On power integral bases for certain pure number fields defined by $x^{18} - m$

Lhoussain El Fadil

Abstract. Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a complex root α of a monic irreducible polynomial $f(x) = x^{18} - m$, $m \neq \mp 1$, is a square free rational integer. We prove that if $m \equiv 2$ or $3 \pmod 4$ and $m \not\equiv \mp 1 \pmod 9$, then the number field K is monogenic. If $m \equiv 1 \pmod 4$ or $m \equiv 1 \pmod 9$, then the number field K is not monogenic.

Keywords: power integral base; theorem of Ore; prime ideal factorization

Classification: 11R04, 11R16, 11R21

Let $K = \mathbb{Q}(\alpha)$ be a pure number field generated by a complex root α of a monic irreducible polynomial $f(x) = x^n - m \in \mathbb{Z}[x]$, $\mathbb{Z}_K$ its ring of integers, $\triangle(f)$ the discriminant of f, d_K the discriminant of the field K, and $\mathrm{ind}(\alpha) = (\mathbb{Z}_K : \mathbb{Z}[\alpha])$ the index of $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_K$. It is well know that the ring $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$ and a well known formula relating $\triangle(f)$, d_K, and $\mathrm{ind}(\alpha)$ says that for every prime rational integer p, $\nu_p(d_K) = \nu_p(\triangle(f)) - 2\nu_p(\mathrm{ind}(\alpha))$. The number field K is said to be monogenic if $\mathbb{Z}_K$ is generated by a single generator θ as a ring; $\mathbb{Z}_K = \mathbb{Z}[\theta]$ for some generator $\theta \in \mathbb{Z}_K$; p does not divide the index $\mathrm{ind}(\alpha)$ for every rational prime integer p. In such a case, $\mathbb{Z}_K$ is said to have a power integral basis $(1, \theta, \cdots, \theta^{n-1})$ or the number field K is said to be monogenic. Otherwise, the number field K is said to be not monogenic. The problem of testing the monogenity of number fields and constructing power integral bases have been intensively studied mainly by I. Gaál, T. Nakahara, A. Pethő, and their research teams, see for instance [1], [9], [10], [11], [16]. In [3], we gave conditions for the existence of power integral bases of pure cubic fields in terms of the index form equation. In [8] T. Funakura studied the integral basis in pure quartic fields. In [12] I. Gaál and L. Remete calculated all generators of power integral bases with coefficients less than 10^{1000} in pure quartic number fields generated by $m^{1/4}$ for $1 < m < 10^7$ and $m \equiv 2, 3 \pmod 4$. In [1] S. Ahmad, T. Nakahara and S. M. Husnine proved that if $m \equiv 2, 3 \pmod 4$ and $m \not\equiv \mp 1 \pmod 9$, then the

DOI 10.14712/1213-7243.2022.005

sextic number field generated by $m^{1/6}$ is monogenic. They also showed in [2] that if $m \equiv 1 \pmod 4$ and $m \not\equiv \mp 1 \pmod 9$, then the sextic number field generated by $m^{1/6}$ is not monogenic. Also in [14] A. Hameed and T. Nakahara proved that if $m \equiv 1 \pmod 4$, then the octic number field generated by $m^{1/8}$ is not monogenic. They also showed with S. M. Husnine and S. Ahmad that if $m \equiv 2, 3 \pmod 4$, then the octic number field generated by $m^{1/8}$ is monogenic. In [13] by applying the explicit form of the index forms, I. Gaál and L. Remete obtained new results on monogenity of the number fields generated by $m^{1/n}$, where $3 \le n \le 9$. 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. In this paper, a new method based on prime ideal factorization is proposed.

Let $K = \mathbb{Q}(\alpha)$ be a pure number field generated by a complex root α of a monic irreducible polynomial $f(x) = x^{18} - m$ with $m \neq \mp 1$ being a square-free rational integer. In this paper, we prove that if $m \equiv 2$ or $3 \pmod 4$ and $m \not\equiv \mp 1 \pmod 9$, then the number field K is monogenic. If $m \equiv 1 \pmod 4$ or $m \equiv 1 \pmod 9$, then the number field K is not monogenic. As their degrees are $2^r \cdot 3^t$, these results are very closed to that proved for the pure number fields defined by $x^{12} - m$ and $x^{24} - m$, with the same techniques in the proofs, see [6], [5].

1. Main results

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a complex root α of a monic irreducible polynomial $f(x) = x^{18} - m$, where $m \neq \mp 1$ is a square free rational integer.

Theorem 1.1. *Under the above hypothesis, if* $m \equiv 2$ *or* $3 \pmod 4$ *and* $m \not\equiv \mp 1 \pmod 9$, *then K is monogenic. More precisely, generated by α.*

Theorem 1.2. *Under the above hypothesis, if* $m \equiv 1 \pmod 4$ *or* $m \equiv 1 \pmod 9$, *then K is not monogenic.*

2. Proofs

We start by recalling some fundamental notions on Newton polygon's techniques. For more details, we refer to [4], [7]. For any prime integer p and for any monic polynomial $\varphi \in \mathbb{Z}[x]$ whose reduction is irreducible in $\mathbb{F}_p[x]$, let $\mathbb{F}_\varphi$ be the field $\mathbb{F}_p[x]/(\overline{\varphi})$. For any monic polynomial $f(x) \in \mathbb{Z}[x]$, upon the euclidean division by successive powers of φ, we expand $f(x)$ as $f(x) = \sum_{i=0}^{l} a_i(x)\varphi(x)^i$, called the φ-expansion of $f(x)$ (for every i, $\deg(a_i(x)) < \deg(\varphi)$). The φ-Newton polygon of $f(x)$ with respect to p, is the lower boundary convex envelope of the set of points $\{(i, \nu_p(a_i(x)))\colon a_i(x) \neq 0\}$ in the euclidean plane, which we denote by $N_\varphi(f)$. For every $i \neq j$, $i,j = 1,\ldots,l$, let $a_i = a_i(x)$ and $\mu_{i,j} = (\nu_p(a_i)-\nu_p(a_j))/(i-j) \in \mathbb{Q}$. Then we obtain the following integers $0 = i_0 < i_1 < \cdots < i_r = l$ satisfying $i_{j+1} = \max\{i,\ \mu_{i_j,i} \leq \mu_{i_j,k}$ for any $i_{j+1} \leq k \leq l\}$. For every $j = 1,\ldots r$, let S_j be the segment joining the points $A_{j-1} = (i_{j-1}, \nu(a_{i_{j-1}}))$ and $A_j = (i_j, \nu(a_{i_j}))$ in the euclidean plane. The segments $S_1,\ldots,S_r$ are called the sides of the polygon $N_\varphi(f)$. For every $j = 1,\ldots,r$, the rational number $\lambda_j = (\nu_p(a_{i_j}) - \nu_p(a_{i_{j-1}}))/(i_j - i_{j-1}) \in \mathbb{Q}$ is called the slope of S_j, $l(S_j) = i_j - i_{j-1}$ is its length, and $h(S_j) = -\lambda_j l(S_j)$ is its height. In what follows $\nu(a_{i_j}) = \nu(a_{i_{j-1}}) + l(S_j)\lambda_j$. The φ-Newton polygon of f is the process of joining the segments $S_1,\ldots,S_r$ ordered by the increasing slopes, which can be expressed as $N_\varphi(f) = S_1 + \cdots + S_r$. Notice that $N_\varphi(f) = S_1 + \cdots + S_r$ is only a notation and not the sum in the euclidean plane. For every side S of the polygon $N_\varphi(f)$, $l(S)$ is the length of its projection to the x-axis, $h(S)$ is the length of its projection to the y-axis, and $d(S) = \gcd(l(S), h(S))$, called the ramification index of S. The principal part of $N_\varphi(f)$, denoted $N_\varphi^+(f)$, is the part of the polygon $N_\varphi(f)$, which is determined by joining all sides of negative slopes.

For instance, for two distinct rational prime integers p and q, and for a monic polynomial $\varphi \in \mathbb{Z}[x]$ whose reduction is irreducible in $\mathbb{F}_p[x]$, let $f(x) = \varphi^7 + q\cdot p^2\varphi^3 + q\cdot p^6\varphi + q\cdot p^6$.

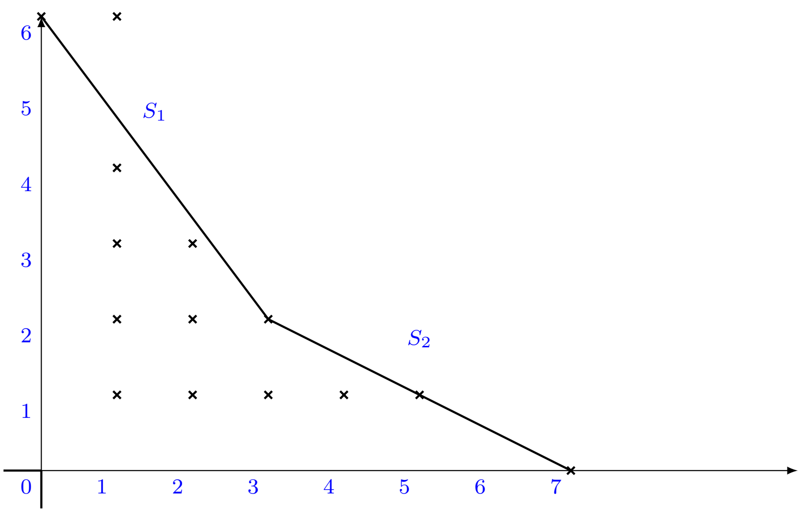

FIGURE 1. $N_\varphi^+(f)$.

For every side S of $N_\varphi(f)$, with initial point (s, u_s) and length l, and for every $0 \le i \le l$, we attach the following residual coefficient $c_i \in \mathbb{F}_\varphi$ as follows:

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

where $(p, \varphi(x))$ 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, and let $d = l/e$ be the degree of S. Notice that the points with positive rational integer coordinates lying in 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 in S, and so, $c_i = 0$. Let $f_S(y) = c_{de}y^d + c_{(d-1)e}y^{d-1} + \cdots + c_e y + c_0 \in \mathbb{F}_\varphi[y]$, called the residual polynomial of $f(x)$ associated to the side S. Let $N_\varphi^+(f) = S_1 + \cdots + S_r$ be the φ-principal Newton polygon of f with respect to p.

We say that f is a φ-regular polynomial with respect to p, if for every $i = 1, \ldots, r$, $f_{S_i}(y)$ is square free in $\mathbb{F}_\varphi[y]$. We say that f is a p-regular polynomial if f is a φ_i-regular polynomial with respect to p for every $i = 1, \ldots, t$ for some monic polynomials $\varphi_1, \ldots, \varphi_t$ with $\overline{f(x)} = \prod_{i=1}^t \overline{\varphi_i}^{\,l_i}$ is the factorization of $\overline{f(x)}$ in $\mathbb{F}_p[x]$.

The theorem of Ö. Ore is a fundamental key for proving our main theorems. Let $\varphi \in \mathbb{Z}[x]$ be a monic polynomial, and $\overline{\varphi(x)}$ is irreducible in $\mathbb{F}_p[x]$. As defined in [7, Definition 1.3], the φ-index of $f(x)$, denoted by $\mathrm{ind}_\varphi(f)$, is $\deg(\varphi)$ times the number of points with natural integer coordinates that lie below or on the polygon $N_\varphi^+(f)$, strictly above the horizontal axis, see Figure 1. In the described case in Figure 1, $\mathrm{ind}_\varphi(f) = 11 \times \deg(\varphi)$.

Now assume that $\overline{f(x)} = \prod_{i=1}^t \overline{\varphi_i}^{\,l_i}$ is the factorization of $\overline{f(x)}$ in $\mathbb{F}_p[x]$, where every $\varphi_i \in \mathbb{Z}[x]$ is monic, $\overline{\varphi_i(x)}$ is irreducible in $\mathbb{F}_p[x]$, $\overline{\varphi_i(x)}$ and $\overline{\varphi_j(x)}$ are coprime when $i \ne j = 1, \ldots, t$. For every $i = 1, \ldots, t$, let $N_{\varphi_i}^+(f) = S_{i1} + \cdots + S_{ir_i}$ 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 $f_{S_{ij}}(y)$ in $\mathbb{F}_{\varphi_i}[y]$. Then we have the following theorem of Ö. Ore, see [7, Theorem 1.7 and Theorem 1.9], [4, Theorem 3.9], and [15]:

Theorem 2.1 (Ö. Ore)**.** *According the above hypothesis, assume that* $\overline{f(x)} = \prod_{i=1}^t \overline{\varphi_i}^{\,l_i}$ *is the factorization of* $\overline{f(x)}$ *in* $\mathbb{F}_p[x]$*. Then*

(1) $\nu_p(\mathrm{ind}(f)) = \nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) \ge \sum_{i=1}^t \mathrm{ind}_{\varphi_i}(f)$ *and equality holds if* $f(x)$ *is* p*-regular;* $a_{ijs} = 1$ *for every* i, j, s*.*

(2) *If every* $a_{ijs} = 1$, *then*

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

where e_{ij} *is the ramification index of the side* S_{ij} *and* $f_{ijs} = \deg(\varphi_i) \times \deg(\psi_{ijs})$ *is the residue degree of* $\mathfrak{p}_{ijs}$ *over* p.

Corollary 2.2. *Under the hypothesis of Theorem* 2.1, *if for every* $i = 1, \dots, t$, $l_i = 1$ *or* $N_{\varphi_i}(f) = S_i$ *has a single side of height* 1, *then* $\nu_p(\mathrm{ind}(f)) = 0$.

Indeed, as for every $i = 1, \dots, t$, $d_i = 1$, f_{S_i} is of degree one, and so it is irreducible over $\mathbb{F}_{\varphi_i}$. Hence by Theorem 2.1, $\nu_p(\mathrm{ind}(f)) = \sum_{i=1}^{t} \mathrm{ind}_{\varphi_i}(f) = 0$.

Let $K = \mathbb{Q}(\alpha)$ be a number field defined by an irreducible polynomial $f(x) = x^{18} - m \in \mathbb{Z}[x]$. The following lemma plays a key role for proving Theorem 1.2. It allows the factorization of $p\,\mathbb{Z}_K = \prod_{i=1}^{t} \mathfrak{p}_i^{e_i}$ into primes ideals of $\mathbb{Z}_K$ for $p = 2, 3$. For every factor $\mathfrak{p}_i$, the residue degree f_i is given too.

Lemma 2.3.

(1) *If* $m \equiv 0 \pmod 2$, *then* $2\mathbb{Z}_K = \mathfrak{p}_{11}^{18}$, *with* $f_{11} = 1$.

(2) *If* $m \equiv 1 \pmod 2$, *then:*

  (a) *If* $m \equiv 3 \pmod 4$, *then* $2\mathbb{Z}_K = \mathfrak{p}_{11}^2\mathfrak{p}_{21}^2\mathfrak{p}_{31}^2$, *with* $f_{11} = 1$, $f_{21} = 2$ *and* $f_{31} = 6$.

  (b) *If* $m \equiv 5 \pmod 8$, *then* $2\mathbb{Z}_K = \mathfrak{p}_{11}\mathfrak{p}_{21}\mathfrak{p}_{22}\mathfrak{p}_{31}\mathfrak{p}_{32}$, *with* $f_{11} = f_{21} = f_{22} = 2$ *and* $f_{31} = f_{32} = 6$.

  (c) *If* $m \equiv 1 \pmod 8$, *then* $2\mathbb{Z}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}\mathfrak{p}_{21}\mathfrak{p}_{22}\mathfrak{p}_{31}\mathfrak{p}_{32}$, *with* $f_{11} = f_{12} = 1$, $f_{21} = f_{22} = 2$, *and* $f_{31} = f_{32} = 6$.

(3) *If* $m \equiv 1 \pmod 3$, *then:*

  (a) *If* $\nu_3(1-m) = 1$, *then* $3\mathbb{Z}_K = \mathfrak{p}_{11}^9\mathfrak{p}_{21}^9$, *where every prime factor is of residue degree* 1.

  (b) *If* $\nu_3(1-m) = 2$, *then* $3\mathbb{Z}_K = \mathfrak{p}_{11}^6\mathfrak{p}_{12}^3\mathfrak{p}_{21}^6\mathfrak{p}_{22}^3$, *where every prime factor is of residue degree* 1.

  (c) *If* $\nu_3(1-m) \geq 3$, *then* $3\mathbb{Z}_K = \mathfrak{p}_{11}^6\mathfrak{p}_{12}^2\mathfrak{p}_{13}\mathfrak{p}_{21}^6\mathfrak{p}_{22}^2\mathfrak{p}_{23}$, *where every prime factor is of residue degree* 1.

(4) *If* $m \equiv -1 \pmod 3$, *then:*

  (a) *If* $\nu_3(1+m) = 1$, *then* $3\mathbb{Z}_K = \mathfrak{p}_{11}^9$, *with residue degree* 2.

  (b) *If* $\nu_3(1+m) = 2$, *then* $3\mathbb{Z}_K = \mathfrak{p}_{11}^6\mathfrak{p}_{12}^3$, *with every prime factor is of residue degree* 2.

  (c) *If* $\nu_3(1+m) \geq 3$, *then* $3\mathbb{Z}_K = \mathfrak{p}_{11}^6\mathfrak{p}_{12}^2\mathfrak{p}_{13}$, *with every prime factor is of residue degree* 2.

Proof: (1) If $m \equiv 0 \pmod 2$, then $f(x) \equiv \varphi_1^{18} \pmod 2$, where $\varphi_1 = x$. As m is square free, $m \equiv 2 \pmod 4$, and so $N_{\varphi_1}^{+}(f) = S_{11}$ has a single side of degree 1.

Thus $f_{S_{11}}(y)$ is irreducible over $\mathbb{F}_{\varphi_1}$ and φ_1 yields a unique prime ideal $\mathfrak{p}_{11}$ with residue degree 1. Namely, $2\mathbb{Z}_K = \mathfrak{p}_{11}^{18}$.

(2) If $m \equiv 1 \pmod 2$, then $f(x) \equiv \varphi_1^2\varphi_2^2\varphi_3^2 \pmod 2$, where $\varphi_1 = x+1$, $\varphi_2 = x^2+x+1$, and $\varphi_3 = x^6+x^3+1$. Let $f(x) = \varphi_1^{18}+\cdots+153\varphi_1^2-18\varphi_1+1-m$, $f(x) = \varphi_2^9+\cdots-45x\varphi_2^2+(-6+6x)\varphi_2+(1-m)$, and $f(x) = \varphi_3^3-3x^3\varphi_3^2+(-2+2x^3)\varphi_3+(1-m)$ be the φ_1, φ_2, and φ_3-expansion, respectively. It follows that:

(a) If $m \equiv 3 \pmod 4$, then for every $i = 1,2,3$, $N_{\varphi_i}^+(f) = S_{i1}$ has a single side (because $\nu_2(1-m) = 1$), where $f_{S_{11}}(y)$, $f_{S_{21}}(y)$, and $f_{S_{31}}(y)$ are of degree 1. So, they are irreducible. Hence for every $i = 1,2,3$, φ_i yields a unique prime ideal $\mathfrak{p}_{i1}$ of $\mathbb{Z}_K$ lying above 2 with residue degree $\deg(\varphi_i)$. Namely, $2\mathbb{Z}_K = \mathfrak{p}_{11}^2\mathfrak{p}_{21}^2\mathfrak{p}_{31}^2$.

(b) If $m \equiv 5 \pmod 8$, then for every $i = 1,2,3$, $N_{\varphi_i}^+(f) = S_{i1}$ has a single side of degree 2, joining the points $(0,2),(1,1)$ and $(2,0)$, where $f_{S_{11}}(y) = y^2+y+1$ is irreducible over $\mathbb{F}_{\varphi_1} \simeq \mathbb{F}_2$, $f_{S_{21}}(y) = xy^2+(1+x)y+1 = x(y+1)(y+1+x)$ in $\mathbb{F}_{\varphi_2}[y]$, and $f_{S_{31}}(y) = x^3y^2+(1+x^3)y+1 = x^3(y+1)(y+x^3+1)$ in $\mathbb{F}_{\varphi_3}[y]$. Thus $2\mathbb{Z}_K = \mathfrak{p}_{11}\mathfrak{p}_{21}\mathfrak{p}_{22}\mathfrak{p}_{31}\mathfrak{p}_{32}$, with $f_{11} = f_{21} = f_{22} = 2$ and $f_{31} = f_{32} = 6$.

(c) If $m \equiv 1 \pmod 8$, then for every $i = 1,2,3$, $N_{\varphi_i}^+(f) = S_{i1}+S_{i2}$ has two sides of degree 2, joining the points $(0,\nu_2(1-m)),(1,1)$ and $(2,0)$ such that for every $i = 1,2,3$ and $j = 1,2$, $f_{S_{ij}}(y)$ is of degree 1. Thus $2\mathbb{Z}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}\mathfrak{p}_{21}\mathfrak{p}_{22}\mathfrak{p}_{31}\mathfrak{p}_{32}$, with $f_{11} = f_{12} = 1$, $f_{21} = f_{22} = 2$, and $f_{31} = f_{32} = 6$.

(3) For $p = 3$ and $m \equiv 1 \pmod 3$, $f(x) \equiv (x-1)^9(x+1)^9 \pmod 3$. Let $\varphi_1 = x-1$, $\varphi_2 = x+1$, $f(x) = \varphi_1^{18}+\cdots-48620\varphi_1^9+43758\varphi_1^8-31824\varphi_1^7+18564\varphi_1^6-8568\varphi_1^5+3060\varphi_1^4-816\varphi_1^3+153\varphi_1^2-18\varphi_1+1-m$, and $f(x) = \varphi_2^{18}+\cdots+48620\varphi_2^9+43758\varphi_2^8+31824\varphi_2^7+18564\varphi_2^6+8568\varphi_2^5+3060\varphi_2^4+816\varphi_2^3+153\varphi_2^2+18\varphi_2+1-m$ be the φ_1 and φ_2-expansion of $f(x)$. It follows that:

(a) If $\nu_3(1-m) = 1$, then for every $i = 1,2$, $N_{\varphi_i}^+(f) = S_{i1}$ with degree 1. Thus $3\mathbb{Z}_K = \mathfrak{p}_{11}^9\mathfrak{p}_{21}^9$, with every prime factor is of residue degree 1.

(b) If $\nu_3(1-m) = 2$, then for every $i = 1,2$, $N_{\varphi_i}^+(f) = S_{i1}+S_{i2}$ has two sides with the same degree 1, joining the points $(0,2),(3,1)$ and $(9,0)$. If $\mathfrak{p}_{ij}$ corresponds to S_{ij}, then write $3\mathbb{Z}_K = \mathfrak{p}_{11}^6\mathfrak{p}_{12}^3\mathfrak{p}_{21}^6\mathfrak{p}_{22}^3$, where every prime factor is of residue degree 1.

(c) If $\nu_3(1-m) \geq 3$, then for every $i = 1,2$, $N_{\varphi_i}^+(f) = S_{i1}+S_{i2}+S_{i3}$ has three sides with the same degree 1, joining the points $(0,\nu_3(m-1)),(1,2),(3,1)$, and $(9,0)$. Thus $3\mathbb{Z}_K = \mathfrak{p}_{11}^2\mathfrak{p}_{12}^2\mathfrak{p}_{13}\mathfrak{p}_{21}^2\mathfrak{p}_{22}^2\mathfrak{p}_{23}$, where every prime factor is of residue degree 1.

(4) Let $p = 3$ and $m \equiv -1 \pmod 3$, $f(x) \equiv (x^2+1)^9 \pmod 3$. Let $\varphi_1 = x^2+1$ and $f(x) = \varphi_1^9+\cdots+84\varphi_1^3-36\varphi_1^2+9\varphi_1-(1+m)$ be the φ_1-expansion of $f(x)$. It follows that:

(a) If $\nu_3(1+m) = 1$, then $N_{\varphi_1}^+(f) = S_{11}$ with degree 1. Thus $3\mathbb{Z}_K = \mathfrak{p}_{11}^9$, with residue degree 2.

(b) If $\nu_3(1+m)=2$, then $N^+_{\varphi_1}(f)=S_{11}+S_{12}$ has two sides with the same degree 1, joining the points $(0,2),(3,1)$, and $(9,0)$. Thus $3\mathbb{Z}_K=\mathfrak{p}_{11}^6\mathfrak{p}_{12}^3$, where every prime factor is of residue degree 2.

(c) If $\nu_3(1+m)\geq 3$, then $N^+_{\varphi_1}(f)=S_{11}+S_{12}+S_{13}$ has three sides with the same degree 1, joining the points $(0,\nu_3(m+1)),(1,2),(3,1)$, and $(9,0)$. Thus $3\mathbb{Z}_K=\mathfrak{p}_{11}^6\mathfrak{p}_{12}^2\mathfrak{p}_{13}$, where every prime factor is of residue degree 2. □

Proof of Theorem 1.1: Since the discriminant of $f(x)$ is $\triangle(f)=\mp 18^{18}m^{17}$, thanks to the well known formula $\nu_p(d_K)=\nu_p(\triangle(f))-2\nu_p(\mathrm{ind}(\alpha))$, in order to prove that $\mathbb{Z}_K=\mathbb{Z}[\alpha]$ under the hypothesis of Theorem 1.1, we need only to show that p does not divide the index $(\mathbb{Z}_K:\mathbb{Z}[\alpha])$ for every prime integer dividing $6\cdot m$. Let p be a prime integer dividing $6\cdot m$.

(1) Assume that p divides m. In this case $\overline{f(x)}=\varphi^{18}$ in $\mathbb{F}_p[x]$, where $\varphi=x$. As $\nu_p(m)=1$, $N_\varphi(f)=S$ has a single side of height 1, by Corollary 2.2, we get $\nu_p(\mathrm{ind}(f))=0$; p does not divide $(\mathbb{Z}_K:\mathbb{Z}[\alpha])$.

(2) Assume that $p=2$ and 2 does not divide m. Then $f(x)\equiv\varphi_1^2\varphi_2^2\varphi_3^2 \pmod 2$, where $\varphi_1=x+1$, $\varphi_2=x^2+x+1$, and $\varphi_3=x^6+x^3+1$. Let $f(x)=\varphi_1^{18}+\cdots+153\varphi_1^2-18\varphi_1+1-m$, $f(x)=\varphi_2^9+\cdots-45x\varphi_2^2+(-6+6x)\varphi_2+(1-m)$, and $f(x)=\varphi_3^3-3x^3\varphi_3^2+(-2+2x^3)\varphi_3+(1-m)$ be the φ_1, φ_2, and φ_3-expansion of $f(x)$, respectively. It follows that if $m\equiv 3 \pmod 4$, then $\nu_2(1-m)=1$ and for every $i=1,2,3$, $N^+_{\varphi_i}(f)=S_i$ has a single side of height 1. Thus, by Corollary 2.2, $\nu_2(\mathrm{ind}(f))=0$, and 2 does not divide $(\mathbb{Z}_K:\mathbb{Z}[\alpha])$.

(3) Assume that $p=3$ and 3 does not divide m. Then $\overline{f(x)}=(x^6-m)^3$ in $\mathbb{F}_3[x]$.

In the first case $m\equiv 1 \pmod 3$, $f(x)\equiv(x-1)^9(x+1)^9 \pmod 3$. Let $\varphi_1=x+1$, $\varphi_2=x-1$, $f(x)=\varphi_1^{18}+\cdots-48620\varphi_1^9+43758\varphi_1^8-31824\varphi_1^7+18564\varphi_1^6-8568\varphi_1^5+3060\varphi_1^4-816\varphi_1^3+153\varphi_1^2-18\varphi_1+1-m$, and $f(x)=\varphi_2^{18}+\cdots+48620\varphi_2^9+43758\varphi_2^8+31824\varphi_2^7+18564\varphi_2^6+8568\varphi_2^5+3060\varphi_2^4+816\varphi_2^3+153\varphi_2^2+18\varphi_2+1-m$ be the φ_1 and φ_2-expansion of $f(x)$. It follows that if $m\not\equiv 1 \pmod 9$, then $\nu_3(1-m)=1$ and therefore, $N_{\varphi_i}(f)=S_i$ has a single side of height 1. Thus, by Corollary 2.2, $\nu_3(\mathrm{ind}(f))=0$, and 3 does not divide $(\mathbb{Z}_K:\mathbb{Z}[\alpha])$.

For $p=3$ and $m\equiv -1 \pmod 3$, $f(x)\equiv(x^2+1)^9 \pmod 3$. Let $\varphi_1=x^2+1$ and $f(x)=\varphi_1^9+\cdots+84\varphi_1^3-36\varphi_1^2+9\varphi_1-(1+m)$ be the φ_1-expansion of $f(x)$. If $m\not\equiv -1 \pmod 9$, then $\nu_3(1+m)=1$ and $N^+_{\varphi_1}(f)=S_1$ has a single side of height 1. So, by Corollary 2.2, $\nu_3(\mathrm{ind}(f))=0$, and 3 does not divide $(\mathbb{Z}_K:\mathbb{Z}[\alpha])$. □

Proof of Theorem 1.2: In every case, we will show the non monogenity of $\mathbb{Z}_K$. The idea is that if there exists $\theta\in\mathbb{Z}_K$ which generates a power integral basis of $\mathbb{Z}_K$, then p does not divide the index $(\mathbb{Z}_K:\mathbb{Z}[\theta])$. In this case, by applying Kummer's theorem, the factorization of $p\mathbb{Z}_K$ is p-analogous to the factorization of $\overline{F}(x)$ modulo p, where $F(x)$ is the minimal polynomial of θ over $\mathbb{Q}$. More precisely, $p\,\mathbb{Z}_K = \prod_{k=1}^{r} \mathfrak{p}_i^{e_i}$, where $\overline{F}(x) = \prod_{k=1}^{r} \overline{g_i^{e_i}}(x)$ is the factorization of $\overline{F}(x)$ into powers of monic irreducible polynomials of $\mathbb{F}_p[x]$.

(1) Assume that $m \equiv 1 \pmod 4$. By Lemma 2.3, the factorization of $2\mathbb{Z}_K$ contains at least 2 distinct prime ideal factors with residue degree 2 each one. So, if Dedekind's theorem is applied, then in $\mathbb{F}_2[x]$, there are at least 2 monic irreducible polynomials of degree 2 each one. That is a contradiction because there is only a unique monic irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, namely $x^2 + x + 1$.

(2) Similarly, if $m \equiv 1 \pmod 9$, then by Lemma 2.3, the factorization of $3\mathbb{Z}_K$ contains four distinct prime ideal factors with residue degree 1 each one, which is a contradiction because there is only three monic irreducible polynomials of degree 1 in $\mathbb{F}_3[x]$. □

Remark. In the proof of Lemma 2.3 for the calculations of the φ-expansions of $f(x)$, we used Maple 12.

Acknowledgement. The author is deeply grateful to the anonymous referee whose valuable comments and suggestions have tremendously improved the quality of this paper. As well as for Professor Enric Nart who introduced him to Newton polygon's techniques.

References

[1] Ahmad S., Nakahara T., Hameed A., *On certain pure sextic fields related to a problem of Hasse*, Int. J. Algebra Comput. **26** (2016), no. 3, 577–583.

[2] Ahmad S., Nakahara T., Husnine S. M., *Power integral bases for certain pure sextic fields*, Int. J. Number Theory **10** (2014), no. 8, 2257–2265.

[3] El Fadil L., *Computation of a power integral basis of a pure cubic number field*, Int. J. Contemp. Math. Sci. **2** (2007), no. 13–16, 601–606.

[4] El Fadil L., *On Newton polygons techniques and factorization of polynomials over Henselian fields*, J. Algebra Appl. **19** (2020), no. 10, 2050188, 9 pages.

[5] El Fadil L., *On power integral bases for certain pure number fields defined by $x^{24} - m$*, Studia Sci. Math. Hungar. **57** (2020), no. 3, 397–407.

[6] El Fadil L., *On power integral bases for certain pure number fields*, Publ. Math. Debrecen **100** (2022), no. 1–2, 219–231.

[7] El Fadil L., Montes J., Nart E., *Newton polygons and p-integral bases of quartic number fields*, J. Algebra Appl. **11** (2012), no. 4, 1250073, 33 pages.

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

[9] Gaál I., *Power integral bases in algebraic number fields*, Ann. Univ. Sci. Budapest. Sect. Comput. **18** (1999), 61–87.

[10] Gaál I., *Diophantine Equations and Power Integral Bases*, Theory and Algorithm, Birkhäuser/Springer, Cham, 2019.

[11] Gaál I., Olajos P., Pohst M., *Power integral bases in orders of composite fields*, Experiment. Math. **11** (2002), no. 1, 87–90.

[12] Gaál I., Remete L., *Binomial Thue equations and power integral bases in pure quartic fields*, J. Algebra Number Theory Appl. **32** (2014), no. 1, 49–61.

[13] Gaál I., Remete L., *Integral bases and monogenity of pure fields*, J. Number Theory **173** (2017), 129–146.

[14] Hameed A., Nakahara T., *Integral bases and relative monogenity of pure octic fields*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **58(106)** (2015), no. 4, 419–433.

[15] Ore Ö., *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), no. 1, 84–117 (German).

[16] Pethő A., Pohst M., *On the indices of multiquadratic number fields*, Acta Arith. **153** (2012), no. 4, 393–414.

L. El Fadil:
Faculty of Sciences Dhar El Mahraz,
Sidi Mohamed Ben Abdellah University,
P. O. Box 1874, Fès-Atlas, 30000 Fès, Morocco

E-mail: lhouelfadil2@gmail.com

(*Received* November 10, 2020, *revised* April 14, 2021)