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

(3s.) **v. 2023 (41)** : 1–9.
ISSN-0037-8712 IN PRESS
doi:10.5269/bspm.62352

On Monogenity of Certain Pure Number Fields Defined by $x^{2^r \cdot 7^s} - m$

Lhoussain El Fadil and Omar Kchit

ABSTRACT: Let K be a pure number field generated by a root of a monic irreducible polynomial $F(x) = x^{2^r \cdot 7^s} - m \in \mathbb{Z}[x]$, where $m \neq \pm 1$ is a square free integer, r and s are two positive integers. In this paper, we study the monogenity of K. We prove that if $m \not\equiv 1 \pmod 4$ and $\overline{m} \notin \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \pmod{49}$, then K is monogenic. But if $r \geq 2$ and $m \equiv 1 \pmod{16}$ or $s \geq 3$, $\overline{m} \in \{\overline{1}, \overline{18}, -\overline{19}\} \pmod{49}$, and $\nu_7(m^6 - 1) \geq 4$, then K is not monogenic. Some illustrating examples are given.

Key Words: Theorem of Dedekind, Theorem of Ore, prime ideal factorization, Newton polygon, index of a number field.

Contents

1. Introduction

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$ and $\mathbb{Z}_K$ its ring of integers. It is well known that the ring $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, and so the Abelian group $\mathbb{Z}_K/\mathbb{Z}[\alpha]$ is finite. Its cardinal order is called the index of $\mathbb{Z}[\alpha]$ and denoted $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. If for some primitive element $\theta \in \mathbb{Z}_K$ of K, we have $(\mathbb{Z}_K : \mathbb{Z}[\theta]) = 1$, then the ring $\mathbb{Z}_K$ has a power integral basis $(1, \theta, \ldots, \theta^{n-1})$. In such a case, the field K is said to be monogenic and not monogenic otherwise. For any primitive element α of $\mathbb{Z}_K$ (that is $\alpha \in \mathbb{Z}_K$ with $K = \mathbb{Q}(\alpha)$) we denote by

$$\mathrm{ind}(\alpha) = (\mathbb{Z}_K : \mathbb{Z}[\alpha])$$

the *index of* α, that is the index of the $\mathbb{Z}$-module $\mathbb{Z}[\alpha]$ in the free-$\mathbb{Z}$-module $\mathbb{Z}_K$ of rank n. As it is known [21], we have the following formula, which links the discriminant of $F(x)$, $\mathrm{ind}(\alpha)$, and the absolute discriminant d_K of K:

$$\triangle(F) = (\mathrm{ind}(\alpha))^2 \cdot d_K$$

where $\triangle(F)$ is the discriminant of $F(x)$. Obviously, $\mathrm{ind}(\alpha) = 1$ if and only if $(1, \alpha, \ldots, \alpha^{n-1})$ is an integral basis of $\mathbb{Z}_K$.

Monogenity of number fields is a classical problem of algebraic number theory, going back to Dedekind, Hasse and Hensel, cf e.g. [28,30] and [21] for the present state of this area. It is called a problem of Hasse to give an arithmetic characterization of those number fields which have a power integral basis [28,30,32]. The problem of testing the monogenity of number fields and constructing power integral bases have been intensively studied during the last decades, see for instance [2,22,35]. An especially delicate and intensively studied problem is the monogenity of *pure fields* K generated by a root α of

2010 *Mathematics Subject Classification:* 11R04, 11Y40, 11R21.
Submitted February 02, 2022. Published June 09, 2022

an irreducible polynomial $x^n - m$, mainly by Gaál, Nakahara, Pohst, and their research teams (see for instance [2,20,21,23,35]). In [10], El Fadil gave conditions for the existence of power integral bases of pure cubic fields in terms of the index form equation. In [19], Funakura, calculated integral bases and studied monogenity of pure quartic number fields. In [24], Gaál and Remete, calculated the elements of index 1 in pure quartic number fields generated by $m^{\frac{1}{4}}$ for $1 < m < 10^7$ and $m \equiv 2, 3 \pmod 4$. In [1], Ahmad, Nakahara, and Husnine proved that if $m \equiv 2, 3 \pmod 4$ and $m \not\equiv \pm 1 \pmod 9$, then the sextic number field generated by $m^{\frac{1}{6}}$ is monogenic. They also showed in [2], that if $m \equiv 1 \pmod 4$ and $m \not\equiv \pm 1 \pmod 9$, then the sextic number field generated by $m^{\frac{1}{6}}$ is not monogenic. In [17], based on prime ideal factorization, El Fadil showed that if $m \equiv 1 \pmod 4$ or $m \not\equiv 1 \pmod 9$, then the sextic number field generated by $m^{\frac{1}{6}}$ is not monogenic. Hameed and Nakahara [27], proved that if $m \equiv 1 \pmod{16}$, then the octic number field generated by $m^{1/8}$ is not monogenic, but if $m \equiv 2, 3 \pmod 4$, then it is monogenic. In [25], by applying the explicit form of the index equation, Gaál and Remete obtained deep new results on monogenity of the number fields generated by $m^{\frac{1}{n}}$, with $3 \leq n \leq 9$. While Gaál and Remete's techniques are based on the index calculation, Nakahara's methods are based on the existence of power relative integral bases of some special sub-fields. In [36], based on Dedekind's criterion, Smith gave some criterion to test monogenity of pure number fields. In [4,5,7,12,13,14,15], El Fadil et al. used Newton polygon techniques to study the monogenity of pure number fields of degrees 12, 24, 36, 60, p^r, $2^r \cdot 5^s$, and $2 \cdot 3^v$. In [6], Ben Yakkou and Kchit proved that if $m \not\equiv \pm 1 \pmod 9$, then the number fields defined by $x^{3^r} - m$ are monogenic, but these fields are not monogenic for $r \geq 3$ and $m \equiv \pm 1 \pmod{81}$. In this paper, based on Newton polygon techniques, we study the monogenity of any pure number field $K = \mathbb{Q}(\alpha)$ generated by a root α of a monic irreducible polynomial $F(x) = x^{2^r \cdot 7^s} - m$, with $m \neq \pm 1$ a square free integer, r and s two positive integers. The cases $r = 0$ or $s = 0$ were investigated in [5]. Recall that for $s = 0$ and $r \geq 2$, the monogenity of pure number fields of degree 2^r are previously studied in [3].

2. Main results

Let K be a pure number field generated by a root α of a monic irreducible polynomial $F(x) = x^{2^r \cdot 7^s} - m$, with $m \neq \pm 1$ a square free integer, r and s two positive integers.

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

Remark that: Based on Theorem 2.1, if $m \equiv 1 \pmod 4$ or $m \equiv \pm 1, \pm 18, \pm 19 \pmod{49}$, then $\mathbb{Z}[\alpha]$ is not the ring of integers of K. But in this case, Theorem 2.1 cannot decide on the monogenity of K. The following theorem gives a partial answer.

Theorem 2.2. *If one of the following conditions holds:*

1. *$r \geq 2$ and $m \equiv 1 \pmod{16}$,*
2. *$s \geq 3$, $\overline{m} \in \{\overline{1}, \overline{18}, -\overline{19}\} \pmod{49}$ and $\nu_7(m^6 - 1) \geq 4$,*

then K is not monogenic.

Theorem 2.3. *Let K be a pure number field generated by a root α of a monic irreducible polynomial $F(x) = x^{2^r \cdot 7^s} - a^u$, with $a \neq \pm 1$ a square free integer, $u < 2^r \times 7^s$ a positive integer, which is coprime to 14, r and s two positive integers. Then*

1. *If $a \not\equiv 1 \pmod 4$ and $a \not\equiv \pm 1, \pm 18, \pm 19 \pmod{49}$, then K is monogenic.*
2. *If $r \geq 2$ and $a \equiv 1 \pmod{16}$ or $s \geq 3$, $\overline{a} \in \{\overline{1}, \overline{18}, -\overline{19}\} \pmod{49}$, and $\nu_7(a^6 - 1) \geq 4$, then K is not monogenic.*

3. Examples

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

1. If $F(x) = x^{14} - 55$, then $F(x)$ is irreducible because it is 5-Eisenstein. Since $m = 55 \equiv 3 \pmod 4$ and $m \equiv 6 \pmod{49}$, by Theorem 2.1 K is monogenic.
2. If $F(x) = x^{56} - 26$, then $F(x)$ is irreducible because it is 2-Eisenstein. Since $m = 26 \equiv 2 \pmod 4$ and $m \equiv 26 \pmod{49}$, by Theorem 2.1 K is monogenic.
3. If $F(x) = x^{28} - 65$, then $m = 65 \equiv 1 \pmod{16}$. By Theorem 2.2, K is not monogenic.
4. If $F(x) = x^{112} - 113^5$, then $m = 113 \equiv 1 \bmod 16$ and $\nu_2(m-1) = 4$. By Theorem 2.3, K is not monogenic.
5. If $F(x) = (x-4)^{392} - 14^9$, then $F(x) \equiv (x-4)^{392} \pmod 2$. As $m = 14 \equiv 14 \pmod{16}$, $m \equiv 14 \pmod{49}$, and 9 is coprime with 14, then by Theorem 2.3, K is monogenic.
6. If $F(x) = x^{686} - 1047$, then $F(x)$ is irreducible because it is 3-Eisenstein. Since $m = 1047 \equiv 18 \pmod{49}$ and $m^6 \equiv 1 \pmod{7^4}$. By Theorem 2.2, K is not monogenic.

4. Preliminaries

Throughout the present section, let us assume that $\overline{F(x)} = \prod_{i=1}^{r} \overline{\phi_i(x)}^{l_i} \pmod p$ is the factorization of $\overline{F(x)}$ over $\mathbb{F}_p$, where p is a rational prime integer, $\forall i = 1, \ldots, r$, $\phi_i \in \mathbb{Z}[x]$ is a monic polynomial whose reduction is irreducible in $\mathbb{F}_p[x]$, and $GCD(\overline{\phi_i}, \overline{\phi_j}) = 1$, for every $i \neq j = 1, \ldots, r$.
Recall that a theorem of Dedekind says that:

Theorem 4.1. (*[33, Chapter I, Proposition 8.3]*)
If p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, then

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

and the residue degree of $\mathfrak{p}_i$ is $f(\mathfrak{p}_i) = deg(\phi_i)$.

In order to apply this theorem in an effective way, one needs a criterion to test whether p divides the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. In this sense, a criterion was developed by Dedekind to test whether p divides $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. In 1878, he considered $M(x) \in \mathbb{Z}[x]$, where $M(x) = \dfrac{F(x) - \prod_{i=1}^{r} \phi_i(x)^{l_i}}{p}$, and proved the following well known Dedekind's criterion:

Theorem 4.2. (*[8, Theorem 6.1.4] and [9]*)
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, p divides the index $(\mathbb{Z}_K : \mathbb{Z}[\theta])$ for every primitive element $\theta \in \mathbb{Z}_K$ of K, then for such primes and number fields, it is not possible to obtain the prime ideal factorization of $p\mathbb{Z}_K$ by Dedekind's theorem of factorization. In 1928, Ore developed an alternative approach for obtaining the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, the absolute discriminant d_K of K, and the prime ideal factorization of the rational primes in a number field K by using Newton polygons. For more details, we refer to [11,18,26,34].

For any prime integer p and for any monic polynomial $\phi \in \mathbb{Z}[x]$ whose reduction is irreducible in $\mathbb{F}_p[x]$, let $\mathbb{F}_\phi$ be the finite field $\mathbb{F}_p[x]/(\overline{\phi})$. For any monic polynomial $F(x) \in \mathbb{Z}[x]$, upon to the successive

Euclidean division by ϕ, we expand $F(x)$ as $F(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_l(x)\phi(x)^l$, called the ϕ-expansion of $F(x)$, (for every i, $\deg(a_i(x)) < \deg(\phi)$). To any coefficient $a_i(x)$ we attach $u_i = \nu_p(a_i(x)) \in \mathbb{Z} \cup \{\infty\}$. The ϕ-Newton polygon of $F(x)$ with respect to p, is the lower boundary convex envelope of the set of points $\{(i, u_i),\ a_i(x) \neq 0\}$ in the Euclidean plane, which we denote by $N_\phi(F)$. The ϕ-Newton polygon of F, is the process of joining the obtained edges $S_1, \ldots, S_t$ ordered by increasing slopes, which can be expressed as $N_\phi(F) = S_1 + \cdots + S_t$. The principal ϕ-Newton polygon of F, denoted $N_\phi^+(F)$, is the part of the polygon $N_\phi(F)$, which is determined by joining all sides of negative slopes. For every side S of $N_\phi^+(F)$, the length of S, denoted $l(S)$, is the length of its projection to the x-axis and its height, denoted $h(S)$, is the length of its projection to the y-axis. Let $d = \gcd(l(S), h(S))$ be the degree of S. For every side S of $N_\phi^+(F)$, with initial point (s, u_s), length l, and for every $i = 0, \ldots, l$, we attach the following *residue coefficient* $c_i \in \mathbb{F}_\phi$ as follows:

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

where $(p, \phi(x))$ is the maximal ideal of $\mathbb{Z}[x]$ generated by p and ϕ. Let $\lambda = -h/e$ be the slope of S, where h and e are two positive coprime integers. Then $d = l/e$ is the degree of S. Since the points with integer coordinates lying on S are exactly

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

if i is not a multiple of e, then $(s+i, u_{s+i})$ does not lie on S, and so $c_i = 0$. Let

$$R_\lambda(F)(y) = t_d y^d + t_{d-1} y^{d-1} + \cdots + t_1 y + t_0 \in \mathbb{F}_\phi[y],$$

called the residual polynomial of $F(x)$ associated to the side S, where for every $i = 0, \ldots, d$, $t_i = c_{ie}$. Let $N_\phi^+(F) = S_1 + \cdots + S_t$ be the principal ϕ-Newton polygon of F with respect to p. We say that F is a ϕ-regular polynomial with respect to p, if $R_{\lambda_j}(F)(y)$ is square free in $\mathbb{F}_\phi[y]$ for every $j = 1, \ldots, t$. The polynomial F is said to be p-regular if F is a ϕ_i-regular polynomial with respect to p for every $i = 1, \ldots, r$.

The theorem of Ore plays a key role for proving our main Theorems.
Let $\phi \in \mathbb{Z}[x]$ be a monic polynomial, with $\overline{\phi(x)}$ is irreducible in $\mathbb{F}_p[x]$. As defined in [18, Def. 1.3], the ϕ-index of $F(x)$, denoted $ind_\phi(F)$, 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).

Example of constructing a Newton polygon: For the monic irreducible polynomial $F(x) = x^8 + 24x^2 + 39$, we have $F(x) \equiv (x-1)^8 \pmod 2$. Let $\phi = x - 1$, we get

$$F(x) = \phi^8 + 8\phi^7 + 28\phi^6 + 56\phi^5 + 70\phi^4 + 56\phi^3 + 52\phi^2 + 56\phi + 64.$$

Thus, $N_\phi^+(F) = S_1 + S_2 + S_3 + S_4$, with respect to 2. The degree of each side is 1, then their attached residual polynomials are irreducible over $\mathbb{F}_\phi$. Thus $F(x)$ is ϕ-regular, and so, it is 2-regular.
In this example, we have $ind_\phi(F) = 7 \times \deg(\phi) = 7$.

For every $i = 1, \ldots, r$, let $N_{\phi_i}^+(F) = S_{i1} + \cdots + S_{it_i}$ be the principal ϕ_i-Newton polygon of F with respect to p. For every $j = 1, \ldots, t_i$, let $R_{\lambda_{ij}}(y) = \prod_{s=1}^{s_{ij}} \psi_{ijs}^{a_{ijs}}(y)$ be the factorization of $R_{\lambda_{ij}}(y)$ in $\mathbb{F}_{\phi_i}[y]$. Then we have the following theorem of index of Ore:

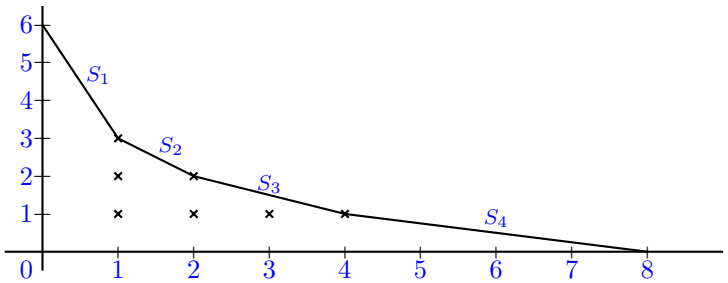

Figure 1: $N_\phi^+(F)$.

Theorem 4.3. (*Theorem of Ore*)
Under the above hypothesis, we have the following:

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

   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 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 for every (i, j, s).

Corollary 4.4. *Under the hypothesis above (Theorem 4.3), if for every $i = 1, \ldots, r$, $l_i = 1$ or $N_\phi^+(F) = S_i$ has a single side of height 1, then $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$.*

An alternative proof of theorem of index of Ore is given in [18, Theorem 1.7 and Theorem 1.9]. In [26], Guàrdia, Montes, and Nart introduced the notion of ϕ-admissible expansion used in order to treat some special cases when the ϕ-expansion is not obvious to calculate. Let

$$F(x) = \sum_{i=0}^{n} A_i'(x)\phi(x)^i, \quad A_i'(x) \in \mathbb{Z}[x], \tag{4.1}$$

be a ϕ-expansion of $F(x)$, not necessarily the ϕ-expansion; $\deg(A_i)$ not necessarily less than $\deg(\phi)$. Take $u_i' = \nu_p(A_i'(x))$, for all $i = 0, \ldots, n$, and let N' be the lower boundary convex envelope of the set of points $\{(i, u_i') \mid 0 \leq i \leq n,\ u_i' \neq \infty\}$. To any $i = 0, \ldots, n$, we attach the residue coefficient as follows:

$$c_i' = \begin{cases} 0, & \text{if } (i, u_i') \text{ lies above } N', \\ \left(\frac{A_i'(x)}{p^{u_i'}}\right) \mod (p, \phi(x)), & \text{if } (i, u_i') \text{ lies on } N'. \end{cases}$$

Likewise, for any side S of N', we can define the residual polynomial attached to S and denoted $R_\lambda'(F)(y)$ (similar to the residual polynomial $R_\lambda(F)(y)$ from the ϕ-expansion). We say that the ϕ-expansion (4.1) is admissible if $c_i' \neq 0$ for each abscissa i of a vertex of N'. For more details, we refer to [26].

Lemma 4.5. (*[26, Lemma 1.12]*)
If a ϕ-expansion of $F(x)$ is admissible, then $N' = N_\phi^+(F)$ and $c_i' = c_i$. In particular, for any side S of N' we have $R_\lambda'(F)(y) = R_\lambda(F)(y)$ up to multiply by a nonzero coefficient of $\mathbb{F}_\phi$.

The following lemma allows to determine the ϕ-Newton polygon of $F(x)$. Its proof will appear in [16].

Lemma 4.6. *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 $n = p^r t$ in $\mathbb{Z}$ with p does not divide t. Then $\overline{F(x)} = \overline{(x^t - m)}^{p^r} \pmod p$. Let $v = \nu_p(m^p - m)$ and $\phi \in \mathbb{Z}[x]$ be a monic polynomial, whose reduction modulo p divides $\overline{F(x)}$. Let us denote $(x^t - m) = \phi(x)Q(x) + R(x)$. Then $\nu_p(R) \geq 1$.*

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 the points $\{(0, v)\} \cup \{(p^j, r - j),\ j = 0, \ldots, r\}$.*
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 the points $\{(0, V)\} \cup \{(p^j, r - j),\ j = 0, \ldots, r\}$ for some integer $V \geq r + 1$.*

4.1. Common index divisor:

The index of a field K is defined by

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

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 $i(K) = 1$. Therefore a field having a prime common index divisor is not monogenic.
The existence of prime 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. 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 is 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 prime integer p to be a prime common index divisor [29].
The following lemma characterizes the prime common index divisors of K.

Lemma 4.7. *([36, Theorem 2.2])*
Let p be a rational prime integer and K be 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 prime common index divisor of K if and only if $\mathcal{P}_f > \mathcal{N}_f$ for some positive integer f.

5. Proofs of main results

Proof of Theorem 2.1.
The proof of this theorem can be concluded by Dedekind's criterion. But as the other results are based on Newton polygon, let us use theorem of index with "if and only if" as it is given in [26, Theorem 4.18], which says that in order to prove that $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$ if and only if $ind_1(F) = 0$, where $ind_1(F)$ is the index obtained by Ore's theorem of index. Since $\Delta(F) = \pm(2^r \times 7^s)^{2^r \cdot 7^s} \times m^{2^r \cdot 7^s - 1}$ and thanks to the formula $\nu_p(\Delta(F)) = \nu_p(d_K) + 2\nu_p(\text{ind}(\alpha))$, $\mathbb{Z}[\alpha]$ 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 p dividing $2 \times 7 \times m$. Let p be a rational prime dividing m, then $F(x) \equiv x^{2^r \cdot 7^s} \pmod p$. Let $\phi = x$. As m is a square free integer, then $\nu_p(m) = 1$, and so $N_\phi(F) = S$ has a single side of height 1. Thus $R_\lambda(F)(y)$ is irreducible over $\mathbb{F}_\phi$ as it is of degree 1. By Corollary 4.4, we conclude that $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$; p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. For $p = 2$ and 2 does not divide m, we have $F(x) \equiv x^{2^r \cdot 7^s} - 1 \equiv (x^{7^s} - 1)^{2^r} \pmod 2$. Let $\phi \in \mathbb{Z}[x]$ be a monic polynomial, whose reduction modulo 2 is an irreducible factor of $\overline{F(x)}$, then $\overline{\phi}$ divides $\overline{x^{7^s} - 1}$ in $\mathbb{F}_2[x]$. By Lemma 4.6, $ind_1(F) = 0$ if and only if $\nu_2(1 - m) = 1$; $m \not\equiv 1 \pmod 4$. Similarly, for $p = 7$ and 7 does not divide m. We have $F(x) \equiv x^{2^r \cdot 7^s} - m \equiv (x^{2^r} - m)^{7^s} \pmod 7$. Let $\phi \in \mathbb{Z}[x]$ be a monic polynomial, whose reduction modulo 7 is an irreducible factor of $\overline{F(x)}$, then $\overline{\phi}$ divides $\overline{x^{2^r} - m}$ in $\mathbb{F}_7[x]$. Again By Lemma 4.6, $ind_1(F) = 0$ if and only if $\nu_7(m^{7^s} - m) = 1$; $m \not\equiv \pm 1, \pm 18, \pm 19 \pmod{49}$.

□

Remark 5.1. *In order to prove Theorem 2.2, we do not need to determine the factorization of $p\mathbb{Z}_K$ explicitly. But according to Lemma 4.7, 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 4.3 could replaced by the following: If $l_i = 1$ or $d_{ij} = 1$ or $a_{ijk} = 1$ for some (i, j, k) according to notation of Theorem 4.3, then ψ_{ijk} provides a prime ideal $\mathfrak{p}_{ijk}$ of $\mathbb{Z}_K$ lying above p with residue degree $f_{ijk} = m_i \times t_{ijk}$, where $t_{ijk} = deg(\psi_{ijk})$ and $p\mathbb{Z}_K = \mathfrak{p}_{ijk}^{e_{ij}} I$, where the factorization of the ideal I can be derived from the other factors of each residual polynomials of $F(x)$.*

Proof of Theorem 2.2.
In every case, let us show that $i(K) > 1$, and so K is not monogenic.

1. $r = 2$ and $m \equiv 1 \pmod{16}$.
   Since $x^{7^s} - 1$ is separable over $\mathbb{F}_2$, $x^{7^s} - 1 = (x-1)U(x)$ with $\overline{x-1}$ does not divide $\overline{U(x)}$ in $\mathbb{F}_2[x]$. For $\phi = x - 1$, if $v = \nu_2(1 - m) \geq 4$, then by Lemma 4.6, $N_\phi^+(F)$ has 3 sides joining the points $(0, v)$, $(1, 2)$, $(2, 1)$, and $(4, 0)$ (see Figure 1). Thus the degree of each side is 1, then by Theorem 4.3, ϕ provides 3 prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each. As there are only 2 monic irreducible polynomials of degree 1 in $\mathbb{F}_2[x]$, by Lemma 4.7, 2 is a common index divisor of K, and so K is not monogenic.

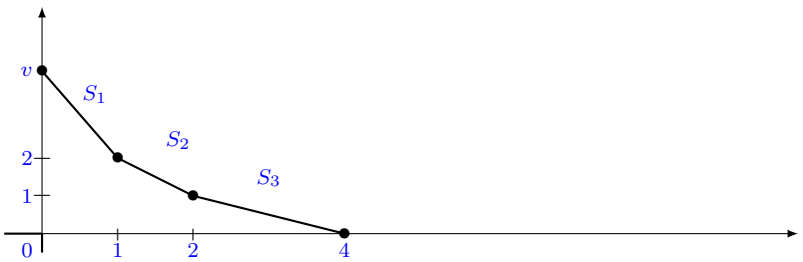

Figure 2: $N_\phi^+(F)$.

2. $r \geq 3$ and $m \equiv 1 \pmod{16}$.
   Since $x^{7^s} - 1$ is separable over $\mathbb{F}_2$, $x^{7^s} - 1 = \overline{\phi_1(x)\phi_2(x)\phi_3(x)}\,\overline{U(x)}$ with $\phi_1 = x - 1$, $\phi_2(x) = x^3 + x + 1$, and $\phi_3(x) = x^3 + x^2 + 1$. Since $v = \nu_2(m - 1) \geq 4$, by Lemma 4.6, we conclude that $N_{\phi_i}^+(F)$ has at least 2 sides joining the points $(2^{r-2}, 2)$, $(2^{r-1}, 1)$, and $(2^r, 0)$ (see Figure 3). Then the degree of each of these 2 sides is 1. Thus, for every $i = 2, 3$, ϕ_i provides at least 2 prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 3 $=\deg(\phi_i)$ each. Applying this for $i = 2$ and $i = 3$, we conclude that there are at least 4 prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 3 each. As there are only 2 monic irreducible polynomials of degree 3 in $\mathbb{F}_2[x]$, namely $x^3 + x + 1$ and $x^3 + x^2 + 1$, by Lemma 4.7, 2 is a common index divisor of K, and so K is not monogenic.

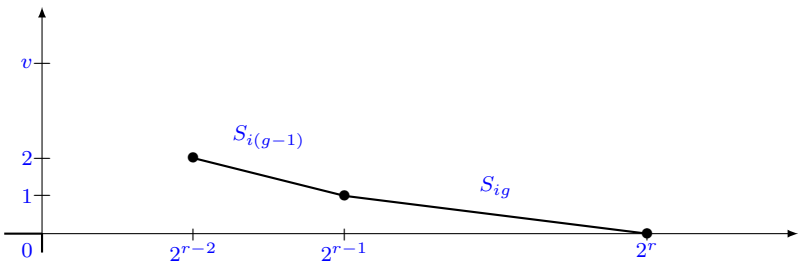

Figure 3: $N_{\phi_i}^+(F)$.

3. $s \geq 3$ and $\nu_7(m^6 - 1) \geq 4$.
   If $m \equiv 1 \pmod{49}$, then $x^{2^r} - 1 \equiv (x+1)(x-1)U_1(x) \pmod 7$.

If $m \equiv -19 \pmod{49}$, then $x^{2^r} - 2 \equiv (x+3)(x-3)U_2(x) \pmod 7$ if r is odd and $x^{2^r} - 2 \equiv (x+2)(x-2)U_3(x) \pmod 7$ if r is even.
If $m \equiv 18 \pmod{49}$, then $x^{2^r} - 4 \equiv (x+2)(x-2)U_4(x) \pmod 7$ if r is odd and $x^{2^r} - 4 \equiv (x+3)(x-3)U_5(x) \pmod 7$ if r is even.
In all these cases, $x^{2^r} - m$ has 2 distinct roots a_1 and a_2 in $\mathbb{F}_7$. Let $\phi_i(x) = x - a_i$. Then $x^{2^r} - m = \phi_i(x)Q_i(x) + 7A_i(x)$ for some polynomials Q_i, A_i in $\mathbb{Z}[x]$ with $\phi_i(x)$ does not divide $Q_i(x)$ in $\mathbb{F}_7[x]$. Since $\nu_7(m^6 - 1) \geq 4$, by Lemma 4.6, we conclude that $N^+_{\phi_i}(F)$ has at least 4 sides joining the points $(0, V)$, $(7^{s-3}, 3)$, $(7^{s-2}, 2)$, $(7^{s-1}, 1)$, and $(7^s, 0)$, with $V \geq 4$. Thus the degree of each of these four sides is 1. Then every ϕ_i provides at least 4 prime ideals of $\mathbb{Z}_K$ lying above 7 with residue degree 1 each. Applying this for $i = 1, 2$, we conclude that there are at least 8 prime ideals of $\mathbb{Z}_K$ lying above 7 with residue degree 1 each. As there are only 7 monic irreducible polynomial of degree 1 in $\mathbb{F}_7[x]$, by Lemma 4.7, 7 is a common index divisor of K, and so K is not monogenic.

□

Proof of Theorem 2.3.
As $\gcd(u, 2^r \times 7^s) = 1$, let $(x, y) \in \mathbb{Z}^2$ be the unique solution of $ux - 2^r \times 7^s y = 1$ with $0 \leq y < u$. Let $\theta = \frac{\alpha^x}{a^y}$. Then $\theta^{2^r \cdot 7^s} = \frac{\alpha^{2^r \cdot 7^s x}}{a^{2^r \cdot 7^s \cdot y}} = a^{ux - 2^r \cdot 7^s y} = a$. Since $g(x) = x^{2^r \cdot 7^s} - a \in \mathbb{Z}[x]$ is an Eisenstein polynomial, $g(x)$ is irreducible over $\mathbb{Q}$. As $\theta \in K$ and $[K : \mathbb{Q}] = \deg(g)$, we conclude that $K = \mathbb{Q}(\theta)$. Therefore, K is generated by a root of the polynomial $x^{2^r \cdot 7^s} - a$ with $a \neq \pm 1$ a square free integer. The proof is therefore an application of Theorem 2.1 and Theorem 2.2.

□

Acknowledgments

The authors are very grateful to the referees for careful reading. The first author is very grateful for Professor István Gaál for his encouragement and for Professor Enric Nart who introduced him to Newton polygon techniques

References

1. Ahmad, S., Nakahara, T., and Husnine, S. M., *Power integral bases for certain pure sextic fields*, Int. J. Number Theory **10**(8), 2257–2265, (2014).
2. Ahmad, S., Nakahara, T., and Husnine, S. M., *On certain pure sextic fields related to a problem of Hasse*, Int. J. Algebra Comput. **26**(3), 577–583, (2016).
3. Ahmad, S., Nakahara, T., and Husnine, S. M.,, *On existence of canonical number system in certain classes of pure algebraic number fields*, J. Prime Res. Math. 7, 19–24, (2011).
4. Ben Yakkou, H., Chillali, A., and EL Fadil, L., *On power integral bases for certain pure number fields defined by* $x^{2^r \cdot 5^s} - m$, Commun. Algebra **49**(7), 2916-2926, (2021).
5. Ben Yakkou, H. and El Fadil, L., *On monogenity of certain pure number fields defined by* $x^{p^r} - m$, Int. J. Number Theory, **17**(10), 2235–2242, (2021).
6. Ben Yakkou, H. and Kchit, O., *On power integral bases for certain pure number fields defined by* $x^{3^r} - m$, São Paulo J. Math. Sci. (2021). https://doi.org/10.1007/s40863-021-00251-2
7. Choulli, H., El Fadil, L., and Kchit, O., *On monogenity of certain number fields defined by* $x^{60} - m$. Acta Math. Vetnam., 1-11 (2022). https://doi.org/10.1007/s40306-022-00481-2.
8. Cohen, H., *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag Berlin Heidelberg (1993).
9. Dedekind, R., *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Göttingen Abhandlungen **23**, 1–23, (1878).
10. El Fadil, L., *Computation of a power integral basis of a pure cubic number field*, Int. J. Contemp. Math. Sci. **2**(13-16), 601–606, (2007).
11. El Fadil, L., *On Newton polygon's techniques and factorization of polynomial over henselian valued fields*, J. Algebra its Appl. **19**(10), 2050188, (2020).
12. El Fadil, L., *On power integral bases for certain pure number fields defined by* $x^{12} - m$, Pub. Math. 100(1-2), 219-231, (2022). doi: 10.1556/012.2020.57.3.1472

13. El Fadil, L., *On power integral bases for certain pure number fields defined by* $x^{24} - m$, Studia Sci. Math. Hungarica, **57**(3), 397–407, (2020).

14. El Fadil, L., *On power integral bases for certain pure number fields defined by* $x^{36} - m$, Studia Sci. Math. Hungarica, **58**(3), 371–380, (2021).

15. El Fadil, L. and Najim, A., *On power integral bases for certain pure number fields defined by* $x^{2^u \cdot 3^v} - m$, (2021). arXiv:2106.01252v2

16. El Fadil, L., *On power integral bases for certain pure number fields defined by* $x^{3^u \cdot 7^v} - m$, Colloc. Math., (2021). doi: 10.4064/cm8574-6-2021

17. El Fadil, L., *On power integral bases for certain pure sextic fields*, Bol. Soc. Paran. Math. 40(3s), 1–7, (2022).

18. El Fadil, L., Montes, J., and Nart, E., *Newton polygons and p-integral bases of quartic number fields*, J. Algebra its Appl. 11(4), 1–33, (2012).

19. Funakura, T., *On integral bases of pure quartic fields*, Math. J. Okayama Univ. 26, 27-–41, (1984).

20. Gaál, I., *Power integer bases in algebraic number fields*, Ann. Univ. Sci. Budapest. Sect. Comp. 18, 61–87, (1999).

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

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

23. Gaál, I., Olajos, P., Pohst, M., *Power integral bases in order of composite fields*, Exp. Math. **11**(1), 87–90, (2002).

24. Gaál, I. and Remete, L., *Binomial Thue equations and power integral bases in pure quartic fields*, JP J. Algebra, Number Theory Appl. 32(1), 49–61, (2014).

25. Gaál, I. and Remete, L., *Integral bases and monogeneity of pure fields*, J. Number Theory **173**(1), 129–146, (2018).

26. Guardia, J., Montes, J., and Nart, E., *Newton polygons of higher order in algebraic number theory*, J. trans. of ams **364**(1), 361–416, (2012).

27. Hameed, A. and Nakahara, T., *Integral bases and relative monogeneity of pure octic fields*, Bull. Math. Soc. Sci. Math. Répub. Soc. Roum. 58(106) No. 4, 419–433, (2015).

28. Hasse, H., *Vorlesungen über Zahlentheorie*, Akademie-Verlag, Berlin, (1963).

29. Hensel, K., *Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung*, J. Reine Angew. Math., 113:128–160, ISSN 0075-4102, (1894). doi: 10.1515/crll.1894.113.128.

30. Hensel, K., *Theorie der algebraischen Zahlen*, Teubner Verlag, Leipzig, Berlin, (1908).

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

32. Motoda, Y., Nakahara, T., and Shah, S. I. A., On a problem of Hasse*, J. Number Theory 96, 326–334, (2002).*

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

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

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

36. Smith, H., The monogeneity of radical extensions. *Acta Arith., 198(3), 313-327, (2021).*

Lhoussain El Fadil,
Department of Mathematics,
Faculty of Sciences Dhar El Mahraz, P.O. Box 1796, Atlas-Fes, Sidi Mohamed ben Abdellah University, Fez Morocco.
E-mail address: lhoussain.elfadil@usmba.ac.ma

and

Omar Kchit,
Department of Mathematics,
Faculty of Sciences Dhar El Mahraz, P.O. Box 1796, Atlas-Fes, Sidi Mohamed ben Abdellah University, Fez Morocco.
E-mail address: omar.kchit@usmba.ac.ma