On Monogenity of Certain Pure Number Fields Defined by $x^{60} - m$

Lhoussain El Fadil¹ · Hanan Choulli¹ · Omar Kchit¹

Received: 20 February 2022 / Revised: 19 March 2022 / Accepted: 1 April 2022 / Published online: 4 July 2022
© Institute of Mathematics, Vietnam Academy of Science and Technology (VAST) and Springer Nature Singapore Pte Ltd. 2022

Abstract
Let $K$ be a pure number field generated by a complex root of a monic irreducible polynomial $F(x) = x^{60} - m \in \mathbb{Z}[x]$, with $m \neq \pm 1$ a square free integer. In this paper, we study the monogenity of $K$. We prove that if $m \not\equiv 1 \pmod{4}$, $m \not\equiv \pm 1 \pmod{9}$ and $m \not\equiv \{\pm 1, \pm 7\} \pmod{25}$, then $K$ is monogenic. But if $m \equiv 1 \pmod{4}$, $m \equiv \pm 1 \pmod{9}$, or $m \equiv \pm 1 \pmod{25}$, then $K$ is not monogenic. Our results are illustrated by examples.

Keywords Theorem of Dedekind · Theorem of Ore · Prime ideal factorization · Newton polygon · Index of a number field · Power integral basis

Mathematics Subject Classification (2010) 11R04 · 11Y40 · 11R21

1 Introduction

Let $K$ be a number field of degree $n$ with ring of integers $\mathbb{Z}_K$, and absolute discriminant $d_K$. The number field $K$ is called monogenic if it admits a power integral basis, that is there exists an integral $\theta \in \mathbb{Z}_K$ such that $(1, \theta, \ldots, \theta^{n-1})$ is a $\mathbb{Z}$-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. [21, 27, 29] 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 [27, 29, 31]. For any primitive element $\theta \in \mathbb{Z}_K$, we denote by

$$\text{ind}(\theta) = (\mathbb{Z}_K : \mathbb{Z}[\theta])$$

References
1. Faculty of Sciences Dhar El Mahraz, Sidi Mohamed ben Abdellah University, P.O. Box 1796, Atlas-Fes, Morocco
the index of $\theta$, that is the index of the subgroup $\mathbb{Z}[\theta]$ in $\mathbb{Z}_K$. As it is known [21], we have

$$|\triangle(F)| = \text{ind}(\theta)^2 \cdot |d_K|,$$

where $\triangle(F)$ is the discriminant of $F$ and $F$ is the minimal polynomial of $\theta$ over $\mathbb{Q}$. The problem of testing the monogenity of pure number fields and constructing power integral bases have been intensively studied these last fourth decades, mainly by Gaál, Győry, Nakahara, Pohst and their research teams (see, for instance [2, 5, 19–21, 27, 29, 31, 35]). In [9], 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 of pure quartic fields and studied their monogenity. In [22], 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 [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 [14], based on prime ideal factorization, El Fadil showed that if $m \equiv 1 \pmod{4}$ or $m \equiv 1 \pmod{9}$, then the sextic number field generated by $m^\frac{1}{6}$ is not monogenic. Hameed and Nakahara [26], 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 [23], by applying the explicit form of the index equation, Gaál and Remete obtained deep new results and they gave a complete answer to the problem of monogenity of number fields generated by $m^\frac{1}{6}$, where $3 \leq n \leq 9$. While Gaál’s 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. Based on Newton polygon techniques, El Fadil et al. studied the monogenity of pure number fields of degrees 6, 12, 18, 24, 36, $2^u \cdot 5^v$, $p^r$, $2^u \cdot 3^v$, $3^u \cdot 7^v$ (see [3, 4, 11–13, 15–17]). In this paper, our purpose is for a square free integer $m \not\equiv \pm 1$ and $F(x) = x^{60} - m$ an irreducible polynomial over $\mathbb{Q}$, we study the monogenity of the number field $K = \mathbb{Q}(\alpha)$ generated by a root $\alpha$ of $F(x)$. Our method applies the Newton polygon techniques and the explicit prime ideal factorization. Recall that a polynomial $F(x)$ of degree $n$ is said to be monogenic, if a root $\alpha$ of $F(x)$ generates a power integral basis $(1, \alpha, \ldots, \alpha^{n-1})$ in $K = \mathbb{Q}(\alpha)$. This is equivalent to the property $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, that is $\mathbb{Z}[\alpha]$ is integrally closed. Even if the problem of the integral closedness of $\mathbb{Z}[\alpha]$ gives a partial answer to the problem of monogenity of $K$, the problem of monogenity is more hard to solve. Unfortunately this notion of monogenity does not coincide with the well known notion of monogenity of number fields, treated by Gaál, Nakahara, Pohst and their collaborators. In fact, let us consider $F(x) = x^3 - 9$ and $K$ the number field generated by a root $\alpha$ of $F(x)$, since 3 divides the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, we conclude that $\mathbb{Z}[\alpha]$ is not integrally closed even if $K$ is monogenic and $\theta = \frac{\alpha^2}{3}$ generates a power integral basis of $K$ (cf. also [8]).

2 Main Results

Let $K$ be a pure number field generated by a complex root $\alpha$ of a monic irreducible polynomial $F(x) = x^{60} - m$, with $m \not\equiv \pm 1$ a square free integer. The main goal of this section is to study the monogenity of pure number fields of degree 60. Theorem 2.1 gives a necessary and sufficient condition on the integral closedness of $\mathbb{Z}[\alpha]$. This theorem covers [24, Theorem 1.1] in the context of pure number fields of degree 60. But on the contrary
On Monogenity of Certain Pure Number Fields Defined by $x^{60} - m$

[24, Theorem 1.1] does not cover our Theorem 2.1. In fact, our theorem gives necessary and sufficient conditions on the integral closedness of $\mathbb{Z}[\alpha]$, unlike Gassert’s results, which gives just one meaning and requires more details to reach our result. Theorem 2.2 gives a partial converse on Theorem 2.1. In fact it gives a full converse for the number fields defined by a monic irreducible polynomial $F(x) = x^{60} - m$, with $m$ a square free integer, except for the cases $m \in \{+7, -7\} \pmod{25}$. Finally Theorem 2.3 gives a partial answer for the cases when $m$ is not necessarily 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 $m \not\equiv \pm 1, \pm 7 \pmod{25}$.

In particular, if $m \not\equiv 1 \pmod{4}$, $m \not\equiv \pm 1 \pmod{9}$, and $m \not\equiv \pm 1, \pm 7 \pmod{25}$, then $K$ is monogenic.

Remark that based on Theorem 2.1, if $m \equiv 1 \pmod{4}$, $m \equiv \pm 1 \pmod{9}$, and $m \equiv \pm 1, \pm 7 \pmod{25}$, then $K$ is not monogenic.

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

1. $m \equiv 1 \pmod{4}$,
2. $m \equiv \pm 1 \pmod{9}$,
3. $m \equiv \pm 1 \pmod{25}$,

then $K$ is not monogenic.

**Theorem 2.3** Let $K$ be a pure number field defined by a root $\alpha$ of a monic irreducible polynomial $F(x) = x^{60} - au$, with $a \not= \pm 1$ a square free integer and $u$ a positive integer which is coprime to 30. Then,

1. If $a \not\equiv 1 \pmod{4}$, $a \not\equiv \pm 1 \pmod{9}$, and $a \not\equiv \pm 1, \pm 7 \pmod{25}$, then $K$ is monogenic.
2. If $a \equiv 1 \pmod{4}$ or $a \equiv \pm 1 \pmod{9}$ or $a \equiv \pm 1 \pmod{25}$, then $K$ is not monogenic.

### 3 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 $i \not= j = 1, \ldots, r$.

Recall that a theorem of Dedekind says that:

**Theorem 3.1** ([33, Chapter I, Proposition 8.3]) If $p$ does not divide the index ($\mathbb{Z}_K : \mathbb{Z}[\alpha]$), then

$$p\mathbb{Z}_K = \prod_{i=1}^{r} p_i^{l_i},$$

where every $p_i = p\mathbb{Z}_K + \phi_i(\alpha)\mathbb{Z}_K$ and the residue degree of $p_i$ is $f(p_i) = \deg(\phi_i)$.

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 proved that $M(x) \in \mathbb{Z}[x]$, where $M(x) = \frac{F(x) - \prod_{i=1}^{r} \phi_i(x)^{l_i}}{p}$, and

**Theorem 3.2** ([6, Theorem 6.1.4] and [7]) 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 $\phi_i(x)$ does not divide $M(x)$ in $\mathbb{F}_p[x]$.

When Dedekind’s criterion fails, that is, $p$ divides the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ for every primitive element $\theta \in \mathbb{Z}_K$, 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 of $K$, and the prime ideal factorization of the rational primes in a number field $K$ by using Newton polygons (see, for instance [18, 30, 34]). Now we recall some fundamental facts on Newton polygons, for more details, we refer to [10, 25]. 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 $\mathbb{F}_p$ be the finite field $\mathbb{F}_p[x]/(\phi)$. For any monic polynomial $F(x) \in \mathbb{Z}[x]$, upon to the Euclidean division by successive powers of $\phi$, we expand $F(x)$ as $F(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_l(x)\phi(x)^l$, called the $\phi$-expansion of $F(x)$ (for every $i$, $\deg(a_i(x)) < \deg(\phi)$). To any coefficient $a_i(x)$ we attach $u_i = v_p(a_i(x)) \in \mathbb{Z} \cup \{\infty\}$. The $\phi$-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 $\phi$-Newton polygon of $F$ is the process of joining the obtained edges $S_1, \ldots, S_r$ ordered by increasing slopes, which can be expressed as $N_\phi(F) = S_1 + \cdots + S_r$. The principal $\phi$-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 $c_i \in \mathbb{F}_p$ as follows:

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

where $(p, \phi(x))$ is the maximal ideal of $\mathbb{Z}[x]$ generated by $p$ and $\phi$. 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

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

which is called the residual polynomial of $F(x)$ associated to the side $S$, where for every $i = 0, \ldots, d, t_i = c_i$. Let $N_\phi^+(F) = S_1 + \cdots + S_r$ be the principal $\phi$-Newton polygon of $F$ with respect to $p$.

We say that $F$ is a $\phi$-regular polynomial with respect to $p$, if $R_{\lambda_j}(F)(y)$ is square free in $\mathbb{F}_p[y]$ for every $j = 1, \ldots, t$. The polynomial $F$ is said to be $p$-regular if $F$ is a $\phi_i$-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, Definition 1.3], the \( \phi \)-index of \( F(x) \), denoted \( \text{ind}_\phi(F) \), 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 Fig. 1).

**Example 3.3** 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 \( v_2 \). The degree of each side is 1, then their residual polynomials are irreducible over \( \mathbb{F}_\phi \). Thus, \( F(x) \) is \( \phi \)-regular, and so, it is 2-regular.

In this example, we have \( \text{ind}_\phi(F) = 7 \times \deg(\phi) = 7 \).

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

**Theorem 3.4** (Theorem of Ore) Under the above hypothesis, we have the following

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

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

2. If \( F(x) \) is \( p \)-regular, then

\[
p\mathbb{Z}_K = \prod_{i=1}^{r} \prod_{j=1}^{t_i} \prod_{s=1}^{s_{ij}} p_{ij_{s}}^{e_{ij}},
\]

where \( e_{ij} \) is the smallest positive integer satisfying that \( e_{ij}\lambda_{ij} \in \mathbb{Z} \) and \( f_{ij_{s}} = \deg(\phi_i) \times \deg(\psi_{ij_{s}}) \) is the residue degree of \( p_{ij_{s}} \) over \( p \) for every \( (i, j, s) \).

**Corollary 3.5** Under the hypothesis above (Theorem 3.4), 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 the theorem of index of Ore is given in [18, Theorem 1.7 and Theorem 1.9]. In [25], Guardia, Montes, and Nart introduced the notion of \( \phi \)-admissible
expansion used in order to treat some special cases when the \( \phi \)-adic expansion is not obvious. Let
\[
F(x) = \sum_{i=0}^{n} A_i'(x)\phi(x)^i, \quad A_i'(x) \in \mathbb{Z}[x],
\]
be a \( \phi \)-expansion of \( F(x) \), not necessarily \( \text{deg}(A_i') \) less than \( \text{deg}(\phi) \). 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:
\[
c'_i = \left\{ \begin{array}{ll}
0 & \text{if } (i, u'_i) \text{ lies above } N', \\
\left( \frac{A_i'(x)}{\nu_p(A_i'(x))} \right) \pmod{(p, \phi(x))} & \text{if } (i, u'_i) \text{ lies on } N'.
\end{array} \right.
\]

Likewise, for any side \( S \) of \( N' \), we can define the residual polynomial attached to \( S \) and denoted \( R_i'(F)(y) \) (similar to the residual polynomial \( R_0(F)(y) \) from the \( \phi \)-adic expansion). We say that the \( \phi \)-expansion (3.1) is admissible if \( c'_i \neq 0 \) for each abscissa \( i \) of a vertex of \( N' \). For more details, we refer to [25].

**Lemma 3.6** ([25, Lemma 1.12]) If a \( \phi \)-expansion of \( F(x) \) is admissible, then \( N' = N_\phi^2(F) \) and \( c'_i = c_i \). In particular, for any side \( S \) of \( N' \) we have \( R_i'(F)(y) = R_\phi(F)(y) \) up to multiply by a nonzero coefficient of \( \mathbb{F}_\phi \).

## 4 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 polygons, let us use theorem of index with “if and only if” as it is given in [25, Theorem 4.18], which says that a necessary and sufficient condition to have \( \nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha]) = 0 \) is that \( \text{ind}_1(F) = 0 \), where \( \text{ind}_1(F) \) is the index obtained by Ore’s index in Theorem 3.4. Since \( \Delta(F) = \pm 60^6 \times m^{59} \), thanks to the known 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 \( 30 \times m \). Let \( p \) be a rational prime dividing \( m \), then \( F(x) \equiv x^60 \pmod{p} \). Let \( \phi = x \). As \( m \) is square free integer, then \( \nu_p(m) = 1 \), and so \( N_p(F) = S \) has a single side of height 1. Thus, \( R_\phi(F)(y) \) is irreducible over \( \mathbb{F}_\phi \) as it is of degree 1. By Corollary 3.5, we get \( \nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha]) = 0 \); \( p \) does not divide \( (\mathbb{Z}_K : \mathbb{Z}[\alpha]) \). For \( p = 2 \) and \( 2 \) does not divide \( m \), we have \( F(x) \equiv x^60 - 1 \equiv (x^{15} - 1)^4 \pmod{2} \). 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 \( x^{15} - 1 \in \mathbb{F}_2[x] \). Let \( x^{15} - 1 = Q(x)\phi + T(x) \), with \( (Q, T) \in \mathbb{Z}[x]^2 \) and \( v_2(T) \geq 1 \). Since \( x^{15} - 1 \) is separable over \( \mathbb{F}_2 \), \( \overline{\phi} \) does not divide \( \overline{Q} \). Let \( F(x) = (x^{15} - 1)^4 + 4(x^{15} - 1)^3 + 6(x^{15} - 1)^2 + 4(x^{15} - 1) + 1 - m = Q(x)^4\phi^4 + 4Q(x)^3\phi^3 + 6Q(x)^2\phi^2 + 4Q(x)\phi + r_0 + 1 - m \), where \( r_0 \) is the remainder upon the Euclidean division of \( F(x) \) by \( (Q(x)^4 + 4Q(x)^3\phi^3 + 6Q(x)^2\phi^2 + 4Q(x)\phi + 1 + m) = 2T(x)K(x) \) for some \( K \in \mathbb{Z}[x] \), we conclude that \( v_2(r_0) \geq 2 \). Since \( \overline{\phi} \) does not divide \( \overline{Q} \), the previous \( \phi \)-expansion is admissible, and by Lemma 3.6, \( \text{ind}_\phi(F) = 0 \) if and only if \( v_2(1 - m) = 1; m \neq 1 \pmod{4} \).

Similarly, for \( p = 3 \) and \( 3 \) does not divide \( m \), we have \( F(x) \equiv x^60 - m \equiv (x^{20} - m)^3 \pmod{3} \). Let \( \phi \in \mathbb{Z}[x] \) be a monic polynomial, whose reduction modulo 3 is an irreducible factor of \( \overline{F}(x) \). Then, \( \overline{\phi} \) divides \( x^{20} - m \in \mathbb{F}_3[x] \). Let \( x^{20} - m = Q(x)\phi + T(x) \), with \( (Q, T) \in \mathbb{Z}[x]^2 \) and \( v_3(T) \geq 1 \). Since \( x^{20} - m \) is separable over \( \mathbb{F}_3 \), \( \overline{\phi} \) does not divide \( \overline{Q} \). Let \( F(x) = (x^{20} - m)^3 + 3m(x^{15} - m)^2 + 3m^2(x^{15} - m) + m^3 - m = Q(x)^3\phi^3 + \)
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 two 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 [28]. For the proof of Theorem 2.2, we need the following lemma and its proof is an immediate consequence of Dedekind’s theorem.

**Lemma 4.1** 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 \( f \).

To apply the last lemma one has to know the number \( \mathcal{N}_f(p) \) of monic irreducible polynomials over \( \mathbb{F}_p \) of degree \( f \). This number was found by Gauss, which it is given by the following proposition:

**Proposition 4.2** ([32, Chapter 4, Proposition 4.35]) For every prime \( p \) and \( f \geq 1 \) one has

\[
\mathcal{N}_f(p) = \frac{1}{f} \sum_{d \mid f} \mu(d) p^{f/d},
\]

where \( \mu(d) \) is the familiar Möbius function.
Proof of Theorem 2.2 In every case, let us show that $i(K) > 1$, and so $K$ is not monogenic.

$(1) \, m \equiv 1 \pmod{4}$. Then, $F(x) = \frac{(x^{15} - 1)}{(x - 1)(x^2 + x + 1)}U(x) \in \mathbb{F}_2[x]$. Let $\phi = x^2 + x + 1$ and $v = v_2(1 - m)$. Since $F(x) = \cdots + (-48165 - 42465x)^4 + (3610 + 6840x)\phi^3 - 570x\phi^2 + (-20 + 20x)\phi + 1 - m$, if $v \geq 4$, then $N_{\phi}^+(F)$ has three sides joining $(0, v), (1, 2), (2, 1)$, and $(4, 0)$. Thus, every side of $N_{\phi}^+(F)$ has degree 1 (see Fig. 2, $v \geq 4$). Thus, by Theorem 3.4, $\phi$ provides three prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each. As there is only one monic irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, namely $x^2 + x + 1$, by Lemma 4.1, 2 is a common index divisor of $K$, and so $K$ is not monogenic. If $v = 2$, then $N_{\phi}^+(F) = S$ has a single side of degree 2 such that $R_{\phi}(F)(y) = (x + 1)^2 + xy + 1 = ((x + 1)(y + 1)(y + 1) \in \mathbb{F}_2[y]$ (see Fig. 2, $v = 2$). So, by Theorem 3.4, $\phi$ provides two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each, and so there are at least 2 prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each. As there is only one monic irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, by Lemma 4.1, 2 is a common index divisor of $K$, and so $K$ is not monogenic. If $v = 3$, then $N_{\phi}^+(F) = S_1 + S_2$ has two sides with degrees $d(S_1) = 2$ and $d(S_2) = 1$ such that $R_{\phi}(F)(y) = xy^2 + (1 + x)y + 1 = (y + 1)(xy + 1) \in \mathbb{F}_2[y]$ (see Fig. 2, $v = 3$). Thus, by Theorem 3.4, $\phi$ provides three prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each. As there is only one monic irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, 2 is a common index divisor of $K$, and so $K$ is not monogenic.

$(2) \, m \equiv \pm 1 \pmod{9}$. For $m = 1 \pmod{9}$, we have $F(x) = \frac{x^{20} + 1}{x^2 - x - 1}$, $\phi_1 = x^2 + x + 1$ and $\frac{\phi_1}{x^2 - x - 1}$ does not divide $U(x)$ in $\mathbb{F}_3[x]$ for every $k = 1, 2$. Consider the following expansions: $F(x) = \cdots + 342200 \phi_3^3 + 1770 \phi_2^2 + 60 \phi_2 + 1 - m$ and $F(x) = \cdots - 342200 \phi_3^3 + 1770 \phi_2^2 - 60 \phi_2 + 1 - m$. We conclude that if $m = 1 \pmod{9}$, then $N_{\phi}^+(F) = S_k$ has two sides joining $(0, V), (1, 1)$, and $(3, 0)$ with $V = v_3(1 - m) \geq 2$. Thus, the degree of each side is 1. Therefore, $\phi_k$ provides two prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. Applying this for every $k = 1, 2$, we conclude that there are four prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. As there are only three monic irreducible polynomials of degree 1 in $\mathbb{F}_3[x]$, 3 is a common index divisor of $K$ and so $K$ is not monogenic.

For $m = -1 \pmod{9}$, we have $F(x) = \frac{(x^20 + 1)^3}{x^2 - x - 1}$, $\phi_1 = x^2 + x + 1$, $\phi_2 = x^2 - x - 1$, and $\frac{\phi_2}{x^2 - x - 1}$ does not divide $U(x)$ in $\mathbb{F}_3[x]$ for every $k = 1, 2$. Consider the following expansions: $F(x) = \cdots + a_3(x) \phi_3^3 + a_2(x) \phi_2^2 + a_1(x) \phi_1 + a_0(x)$ and $F(x) = \cdots + b_3(x) \phi_3^3 + b_2(x) \phi_2^2 + b_1(x) \phi_2 + b_0(x)$, where $a_1(x) = 16175489617620 - 2505234232720x$, $a_0(x) = -1548008755920 + 956722026041 - m$, $b_1(x) = 16175489617620 + 2505234232720x$, and $b_0(x) = 1548008755920 + 956722026041 - m$. Since

Fig. 2 The principal $\phi$-Newton polygon of $F(x)$
\( v_3(a(x)b(x)) = 0, v_5(a(x)) \geq 1, v_5(b(x)) \geq 1, v_5(a_1(x)) = v_5(b_1(x)) = 1, \) we conclude that if \( m \equiv -1 \pmod 9, \) then \( v_3(a_0(x)) \geq 2 \) and \( v_5(b_0(x)) \geq 2, \) and so \( N_{\phi_k}^+ = S_k1 + S_k2 \) has two sides joining \((0, V_k), (1, 1), \) and \((3, 0)\) with \( V_1 = v_3(a_0(x)) \geq 2 \) and \( V_2 = v_5(b_0(x)) \geq 2. \) Thus, the degree of each side is 1. Therefore, \( \phi_k \) provides two prime ideals of \( \mathbb{Z}_K \) lying above 3 with residue degree 2 each for \( k = 1, 2, \) then there are four 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 \( \mathbb{F}_3[x] \) namely \( x^2 + x - 1, x^2 - x - 1, \) and \( x^2 + 1, 3 \) is a common index divisor, and so \( K \) is not monogenic.

(3) For \( m \equiv \pm 1 \pmod{25}, \)

If \( m \equiv 1 \pmod{25}, \) we have \( \overline{F(x)} = (x^{12} - 1)^5 = \prod_{k=1}^{4} \phi_k U(x)^5 \) in \( \mathbb{F}_5[x], \) with \( \phi_k = x - k \) for every \( k = 1, \ldots, 4 \) and \( \phi_k \) does not divide \( \overline{U(x)} \) in \( \mathbb{F}_5[x]. \) Similarly, by considering the \( \phi_k \)-expansion of \( F(x), \) if \( v_5(m) \geq 2, \) then \( m \equiv 1 \pmod{25}, \) then \( N_{\phi_k}^+(F) = S_k1 + S_k2 \) has two sides joining \((0, V_k), (1, 1), \) and \((5, 0), \) with \( V_k \geq 2. \) Thus, each side of \( N_{\phi_k}^+(F) \) is of degree 1. Therefore, \( \phi_k \) provides two prime ideals of \( \mathbb{Z}_K \) lying above 5 with residue degree 1 each. Applying this for every \( k = 1, \ldots, 4, \) we conclude that there are 8 prime ideals of \( \mathbb{Z}_K \) lying above 5 with residue degree 1 each. As there are only 5 monic irreducible polynomials of degree 1 in \( \mathbb{F}_5[x], \) by Lemma 4.1, 5 is a common index divisor, and so \( K \) is not monogenic.

If \( m \equiv -1 \pmod{25}, \) then \( \overline{F(x)} = (x^{12} + 1)^5 = \prod_{k=1}^{6} \phi_k U(x) \pmod{5}, \) with \( \phi_1 = x^2 + 2, \phi_2 = x^2 + 3, \phi_3 = x^2 + x + 2, \phi_4 = x^2 + 2x + 3, \phi_5 = x^2 + 3x + 3, \phi_6 = x^2 + 4x + 2, \) and \( \phi_k \nmid U(x) \) for every \( k = 1, \ldots, 6. \) Fix \( k = 1, \ldots, 6 \) and consider the \( \phi_k \)-expansion of \( F(x). \) If \( v_5(m + 1) \geq 2, \) then \( N_{\phi_k}^+(F) = S_k1 + S_k2 \) has 2 sides joining \((0, V_k), (1, 1), \) and \((5, 0), \) with \( V_k \geq 2. \) Thus, every side of \( N_{\phi_k}^+(F) \) is of degree 1. It follows by Theorem 3.4 that \( \phi_k \) provides two prime ideals of \( \mathbb{Z}_K \) lying above 5 with residue degree 2 each. Applying this for every \( k = 1, \ldots, 6, \) we conclude that there are 12 prime ideals of \( \mathbb{Z}_K \) lying above 5 with residue degree 2 each. By Proposition 4.2 there are only 10 monic irreducible polynomials of degree 2 in \( \mathbb{F}_5[x], \) by Lemma 4.1, 5 is a common index divisor, and so \( K \) is not monogenic.

Remark 4.3 Let \( F(x) = x^n - m \in \mathbb{Z}[x] \) be an irreducible polynomial over \( \mathbb{Q} \) and \( K = \mathbb{Q}(\alpha) \) with \( \alpha \) a complex root of \( F(x). \) Let \( p \) be a prime integer dividing \( n \) and does not divide \( m, \) and let \( r = v_p(n). \) In \([24],\) Gassert claimed that \( N_{\phi}^+(F) \) is the convex envelope of the set of points \( \{(0, v_p((m^p - m)))\: k=1,\ldots, r\}. \) The following example shows that this claim is not correct. \( F(x) = x^{60} - m \) with \( m \neq \pm 1 \) a square free integer such that \( m \equiv -1 \pmod{27}. \) Then, for \( p = 3 \) and \( \phi = x^2 + x - 1, \) we have \( F(x) = \cdots + a_3(x)\phi_1(x)^3 + a_2(x)\phi_1(x)^2 + a_1(x)\phi_1(x) + a_0(x), \) with \( a_1(x) = 16175489617620 - 2502342327220x, \)
\( a_0(x) = -1548008755920x + 956722026041 - m. \) As \( v_3(a_0(x)) = 2, \) then \( N_{\phi}^+(F) \) is the convex envelope of the set of points \( \{(0, 2), (1, 1), (3, 0)\} \) contrary to the claim, which says that it will be the convex envelope of the set of points \( \{(0, V), (1, 1), (3, 0)\} \) with \( V \geq 3. \)

Proof of Theorem 2.3 As \( \gcd(u, 30) = 1 \), let \( (x, y) \in \mathbb{Z}^2 \) be the unique solution of \( ux - 60y = 1 \) with \( 0 \leq y < u \) and let \( \theta = \frac{a^x}{a^y}. \) Then, \( \theta^{60} = \frac{a^{60x}}{a^{60y}} = a^{ux-60y} = a. \) Since \( g(x) = x^{60} - a \in \mathbb{Z}[x] \) 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 \( g(x) = x^{60} - a \) with \( a \neq \pm 1 \) a square free integer. The proof is therefore an application of Theorem 2.1 and Theorem 2.2. □
In order to illustrate the efficiency of our results, we finalize the paper by the following numerical examples.

**Example 4.4** Let \( F(x) \in \mathbb{Z}[x] \) be a monic irreducible polynomial and \( K \) the number field generated by a complex root of \( F(x) \).

1. If \( F(x) = x^{60} - 67 \), then \( F(x) \) is irreducible because it is 67-Eisenstein. Since \( m \equiv 3 \pmod{4} \), \( m \equiv 4 \pmod{9} \) and \( m \equiv 17 \pmod{25} \), by Theorem 2.1 \( K \) is monogenic.
2. If \( F(x) = x^{60} - 302 \), then \( F(x) \) is irreducible because it is 2-Eisenstein. Since \( m \equiv 2 \pmod{4} \), \( m \equiv 5 \pmod{9} \) and \( m \equiv 6 \pmod{25} \), by Theorem 2.1 \( K \) is monogenic.
3. If \( F(x) = x^{60} - 106 \), then \( F(x) \) is irreducible because it is 2-Eisenstein. Since \( m \equiv 1 \pmod{5} \), by Theorem 2.2 \( K \) is not monogenic.
4. If \( F(x) = x^{60} - 226 \), then \( F(x) \) is irreducible because it is 2-Eisenstein. Since \( m \equiv 1 \pmod{9} \), by Theorem 2.2 \( K \) is not monogenic.
5. If \( F(x) = (x - 5)^{60} - 70^{13} \), then \( F(x) \equiv x^{60} \pmod{5} \). As \( 70 \equiv 2 \pmod{4} \), \( 70 \equiv 7 \pmod{9} \) and \( 70 \equiv -5 \pmod{25} \), by Theorem 2.3, \( K \) is monogenic.
6. If \( F(x) = (x - 4)^{60} - 26^{31} \), then \( F(x) \equiv x^{60} \pmod{2} \). As \( 26 \equiv 1 \pmod{25} \), by Theorem 2.3, \( K \) is not monogenic.

**Remark 4.5** In all calculations of \( \phi \)-expansions, we used Maple 12 which takes a short running time.

**Acknowledgements** The authors are very grateful to the anonymous referee whose valuable comments and suggestions have tremendously improved the quality of this paper. The first author is very grateful to Professor István Gaál for his advice and encouragement as well as to Professor Enric Nart who introduced him to Newton polygon techniques.

**References**

1. Ahmad, S., Nakahara, T., 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., Hameed, A.: On certain pure sextic fields related to a problem of Hasse. Internat. J. Algebra Comput. 26(3), 577–583 (2016)
3. Ben Yakou, H., Chillali, A., El Fadil, L.: On power integral bases for certain pure number fields defined by \( x^{2r} \cdot 5^s - m \). Comm. Algebra 49(7), 2916–2926 (2021)
4. Ben Yakou, H., El Fadil, L.: On monogenity of certain pure number fields defined by \( x^{2r} - m \). Int. J. Number Theory 17(10), 2235–2242 (2021)
5. Bérczes, A., Evertse, J.H., Győry, K.: Multiply monogenic orders. Annali della Scuola Normale Superiore di Pisa-Classe di Scienze 5(12), 467–497 (2013)
6. Cohen, H.: A Course in Computational Algebraic Number Theory. Springer, Heidelberg, Berlin (1993)
7. Dedekind, R.: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. Göttingen Abhandlungen 23, 1–23 (1878)
8. El Fadil, L.: A note on the monogenity of pure number fields. arXiv:2106.00004
9. 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)
10. El Fadil, L.: On Newton polygon’s techniques and factorization of polynomial over Henselian valued fields. J. Algebra Appl., https://doi.org/S0219498820501881 (2020)
11. El Fadil, L.: On power integral bases for certain pure number fields defined by \( x^{24} - m \). Stud. Sci. Math. Hung. 57(3), 397–407 (2020)
12. El Fadil, L.: On integral bases and monogeneity of pure sextic number fields with non-squarefree coefficients. J. Number Theory 228, 375–389 (2021)
13. El Fadil, L.: On power integral bases for certain pure number fields defined by \( x^{36} - m \). Stud. Sci. Math. Hung. 58(3), 371–380 (2021)
14. El Fadil, L.: On power integral bases for certain pure sextic fields. Boletim da Sociedade Paranaense de Matematica 40(3s), 1–7 (2022)
15. El Fadil, L.: On power integral bases for certain pure number fields defined by $x^{2u^3v^7} - m$. Matematicum, available online March 11, 2022. https://doi.org/10.4064/cm8574-6-2021 (2022)
16. El Fadil, L.: On power integral bases for certain pure number fields. Publ. Math. Debr. 100(1–2), 219–231 (2022)
17. El Fadil, L., Najim, A.: On power integral bases for certain pure number fields defined by $x^{2u^3v^7} - m$. To appear in Acta Scientiarum Mathematicarum. https://doi.org/10.48550/arXiv.2106.01252
18. El Fadil, L., Montes, J., Nart, E.: Newton polygons and $p$-integral bases of quartic number fields. J. Algebra Appl. 11(4), 1250073 (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. Annales Universitatis Scientiarum Budapestinensis de Ronaldo Eotvos Nominate sectio Computatorica 18, 61–87 (1999)
21. Gaál, I.: Diophantine Equations and Power Integral Bases. Theory and Algorithm, 2nd edn. Boston, Birkhäuser (2019)
22. Gaál, I., Remete, L.: Binomial Thue equations and power integral bases in pure quartic fields. JP J. Algebra Number Theory Appl. 32(1), 49–61 (2014)
23. Gaál, I., Remete, L.: Power integral bases and monogeneity of pure fields. J. Number Theory 173(7), 129–146 (2017)
24. Gassert, T.A.: A note on the monogeneity of power maps. Albanian J. Math. 11(1), 3–12 (2017)
25. Guardia, J., Montes, J., Nart, E.: Newton polygons of higher order in algebraic number theory. Tran. Am. Math. Soc. 364(1), 361–416 (2012)
26. Hameed, A., Nakahara, T.: Integral bases and relative monogeneity of pure octic fields. Bulletin Mathématique de la Société des Sciences Mathématiques de Roumanie 58(106 (4)), 419–433 (2015)
27. Hasse, H.: Zahlentheorie. Akademie-Verlag, Berlin (1963)
28. Hensel, K.: Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung. J. Reine Angew. Math. 113, 128–160 (1894)
29. Hensel, K.: Theorie Der Algebraischen Zahlen. Teubner Verlag, Leipzig, Berlin (1908)
30. Montes, J., Nart, E.: On a theorem of Ore. J. Algebra 146(2), 318–334 (1992)
31. Motoda, Y., Nakahara, T., Shah, S.I.A.: On a problem of Hasse for certain imaginary abelian fields. J. Number Theory 96(2), 326–334 (2002)
32. Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers. Springer, Heidelberg, Berlin (2004)
33. Neukirch, J.: Algebraic Number Theory. Springer, Heidelberg, Berlin (1999)
34. Ore, O.: Newtonsche Polygone in der Theorie der algebraischen Korper. Math. Ann. 99(1), 84–117 (1928)
35. Pethő, A., Pohst, M.: On the indices of multiquadratic number fields. Acta Arith. 153(4), 393–414 (2012)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.