sciendo

Tatra Mountains
Mathematical Publications
DOI: 10.2478/tmmp-2023-0006
Tatra Mt. Math. Publ. **83** (2023), 61–86

INTEGRAL BASES AND MONOGENITY OF PURE NUMBER FIELDS WITH NON-SQUARE FREE PARAMETERS UP TO DEGREE 9

Lhoussain El Fadil[1] — István Gaál[2]

[1]Faculty of Sciences Dhar El Mahraz, Sidi Mohamed ben Abdellah University, Atlas-Fez, MOROCCO

[2]Institute of Mathematics, University of Debrecen, Debrecen, HUNGARY

ABSTRACT. Let K be a pure number field generated by a root α of a monic irreducible polynomial $f(x) = x^n - m$ with m a rational integer and $3 \le n \le 9$ an integer. In this paper, we calculate an integral basis of $\mathbb{Z}_K$, and we study the monogenity of K, extending former results to the case when m is not necessarily square-free. Collecting and completing the corresponding results in this more general case, our purpose is to provide a parallel to [Gaál, I.—Remete, L.: *Power integral bases and monogenity of pure fields*, J. Number Theory, **173** (2017), 129–146], where only square-free values of m were considered.

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 an integral basis of type $(1, \alpha, \ldots, \alpha^{n-1})$ with some $\alpha \in \mathbb{Z}_K$. Monogenity of number fields is a classical problem of algebraic number theory, going back to Dedekind, Hasse and Hensel, cf., e.g., [22, 23] and [17] 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 [22,23, 26].

2020 Mathematics Subject Classification: 11R04,11R16, 11R21.
Keywords: integral bases, power integral basis, index, theorem of Ore, Newton polygon.

For any primitive element α of $\mathbb{Z}_K$ (that is $\alpha \in \mathbb{Z}_K$ with $K = \mathbb{Q}(\alpha)$) we denote by

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

the *index of* α, that is the index of the $\mathbb{Z}$-module $\mathbb{Z}[\alpha]$ in the free-$\mathbb{Z}$-module $\mathbb{Z}_K$ of rank n. As it is known [17], we have

$$\triangle(\alpha) = \operatorname{ind}(\alpha)^2 \cdot d_K,$$

where $\triangle(\alpha)$ is the discriminant of α.

Let $(1, \omega_1, \dots, \omega_{n-1})$ be an integral basis of $\mathbb{Z}_K$. The discriminant

$$\triangle\big(L(X_1, \dots, X_n)\big)$$

of the linear form

$$L(X_1, \dots, X_{n-1}) = \omega_1 X_1 + \dots + \omega_{n-1} X_{n-1}$$

can be written (cf. [17]) as

$$\triangle\big(L(X_1, \dots, X_{n-1})\big) = \big(\operatorname{ind}(X_1, \dots, X_{n-1})\big)^2 \cdot d_K,$$

where $\operatorname{ind}(X_1, \dots, X_{n-1})$ is the *index form* corresponding to the integral basis $(1, \omega_1, \dots, \omega_{n-1})$ having the property that for any

$$\alpha = x_0 + \omega_1 x_1 + \dots + \omega_{n-1} x_{n-1} \in \mathbb{Z}_K \quad (\text{with} \quad x_0, x_1, \dots, x_{n-1} \in \mathbb{Z})$$

we have $\operatorname{ind}(\alpha) = |\operatorname{ind}(x_1, \dots, x_{n-1})|$.

Obviously, $\operatorname{ind}(\alpha) = 1$ if and only if $(1, \alpha, \dots, \alpha^{n-1})$ is an integral basis of $\mathbb{Z}_K$. Therefore α is a *generator of a power integral basis* if and only if $x_1, \dots, x_{n-1} \in \mathbb{Z}$ is a solution of the *index form equation*

$$\operatorname{ind}\big(x_1, \dots, x_{n-1}\big) = \pm 1 \ \text{ in } \ x_1, \dots, x_{n-1} \in \mathbb{Z}.$$

If $f \in \mathbb{Z}[x]$ is a monic irreducible polynomial having α as a root, then

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

is called the *index of the polynomial* f, where K is the number field generated by α. Analogously,

$$\triangle(f) = \operatorname{ind}(f)^2 \cdot d_K$$

$\triangle(f)$ denoting the discriminant of f.

Throughout the paper $\nu_p(a)$ denoted the p-exponent of the rational integer a.

The problem of testing the monogenity of number fields and constructing power integral bases have been intensively studied during the last decades, see for instance [2, 18, 29].

An especially delicate and intensively studied problem is the monogenity of *pure fields* K generated by a root α of an irreducible polynomial $x^n - m$. In all former results it was assumed that $m \neq \pm 1$ is a square-free integer.

Funakura [16] studied the integral basis in pure quartic fields. Gaál and Remete [19] calculated the elements of index 1 (that is generators of power integral bases), with coefficients of absolute value $< 10^{1000}$ in an integral basis, of pure quartic fields generated by $m^{\frac{1}{4}}$ for $1 < m < 10^7$ and $m \equiv 2, 3 \pmod 4$. Ahmad, Nakahara, and Husnine [1] proved that if $m \equiv 2, 3 \pmod 4$ and $m \not\equiv \mp 1 \pmod 9$, then the sextic number field generated by $m^{\frac{1}{6}}$ is monogenic. They also showed [2] that if $m \equiv 1 \pmod 4$ and $m \not\equiv \mp 1 \pmod 9$, then the sextic number field generated by $m^{\frac{1}{6}}$ is not monogenic. Based on prime ideal factorization, El Fadil [11] 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 [5], 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. Applying the explicit form of the index forms, Gaál and Remete [20] obtained new results on monogenity of the number fields generated by $m^{\frac{1}{n}}$, where $3 \leq n \leq 9$. While Gaál's and Remete's techniques are based on determining elements of index 1, El Fadil used a new method based on Newton polygons to study the monogenity of some pure fields.

In this paper, we calculate an integral basis and we study the monogenity of pure fields K for degrees $3 \leq n \leq 9$, *without assuming that m is square-free.* In this way, our results generalize those given in [1, 2, 5, 11, 16, 20]. For $n = 6, 8$, we shall refer to the results of El Fadil [12] and El Fadil and Gaál [14] where pure sextic resp. pure octic fields were studied without assuming that m is square-free.

2. Pure cubic fields

In this section, K is a pure cubic number field generated by $\alpha = m^{\frac{1}{3}}$ with $m = a_1 a_2^2$, a_1 and a_2 two coprime square free integers and $m \neq \pm 1$. The following theorem allows the calculation of an integral basis of $\mathbb{Z}_K$ (cf. also Alaca [3], El Fadil [9]).

Theorem 2.1.

(1) *If* $m \not\equiv \pm 1 \pmod 9$, *then* $(1, \alpha, \frac{\alpha^2}{a_2})$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$.

(2) *If* $m \equiv \pm 1 \pmod 9$, *then* $(1, \alpha, \frac{\alpha^2 + m\alpha + m^2}{3a_2})$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$.

Based on these integral bases we have

Corollary 2.2. $\mathbb{Z}[\alpha]$ *is the ring of integers of* K *if and only if* $m \not\equiv \pm 1 \pmod 9$ *and* m *is a square free integer.*

For pure cubic number fields, the explicit form of the index form is obtained by direct calculations:

Lemma 2.3. *Let* $x_0, x_1, x_2 \in \mathbb{Z}$.

(1) *If* $m \not\equiv \pm 1 \pmod 9$, *then for any* $\theta = x_0 + x_1\alpha + \frac{x_2\alpha^2}{a_2} \in \mathbb{Z}_K$ *we have*

$$\operatorname{ind}(\theta) = \left|a_2 x_1^3 - a_1 x_2^3\right|.$$

In particular, if m *is a square free integer, then*

$$\operatorname{ind}(\theta) = \left|x_1^3 - m x_2^3\right|.$$

(2) *If* $m \equiv \pm 1 \pmod 9$, *then for any* $\theta = x_0 + x_1\alpha + x_2\frac{\alpha^2+m\alpha+m^2}{3a_2} \in \mathbb{Z}_K$ *we have*

$$\operatorname{ind}(\theta) = \left|3a_2x_1^3 + (2m+1)x_1^2x_2 + ma_1a_2x_1x_2^2 - a_1\frac{1-m^2}{9}x_2^3\right|.$$

In particular, if m *is a square free integer, then*

$$\operatorname{ind}(\theta) = \left|3x_1^3 + (2m+1)x_1^2x_2 + m^2x_1x_2^2 - m\frac{1-m^2}{9}x_2^3\right|.$$

As a special case, we have

Corollary 2.4. *Assume that* $m = a^2$ *with* $a \neq \pm 1$ *a square free integer. Then if* $a \not\equiv \pm 1 \pmod 9$, *then* K *is monogenic.*

Remark.

(1) If $a \equiv 1 \pmod 9$, then let $a = 1 + 9k$ for some integer k. Based on the results given in [20], the index form equation is solvable for $k = 27, 37$, but not solvable for $k = 10, 11, 12$.

(2) If $a \equiv -1 \pmod 9$, then let $a = -1 + 9k$ for some integer k. Based on the results given in [20], the index form equation is solvable for $k = 1, 4, 12$, but not solvable for $k = 2, 3, 5, 6, 7$.

3. Pure quartic fields

In this section, K is a pure quartic number field generated by $\alpha = m^{\frac{1}{4}}$, with $m = a_1a_2^2a_3^3$, a_1, a_2, and a_3 pairwise coprime square free integers and $m \neq \pm 1$. Let $A_1 = 1$, $A_2 = a_2a_3$, and $A_3 = a_2a_3^2$. The following theorem explicitly gives an integral basis of $\mathbb{Z}_K$ (cf. also Alaca and Williams [4]).

Theorem 3.1.

(1) *If* $\nu_2(m)$ *is odd or* $\nu_2(m-1) = 1$, *then* $(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3})$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$.

(2) *If* $m \equiv 4 \pmod{16}$, *then* $(1, \alpha, \frac{\alpha^2+A_2}{2A_2}, \frac{\alpha^3+A_2\alpha}{2A_3})$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$.

(3) *If* $m \equiv 12 \pmod{32}$, *then* $(1, \alpha, \frac{\alpha^2+A_2\alpha-A_2}{2A_2}, \frac{\alpha^3+A_3\alpha^2-A_3\alpha}{2A_3})$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$.

(4) *If* $m \equiv 28 \pmod{32}$, *then* $(1, \alpha, \frac{\alpha^2+A_2\alpha+A_2}{2A_2}, \frac{\alpha^3+A_3\alpha^2+A_3\alpha}{4A_3})$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$.

(5) *If* $m \equiv 5 \pmod 8$, *then* $(1, \alpha, \frac{\alpha^2+m}{2A_2}, \frac{\alpha^3+m\alpha^2+m\alpha+m}{2A_3})$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$.

(6) *If* $m \equiv 1 \pmod 8$, *then* $(1, \alpha, \frac{\alpha^2+m}{2A_2}, \frac{\alpha^3+m\alpha^2+m\alpha+m}{4A_3})$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$.

Based on these integral bases we have:

Corollary 3.2. *$\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if $m \neq \pm 1$ is a square free integer and $m \not\equiv 1 \pmod 4$.*

Also for pure quartic number fields, the explicit form of the index form can be obtained by direct calculations. For brevity we only give it in case (1).

Lemma 3.3. *Let $x_0, x_1, x_2, x_3 \in \mathbb{Z}$. If $\nu_2(m)$ is odd or $\nu_2(m-1)=1$, then for any*

$$\theta = x_0 + x_1\alpha + \frac{x_2\alpha^2}{A_2} + \frac{x_3\alpha^3}{A_3}$$

we have

$$\begin{aligned}\operatorname{ind}(\theta) = \big|&(a_3x_1^2 - a_1x_3^2)\\ &\times \big((a_2a_3)^2x_1^4 + 2a_1a_2^2a_3x_1^2x_3^2 + 4a_1a_3x_2^4\\ &-8a_1a_2a_3x_1x_2^2x_3 + (a_1a_2)^2x_3^4\big)\big|.\end{aligned}$$

As a special case, we have

Corollary 3.4. *Assume that $m = a^u$ with $a \neq \pm 1$ a square free integer and $u \in \{1, 3\}$ a positive integer. Then*

(1) *If* $a \not\equiv 1 \pmod 4$, *then K is monogenic.*

(2) *If* $a \not\equiv 1 \pmod{16}$, *then K is not monogenic.*

Remark. Based on the results given in [20], if $a \equiv 1 \pmod 4$, then K is monogenic for $a \in \{-3, 73, 89\}$.

Remark. Similarly to the case (1) in Lemma 3.3 the index form in pure quartic fields is a product of a quadratic factor F_2 and a quartic factor F_4 in all cases. Eliminating x_1^4 from a linear combination of F_2^2 and F_4 we obtain a divisibility relation which is a necessary condition for the monogenity of pure quartic fields.

Corollary 3.5. *The following are the necessary conditions for monogenity of pure quartic number fields:*

(1) *If $\nu_2(m)$ is odd or $\nu_2(m-1) = 1$, then $4a_1a_3$ divides $(a_2^2 \pm 1)$.*

(2) *If* $m \equiv 4 \pmod{16}$*, then* a_1a_3 *divides* $(4a_2^2 \pm 1)$*.*

(3) *If* $m \equiv 12 \pmod{32}$*, then* $4a_1a_3$ *divides* $(a_2^2 \pm 16)$*.*

(4) *If* $m \equiv 28 \pmod{32}$*, then* a_1a_3 *divides* $(a_2^2 \pm 64)$*.*

(5) *If* $m \equiv 5 \pmod{8}$*, then* a_1a_3 *divides* $(4a_2^2 \pm 1)$*.*

(6) *If* $m \equiv 1 \pmod{8}$*, then* a_1a_3 *divides* $(a_2^2 \pm 1)$*.*

4. Pure quintic fields

In this section, K is a pure quintic number field generated by $\alpha = m^{\frac{1}{5}}$, where $m \in \mathbb{Z}$ is not necessarily a square free integer and $m \neq \pm 1$. It is well known that we can assume that $\nu_p(m) \leq 4$ for every prime integer p, and so $m = a_1a_2^2a_3^3a_4^4$, where $a_1, \dots, a_4$ are pairwise coprime square-free integers. Let $A_1 = 1$, $A_2 = a_3a_4$, $A_3 = a_2a_3a_4^2$, and $A_4 = a_2a_3^2a_4^3$. The following theorem explicitly gives an integral basis of $\mathbb{Z}_K$ (cf. also El Fadil [10]). For every positive integer n and for every integer x, the notation $\overline{m} = \overline{x} \pmod{n}$ means that $m \equiv x \pmod{n}$.

Theorem 4.1.

(1) *If* $\overline{m} \notin \{\overline{1}, \overline{7}, \overline{18}, \overline{24}\} \pmod{25}$*, then* $\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}\right)$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$*.*

(2) *If* $\overline{m} \in \{\overline{1}, \overline{7}, \overline{18}, \overline{24}\} \pmod{25}$*, then* $\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{(\alpha - m)^4}{5A_4}\right)$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$*.*

Based on these integral bases we have:

Corollary 4.2. $\mathbb{Z}[\alpha]$ *is the ring of integers of* K *if and only if* $m \neq \pm 1$ *is a square free integer and* $\overline{m} \notin \{\overline{1}, \overline{7}, \overline{18}, \overline{24}\} \pmod{25}$*.*

The index form can be directly calculated, for brevity we give it in case (1) only.

Lemma 4.3. *Let* $x_0, x_1, x_2, x_3, x_4 \in \mathbb{Z}$*. If* $\overline{m} \notin \{\overline{1}, \overline{7}, \overline{18}, \overline{24}\} \pmod{25}$*, then for any*

$$\theta = x_0 + x_1\alpha + \frac{x_2\alpha^2}{A_2} + \frac{x_3\alpha^3}{A_3} + \frac{x_4\alpha^4}{A_4}$$

we have

$$
\begin{aligned}
\operatorname{ind}(\theta) = \Big| & 11a_1^4a_2^5a_3a_4^2x_2^5x_4^5 && - 11a_1^5a_2^2a_3^4a_4x_3^5x_4^5\\
& - 2a_1^3a_2^3a_3^3a_4^3x_1^5x_4^5 && - a_1^4a_3^6a_4^2x_3^{10}\\
& - a_1^2a_2^6a_4^4x_2^{10} && + 11a_1^2a_2a_3^5a_4^4x_1^5x_3^5\\
& + a_2^2a_3^4a_4^6x_1^{10} && - 11a_1a_2^4a_3^2a_4^5x_1^5x_2^5\\
& + x_4^{10}a_2^4a_3^2a_1^6 && - 20a_1^5a_2^4a_3^2a_4x_2^2x_3x_4^7\\
& + 5a_1^5a_2^4a_3^2a_4x_1x_2x_4^8 && + 35a_1^5a_2^3a_3^3a_4x_2x_3^3x_4^6\\
& - 15a_1^5a_2^3a_3^3a_4x_1x_3^2x_4^7 && - 5a_1^4a_2^3a_3^3a_4^2x_1^3x_3x_4^6\\
& + 2a_1^3a_2^3a_3^3a_4^3x_2^5x_3^5 && + 20a_1^4a_2a_3^5a_4^2x_1x_3^7x_4^2\\
& - 75a_1^4a_2^3a_3^3a_4^2x_1x_2^2x_3^3x_4^4 && + 45a_1^4a_2^3a_3^3a_4^2x_1^2x_2x_3^2x_4^5\\
& + 40a_1^4a_2^4a_3^2a_4^2x_1x_2^3x_3x_4^5 && - 40a_1^4a_2^2a_3^4a_4^2x_1x_2x_3^5x_4^3\\
& - 75a_1^2a_2^3a_3^3a_4^4x_1^4x_2^3x_3^2x_4 && - 40a_1^2a_2^4a_3^2a_4^4x_1^3x_2^5x_3x_4\\
& + 45a_1^2a_2^3a_3^3a_4^4x_1^5x_2^2x_3x_4^2 && + 40a_1^2a_2^2a_3^4a_4^4x_1^5x_2x_3^3x_4\\
& + 75a_1^3a_2^2a_3^4a_4^3x_1^3x_2x_3^4x_4^2 && + 75a_1^3a_2^4a_3^2a_4^3x_1^2x_2^4x_3x_4^3\\
& + 50a_1^3a_2^3a_3^3a_4^3x_1^4x_2x_3x_4^4 && - 200a_1^3a_2^3a_3^3a_4^3x_1^3x_2^2x_3^2x_4^3\\
& + 200a_1^3a_2^3a_3^3a_4^3x_1^2x_2^3x_3^3x_4^2 && - 45a_1^3a_2^2a_3^4a_4^3x_1^2x_2^2x_3^5x_4\\
& - 45a_1^3a_2^4a_3^2a_4^3x_1x_2^5x_3^2x_4^2 && - 50a_1^3a_2^3a_3^3a_4^3x_1x_2^4x_3^4x_4\\
& + 25a_1^4a_2^2a_3^4a_4^2x_1^2x_3^4x_4^4 && - 25a_1^4a_2^4a_3^2a_4^2x_2^4x_3^2x_4^4\\
& + 25a_1^4a_2^3a_3^3a_4^2x_2^3x_3^4x_4^3 && - 5a_1^4a_2a_3^5a_4^2x_2x_3^8x_4\\
& - 10a_1^4a_2^4a_3^2a_4^2x_1^2x_2^2x_4^6 && + 10a_1^4a_2^2a_3^4a_4^2x_2^2x_3^6x_4^2\\
& - 15a_1a_2^3a_3^3a_4^5x_1^7x_2^2x_4 && - 20a_1a_2^2a_3^4a_4^5x_1^7x_2x_3^2\\
& + 5a_1a_2^2a_3^4a_4^5x_1^8x_3x_4 && + 35a_1a_2^3a_3^3a_4^5x_1^6x_2^3x_3\\
& + 20a_1^2a_2^5a_3a_4^4x_1^2x_2^7x_4 && - 5a_1^2a_2^3a_3^3a_4^4x_1^6x_2x_4^3\\
& + 25a_1^2a_2^4a_3^2a_4^4x_1^4x_2^4x_4^2 && - 25a_1^2a_2^2a_3^4a_4^4x_1^4x_2^2x_3^4\\
& + 25a_1^2a_2^3a_3^3a_4^4x_1^3x_2^4x_3^3 && - 5a_1^2a_2^5a_3a_4^4x_1x_2^8x_3\\
& - 10a_1^2a_2^2a_3^4a_4^4x_1^6x_3^2x_4^2 && + 10a_1^2a_2^4a_3^2a_4^4x_1^2x_2^6x_3^2\\
& - 35a_1^3a_2a_3^5a_4^3x_1^3x_3^6x_4 && + 15a_1^3a_2a_3^5a_4^3x_1^2x_2x_3^7\\
& - 35a_1^3a_2^5a_3a_4^3x_1x_2^6x_4^3 && + 5a_1^3a_2^2a_3^4a_4^3x_1x_2^3x_3^6\\
& + 15a_1^3a_2^5a_3a_4^3x_2^7x_3x_4^2 && + 5a_1^3a_2^4a_3^2a_4^3x_2^6x_3^3x_4\\
& - 25a_1^3a_2^2a_3^4a_4^3x_1^4x_3^3x_4^3 && - 25a_1^3a_2^4a_3^2a_4^3x_1^3x_2^3x_4^4\Big|.
\end{aligned}
$$

We also prove the following statement

Corollary 4.4. *Assume that* $m = a^u$ *with* $a \neq \pm 1$ *a square free integer and* $1 \leq u \leq 4$ *a positive integer. Then*

(1) *If* $\overline{a} \notin \{\overline{1}, \overline{7}, \overline{18}, \overline{24}\} \pmod{25}$*, then* K *is monogenic.*

(2) *If* $\overline{a} \in \{\overline{1}, \overline{7}, \overline{18}, \overline{24}\} \pmod{25}$*, then* K *is not monogenic with the exception of* $a = 7$*, in which case* K *is monogenic.*

5. Pure sextic fields

In this section, K is a pure sextic number field generated by $\alpha = m^{\frac{1}{6}}$, with $m = a_1 a_2^2 a_3^3 a_4^4 a_5^5$, where a_1, a_2, a_3, a_4, and a_5 are pairwise coprime square free integers and $m \neq \pm 1$. Let

$$A_1 = 1, \qquad A_2 = a_3 a_4 a_5\,,$$
$$A_3 = a_2 a_3 a_4^2 a_5^2\,, \quad A_4 = a_2 a_3^2 a_4^2 a_5^3\,,$$

and

$$A_5 = a_2 a_3^2 a_4^3 a_5^4.$$

A detailed table of integral bases is given in [12] that we do not repeat here. Based on these integral bases we have:

Corollary 5.1. $\mathbb{Z}[\alpha]$ *is the ring of integers of* K *if and only if* $m \neq \pm 1$ *is a square free integer,* $m \not\equiv 1 \pmod 4$*, and* $m \not\equiv \pm 1 \pmod 9$*.*

The index form can be directly calculated, for brevity we only give it explicitly in case the integral basis $(1, \alpha, \alpha^2/A_2, \alpha^3/A_3, \alpha^4/A_4, \alpha^5/A_5)$ is valid.

Lemma 5.2. *Assume that* 6 *divides* m*,* $\nu_2(m)$ *is odd, and* $\nu_3(m) \neq 3$*. Let* $(x_0, x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^6$*. Then for any*

$$\theta = x_0 + x_1\alpha + x_2\frac{\alpha^2}{A_2} + x_3\frac{\alpha^3}{A_3} + x_4\frac{\alpha^4}{A_4} + x_5\frac{\alpha^5}{A_5}$$

we have

$$\mathrm{ind}(\theta) = |G_1 \cdot G_2 \cdot G_3|$$

with sextic factors G_1*,* G_3 *and a cubic factor* G_2*, where*

$$
\begin{aligned}
G_1 = {} & a_2^2a_3^3a_4^4a_5^4x_1^6 && - 216a_1^2a_2^3a_3a_4^2a_5^2x_2^3x_3x_4x_5 \\
& - 72a_1a_2^2a_3^2a_4^3a_5^3x_1^3x_2x_3x_4 && - 216a_1^2a_2^2a_3a_4^3a_5^2x_1x_2x_3x_4^3 \\
& - 54a_1^2a_2^3a_3^2a_4^3a_5^2x_1^2x_2x_4x_5^2 && - 72a_1^3a_2^3a_3^2a_4^2a_5x_2x_3x_4x_5^3 \\
& + 27a_1^3a_2^2a_4^4a_5x_4^6 && + 162a_1^2a_2^3a_3a_4^3a_5^2x_1x_2^2x_4^2x_5 \\
& + a_1^4a_2^2a_3^3a_4^2x_5^6 && + 27a_1a_2^4a_4^2a_5^3x_2^6 \\
& + 9a_1^3a_2^4a_3^2a_4^2a_5x_2^2x_5^4 && + 9a_1a_2^2a_3^2a_4^4a_5^3x_1^4x_4^2 \\
& - 96a_1^2a_2a_3^3a_4a_5^2x_1x_3^4x_5 && + 144a_1^2a_2a_3^2a_4^2a_5^2x_1x_3^3x_4^2 \\
& - 288a_1^2a_2a_3^2a_4a_5^2x_2x_3^4x_4 && + 12a_1^3a_2^3a_3^3a_4^2a_5x_1x_3x_5^4 \\
& + 36a_1^2a_2^2a_3^3a_4^2a_5^2x_1^2x_3^2x_5^2 && - 108a_1^3a_2^2a_3a_4^3a_5x_3x_4^4x_5 \\
& + 54a_1^3a_2^3a_3a_4^3a_5x_2x_4^3x_5^2 && - 18a_1^3a_2^3a_3^2a_4^3a_5x_1x_4^2x_5^3 \\
& + 108a_1a_2^2a_3^2a_4^2a_5^3x_1^2x_2^2x_3^2 && + 108a_1^3a_2^2a_3^2a_4^2a_5x_3^2x_4^2x_5^2 \\
& + 54a_1a_2^3a_3a_4^3a_5^3x_1^2x_2^3x_4 && - 18a_1a_2^3a_3^2a_4^3a_5^3x_1^3x_2^2x_5 \\
& + 12a_1a_2^2a_3^3a_4^3a_5^3x_1^4x_3x_5 && - 108a_1a_2^3a_3a_4^2a_5^3x_1x_2^4x_3 \\
& + 2a_1^2a_2^3a_3^3a_4^3a_5^2x_1^3x_5^3 && + 27a_1^2a_2^2a_3a_4^4a_5^2x_1^2x_4^4 \\
& - 54a_1^2a_2^3a_4^3a_5^2x_2^3x_4^3 && + 27a_1^2a_2^4a_3a_4^2a_5^2x_2^4x_5^2 \\
& - 16a_1a_2a_3^3a_4^2a_5^3x_1^3x_3^3 && - 16a_1^3a_2^2a_3^3a_4a_5x_3^3x_5^3 \\
& + 64a_1^2a_2^3a_3^3a_5^2x_3^6 && + 144a_1^2a_2^2a_3^2a_4a_5^2x_2^2x_3^3x_5 \\
& + 324a_1^2a_2^2a_3a_4^2a_5^2x_2^2x_3^2x_4^2,
\end{aligned} \tag{1}
$$

$$
\begin{aligned}
G_2 = {} & - 3a_1a_2a_4a_5x_1x_3x_5 && + a_2a_4^2a_5^2x_1^3 \\
& + a_1a_5x_3^3 && + a_1^2a_2^2a_4x_5^3,
\end{aligned} \tag{2}
$$

$$
\begin{aligned}
G_3 = {} & 18a_1^2a_2a_3^2a_4a_5^2x_1^2x_2x_4x_5^2 && - 18a_1^2a_2a_3a_4a_5^2x_1x_2^2x_4^2x_5 \\
& - 3a_1^3a_2^2a_3^2a_5x_2^2x_5^4 && - 2a_1^2a_2a_3^3a_4a_5^2x_1^3x_5^3 \\
& + 3a_1^2a_3a_4^2a_5^2x_1^2x_4^4 && + 3a_1^2a_2^2a_3a_5^2x_2^4x_5^2 \\
& + 2a_1^2a_2a_4a_5^2x_2^3x_4^3 && - 3a_1a_3^2a_4^2a_5^3x_1^4x_4^2 \\
& - 6a_1^3a_2a_3^2a_4a_5x_1x_4^2x_5^3 && + 6a_1^3a_2a_3a_4a_5x_2x_4^3x_5^2 \\
& - 6a_1a_2a_3^2a_4a_5^3x_1^3x_2^2x_5 && + 6a_1a_2a_3a_4a_5^3x_1^2x_2^3x_4 \\
& + a_1^4a_2^2a_3^3x_5^6 && - a_1^3a_4^2a_5x_4^6 \\
& - a_1a_2^2a_5^3x_2^6 && + a_3^3a_4^2a_5^4x_1^6.
\end{aligned} \tag{3}
$$

Remark. In other cases, the integral basis and the index form is more complicated but the index form has similarly three factors. By eliminating x_1^6 from a linear combination of G_1 and G_2^2, we obtain a divisibility relation which is a necessary condition for monogenity of pure sextic number fields defined by $x^6 - m$ as follows.

Corollary 5.3.

(1) *If $\nu_2(m)$ is odd and $\nu_3(m) \neq 3$, then a_1a_5 divides $(a_3^2 \pm a_2^2a_4^2)$ is a necessary condition for monogenity of K.*
(2) *If $m \equiv 4 \pmod{16}$ and $\nu_3(m) \neq 3$, then a_1a_5 divides $(a_3^2 \pm 64a_2^2a_4^2)$ is a necessary condition for monogenity of K.*
(3) *If $m \equiv 12 \pmod{16}$ and $\nu_3(m) \neq 3$, then a_1a_5 divides $(-a_3^2 \pm 4a_2^2)$ is a necessary condition for monogenity of K.*

In the remaining cases the formulas become far too complicated.
The following results are proved in [12].

Corollary 5.4. *Assume that $m = e^5$ such that $e \neq \mp 1$ is a square free rational integer. Then*

(1) *If $e \not\equiv 1 \pmod 4$ and $e \not\equiv \pm 1 \pmod 9$, then K is monogenic and $\mathbb{Z}_K = \mathbb{Z}[\theta]$ with $\theta = \frac{\alpha^5}{e^4}$.*
(2) *If $e \equiv 1 \pmod 4$ or $e \equiv \pm 1 \pmod 9$, then K is not monogenic.*

Remark. When $m \neq \pm 1$ is a square free integer, we refer to [20] for further results on the monogenity of pure sextic number fields defined by $x^6 - m$. For integral bases and monogenity of sextic fields with a quadratic and a cubic subfield see Charkani and Sahmoudi [6].

6. Pure septic fields

In this section, K is a pure septic number field generated by $\alpha = m^{\frac{1}{7}}$, where $m \in \mathbb{Z}$ is not necessarily a square free integer and $m \neq \pm 1$. It is well-known that we can assume that $\nu_p(m) \leq 6$ for every prime integer p, and so

$$m = a_1a_2^2a_3^3a_4^4a_5^5a_6^6$$

, where $a_1, \ldots, a_6$ are pairwise coprime square-free integers. Let

$$A_1 = 1, \qquad A_2 = a_4a_5a_6, \qquad A_3 = a_3a_4a_5^2a_6^2,$$

$$A_4 = a_2a_3a_4^2a_5^2a_6^3, \quad A_5 = a_2a_3^2a_4^2a_5^3a_6^4 \quad \text{and} \quad A_6 = a_2a_3^2a_4^3a_5^4a_6^5.$$

The following theorem explicitly gives an integral basis of $\mathbb{Z}_K$.

Theorem 6.1.

(1) *If* $\overline{m} \notin \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \pmod{49}$, *then* $\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}\right)$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$.

(2) *If* $\overline{m} \in \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \pmod{49}$, *then*
$$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{(\alpha-m)^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6-\alpha^5+\alpha^4-\alpha^3+\alpha^2-\alpha+1}{7A_6}\right)$$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$.

Based on these integral bases we have

Corollary 6.2. $\mathbb{Z}[\alpha]$ *is the ring of integers of* K *if and only if* $m \neq \pm 1$ *is a square free integer and* $\overline{m} \notin \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \pmod{49}$.

As a special case, we have:

Corollary 6.3. *Assume that* $m = a^u$ *with* $a \neq \pm 1$ *a square free integer and* $1 \leq u \leq 6$ *a positive integer. If* $\overline{a} \notin \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \pmod{49}$, *then* K *is monogenic.*

7. Pure octic fields

In this section K is a pure octic number field generated by $m^{\frac{1}{8}}$, with $m \neq \pm 1$ a rational integer, not necessarily square-free. Let $m = a_1 a_2^2 a_3^3 a_4^4 a_5^5 a_6^6 a_7^7$, where $a_1, \dots, a_7$ are pairwise coprime square free rational integers. Let
$$A_2 = a_4a_5a_6a_7, \qquad A_3 = a_3a_4a_5a_6^2a_7^2, \qquad A_4 = a_2a_3a_4^2a_5^2a_6^3a_7^3,$$
$$A_5 = a_2a_3a_4^2a_5^3a_6^3a_7^4, \quad A_6 = a_2a_3^2a_4^3a_5^3a_6^4a_7^5, \quad \text{and} \quad A_7 = a_2a_3^2a_4^3a_5^4a_6^5a_7^6.$$
A detailed table for integral bases is given in [14] that we do not repeat here. Based on these integral bases we have:

Corollary 7.1. $\mathbb{Z}[\alpha]$ *is the ring of integers of* K *if and only if* $m \neq \pm 1$ *is a square free integer and* $m \not\equiv 1 \pmod 4$.

The following theorem will appear in [14], it gives sufficient conditions on m for the non-monogenity of K. It relaxes the condition m is a square free rational integer required in [5, 20].

Theorem 7.2. *If one of the following conditions holds:*

(1) $m \equiv 1 \pmod{32}$,

(2) $m \equiv 272 \pmod{512}$,

(3) $\nu_2(m)$ *is odd and* $a_2a_6 \pmod 8 \in \{2, 6\}$,

then K *is not monogenic.*

The following theorem will appear in [14].

Theorem 7.3. *Assume that* $m = a^t$ *with* $a \neq \pm 1$ *is a square free rational integer and* $t \in \{3, 5, 7\}$*. Then*

(1) *If* $a \not\equiv 1 \pmod 4$*, then* K *is monogenic and* $\mathbb{Z}_K = \mathbb{Z}[\theta]$ *with* $\theta = \dfrac{\alpha^u}{a^v}$*, where* $(u, v) \in \mathbb{Z}^2$ *is a solution of* $tu - 8v = 1$ *with* $u < 8$ *and* $u, v \geq 0$*.*

(2) *If* $a \equiv 1 \pmod 4$*, then* K *is not monogenic with the exception on* $a = -3$*.*

8. Pure nonic fields

In this section, K is a pure nonic number field generated by $m^{\frac{1}{9}}$, where $m \in \mathbb{Z}$ is not necessarily a square free integer and $m \neq \pm 1$. It is well known that we can assume that $\nu_p(m) \leq 8$ for every prime integer p, and so $m = a_1 a_2^2 a_3^3 a_4^4 a_5^5 a_6^6 a_7^7 a_8^8$, where $a_1, \ldots, a_8$ are pairwise coprime square-free integers. Let

$$A_1 = 1, \qquad A_2 = a_5 a_6 a_7 a_8, \qquad A_3 = a_3 a_4 a_5 a_6^2 a_7^2 a_8^2,$$

$$A_4 = a_3 a_4 a_5^2 a_6^2 a_7^3 a_8^3, \quad A_5 = a_2 a_3 a_4^2 a_5^2 a_6^3 a_7^3 a_8^4, \quad A_6 = a_2 a_3^2 a_4^2 a_5^3 a_6^4 a_7^4 a_8^5,$$

$$A_7 = a_2 a_3^2 a_4^3 a_5^3 a_6^4 a_7^5 a_8^6, \quad \text{and} \quad A_8 = a_2 a_3^2 a_4^3 a_5^4 a_6^5 a_7^6 a_8^7.$$

The following theorem gives explicitly an integral basis $\mathbf{B}$ of $\mathbb{Z}_K$.

Theorem 8.1. *In the following Table 1,* $\mathbf{B}$ *is a* $\mathbb{Z}$*-integral basis of* $\mathbb{Z}_K$*. The notation* m_3 *stands for* $m/3^{\nu_3(m)}$*.*

Based on these integral bases we have

Corollary 8.2. $\mathbb{Z}[\alpha]$ *is the ring of integers of* K *if and only if* $m \neq \pm 1$ *is a square free integer and* $m \not\equiv \pm 1 \pmod 9$*.*

As a special case, we have

Corollary 8.3. *Assume that* $m = a^u$ *with* $a \neq \pm 1$ *a square free integer,* $1 \leq u \leq 8$ *a positive integer. If* $a \not\equiv \pm 1 \pmod 9$*, then* K *is monogenic.*

9. Preliminaries

In order to prove our results, we recall some fundamental facts on *Newton polygon techniques.* Namely, the theorems of index and prime ideal factorization. Let $f(x) \in \mathbb{Z}[x]$ be the defining polynomial of α and let $\overline{f(x)} = \prod_{i=1}^{r} \overline{\phi_i(x)}^{l_i}$ modulo p be the factorization of $\overline{f(x)}$ into powers of monic irreducible coprime polynomials of $\mathbb{F}_p[x]$. Recall Dedekind's well known theorem says

TABLE 1.

Conditions	**B**
$\nu_3(m) \geq 1$ and $\nu_3(m) \notin \{3,6\}$ or $\nu_3(m^2-1) = 1$	$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}, \frac{\alpha^7}{A_7}, \frac{\alpha^8}{A_8}\right)$
$\nu_3(m^2-1) = 2$	$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6+m\alpha^3+m}{3A_6}, \frac{\alpha^7+2m\alpha^6+m\alpha^4-m\alpha^3+\alpha+m}{3A_7}, \frac{\beta}{3A_8}\right)$ $\beta = \alpha^8 + m\alpha^7 + \alpha^6 + m\alpha^5 + \alpha^4 + m\alpha - 2$
$\nu_3(m^2-1) \geq 3$	$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6+m\alpha^3+m}{3A_6}, \frac{\alpha^7+2m\alpha^6+m\alpha^4-m\alpha^3-2\alpha+m}{3A_7}, \frac{\beta}{9A_8}\right)$ $\beta = \alpha^8 + m\alpha^7 + 4\alpha^6 - 2m\alpha^5 - 2\alpha^4 + 3\alpha^2 + m\alpha - 2 + 3m$
$\nu_3(m) = 3$ $\nu_3(m_3^2-1) = 1$	$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^2\phi_2(\alpha)}{3A_5}, \frac{(\phi_2(\alpha))^2}{3A_6}, \frac{\alpha(\phi_2(\alpha))^2}{3A_7}, \frac{\alpha^2(\phi_2(\alpha))^2}{3A_8}\right)$ $\phi_2(\alpha) = \alpha^3 - 3m_3u\alpha - 3m_3,\ u = (m_3^2-1)/3$ and $m_3 = m/3^{\nu_3(m)}$
$\nu_3(m) = 3$ $\nu_3(m_3^2-1) \geq 1$	$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^2\phi_2(\alpha)}{3A_5}, \frac{(\phi_2(\alpha))^2}{3A_6}, \frac{\alpha(\phi_2(\alpha))^2}{3A_7}, \frac{\alpha^2(\phi_2(\alpha))^2}{3A_8}\right)$ $\phi_2(\alpha) = \alpha^3 - 3m_3,\ m_3 = m/3^{\nu_3(m)}$
$\nu_3(m) = 6$ $\nu_3(m_3^2-1) = 1$	$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^2\phi_2(\alpha)}{3A_5}, \frac{(\phi_2(\alpha))^2}{3A_6}, \frac{\alpha(\phi_2(\alpha))^2}{3A_7}, \frac{\alpha^2(\phi_2(\alpha))^2}{3A_8}\right)$ $\phi_2(\alpha) = \alpha^3 - 3m_3u\alpha^2 - 9m_3,\ u = (m_3^2-1)/3$ and $m_3 = m/3^{\nu_3(m)}$
$\nu_3(m) = 6$ $\nu_3(m_3^2-1) \geq 1$	$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^2\phi_2(\alpha)}{3A_5}, \frac{(\phi_2(\alpha))^2}{3A_6}, \frac{\alpha(\phi_2(\alpha))^2}{3A_7}, \frac{\alpha^2(\phi_2(\alpha))^2}{3A_8}\right)$ $\phi_2(\alpha) = \alpha^3 - 9m_3,\ m_3 = m/3^{\nu_3(m)}$

Theorem 9.1 ([27] Chapter I, Proposition 8.3). *If p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, then $p\mathbb{Z}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{l_i}$, where every $\mathfrak{p}_i = p\mathbb{Z}_K + \phi_i(\alpha)\mathbb{Z}_K$ and the residue degree of $\mathfrak{p}_i$ is $f(\mathfrak{p}_i) = \deg(\phi_i)$.*

In order to apply this theorem in an efficient way one needs a criterion to test whether p divides the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. In 1878, Dedekind gave the following criterion

Theorem 9.2 (Dedekind's Criterion [7], Theorem 6.1.4 and [8]). *For a number field K generated by a root α of a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ and a rational prime integer p, let $\overline{f}(x) = \prod_{i=1}^{r} \overline{\phi_i}^{l_i}(x) \pmod{p}$ be the factorization of $\overline{f}(x)$ in $\mathbb{F}_p[x]$, where the polynomials $\phi_i \in \mathbb{Z}[x]$ are monic with their reductions irreducible over $\mathbb{F}_p$ and $\gcd(\overline{\phi_i}, \overline{\phi_j}) = 1$ for every $i \neq j$. If we set*

$$M(x) = \frac{f(x) - \prod_{i=1}^{r} {\phi_i}^{l_i}(x)}{p},$$

then $M(x) \in \mathbb{Z}[x]$ and the following statements are equivalent:

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

When Dedekind's criterion fails, then we use the Newton polygon method, which is an alternative approach developed by Ore 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 (see [15, 25, 28], for more details [13, 21]). For a prime p, let ν_p be the p-adic valuation of $\mathbb{Q}$, $\mathbb{Q}_p$ its p-adic completion, and $\mathbb{Z}_p$ the ring of p-adic integers. Let also ν_p be the Gauss's extension of ν_p to $\mathbb{Q}_p(x)$. For any polynomial

$$P = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}_p[x]$$

set $\nu_p(P) = \min\big(\nu_p(a_i),\, i = 0, \dots, n\big)$, and for every nonzero polynomials P and Q of $\mathbb{Q}_p[x]$ set

$$\nu_p(P/Q) = \nu_p(P) - \nu_p(Q).$$

Let $\phi \in \mathbb{Z}_p[x]$ be a monic polynomial 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 $f(x) \in \mathbb{Z}_p[x]$. Using 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, $\deg\big(a_i(x)\big) < \deg(\phi)$). The *$\phi$-Newton polygon* of $f(x)$ with respect to p, is the lower boundary convex envelope of the set of points $\{(i,\nu_p(a_i(x))),\ a_i(x)\neq 0\}$ in the Euclidean plane, which we denote by $N_\phi(f)$. Geometrically, the ϕ-Newton polygon of $f(x)$ is the process of joining the obtained segments $S_1,\dots,S_t$ ordered by the increasing slopes, which can be expressed as $N_\phi(f)=S_1+\cdots+S_t$. These segments are called the sides of the polygon $N_\phi(f)$. For every $j=1,\dots,t$, let $l(S_j)$ be the length of the projection of S_j to the x-axis and $h(S_j)$ the length of its projection to the y-axis. Then $l(S_j)$ is called the length of S_j, $h(S_j)$ is its height, and $-\lambda_j=-h(S_j)/l(S_j)$ is its slope. The *principal ϕ-Newton polygon* of $f(x)$, 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 the polygon $N_\phi^+(f)$ of length $l(S)$ and height $h(S)$, let $d(S)=\gcd\big(l(S),h(S)\big)$ be the degree of S. For every side S of $N_\phi^+(f)$, with initial point (s,u_s) and length l, and for every $0\le i\le l$, we attach the *residue coefficient* $c_i\in\mathbb{F}_\phi$:

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

where $(p,\phi(x))$ is the maximal ideal of $\mathbb{Z}_p[x]$ 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 in S, and so $c_i=0$. The polynomial

$$f_S(y)=t_dy^d+t_{d-1}y^{d-1}+\cdots+t_1y+t_0\in\mathbb{F}_\phi[y]$$

is called the *residual polynomial* of $f(x)$ associated to the side S, where for every $i=0,\dots,d$, $t_i=c_{ie}$. Notice that as $t_d\neq 0$, $\deg(f_S)=d$.

Let $N_\phi^+(f)=S_1+\cdots+S_t$ be the principal ϕ-Newton polygon of f with respect to p. We say that f is a *ϕ-regular polynomial* with respect to p, if $f_{S_i}(y)$ is square free in $\mathbb{F}_\phi[y]$ for every $i=1,\dots,r$. The polynomial f is said to be *p-regular* if $\overline{f(x)}=\prod_{i=1}^r\overline{\phi_i}^{l_i}$ for some monic polynomials $\phi_1,\dots,\phi_r$ of $\mathbb{Z}[x]$ such that $\overline{\phi_1},\dots,\overline{\phi_r}$ are irreducible coprime polynomials over $\mathbb{F}_p$ and f is a ϕ_i-regular polynomial with respect to p for every $i=1,\dots,r$.

The theorem of Ore plays a key role for proving our main Theorems. Let $\phi\in\mathbb{Z}_p[x]$ be a monic polynomial, assume that $\overline{\phi(x)}$ is irreducible in $\mathbb{F}_p[x]$. As defined in [15, Def. 1.3], the *ϕ-index* of $f(x)$, denoted by $\mathrm{ind}_\phi(f)$, is $\deg(\phi)$ times 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).

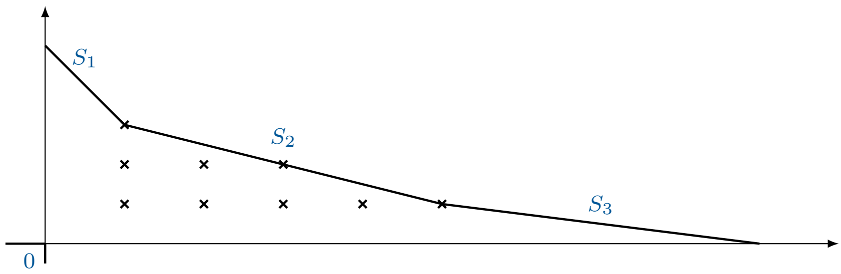

FIGURE 1. $N_\phi^+(f)$.

Now 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 every $\phi_i \in \mathbb{Z}[x]$ is monic polynomial, such that $\overline{\phi_i(x)}$ is irreducible in $\mathbb{F}_p[x]$, $\overline{\phi_i(x)}$ and $\overline{\phi_j(x)}$ are coprime when $i \neq j$ and $i, j = 1, \dots, r$. For every $i = 1, \dots, r$, let $N_{\phi_i}^+(f) = S_{i1} + \dots + S_{ir_i}$ be the principal ϕ_i-Newton polygon of f with respect to p. For every $j = 1, \dots, r_i$, let $f_{S_{ij}}(y) = \prod_{k=1}^{s_{ij}} \psi_{ijk}^{a_{ijk}}(y)$ be the factorization of $f_{S_{ij}}(y)$ in $\mathbb{F}_{\phi_i}[y]$. Then we have the following index theorem of Ore (see [15, Theorem 1.7 and Theorem 1.9]).

THEOREM 9.3 (Theorem of Ore)**.**

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

The equality holds if $f(x)$ is p-regular.

If $f(x)$ is p-regular, then

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

is the factorization of $p\mathbb{Z}_K$ into powers of prime ideals of $\mathbb{Z}_K$ lying above p, where $e_{ij} = l_{ij}/d_{ij}$, l_{ij} is the length of S_{ij}, d_{ij} is the ramification degree of S_{ij}, and $f_{ijk} = deg(\phi_i) \times deg(\psi_{ijk})$ is the residue degree of the prime ideal $\mathfrak{p}_{ijk}$ over p.

If some factors of $f(x)$ provided by Hensel's factorization and refined by first order Newton polygon (Ore program) are not irreducible over $\mathbb{Q}_p$, then in order to complete the factorization of $f(x)$, Guardia, Montes, and Nart introduced the notion of *high order Newton polygon*. Using the theorem of index they showed that after a finite number of iterations this process yields all monic irreducible factors of $f(x)$, all prime ideals of $\mathbb{Z}_K$ lying above a prime integer p, the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, and the absolute discriminant of K. We recall here some fundamental techniques of Newton polygons of high order. For more details, we refer to [21]. As introduced in [21], a type of order $r-1$ is a data

$$\mathbf{t} = \big(g_1(x), -\lambda_1, g_2(x), -\lambda_2, \ldots, g_{r-1}(x), -\lambda_{r-1}, \psi_{r-1}(x)\big),$$

where every $g_i(x)$ is a monic polynomial in $\mathbb{Z}_p[x]$, $\lambda_i \in \mathbb{Q}^+$, and $\psi_{r-1}(y)$ is a polynomial over a finite field of p^H elements with $H = \prod_{i=0}^{r-2} f_i$, here $f_i = \deg(\psi_i(x))$, satisfying the following recursive properties:

(1) $g_1(x)$ is irreducible modulo p, $\psi_0(y) \in \mathbb{F}[y]$ ($\mathbb{F}_0 = \mathbb{F}_p$) being the polynomial obtained by reduction of $g_1(x)$ modulo p, and $\mathbb{F}_1 := \mathbb{F}_0[y]/\big(\psi_0(y)\big)$.

(2) For every $i = 1, \ldots, r-1$, the Newton polygon of ith order, $N_i\big(g_{i+1}(x)\big)$, has a single side of slope $-\lambda_i$.

(3) For every $i = 1, \ldots, r-1$, the residual polynomial of i^{th} order, $R_i(g_{i+1})(y)$ is an irreducible polynomial in $\mathbb{F}_i[y]$, $\psi_i(y) \in \mathbb{F}_i[y]$ being the monic polynomial determined by $R_i(g_{i+1})(y) \simeq \psi_i(y)$ are equal up to multiplication by a nonzero element of $\mathbb{F}_i$, and $\mathbb{F}_{i+1} = \mathbb{F}_i[y]/\big(\psi_i(y)\big)$. Thus, $\mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_r$ is a tower of finite fields.

(4) For every $i = 1, \ldots, r-1$, $g_{i+1}(x)$ has minimal degree among all monic polynomials in $\mathbb{Z}_p[x]$ satisfying (2) and (3).

(5) $\psi_{r-1}(y) \in \mathbb{F}_{r-1}[y]$ is a monic irreducible polynomial, $\psi_{r-1}(y) \neq y$, and $\mathbb{F}_r = \mathbb{F}_{r-1}[y]/\big(\psi_{r-1}(y)\big)$.

Here the field $\mathbb{F}_i$ should not be confused with the finite field of i elements. Let $\omega_0 = [\nu_p, x, 0]$ be the Gauss's extension of ν_p to $\mathbb{Q}_p(x)$. Since $R_i(g_{i+1})(y)$ ($i = 1, \ldots, r-1$) is irreducible in $\mathbb{F}_i[y]$ hence according to MacLane's notations and definitions (cf. [24]), $g_{i+1}(x)$ is a key polynomial of ω_i, and so it induces a valuation on $\mathbb{Q}_p(x)$, denoted by $\omega_{i+1} = e_{i+1}[\omega_i, g_{i+1}, \lambda_{i+1}]$, where $\lambda_{i+1} = h_{i+1}/e_{i+1}$, e_{i+1} and h_{i+1} are positive coprime integers. The valuation ω_{i+1} is called the *augmented valuation* of ν_p with respect to ϕ and λ is defined over $\mathbb{Q}_p[x]$ as follows

$$\omega_{i+1}\big(f(x)\big) = \min\{e_{i+1}\omega_i\big(a_j^{i+1}(x)\big) + jh_{i+1},\ j = 0, \ldots, n_{i+1}\},$$

where $f(X) = \sum_{j=0}^{n_{i+1}} a_j^{i+1}(x) g_{i+1}^j(x)$ is the $g_{i+1}(x)$-expansion of $f(x)$. According to the terminology in [21], the valuation ω_r is called the rth-order valuation associated to the data $\mathbf{t}$. For every order $r \geq 1$, the g_r-*Newton polygon* of $f(x)$, with respect to the valuation ω_r is the lower boundary of the convex envelope of the set of points $\{(i, \mu_i), i = 0, \ldots, n_r\}$ in the Euclidean plane, where $\mu_i = \omega_r\big(a_i^r(x) g_r^i(x)\big)$.

The following are the relevant theorems from Montes-Guardia-Nart's work on high order Newton polygons

Theorem 9.4 ([21] Theorem 3.1). *Let $f \in \mathbb{Z}_p[x]$ be a monic polynomial such that $\overline{f(x)}$ is a positive power of $\overline{\phi}$. If $N_r(f) = S_1 + \cdots + S_g$ has g sides, then we can split $f(x) = f_1 \times \cdots \times f_g(x)$ in $\mathbb{Z}_p[X]$, such that $N_r(f_i) = S_i$ and*

$R_r(f_i)(y) = R_r(f)(y)$ up to multiplication by a nonzero element of $\mathbb{F}_r$ for every $i = 1, \dots, g$.

Theorem 9.5 ([21] Theorem 3.7). *Let $f \in \mathbb{Z}_p[x]$ be a monic polynomial such that $N_r(f) = S$ has a single side of finite slope $-\lambda_r$. If $R_r(f)(y) = \prod_{i=1}^{t} \psi_i(y)^{a_i}$ is the factorization in $\mathbb{F}_r[y]$, then $f(x)$ splits as $f(x) = f_1(x) \times \cdots \times f_t(x)$ in $\mathbb{Z}_p[x]$ such that $N_r(f_i) = S$ has a single side of slope $-\lambda_r$ and $R_r(f_i)(y) = \psi_i(y)^{a_i}$ up to multiplication by a nonzero element of $\mathbb{F}_r$ for every $i = 1, \dots, t$.*

In [21, Definition 4.15], the authors introduced the notion of rth-*order index of a monic polynomial* $f \in \mathbb{Z}[x]$ as follows.

For a fixed data

$$\mathbf{t} = \big(g_1(x), -\lambda_1, g_2(x), -\lambda_2, \dots, g_{r-1}(x), -\lambda_{r-1}, \psi_{r-1}(x)\big),$$

let $N_r(f)$ be the Newton polygon of r^{th}-order with respect to the data $\mathbf{t}$ and

$$\mathrm{ind}_t(f) = f_0 \cdots f_{r-1} \,\mathrm{ind}\big(N_r(f)\big),$$

where $\mathrm{ind}\big(N_r(f)\big)$ is the index of the polygon $N_r(f)$; the number of points with natural integer coordinates that lie below or on the polygon $N_\phi^+(f)$, strictly above the horizontal line of equation $y = \omega_r(f)$, and strictly beyond the vertical axis. In [21, Theorem 4.18], they showed the following *index formula* which generalizes the theorem of index of Ore

$$\mathrm{ind}(f) \geq \mathrm{ind}_1(f) + \cdots + \mathrm{ind}_r(f).$$

10. Proofs of main results

10.1. Pure cubic fields

Proof of Theorem 2.1. Since the discriminant of $f(x) = x^3 - m$ is $\triangle(f) = -3^3 m^2$, thank to the formula $\triangle(f) = (\mathbb{Z}_K : \mathbb{Z}[\alpha])^2 d_K$, linking the absolute discriminant of d_K of K, the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ and $\triangle(f)$, we need only to calculate $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha]))$ and a p-integral basis of $\mathbb{Z}_K$ for every prime integer p dividing $3 \cdot m$. Let p be a prime integer dividing $3 \cdot m$.

(1) Assume p divides m. In this case $\overline{f(x)} = \phi^3$ in $\mathbb{F}_p[x]$, where $\phi = x$. Let $v = \nu_p(m)$. Then $N_\phi(f) = S$ has a single side joining $(0, v)$ and $(3, 0)$. As $v \in \{1, 2\}$, then $d = 1$ is the degree of $f_S(y)$, and so by Theorem 9.3, we get $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \mathrm{ind}_\phi(f)$ and $(1, \alpha, \frac{\alpha^2}{a_2})$ is a p-integral basis of $\mathbb{Z}_K$.

(2) For $p = 3$ and 3 does not divide m, $f(x) = \phi^3 + 3m\phi^2 + 3m^2\phi + m^3 - m$, where $\phi = x - m$. It follows that:
   (a) If $\nu_3(m^2 - 1) = 1$, then $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$ and $(1, \alpha, \frac{\alpha^2}{a_2})$ is an integral basis of $\mathbb{Z}_K$.

(b) If $\nu_3(m^2-1) \geq 2$; $m \equiv \pm 1 \pmod 9$, then $\nu_3((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 1$ and $(1, \alpha, \frac{\alpha^2+m\alpha+m^2}{3a_2})$ is an integral basis of $\mathbb{Z}_K$. $\square$

Proof of Corollary 2.4. Under the hypothesis $a_1 = \pm 1$ and $a_2 = a$. So if $a \not\equiv \pm 1 \pmod 9$, then

$$\operatorname{ind}(\theta) = \left|ax_1^3 \pm x_2^3\right|.$$

is the index from of K. Thus for $(x_1, x_2) = (0, 1)$, we have $\operatorname{ind}(\theta) = 1$ and K is monogenic. $\square$

10.2. Pure quartic fields

Proof of Theorem 3.1. Since the discriminant of $f(x) = x^4 - m$ is $\triangle(f) = -4^4 m^3$, thank to the formula linking the discriminant of K, the index, and $\triangle(f)$, we need only to calculate $\nu_p\big(\operatorname{ind}(f)\big)$ and a p-integral basis of $\mathbb{Z}_K$ for every prime integer p dividing $2 \cdot m$. Let p be a prime integer dividing $2 \cdot m$.

(1) p divides m. In this case $\overline{f(x)} = \phi^4$ in $\mathbb{F}_p[x]$, where $\phi = x$. Let $v = \nu_p(m)$. Then $N_\phi(f) = S$ has a single side joining $(0, v)$ and $(4, 0)$. Let $\gcd(v, 4) = d$. Then $d \in \{1, 2\}$. It follows that
   (a) If $p \neq 2$ or $d = 1$, then $f_S(y)$ is square-free in $\mathbb{F}_p[x]$. By Theorem 9.3, we get $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \operatorname{ind}_\phi(f)$ and $(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3})$ is a p-integral basis of $\mathbb{Z}_K$.
   (b) For $p = 2$ and $d = 2$; $\nu_2(m) = 2$, we have $f_S(y) = (y-1)^2$. Thus, we have to use second order Newton polygon techniques. The following table gives the adequate ϕ_2 in order to have $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \operatorname{ind}_1(f) + \operatorname{ind}_2(f)$ and a lower bound of $V(\phi_2(\alpha))$ for any valuation V of K extending ν_2.

Conditions	ϕ_2	$V\big(\phi_2(\alpha)\big)$
$m \equiv 4 \pmod{16}$	x^2+2	≥ 2
$m \equiv 12 \pmod{32}$	x^2-2x+6	$\geq 5/2$
$m \equiv 28 \pmod{32}$	x^2-2x+2	$\geq 5/2$

(2) If 2 does not divide m, then $f(x) = \phi^4 + 4m\phi^3 + 6m^2\phi^2 + 4m^3\phi + m^4 - m$, where $\phi = x - m$.
   (a) If $\nu_2(m-1) = 1$, then $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 0$ and $\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}\right)$ is an integral basis of $\mathbb{Z}_K$.
   (b) If $\nu_2(m-1) = 2$, then $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 2$ and $\left(1, \alpha, \frac{\alpha^2+m^2}{2A_2}, \frac{\alpha^3+m^2\alpha}{2A_3}\right)$ is an integral basis of $\mathbb{Z}_K$.

(c) If $\nu_2(m-1) \geq 3$, then $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 3$ and
$$\left(1, \alpha, \frac{\alpha^2+m^2}{2A_2}, \frac{\alpha^3-m\alpha^2-m^2\alpha+2m^4-m^3}{4A_3}\right)$$
is an integral basis of $\mathbb{Z}_K$. □

Proof of Corollary 3.4. If $m = a$, then $a_1 = a$ and $a_2 = a_3 = 1$. So if $a \not\equiv \pm 1 \pmod 4$, then
$$\mathrm{ind}(\theta) = \left|(x_1^2 - ax_3^2)(x_1^4 + 2a^2x_1^2x_3^2 + 4ax_2^4 - 8ax_1x_2^2x_3 + a^2x_3^4)\right|.$$
is the index from of K. Thus for $(x_1, x_2, x_3) = (1, 0, 0)$, we have $\mathrm{ind}(\theta) = 1$. Similarly, if $m = a^3$, then $a_3 = a$ and $a_2 = a_1 = 1$. So if $a \not\equiv \pm 1 \pmod 4$, then $\mathrm{ind}(\theta) = \left|(ax_1^2 - x_3^2)(a^2x_1^4 + 2ax_1^2x_3^2 + 4ax_2^4 - 8ax_1x_2^2x_3 + x_3^4)\right|$. is the index form of K. Thus for $(x_1, x_2, x_3) = (0, 0, 1)$, we have $\mathrm{ind}(\theta) = 1$. In both cases, K is monogenic. □

10.3. Pure quintic fields

Proof of Theorem 4.1. Since the discriminant of $f(x) = x^5 - m$ is $\triangle(f) = 5^5m^4$, thank to the formula linking the discriminant of K, the index, and $\triangle(f)$, we need only to calculate $\nu_p(\mathrm{ind}(f))$ and a p-integral basis of $\mathbb{Z}_K$ for every prime integer p dividing $5 \cdot m$. Let p be a prime integer dividing $5 \cdot m$.

(1) If p divides m, then $\overline{f(x)} = \phi^5$ in $\mathbb{F}_p[x]$, where $\phi = x$. Let $v = \nu_p(m)$. Then $N_\phi(f) = S$ has a single side joining $(0, v)$ and $(5, 0)$. Since $1 \leq v \leq 4$, $\gcd(v, 5) = 1$, and so the side is of degree 1. Thus $f_S(y)$ is irreducible over $\mathbb{F}_\phi$. By Theorem 9.3, we get $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \mathrm{ind}_\phi(f)$ and $(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4})$ is a p-integral basis of $\mathbb{Z}_K$.

(2) If $p = 5$ and 5 does not divide m, then $\overline{f(x)} = \phi^5$ is the factorization of $\overline{f(x)}$ in $\mathbb{F}_5[x]$, where $\phi = x - m$. By considering $f(x + m)$, let $f(x) = \phi^5 + 5m\phi^4 + 10m^2\phi^3 + 10m^3\phi^2 + 5m^4\phi + m^5 - m$ be the ϕ-expansion of $f(x)$ with $\phi = x - m$. Thus, if $\nu_5(m^5 - m) = 1$, then $N_\phi^+(f)$ has a single side of height 1, and so 5 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. If $\nu_5(m^5 - m) \geq 2$, then $N_\phi^+(f) = S_1 + S_2$ has two sides joining $(0, v)$, $(1, 1)$, and $(5, 0)$. Thus each side is of degree 1, and so by Theorem 9.3, $\nu_5((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \mathrm{ind}_\phi(f) = 1$ and $(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\phi(\alpha)}{5A_4})$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, where $\phi(\alpha) = \alpha - m$. □

Proof of Lemma 4.3.
If 5 divides m or $\nu_5(m^4 - 1) = 1$, then $\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}\right)$ is a $\mathbb{Z}$-integral basis of $\mathbb{Z}_K$ and $(\mathbb{Z}[\theta] : \mathbb{Z}[\alpha]) = a_2^2a_3^4a_4^6$. Now for every $(x_0, x_1, x_2, x_3, x_4) \in \mathbb{Z}^5$, let $\theta = x_0 + x_1\alpha + x_2\frac{\alpha^2}{a_3a_4} + x_3\frac{\alpha^3}{a_2a_3a_4^2} + x_4\frac{\alpha^4}{a_2a_3^2a_4^3}$. If we replace
$$(x_1, x_2, x_3, x_4) \quad \text{by} \quad \left(x_1, \frac{x_2}{a_3a_4}, \frac{x_3}{a_2a_3a_4^2}, \frac{x_4}{a_2a_3^2a_4^3}\right)$$

in the index formula given in [20, 5.3, p. 139], we can compute the index $(\mathbb{Z}[\alpha] : \mathbb{Z}[\theta])$. Thus,
$(\mathbb{Z}_K : \mathbb{Z}[\theta]) = (\mathbb{Z}_K : \mathbb{Z}[\alpha]) \cdot (\mathbb{Z}[\alpha] : \mathbb{Z}[\theta]) = \left| a_2^2 a_3^4 a_4^6 \cdot \mathrm{ind}\left(x_1, \frac{x_2}{a_3 a_4}, \frac{x_3}{a_2 a_3 a_4^2}, \frac{x_4}{a_2 a_3^2 a_4^3}\right) \right|,$
and we conclude the desired index form $\mathrm{ind}(x_1, x_2, x_3, x_4)$. □

Proof of Corollary 4.4.

(1) If $m^4 \not\equiv 1 \pmod{25}$ that is $m \equiv 1, 7, 18, 24 \pmod{25}$, then $\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}\right)$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$. Denote by $\mathrm{ind}(x_1, x_2, x_3, x_4)$ the index form corresponding to this integral basis. We can apply the index formula given in Lemma 4.3. We have, $\mathrm{ind}(x_1, x_2, x_3, x_4) \equiv \pm B_i x_i^{10} \pmod{a_{j_i}}$ with

$$\begin{aligned} j_1 &= 1, \quad B_1 = a_2^2 a_3^4 a_4^6, & j_2 &= 3, \quad B_2 = -a_1^2 a_2^6 a_4^4, \\ j_3 &= 2, \quad B_3 = -a_1^4 a_3^6 a_4^2, \quad \text{and} & j_4 &= 4, \quad B_4 = a_1^6 a_2^4 a_3^2. \end{aligned}$$

Let δ_i^j be the Kronecker symbol, that is $\delta_i^i = 1$ and $\delta_i^j = 0$ for $i \neq j$. Thus for $m = a_{j_i}^u$ we have $a_k = 1$ for every $k \neq j_i$, and so $B_i = \pm 1$, and $\mathrm{ind}\left(\delta_{j_i}^1, \delta_{j_i}^2, \delta_{j_i}^3, \delta_{j_i}^4\right) = B_{j_i} \cdot 1^{10} = \pm 1$. Therefore K is monogenic.

(2) If $m = a^u$, then let $(x_0, y_0) \in \mathbb{Z}^2$ be the unique solution of $ux_0 - 5y_0 = 1$ with $1 \leq x_0 \leq 4$; x_0 is the unique integer satisfying $1 \leq x_0 \leq 4$ and $ux_0 - 5y_0 = 1$. Since $\theta^5 = a$, $g(x) = x^5 - a$ is the minimal polynomial of $\theta = \frac{\alpha^{x_0}}{a}$ over $\mathbb{Q}$, and so θ is a primitive element of K. Since $a \neq \pm 1$ is a square free integer, by [20, 5.3, Remark 6], we conclude that if $a^4 \equiv 1 \pmod{25}$, then K is not monogenic with the unique exception $a = 7$. □

10.4. Pure septic fields

Proof of Theorem 6.1. Since the discriminant of $f(x) = x^7 - m$ is $\triangle(f) = -7^7 m^6$, thank to the formula linking the discriminant of K, the index, and $\triangle(f)$, we need only to calculate $\nu_p(\mathrm{ind}(f))$ and a p-integral basis of $\mathbb{Z}_K$ for every prime integer p dividing $7 \cdot m$. Let p be a prime integer dividing $7 \cdot m$.

(1) If p divides m, then $\overline{f(x)} = \phi^7$ in $\mathbb{F}_p[x]$, where $\phi = x$. Let $v = \nu_p(m)$. Then $N_\phi(f) = S$ has a single side joinining $(0, v)$ and $(7, 0)$ with $v = \nu_p(m)$. Since $1 \leq v \leq 6$, $\gcd(v, 7) = 1$, and so the side is of degree 1. Thus $f_S(y)$ is irreducible over $\mathbb{F}_\phi$. By Theorem 9.3, we get $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \mathrm{ind}_\phi(f)$ and $\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}\right)$ is a p-integral basis of $\mathbb{Z}_K$.

(2) If $p = 7$ and 7 does not divide m, then $\overline{f(x)} = \phi^7$ is the factorization of $\overline{f(x)}$ in $\mathbb{F}_7[x]$, where $\phi = x - m$. By considering $f(x + m)$, let $f(x) = \phi^7 + 7m\phi^6 + 21m^2\phi^5 + 35m^3\phi^4 + 35m^4\phi^3 + 21m^5\phi^2 + 7m^6\phi + m^7 - m$ be the ϕ-expansion of $f(x)$ with $\phi = x - m$. Thus, if $\nu_7(m^6 - 1) = 1$, then $N_\phi^+(f)$ has a single side of height 1, and so 7 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. If $\nu_7(m^6 - 1) \geq 2$;

$m \equiv \pm 1, \pm 18, \pm 19$, then $N_\phi^+(f) = S_1 + S_2$ has two sides joining $(0, v)$, $(1, 1)$, and $(7, 0)$. Thus each side is of degree 1, and so by Theorem 9.3, $\nu_7((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \mathrm{ind}_\phi(f) = 1$ and $\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\phi(\alpha)^6}{7A_6}\right)$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, where $\phi(\alpha) = \alpha - m$. □

Proof of Corollary 6.3.
Let (x, y) be the unique solution of $u \cdot x - 7y = 1$ and $0 \leq x \leq 6$. Let $\theta = \frac{\alpha^x}{a^y}$. Then θ is a complex root of the polynomial $g(x) = x^7 - a$. Since $a \neq \pm 1$ is a square free integer and $\overline{a} \notin \{\pm\overline{1}, \pm\overline{18}, \pm\overline{19}\} \pmod{49}$, then by Theorem 6.1, $(1, \theta, \ldots, \theta^6)$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, which means that K is monogenic. □

10.5. Pure nonic fields

Proof of Theorem 8.1. Since the discriminant of $f(x) = x^9 - m$ is $\triangle(f) = 9^9 m^8$, thank to the formula linking the absolute discriminant d_K of K, the index, and $\triangle(f)$, we need only to calculate $\nu_p(\mathrm{ind}(f))$ and a p-integral basis of $\mathbb{Z}_K$ for every prime integer p dividing $3 \cdot m$. Let p be a prime integer dividing $3 \cdot m$.

(1):
If p divides m, then $\overline{f(x)} = \phi^9$ in $\mathbb{F}_p[x]$, where $\phi = x$. Let $v = \nu_p(m)$. Then $N_\phi(f) = S$ has a single side joining $(0, v)$ and $(9, 0)$. Let $d = \gcd(v, 9)$. If 3 does not divide v, then $d = 1$, and so the side S is of degree 1 and $f_S(y)$ is irreducible over $\mathbb{F}_\phi$. By Theorem 9.3, we get

$$\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \mathrm{ind}_\phi(f).$$

Similarly if $d \in \{3, 6\}$ and $p \neq 3$, then $f_S(y) = y^d - m$ is a separable polynomial over $\mathbb{F}_\phi = \mathbb{F}_p$, and so $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \mathrm{ind}_\phi(f)$. In both cases $\big(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}, \frac{\alpha^7}{A_7}, \frac{\alpha^8}{A_8}\big)$ is a p-integral basis of $\mathbb{Z}_K$. For $p = 3$, 3 divides m, and $\nu_3(m) \in \{3, 6\}$.

(1/a):
If $\nu_3(m) = 3$, then for $\phi = x$, $N_\phi(f) = S$ has a single side of slope $-\lambda = -1/3$, and $f_S(y) = (y - m_3)^3$. Thus we have to use second order Newton polygon techniques. According to Nart's notations in [21], let ω_2 be the valuation of second order Newton polygon associated to the data (ϕ, λ, ψ) with $\psi(y) = y - m_3$ and $\phi_2 = x^3 - 3m_3$, where $m_3 = m/3^{\nu_3(m)}$. Let also $f(x) = \phi_2^3 + 9m_3\phi_2^2 + 27m_3^2\phi_2 + 27m_3(m_3^2 - 1)$ be the ϕ_2-expansion of $f(x)$ and $N_2(f)$ be the ϕ_2-Newton polygon of f with respect to ω_2. Then $\omega_2(\phi_2^3) = 9$, $\omega_2(9m_3\phi_2^2) = 12$, and $\omega_2(27m_3^2\phi_2) = 12$. It follows that:

(1/a/i):
If $\nu_3(m_3^2 - 1) \geq 2$, then $\omega_2(27m_3(m_3^2 - 1)) \geq 15$, and so $N_2(f) = S_1 + S_2$ has two sides joining the points $(0, v)$, $(1, 12)$, and $(3, 9)$ with $v \geq 15$. Thus, each side S_i is of degree 1, and so $\nu_3(\mathrm{ind}(f)) = \mathrm{ind}_1(f) + \mathrm{ind}_2(f) = 9 + 4 = 13$. Let V be a

valuation of K extending ν_3 and $r = V(\phi_2(\alpha))$. Since $\phi_2(\alpha)$ is integral over $\mathbb{Z}$, then $r \geq 0$. As $V(f(\alpha)) = \infty$, and $N_2(f) = S_1 + S_2$, we conclude that $3r = 3 + r$ or $3 + r = v/3$). Thus $2r = 3$ or $r \geq 2$. Hence $V(\phi_2(\alpha)) \geq 3/2$. Let us show that

$$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5 - 3m_3\alpha^2}{3A_5}, \frac{\alpha^6 - 6m_3\alpha^3 + 9m_3^2}{3A_6}, \right.$$
$$\left. \frac{\alpha^7 - 6m_3\alpha^4 + 9m_3^2\alpha}{3A_7}, \frac{\alpha^8 - 6m_3\alpha^5 + 9m_3^2\alpha^2}{3A_8}\right)$$

is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$. Based on the calculation of the index $\mathrm{ind}(f)$, we need to show that every element of this basis is integral. In order to show that each of these elements is integral, we need to verify that for every valuation V of K extending ν_3, we have the V-valuations of these elements are greater than or equal to 0. This technique will be repeated in all of the following cases.

(1/a/ii):
If $\nu_3(m_3^2 - 1) = 1$, then $N_2(f) = S$ has a single side of slope -1. Replace ϕ_2 by $\phi_2 - 3m_3ux$ with $u = (m_3^2 - 1)/3$, we get $N_2(f) = S_1 + S_2$ has two sides joining the points $(0, v)$, $(1, 12)$, and $(3, 9)$ with $v \geq 15$. Therefore,

$$\nu_3\big(\mathrm{ind}(f)\big) = \mathrm{ind}_1(f) + \mathrm{ind}_2(f) = 9 + 4 = 13$$

and

$$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5 - 3m_3u\alpha - 3m_3\alpha^2}{3A_5}, \frac{\phi_2(\alpha)^2}{3A_6}, \frac{\alpha\phi_2(\alpha)^2}{3A_7}, \frac{\alpha^2\phi_2(\alpha)^2}{3A_8}\right)$$

is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, where $\phi_2(x) = x^3 - 3m_3ux - 3m_3$.

(1/b):
If $\nu_3(m) = 6$, then for $\phi = x$, $N_\phi(f) = S$ has a single side of slope $-\lambda = -2/3$, and $f_S(y) = (y - m_3)^3$. Let ω_2 be the valuation of second order Newton polygon associated to the data (ϕ, λ, ψ) with $\psi(y) = y - m_3$ and $\phi_2 = x^3 - 9m_3$. Let also $f(x) = \phi_2^3 + 27m_3\phi_2^2 + 243m_3^2\phi_2 + 729m_3(m_3^2 - 1)$ be the ϕ_2-expansion of $f(x)$ and $N_2(f)$ be the ϕ_2-Newton polygon of f with respect to ω_2. Similarly to the previous case, we have the following cases

(1/b/i):
If $\nu_3(m) = 6$, then for $\phi = x$, $N_\phi(f) = S$ has a single side of slope $-\lambda = -2/3$, and $f_S(y) = (y - m_3)^3$. Let ω_2 be the valuation of second order Newton polygon associated to the data (ϕ, λ, ψ) with $\psi(y) = y - m_3$ and $\phi_2 = x^3 - 3^2m_3$. Let also $f(x) = \phi_2^3 + 27m_3\phi_2^2 + 243m_3^2\phi_2 + 729m_3(m_3^2 - 1)$ be the ϕ_2-expansion of $f(x)$ and $N_2(f)$ be the ϕ_2-Newton polygon of f with respect to ω_2. It follows that

(1/b/i/A):
If $\nu_3(m_3^2 - 1) \geq 2$, then $N_2(f) = S_1 + S_2$ has two sides joining the points $(0, v)$, $(1, 21)$, and $(3, 18)$ with $v \geq 24$. Thus, each side is of degree 1, and so

$\nu_3(\mathrm{ind}(f)) = \mathrm{ind}_1(f)+\mathrm{ind}_2(f) = 21+4 = 25$. Let V be a valuation of K extending ν_3 and $r = V\big(\phi_2(\alpha)\big)$.Based on $N_2(f)$, we conclude that $V\big(\phi_2(\alpha)\big) \geq 5/2$. Therefore

$$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4 - 9m_3\alpha}{3A_4}, \frac{\alpha^5}{A_5}, \frac{\phi_2(\alpha)^2}{3A_6}, \frac{\alpha\phi_2(\alpha)^2}{3A_7}, \frac{\alpha^2\phi_2(\alpha)^2}{3A_8}\right)$$

is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, where $\phi_2(x) = x^3 - 3^2m_3$.

(1/b/i/B):
If $\nu_3(m_3^2 - 1) = 1$, then $N_2(f) = S$ has a single side joining $(0, 21)$ and $(3, 18)$, and so is of slope -1. By replacing ϕ_2 by $\phi_2 - 3m_3ux^2$ with $u = (m_3^2 - 1)/3$, we get $N_2(f) = S_1 + S_2$ has two sides joining the points $(0, v)$, $(1, 21)$, and $(3, 18)$ with $v \geq 24$. Therefore, $\nu_3(\mathrm{ind}(f)) = \mathrm{ind}_1(f) + \mathrm{ind}_2(f) = 21 + 4 = 25$ and so

$$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4 - 9m_3u\alpha^2 - 9m_3\alpha}{3A_4}, \frac{\alpha^5}{A_5}, \frac{\phi_2(\alpha)^2}{3A_6}, \frac{\alpha\phi_2(\alpha)^2}{3A_7}, \frac{\alpha^2\phi_2(\alpha)^2}{3A_8}\right)$$

is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, where $\phi_2(x) = x^3 - 3m_3ux^2 - 3^2m_3$.

(1/b/ii):
For $p=3$ and 3 does not divide m, $\overline{f(x)}=\phi^9$ is the factorization of $\overline{f(x)}$ in $\mathbb{F}_3[x]$, where $\phi = x - m$. Let $f(x) = \phi^9 + 9m\phi^8 + 36m^2\phi^7 + 84m^3\phi^6 + 126m^4\phi^5 + 126m^5\phi^4 + 84m^6\phi^3 + 36m^7\phi^2 + 9m^8\phi + m^9 - m$ be the ϕ-expansion of $f(x)$ with $\phi = x - m$.

(1/b/ii/A):
If $\nu_3(m^2 - 1) = 1$; $\nu_3(m^9 - m) = 1$, then $N_\phi^+(f)$ has a single side of height 1, and so 3 does not divide $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. Then

$$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}, \frac{\alpha^7}{A_7}, \frac{\alpha^8}{A_8}\right) \quad \text{is a } \mathbb{Z}\text{-basis of } \mathbb{Z}_K.$$

(1/b/ii/B):
If $\nu_3(m^2 - 1) = 2$, then $N_\phi^+(f)$ has two sides joining $(0, 2)$, $(3, 1)$, and $(9, 0)$. Thus each side of $N_\phi^+(f)$ has degree 1, and so $\nu_3((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 2$ and

$$\left(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6 + m\alpha^3 + m}{3A_6}, \frac{\alpha^7 + m\alpha^4 + m\alpha}{3A_7}, \frac{\alpha^8 + m\alpha^5 + m\alpha^2}{3A_8}\right)$$

is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$.

(1/b/ii/C):
If $\nu_3(m^2 - 1) \geq 3$, then $N_\phi^+(f)$ has a three sides joining $(0, v)$, $(1, 2)$, $(3, 1)$, and $(9, 0)$. Thus each side of $N_\phi^+(f)$ has degree 1, and so $\nu_3((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = 4$

and

$$\Big(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6 + m\alpha^3 + m}{3A_6}, \frac{\alpha^7 + m\alpha^4 + m\alpha}{3A_7}, \frac{\alpha^8 + m\alpha^7 + 4\alpha^6 - 2m\alpha^5 - 2\alpha^4 + 3\alpha^2 + m\alpha - 2 + 3m}{9A_8}\Big)$$

is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$. □

Proof of Corollary 8.3.
Since $\mathrm{GCD}(u, 9) = 1$, let (x, y) be the unique solution of $u \cdot x - 9y = 1$ and $0 \le x \le 8$. Let $\theta = \frac{\alpha^x}{a^y}$. Then θ is a complex root of the polynomial $g(x) = x^9 - a$. Since $a \ne \pm 1$ is a square free integer and $a \not\equiv \pm 1 \pmod 9$, then by Corollary 8.2, $(1, \theta, \ldots, \theta^8)$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, which means that K is monogenic. □

REFERENCES

[1] AHMAD, S.—NAKAHARA, T.– HUSNINE, S. M. HUSNINE: *Power integral bases for certain pure sextic fields*, Int. J. Number Theory **10**, (2014), no. 8, 2257–2265.

[2] AHMAD, S.—NAKAHARA, T.—HAMEED, A.: *On certain pure sextic fields related to a problem of Hasse*, Int. J. Alg. Comput., **26**, No 3 (2016), no. 3, 577–583 .

[3] ALACA, S.: *p-integral bases of a cubic field*, Proc. Am. Math. Soc. **126** (1998), 1949–1953.

[4] ALACA, S.—WILLIAMS, K.: *p-integral bases of a quartic field defined by a trinomial* $x^4 + ax + b$, Far. East. J. Math. Sci. **12** (2004), 137–168.

[5] 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.

[6] CHARKANI, M. E.—SAHMOUDI, M.: *Sextic extension with cubic subfield*, JP J. Algebra Number Theory Appl. **34** (2014), no. 2, 139–150.

[7] COHEN, H.: *A Course in Computational Algebraic Number Theory*, GTM 138, Springer--Verlag, Berlin, 1993.

[8] DEDEKIND, R.: *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen*, Göttingen Abhandlungen, **23** (1878), 1–23.

[9] EL FADIL, L.: *Computation of a power integral basis of a pure cubic number field*, Int. J. Contemp. Math. Sci. **2** (2007), 601–606.

[10] EL FADIL, L.: *Prime ideal factorization and p-integral basis of quintic number fields defined by* $X^5 + aX + b$, Gulf J. Math. **6** (2018), no. 4, 1–13.

[11] EL FADIL, L.: *On Power integral bases for certain pure sextic fields*, Bol. Soc. Paran. Math. (to appear)

[12] EL FADIL, L.: *On Power integral bases for certain pure sextic fields with non-square free coefficients*, J. Number Theory, **228** (2021), 375–389.

[13] EL FADIL, L.: *On Newton polygon's techniques and factorization of polynomial over Henselian valued fields*, J. of Algebra and its Appl. **19** (2020), no. 10, Article id. 2050188. `https://doi.org/10.1142/S0219498820501881`

[14] EL FADIL, L.—GAÁL, I.: *On integral bases and monogeneity of pure octic number fields with non-square free parameters*, Glasnik Mat. (submitted) arXiv preprint, arXiv:2202.04417, 2022.

[15] EL FADIL, L.—MONTES, J.—NART, E.: *Newton polygons and p-integral bases of quartic number fields*, J. Algebra and Appl. **11** (2012), no. 4, Article id. 1250073. https://doi.org/10.1142/S0219498812500739

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

[17] GAÁL, I.: *Diophantine Equations and Power Integral Bases. Theory and Algorithms.* 2nd edition, Birkhäuser/Springer, Cham, 2019.

[18] GAÁL, I. — GYŐRY, K.: *Index form equations in quintic fields*, Acta Arith. **89** (1999), 379–396.

[19] GAÁL, I.—REMETE, L.: *Binomial Thue equations and power integral bases in pure quartic fields*, JP J. Algebra Number Theory Appl. **32** (2014), no. 1, 49–61.

[20] GAÁL, I.—REMETE, L.: *Power integral bases and monogenity of pure fields*, J. Number Theory, **173** (2017), 129–146.

[21] GUÀRDIA, J.—MONTES, J.—NART, E.: *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416.

[22] HASSE, H.: *Zahlentheorie*. Akademie-Verlag, Berlin, 1963.

[23] HENSEL, K.: *Theorie der algebraischen Zahlen*. Teubner Verlag, Leipzig, Berlin, 1908.

[24] MACLANE, S.: *A construction for absolute values in polynomial rings*, Trans. Amer. Math. Soc. **40** (1936), 363–395.

[25] MONTES, J.—NART, E.: *On a theorem of Ore*, J. Algebra, **146** (1992), no. 2, 318–334.

[26] MOTODA, Y.—NAKAHARA, T.—SHAH, S. I. A.: *On a problem of Hasse*, J. Number Theory, **96** (2002), 326–334.

[27] NEUKIRCH, J.: *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.

[28] ORE, O.: *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), 84–117.

[29] PETHŐ, A.—POHST, M.: *On the indices of multiquadratic number fields*, Acta Arith. **153** (2012), no. 4, 393–414.

Received November 10, 2022

Faculty of Sciences
Dhar El Mahraz
Sidi Mohamed ben Abdellah University
P.O. Box 1796
Fez
MOROCCO
E-mail: lhouelfadil2@gmail.com

Institute of Mathematics
University of Debrecen
H-4002 Debrecen
Pf. 400
HUNGARY
E-mail: gaal.istvan@unideb.hu