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

(3s.) **v. 2025 (43)** : 1–17.
ISSN-0037-8712
doi:10.5269/bspm.67298

On integral bases and monogenity of pure octic number fields with non-square free parameters

Lhoussain El Fadil and István Gaál*

ABSTRACT: In all available papers, on power integral bases of pure octic number fields K, generated by a root α of a monic irreducible polynomial $f(x) = x^8 - m \in \mathbb{Z}[x]$, it was assumed that $m \neq \pm 1$ is square free. In this paper, we investigate the monogenity of any pure octic number field, without the condition that m is square free. We start by calculating an integral basis of $\mathbb{Z}_K$, the ring of integers of K. In particular, we characterize when $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. We give sufficient conditions on m, which guarantee that K is not monogenic. We finish the paper by investigating the case when $m = a^u$, $u \in \{1, 3, 5, 7\}$ and $a \neq \mp 1$ is a square free rational integer.

Key Words: Power integral basis, index, Theorem of Ore, prime ideal factorization

Contents

1. Introduction

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a root α of a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n. Denote by $\mathbb{Z}_K$ its ring of integers and d_K its absolute discriminant. The ring $\mathbb{Z}_K$ is said to have a *power integral basis* if it has a $\mathbb{Z}$-basis $(1, \theta, \cdots, \theta^{n-1})$ for some $\theta \in \mathbb{Z}_K$. That means $\mathbb{Z}_K = \mathbb{Z}[\theta]$, that is $\mathbb{Z}_K$ is mono-generated as a ring, with a single generator θ. In this case, the field K is said to be *monogenic* and not monogenic otherwise.

The problem of deciding the monogenity of a number field and constructing power integral bases is a classical problem of algebraic number theory, going back to Dedekind [6], Hensel [18] and Hasse [16]. This area is intensively studied even nowadays, cf. [10] for the present state of this research.

It is well-known that $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank n. For any primitive element $\theta \in \mathbb{Z}_K$ (that is $K = \mathbb{Q}(\theta)$), $\mathbb{Z}[\theta]$ is a subgroup of $\mathbb{Z}_K$ of finite index. We call

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

the *index of* θ. Obviously, $\mathrm{ind}(\theta) = 1$ if and only if $(1, \theta, \ldots, \theta^{n-1})$ is an integral basis of $\mathbb{Z}_K$. As it is known [10], we have

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

where $\triangle(\theta)$ is the discriminant of the minimal polynomial of θ.

The greatest common divisor $i(K)$ of the indices of the primitive elements $\theta \in \mathbb{Z}_K$ of K is called the *(field) index of* K. It is clear that if $i(K) > 1$, then K is not monogenic. On the other hand, $i(K) = 1$ does not imply that K is monogenic. If a prime p divides $i(K)$, then p is called a prime *common index divisor* of K.

* Corresponding author
2010 *Mathematics Subject Classification:* 11R04, 11R16, 11R21.
Submitted February 28, 2023. Published March 07, 2024

Let $(1,\omega_1,\dots,\omega_{n-1})$ be an integral basis of $\mathbb{Z}_K$. The discriminant $\triangle(L(X_1,\dots,X_n))$ of the linear form $L(X_1,\dots,X_{n-1})=\omega_1X_1+\dots+\omega_{n-1}X_{n-1}$ can be written (cf. [10]) as

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

where $\mathrm{ind}(X_1,\dots,X_{n-1})$ is the *index form* corresponding to the integer basis $(1,\omega_1,\dots,\omega_{n-1})$ having the property that for any $\theta=x_0+\omega_1x_1+\dots+\omega_{n-1}x_{n-1}\in\mathbb{Z}_K$ (with $x_0,x_1,\dots,x_{n-1}\in\mathbb{Z}$) we have $\mathrm{ind}(\theta)=|\mathrm{ind}(x_1,\dots,x_{n-1})|$. Therefore θ 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* $\mathrm{ind}(x_1,\dots,x_{n-1})=\pm1$.

According to our notation K is generated by a root α of a monic irreducible polynomial $f\in\mathbb{Z}[x]$. The index

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

is called the *index of the polynomial* f and we also have

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

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

Among all types of number fields, most investigations deal with pure number fields K generated by a root of an irreducible polynomial x^n-m. Assuming that m is square free, Gaál and Remete [11] studied pure quartic fields, Ahmad, Nakahara and Husnine [2,3], Ahmad, Nakahara and Hameed [1], El Fadil [8] pure sextic fields. Applying the index forms, Gaál and Remete [12] investigated pure number fields of degrees $3\le n\le 9$.

The subject of our present paper is the monogenity of pure octic fields. For square free m Hameed and Nakahara [15], proved that if $m\equiv 1 \pmod{16}$, then the octic number field generated by $m^{1/8}$ is not monogenic, but if $m\equiv 2,3 \pmod 4$, then it is monogenic.

In all above quoted papers, the authors consider only pure octic number fields generated by a root of a monic polynomial $f(x)=x^8-m$, where $m\neq\pm1$ is a square free rational integer. Our purpose is to extend these results to arbitrary parameters m, without assuming that m is square free. We start by calculating an integral basis of $\mathbb{Z}_K$ in Theorem 2.1. We give sufficient conditions on m, which guarantee the non monogenity of K. We conclude the paper by studying the case where $m=a^u$, $u\in\{1,3,5,7\}$, and $a\neq\mp1$ is a square free rational integer.

2. Main results

Throughout this paper, $m\neq\pm1$ is a rational integer such that the polynomial $f(x)=x^8-m$ is irreducible over $\mathbb{Q}$. Let α be a root of $f(x)$, let $K=\mathbb{Q}(\alpha)$ with ring of integers $\mathbb{Z}_K$. Replacing α by $\frac{\alpha}{p}$ and m by $\frac{m}{p^8}$, and repeating this process until we get $\nu_p(m)<8$ for every prime integer p, we can assume that $m=a_1a_2^2a_3^3a_4^4a_5^5a_6^6a_7^7$, where $a_1,\dots,a_7$ are square free pairwise coprime rational integers. Set $A_2=a_4a_5a_6a_7$, $A_3=a_3a_4a_5a_6^2a_7^2$, $A_4=a_2a_3a_4^2a_5^2a_6^3a_7^3$, $A_5=a_2a_3a_4^2a_5^3a_6^3a_7^4$, $A_6=a_2a_3^2a_4^3a_5^3a_6^4a_7^5$, and $A_7=a_2a_3^2a_4^3a_5^4a_6^5a_7^6$.

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

Theorem 2.1 *Using the above notations let* $m_2=\frac{m}{2^{\nu_2(m)}}$ *and let* $u\in\mathbb{Z}$ *such that* $m_2u\equiv 1 \pmod{2^6}$. *In the following table* **B** *is an explicitly given integral basis of* K.

Table A :

conditions	**B**
$\nu_2(m)$ *is odd*	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}, \frac{\alpha^7}{A_7})$
$m \equiv 28 \pmod{32}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\phi_2(\alpha)}{2A_4}, \frac{\alpha\phi_2(\alpha)}{2A_5}, \frac{\alpha^2\phi_2(\alpha)}{4A_6}, \frac{\alpha^3\phi_2(\alpha)}{4A_7})$ $\phi_2(\alpha) = \alpha^4 + 2m_2u\alpha^2 + 2m_2u$
$m \equiv 12 \pmod{32}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\phi_2(\alpha)}{2A_4}, \frac{\alpha\phi_2(\alpha)}{2A_5}, \frac{\alpha^2\phi_2(\alpha)}{2A_6}, \frac{\alpha^3\phi_2(\alpha)}{4A_7})$ $\phi_2(\alpha) = \alpha^4 + 2m_2u\alpha^2 + 4m_2u\alpha + 6m_2u$
$m \equiv 4 \pmod{16}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\phi_2(\alpha)}{2A_4}, \frac{\alpha\phi_2(\alpha)}{2A_5}, \frac{\alpha^2\phi_2(\alpha)}{2A_6}, \frac{\alpha^3\phi_2(\alpha)}{2A_7})$ $\phi_2(\alpha) = \alpha^4 + 2m_2u$
$m \equiv 48 \pmod{64}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha\phi_2(\alpha)^2}{2A_5}, \frac{\alpha^6}{A_6}, \frac{\alpha^3\phi_2(\alpha)^2}{2A_7})$ $\phi_2(\alpha) = \alpha^2 + 2m_2u$
$m \equiv 80 \pmod{128}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha\phi_2(\alpha)}{2A_3}, \frac{(\phi_2(\alpha))^2}{2A_4}, \frac{\alpha(\phi_2(\alpha))^2}{2A_5}, \frac{\alpha^2(\phi_2(\alpha))^2}{2A_6}, \frac{\alpha(\phi_2(\alpha))^3}{4A_7})$ $\phi_2(\alpha) = \alpha^2 + 2m_2u$
$m \equiv 144 \pmod{256}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\phi_2(\alpha)^2}{2A_4}, \frac{\alpha\phi_2(\alpha)^2}{2A_5}, \frac{\theta}{4A_6}, \frac{\alpha\cdot\theta}{4A_7})$ $\phi_2(\alpha) = \alpha^2 + 2m_2u$ *and* $\theta = \phi_2^3(\alpha) - 8m_2u\phi_2^2(\alpha) + 24m_2u\phi_2(\alpha) - 32m_2u$
$m \equiv 16 \pmod{256}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\phi_2(\alpha)^2}{2A_4}, \frac{\alpha\phi_2(\alpha)^2}{2A_5}, \frac{\theta}{4A_6}, \frac{\alpha\cdot\theta}{8A_7})$ $\phi_2(\alpha) = \alpha^2 + 2m_2u$ *and* $\theta = \phi_2^3(\alpha) - 8m_2u\phi_2^2(\alpha) + 24m_2u\phi_2(\alpha) - 32m_2u$
$m \equiv 448 \pmod{512}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\phi_2(\alpha)}{2A_4}, \frac{\alpha\phi_2(\alpha)}{4A_5}, \frac{\alpha^2\phi_2(\alpha)}{2A_6}, \frac{\alpha^3\phi_2(\alpha)}{2A_7})$ $\phi_2(\alpha) = \alpha^4 + 4m_2u\alpha^3 + 12m_2u\alpha^2 + 24m_2u$
$m \equiv 192 \pmod{512}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\phi_2(\alpha)}{2A_4}, \frac{\alpha\phi_2(\alpha)}{4A_5}, \frac{\alpha^2\phi_2(\alpha)}{4A_6}, \frac{\alpha^3\phi_2(\alpha)}{2A_7})$ $\phi_2(\alpha) = \alpha^4 + 4m_2u\alpha^2 + 8m_2u$
$m \equiv 64 \pmod{256}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\phi_2(\alpha)}{2A_4}, \frac{\alpha\phi_2(\alpha)}{2A_5}, \frac{\alpha^2\phi_2(\alpha)}{2A_6}, \frac{\alpha^3\phi_2(\alpha)}{2A_7})$ $\phi_2(\alpha) = \alpha^4 + 8m_2u$
$m \equiv 3 \pmod{4}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}, \frac{\alpha^7}{A_7})$
$m \equiv 5 \pmod{8}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4+m^4}{2A_4}, \frac{\alpha^5+m^4\alpha}{2A_5}, \frac{\alpha^6+m^4\alpha^2}{2A_6}, \frac{\alpha^7+m^4\alpha^3}{2A_7})$
$m \equiv 9 \pmod{16}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4+m^4}{2A_4}, \frac{\alpha^5+m^4\alpha}{2A_5}, \frac{\alpha^6-2m\alpha^5-m^2\alpha^4+m^2\alpha^2+2m\alpha+3m^2}{4A_6},$ $\frac{\alpha^7-m\alpha^6+m^2\alpha^5-m\alpha^4+m^2\alpha^3-m\alpha^2+(m^2+4m)\alpha+m}{4A_7})$
$m \equiv 1 \pmod{16}$	$(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4+m^2}{2A_4}, \frac{\alpha^5+m^2\alpha}{2A_5}, \frac{\alpha^6-2m\alpha^5-m^2\alpha^4+m^2\alpha^2+2m\alpha+3m^2}{4A_6},$ $\frac{\alpha^7-m\alpha^6+m^2\alpha^5-m\alpha^4+m^2\alpha^3-m\alpha^2+(m^2+4m)\alpha+m}{8A_7})$

As a consequence we obtain:

Corollary 2.1 *Let $K = \mathbb{Q}(\alpha)$ be a pure octic number field generated by a root α of a monic irreducible polynomial $f(x) = x^8 - m \in \mathbb{Z}[x]$. Then $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ if and only if m is a square free integer and* $m \not\equiv 1 \pmod{4}$.

In case of the integral basis $(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}, \frac{\alpha^7}{A_7})$, considering the explicit form of factors of the index form we conclude:

Theorem 2.2 *Keeping the notation of Section 2, if $\nu_2(m)$ is odd or $m \equiv 3 \pmod{4}$, then*

$$8a_1a_3a_5a_7 | (a_2^2a_6^2 \pm 1)$$

is a necessary condition for the monogenity of K.

By the $\pm$ sign we mean that for the monogenity of K the divisibility condition must hold with at least one of the signs. Note that similar conditions can be derived also in the other cases of the integral basis, but the calculation becomes far too complicated.

Our next main result gives sufficient conditions on m for the non-monogenity of K. It relaxes the condition m is square free required in [15,12].

Theorem 2.3 *Let $K = \mathbb{Q}(\alpha)$ be a pure octic number field generated by a root α of a monic irreducible polynomial $f(x) = x^8 - m \in \mathbb{Z}[x]$. If one of the following conditions holds*

1. $m \equiv 1 \pmod{32}$,
2. $m \equiv 16 \pmod{512}$,
3. $\nu_2(m)$ *is odd and* $a_2a_6 \pmod 8 \in \{2, 6\}$,

then K is not monogenic.

Finally, we consider monogenity of pure octic fields for m of type a^u:

Theorem 2.4 *Assume that $m = a^u$ with $a \neq \pm 1$ a square free rational integer and $u \in \{3, 5, 7\}$. Then*

1. *If $a \not\equiv 1 \pmod 4$, then K is monogenic and $\mathbb{Z}_K$ is generated by $\theta = \frac{\alpha^x}{a^y}$, where $(x, y) \in \mathbb{Z}^2$ is the unique solution in non negative integers of the equation $ux - 8y = 1$ with $x < 8$.*
2. *If $a \equiv 1 \pmod 4$, then K is not monogenic with the exception of $a = -3$.*

3. Preliminaries

In order to show Theorem 2.1 and Theorem 2.3, we recall some fundamental facts of Newton polygon techniques applied to algebraic number theory. Namely, the theorems on the index and on the prime ideal factorization. For a detailed presentation of this theory we refer to the paper of Guardia and Nart [14].

Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial with a root α, 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 that a well-known theorem of Dedekind says that:

Theorem 3.1 *([21, Chapter I, Proposition 8.3])*

$$\text{If } p \text{ does not divide the index } (\mathbb{Z}_K : \mathbb{Z}[\alpha]), \text{ then } p\mathbb{Z}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{l_i}, \text{ where } \mathfrak{p}_i = p\mathbb{Z}_K + \phi_i(\alpha)\mathbb{Z}_K$$

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

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

Theorem 3.2 (*Dedekind's criterion [5, Theorem 6.1.4] and [6]*)
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 $M(x) = \dfrac{f(x) - \prod_{i=1}^{r} {\phi_i}^{l_i}(x)}{p}$, 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 $i = 1, \ldots, r$, either $l_i = 1$ or $l_i \geq 2$ and $\overline{\phi_i}(x)$ does not divide $\overline{M}(x)$ in $\mathbb{F}_p[x]$.*

When Dedekind's criterion fails, that is, p divides the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ for every primitive element $\alpha \in \mathbb{Z}_K$ of K, then it is not possible to obtain the prime ideal factorization of $p\mathbb{Z}_K$ by Dedekind's theorem. In 1928, Ore developed an alternative approach for obtaining the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, the absolute discriminant, and the prime ideal factorization of the rational primes in a number field K by using Newton polygons (see [19,22]). For more details on Newton polygon techniques, we refer to [7,13]. For any prime integer 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 ν_p be the Gauss's extension of ν_p to $\mathbb{Q}_p(x)$; $\nu_p(P) = \min(\nu_p(a_i), i = 0, \dots, n)$ for any polynomial $P = \sum_{i=0}^n a_i x^i \in \mathbb{Q}_p[x]$ and extended by $\nu_p(P/Q) = \nu_p(P) - \nu_p(Q)$ for every nonzero polynomials P and Q of $\mathbb{Q}_p[x]$. 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 $f(x) \in \mathbb{Z}_p[x]$, upon the Euclidean division by successive powers of ϕ, we expand $f(x)$ as follows: $f(x) = \sum_{i=0}^l a_i(x)\phi(x)^i$, called the *$\phi$-expansion* of $f(x)$ (for every i, $\deg(a_i(x)) < \deg(\phi)$). 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 $N_\phi(f)$. The ϕ-Newton polygon of f, is the process of joining the obtained edges $S_1, \dots, S_r$ ordered by increasing slopes, which can be expressed as $N_\phi(f) = S_1 + \cdots + S_r$. For every side S_i of $N_\phi(f)$, the length of S_i, denoted $l(S_i)$ is the length of its projection to the x-axis and its height , denoted $h(S_i)$ is the length of its projection to the y-axis. Let $d(S_i) = \gcd(l(S_i), h(S_i))$ be the ramification degree of S. The *principal ϕ-Newton polygon* of f, denoted $N_\phi^-(f)$, is the part of the polygon $N_\phi(f)$, which is determined by joining all sides of negative slopes. For every side S of $N_\phi^-(f)$, with initial point (s, u_s) and length l, and for every $0 \leq i \leq l$, we attach the following residue coefficient $c_i \in \mathbb{F}_\phi$ as follows:

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

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

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

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

Let $N_\phi^-(f) = S_1 + \cdots + S_r$ 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 $\phi_1, \dots, \phi_t$ of $\mathbb{Z}[x]$ such that $\overline{\phi_1}, \dots, \overline{\phi_t}$ are irreducible coprime polynomials over $\mathbb{F}_p$ and f is a ϕ_i-regular polynomial with respect to p for every $i = 1, \dots, t$.

The theorem of Ore plays a fundamental role for proving our main Theorems:
Let $\phi \in \mathbb{Z}_p[x]$ be a monic polynomial, with $\overline{\phi(x)}$ irreducible in $\mathbb{F}_p[x]$. As defined in [9, 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).

In the example of *Figure* 1, $\mathrm{ind}_\phi(f) = 9 \times \deg(\phi)$.

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, with $\overline{\phi_i(x)}$ is irreducible in $\mathbb{F}_p[x]$, $\overline{\phi_i(x)}$ and $\overline{\phi_j(x)}$ are coprime when $i \neq j$ and $i, j = 1, \dots, t$. For every $i = 1, \dots, t$, let $N_{\phi_i}^-(f) = S_{i1} + \cdots + S_{ir_i}$ 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

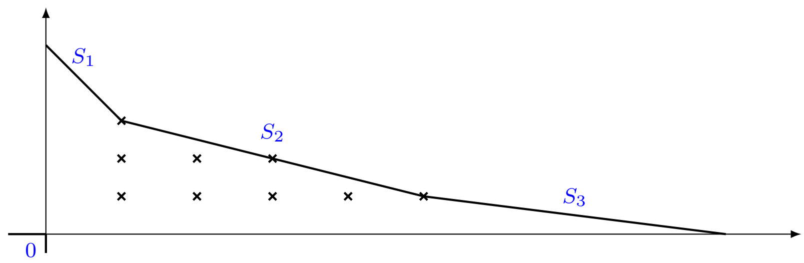

Figure 1: $N_\phi^-(f)$.

we have the following index theorem of Ore (see [9, Theorem 1.7 and Theorem 1.9], [7, Theorem 3.9], [19, pp: 323–325], and [22]).

Theorem 3.3 (*Theorem of Ore*)

1.
$$\nu_p(ind(f)) \geq \sum_{i=1}^{r} ind_{\phi_i}(f).$$
The equality holds if $f(x)$ is p-regular.

2. *If $f(x)$ is p-regular, then*
$$p\mathbb{Z}_K = \prod_{i=1}^{r}\prod_{j=1}^{r_i}\prod_{k=1}^{s_{ij}} \mathfrak{p}_{ijk}^{e_{ij}},$$
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.

When Ore's program fails; that is if $f(x)$ is not p-regular, then it may happen that some factors of $f(x)$ provided by Hensel's lemma and refined by first order Newton polygon techniques are not irreducible over $\mathbb{Q}_p$. In this case in order to complete the factorization of $f(x)$ in $\mathbb{Q}_p[x]$, Guardia, Montes, and Nart introduced the notion of *high order Newton polygon*. They showed, thanks to a theorem of index [13, Theorem 4. 18], that after a finite number of iterations this process yields all monic irreducible factors of $f(x)$ in $\mathbb{Q}_p[x]$, all prime ideals of $\mathbb{Z}_K$ lying above a prime integer p, the p-valuation of the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, and so up to a sign the absolute discriminant of K.

We recall here some fundamental techniques of Newton polygons of high order. For more details, we refer to [13] and [14]. As introduced in [13], a *type of order* $r-1$ is a data $\mathbf{t} = (g_1(x), -\lambda_1, g_2(x), -\lambda_2, \dots, g_{r-1}(x), -\lambda_{r-1}, \psi_{r-1}(x))$, 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 and $H = \prod_{i=0}^{r-2} f_i$, with $f_i = \deg(\psi_i(x))$, satisfying the following recursive properties:

1. $g_1(x)$ is irreducible modulo p, $\psi_0(y) \in \mathbb{F}[y]$ ($\mathbb{F}_0 = \mathbb{F}_p$) is the polynomial obtained by reduction of $g_1(x)$ modulo p, and $\mathbb{F}_1 := \mathbb{F}_0[y]/(\psi_0(y)))$.
2. For every $i = 1, \dots, r-1$, the Newton polygon of i^{th} order, $N_i(g_{i+1}(x))$, has a single sided of slope $-\lambda_i$.

3. For every $i = 1, \dots, r-1$, the residual polynomial of i^{th} order, $R_i(g_{i+1})(y)$ is an irreducible polynomial in $\mathbb{F}_i[y]$. Let $\psi_i(y) \in \mathbb{F}_i[y]$ be 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 $\mathbb{F}_{i+1} = \mathbb{F}_i[y]/(\psi_i(y))$. Thus, $\mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_r$ is a tower of finite fields.

4. For every $i = 1, \dots, r-1$, $g_{i+1}(x)$ 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 $\mathbb{F}_r = \mathbb{F}_{r-1}[Y]/(\psi_{r-1}(y))$.

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 $\mathbb{Q}_p(x)$. As for every $i = 1, \dots, r-1$, the residual polynomial of the i^{th} order, $R_i(g_{i+1})(y)$ is an irreducible polynomial in $\mathbb{F}_i[y]$, then according to MacLane's notations and definitions [20], $g_{i+1}(x)$ induces a valuation on $\mathbb{Q}_p(x)$, denoted by $\omega_{i+1} = e_i[\omega_i, g_{i+1}, \lambda_{i+1}]$, where $\lambda_i = h_i/e_i$, e_i and h_i are positive coprime integers. The valuation ω_{i+1} is called the *augmented valuation* of ω_i with respect to g_{i+1} and λ_{i+1}, defined over $\mathbb{Q}_p[x]$ as follows:

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

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 [13], the valuation ω_r is called the r^{th}-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, denoted $N_r(f)$ is the lower boundary of the convex envelope of the set of points $\{(i, \mu_i), i = 0, \dots, n_r\}$ in the Euclidean plane, where $\mu_i = \omega_r(a_i^r(x) g_r^i(x))$. Its principal part is denoted $N_r^-(f)$. The following are the relevant theorems from Guardia-Montes-Nart's work (high order Newton polygon):

Theorem 3.4 (*[13, Theorem 3.1]*)
Let $f(x) \in \mathbb{Z}_p[x]$ be a monic polynomial such that $\overline{f(x)}$ is a positive power of $\overline{\phi(x)}$ for some monic polynomial $\phi(x)$ such that $\overline{\phi(x)}$ is irreducible over $\mathbb{F}_0$. If $N_r^-(f) = S_1 + \cdots + S_g$ has g sides, then we can split $f(x) = F_0(x) \times F_1(x) \times \cdots \times F_g(x)$ 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 $i = 1, \cdots, g$.

Theorem 3.5 (*[13, Theorem 3.7]*)
Let $f(x) \in \mathbb{Z}_p[x]$ 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 $f(x) = F_0(x) \times F_1(x) \times \cdots \times F_t(x)$ 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 $i = 1, \cdots, t$.

Remark 3.1 The statement of Theorem 3.4 coincides with that given in [13, Theorem 3.1], with $f_{\mathbf{t}} = F_1(x) \times \cdots \times F_g(x)$.
The statement of Theorem 3.5 coincides with that given in [13, Theorem 3.7], with $f_{(\mathbf{t},\lambda_\mathbf{r})} = F_1(x) \times \cdots \times F_t(x)$.

In [13, Definition 4.11], the authors introduced a definition of the index of a polynomial $f(x)$ which is not necessarily irreducible over $\mathbb{Q}$ as follows: $\text{ind}(f) = \sum_{i=1}^k \text{ind}(F_i) + \sum_{1 \leq i < j \leq k} \nu_p(res(F_i, F_j))$, where $f(x) = \prod_{i=1}^k F_i$ is the factorization of $f(x)$ in $\mathbb{Q}_p[x]$, $\text{ind}(F_i) = \nu_p((\mathbb{Z}_i : \mathbb{Z}_p[\alpha_i]))$, α_i a root of $F_i(x)$ in $\overline{\mathbb{Q}}_p$,

$\mathbb{Z}_i$ the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_p(\alpha_i)$, and $res(F_i, F_j)$ is the resultant of F_i and F_j. This definition of index extends the known one of $\text{ind}(f) = (\mathbb{Z}_K : \mathbb{Z}[\alpha])$, with $\alpha \in \mathbb{Z}_K$ a primitive element of K and f its minimal polynomial over $\mathbb{Q}$. For a fixed irreducible polynomial $F(x)$ in $\mathbb{Z}_p[x]$ and a fixed data

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

the authors introduced in [13, Definition 4.15], the notion of r^{th}-*order index of* $f(x) \in \mathbb{Z}_p[x]$ as follows: Let $N_r(f)$ be the Newton polygon of r^{th}-order with respect to the data $\mathbf{t}$ and $\text{ind}_r(f) = f_0 \cdots f_{r-1} \text{ind}(N_r(f))$, where $f_i = \deg(\psi_i(x))$ and $\text{ind}(N_r(f))$ is the index of the polygon $N_r(f)$; the number of points with natural integer coordinates that lie below or on the polygon $N_r(F)$, strictly above the horizontal line of equation $y = \omega_r(f)$, and strictly beyond the vertical axis. They showed the following theorem on the index which generalizes the theorem of index of Ore as follows: Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial, which is irreducible over $\mathbb{Q}_p$ and

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

a fixed data such that $N_r(f)$ has a single side of negative slope ($\psi_{r-1}(y)$ divides $R_r(f)(y)$). Then we have the following theorem of index:

Theorem 3.6 (*[13, Theorem 4.18]*)

$$\nu_p(ind(f)) \geq ind_1(f) + \cdots + ind_r(f).$$

The equality holds if and only if $ind_{r+1}(f) = 0$.

Recall that by definition $\text{ind}(N_{r+1}(f)) = 0$ if and only if $N_{r+1}(f)$ has a single side of length 1 or height 1. By [13, Lemma 2.17] (2), if $R_r(f)$ is square free, then the length of $N_r(f)$ is 1. Thus if $R_r(f)$ is square free, then $\text{ind}_{r+1}(f) = 0$, and so the equality $\nu_p(\text{ind}(f)) = \text{ind}_1(f) + \cdots + \text{ind}_r(f)$ holds.

In order to complete the calculation of the index of any separable polynomial $f \in \mathbb{Z}[x]$, the authors introduced an iterative method to evaluate $\nu_p(res(F_i, F_j)$, with $f(x) = \prod_{i=1}^k F_i$ the factorization of $f(x)$ in $\mathbb{Q}_p[x]$, as follows: if $\overline{F_i}$ and $\overline{F_j}$ are coprime modulo p, then $res_r(F_i, F_j) = 0$. If $\overline{F_i}$ and $\overline{F_j}$ are congruent to a power of a monic irreducible polynomial $\overline{g_1} \in \mathbb{F}_0[x]$, then the authors introduced the r^{th}-resultant of F_i and F_i as follows:

$$res_r(F_i, F_j) = f_0 \cdots f_{r-1} \times \min(E_i H_j, E_j H_i),$$

where E_i and H_i are the length and height of the sides S_i of $N_r^-(F_i)$. Recall the following convention: If S_i is reduced to a single point, then $E_i = H_i = 0$ and $R_r(F_i)$ is a constant of $\mathbb{F}_r$.
Thanks to [13, Lemma 4.8] and [13, Theorem 4.10], we have the following:

$$\nu_p(res(F_i, F_j)) \geq res_1(F_i, F_j) + \cdots + res_r(F_i, F_j).$$

Moreover, if the data

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

satisfies the condition $N_r(F_i)$ has a single side of negative slope; $\psi_r(y)$ divides $R_r(F_i)(y)$, then the equality holds if and only if $R_{r+1}(F_i)(y)$ and $R_{r+1}(F_j)(y)$ are coprime.
In particular, if $\overline{F_i}$ and $\overline{F_j}$ are coprime modulo p, then $\nu_p(res(F_i, F_j)) = 0$.
If for some integer $r = 1, \dots, k$, $\psi_r(y)$ does not divide $R_r(F_s)$ for some $s = 1, 2$, then the equality holds.

4. Proofs of main results

Proof of Theorem 2.1.
During this proof, $\mathbb{F}_i$ is the i^{th} field of the tower provided by Montes algorithm. Since $\triangle(f) = \mp 8^8 m^7$ is the discriminant of f, thanks to the formula $\triangle(f) = (\mathbb{Z}_K : \mathbb{Z}[\alpha])^2 d_K$, the prime candidates to divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ are those dividing $2 \cdot m$.

1. Let p be a prime dividing m. Then $\overline{f(x)} = x^8 \pmod{p}$. For $\phi = x$, $N_\phi(f) = S$ has a single side joining the points $(0, \nu_p(m))$ and $(8, 0)$. Then $\mathrm{ind}_1(f) = \mathrm{ind}_\phi(f) = \nu_p(\prod_{i=2}^{7} A_i)$. Also by [9, Theorem 2.7], $(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}, \frac{\alpha^7}{A_7})$ is a free $\mathbb{Z}$-sub-module of $\mathbb{Z}_K$. Now, let $d = \gcd(\nu_p(m), 8)$. Then $R_1(f)(y) = y^d - \overline{m_p}$, where $m_p = m/p^{\nu_p(m)}$. If 2 does not divide $\nu_p(m)$, then $d = 1$, $R_1(f)(y)$ is irreducible over $\mathbb{F}_1$, and so by Theorem 3.3, $\mathrm{ind}(f) = \mathrm{ind}_\phi(f)$ and $(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}, \frac{\alpha^7}{A_7})$ is a p-integral basis of $\mathbb{Z}_K$. If 2 divides d, then $d \in \{2, 4\}$. In this case if $p \neq 2$, then $R_1(f)(y) = y^d - \overline{m_p}$ is square free over $\mathbb{F}_1 \simeq \mathbb{F}_0$ (because $\phi = x$, and so $\deg(\phi) = 1 = [\mathbb{F}_1 : \mathbb{F}_0]$). Thus by Theorem 3.3, $\nu_p(\mathrm{ind}(f)) = \mathrm{ind}_1(f)$ and $(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}, \frac{\alpha^7}{A_7})$ is a p-integral basis of $\mathbb{Z}_K$. It follows that if 2 divides m and $\nu_2(m)$ is odd, then $(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\alpha^4}{A_4}, \frac{\alpha^5}{A_5}, \frac{\alpha^6}{A_6}, \frac{\alpha^7}{A_7})$ is an integral basis of $\mathbb{Z}_K$.
   If $d \in \{2, 4\}$ and $p = 2$, then $R_1(f)(y) = (y - \overline{m_2})^d$ is not square free and we have to use second order Newton polygon techniques.

   (a) If $\nu_2(m) = 2$, then for $\phi = x$, we have $\overline{f(x)} = \phi^8 \pmod{2}$, $N_1(f) = S$ has a single side of slope $-\lambda_1 = -1/4$, $e_1 = 4$, and $R_1(f)(y) = y^2 + 1 = (y+1)^2$. According to the definitions and notations of [13,20], let $\omega_2 = e_1[\nu_2, \lambda_1]$ be the valuation of second order Newton polygon defined by $\omega_2(a) = e_1\nu_2(a) = 4\nu_2(a)$ for every $a \in \mathbb{Q}_2$ and $\omega_2(x) = e_1\lambda_1 = 1$. Let $\phi_2 = x^4 + 2$ be a key polynomial of ω_2 and $f(x) = \phi_2^2 - 4\phi_2 + (4 - m)$ the ϕ_2-expansion of $f(x)$. As $\omega_2(\phi_2) = 4$, $\omega_2(\phi_2^2) = 8$, and $\omega_2(4\phi_2) = 12$. It follows that:

      i. If $\nu_2(4 - m) = 3$; $m \equiv 12 \pmod{16}$, then there are 2 cases :
      If $\nu_2(12 - m) = 4$; $m \equiv 28 \pmod{32}$, then for $\phi_2 = x^4 + 2x^2 + 2$, we have $f(x) = \phi_2^2 - 4x^2\phi_2 - (4 + m)$ is the ϕ_2-expansion of $f(x)$. As $\omega_2(\phi_2^2) = 8$, $\omega_2((-4x^2)\phi_2) = 14$, and $\omega_2(4 + m) \geq 20$, we conclude that if $\omega_2(4 + m) = 20$, then $N_2(f)$ has a single side, $\mathrm{ind}_2(f) = 6$, and $R_2(f)(y) = y^2 + y + 1$. Thus $f(x)$ is irreducible over $\mathbb{Q}_2$ and $\nu_2(\mathrm{ind}(f)) = \mathrm{ind}_1(f) + \mathrm{ind}_2(f) = 4 + 6 = 10$. If $\omega_2(4 + m) > 20$, then $N_2(f)$ has two sides of degree 1 each. $f(x) = F_1(x)F_2(x)$ and $\nu_2(\mathrm{ind}(f)) = \nu_2(\mathrm{ind}(F_1)) + \nu_2(\mathrm{ind}(F_2)) + \nu_2(res(F_1, F_2)) = 0 + 0 + res_1(F_1, F_2) + res_2(F_1, F_2) = 4 + 6 = 10$. Based on the polygon $N_1(f)$, we conclude that $V(\alpha) = 1/4$. Similarly, based on $N_2(f)$, we conclude that $V(\phi_2(\alpha)) \geq 5/2$, and so $(1, \alpha, \alpha^2, \alpha^3, \frac{\phi_2(\alpha)}{4}, \frac{\alpha\phi_2(\alpha)}{4}, \frac{\alpha^2\phi_2(\alpha)}{8}, \frac{\alpha^3\phi_2(\alpha)}{8})$ is a 2-integral basis of $\mathbb{Z}_K$. Since the Montes algorithm is local; the algorithm provides p-integral bases, sometimes we have to replace $\phi_2(x)$ by an ω_2-equivalent polynomial. For example, in our case, if $\nu_p(A_i) \geq 1$ for some $i = 2, \ldots, 7$ and for some odd prime integer p, then $\frac{\alpha^3\phi_2(\alpha)}{8A_7}$ is not p-integral ($V(\frac{\alpha^3\phi_2(\alpha)}{8A_7}) < 0$ for some valuation V of K extending ν_p). So, we have to replace $\phi_2(x)$ by $g(x) = x^4 + 2m_2ux^2 + 2m_2u$ with u an integer which satisfies $um_2 \equiv 1 \pmod{32}$ and show that $\mathcal{B} = (1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{g(\alpha)}{2A_4}, \frac{\alpha g(\alpha)}{2A_5}, \frac{\alpha^2 g(\alpha)}{4A_6}, \frac{\alpha^3 g(\alpha)}{4A_7})$ is an integral basis of $\mathbb{Z}_K$. Since for every prime integer p, $\nu_p(\mathbb{Z}_K : \mathbb{Z}[\alpha]) = \nu_p(2^6\prod_{i=2}^{7} A_i)$, we need only to show that every element of $\mathbf{B}$ is integral over $\mathbb{Z}$. By the definition of $g(x)$ and by the first point of this proof the V-valuation of each element of $\mathbf{B}$ is greater or equal than 0 for every valuation V of K extending ν_p for every odd prime integer p. Let us show the same result for $p = 2$. For this reason we need to give a lower bound of $V(\alpha)$ and $V(\phi_2(\alpha))$ for every valuation V of K extending ν_2. Let V be a valuation of K extending ν_2. Since $V(\alpha) = 1/4$, $V(\phi_2(\alpha)) \geq 5/2$, $\nu_2(g(x) - \phi_2(x)) \geq 5$, and $\alpha \in \mathbb{Z}_K$, we conclude that $V(g(\alpha) - \phi_2(\alpha)) \geq 5$. Thus $V(g(\alpha)) \geq 5/2$, and so by a simple verification, the V-valuation of each element of $\mathbf{B}$ is greater or equal than 0. Hence $(1, \alpha, \frac{\alpha^2}{A_2}, \frac{\alpha^3}{A_3}, \frac{\phi_2(\alpha)}{2A_4}, \frac{\alpha\phi_2(\alpha)}{2A_5}, \frac{\alpha^2\phi_2(\alpha)}{4A_6}, \frac{\alpha^3\phi_2(\alpha)}{4A_7})$ is an integral basis of $\mathbb{Z}_K$.
      In the remainder of this proof, these techniques will be repeated. So in every case, we give an adequate $\phi_2(x)$ for which $f(x)$ is regular with respect to ω_2, we give the ϕ_2-expansion of $f(x)$, and a lower bound of $V(\phi_2(\alpha))$ for every valuation V of K extending ν_2.
      If $\nu_2(12 - m) \geq 5$ ($m \equiv 12 \pmod{32}$), then for $\phi_2 = x^4 + 2x^2 + 4x + 6$, $f(x) = \phi_2^2 + (-8 - 4x^2 - 8x)\phi_2 + (12 - m + 16x^3 + 32x^2 + 32x)$ is the ϕ_2-expansion of $f(x)$. As $\omega_2(\phi_2^2) = 8$, $\omega_2((-8 - 4x^2 - 8x)\phi_2) = 14$, and $\omega_2(12 - m + 16x^3 + 32x^2 + 32x) = \omega_2(16x^3) = 19$, we

conclude that $N_2(f)=S$ has a single side joining $(0,19)$ and $(2,8)$. Therefore $\mathrm{ind}_2(f)=5$, the side S is of degree 1, $f(x)$ is irreducible over $\mathbb{Q}_2$, and by Theorem 3.6 $\nu_2(\mathrm{ind}(f))=\mathrm{ind}_1(f)+5$. Thus $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{\phi_2(\alpha)}{2A_4},\frac{\alpha\phi_2(\alpha)}{2A_5},\frac{\alpha^2\phi_2(\alpha)}{2A_6},\frac{\alpha^3\phi_2(\alpha)}{4A_7})$ is a 2-integral basis of $\mathbb{Z}_K$. Now by replacing $\phi_2(x)$ by $g(x)=x^4+2m_2ux^2+4m_2ux+6m_2u$ with u an integer which satisfies $um_2\equiv 1 \pmod{16}$, we conclude that $\mathcal{B}=(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{g(\alpha)}{2A_4},\frac{\alpha g(\alpha)}{2A_5},\frac{\alpha^2 g(\alpha)}{2A_6},\frac{\alpha^3 g(\alpha)}{4A_7})$ is an integral basis of $\mathbb{Z}_K$.

ii. If $\nu_2(4-m)=4$; $m\equiv 20 \pmod{32}$, then $\omega_2(4-m)=16$ and $N_2(f)=T$ has a single side joining the points $(0,16)$, $(1,12)$, and $(2,8)$. Thus, $\mathrm{ind}_1(f)=4$ and $R_2(f)(y)=y^2+y+1$ is irreducible over $\mathbb{F}_2=\mathbb{F}_1=\mathbb{F}_0$ (because $\deg(\phi)=\deg(\psi_1)=1$). Hence , $f(x)$ is irreducible over $\mathbb{Q}_2$ and by Theorem 3.6 $\nu_2(\mathrm{ind}(f))=\mathrm{ind}_1(f)+4$. Based on the polygon $N_2(f)$, we conclude that $V(\phi_2(\alpha))=2$. Replacing $\phi_2(x)$ by x^4+2m_2u with an integer u satisfying $um_2\equiv 1 \pmod{16}$, we conclude that $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{\phi_2(\alpha)}{2A_4},\frac{\alpha\phi_2(\alpha)}{2A_5},\frac{\alpha^2\phi_2(\alpha)}{2A_6},\frac{\alpha^3\phi_2(\alpha)}{2A_7})$ is an integral basis of $\mathbb{Z}_K$.

iii. If $\nu_2(4-m)\geq 5$; $m\equiv 4 \pmod{32}$, then $\omega_2(4-m)\geq 20$ and $N_2(f)=T_1+T_2$ has two sides joining $(0,v)$, $(1,12)$, and $(2,8)$ with $v\geq 20$. Thus each side is of degree 1, and so $f(x)=F_1(x)F_2(x)$ with every $F_i(x)$ irreducible over $\mathbb{Q}_2$. Thus $\nu_2(\mathrm{ind}(f))=\mathrm{ind}_1(F_1)+\mathrm{ind}_1(F_2)+res_1(F_1,F_2)+\mathrm{ind}_2(F_1)+\mathrm{ind}_2(F_2)+res_2(F_1,F_2)=res_1(F_1,F_2)+res_2(F_1,F_2)=4+4=8$. Based on $N_2(f)$, we have $V(\phi_2(\alpha))\geq 2$, and so by replacing $\phi_2(x)$ by x^4+2m_2u with an integer u satisfying $um_2\equiv 1 \pmod{16}$, we conclude that
$(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{\alpha^4+2m_2u}{2A_4},\frac{\alpha^5+2m_2u\alpha}{2A_5},\frac{\alpha^6+2m_2u\alpha^2}{2A_6},\frac{\alpha^7+2m_2u\alpha^3}{2A_7})$ is an integral basis of $\mathbb{Z}_K$.
Note that the two cases (i) and (ii) could combined into one case, namely $\nu_2(4-m)\geq 4$.

(b) If $\nu_2(m)=4$; $m\equiv 16 \pmod{32}$, then for $\phi=x$, $\overline{f(x)}=\phi^8 \pmod 2$, $N_\phi(f)=S$ has a single side of slope $-1/2$, $R_1(f)(y)=y^4+1=(y+1)^4$. Let ω_2 be the valuation of second order Newton polygon defined by $\omega_2(a)=2\nu_2(a)$ for every $a\in\mathbb{Q}_2$ and $\omega_2(x)=1$. Let $\phi_2=x^2+2$ and $f(x)=\phi_2^4-8\phi_2^3+24\phi_2^2-32\phi_2+(16-m)$ the ϕ_2-expansion of $f(x)$. Since $m\equiv 16 \pmod{32}$, then $\nu_2(m-16)\geq 5$. It follows that:

i. If $\nu_2(16-m)=5$; $m\equiv 48 \pmod{64}$, then $N_2(f)=T$ has a single side joining the points $(0,10)$ and $(4,8)$ with slope $-1/2$, $\mathrm{ind}_2(f)=2$, and residual polynomial $R_2(f)(y)=(y+1)^2$. Let us use the third order Newton polygon associated to the data $t=(x,1/2,\phi_2,1/2,\phi_3)$, where $\phi_3=\phi_2^2(x)+4x=x^4+4x^2+4x+4$ is a key polynomial of ω_2 and let $\omega_3=2[\omega_2,1/2]$ be the valuation of third order Newton polygon; $\omega_3(a)=4\nu_2(a)$ for every $a\in\mathbb{Q}_2$, $\omega_3(x)=2$, and $\omega_3(\phi_2)=2(2+1/2)=5$. Let $f(x)=\phi_3^2+(8-8x^2-8x)\phi_3+(-m-48-16x^2-32x+32x^3)$ be the ϕ_3-expansion of $f(x)$. Since $m=48+64k$ for some integer k, $-m-48-16x^2-32x+32x^3=-16\phi_2(x)-64+64k-32x+32x^3$, and so $\omega_3(-m-48-16x^2-32x+32x^3)=\omega_3(16)+\omega_3(\phi_2)=21$. Thus $N_3(f)=T$ has a single side joining the points $(0,21)$ and $(2,20)$. It follows that its height is 1, $\mathrm{ind}_3(f)=0$ and $f(x)$ is irreducible over $\mathbb{Q}_2$. By Theorem 3.6 $\nu_2(\mathrm{ind}(f))=\mathrm{ind}_1(f)+\mathrm{ind}_2(f)=\mathrm{ind}_1(f)+2$. Based on $N_1(f)$, we have $V(\alpha)=1/2$ and based on $N_2(f)$, we get $V(\phi_2(\alpha))=5/4$. Replacing $\phi_2(x)$ by by x^2+2m_2u with $um_2\equiv 1 \pmod{16}$, we get $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{\alpha^4}{A_4},\frac{\alpha\phi_2^2(\alpha)}{2A_5},\frac{\alpha^6}{A_6},\frac{\alpha^3\phi_2^2(\alpha)}{2A_7})$ is an integral basis of $\mathbb{Z}_K$.

ii. If $\nu_2(16-m)=6$ ($m\equiv 80 \pmod{128}$), then $N_2(f)=T_2$ has a single side joining the points $(0,12)$ and $(4,8)$. Thus $\mathrm{ind}_2(f)=6$. As T is of degree 4 and $R_2(f)(y)=y^4+y^2+1=(y^2+y+1)^2$, we have to use third order Newton polygon techniques. Let ω_3 be the valuation of third order Newton polygon, $\phi_3=\phi_2^2+2x\phi_2+4x^2$ and $f(x)=\phi_3^2+(-(4x+12)\phi_2+16+24x)\phi_3+(-(128x+32)\phi_2+192x-m+80)$. Since $\omega_3(\phi_2)=3$, we conclude that $N_3(f)=T_3$ has a single side joining the points $(0,12)$ and $(2,13)$, which is of degree 1. Thus $\mathrm{ind}_3(f)=0$, $f(x)$ is irreducible over $\mathbb{Q}_2$ and by Theorem 3.6 $\nu_2(\mathrm{ind}(f))=\mathrm{ind}_1(f)+6$. Based on $N_1(f)$ and $N_2(f)$, we get $V(\alpha)=1/2$ and $V(\phi_2(\alpha))=3/2$. Replacing $\phi_2(x)$ by x^2+2m_2u by $um_2\equiv 1 \pmod{16}$, $V(\phi_2(\alpha))=3/2$ and $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha\phi_2(\alpha)}{2A_3},\frac{\phi_2^2(\alpha)}{2A_4},\frac{\alpha\phi_2^2(\alpha)}{2A_5},\frac{\alpha^2\phi_2^2(\alpha)}{2A_6},\frac{\alpha\phi_2^3(\alpha)}{4A_7})$ is an integral basis of $\mathbb{Z}_K$.

iii. If $\nu_2(16-m)=7$; $m\equiv 144 \pmod{256}$, then $\omega_2(16-m)=14$ and $N_2(f)=T_1+T_2$ has 2 sides joining the points $(0,14)$, $(1,12)$, $(2,10)$, and $(4,8)$. Thus $\text{ind}_2(f)=7$. Since the attached residual polynomials of $f(x)$ are $R_{12}(f)(y)=y^2+y+1$ and $R_{22}(f)(y)=(y+1)^2$, in order to complete the calculation of the index $\nu_2(\text{ind}(f))$, we have to use third order Newton polygon. Let $\phi_3=\phi_2+4x=x^2+4x+2$ be the key polynomial of ω_2, $\omega_3=[\omega_2,1]$ the valuation of third order Newton polygon; $\omega_3(a)=2\nu_2(a)$ for every $a\in\mathbb{Q}_2$, $\omega_3(x)=1$, and $\omega_3(\phi_2)=3$. Let $f(x)=\phi_3^4+(88-16x)\phi_3^3+(728-544x)\phi_3^2+(96-3776x)\phi_3-(6528x+m+3824)$ be the ϕ_3-expansion of $f(x)$. As $\omega_3((728-544x)\phi_3^2)=12$, $\omega_3((96-3776x)\phi_3)=13$, and $\omega_3(6528x+m+3824)=13$, $N_3^-(f)=T$ has a single side joining the points $(0,13)$ and $(2,12)$. Thus T is of height 1, $\text{ind}_3(f)=0$ and $f(x)$ is irreducible over $\mathbb{Q}_2$. By Theorem 3.6 $\nu_2(\text{ind}(f))=\text{ind}_1(f)+\text{ind}_2(f)=\text{ind}_1(f)+7$. Based on $N_1(f)$, $N_2(f)$, and $N_3(f)$, we get $V(\alpha)=1/2$ and $V(\phi_2(\alpha))\geq 3/2$. Let $\theta=\phi_2^3(\alpha)-8\phi_2^2(\alpha)+24\phi_2(\alpha)-32$. We need to show that $\frac{\theta}{2^5}\in\mathbb{Z}_K$. For this reason we have to show that $V(\theta)\geq 5$ for every valuation V of K extending ν_2. Since $N_2(f)$ has two sides of slopes -2 and -1, by Theorem 3.4, $f(x)=f_1(x)\times f_2(x)$ in $\mathbb{Z}_2[x]$ and there are two distinct valuations V_1 and V_2 of K extending ν_2 which satisfy $V_1(\phi_2(\alpha))=2$ and $V_2(\phi_2(\alpha))=3/2$. If $V(\phi_2(\alpha))=2$, then a simple verification shows that $V(\theta)\geq 0$. If $V(\phi_2(\alpha))=3/2$, as $f(\alpha)=0$, we have $\theta=\frac{m-16}{\phi_2(\alpha)}$, and so $V(\theta)=7-3/2\geq 5$. Hence $\frac{\theta}{2^5}\in\mathbb{Z}_K$ and $(1,\alpha,\frac{\alpha^2)}{2},\frac{\alpha\phi_2(\alpha)}{4},\frac{\phi_2^2(\alpha)}{8},\frac{\alpha\phi_2^2(\alpha)}{8},\frac{\theta}{32},\frac{\alpha\theta}{32})$ is a 2-integral basis of $\mathbb{Z}_K$. By replacing $\phi_2(x)$ by x^2+2m_2u with $m_2u\equiv 1 \pmod{32}$, we get $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha\phi_2(\alpha)}{2A_3},\frac{\phi_2^2(\alpha)}{2A_4},\frac{\alpha\phi_2^2(\alpha)}{2A_5},\frac{\theta}{4A_6},\frac{\alpha\theta}{4A_7})$ is an integral basis of $\mathbb{Z}_K$, where $\theta=\phi_2^3(\alpha)-8m_2u\phi_2^2(\alpha)+24m_2u\phi_2(\alpha)-32m_2u$.

iv. If $\nu_2(16-m)\geq 8$; $m\equiv 16 \pmod{256}$, then let $v=\omega_2(16-m)$, $\phi_2=x^2-2x+2$ and $f(x)=\phi_2^4+(16+8x)\phi_2^3+(-40+32x)\phi_2^2-32x\phi_2+(16-m)$ be the ϕ_2-expansion of $f(x)$. If $v\geq 9$, then $N_2(f)=T_1+T_2+T_3$ has 3 sides joining the points $(0,2v)$, $(1,13)$, $(2,10)$, and $(4,8)$. In this case $f(x)=F_1(x)\times F_2(x)\times F_3(x)$ with $F_1(x)$ and $F_2(x)$ irreducible over $\mathbb{Q}_2$. For $F_3(x)$, since its residual polynomial attached to T_3 is $R_2(f)(y)=(y+1)^2$, we have to use third order Newton polygon techniques. Let $\phi_3=\phi_2+2x=x^2+4x+2$ be the key polynomial of ω_2, ω_3 the valuation of third order Newton polygon and $f(x)=\phi_3^4+(88-16x)\phi_3^3+(728-544x)\phi_3^2+(96-3776x)\phi_3-(6528x+m+3824)$ the ϕ_3-expansion of $f(x)$. As $\omega_3((728-544x)\phi_3^2)=12$, $\omega_3((96-3776x)\phi_3)=13$ and $\omega_3(6528x+m+3824)=13$, $N_3^-(f)=T$ has a single side joining the points $(2,13)$ and $(2,12)$ with height 1. Thus $F_3(x)$ is irreducible over $\mathbb{Q}_2$ and $\text{ind}_3(f)=0$, $\nu_2(\text{ind}(f))=\text{ind}_1(f)+\text{ind}_2(f)=\text{ind}_1(f)+8$. Thus $\nu_2(\text{ind}(f))=\text{ind}_1(F_1)+\text{ind}_1(F_2)+\text{ind}_1(F_3)+res_1(F_1,F_2)+res_1(F_1,F_3)+res_1(F_2,F_3)+\text{ind}_2(F_1)+\text{ind}_2(F_2)+\text{ind}_2(F_3)+res_2(F_1,F_2)+res_2(F_1,F_3)+res_2(F_2,F_3)=0+0+1+1+2+2+0+0+2+2+2+2=\text{ind}_1(f)+8$. If $v=8$, then $N_2(f)=T_1+T_2$ has 2 sides joining the points $(0,16)$, $(1,13)$, $(2,10)$, and $(4,8)$. In this case $f(x)=F_1(x)\times F_2(x)$. Since the residual polynomial of $f(x)$ attached to T_1; $R_2(f)(y)=y^2+y+1$ is irreducible over $\mathbb{F}_2$, we conclude that $F_1(x)$ is irreducible over $\mathbb{Q}_2$. For $F_2(x)$, Since the attached residual polynomial of the last side is $R_2(f)(y)=(y+1)^2$, we have to use third order Newton polygon techniques. Let $\phi_3=\phi_2+2x=x^2+4x+2$ be the key polynomial of ω_2, ω_3 the valuation of third order Newton polygon, and $f(x)=\phi_3^4+(88-16x)\phi_3^3+(728-544x)\phi_3^2+(96-3776x)\phi_3-(6528x+m+3824)$ the ϕ_3-expansion of $f(x)$. As $\omega_3((728-544x)\phi_3^2)=12$, $\omega_3((96-3776x)\phi_3)=13$, and $\omega_3(6528x+m+3824)=13$, $N_3^-(f)=T$ has a single side joining the points $(2,13)$ and $(2,12)$ with height 1. In this case we have also $\nu_2(\text{ind}(f))=\text{ind}_1(f)+8$. Let V be a valuation of K extending ν_2. In both cases, based on $N_1(f)$ and $N_2(f)$, we get $V(\alpha)=1/2$ and $V(\phi_2(\alpha))\geq 3/2$. If $V(\phi_2(\alpha))\geq 5/2$, then $V(\phi_2^3(\alpha)+(16+8\alpha)\phi_2^2(\alpha)+(-40+32\alpha)\phi_2(\alpha)-32\alpha)\geq 11/2$, and so $V(\frac{\alpha\theta}{2^6}\geq 0$, where $\theta=\phi_2^3(\alpha)+(16+8\alpha)\phi_2^2(\alpha)+(-40+32\alpha)\phi_2(\alpha)-32\alpha$. If $V(\phi_2(\alpha))=3/2$, then $V(\frac{\phi_2^3(\alpha)+(16+8\alpha)\phi_2^2(\alpha)+(-40+32\alpha)\phi_2(\alpha)-32\alpha}{2^5})=V(\frac{16-m}{2^5\phi_2(\alpha)})\geq 8-5$. Thus $V(\frac{\theta}{2^5})\geq 0$ and $V(\frac{\alpha\theta}{2^6})\geq 0$ for every valuation V of K extending ν_2. Thus $(1,\alpha,\frac{\alpha^2}{2},\frac{\alpha\phi_2(\alpha)}{4},\frac{\phi_2^2(\alpha)}{8},\frac{\alpha\phi_2^2(\alpha)}{8},\frac{\theta}{32},\frac{\alpha\theta}{64})$ is a 2-integral basis of $\mathbb{Z}_K$. Replace $\phi_2(x)$ by x^2-

$2m_2ux+2m_2u$ with $m_2u\equiv 1 \pmod{64}$, we conclude that $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha\phi_2(\alpha)}{2A_3},\frac{\phi_2^2(\alpha)}{2A_4},\frac{\alpha\phi_2^2(\alpha)}{2A_5},\frac{\theta}{4A_6},\frac{\alpha\theta}{8A_7})$ is an integral basis of $\mathbb{Z}_K$, where $\theta=\phi_2^3(\alpha)+(16m_2u+8m_2u\alpha)\phi_2^2(\alpha)+(-40m_2u+32m_2u\alpha)\phi_2(\alpha)-32m_2u\alpha$.

(c) If $\nu_2(m)=6$; $m\equiv 64 \pmod{128}$, then for $\phi=x$, we have $\overline{f(x)}=\phi^8 \pmod 2$, $N_\phi(f)=S$ has a single side of slope $-\lambda_1=-3/4$, $e_1=4$, and $R_1(f)(y)=y^2+1=(y+1)^2$. Let ω_2 be the valuation of second order Newton polygon defined by $\omega_2(a)=e_1\nu_2(a)=4\nu_2(a)$ for every $a\in\mathbb{Q}_2$ and $\omega_2(x)=e_1\lambda_1=3$. It follows that:

i. If $\nu_2(m-64)=7$ ($m\equiv 192 \pmod{256}$), then there are two case:
If $\nu_2(m-192)=8$ ($m\equiv 448 \pmod{512}$), then for $\phi_2=x^4+4x^3+12x^2+24$, we have $f(x)=\phi_2^2+(-224-8x^3-8x^2+32x)\phi_2+(4800-m+512x^3+2304x^2-768x)$ is the ϕ_2-expansion of $f(x)$. As $\omega_2(\phi_2^2)=24$, $\omega_2((-224-8x^3-8x^2+32x)\phi_2)=30$, and $\omega_2(4800-m+512x^3+2304x^2-768x)=\omega_2(768x)=35$, we conclude that $N_2(f)$ has a single side of degree 1. Thus $f(x)$ is irreducible over $\mathbb{Q}_2$, $\text{ind}_2(f)=5$ and $\nu_2(\text{ind}(f))=\text{ind}_1(f)+5$. Since $V(\alpha)=3/4$ and $V(\phi_2(\alpha))=35/8$. By replacing $\phi_2(x)$ by $x^4+4um_2x^3+12um_2x^2+24um_2$ with $m_2u\equiv 1 \pmod{32}$, we get $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{\phi_2(\alpha)}{2A_4},\frac{\alpha\phi_2(\alpha)}{4A_5},\frac{\alpha^2\phi_2(\alpha)}{2A_6},\frac{\alpha^3\phi_2(\alpha)}{2A_7})$ is an integral basis of $\mathbb{Z}_K$.
If $\nu_2(m-192)\geq 9$ ($m\equiv 192 \pmod{512}$), then for $\phi_2=x^4+4x^2+8$, we have $f(x)=\phi_2^2-8x^2\phi_2-(64+m)$ is the ϕ_2-expansion of $f(x)$. As $\omega_2(\phi_2^2)=24$, $\omega_2(-8x^2\phi_2)=30$, and $\omega_2(64+m)=\omega_2(m-192)\geq 36$, if $\nu_2(m-192)=9$ ($\omega_2(m-192)=36$), then $N_2(f)$ has a single side with $R_2(f)(y)=y^2+y+1$, $f(x)$ is irreducible over $\mathbb{Q}_2$ and $\nu_2(\text{ind}(f))=\text{ind}_1(f)+6$.
If $\nu_2(m-192)\geq 10$, then $N_2(f)$ has 2 sides of degree 1 each. Thus $f(x)=F_1(x)\times F_2(x)$ with each F_i is irreducible over $\mathbb{Q}_2$. In this case we have also $\nu_2(\text{ind}(f))=\text{ind}_1(f)+6$. Since $V(\phi_2(\alpha))\geq 9/2$ and $V(\alpha)=3/4$, if we replace $\phi_2(x)$ by $x^4+4m_2ux+8m_2u$ with $um_2\equiv 1 \pmod{32}$, then $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{\phi_2(\alpha)}{2A_4},\frac{\alpha\phi_2(\alpha)}{4A_5},\frac{\alpha^2\phi_2(\alpha)}{4A_6},\frac{\alpha^3\phi_2(\alpha)}{2A_7})$ is an integral basis of $\mathbb{Z}_K$.

ii. If $\nu_2(m-64)\geq 8$ ($m\equiv 64 \pmod{256}$), then for $\phi_2=x^4+8$, we have $f(x)=\phi_2^2-16\phi_2+(64-m)$ is the ϕ_2-expansion of $f(x)$. Since $\omega_2(\phi_2^2)=24$, $\omega_2(16\phi_2)=28$, and $\omega_2(64-m)\geq 32$, it follows that if $\omega_2(64-m)=32$, then $N_2(f)$ has a single side with $R_2(f)(y)=y^2+y+1$. So $\nu_2(\text{ind}(f))=\text{ind}_2(f)+4$. If $\omega_2(64-m)>32$, then $N_2(f)$ has two side with degree 1 each. In this case, we have also $\nu_2(\text{ind}(f))=\text{ind}_2(f)+4$. In both cases we have $V(\alpha)=3/2$ and $V(\phi_2(\alpha))\geq 4$. Replacing ϕ_2 by $\phi_2=x^4+8um_2$ with $um_2\equiv 1 \pmod{32}$, we get $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{\phi_2(\alpha)}{2A_4},\frac{\alpha\phi_2(\alpha)}{2A_5},\frac{\alpha^2\phi_2(\alpha)}{2A_6},\frac{\alpha^3\phi_2(\alpha)}{2A_7})$ an integral basis of $\mathbb{Z}_K$.

2. If $m\equiv 1 \pmod 2$, then $f(x)\equiv (x-1)^8 \pmod 2$. Let $\phi=x-1$, $f(x)=\phi^8+8\phi^7+28\phi^6+56\phi^5+70\phi^4+56\phi^3+28\phi^2+8\phi+1-m$. It follows that:

(a) If $\nu_2(1-m)=1$; $m\equiv 3 \pmod 4$, then $N_\phi(f)=S$ has a single side joining $(0,1)$ and $(8,0)$. Thus $\nu_2(\text{ind}(f))=\text{ind}_\phi(f)=0$. It follows that $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha\phi_2(\alpha)}{A_3},\frac{\alpha^4}{A_4},\frac{\alpha^5}{A_5},\frac{\alpha^6}{A_6},\frac{\alpha^7}{A_7})$ is an integral basis of $\mathbb{Z}_K$.

(b) If $\nu_2(1-m)=2$; $m\equiv 5 \pmod 8$, then $N_\phi(f)=S_1$ has a single side joining $(0,2)$, $(4,1)$ and $(8,0)$ with residual polynomial $R_1(f)(y)=y^2+y+1$, which is irreducible over $\mathbb{F}_1=\mathbb{F}_0$. Thus $\nu_2(\text{ind}(f))=\text{ind}_1(f)=4$ and
$(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{\alpha^4+m^4}{2A_4},\frac{\alpha^5+m^4\alpha}{2A_5},\frac{\alpha^6+m^4\alpha^2}{2A_6},\frac{\alpha^7+m^4\alpha^3}{2A_7})$ is an integral basis of $\mathbb{Z}_K$.

(c) If $\nu_2(1-m)=3$; $m\equiv 9 \pmod{16}$, then $N_\phi(f)=S_1+S_2$ has 2 sides joining $(0,3)$, $(2,2)$, $(4,1)$, and $(8,0)$. Thus $R_{11}(f)(y)=y^2+y+1$ and $R_{21}(f)(y)=y+1$. It follows by Theorem 3.3 that $\nu_2(\text{ind}(f))=\text{ind}_1(f)=6$ and
$(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{\alpha^4+m^4}{2A_4},\frac{\alpha^5+m^4\alpha}{2A_5},\frac{\alpha^6+2m\alpha^5+3m^2\alpha^4+m\alpha^2+2m\alpha+3m^2}{4A_6},$
$\frac{\alpha^7+2m\alpha^6+3m^2\alpha^5+m\alpha^3+2m\alpha^2+3m^2\alpha}{4A_7})$ is an integral basis of $\mathbb{Z}_K$.

(d) If $\nu_2(1-m)=4$; $m\equiv 17 \pmod{32}$, then $N_\phi(f)=S_1+S_2+S_3$ has 3 sides joining $(0,4)$, $(1,3)$, $(2,2)$, $(4,1)$, and $(8,0)$. Thus $R_{11}(f)(y)=y^2+y+1$ and $R_{i1}(f)(y)=y+1$ for every $i=2,3$. It follows by Theorem 3.3 that $\nu_2(\mathrm{ind}(f))=\mathrm{ind}_1(f)=7$ and $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{\alpha^4+m^4}{2A_4},\frac{\alpha^5+m^4\alpha}{2A_5},\frac{\alpha^6-2m\alpha^5-m^2\alpha^4+m^2\alpha^2+2m\alpha+3m^2}{4A_6},$ $\frac{\alpha^7-m\alpha^6+m^2\alpha^5-m\alpha^4+m^2\alpha^3-m\alpha^2+(m^2+4m)\alpha+m}{8A_7})$ is an integral basis of $\mathbb{Z}_K$.

(e) If $\nu_2(1-m)\geq 5$; $m\equiv 1 \pmod{32}$, then $N_\phi(f)=S_1+S_2+S_3+S_4$ has 4 sides joining $(0,v)$, $(1,3)$, $(2,2)$, $(4,1)$, and $(8,0)$ with $v=\nu_2(1-m)\geq 5$. Thus $R_{i1}(f)(y)=y+1$ for every $i=1,2,3,4$. It follows by Theorem 3.3 that $\nu_2(\mathrm{ind}(f))=\mathrm{ind}_1(f)=7$ and $(1,\alpha,\frac{\alpha^2}{A_2},\frac{\alpha^3}{A_3},\frac{\alpha^4+m^4}{2A_4},\frac{\alpha^5+m^4\alpha}{2A_5},\frac{\alpha^6-2m\alpha^5-m^2\alpha^4+m^2\alpha^2+2m\alpha+3m^2}{4A_6},$ $\frac{\alpha^7-m\alpha^6+m^2\alpha^5-m\alpha^4+m^2\alpha^3-m\alpha^2+(m^2+4m)\alpha+m}{8A_7})$ is an integral basis of $\mathbb{Z}_K$.

□

Proof of Theorem 2.2.
Let α be a root of $f(x)=x^8-m$ as above, ζ a primitive eighth root of unity. The conjugates of α are $\alpha^{(1)}=\alpha,\alpha^{(2)}=\zeta\alpha,\dots,\alpha^{(7)}=\zeta^6\alpha,\alpha^{(8)}=\zeta^7\alpha$. For every $k=1,\dots,8$, let σ_k be the embedding of K defined by $\sigma_k(\alpha)=\zeta^k\alpha$. Then $\sigma_1,\sigma_2,\dots,\sigma_8$ are the embeddings of the number field K.

Let $L(x)=\alpha x_1+\alpha^2x_2+\alpha^3x_3+\alpha^4x_4+\alpha^5x_5+\alpha^6x_6+\alpha^7x_7$ and denote by $L^{(i)}(x)$ its conjugates, corresponding to $\alpha^{(i)}$ $(1\leq i\leq 8)$. Let

$$H_{ij}(x)=\frac{L^{(i)}(x)-L^{(j)}(x)}{\alpha^{(i)}-\alpha^{(j)}}$$

for $1\leq i<j\leq 8$. We have $\sigma(H_{ij}(x))=H_{\overline{i+1},\overline{j+1}}(x)$ where $\overline{i+1}=i+1$ for $1\leq i\leq 7$ and $\overline{i+1}=1$ for $i=8$, and similarly $\overline{j+1}$. Set

$$\begin{aligned}F_4(x)&=H_{15}(x)\cdot H_{26}(x)\cdot H_{37}(x)\cdot H_{48}(x),\\ F_8(x)&=H_{12}(x)\cdot H_{23}(x)\cdot H_{34}(x)\cdot H_{45}(x)\cdot H_{56}(x)\cdot H_{67}(x)\cdot H_{78}(x)\cdot H_{81}(x).\end{aligned}$$

Using symmetric polynomials these factors were explicitly calculated by using Maple [4] which showed that they have rational integer coefficients. (It also follows from the fact that these products remain fixed under any element of the Galois group of the normal closure of K.) These polynomials divide the index form

$$J(x_1,\dots,x_7)=\prod_{1\leq i<j\leq 8}|H_{ij}(x)|$$

of the basis $(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7)$ of K, which is also of integer coefficients. Denote by $F_{16}(x)$ the third factor of the above product. ($F_{16}(x)$ is of degree 16, since the index form has 28 factors.)

Therefore we obtain

$$J(x_1,\dots,x_7)=\pm F_4(x)\cdot F_8(x)\cdot F_{16}(x),$$

where the factors $F_4(x),F_8(x),F_{16}(x)$ have integer coefficients, of degrees 4, 8, 16, having 10, 169, 9185 terms, respectively.

If $\nu_2(m)$ is odd or $m\equiv 3 \pmod 4$, then $K=\mathbb{Q}(\sqrt[8]{m})$ has integral basis

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

Therefore

$$\sqrt{|D_K|}=\frac{\sqrt{|D(\alpha)|}}{A_2A_3A_4A_5A_6A_7}=\frac{\prod_{1\leq i<j\leq 8}|\alpha^{(i)}-\alpha^{(j)}|}{A_2A_3A_4A_5A_6A_7}.$$

Any algebraic integer $\vartheta\in\mathbb{Z}_K$ can be written as

$$\vartheta=\sum_{k=0}^{7}y_k\frac{\alpha^k}{A_k}=\frac{1}{A_7}\sum_{k=0}^{7}\frac{A_7}{A_k}y_k\alpha^k=\frac{1}{A_7}\sum_{k=0}^{7}z_k\alpha^k,$$

where $A_0=1$, A_7/A_k and y_k are integers, $z_k=\frac{A_7}{A_k}y_k$, $(k=0,1,\ldots,7)$. Hence

$$\begin{aligned}\mathrm{ind}(\vartheta) &= \frac{1}{\sqrt{|D_K|}}\prod_{1\le i<j\le 8}|\vartheta^{(i)}-\vartheta^{(j)}| \\ &= \frac{A_2A_3A_4A_5A_6A_7}{\prod_{1\le i<j\le 8}|\alpha^{(i)}-\alpha^{(j)}|}\cdot\frac{1}{A_7^{28}}\cdot\prod_{1\le i<j\le 8}(L^{(i)}(z)-L^{(j)}(z)) \\ &= \frac{A_2A_3A_4A_5A_6A_7}{A_7^{28}}\prod_{1\le i<j\le 8}\frac{L^{(i)}(z)-L^{(j)}(z)}{\alpha^{(i)}-\alpha^{(j)}}.\end{aligned}$$

We obtain

$$\mathrm{ind}(\vartheta)=\frac{A_2A_3A_4A_5A_6A_7}{A_7^{28}}\cdot F_4(z)\cdot F_8(z)\cdot F_{16}(z).$$

In $F_4(z),F_8(z),F_{16}(z)$ we substitute the representations of $A_2,\ldots,A_7$ and m in terms of $a_1,\ldots,a_7$. We extract the gcd-s W_4,W_8,W_{16} of the coefficients of $F_4(z),F_8(z),F_{16}(z)$, respectively, then we obtain

$$F_4(z)=W_4\cdot G_4(z),\ F_8(z)=W_8\cdot G_8(z),\ F_{16}(z)=W_{16}\cdot G_{16}(z),$$

where $G_4(z),G_8(z),G_{16}(z)$ are polynomials of $z_1,\ldots,z_7$ with integer coefficients, and

$$W_4W_8W_{16}=\frac{A_7^{28}}{A_2A_3A_4A_5A_6A_7}.$$

Therefore

$$\mathrm{ind}(\vartheta)=G_4(z)\cdot G_8(z)\cdot G_{16}(z).$$

Calculating explicitly $G_{16}(z)-a_2^2a_6^2G_8^2(z)$ we obtain

$$8a_1a_3a_5a_7|(G_{16}(z)-a_2^2a_6^2G_8^2(z)).$$

If K is monogenic, then for some $z_1,\ldots,z_7\in\mathbb{Z}$ we have $\mathrm{ind}(\vartheta)=1$. Hence $G_4(z)=\pm1,G_8(z)=\pm1,G_{16}(z)=\pm1$, that is the above divisibility relation implies

$$8a_1a_3a_5a_7|(a_2^2a_6^2\pm 1).$$

with at least one of the signs. □

The existence of prime common index divisors was first established in 1871 by Dedekind who exhibited examples in cubic number fields. For example, he considered the cubic field K generated by a root of x^3-x^2-2x-8 and he showed that the prime 2 splits completely in $\mathbb{Z}_K$. So, if we suppose that K is monogenic, then we would be able to find a cubic polynomial generating K, that splits completely into distinct polynomials of degree 1 in $\mathbb{F}_2[x]$. Since there are only 2 distinct polynomials of degree 1 in $\mathbb{F}_2[x]$, this is impossible. Based on these ideas and using Kronecker's theory of algebraic numbers, Hensel gave a necessary and sufficient condition on the so-called "index divisors" for any prime integer p to be a prime common index divisor [17].

In order to prove Theorem 2.3, we need the following two lemmas. The first one is an immediate consequence of Dedekind's theorem. The second one follows from [13, Corollary 3.8].

Lemma 4.1 *Let p be a rational prime integer and K a number field. For every positive integer f, let P_f be the number of distinct prime ideals of $\mathbb{Z}_K$ lying above p with residue degree f and N_f the number of monic irreducible polynomials of $\mathbb{F}_p[x]$ of degree f. If $P_f>N_f$ for some positive integer f, then p is a common index divisor of K.*

By Hensel's correspondence and [13, Corollary 3.3], the following Lemma allows to calculate the ramification index and the residue degree of each prime ideal of K lying above a prime integer p.

Lemma 4.2 *Let p be a prime integer, $f(x) \in \mathbb{Z}_p[x]$ a monic polynomial such that $\overline{f(x)}$ is a power of $\overline{\phi(x)}$ for some monic polynomial $\phi \in \mathbb{Z}_p[x]$, whose reduction is irreducible over $\mathbb{F}_p$, $N_i(f) = S_i$ has a single side of slope $-\lambda_i$ and $R_i(f)(y) = \psi_i^{a_i}(y)$ for some monic irreducible polynomial $\psi_i \in \mathbb{F}_i[y]$ for every $i = 1, \dots, r-1$. Let e_i be the smallest positive integer satisfying $e_i\lambda_i \in \mathbb{Z}$ for every $i = 1, \dots, r-1$. If $N_r(f) = T$ has a single side of degree 1, then $f(x)$ is irreducible over $\mathbb{Q}_p$. Let $\mathfrak{p}$ be the unique prime ideal of $\mathbb{Q}(\beta)$ lying above p, where β is a root of $f(x)$. Then $e(\mathfrak{p}/p) = e_1 \times \cdots \times e_r$ is the ramification index of $\mathfrak{p}$ and $f(\mathfrak{p}/p) = deg(\phi) \times \prod_{i=1}^{r-1} deg(\psi_i)$ is its residue degree.*

Proof of Theorem 2.3

1. If $m \equiv 1 \pmod{32}$, then $\overline{f(x)} = \overline{\phi(x)}^8 \pmod 2$ and $N_\phi(f) = S_1 + S_2 + S_3 + S_4$ has 4 sides joining $(0, v)$, $(1, 3)$, $(2, 2)$, $(4, 1)$, and $(8, 0)$, where $v = \nu_2(1-m)$. Thus each side is of degree 1, and so there are 4 prime ideals of $\mathbb{Z}_K$ lying above 2. Since there are only 2 monic irreducible polynomial of degree modulo 2. By Lemma 4.1, 2 divides $i(K)$, and so K is not monogenic.

2. If $\nu_2(16-m) \geq 8$; $m \equiv 16 \pmod{512}$, then $\overline{f(x)} = x^8$ and $N_1(f) = S$ has a single side of slope $-\lambda_1 = -1/2$ (see Figure 2). Then $e_1 = 2$ is the ramification index of S. Also for $\phi_2 = x^2 + 2$, we have $f(x) = \phi_2^4 - 8\phi_2^3 + 24\phi_2^2 - 32\phi_2 + 16 - m$. So, $N_2(f) = T_1 + T_2 + T_3$ has 3 sides joining the points $(0, v)$, $(1, 12)$, $(2, 10)$, and $(2, 8)$ (see Figue 3) with $v = \omega_2(16-m) \geq 16$, residual polynomials $R_{i2}(f)(y) = y+1$ for $i = 1, 2$ and $R_{32}(f)(y) = (y+1)^2$. By Theorem 3.4, $f(x) = F_1(x) \times F_2(x) \times F_3(x)$ in $\mathbb{Z}_2[x]$ where $F_i(x)$ is monic irreducible over $\mathbb{Q}_2$ for $i = 1, 2$ and $F_3(x)$ is monic. In order to complete the factorization of $F_3(x)$, we have to use third order Newton polygon. For $\phi_3 = \phi_2 + 4x = x^2 + 4x + 2$, we have $f(x) = \phi_3^4 + (88 - 16x)\phi_2^3 + (728 - 544x)\phi_2^2 + (96 - 3776x)\phi_2 - (m + 3824 + 6528x)$. So, $N_3^{(}F_3) = N_3^{-}(f) = U_1 + U_2$ has two sides joining $(0, 15)$, $(1, 13)$ and $(2, 12)$ (see Figure 4). Thus $F_3(x) = F_{31}(x)F_{32}(x)$ with each $F_{3i}(x)$ irreducible over $\mathbb{Q}_2$ for each $i = 1, 2$. By Hensel's correspondence, there are exactly 4 prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_{31}$ an $\mathfrak{p}_{32}$ of $\mathbb{Z}_K$ lying above 2. By Lemma 4.2, $e(\mathfrak{p}_i) = e_1 \times e_2 = 2$ for $i = 1, 2$ and $e(\mathfrak{p}_{3i}) = e_1 \times e_2 \times e_3 = 2$ for each $i = 1, 2$. We have also $f(\mathfrak{p}) = 1$ for each prime ideal factor $\mathfrak{p} \in \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_{31}, \mathfrak{p}_{32}\}$. As there are only two monic irreducible polynomial in $\mathbb{F}_0[x]$, 2 divides $i(K)$, and so K is not monogenic.

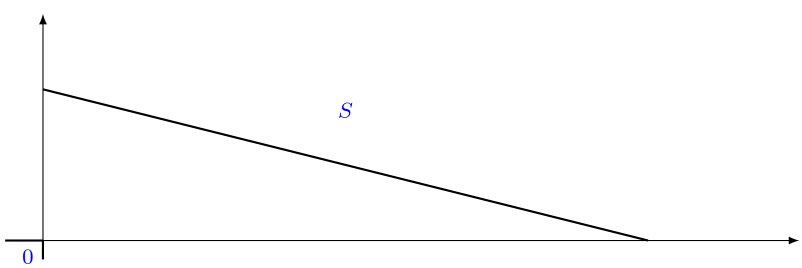

Figure 2: $N_1(f)$.

3. If $\nu_2(m)$ is odd, then by Theorem 2.2,

$$8a_1a_3a_5a_7 | (a_2^2a_6^2 \pm 1)$$

is a necessary condition for monogenity of K with at least one of the signs. Thus if $a_2a_6 \equiv 2 \pmod 8$ or $a_2a_6 \equiv 6 \pmod 8$, then $8a_1a_3a_5a_7$ does not divide $(a_2a_6)^2 \pm 1$ with neither of the signs. Thus K is not monogenic.

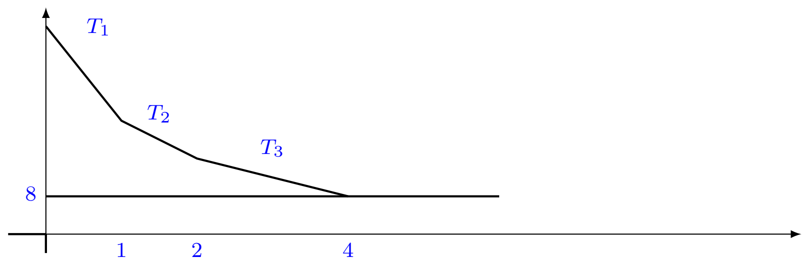

Figure 3: $N_2(f)$.

Figure 4: $N_3^-(f)$.

□

Proof of of Theorem 2.4
Assume that $m = a^t$ with $a \neq \pm 1$ is a square free rational integer and $t \in \{3, 5, 7\}$. Since $\gcd(t, 8) = 1$, let (u, v) be two non-negative integers solution of $tu - 8v = 1$ and $u < 8$ and $\theta = \frac{\alpha^u}{a^v}$. Since $\theta^8 = \frac{\alpha^{8u}}{a^{8v}} = \frac{m^u}{a^{8v}} = \frac{a^{tu}}{a^{8v}} = a$ and $x^8 - a$ is irreducible over $\mathbb{Q}$ (because it is an Eisenstein polynomial), hence $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha) = K$. Thus K is the octic number field generated by a root θ of $g(x) = x^8 - a$ with a square free integer a. Applying [12, Theorem 8], we get the following results:

1. If $a \not\equiv 1 \pmod 4$, then K is monogenic and $\mathbb{Z}_K$ is generated by θ.

2. If $a \equiv 1 \pmod 4$, then K is not monogenic, except for $a = -3$.

□

Acknowledgments

The authors are deeply grateful to the anonymous referee whose valuable comments and suggestions have tremendously improved the quality of this paper. Also, the first author is deeply grateful to Professor Enric Nart who introduced him to Newton polygon techniques when he was a post-doc at CRM of Barcelona (2007–2008).

References

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

2. S. Ahmad, T. Nakahara and S. M. Husnine, *Non-monogenesis of a family of pure sextic fields*, Arch. Sci. (Geneva) 65(7) (2012), 42.

3. S. Ahmad, T. Nakahara, and S. M. Husnine, *Power integral bases for certain pure sextic fields*, Int. J. of Number Theory 10(8) (2014), 2257– 2265.

4. B. W. Char, K. O. Geddes, G. H. Gonnet, M. B. Monagan, S. M. Watt (eds.), MAPLE, Reference Manual, Watcom Publications, Waterloo, Canada, 1988.

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

6. R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Göttingen Abhandlungen 23 (1878), 1–23.

7. L. El Fadil, *On Newton polygon techniques and factorization of polynomial over Henselian valued fields*, J. of Algebra and its Appl. 19(10) (2020), 2050188.

8. L. El Fadil, *On Power integral bases for certain pure sextic fields*, Bol. Soc. Parana. Math. (3) 40, paper No 143, 7p. (2022).

9. L. El Fadil, J. Montes E. Nart, *Newton polygons and p-integral bases of quartic number fields*, J. Algebra and Appl. 11(4)(2012), Article ID 1250073.

10. I.Gaál, Diophantine equations and power integral bases, Theory and algorithms, Second edition, Boston, Birkhäuser, 2019.

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

12. I. Gaál and L. Remete, *Power integral bases and monogenity of pure fields*, J. of Number Theory 173 (2017) 129–146.

13. J. Guardia, J. Montes and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. 364 (1) (2012) 361–416.

14. J. Guardia and E. Nart, *Genetics of polynomials over local fields*, Contemp. Math. 637 (2015), 207–241.

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

16. H. Hasse, Zahlentheorie, Akademie-Verlag, Berlin, 1963.

17. K. Hensel, *Arithemetishe untersuchungen uber die gemeinsamen ausserwesentliche Discriminantentheiler einer Gattung*, J. Reine Angew Math, 113 (1894), 128–160.

18. K. Hensel, Theorie der algebraischen Zahlen, Teubner Verlag, Leipzig, Berlin, 1908.

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

20. S. MacLane, *A construction for absolute values in polynomial rings*, Trans. Amer. Math. Soc. 40 (1936), 363–395.

21. J. Neukirch, Algebraic Number Theory, Springer-Verlag, Berlin, 1999.

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

Lhoussain El Fadil ,

Faculty of Sciences Dhar El Mahraz, P.O. Box 1796 Atlas-Fes, Sidi Mohamed ben Abdellah University, Morocco.

E-mail address: lhouelfadil2@gmail.com

and

István Gaál,

University of Debrecen, Mathematical Institute, H-4002 Debrecen Pf.400, Hungary.

E-mail address: gaal.istvan@unideb.hu