ON MONOGENITY OF CERTAIN PURE NUMBER FIELDS DEFINED BY $x^{2^u\cdot 3^v\cdot 5^t}-m$

LHOUSSAIN EL FADIL

Abstract. Let $K=\mathbb{Q}(\alpha)$ be a pure number field generated by a root α of a monic irreducible polynomial $F(x)=x^{2^u\cdot 3^v\cdot 5^t}-m$, with $m\neq\pm1$ a square free rational integer, u, v and t three positive integers. In this paper, we study the monogenity of K. We prove that if $m\not\equiv 1 \pmod 4$, $m\not\equiv\pm1 \pmod 9$, and $m\notin\{\pm1,\pm7\} \pmod{25}$, then K is monogenic. But if $m\equiv 1 \pmod 4$ or $m\equiv 1 \pmod 9$ or $m\equiv -1 \pmod 9$ and $u=2k$ for some odd integer k or $u\geq 2$ and $m\equiv 1 \pmod{25}$ or $m\equiv -1 \pmod{25}$ and $u=2k$ for some odd integer k or $u=v=1$ and $m\equiv\pm82 \pmod{5^4}$, then K is not monogenic.

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 know that the ring $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank $n=[K:\mathbb{Q}]$. Thus by the fundamental theorem of finitely generated Abelian groups, the Abelian group $\mathbb{Z}_K/\mathbb{Z}[\alpha]$ is finite. Its cardinal order is called the index of $\mathbb{Z}[\alpha]$, and denoted by $(\mathbb{Z}_K:\mathbb{Z}[\alpha])$. The ring $\mathbb{Z}_K$ is said to be monogenic if it has a power integral basis as a $\mathbb{Z}$-module. That is $(1,\theta,\cdots,\theta^{n-1})$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$ for some $\theta\in\mathbb{Z}_K$. K is said to be not monogenic otherwise. Monogenity of number fields is a classical problem of algebraic number theory, going back to Dedekind, Hasse, and Hensel (see for instance [22]). The problem of testing the monogenity of number fields and the construction of power integral bases has been intensively studied these last four decades, mainly by Gaál, Nakahara, Pohst, and their collaborators (see for instance [2, 21, 22, 23, 34]). In [19], Funakura, calculated integral bases and studied monogenity of pure quartic fields. In [24], Gaál and Remete, calculated the elements of index 1 in pure quartic fields generated by $m^{\frac14}$ 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 $m\not\equiv\pm1 \pmod 9$, then the sextic number field generated by $m^{\frac16}$ is monogenic. They also showed in [2], that if $m\equiv 1 \pmod 4$ and $m\not\equiv\pm1 \pmod 9$, then the sextic number field generated by $m^{\frac16}$ is not monogenic. In [8], 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 $m^{\frac16}$ is not monogenic. Hameed and Nakahara proved that if $m\equiv 1 \pmod 4$, 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 ([27]). In [25], by applying the explicit form of the index equation, Gaál and Remete

Date: April 7, 2022.

2010 *Mathematics Subject Classification.* 11R04, 11R16, 11R21.

Key words and phrases. Power integral basis, Theorem of Ore, prime ideal factorization, Newton polygons.

obtained deep new results on monogenity of number fields generated by $m^{\frac{1}{n}}$, with $3 \le n \le 9$ and $m \neq \pm 1$ a square free integer. In [3, 4, 18, 8, 9, 10, 11, 12, 13], based on Newton polygon's techniques, El Fadil et al. studied the monogenity of some pure number fields. Also El Fadil, Chouli, and Kchit studied the monogenity of pure number fields defined by $x^{60} - m \in \mathbb{Z}[x]$ with m a square free integer. The goal of this paper is to study the monogenity of pure number fields defined by $x^{2^u \cdot 3^v \cdot 5^t} - m$, where $m \neq \pm 1$ is a square free integer, u, v, and t are three natural integers. The cases $uvt = 0$ have been studied in [3, 28, 4, 18]. Also the case $u = 2$ and $t = v = 1$ has been studied by in [15]. Our proofs are based on Newton's polygon techniques and on index divisors as introduced by Hensel as follows: 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.

2. Main results

Let K be a number field generated by a complex root α of a monic irreducible polynomial $F(x) = x^{2^u \cdot 3^v \cdot 5^t} - m$, with $m \neq \pm 1$ a square free rational integer, u, v, and t three positive integers.

Theorem 2.1. *The ring $\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if $m \not\equiv 1 \pmod 4$, $m \not\equiv \pm 1 \pmod 9$, and $m \notin \{\pm 1, \pm 7\} \pmod{25}$.*

Remark. If $m \equiv 1 \pmod 4$, $m \not\equiv \pm 1 \pmod 9$, and $m \notin \{\pm 1, \pm 7\} \pmod{25}$, then $\mathbb{Z}[\alpha]$ is not integrally closed. But in this case, Theorem 2.1 cannot decide on monogenity of K. The following theorems give an answer.

Theorem 2.2. (1) *$m \equiv 1 \pmod 4$, then 2 divides $i(K)$.*

(2) *$m \equiv 1 \pmod 9$ or $m \equiv -1 \pmod 9$ and $u = 2k$ for some odd integer k or $u = 1$, $m \equiv -1 \pmod{27}$, and $v \ge 3$, then 3 divides $i(K)$.*

(3) *$m \equiv \pm 1 \pmod{25}$ and $u = 2k$ for some odd integer k or $u = 1$, $m \equiv \pm 1 \pmod{125}$, and $t \ge 2$ or $u = v = 1$, $m \equiv \pm 82 \pmod{5^4}$, and $t \ge 3$, then 5 divides $i(K)$.*

In particular, if one of these following conditions holds, then K is not monogenic.

Corollary 2.3. *Let $a \neq \pm 1$ be a square free rational integer, u, v and t three positive integers, and $s < 2^u \cdot 3^v \cdot 5^t$ a positive integer, which is coprime to 30. Then $F(x) = x^{2^u \cdot 3^v \cdot 5^t} - a^s$ is irreducible over $\mathbb{Q}$. Let K be the number field generated by a complex root α of the monic irreducible polynomial $F(x)$.*

(1) *If $a \not\equiv 1 \pmod 4$, $m \not\equiv \pm 1 \pmod 9$, and $m \notin \{\pm 1, \pm 7\} \pmod{25}$ then K is monogenic.*

(2) *If one of the following conditions holds*

(a) $a \equiv 1 \pmod 4$,

(b) $a \equiv 1 \pmod 9$,

(c) $a \equiv -1 \pmod 9$ *and $u = 2k$ for some positive odd integer k,*

(d) $a \equiv -1 \pmod{27}$ *and $v \ge 3$,*

(e) $a \equiv 1 \pmod{25}$ *and $u \ge 2$,*

(f) $a \equiv -1 \pmod{25}$ *and $u = 2k$ for some positive odd integer k,*

(g) $a \equiv \pm 82 \pmod{5^4}$, $u = v = 1$, *and $t \ge 3$,* *then K is not monogenic.*

3. Preliminaries

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$, $\mathbb{Z}_K$ its ring of integers, and $ind(\alpha) = (\mathbb{Z}_K : \mathbb{Z}[\alpha])$ 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, $p\mathbb{Z}_K = \prod_{i=0}^{r} \mathfrak{p}_i^{l_i}$, where every $\mathfrak{p}_i = p\mathbb{Z}_K + \phi_i(\alpha)\mathbb{Z}_K$ and $\overline{F(x)} = \prod_{i=1}^{r} \overline{\phi_i(x)}^{l_i}$ modulo p 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 [32, Chapter I, Proposition 8.3]). 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 1878, Dedekind proved the well known Dedekind's criterion which allows to test if a prime integer p divides $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ [5, Theorem 6.1.4] and [6]. 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 it is not possible 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 primes in a number field K by using Newton polygons (see [31, 33]). For the convenience of the reader, as it is necessary for the proof of our main results, we refer to our paper [20].

We start by recalling some fundamental facts about Newton polygons applied in algebraic number theory. For more details, we refer to [16, 17, 26]. For a prime integer p and for a monic polynomial $\phi \in \mathbb{Z}[x]$ whose reduction is irreducible in $\mathbb{F}_p[x]$, let $\mathbb{F}_\phi$ be the field $\frac{\mathbb{F}_p[x]}{(\overline{\phi})}$. For any monic polynomial $F(x) \in \mathbb{Z}[x]$, upon the Euclidean division by successive powers of ϕ, we expand $F(x)$ as $F(x) = \sum_{i=0}^{l} a_i(x)\phi(x)^i$, called the ϕ-expansion of $F(x)$ (for every i, $deg(a_i(x)) < deg(\phi)$). The ϕ-Newton polygon of $F(x)$ with respect to p, is the lower boundary of the convex envelope of the set of points $\{(i, \nu_p(a_i(x))), a_i(x) \neq 0\}$ in the Euclidean plane, which is denoted by $N_\phi(F)$. Let $S_1, S_2, \dots, S_t$ 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, 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. If $\lambda \neq 0$, then $\lambda = h/e$ with e and h two positive coprime integer. Notice that $e = l(S)/d$, called the ramification index of S and $h = H(S)/d$, where $d = \gcd(l(S), H(S))$ is called the degree of S. Thus $N_\phi(F)$ is the join of its different sides ordered by increasing slopes, which we can express by $N_\phi(F) = S_1 + S_2 + \cdots + S_t$. 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 all sides of negative slopes of $N_\phi(F)$. For every side S of $N_\phi^+(F)$, with initial point (s, u_s) and length l, and for every $i = 0, \dots, l$, we attach the following residue coefficient $c_i \in \mathbb{F}_\phi$ as follows:

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

where $(p, \phi(x))$ is the maximal ideal of $\mathbb{Z}[x]$ generated by p and 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. Notice that, the points with integer coordinates lying on S are exactly $(s, u_s), (s+e, u_s - h), \cdots, (s+de, u_s - dh)$. Thus, 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 $F_S(y) = t_d y^d + t_{d-1} y^{d-1} + \cdots + t_1 y + t_0 \in \mathbb{F}_\phi[y]$, called the residual polynomial of $F(x)$ associated to the side S, where for every $i = 0, \ldots, d$, $t_i = c_{ie}$. The theorem of Ore plays a key role for proving our main theorems:
Let $\phi \in \mathbb{Z}[x]$ be a monic polynomial, with $\overline{\phi(x)}$ irreducible in $\mathbb{F}_p[x]$. As defined in [17, 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). Assume that $\overline{F(x)} = \prod_{i=1}^r \overline{\phi_i}^{l_i}$ is the factorization of $\overline{F(x)}$ in $\mathbb{F}_p[x]$, where $\phi_1, \ldots, \phi_r$

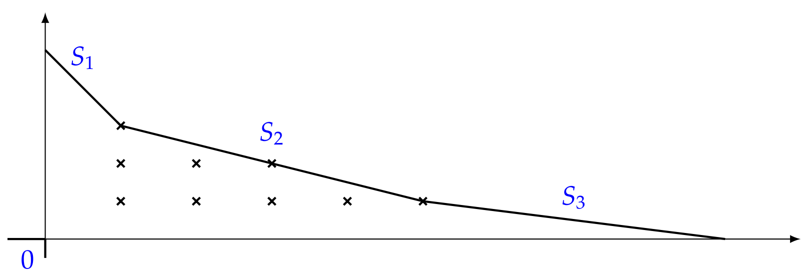

FIGURE 1. $N_\phi^+(F)$.

are monic polynomials lying in $\mathbb{Z}[x]$ and $\overline{\phi_1}, \ldots, \overline{\phi_r}$ are pairwise coprime irreducible polynomials over $\mathbb{F}_p$. For every $i = 1, \ldots, r$, let $N_{\phi_i}^+(F) = S_{i1} + \cdots + S_{ir_i}$ be the principal part of the ϕ_i-Newton polygon of F with respect to p. For every $j = 1, \ldots, r_i$, let $F_{S_{ij}}(y) = \prod_{s=1}^{s_{ij}} \psi_{ijs}^{a_{ijs}}(y)$ be the factorization of $F_{S_{ij}}(y)$ into powers of monic irreducible polynomials of $\mathbb{F}_{\phi_i}[y]$. Then we have the following theorem of Ore (see [17, Theorem 1.7 and Theorem 1.9], [16, Theorem 3.9], and [31]):

Theorem 3.1. *(Theorem of Ore)*

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

The equality holds if $a_{ijs} = 1$ for every i, j, s.

(2) *If* $a_{ijs} = 1$ *for every* i, j, s, *then*

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

is the factorization of $p\mathbb{Z}_K$ *into powers of prime ideals of* $\mathbb{Z}_K$ *lying above* p, *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* $i = 1, \dots, r$, $j = 1, \dots, r_i$, *and* $s = 1, \dots, s_{ij}$.

Corollary 3.2. *Under the assumptions above Theorem 3.1, if for every* $i = 1, \dots, r$, $l_i = 1$ *or* $N_{\phi_i}(F) = S_i$ *has a single side of height* 1, *then* $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$.

The following lemma allows to evaluate the p-adic valuation of the binomial coefficient $\binom{p^r}{j}$. For its proof, we refer to [4].

Lemma 3.3. *Let* p *be a rational prime integer and* r *be a positive integer. Then* $\nu_p\left(\binom{p^r}{j}\right) = r - \nu_p(j)$ *for any integer* $j = 1, \dots, p^r - 1$.

The following lemma allows to determine the ϕ-Newton polygon of $F(x)$.

Lemma 3.4. *Let* $F(x) = x^n - m \in \mathbb{Z}[x]$ *be an irreducible polynomial and* p *a 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* $\overline{F(x)} = \overline{(x^t - m)}^{p^r}$. *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* $\{(0, v)\} \cup \{(p^j, r - j),\ j = 0, \dots, r\}$.

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

4. Proofs of main results

Proof. of Theorem 2.1.

The proof of Theorem 2.1 can be done by using Dedekind's criterion as it was shown in the proof of [29, Theorem 6.1]. But as the other results are based on Newton polygon's techniques, let us use theorem of index with "if and only if" as it is given in [26, Theorem 4.18], which says 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 given in Theorem 3.1. Since $\triangle(F) = \mp(2^u \cdot 3^v \cdot 5^t)^{2^u \cdot 3^v \cdot 5^t} m^{2^u \cdot 3^v \cdot 5^t - 1}$, by the formula $\nu_p(\triangle(F)) = 2\nu_p(ind(F)) + \nu_p(d_K)$, where d_K is the absolute discriminant of K and $ind(F) = (\mathbb{Z}_K : \mathbb{Z}[\alpha])$, we conclude that $\mathbb{Z}[\alpha]$ is integrally closed if and only if p does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ for every rational prime integer p dividing $30m$. Let p be a rational prime dividing m, then $F(x) \equiv \phi^{2^u \cdot 3^v \cdot 5^t} (\ mod\ p)$, where $\phi = x$. As m is a square free integer, the ϕ-principal Newton polygon with respect to ν_p, $N_\phi^+(F) = S$ has a single side of height $\nu_p(m)$. As $l(S) = 2^u \cdot 3^v \cdot 5^t \geq 2$, $ind_\phi(F) = 0$ if and only if S has height 1, which means $\nu_p(m) = 1$. It follows that the unique prime candidates to divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ are 2, 3, and 5.

For $p = 2$ and 2 does not divide m, let $\phi \in \mathbb{Z}[x]$ be a monic polynomial, whose

reduction is an irreducible factor of $(x^{3^v\cdot 5^t}-1)$ in $\mathbb{F}_2[x]$. Again as $l(N_\phi^+(F)) = 2^u \geq 2$, $ind_\phi(F) = 0$ if and only if $N_\phi^+(F)$ has a single side of height 1, which means by Lemma 3.4 that $\nu_2(1-m) = 1$; $m \not\equiv 1 \pmod 4$.
Similarly, for $p = 3$ and 3 does not divide m, let $\phi \in \mathbb{Z}[x]$ be a monic polynomial, whose reduction is an irreducible factor of $(x^{2^u\cdot 5^t}-m)$ in $\mathbb{F}_3[x]$. Again as $l(N_\phi^+(F)) = 3^v \geq 2$, $ind_\phi F = 0$ if and only if $N_\phi^+(F)$ has a single side of height 1, which means by Lemma 3.4 that $\nu_3(m^2-1) = 1 = 1$; $m \not\equiv \mp 1 \pmod 9$.
Again, for $p = 5$ and 5 does not divide m, let $\phi \in \mathbb{Z}[x]$ be a monic polynomial, whose reduction is an irreducible factor of $(x^{2^u\cdot 3^v}-m)$ in $\mathbb{F}_5[x]$. As $l(N_\phi^+(F)) = 5^t \geq 2$, $ind_\phi F = 0$ if and only if $N_\phi^+(F)$ has a single side of height 1, which means by Lemma 3.4 that $\nu_5(m^4-1) = 1 = 1$; $m \notin \{\mp 1, \pm 7\} \pmod{25}$. □

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 $F(x) = x^3 - x^2 - 2x - 8$ 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 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 prime integer p to be a prime common index divisor [30]. (For more details see [29]). For the proof of Theorem 2.2, we need the following lemma, which characterizes the prime common index divisors of K. We need to use only one way, which 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.*

Remark. As it was shown in the proof of Theorem 2.1, the unique prime candidates to be a prime common index divisors of K are 2, 3, and 3, because if $p \notin \{2,3,5\}$, 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 $x^{2^u\cdot 3^v\cdot 5^t} - m$ 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 3.1, could be 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 Theroem 3.1, 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(ψ_{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.

(1) Assume that $m \equiv 1 \pmod 4$. Let $3^v \cdot 5^t = 3s$ for some odd integer $s \in \mathbb{Z}$. Then $\overline{F(x)} = \overline{((x^3-1)(U(x))^{2^u}} = \overline{(x^2+x+1)T(x)}^{2^u}$ in $\mathbb{F}_2[x]$ for some monic polynomials U and T in $\mathbb{Z}[x]$ such that $\overline{(x^2+x+1)}$ and $\overline{T(x)}$ are coprime over $\mathbb{F}_2[x]$ because $\overline{(x^{3s}-1)}$ is separable over $\mathbb{F}_2[x]$. Let $\phi = x^2+x+1$ and $x^{3s}-1 = \phi(x)T(x)+2a$ for some integer $a \in \mathbb{Z}$.

(a) $\nu_2(1-m) = 2$, then by Lemmas 3.4 and 3.3, $N_\phi^+(F) = S$ has a single side of degree $d = 2$. By using $F(x) = ((x^{3s}-1)+1)^{2^u} - m = (\phi(x)T(x)+2a)^{2^u} + \sum_{j=1}^{2^u-1}\binom{2^u}{j}(T\phi+2a)^{3^v-j}\cdots+1-m$, we have $F_S(y) = t^2y^2+ty+1$, where $t \equiv T(x) \pmod{2,\phi}$ is a nonzero element of $\mathbb{F}_\phi$ (because $\overline{\phi}$ does not divide $\overline{T(x)}$ in $\mathbb{F}_2[x]$). Hence $F_S(y) = (ty-x)(ty-x^2)$ in $\mathbb{F}_\phi[y]$. Thus by Remark 4, ϕ provides 2 distinct prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 2 each. If $\nu_2(1-m) = 3$, then by Lemmas 3.4 and 3.3, $N_\phi^+(F)$ has two sides S_1 and S_2 joining the point $(0,3)$, $(2^{u-1},1)$, and $(2^u,0)$ (see *FIGURE* 2). Thus S_1 is a side of degree 2 and S_2 is a side of degree 1. By using $F(x) = ((x^{3s}-1)+1)^{2^u} - m = (\phi(x)T(x)+2a)^{2^u} + \sum_{j=1}^{2^u-1}\binom{2^u}{j}(T\phi+2a)^{3^v-j}\cdots+1-m$, we conclude that $F_{S_1}(y) = t^2y^2+ty+1 = (ty-x)(ty-x^2)$, where $t \equiv T(x) \pmod{2,\phi}$ is a nonzero element of $\mathbb{F}_\phi$ and $F_{S_2}(y)$ is of degree 1. By Remark 4, ϕ provides three prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree $\deg(\phi) = 2$ each. As x^2+x+1 is the unique monic irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, by Lemma 4.1, 2 divides $i(K)$ and K is not monogenic.

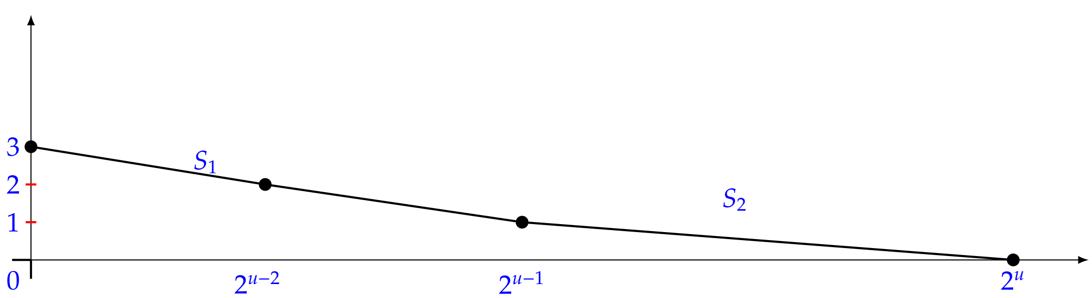

FIGURE 2. $N_\phi^+(F)$ for $v_2 = 3$.

(b) If $v_2 \geq 4$, then by Lemma 3.4, $N_\phi^+(F)$ has $g \geq 2$ sides for which the last two sides S_g and S_{g-1} are of height 1 each (see *FIGURE*3). Thus, $F_{S_g}(y)$ and $F_{S_{g-1}}(y)$ are of degree 1. By Remark 4, ϕ provides at least two prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree $\deg(\phi) = 2$ each. As x^2+x+1 is the unique monic irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, by Lemma 4.1, 2 divides $i(K)$ and K is not monogenic.

(2) Assume $m \equiv 1 \pmod 9$. Let $2^u \cdot 5^t = 2s$ for some integer $s \in \mathbb{Z}$. Then $\overline{F(x)} = (x^{2s}-1)^{3^v} = ((x-1)(x+1)U(x))^{3^v}$ in $\mathbb{F}_3[x]$ for some monic polynomial

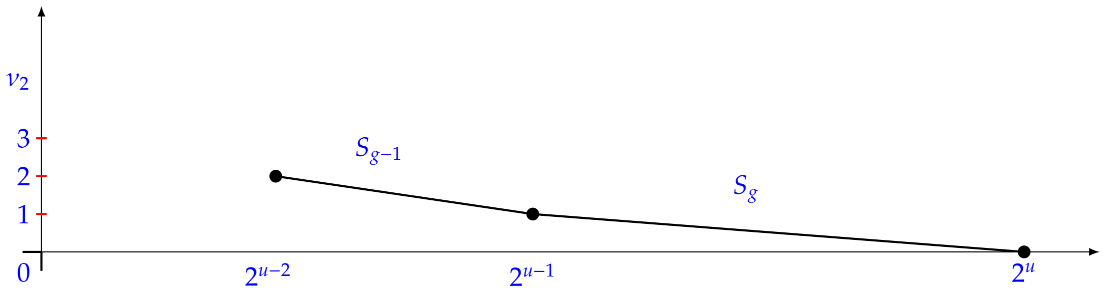

FIGURE 3. $N_{\phi}^{+}(F)$ for $v_2 \geq 4$.

$U(x) \in \mathbb{F}_3[x]$. Let $\phi_1 = x-1$, $\phi_2 = x+1$, and $v_3 = \nu_3(1-m)$. If $v_3 \geq 2$, then by Lemmas 3.4 and 3.3, $N_{\phi_i}^{+}(F)$ has $g \geq 2$ sides of which the last two sides S_{ig} and S_{ig-1} are of height 1 each for every $i = 1, 2$ (see *FIGURE*4 and *FIGURE*5). Thus $F_{S_{ig}}(y)$ and $F_{S_{ig-1}}(y)$ are of degree 1 for every $i = 1, 2$. By Remark 4, every ϕ_i provides at least 2 prime ideals $\mathfrak{p}_{ij}$ of $\mathbb{Z}_K$ lying above 3 with residue degree $f_{ij} = 1$ for every $i, j = 1, 2$. Therefore, there are at least 4 prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each. As there is only 3 monic irreducible polynomial of degree 1 in $\mathbb{F}_3[x]$, by Lemma 4.1, 3 divides $i(K)$ and K is not monogenic.

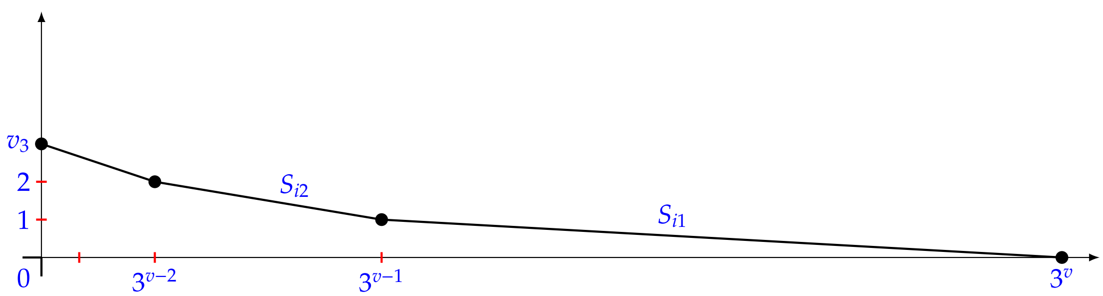

FIGURE 4. $N_{\phi_i}^{+}(F)$ for $v \geq 2$ and $v_3 = 3$.

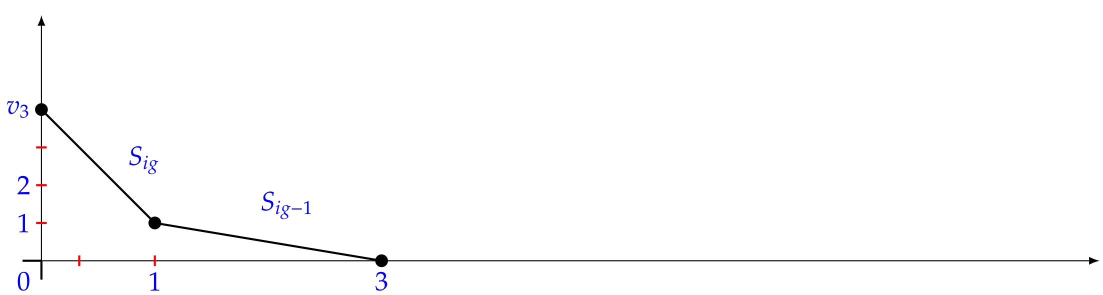

FIGURE 5. $N_{\phi_i}^{+}(F)$ for $v = 1$ and $v_3 \geq 3$.

(3) Assume that $m \equiv -1 \pmod 9$ and $u = 2k$ for some odd integer k. Then $2^u \cdot 5^t = 4s$ for some odd nonnegative integer s. Thus $\overline{F(x)} = \overline{(x^4+1)U(x)^{3^v}} = ((x^2+x-1)(x^2-x-1)U(x))^{3^v}$ in $\mathbb{F}_3[x]$ for some monic polynomial $U \in \mathbb{Z}[x]$. Let $\phi_1 = x^2+x-1$, $\phi_2 = x^2-x-1$, and $v_3 = \nu_3(1-m)$. Since 3 does not divide $4s = 2^u \cdot 5^t$, $\overline{(x^{4s}+1)}$ is separable over $\mathbb{F}_3$. So, $\overline{\phi_1\phi_2(x)}$ and $\overline{U(x)}$ are coprime in $\mathbb{F}_3[x]$. By Lemmas 3.4 and 3.3, for every $i = 1, 2$, $N^+_{\phi_i}(F)$ has at least two sides S_{i1} and S_{i2} with height 1 each. Thus $F_{S_{ij}}(y)$ is irreducible over $\mathbb{F}_{\phi_i}$ as it is of degree 1 for every $i, j = 1, 2$. By Remark 4, every factor ϕ_i provides at least two distinct prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree $f = 2$ each. Thus there are at least four distinct prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree $f = 2$ each. As x^2+1, x^2+x-1, and x^2-x-1 are the unique monic irreducible polynomials of degree 2 in $\mathbb{F}_3[x]$, by Lemma 4.1, 3 divides $i(K)$, and so K is not monogenic.

(4) Similarly, if we assume that $u = 1$, $m \equiv \pm 1 \pmod{81}$, and $v \geq 3$, then let $\phi = x^2+1$. By Lemmas 3.4 and 3.3, $N^+_{\phi}(F)$ has at least four sides of degree 1 each. Thus ϕ provides at least four prime ideals of $\mathbb{Z}_K$ lying above 3 with residue degree 1 each.

(5) Assume that $m \equiv \pm 1 \pmod{125}$ and $t \geq 2$. Then $\overline{F(x)}$ has two monic factors ϕ_1 and ϕ_2 of degree 1 each in $\mathbb{F}_5[x]$. Let $\overline{\phi}$ be one fixed factor of $\overline{F(x)}$ of degree 1. Since $m \equiv \pm 1 \pmod{125}$, by Lemmas 3.4 and 3.3, we conclude that $N^+_{\phi}(F)$ has at least 3 sides of degree 1 each. Thus ϕ provides at least 3 prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each. Hence the two factors ϕ_1 and ϕ_2 provide at least 6 prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each. Therefore 5 divides $i(K)$, and so K is not monogenic.

(6) Assume that $m \equiv 1 \pmod{25}$ and $u \geq 2$. By the litle Fermat's theorem, $\overline{x^4-1}$ has four distinct monic factors of degree 1 each in $\mathbb{F}_5[x]$. Let $\overline{\phi}$ be one fixed factor of degree 1 of $\overline{F(x)}$ in $\mathbb{F}_5[x]$. Since $m \equiv 1 \pmod{25}$, by Lemmas 3.4 and 3.3, we conclude that $N^+_{\phi}(F)$ has at least 2 sides of degree 1 each. Thus ϕ provides at least 2 prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 2 each. It follows that the four factors provide at least 8 prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 1 each. Thus, 5 divides $i(K)$, and so K is not monogenic.

(7) If $m \equiv -1 \pmod{25}$ and $u = 2k$, then $\overline{x^{12}+1}$ divides $\overline{F(x)}$ in $\mathbb{F}_5[x]$ and $\overline{x^{12}+1} = \overline{(x^2+4x+2)(x^2+3x+3)(x^2+2)(x^2+x+2)(x^2+2x+3)(x^2+3)}$ in $\mathbb{F}_5[x]$. Let $\overline{\phi}$ be one fixed of these factors. Since $m \equiv 1 \pmod{25}$, by Lemmas 3.4 and 3.3, $N^+_{\phi}(F)$ has at least 2 sides of degree 1 each. Thus ϕ provides at least 2 prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 2 each. Hence there are at least 12 prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 2 each. As there are only 10 monic irreducible polynomial of degree 2 in $\mathbb{F}_5[x]$, by Lemma 4.1, 5 divides $i(K)$, and so K is not monogenic.

(8) Assume that $u = v = 1$, $m \equiv \pm 82 \pmod{5^4}$, and $t \geq 3$. Since $\overline{x^6 - 2} = \overline{(x^2+4x+2)(x^2+x+2)(x^2+2)}$ and $\overline{x^6+2} = \overline{(x^2+3)(x^2+3x+3)(x^2+2x+3)}$ in $\mathbb{F}_5[x]$. Let $\overline{\phi}$ be one fixed irreducible factor of $\overline{F(x)}$ of degree 2. Since $m \equiv \pm 82 \pmod{5^4}$, we have $\nu_5(m^4+1) \geq 4$. So, by Lemmas 3.4 and 3.3, we conclude that $N_\phi^+(F)$ has at least 4 sides of degree 1 each. Thus ϕ provides at least 4 prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 2 each. Since $\overline{F(x)}$ has 3 distinct monic irreducible factors in $\mathbb{F}_5[x]$ of degree 2 each, we conclude that there are at least 12 prime ideals of $\mathbb{Z}_K$ lying above 5 with residue degree 2 each. As there is only 10 monic irreducible polynomial of degree 2 in $\mathbb{F}_5[x]$, by Lemma 4.1, 5 divides $i(K)$, and so K is not monogenic.

□

Proof. of Theorem 2.3.
Since $\gcd(k, 30) = 1$, let $(x, y) \in \mathbb{Z}^2$ be the unique solution of the equation $k \cdot x - 2^u \cdot 3^v \cdot 5^t \cdot y = 1$ and $\theta = \frac{\alpha^x}{a^y}$. Then $\theta^{2^u \cdot 3^v \cdot 5^t} = a$, and so $g(x) = x^{2^u \cdot 3^v \cdot 5^t} - a$ is the minimal polynomial of θ over $\mathbb{Q}$; $\theta \in \mathbb{Z}_K$ is a primitive element of K. Since $a \neq \pm 1$ is a square free integer, we can apply Theorems 2.1 and 2.2, and get the desired result. □

References

[1] S. Ahmad, T. Nakahara, and S. M. Husnine, *Power integral bases for certain pure sextic fields*, Int. J. of Number Theory v:10, No 8 (2014) 2257–2265.

[2] S. Ahmad, T. Nakahara, and A. Hameed, *On certain pure sextic fields related to a problem of Hasse*, Int. J. Alg. and Comput. 26(3) (2016) 577–583

[3] H. Ben Yakou and L. El Fadil, *on power integral bases for certain pure number fields defined by* $x^{p^r} - m$, Int. J. Number theory, 2021, doi:10.1142/S1793042121500858

[4] H. Ben yakkou, L. El Fadil, and A. Chillali, *On Power integral bases for certain pure number fields defined by* $x^{2^r \cdot 5^s} - m$, Comm. in Algebra, 2021, doi: 10.1080/0092782.2021.1883642

[5] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag Berlin Heidelberg (1993)

[6] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Göttingen Abhandlungen **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(13-16)(2007) 601–606

[8] L. El Fadil, *On Power integral bases for certain pure sextic fields* (To appear in a forthcoming issue of Bol. Soc. Paran. Math.)

[9] L. El Fadil, *On Power integral bases for certain pure sextic fields*J, J. Number Theory, 228 (2021) 375–389

[10] L. El Fadil, *On Power integral bases for certain pure number fields* (To appear in a forthcoming issue of Publicationes Mathematicae)

[11] L. El Fadil, *On Power integral bases for certain pure number fields defined by* $x^{24} - m$, Stud. Sci. Math. Hung. **57**(3) (2020) 397–407

[12] L. El Fadil, *On Power integral bases for certain pure number fields defined by* $x^{18} - m$, (To appear in Comm. Math. Uni. of Carolina)

[13] L. El Fadil, *On Power integral bases for certain pure number fields defined by* $x^{2 \cdot 3^k} - m$ (To appear in a forthcoming issue of Act. Arith.)

[14] L. El Fadil, *On Power integral bases for certain pure number fields defined by* $x^{2 \cdot 3^k} - m$, Colloquium Mathematicum, 2022, doi:10.4064/cm8574-6-2021

[15] L. El Fadil, *On Power integral bases for certain pure number fields defined by* $x^{60} - m$, (To appear in Acta Mathematica Vietnamica)
[16] L. El Fadil,*On Newton polygon's techniques and factorization of polynomial over Henselian valued fields*, J. of Algebra and its Appl. (2020), doi: S0219498820501881
[17] L. El Fadil, J. Montes and E. Nart, *Newton polygons and p-integral bases of quartic number fields*, J. Algebra and Appl. 11(4) (2012) 1250073
[18] L. El Fadil and A. Najim, *On Power integral bases for certain pure number fields defined by* $x^{2^u \cdot 3^v} - m$ (To appear in ASM)
[19] T. Funakura, *On integral bases of pure quartic fields*, Math. J. Okayama Univ. 26 (1984) 27–41
[20] L. El Fadil and I. Gaál, *On integral bases and monogeneity of pure octic number fields with non-square free parameters*, (To appear in Glasnik Mat.)
[21] I. Gaál, *Power integral bases in algebraic number fields*, Ann. Univ. Sci. Budapest. Sect. Comp. 18 (1999) 61–87
[22] I. Gaál, Diophantine equations and power integral bases, Theory and algorithm, Second edition, Boston, Birkhäuser, 2019
[23] I. Gaál, P. Olajos, and M. Pohst, *Power integral bases in orders of composite fields*, Exp. Math. 11(1) (2002) 87–90.
[24] I. Gaál and L. Remete, *Binomial Thue equations and power integral bases in pure quartic fields*, JP Journal of Algebra Number Theory Appl. 32(1) (2014) 49–61
[25] I. Gaál and L. Remete, *Power integral bases and monogenity of pure fields*, J. of Number Theory 173 (2017) 129–146
[26] J. Guardia, J. Montes and E. Nart,*Newton polygons of higher order in algebraic number theory*, J. trans. of ams **364**(1) (2012) 361–416
[27] A.Hameed and T.Nakahara, *Integral bases and relative monogenity of pure octic fields*, Bull. Math. Soc. Sci. Math. R épub. Soc. Roum. 58(106) No. 4(2015) 419–433
[28] A. Hameed, T. Nakahara, S. M. Husnine, On existence of canonical number system in certain classes of pure algebraic number fields, J. Prime Res. Math. 7(2011) 19–24.
[29] H. Smith, The monogenity of radical extension, *Acta Arithmitica*, **198**(2021), 313–327.
[30] K. Hensel, *Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung*, J. Reine Angew. Math., 113:128–160, 1894. ISSN 0075-4102. doi: 10.1515/crll.1894.113.128.
[31] J. Montes and E. Nart, *On a theorem of Ore*, J. Algebra **146**(2) (1992) 318–334
[32] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.
[33] O. Ore, *Newtonsche Polygone in der Theorie der algebraischen Korper*, Math. Ann., 99 (1928), 84–117
[34] A. Pethö and M. Pohst, *On the indices of multiquadratic number fields*, Acta Arith. 153(4) (2012) 393–414

Faculty of Sciences Dhar El Mahraz, P.O. Box 1796 Atlas-Fez , Sidi Mohamed Ben Abdellah University, Fez– Morocco
Email address: lhoussain.elfadil@usmba.ac.ma