REVISTA DE LA UNIÓN MATEMÁTICA ARGENTINA
Vol. 65, No. 1, 2023, Pages 197–211
Published online: June 28, 2023
https://doi.org/10.33044/revuma.2836

ON POWER INTEGRAL BASES OF CERTAIN PURE NUMBER FIELDS DEFINED BY $x^{84} - m$

LHOUSSAIN EL FADIL AND MOHAMED FARIS

Abstract. Let $K = \mathbb{Q}(\alpha)$ be a pure number field generated by a complex root α of a monic irreducible polynomial $F(x) = x^{84} - m$, with $m \neq \pm 1$ a square-free integer. In this paper, we study the monogeneity of K. We prove that if $m \not\equiv 1 \pmod 4$, $m \not\equiv \pm 1 \pmod 9$, and $\overline{m} \notin \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \pmod{49}$, then K is monogenic. But if $m \equiv 1 \pmod 4$ or $m \equiv \pm 1 \pmod 9$ or $m \equiv 1 \pmod{49}$, then K is not monogenic. Some illustrating examples are given.

1. Introduction

Let K be a number field generated by a complex root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$ and $\mathbb{Z}_K$ its ring of integers. Let $\theta \in \mathbb{Z}_K$ be a primitive element of K. It is well known that the ring $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$. Thus, the Abelian group $\mathbb{Z}_K/\mathbb{Z}[\theta]$ is finite. Its cardinal order is called the index of $\mathbb{Z}[\theta]$, denoted by $\mathrm{ind}(\theta) = (\mathbb{Z}_K : \mathbb{Z}[\theta])$. For a rational prime integer p, if p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\theta])$, then thanks to a well-known theorem of Dedekind, the factorization of the ideal $p\mathbb{Z}_K$ can be derived directly from the factorization of $\overline{F}(x)$ over $\mathbb{F}_p$. In 1878, Dedekind gave a criterion to test whether p divides or not the index $(\mathbb{Z}_K : \mathbb{Z}[\theta])$ ([5]). If p does not divide $\mathrm{ind}(\theta)$ for every rational prime integer p for some primitive element $\theta \in \mathbb{Z}_K$ of K, then $\mathbb{Z}_K$ admits $(1, \theta, \ldots, \theta^{n-1})$ as a power $\mathbb{Z}$-integral basis. The field K is said to be monogenic in such a case, and not monogenic otherwise. The problem of testing the monogeneity of number fields and constructing power integral bases has been intensively studied over the last four decades, mainly by Gaál, Nakahara, Pohst, and their collaborators (see, for instance, [1, 18, 19, 20, 33, 29, 26, 27, 17]). In [17], Funakura calculated integral bases of pure quartic fields and studied their monogeneity. In [21], Gaál and Remete calculated the elements of index 1 of pure quartic fields generated by $m^{\frac{1}{4}}$ for $1 < m < 10^7$ and $m \equiv 2, 3 \pmod 4$. In [2], Ahmad, Nakahara, and Husnine proved that if $m \equiv 2, 3 \pmod 4$ and $m \not\equiv \mp 1 \pmod 9$, then the sextic number field generated by $m^{\frac{1}{6}}$ is monogenic. They also showed in [1] that if $m \equiv 1 \pmod 4$ and $m \not\equiv \mp 1 \pmod 9$, then the sextic number field generated by $m^{\frac{1}{6}}$ is not monogenic. In [11], based on prime ideal factorization, El Fadil showed that if $m \equiv 1 \pmod 4$

2020 *Mathematics Subject Classification.* 11R04, 11Y40, 11R21.
Key words and phrases. Index theorem, extension of valuations, Newton polygon.

or $m \equiv 1 \pmod 9$, then the sextic number field generated by $m^{\frac{1}{6}}$ is not monogenic. Also, Hameed and Nakahara [25] proved that if $m \equiv 1 \pmod{16}$, then the octic number field generated by $m^{\frac{1}{8}}$ is not monogenic, but if $m \equiv 2, 3 \pmod 4$, then it is monogenic. In [22], by applying the explicit form of the index, Gaál and Remete obtained new deep results on monogeneity of pure number fields generated by $m^{\frac{1}{n}}$, where $3 \leq n \leq 9$. In 2020, based on Newton polygon techniques, El Fadil et al. studied the monogeneity of some pure number fields [12, 13, 14, 9, 10], namely pure number fields of degrees $12, 18, 20, 24$, and 36. In this paper, we study the monogeneity of any pure number field K of degree 84, generated by a complex root α of a monic irreducible polynomial $F(x) = x^{84} - m$, with $m \neq \pm 1$ a square-free integer.

2. Main results

Let K be a pure number field generated by a complex root α of a monic irreducible polynomial $F(x) = x^{84} - m$, where $m \neq \pm 1$ is a square-free integer.

Theorem 2.1. *The ring $\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if $m \not\equiv 1 \pmod 4$, $m \not\equiv \pm 1 \pmod 9$, and $\overline{m} \notin \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \pmod{49}$.*

Remark that based on Theorem 2.1, if $m \equiv 1 \pmod 4$ or $m \equiv \pm 1 \pmod 9$ or $\overline{m} \in \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \pmod{49}$, then $\mathbb{Z}[\alpha]$ is not integrally closed. But in this case, Theorem 2.1 cannot decide on the monogeneity of K. The following theorem gives a partial answer. It does give an answer for the cases $\overline{m} \in \{-\overline{1}, \pm\overline{18}, \pm\overline{19}\} \pmod{49}$.

Theorem 2.2. *If one of the following statements holds,*

(1) $m \equiv 1 \pmod 4$,
(2) $m \equiv \pm 1 \pmod 9$,
(3) $m \equiv 1 \pmod{49}$,

then K is not monogenic.

Corollary 2.3. *Let $F(x) = x^{84} - a^u$, with $a \neq \pm 1$ a square-free integer and $u < 84$ a positive integer which is coprime to 42. Then $F(x)$ is irreducible over $\mathbb{Q}$. Let K be the pure number field generated by a complex root α of $F(x)$. Then we have the following results:*

(1) *If $a \not\equiv 1 \pmod 4$, $a \not\equiv \pm 1 \pmod 9$, and $\overline{a} \notin \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \pmod{49}$, then K is monogenic.*
(2) *If $a \equiv 1 \pmod 4$ or $a \equiv \pm 1 \pmod 9$ or $a \equiv 1 \pmod{49}$, then K is not monogenic.*

3. Preliminaries

For the convenience of the reader, the content of this section is copied from [12], as it is necessary for the proof of our main results.

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a complex root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$, $\mathbb{Z}_K$ its ring of integers, and $\operatorname{ind}(\alpha) = (\mathbb{Z}_K : \mathbb{Z}[\alpha])$ the index of $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_K$. For a rational prime integer p, if p does not divide

$(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, then a well-known theorem of Dedekind says that the factorization of $p\mathbb{Z}_K$ can be derived directly from the factorization of $\overline{F}(x)$ in $\mathbb{F}_p[x]$. Namely:

$$p\mathbb{Z}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{l_i} \quad \text{with every } \mathfrak{p}_i = p\mathbb{Z}_K + \phi_i(\alpha)\mathbb{Z}_K,$$

where $\overline{F}(x) = \prod_{i=1}^{r} \overline{\phi}_i(x)^{l_i}$ is the factorization of $\overline{F}(x)$ into powers of monic irreducible coprime polynomials of $\mathbb{F}_p[x]$. So, $f(\mathfrak{p}_i) = \deg(\phi_i)$ is the residue degree of $\mathfrak{p}_i$ (see [31, Chapter I, Proposition 8.3]). In order to apply this theorem in an effective way, one needs a criterion to test whether p divides or not the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. In 1878, Dedekind proved the following criterion: For a number field K generated by a complex root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$ and a rational prime integer p, let $\overline{F}(x) = \prod_{i=1}^{r} \overline{\phi}_i(x)^{l_i}$ be the factorization of $\overline{F}(x)$ in $\mathbb{F}_p[x]$, where $\phi_1(x), \ldots, \phi_r(x)$ are monic polynomials of $\mathbb{Z}[x]$ and their reductions modulo p are pairwise coprime irreducible polynomials over $\mathbb{F}_p$. He considered $M(x) = \frac{1}{p}\left(F(x) - \prod_{i=1}^{r} \phi_i(x)^{l_i}\right)$ and proved the following theorem.

Theorem 3.1 ([5, Theorem 6.1.4] and [6])**.** *The following statements are equivalent:*

(1) *p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$.*
(2) *For every $i = 1, \ldots, r$, either $l_i = 1$ or $l_i \geq 2$ and $\overline{\phi_i}(x)$ does not divide $\overline{M}(x)$ in $\mathbb{F}_p[x]$.*

When Dedekind's criterion fails, that is, when p divides the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ for every primitive element $\alpha \in \mathbb{Z}_K$ of K, it is impossible to obtain the prime ideal factorization of $p\mathbb{Z}_K$ by applying Dedekind's theorem. In 1928, Ore developed an alternative approach for obtaining the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, the absolute discriminant, and the prime ideal factorization of the rational prime integer p in $\mathbb{Z}_K$ by using Newton polygon techniques (see, for instance, [16, 28, 32]). We start by recalling some fundamental facts on Newton polygons applied in algebraic number theory. For more details, we refer the reader to [8] and [24]. For any rational prime integer p and for any monic polynomial $\phi(x) \in \mathbb{Z}[x]$ whose reduction modulo p is irreducible in $\mathbb{F}_p[x]$, let $\mathbb{F}_\phi$ be the finite field $\frac{\mathbb{F}_p[x]}{(\overline{\phi}(x))}$. For any monic polynomial $F(x) \in \mathbb{Z}[x]$, upon the Euclidean division by successive powers of $\phi(x)$, we expand $F(x)$ as follows: $F(x) = \sum_{i=0}^{L} a_i(x)\phi(x)^i$ with $\deg(a_i) < \deg(\phi)$ for every $i = 0, \ldots, L$. This expansion is unique and is called the ϕ-expansion of $F(x)$. Let ν_p be the Gauss extension of ν_p to $\mathbb{Q}_p[x]$, defined by $\nu_p(a(x)) = \min\{\nu_p(a_i),\, i = 0, \ldots, n\}$ for every polynomial $a(x) = \sum_{i=0}^{n} a_i x^i$ with $a_i \in \mathbb{Q}_p$ for every $i = 0, \ldots, n$. The ϕ-Newton polygon of $F(x)$ with respect to p is the lower boundary of the convex envelope of the set of points $\{(i, \nu_p(a_i)) \mid i = 0, \ldots, L, a_i(x) \neq 0\}$ in the Euclidean plane, which is denoted by $N_\phi(F)$. Let $S_1, \ldots, S_t$ be the sides of $N_\phi(F)$. For every side S of $N_\phi(F)$, the length of S, denoted by $l(S)$, is the length of its projection to the x-axis, and its height, denoted by $H(S)$, is the length of its projection to the y-axis. Let $\lambda = H(S)/l(S)$; then $-\lambda$ is the slope of S. Let $\lambda = h/e$ with e and h two positive coprimes for $\lambda > 0$, $h = 0$ and $e = 1$ for $\lambda = 0$. Then e is called

the ramification index of S. Let $d = l(S)/e$ be the degree of S. If $\lambda \neq 0$, then $d = \gcd(l(S), H(S))$ and $h = H(S)/d$. Geometrically, $N_\phi(F)$ can be viewed as the process of joining different sides of $N_\phi(F)$, ordered by increasing slopes, which can be expressed by $N_\phi(F) = S_1 + \cdots + S_t$. The principal ϕ-Newton polygon of $F(x)$, denoted by $N_\phi^+(F)$, is the part of the polygon $N_\phi(F)$ which is determined by joining all sides of negative slopes. Let S be a side of $N_\phi(F)$ of length l, with initial point (s, u_s) and end point $(s+l, u_{s+l})$, where $u_i = \nu_p(a_i)$. For every $i = 1, \ldots, l$, we define the residue coefficients $c_i \in \mathbb{F}_\phi$ as follows:

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

where $(p, \phi(x))$ is the maximal ideal of $\mathbb{Z}[x]$ generated by p and $\phi(x)$. Let $-\lambda = -h/e$ be the slope of S, with h a non-negative integer and e a positive integer which is coprime to h. Let $d = l/e$ be the degree of S. Notice that as e is the smallest positive integer satisfying $e\lambda \in \mathbb{Z}$, the points with integer coordinates lying on S are exactly $(s, u_s), (s+e, u_s - h), \ldots, (s+de, u_s - dh)$. Thus, if i is not a multiple of e, then $(s+i, u_{s+i})$ lies strictly above S, and so $c_i = 0$. Let $R_\lambda(F)(y) = t_d y^d + t_{d-1} y^{d-1} + \cdots + t_1 y + t_0 \in \mathbb{F}_\phi[y]$, with $t_i = c_{ie}$ for every $i = 0, \ldots, d$, called the residual polynomial of $F(x)$ associated to the side S.

Remark. (1) Notice that, since (s, u_s) and $(s+l, u_{s+l})$ lie on S, we conclude that $t_d t_0 \neq 0$ in $\mathbb{F}_\phi$, $\deg(R_\lambda(F)) = d$, and $R_\lambda(F)(0) \neq 0$.

(2) Notice also that if $\nu_p(a_s) = 0$, $\lambda = 0$, and $\phi = x$, then $\mathbb{F}_\phi = \mathbb{F}_p$, and $c_i = \overline{a_{s+i}} \in \mathbb{F}_p$ for every $i = 0, \ldots, l$. Thus, this notion of residual coefficient generalizes the reduction modulo a maximal ideal and $R_\lambda(F)(y) \in \mathbb{F}_p[y]$ coincides with the reduction of $F(x)$ modulo the maximal ideal (p).

Let $N_\phi^+(F) = S_1 + \cdots + S_t$ be the principal ϕ-Newton polygon of $F(x)$ with respect to p, and $-\lambda_i$ the negative slope of the side S_i for every $i = 1 \ldots, t$. The polynomial $F(x)$ is said to be ϕ-regular with respect to p if $R_{\lambda_i}(F)(y)$ is square-free in $\mathbb{F}_\phi[y]$ for every $i = 1, \ldots, t$. Let $\overline{F}(x) = \prod_{i=1}^r \overline{\phi}_i(x)^{l_i}$ be the factorization of $\overline{F}(x)$ in $\mathbb{F}_p[x]$ for some monic polynomials $\phi_1(x), \ldots, \phi_r(x)$ of $\mathbb{Z}[x]$ such that their reductions are pairwise coprime in $\mathbb{F}_p[x]$. The polynomial $F(x)$ is said to be p-regular if $F(x)$ is ϕ_i-regular for every $i = 1, \ldots, r$. The theorem of Ore plays a key role in proving our main theorems: Let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial, with $\overline{\phi}(x)$ irreducible in $\mathbb{F}_p[x]$. As defined in [16, Def. 1.3], the ϕ-index of $F(x)$, denoted by $\operatorname{ind}_\phi(F)$, 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).

Now assume that $\overline{F}(x) = \prod_{i=1}^r \overline{\phi}_i(x)^{l_i}$ is the factorization of $\overline{F}(x)$ in $\mathbb{F}_p[x]$, where $\phi_1(x), \ldots, \phi_r(x)$ are monic polynomials of $\mathbb{Z}[x]$ and $\overline{\phi}_1(x), \ldots, \overline{\phi}_r(x)$ are pairwise coprime irreducible polynomials over $\mathbb{F}_p$. For every $i = 1, \ldots, r$, let $N_{\phi_i}^+(F) = S_{i1} + \cdots + S_{it_i}$ be the principal part of the ϕ_i-Newton polygon of $F(x)$ with respect to p. For every $j = 1, \ldots, t_i$, let $R_{\lambda_{ij}}(F)(y) = \prod_{s=1}^{s_{ij}} \psi_{ijs}(y)^{a_{ijs}}$ be the factorization

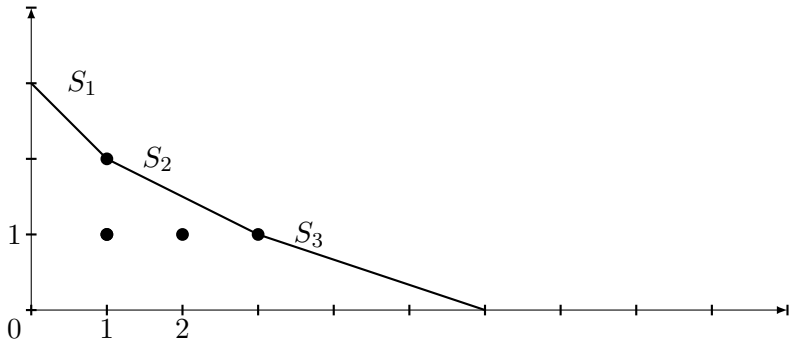

FIGURE 1. $N_\phi^+(F)$.

of $R_{\lambda_{ij}}(F)(y)$ into powers of monic irreducible polynomials in $\mathbb{F}_{\phi_i}[y]$. Then we have the following theorem of Ore (see [16, Theorems 1.7 and 1.9], [8, Theorem 3.9], and [28]):

Theorem 3.2 (Theorem of Ore)**.**

(1) $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) \geq \sum_{i=1}^{r} \operatorname{ind}_{\phi_i}(F)$. *The equality holds if $F(x)$ is p-regular.*

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

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

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 for every $i = 1, \ldots, r$, $j = 1, \ldots, t_i$, and $s = 1, \ldots, s_{ij}$.

Corollary 3.3. *Under the hypothesis before Theorem 3.2, if $l_i = 1$ or $N_{\phi_i}^+(F) = S_i$ has a single side of height 1 for every $i = 1, \ldots, r$, then $F(x)$ is p-regular and $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$.*

A proof of Ore's theorem of index is given in [16, Theorem 1.7 and Theorem 1.9].

Remark. We recall a generalization of the theorem of index of Ore, given in [24, Theorem 4.18], in which Guardia, Montes, and Nart introduced the notion of the r-index of $F(x)$, $\operatorname{ind}_r(F)$, for each order $r \geq 1$, where $\operatorname{ind}_1(F)$ coincides with the index given in Theorem 3.2. They showed that

$$\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) \geq \sum_{i=1}^{r} \operatorname{ind}_i(F),$$

and the equality holds if and only if $\operatorname{ind}_r(F) = 0$. In particular, $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$ if and only if $\operatorname{ind}_1(F) = 0$.

The following lemma allows one to determine the ϕ-Newton polygon of $F(x)$. For its proof, we refer the reader to [15].

Lemma 3.4. *Let $F(x) = x^n - m \in \mathbb{Z}[x]$ be an irreducible polynomial and p a rational prime integer which divides n and does not divide m. Let $n = p^r t$ with p not dividing t in $\mathbb{Z}$. Then $\overline{F}(x) = (x^t - m)^{p^r}$ in $\mathbb{F}_p[x]$. Let $v = \nu_p(m^p - m)$ and let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $\overline{\phi}(x)$ divides $\overline{F}(x)$ in $\mathbb{F}_p[x]$. Let $x^t - m = \phi(x)Q(x) + R(x)$. Then $\nu_p(R) \geq 1$. Moreover,*

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

4. Proofs of the main results

Proof of Theorem 2.1.

Proof. The proof of this theorem can be established by Dedekind's criterion, as shown in [34, Theorem 6.1]. But as the other results are based on Newton polygon techniques, let us use the theorem of the index as it is given in [24, Theorem 4.18], which establishes an equivalence between $\nu_p(\mathbb{Z}_K : \mathbb{Z}[\alpha]) = 0$ and $\mathrm{ind}_1(F) = 0$, where $\mathrm{ind}_1(F)$ is the index of $F(x)$ obtained by Ore's index theorem. Since $\Delta(F) = \pm(84)^{84} \cdot m^{83}$, thanks to the formula $\nu_p(\Delta(F)) = \nu_p(d_K) + 2\nu_p(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, $\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ for every rational prime integer dividing $2 \cdot 3 \cdot 7 \cdot m$.

(1) Let p be a rational prime integer dividing m; then $F(x) \equiv x^{84} \pmod{p}$ and $\phi = x$. Since m is a square-free integer, $\nu_p(m) = 1$, and so $N_\phi(F) = S$ has a single side joining the points $(0, 1)$ and $(84, 0)$. Thus, $\mathrm{ind}_1(F) = 0$, which means that $\nu_p(\mathbb{Z}_K : \mathbb{Z}[\alpha]) = 0$; p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. Therefore the unique rational prime candidates to divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ are 2, 3, and 7.

(2) If $p = 2$ and 2 does not divide m, then $F(x) \equiv x^{84} - 1 \equiv (x^{21} - 1)^4 \pmod{2}$. Let $v = \nu_2(m-1)$ and let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial whose reduction modulo 2 is an irreducible factor of $\overline{F}(x)$ in $\mathbb{F}_2[x]$. By Lemma 3.4, $N_\phi^+(F)$ is the lower boundary of the convex envelope of the set of points $\{(0, v), (1, 2), (2, 1), (4, 0)\}$ or $\{(0, V), (2, 1), (4, 0)\}$ for some integer $V \geq 3$. By [24, Theorem 4.18], $\nu_2((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$ if and only if $\mathrm{ind}_\phi(F) = 0$, where $\mathrm{ind}_\phi(F)$ is the ϕ-index of F calculated by the theorem of index of Ore. Thus, $\nu_2((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$ if and only if $N_\phi^+(F)$ has a single side of height 1, say $v = 1$, which means that $m \not\equiv 1 \pmod{4}$.

(3) Similarly, if $p = 3$ and 3 does not divide m, we have $F(x) = (x^{28} - m)^3 \pmod{3}$. Let $v = \nu_3(m^2 - 1)$ and let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial whose reduction modulo 3 is an irreducible factor of $\overline{F}(x)$ in $\mathbb{F}_3[x]$. Then $N_\phi^+(F)$ is the lower boundary of the convex envelope of the set of points $\{(0, v), (1, 1), (3, 0)\}$ or $\{(0, V), (1, 1), (3, 0)\}$ for some integer $V \geq 2$. By [24, Theorem 4.18], $\nu_3((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$ if and only if $v = 1$, which means that $m \not\equiv \pm 1 \pmod{9}$.

(4) Finally, if $p = 7$ and 7 does not divide m, we have $F(x) = (x^{12} - m)^7 \pmod 7$. Let $v = \nu_7(m^6 - 1)$ and $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial whose reduction modulo 7 is an irreducible factor of $\overline{F}(x)$ in $\mathbb{F}_7[x]$. Then $N_\phi^+(F)$ is the lower boundary of the convex envelope of the set of points $\{(0, v), (1, 1), (7, 0)\}$ or $\{(0, V), (1, 1), (7, 0)\}$ for some integer $V \geq 2$. By [24, Theorem 4.18], $\nu_7((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$ if and only if $v = 1$, which means that $m \notin \{\pm 1, \pm 18, \pm 19\} \pmod{49}$. □

The index of a field K is defined as $i(K) = \gcd\{(\mathbb{Z}_K : \mathbb{Z}[\theta]) \mid K = \mathbb{Q}(\theta) \text{ and } \theta \in \mathbb{Z}_K\}$. A rational prime integer p dividing $i(K)$ is called a common index divisor of K. If $\mathbb{Z}_K$ has a power integral basis, then $i(K) = 1$. Therefore a field having a common index divisor is not monogenic. The existence of common index divisors was first established in 1871 by Dedekind, who exhibited examples in fields of third and fourth degrees. For example, he considered the cubic field K defined by $x^3 - x^2 - 2x - 8$ and he showed that the prime 2 splits completely in $\mathbb{Z}_K$. So, if we suppose that K is monogenic, then we would be able to find a cubic polynomial generating K that splits completely into distinct polynomials of degree 1 in $\mathbb{F}_2[x]$. Since there are only 2 distinct polynomials of degree 1 in $\mathbb{F}_2[x]$, this is impossible. Based on these ideas and using Kronecker's theory of algebraic numbers, Hensel gave a necessary and sufficient condition on the so-called "index divisors" for any rational prime integer p to be a common index divisor [27]. (For more details, see [34]). For the proof of Theorem 2.2, we need the following lemma, which characterizes the common index divisors of K. We need to use only one way, which is an immediate consequence of Dedekind's theorem.

Lemma 4.1 ([34, Theorem 2.2])**.** *Let p be a rational prime integer and K a number field. For every positive integer f, let $\mathcal{P}_f$ be the number of distinct prime ideals of $\mathbb{Z}_K$ lying above p with residue degree f and $\mathcal{N}_f$ the number of monic irreducible polynomials of $\mathbb{F}_p[x]$ of degree f. Then p is a common index divisor of K if and only if $\mathcal{P}_f > \mathcal{N}_f$ for some positive integer f.*

Remark. As it was shown in the proof of Theorem 2.1, the only rational prime integers which can be common index divisors of K are 2, 3, and 7, because if $p \notin \{2, 3, 7\}$ then p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, and so the factorization of $p\mathbb{Z}_K$ is analogous to the factorization of $x^{84} - m$ in $\mathbb{F}_p[x]$.

Remark. In order to prove Theorem 2.2, we don't need to determine the factorization of $p\mathbb{Z}_K$ explicitly. But according to Lemma 4.1, we need only to show that $\mathcal{P}_f > \mathcal{N}_f$ for an adequate positive integer f. So, in practice, the second point of Theorem 3.2, could be replaced by the following: If $l_i = 1$ or $d_{ij} = 1$ or $a_{ijs} = 1$ for some (i, j, s) according to the notations of Theorem 3.2, then ψ_{ijs} provides a prime ideal $\mathfrak{p}_{ijs}$ of $\mathbb{Z}_K$ lying above p with residue degree $f_{ijs} = \deg(\phi_i) \times t_{ijs}$, where $t_{ijs} = \deg(\psi_{ijs})$ and $p\mathbb{Z}_K = \mathfrak{p}_{ijs}^{e_{ij}} I$, where the factorization of the ideal I can be derived from the other factors of each residual polynomial of $F(x)$.

If p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, then thanks to Dedekind's theorem, the factorization of $p\mathbb{Z}_K$ can be derived directly from the factorization of $\overline{F}(x)$ in $\mathbb{F}_p[x]$.

For $p \in \{2, 3, 7\}$, the following lemma gives an idea about the factorization of $p\mathbb{Z}_K$ into prime ideals of $\mathbb{Z}_K$.

Lemma 4.2.

(1) If $m \equiv 1 \pmod 4$, then there are at least 2 prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each.

(2) If $m \equiv 1 \pmod 9$, then $3\mathbb{Z}_K = \prod_{i=1}^{7} \mathfrak{p}_{i11}\mathfrak{p}_{i21}^2$, where $\mathfrak{p}_{ij1}$ is a prime ideal of $\mathbb{Z}_K$ lying above 3 for every $i = 1, \ldots, 7$, $j = 1, 2$.

(3) If $m \equiv -1 \pmod 9$, then $3\mathbb{Z}_K = \prod_{i=1}^{6} \mathfrak{p}_{i11}\mathfrak{p}_{i21}^2$, where $\mathfrak{p}_{ij1}$ is a prime ideal of $\mathbb{Z}_K$ lying above 3 for every $i = 1, \ldots, 6$, $j = 1, 2$.

(4) If $m \equiv 1 \pmod{49}$, then $7\mathbb{Z}_K = \prod_{i=1}^{9} \mathfrak{p}_{i11}\mathfrak{p}_{i21}^6$, where $\mathfrak{p}_{ij1}$ is a prime ideal of $\mathbb{Z}_K$ lying above 7 for every $i = 1, \ldots, 9$, $j = 1, 2$.

Proof. (1) Assume that $m \equiv 1 \pmod 4$. Then $\overline{F}(x) = (x^{21}-1)^{2^2} = \prod_{i=1}^{6} \overline{\phi}_i(x)^4$ in $\mathbb{F}_2[x]$, with $\phi_1(x) = x-1$, $\phi_2(x) = x^2+x+1$, $\phi_3(x) = x^3+x+1$, $\phi_4(x) = x^3+x^2+1$, $\phi_5(x) = x^6 + x^4 + x^2 + x + 1$, $\phi_6(x) = x^6 + x^5 + x^4 + x^2 + 1$. Let $v = \nu_2(m-1)$.

(a) If $m \equiv 1 \pmod 8$, then $v \geq 3$. By Lemma 3.4, $N_{\phi_i}^+(F)$ is the lower boundary of the convex envelope of the set of points $(0, V_i)$, $(1, 2)$, $(2, 1)$, and $(4, 0)$ for some integer $V_i \geq 3$ for every $i = 1, \ldots, 6$. Let us show that there are at least 2 prime ideals of $\mathbb{Z}_K$ lying above 2 of residue degree 2 each. For $i = 2$, $\phi_2(x) = x^2 + x + 1$; if $V_2 = 3$, then $N_{\phi_2}^+(F) = S_{21} + S_{22}$ with respective residue degrees $d(S_{21}) = 2$ and $d(S_{22}) = 1$ (see Figure 2). Then the attached residual polynomial of $F(x)$ associated to S_{21} is $R_{\lambda_{21}}(F) = 1 + (x+1)y + xy^2 = (1+xy)(1+y) \in \mathbb{F}_{\phi_2}[y]$. Thus, ϕ_2 provides at least 2 different prime ideals lying above 2 with residue degree $2 \times 1 = 2$ each.

If $V_2 \geq 4$, then $N_{\phi_2}^+(F) = S_{21} + S_{22} + S_{23}$ has 3 distinct sides with the same residue degree 1 (see Figure 3). Then the attached residual polynomial $R_{\lambda_{2i}}(F)$ of $F(x)$ associated to S_{2i} has degree 1 for every $i = 1, 2, 3$. Thus, ϕ_2 provides at least 3 different prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree $2 \times 1 = 2$ each.

(b) If $m \equiv 5 \pmod 8$, then $v = 2$. By Lemma 3.4, $N_{\phi_2}^+(F) = S$ has a single side S joining the points $(0, 2)$, $(2, 1)$, and $(4, 0)$ (see Figure 4). Then the attached residual polynomial $R_{\lambda_2}(F)(y)$ of $F(x)$ associated to S is $R_{\lambda_2}(F)(y) = 1 + xy + (1+x)y^2 = (1+y)(1+(x+1)y) \in \mathbb{F}_{\phi_2}[y]$. Therefore ϕ_2 provides at least 2 different prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree $2 \times 1 = 2$ each.

(2) If $m \equiv 1 \pmod 9$, then $\overline{F}(x) = (x^{28} - 1)^3 = \prod_{i=1}^{7} \overline{\phi}_i(x)^3$ in $\mathbb{F}_3[x]$, with $\phi_1(x) = x - 1$, $\phi_2(x) = x + 1$, $\phi_3(x) = x^2 + 1$, $\phi_4(x) = x^6 + x^5 + x^3 + x + 1$, $\phi_5(x) = x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 2x + 1$, $\phi_6(x) = x^6 + 2x^5 + 2x^3 + 2x + 1$ and $\phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Let $v = \nu_3(m^2 - 1)$. Since $m \equiv 1 \pmod 9$, we conclude that $v \geq 2$. By Lemma 3.4, $N_{\phi_i}^+(F) = S_{i1} + S_{i2}$ has 2 sides joining $(0, V_i), (1, 1)$ and $(3, 0)$ for some integer $V_i \geq 2$. Thus, the degree of each side S_{ij} is 1 (see Figure 5) for every $i = 1, \ldots, 7$ and $j = 1, 2$. The ramification index of each prime ideal factor is given in the following table:

	$j=1$	$j=2$
$i=1$	1	2
$i=2$	1	2
$i=3$	1	2
$i=4$	1	2
$i=5$	1	2
$i=6$	1	2
$i=6$	1	2
$i=7$	1	2

By Theorem 3.2, we have $3\mathbb{Z}_K = \prod_{i=1}^{7} \mathfrak{p}_{i11}\mathfrak{p}_{i21}^2$, where $\mathfrak{p}_{ij1}$ is a prime ideal of $\mathbb{Z}_K$ lying above 3 for every $i = 1, \ldots, 7$ and $j = 1, 2$.

The residue degree f_{ij1} of each prime ideal factor is given in the following table:

	$j=1$	$j=2$
$i=1$	1	1
$i=2$	1	1
$i=3$	2	2
$i=4$	6	6
$i=5$	6	6
$i=6$	6	6
$i=7$	6	6

(3) If $m \equiv -1 \pmod 9$, then $\overline{F}(x) = (x^{28}+1)^3 = \prod_{i=1}^{6} \overline{\phi}_i(x)^3$ in $\mathbb{F}_3[x]$ with $\phi_1(x) = x^2+x+2$, $\phi_2(x) = x^2+2x+2$, $\phi_3(x) = x^6+2x^5+2x+2$, $\phi_4(x) = x^6+2x^4+2x^3+x^2+2$, $\phi_5(x) = x^6+x^5+x+2$, and $\phi_6(x) = x^6+2x^4+x^3+x^2+2$. Let $v = \nu_3(m^2-1)$. Since $m \equiv -1 \pmod 9$, we have $v \geq 2$. By Lemma 3.4, $N^+_{\phi_i}(F) = S_{i1} + S_{i2}$ has 2 sides joining $(0, V_i)$, $(1, 1)$, and $(3, 0)$ for some integer $V_i \geq 2$. Thus, the degree of each side S_{ij} is 1 (see Figure 5). The ramification index of each prime ideal factor is given in the following table:

	$j=1$	$j=2$
$i=1$	1	2
$i=2$	1	2
$i=3$	1	2
$i=4$	1	2
$i=5$	1	2
$i=6$	1	2

By Theorem 3.2, we conclude that $3\mathbb{Z}_K = \prod_{i=1}^{6} \mathfrak{p}_{i11}\mathfrak{p}_{i21}^2$, where $\mathfrak{p}_{ij1}$ is a prime ideal of $\mathbb{Z}_K$ lying above 3 for every $i = 1, \ldots, 6$, $j = 1, 2$. The residue degree f_{ij1} of each prime ideal factor is given by the following table:

	$j=1$	$j=2$
$i=1$	2	2
$i=2$	2	2
$i=3$	6	6
$i=4$	6	6
$i=5$	6	6
$i=6$	6	6

(4) If $m \equiv 1 \pmod{49}$, then $\overline{F}(x) = (x^{12}-1)^7 = \prod_{i=1}^{9} \overline{\phi}_i(x)^7$ in $\mathbb{F}_7[x]$, with $\phi_k(x) = x - i$ for every $i = 1, \ldots, 6$, $\phi_7(x) = x^2 + 1$, $\phi_8(x) = x^2 + 2$, and $\phi_9(x) = x^2 + 4$. Let $v = \nu_7(m^6 - 1)$. Since $m \equiv 1 \pmod{49}$, we have $v \geq 2$. By Lemma 3.4, $N_{\phi_i}^{+}(F) = S_{i1} + S_{i2}$ has 2 sides joining $(0, V_i), (1, 1)$, and $(7, 0)$ for some integer $V_i \geq 2$. Thus, each side S_{ij} of $N_{\phi_i}^{+}(F)$ has degree 1 (see Figure 6). The ramification index of each prime ideal factor is given by the following table:

	$j=1$	$j=2$
$i=1$	1	6
$i=2$	1	6
$i=3$	1	6
$i=4$	1	6
$i=5$	1	6
$i=6$	1	6
$i=7$	1	6
$i=8$	1	6
$i=9$	1	6

By Theorem 3.2, we have $7\mathbb{Z}_K = \prod_{i=1}^{9} \mathfrak{p}_{i11}\mathfrak{p}_{i21}^6$, where $\mathfrak{p}_{ij1}$ is a prime ideal of $\mathbb{Z}_K$ lying above 7 for every $i = 1, \ldots, 9$, $j = 1, 2$. The residue degree f_{ij1} of each prime ideal factor is given by the following table:

	$j=1$	$j=2$
$i=1$	1	1
$i=2$	1	1
$i=3$	1	1
$i=4$	1	1
$i=5$	1	1
$i=6$	1	1
$i=7$	2	2
$i=8$	2	2
$i=9$	2	2

□

Proof of Theorem 2.2

In every case, let us show that $i(K) > 1$. According to Lemma 4.1, it suffices to show that, for an adequate rational prime integer p, there are at least $N_f + 1$ prime ideals of $\mathbb{Z}_K$ lying above p for an adequate positive integer f.

Proof. (1) For $m \equiv 1 \pmod 4$, by Lemma 4.2, there are at least 2 distinct prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each. There is only one monic irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, namely, $x^2 + x + 1$. By Lemma 4.1, we conclude that 2 divides $i(K)$, and so K is not monogenic.

(2) For $m \equiv 1 \pmod 9$, by Lemma 4.2 there are 4 prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. As there are only 3 monic irreducible polynomials of degree 1 in $\mathbb{F}_3[x]$, by Lemma 4.1 we conclude that 3 is a common index divisor of K, and so K is not monogenic. If $m \equiv -1 \pmod 9$, then by Lemma 4.2 there are 4 prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 2 each. As there are only 3 monic irreducible polynomials of degree 2 in $\mathbb{F}_3[x]$, by Lemma 4.1 we conclude that 3 is a common index divisor of K, and so K is not monogenic.

(3) If $m \equiv 1 \pmod{49}$, then by Lemma 4.2 there are at least 12 prime ideals of $\mathbb{Z}_K$ lying above 7 with residue degree 1 each. As there are only 7 monic irreducible polynomials of degree 1 in $\mathbb{F}_7[x]$, by Lemma 4.1 we conclude that 7 is a common index divisor of K, and so K is not monogenic. □

Proof of Corollary 2.3

Proof. Let α be a complex root of $F(x)$ and $K = \mathbb{Q}(\alpha)$. Since u is coprime to 84, let $(x, y) \in \mathbb{Z}^2$ be the unique solution of $ux - 84y = 1$ with $0 \leq x < 84$. Let also $\theta = \frac{\alpha^x}{a^y}$. Then $\theta^{84} = \frac{\alpha^{84x}}{a^{84y}} = \frac{a^{ux}}{a^{84y}} = a^1$. Since $a \neq \pm 1$ is a square-free integer, $g(x) = x^{84} - a$ is an Eisenstein polynomial, and so is irreducible over $\mathbb{Q}$. Thus, $g(x)$ is the minimal polynomial of θ over $\mathbb{Q}$. The fact that $\theta \in K$ implies that $[K : \mathbb{Q}] \geq [\mathbb{Q}(\theta) : \mathbb{Q}] = 84$. By definition of K and α, we have $[K : \mathbb{Q}] \leq 84$. Therefore, $[K : \mathbb{Q}] = 84$, and so $F(x)$ is irreducible over $\mathbb{Q}$. Since $\theta \in \mathbb{Z}_K$ is a primitive element of K, we conclude

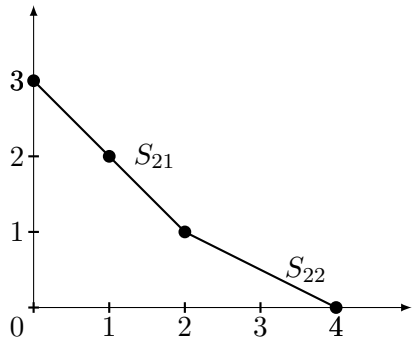

FIGURE 2. $N^+_{\phi_2}(F)$.

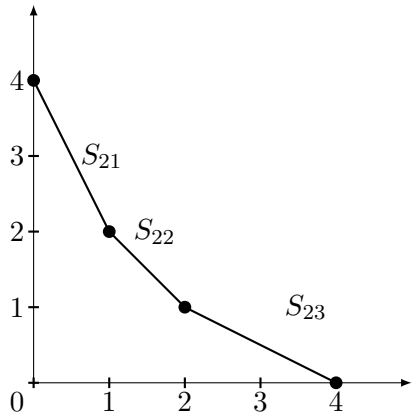

FIGURE 3. $N^+_{\phi_2}(F)$.

that K is generated by θ a root of $g(x) = x^{84} - a$ with $a \neq \pm 1$ a square-free integer. Therefore we can apply Theorems 2.1 and 2.2. □

5. Examples

Let $F(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial over $\mathbb{Q}$ and K the number field generated by a complex root α of $F(x)$.

(1) For $F(x) = x^{84} - 47$, $m = 47$; since $m \equiv 3 \pmod 4$, $m \equiv 2 \pmod 9$, and $m \equiv -2 \pmod{49}$, by Theorem 2.1, K is monogenic.
(2) For $F(x) = x^{84} - 25$, $m = 25$; since $m \equiv 1 \pmod 4$, by Theorem 2.2, K is not monogenic.
(3) For $F(x) = x^{84} - 42^{11}$, $a = 42$ and $u = 11$ is coprime to 42. Since $42 \equiv 2 \pmod 4$, $42 \equiv 6 \pmod 9$, and $42 \equiv -7 \pmod{49}$, by Corollary 2.3, K is monogenic.

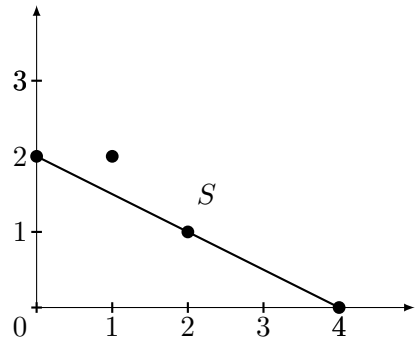

FIGURE 4. $N^+_{\phi_i}(F)$.

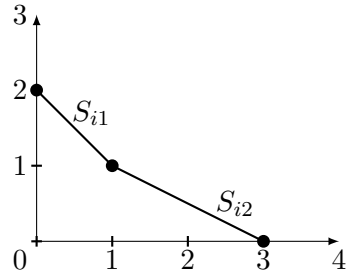

FIGURE 5. $N^+_{\phi_i}(F)$.

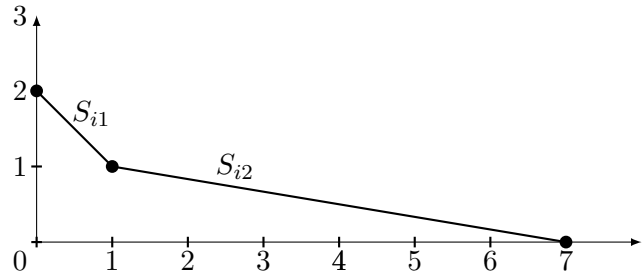

FIGURE 6. $N^+_{\phi_i}(F)$.

(4) For $F(x) = (x+7)^{84} - 14^{13}$, let $G(x) = F(x-7)$; then $G(x) = x^{84} - 14^{13}$, so $a = 14$ and $u = 13$ is coprime to 42. Since $14 \equiv 2 \pmod 4$, $14 \equiv 5 \pmod 9$, and $14 \equiv 14 \pmod{49}$, by Corollary 2.3, $F(x)$ is irreducible over $\mathbb{Q}$. Let K be the number field generated by a complex root α of $F(x)$. Then K is monogenic. More precisely, $\mathbb{Z}_K = \mathbb{Z}[\theta]$, where $\theta = \frac{(\alpha-7)^{13}}{14^2}$.

Acknowledgments

The authors are deeply grateful to the anonymous referee whose valuable comments and suggestions have tremendously improved the quality of this paper. The first author is deeply grateful to Professor István Gaál for his advice and encouragement to work on monogeneity of number fields. He would also like to thank Professor Enric Nart, who introduced him to Newton polygon techniques.

References

[1] S. Ahmad, T. Nakahara, and A. Hameed, On certain pure sextic fields related to a problem of Hasse, *Internat. J. Algebra Comput.* **26** (2016), no. 3, 577–583. MR 3506350.
[2] S. Ahmad, T. Nakahara, and S. M. Husnine, Power integral bases for certain pure sextic fields, *Int. J. Number Theory* **10** (2014), no. 8, 2257–2265. MR 3273484.
[3] M. Bauer, Über die außerwesentlichen Diskriminantenteiler einer Gattung, *Math. Ann.* **64** (1907), no. 4, 573–576. MR 1511458.
[4] A. Bérczes, J.-H. Evertse, and K. Győry, Multiply monogenic orders, *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)* **12** (2013), no. 2, 467–497. MR 3114010.
[5] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, 138, Springer, Berlin, 1993. MR 1228206.
[6] R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, *Göttingen Abh.* **23** (1878), 1–23.
[7] L. El Fadil, Computation of a power integral basis of a pure cubic number field, *Int. J. Contemp. Math. Sci.* **2** (2007), no. 13-16, 601–606. MR 2355834.
[8] L. El Fadil, On Newton polygons techniques and factorization of polynomials over Henselian fields, *J. Algebra Appl.* **19** (2020), no. 10, 2050188, 9 pp. MR 4140128.
[9] L. El Fadil, On power integral bases for certain pure number fields defined by $x^{24}-m$, *Studia Sci. Math. Hungar.* **57** (2020), no. 3, 397–407. MR 4188148.
[10] L. El Fadil, On power integral bases for certain pure number fields defined by $x^{36}-m$, *Studia Sci. Math. Hungar.* **58** (2021), no. 3, 371–380. https://doi.org/10.1556/012.2021.58.3.1506.
[11] L. El Fadil, On power integral bases for certain pure sextic fields, *Bol. Soc. Parana. Mat. (3)* **40** (2022), 7 pp. MR 4416656.
[12] L. El Fadil, On power integral bases for certain pure number fields, *Publ. Math. Debrecen* **100** (2022), no. 1-2, 219–231. MR 4389255.
[13] L. El Fadil, On power integral bases for certain pure number fields defined by $x^{18}-m$, *Comment. Math. Univ. Carolin.* **63** (2022), no. 1, 11–19. MR 4445734.
[14] L. El Fadil, On monogenity of certain pure number fields defined by $x^{20}-m$, *São Paulo J. Math. Sci.* **16** (2022), no. 2, 1063–1071. MR4515947.
[15] L. El Fadil, On power integral bases of certain pure number fields defined by $x^{3^r\cdot 7^s}-m$, *Colloq. Math.* **169** (2022), no. 2, 307–317. MR 4443656.
[16] L. El Fadil, J. Montes, and E. Nart, Newton polygons and p-integral bases of quartic number fields, *J. Algebra Appl.* **11** (2012), no. 4, 1250073, 33 pp. MR 2959422.
[17] T. Funakura, On integral bases of pure quartic fields, *Math. J. Okayama Univ.* **26** (1984), 27–41. MR 0779772.
[18] I. Gaál, Power integer bases in algebraic number fields, *Ann. Univ. Sci. Budapest. Sect. Comput.* **18** (1999), 61–87. MR 2118246.
[19] I. Gaál, *Diophantine Equations and Power Integral Bases*, second edition, Birkhäuser, Cham, 2019. MR 3970246.
[20] I. Gaál, P. Olajos, and M. E. Pohst, Power integral bases in orders of composite fields, *Experiment. Math.* **11** (2002), no. 1, 87–90. MR 1960303.
[21] I. Gaál and L. Remete, *Binomial Thue equations and power integral bases in pure quartic fields*, *JP J. Algebra Number Theory Appl.* **32** (2014), no. 1, 49–61.

[22] I. Gaál and L. Remete, Integral bases and monogenity of pure fields, *J. Number Theory* **173** (2017), 129–146. MR 3581912.
[23] T. A. Gassert, A note on the monogeneity of power maps, *Albanian J. Math.* **11** (2017), no. 1, 3–12. MR 3659215.
[24] J. Guàrdia, J. Montes, and E. Nart, Newton polygons of higher order in algebraic number theory, *Trans. Amer. Math. Soc.* **364** (2012), no. 1, 361–416. MR 2833586.
[25] A. Hameed and T. Nakahara, Integral bases and relative monogenity of pure octic fields, *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)* **58(106)** (2015), no. 4, 419–433. MR 3443598.
[26] H. Hasse, *Zahlentheorie*, zweite erweiterte Auflage, Akademie-Verlag, Berlin, 1963. MR 0153659.
[27] K. Hensel, *Theorie der algebraischen Zahlen*, B. G. Teubner, Leipzig, Berlin, 1908.
[28] J. Montes and E. Nart, On a theorem of Ore, *J. Algebra* **146** (1992), no. 2, 318–334. MR 1152908.
[29] Y. Motoda, T. Nakahara, and S. I. A. Shah, On a problem of Hasse for certain imaginary abelian fields, *J. Number Theory* **96** (2002), no. 2, 326–334. MR 1932459.
[30] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, third edition, Springer Monographs in Mathematics, Springer, Berlin, 2004. MR 2078267.
[31] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, 322, Springer, Berlin, 1999. MR 1697859.
[32] O. Ore, Newtonsche Polygone in der Theorie der algebraischen Körper, *Math. Ann.* **99** (1928), no. 1, 84–117. MR 1512440.
[33] A. Pethő and M. E. Pohst, On the indices of multiquadratic number fields, *Acta Arith.* **153** (2012), no. 4, 393–414. MR 2925379.
[34] H. Smith, The monogeneity of radical extensions, *Acta Arith.* **198** (2021), no. 3, 313–327. MR 4232416.

Lhoussain El Fadil✉
Department of Mathematics, Faculty of Sciences Dhar-El Mahraz, University of Sidi Mohamed Ben Abdellah, P.O.B. 1796, Fes, Morocco
lhouelfadil2@gmail.com

Mohamed Faris
Department of Mathematics, Faculty of Sciences Dhar-El Mahraz, University of Sidi Mohamed Ben Abdellah, P.O.B. 1796, Fes, Morocco
mohamedfaris9293@gmail.com

Received: August 27, 2021
Accepted: November 2, 2021