5^s \cdot 7^t - 1}) \\ &= \pm(3^r \cdot 5^s \cdot 7^t)^{3^r \cdot 5^s \cdot 7^t - 1} N_{K/\mathbb{Q}}(\alpha)^{3^r \cdot 5^s \cdot 7^t - 1} = \pm(3^r \cdot 5^s \cdot 7^t)^{3^r \cdot 5^s \cdot 7^t} m^{3^r \cdot 5^s \cdot 7^t - 1} \\ &= (\mathfrak{o}_K : \mathbb{Z}[\alpha])^2 \cdot d_K. \end{aligned}$$

Then $\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if p does not divide the index $(\mathfrak{o}_K : \mathbb{Z}[\alpha])$ for every rational prime integer p dividing $3 \cdot 5 \cdot 7 \cdot m$.

-
  - Let $p = 3$, let $m \not\equiv 0\ (mod\, 3)$, and let $\phi \in \mathbb{Z}[x]$ be a monic polynomial whose reduction $\overline{\phi}$ is an irreducible factor of $\overline{F(x)}$ in $\mathbb{F}_3[x]$. So, by Lemma 1.4, the principal Newton polygon $N_{\phi}^{+}(F)$ has a single side S of height 1 if and only if $\nu_3(m^2 - 1) = 1$, which means that $m \not\equiv \pm 1\,(mod\, 9)$. Therefore, by Corollary 1.3, $\nu_3((\mathfrak{o}_K : \mathbb{Z}[\alpha])) = \sum_{i=1}^{t} ind_{\phi_i}(F) = 0$, with t the number of distinct irreducible factors of $F(x)$ modulo 3 that the rational prime integer 3 does not divide $(\mathfrak{o}_K : \mathbb{Z}[\alpha])$.
  - Similarly, let $p = 5$, let $m \not\equiv 0\ (mod\, 5)$, and let $\phi \in \mathbb{Z}[x]$ be a monic polynomial whose reduction $\overline{\phi}$ is an irreducible factor of $\overline{F(x)}$ in $\mathbb{F}_5[x]$. By Lemma 1.4, $N_{\phi}^{+}(F)$ has a single side S of height 1 if and only if $\nu_5(m^4 - 1) = 1$, which means that $\overline{m} \not\in \{\overline{\pm 1}, \overline{\pm 7}\}\,(mod\, 25)$. Therefore, by Corollary 1.3, $\nu_5((\mathfrak{o}_K : \mathbb{Z}[\alpha])) = \sum_{i=1}^{t} ind_{\phi_i}(F) = 0$, with t is the number of distinct irreducible factors of $F(x)$ modulo 5; that is, to say that the rational prime integer 5 does not divide $(\mathfrak{o}_K : \mathbb{Z}[\alpha])$.
  - Finally, for $p = 7$, and 7 does not divide m. By Lemma 1.4, $N_{\phi}^{+}(F) = S$ has a single side of height 1 for every irreducible factor $\overline{\phi}$ of $\overline{F(x)}$ modulo 7. By Lemma 1.4, $N_{\phi}^{+}(F) = S$ has a single side of height 1 if and only if $\nu_7(m^6 - 1) = 1$ is equivalent to $m^6 \not\equiv 1\,(mod\, 49$, which means that $\overline{m} \not\in \{\overline{\pm 1}, \overline{\pm 18}, \overline{\pm 19}\}\,(mod\, 49)$.
- Let p be a prime integer dividing m. Then, $F(x) \equiv \phi^{3^r \cdot 5^s \cdot 7^t}\ (mod\, p)$, where $\phi = x$. We see immediately that the remainder of the Euclidean division of F by x is $r(x) = m$. This completes the proof in this case in view of Theorem 1.1. Namely, m is a square free rational integer.

□

The index of a field K is defined by

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

A rational prime p is called a prime common index divisor of K if p divides $i(K)$, in such case K is not monogenic. For example, Dedekind regards the cubic field K, which is given by $F(x) = x^3 - x^2 - 2x - 8$, and proves that the prime divisor 2 splits completely. Therefore, if we assume that K is monogenic, we can find a cubic polynomial generating K that splits completely into distinct polynomials of degree one in $\mathbb{F}_2[x]$. This is not possible because $\mathbb{F}_2[x]$ contains only two distinct polynomials of degree one.

Remark 3.1. If $p \notin \{3, 5, 7\}$, then p does not divide the index $(\mathfrak{o}_K : \mathbb{Z}[\alpha])$ if and only if m is square-free; thus, the factorization of $p\mathfrak{o}_K$ is analogous to the factorization of $\overline{F(x)} = \overline{x^{3^r\cdot 5^s\cdot 7^t} - m}$ in $\mathbb{F}_p[x]$. Therefore, it remains to study the prime numbers $p \in \{3, 5, 7\}$.

For the proof of Theorem 2.3, we require the following lemma, which characterizes the prime common index divisors of K.

Lemma 3.2 ([23, Theorem 2.2])**.** *Let p be a rational prime integer and let K be a number field. For every positive integer f, let $\mathcal{P}_f$ be the number of distinct prime ideals of $\mathfrak{o}_K$ lying above p with residue degrees f and let $\mathcal{N}_f$ be the number of monic irreducible polynomials of $\mathbb{F}_p[x]$ of degree f. Then, p is a prime common index divisor of K if and only if $\mathcal{P}_f > \mathcal{N}_f$ for a positive integer f.*

Remark 3.3 ([10]). To prove Theorem 2.3, we do not need to determine the explicit factorization of $p\mathfrak{o}_K$. From Lemma 3.2, it is sufficient to show that $P_f > N_f$ for a proper positive integer f. Thus, in practice, the second item of Theorem 1.2 could be changed to the following: If $l_i = 1$ or $d_{ij} = 1$ (degree of $R_{\lambda_{ij}}(F)(y)$) or $n_{ijk} = 1$ for some (i, j, k), according to the notation of Theorem 1.2, then ψ_{ijk} provides a prime ideal $\mathfrak{p}_{ijk}$ of $\mathfrak{o}_K$ lying above p with residue degree $f_{ijk} = m_i \cdot t_{ijk}$, where t_{ijk} =deg(ψ_{ijk}) and $p\mathfrak{o}_K = \mathfrak{p}_{ijk}^{e_{ij}} I$, where the factorization of the ideal I can be derived from the other factors of each residual polynomial of $F(x)$.

Proof of Theorem 2.3. In all cases, we show that $i(K) > 1$, which implies K is not monogenic.

(1) If $r \geq 3$ and $m \equiv \pm 1 \, (mod\, 81)$, then $F(x) = \overline{\phi(x)U(x)}^{3^r}$ in $\mathbb{F}_3[x]$. Let $\phi(x) = x - m$ be its reduction modulo p, let $\overline{\phi(x)}$ be a monic irreducible factor of $\overline{F(x)}$ in $\mathbb{F}_3[x]$. According to Lemma 1.4, $N_\phi^+(F) = S_1 + S_2 + \cdots + S_t$ has t sides of degree 1 each with $t \geq 4$. More precisely, $N_\phi^+(F)$ is the ϕ-principal Newton polygon of $F(x)$ joining the points $(0, \omega_0)$, $(1, r)$, $(3, r - 1), \ldots,$ and $(3^r, 0)$, with $\omega_0 \geq \min\{r + 1, \nu_3(m^2 - 1)\} \geq 4$ (see Figure2 as example). As $R_{\lambda_i}(F)(y)$ is of degree 1 for every $i = 1, 2, \ldots, t$. Thus, it is irreducible over $\mathbb{F}_\phi \simeq \mathbb{F}_3$. By Theorem 1.2, $3\mathfrak{o}_K = \prod_{i=1}^{t} \mathfrak{p}_i^{e_i} \cdot I_3$, where $\mathfrak{p}_i$ is a prime ideal of $\mathfrak{o}_K$ with $f(\mathfrak{p}_i/3) = 1$ for every $i = 1, \ldots, t$ and I_3 is a proper ideal of $\mathfrak{o}_K$. So, there are at least four prime ideals 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 $x - 2$, then, by Lemma 3.2. Thus 3 divides $i(K)$ and K is not monogenic.

(2) Since 5 does not divide m, then, the polynomial $x^{3^r.7^t} - m$ is divisible by a monic linear irreducible factor modulo 5. If $m \equiv \pm 1 \, (mod\, 5)$, then

the result is obvious. For $m \equiv 2\,(mod\,5)$, r odd and t even, or r even, and t odd, the polynomial $x^{3^r.7^t} - 2 = x^{3^r.7^t} - 3^{3^r.7^t} + 3^{3^r.7^t} - 2 = (x-3)U(x) + 3^{3^r.7^t} - 2$ for some polynomial $U(x) \in \mathbb{Z}[x]$. By induction on r and t, we show 5 divides $3^{3^r.7^t} - 2$. So, $x^{3^r.7^t} - 2 \equiv (x-3)U(x)\,(mod\,5)$. Similarly, if $m \equiv 3\,(mod\,5)$, r odd and t even or r even and t odd, then we get that $x-2$ is a monic irreducible factor of $x^{3^r.7^t} - m$ modulo 5. Finally, $\overline{F(x)} = \overline{(\phi(x)V(x))}^{5^s}$ in $\mathbb{F}_5[x]$, where $\deg(\phi(x)) = 1$, $V(x) \in \mathbb{Z}[x]$, and $\overline{\phi(x)}$ does not divide $\overline{V(x)}$. Since $s \geq 5$ and $\overline{m} \in \{\overline{\pm1}, \overline{\pm7}\}\,(mod\,5^6)$ or $m^2 \equiv -1\,(mod\,5^6)$, by Lemma 1.4, $N_\phi^+(F) = S_1 + S_2 + \cdots + S_t$ has t sides of degree 1 each, with $t \geq 6$, and $R_{_i}(F)(y)$ is irreducible over $\mathbb{F}_\phi \simeq \mathbb{F}_3$ for every $i = 1, 2, \ldots, t$. By Theorem 1.2, $5\mathfrak{o}_K = \prod_{i=1}^t \mathfrak{p}_i^{e_i} \cdot I_5$, where I_5 is a proper ideal of $\mathfrak{o}_K$ and $\mathfrak{p}_i$ is a prime ideal of $\mathfrak{o}_K$ with $f(\mathfrak{p}_i/5) = 1$ for every $i = 1, \ldots, t$. So, there are at least six prime ideals of residue degree 1 each lying above the rational prime integer 5. As there are only five monic irreducible polynomials of degree 1 in $\mathbb{F}_5[x]$, namely, x, $x-1$, $x-2$, $x-3$, and $x-4$. By Lemma 3.2, then 5 divides $i(K)$. Thus, K is not monogenic.

(3) For $t \geq 7$ and $m \equiv \pm1\,(mod\,7^8)$, we conclude that $\overline{F(x)} = \overline{(\phi(x)V(x))}^{7^t}$ in $\mathbb{F}_7[x]$, where $\deg(\phi(x)) = 1$, $V(x) \in \mathbb{Z}[x]$, and $\overline{\phi(x)}$ does not divide $\overline{V(x)}$. By Lemma 1.4, $N_\phi^+(F) = S_1 + S_2 + \cdots + S_t$ has t sides of degree 1 each, with $t \geq 8$. Thus, $R_{\lambda_i}(F)(y)$ is irreducible over $\mathbb{F}_\phi \simeq \mathbb{F}_7$ for every $i = 1, 2, \ldots, t$. By Theorem 1.2, $7\mathfrak{o}_K = \prod_{i=1}^t \mathfrak{p}_i^{e_i} \cdot I_7F$, where $\mathfrak{p}_i$ is a prime ideal of $\mathfrak{o}_K$ with $f(\mathfrak{p}_i/7) = 1$ for every $i = 1, \ldots, t$ and I_7 is a proper ideal of $\mathfrak{o}_K$. Then there are at least eight prime ideals of residue degree 1 each lying above the rational prime integer 7. As 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 3.2, thus 7 divides $i(K)$. Consequently, K is not monogenic.

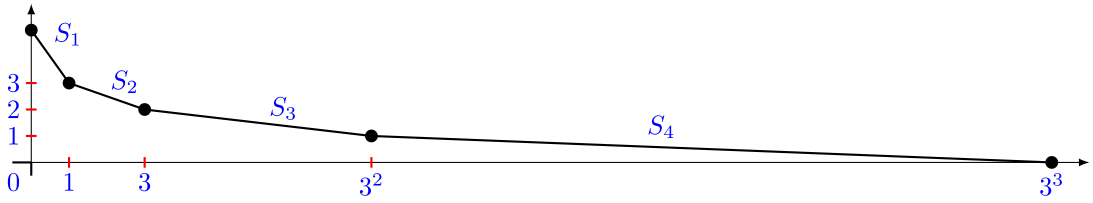

FIGURE 2. N_ϕ^+F at $p = 3$ with $m \equiv \pm1 \mod 81$ and $r = 3$.

□

Poof of Theorem 2.4. Since $\gcd(u, 105) = 1$, let (x, y) be the solution of

$$xu - 3^r \cdot 5^s \cdot 7^t y = 1$$

with $1 \leq y < 3^r \cdot 5^s \cdot 7^t$, and let $\theta = \frac{\alpha^x}{a^y}$. Then, $\theta^{3^r \cdot 5^s \cdot 7^t} = \frac{\alpha^{3^r \cdot 5^s \cdot 7^t x}}{a^{3^r \cdot 5^s \cdot 7^t y}} = a$. Thus, θ is a root of the monic polynomial $g(x) = x^{3^r \cdot 5^s \cdot 7^t} - a$. Since a is square-free, $g(x)$ is a p-Eisenstein polynomial with respect to any prime divisor p of a. It follows that $g(x)$

is irreducible over $\mathbb{Q}$. As $\theta \in K$, so $[K : \mathbb{Q}] = 3^r \cdot 5^s \cdot 7^t = \deg(g(x))$. Therefore, K is generated by θ, a root of $g(x)$. The proof is therefore an application of Theorems 2.1 and 2.3. □

4. Examples

Let $F(x)$ be a monic irreducible polynomial and let K be the number field defined by a complex root of $F(x)$.

(1) If $F(x) = x^{105} - 29$, as $F(x)$ is 29-Eisenstein polynomial, then it is irreducible over $\mathbb{Q}$. Since $m \equiv 2\,(mod\,9)$, $m \equiv 4\,(mod\,29)$, and $m \equiv 20\,(mod\,49)$, so, by Theorem 2.1, K is monogenic.

(2) If $F(x) = x^{3^r.7^s.7^t} - 59$, as $F(x)$ is 59-Eisenstein polynomial, then it is irreducible over $\mathbb{Q}$. Since $m \equiv 5\,(mod\,9)$, $m \equiv 9\,(mod\,25)$, and $m \equiv 10\,(mod\,49)$, so, by Theorem 2.3, K is monogenic.

(3) If $F(x) = x^{2835} - 163$, then $F(x)$ is an irreducible polynomial over $\mathbb{Q}$. Since $m \equiv 1\,(mod\,81)$, so, by Theorem 2.3, K is not monogenic.

(4) If $F(x) = x^{1148175} - 323$, then $F(x)$ is an irreducible polynomial over $\mathbb{Q}$. Since $m \equiv -1\,(mod\,81)$, so, by Theorem 2.3, K is not monogenic.

(5) If $F(x) = x^{65625} - 7$, as $F(x)$ is 7-Eisenstein polynomial, then it is irreducible over $\mathbb{Q}$. Since $m \equiv 7\,(mod\,5^6)$, so, by Theorem 2.3, K is not monogenic.

(6) If $F(x) = x^{315} - 77^{19}$, $a = 77$, and $u = 19$, since $a \equiv 5\,(mod\,9)$, $a \equiv 2\,(mod\,25)$, and $a \equiv 28\,(mod\,49)$, then, by Theorem 2.4, K is monogenic.

(7) If $F(x) = x^{735} - 55^{23}$, $a = 55$, and $u = 23$, since $a \equiv 1\,(mod\,9)$, then by Theorem 2.4, K is not monogenic.

Acknowledgement. The authors would like to express their sincere gratitude to the anonymous referee, whose insightful criticism and advice significantly raised the caliber of this paper.

References

1. H. Ben Yakkou, A. Chillali and L. El Fadil, *On power integral bases for certain pure number fields defined by* $x^{2^r \cdot 5^s} - m$, Comm. Algebra **49** (2021), no. 7, 2916–2926.
2. M.E. Charkani and M. Sahmoudi, *Sextic extension with cubic subfield*, Jp J. Algebra Number Theory Appl. **34** (2014), no. 2, 139–150.
3. A. Deajim and L. El Fadil, *On the integral closedness of* $R[\alpha]$, Math. Rep. (Bucur.) **24(74)** (2022), no. 3, 571–581.
4. L. El Fadil, *On power integral bases of any pure number field defined by* $x^{36} - m$, Studia Sci. Math. Hungar. **58** (2021), no. 3, 371–380.
5. L. El Fadil, *On monogenity of certain pure number fields defined by* $x^{20} - m$, Sao Paulo J. Math. Sci. **16** (2021) 1063–1071.
6. L. El Fadil, *On integral bases and monogeneity of pure sextic number fields with non-square coefficients*, J. Number Theory **228** (2021) 375–389.
7. L. El Fadil, *On power integral bases for certain pure number fields*, Publ. Math. Debrecen **100** (2022), no. 1-2, 219–231.
8. L. El Fadil, *On power integral bases of certain pure numberfields defined by* $x^{3^r.7^s} - m$, Colloq. Math. **169** (2022), no. 2, 307–317.
9. L. El Fadil, J. Montes and E. Nart, *Newton polygons and p-integral bases of quartic number fields*, J. Algebra and Appl. **11** (2012), no. 4, 1250073.

10. L. El Fadil and A. Najim, *On monogenity of certain pure number fields defined by* $x^{2^r \cdot 3^s} - m$, Acta Sci. Math. **88** (2022), no. 3-4, 581–594.
11. I. Gaál and L. Remete, *Non-monogeneity in a family of octic fields*, Rocky Mountain J. Math., **47** (2017), no. 3, 817–824.
12. I. Gaál and L. Remete, *Power integral bases and monogeneity of pure fields*, J. Number Theory **173** (2017) 129–146.
13. J. Guárdia, J. Montes and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416.
14. A. Hameed, T. Nakahara, S. M. Husnine and S. Ahmed, *On the existence of canonical number system in certain classes of pure algebraic number fields*, J. Prime Res. Math. **7** (2011) 19–24.
15. N. Khan, T. Nakahara and H. Sekiguchi, *On the monogeneity of cyclic sextic fields of composite conductor*, J. Math. **50** (2018), no. 3, 67–73.
16. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.
17. O. Ore, *Newtonsche polygone in der theorie der algebraischen Korper*, Math. Ann. **99** (1928) 84–117.
18. M. Sahmoudi and M.E. Charkani, *On relative pure cyclic fields with power integral bases*, Math. Bohem. **148** (2022), no.1, 1-12.
19. M. Sahmoudi, M.E. Charkani and A. Soullami, *Tower Index formula and monogenecity*, Comm. Algebra **48** (2021), no. 1, 139–150.
20. M. Sahmoudi and A. Soullami, *On sextic integral bases using relative quadratic extension*, Bol. Soc. Parana. Mat. (3) **38** (2020), no. 4, 175–180.
21. M. Sahmoudi and A. Soullami, *On monogenicity of relative cubic-power pure extensions*, Adv. Math. Sci. J. **9** (2020), no.9, 6817–6827.
22. M. Sahmoudi, A. Soullami and O. Boughaleb, *Power integral basis for relative extensions of* p^n*-power number fields*, submitted.
23. H. Smith, *The monogeneity of radical extensions*, Acta Arith. **198** (2021), no. 3, 313–327.
24. A. Soullami, M. Sahmoudi and O. Boughaleb, *On relative power integral bases in a family of numbers fields*, Rocky Mountain J. Math. **51** (2021), no. 4, 1443–1452.

[1]Sidi Mohamed Ben Abdellah University, Polydisciplinary Faculty of Taza, Laboratory of Engineering Sciences, Road to Oujda B.P. 1223, Taza, Morocco.

[2]Moulay Ismail University, Faculty of Sciences Meknes, Laboratory of Pure Mathematics, B.P. 11201 Zitoune, Meknes, Morocco.

Email address: jalal.didi@usmba.ac.ma; m.sahmoudi@umi.ac.ma; abdelhakim.chillali@usmba.ac.ma