Palestine Journal of Mathematics

Vol 13(2)(2024) , 18–29

On integral bases and monogenity of certain pure number fields defined by $x^{p^r} - a$

Omar Kchit

Communicated by Ayman Badawi

MSC 2010 Classifications: 11R04, 11Y40, 11R21.

Keywords and phrases: Theorem of Dedekind, Theorem of Ore, Prime ideal factorization, Newton polygon, Index of a number field.

The author is deeply grateful to Professor István Gaál for his advice and encouragement, as well as for Professors Lhoussain El Fadil and Hanan Choulli for their help and encouragement.

Abstract Let $K = \mathbb{Q}(\alpha)$ be a pure number field generated by a root α of a monic irreducible polynomial $x^{p^r} - a \in \mathbb{Z}[x]$, where p is a rational prime and r is a positive integer. Let $\mathbb{Z}_K$ be the ring of integers of K. In this paper, we calculate an integral basis of $\mathbb{Z}_K$ and study the monogenity of K in some particular cases.

1 Introduction

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$, $\mathbb{Z}_K$ its ring of integers, $\Delta(F)$ the discriminant of $F(x)$, and d_K the absolute discriminant of K. It is well known that the ring $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, and so the Abelian group $\mathbb{Z}_K/\mathbb{Z}[\alpha]$ is finite. Its cardinal order is called the index of $\mathbb{Z}[\alpha]$ and denoted $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ or ind(α). A well known formula linking $\Delta(F)$, d_K, and ind(α) says that for every rational prime p, $\nu_p(\Delta(F)) = \nu_p(d_K) + 2\nu_p(\text{ind}(\alpha))$. If $\mathbb{Z}_K = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} + \cdots + \omega_n\mathbb{Z}$ for some $(\omega_1, \omega_2, \ldots, \omega_n) \in \mathbb{Z}_K^n$, then $\{\omega_1, \omega_2, \ldots, \omega_n\}$ is said to be an integral basis of $\mathbb{Z}_K$. If $\mathbb{Z}_K$ has an integral basis of the form $(1, \theta, \ldots, \theta^{n-1})$ for some $\theta \in \mathbb{Z}_K$, then $\mathbb{Z}_K$ is said to have a power integral basis and the field K is said to be monogenic. Otherwise, the field K is said to be not monogenic. In 1871, Dedekind was the first who gave an example of a non-monogenic number field ([6, § 5, page 30]). He considered the cubic field K generated by a root of $x^3 - x^2 - 2x - 8$ and showed that the rational prime 2 splits completely in 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 two distinct polynomials of degree 1 in $\mathbb{F}_2[x]$, this is impossible. Based on these ideas and using Kronecker's theory of algebraic number fields, Hensel gave necessary and sufficient condition on the so-called "index divisors of K" for any rational prime p to be a prime common index divisor [17]. The problem of determining an integral basis of $\mathbb{Z}_K$ and studying the monogenity of a number field K has been studied by several authors. Namely, Westlund calculated an integral basis of pure prime number fields of degree p (see [28]). In [9], Funakura, calculated integral bases and studied the monogenity of pure quartic number fields. In [14], Hameed and Nakahara showed that if $m \equiv 2, 3 \pmod 4$, then the octic number field generated by $m^{\frac{1}{8}}$ is monogenic. Also, in [15], Hameed et al. proved that if $m \equiv 1 \pmod 4$, then the octic number field generated by $m^{\frac{1}{8}}$ is not monogenic. In [10], by applying the explicit form of the index, Gaál and Remete obtained new results on monogenity of the number fields generated by $m^{\frac{1}{n}}$, where $3 \le n \le 9$. In [16], Hameed et al. studied the monogenity of pure number fields of degree 2^r. In [18], Jakhar reshowed Westlund's results. In [19], Jakhar et al. gave an integral bases of pure number fields in some particular cases. In [3], Ben Yakkou and El Fadil studied the monogenity of pure number fields of degree p^r with the square-free parameter. In [4] Ben Yakou and Kchit showed that if $m \not\equiv \pm 1 \pmod 9$, then the number fields defined by $x^{3^r} - m$ are monogenic, but these fields are not monogenic if $r \geq 3$ and $m \equiv \pm 1 \pmod{81}$. In [7], El Fadil and Gaál gave integral bases and studied the monogenity of pure octic number fields. In [26], under the regularity of polynomials, Remete gave explicitly an integral basis of the field $\mathbb{Q}(\sqrt[n]{m})$, where $m \neq \pm 1$ is square-free and $n \geq 2$. In [20], we studied the monogenity of pure number fields defined by $x^{p^r} - a$ in some particular cases. The main goal of this paper is to calculate an integral basis of any pure number field generated by a root α of a monic irreducible polynomial $F(x) = x^{p^r} - a$, with p a rational prime, r a positive integer and $a \in \mathbb{Z}$, and to study the monogenity of these number fields in some particular cases. In particular, our results generalize the previously given in [3, 4, 7, 9, 14, 15, 18, 19, 28].

2 Main results

Let $K = \mathbb{Q}(\alpha)$ be a pure number field generated by a root α of a monic irreducible polynomial $F(x) = x^{p^r} - a \in \mathbb{Z}[x]$, with p a fixed rational prime and r a positive integer. It is well known that up to replace α by $\frac{\alpha}{q^s}$, and so a by $\frac{a}{q^s}$, where s is the quotient of the Euclidean algorithm of $\nu_q(a)$ by p^r, we can assume that $\nu_q(a) < p^r$ for every rational prime q. In such a way, without loss of generality, we can assume that $a = \prod_{j=1}^{p^r-1} a_j^j$, with $a_1, \dots, a_{p^r-1}$ are square-free pairwise coprime integers. Let $\mathbb{Z}_K$ be the ring of integers of K and $C_i = \prod_{j=1}^{p^r-1} a_j^{\lfloor i\frac{j}{p^r}\rfloor}$ for $i = 1, \dots, p^r - 1$.
In Theorems 2.1 and 2.2, we give an integral basis of any number field defined by $F(x) = x^{p^r} - a \in \mathbb{Z}[x]$, and their proofs are slightly simpler than the proofs given by Jakhar et al. ([19]).

Theorem 2.1. $\mathcal{B}_1 = \left(1, \alpha, \frac{\alpha^2}{C_2}, \dots, \frac{\alpha^{p^r-1}}{C_{p^r-1}}\right)$ *is a $\mathbb{Z}$-integral basis of $\mathbb{Z}_K$ if and only if p divides a and p does not divide $\nu_p(a)$ or p does not divide a and $\nu_p(a^{p-1} - 1) = 1$.*

Theorem 2.2. *If p does not divide a and $\nu_p(a^{p-1} - 1) \geq 2$, then*

$$\mathcal{B}_2 = \left(1, \frac{q_i(\alpha)}{p^{\lfloor y_i \rfloor} C_{p^r-i}}, 1 \leq i \leq p^r - 1\right)$$

is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, where for every $0 \leq i \leq p^r$, $q_i(x)$ is the quotient upon to the Euclidean division of $F(x)$ by $\phi(x)^i = (x - a)^i$ and

(i) if $\nu_p(a^{p-1} - 1) = v \geq r + 2$, then

$$\lfloor y_i \rfloor = r - t_i - 1,$$

(ii) if $\nu_p(a^{p^r} - a) = v \leq r + 1$, then

$$\lfloor y_i \rfloor = \begin{cases} v - 1 & \text{if } \ i \leq p^{r-v+1}, \\ r - t_i - 1 & \text{if } \ i \geq p^{r-v+1}. \end{cases}$$

Where $t_i \in \{0, \dots, r - 1\}$ is the smallest positive integer such that $i - p^{t_i+1} \leq 0$ for every $i = 0, \dots, p^r$.

The following corollary characterizes when does $\mathbb{Z}_K = \mathbb{Z}[\alpha]$; that is when $\mathbb{Z}_K$ is generated by α and K is monogenic, unlike Gassert's results [11, Theorem 1.1], which give just one meaning and requires more details to reach our result.

Corollary 2.3. $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ *if and only if a is a square-free integer and $\nu_p(a^p - a) = 1$.*

The following theorem generalizes the result given in [3, Theorem 2.2], where a is a square-free rational integer was previously considered.

Theorem 2.4. *If p does not divide a and one of the following conditions holds:*

(i) $p \neq 2$, $r \geq p$ *and* $\nu_p(a^p - a) \geq p+1$,

(ii) $p = 2$, $r = 2$ *and* $\nu_2(a-1) \geq 4$,

(iii) $p = 2$, $r \geq 3$ *and* $\nu_2(a-1) \geq 5$,

then K *is not monogenic.*

3 Preliminaries

Newton polygon techniques is a standard method which is rather technical but very efficient to apply. We briefly describe the use of these techniques, which makes our proofs understandable. For more details, we refer to [8] and [12].
Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a root α of a monic irreducible polynomial $F(x) \in \mathbb{Z}[x]$. We shall use Dedekind's theorem [24, Chapter I, Proposition 8.3] relating the prime ideal factorization of $p\mathbb{Z}_K$ and the factorization of $F(x)$ modulo p (for rational primes p not dividing $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$). Also, we shall need Dedekind's criterion [5, Theorem 6.1.4] on the divisibility of $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ by rational primes.
For any rational 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. We keep the same notation for the Gauss's extension of ν_p to $\mathbb{Q}_p(x)$, which is defined on $\mathbb{Q}_p[x]$ by $\nu_p(\sum_{i=0}^{n} a_i x^i) = \min_i\{\nu_p(a_i)\}, a_i \in \mathbb{Q}_p$. Also, for nonzero polynomials, $P, Q \in \mathbb{Q}_p[x]$, we extend this valuation to $\nu_p(P/Q) = \nu_p(P) - \nu_p(Q)$. Let $\phi \in \mathbb{Z}_p[x]$ be a monic lift to an irreducible factor of $F(x)$ modulo p. Upon to the Euclidean division by successive powers of ϕ, there is a unique ϕ-expansion of $F(x)$; that is $F(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_l(x)\phi(x)^l$, where $a_i(x) \in \mathbb{Z}_p[x]$ and $\deg(a_i) < \deg(\phi)$. For every $i = 0, \ldots, l$, let $u_i = \nu_p(a_i(x))$. The ϕ-Newton polygon of $F(x)$ with respect to p, is the lower boundary convex envelope of the set of points $\{(i, u_i),\ a_i(x) \neq 0\}$ in the Euclidean plane, which we denote by $N_\phi(F)$. It is the process of joining the obtained edges $S_1, \ldots, S_t$ ordered by increasing slopes, which can be expressed as $N_\phi(F) = S_1 + \cdots + S_t$. For every side S_i of $N_\phi(F)$, its length $l(S_i)$ is the length of its projection to the x-axis and its height $h(S_i)$ is the length of its projection to the y-axis. We call $d(S_i) = \gcd(l(S_i), h(S_i))$ the degree of S_i. The polygon determined by the sides of the ϕ-Newton polygon with negative slopes is called the principal ϕ-Newton polygon of $F(x)$, and it is denoted by $N_\phi^+(F)$. As defined in [8, Def. 1.3], the ϕ-index of $F(x)$, denoted $\mathrm{ind}_\phi(F)$, is $\deg(\phi)$ multiplied by the number of points with natural integer coordinates that lie below or on the polygon $N_\phi^+(F)$, strictly above the horizontal axis, and strictly beyond the vertical axis. Let $\mathbb{F}_\phi$ be the field $\mathbb{F}_p[x]/(\overline{\phi})$, then to every side S of $N_\phi^+(F)$, with initial point (s, u_s), and every $i = 0, \ldots, l = l(S)$, let the residue coefficient $c_i \in \mathbb{F}_\phi$ be defined as

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

where $(p, \phi(x))$ is the maximal ideal of $\mathbb{Z}_p[x]$ generated by p and ϕ. Let $\lambda = -h/e$ be the slope of S, where h and e are two positive coprime integers and $l = l(S)$. Then $d = l/e$ is the degree of S. Since the points with integer coordinates lying on S are exactly $(s, u_s), (s+e, u_s - h), \ldots, (s+de, u_s - dh)$. Thus if i is not a multiple of e, then $(s+i, u_{s+i})$ does not lie on S, and so $c_i = 0$. Let $R_\lambda(F)(y) = t_d y^d + t_{d-1} y^{d-1} + \cdots + t_1 y + t_0 \in \mathbb{F}_\phi[y]$, called the residual polynomial of $F(x)$ associated to the side S, where for every $i = 0, \ldots, d$, $t_i = c_{s+ie}$. If $R_\lambda(F)(y)$ is square-free for each side of the polygon $N_\phi^+(F)$, then we say that $F(x)$ is ϕ-regular. Let $\overline{F(x)} = \prod_{i=1}^{r} \overline{\phi_i}^{l_i}$ be the factorization of $F(x)$ into powers of monic irreducible coprime polynomials over $\mathbb{F}_p$, we say that the polynomial $F(x)$ is p-regular if $F(x)$ is a ϕ_i-regular polynomial with respect to p for every $i = 1, \ldots, r$. Let $N_{\phi_i}^+(F) = S_{i1} + \cdots + S_{ir_i}$ be the ϕ_i-principal Newton polygon of $F(x)$ with respect to p. For every $j = 1, \ldots, r_i$, let $R_{\lambda_{ij}}(F)(y) = \prod_{s=1}^{s_{ij}} \psi_{ijs}^{a_{ijs}}(y)$ be the factorization of $R_{\lambda_{ij}}(F)(y)$ in $\mathbb{F}_{\phi_i}[y]$. Then we have the following theorem of index of Ore:

Theorem 3.1. (*Theorem of Ore*)
Under the above hypothesis, we have the following:

(i)

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

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

(ii) If $F(x)$ is p-regular, then

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

is the factorization of $p\mathbb{Z}_K$ into powers of prime ideals of $\mathbb{Z}_K$, where e_{ij} is the smallest positive integer satisfying $e_{ij}\lambda_{ij} \in \mathbb{Z}$ and the residue degree of $\mathfrak{p}_{ijs}$ over p is given by $f_{ijs} = \deg(\phi_i) \cdot \deg(\psi_{ijs})$ for every (i, j, s).

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

An alternative proof of the index theorem of Ore is proposed in [8]. The main advantage of that proposed proof is it gives an efficient method to calculate p-integral bases of $\mathbb{Z}_K$. We recall here how one can do it. Assume that $F(x) \equiv \prod_{i=1}^{t} \overline{\phi_i}^{l_i} \pmod p$ for some monic polynomials $\phi_i \in \mathbb{Z}[x]$ of degree m_i, whose reductions are irreducible over $\mathbb{F}_p$. We fix one of these polynomials $\phi(x) = \phi_i(x)$.
Let $F(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_l(x)\phi(x)^l$ be the ϕ-expansion of $F(x)$, $q_i(x)$ the quotient of the Euclidean division of $F(x)$ by $\phi^i(x)$. Then $q_1(x), \ldots, q_l(x)$ are obtained along the computation of the coefficients of the ϕ-expansion of $F(x)$:

$$\begin{array}{rcl} F(x) & = & \phi(x)q_1(x) + a_0(x), \\ q_1(x) & = & \phi(x)q_2(x) + a_1(x), \\ \vdots & & \vdots \\ q_l(x) & = & \phi(x)\cdot 0 + a_l(x) = a_l(x). \end{array}$$

Let $r_i(x)$ be the residue of the Euclidean division of $F(x)$ by $\phi(x)^i$. Thus, for every $i = 1, \ldots, l$, we have:

$$F(x) = r_i(x) + q_i(x)\phi(x)^i,$$

$$r_i(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_{i-1}(x)\phi(x)^{i-1},$$

$$q_i(x) = a_i(x) + a_{i+1}(x)\phi(x) + \cdots + a_l(x)\phi(x)^{l-i}.$$

Let $N^+_{\phi_i}(F) = S_1 + \cdots + S_{t_i}$, with $l_i = l(N^+_{\phi_i}(F))$. For every integer abscissa $j = 0, \ldots, l_i$, let $y_{ij} \in \mathbb{Q}$ be the ordinate of the point $N \in N^+_{\phi_i}(F)$ of abscissa j. Then we have the following theorem:

Theorem 3.3. *([8, Theorem 2.7])*
If $F(x)$ is p-regular, then the family
$\left\{q_{ij}(\alpha)\alpha^k/p^{\lfloor y_{ij}\rfloor},\ 1 \leq i \leq t,\ 1 \leq j \leq l_i,\ 0 \leq k \leq m_i\right\}$ *is a p-integral basis of $\mathbb{Z}_K$.*

In what follows, we obtain

$$\nu_p(\text{ind}(\alpha)) \geq \sum_{i=1}^{t} \text{ind}_{\phi_i}(F) = \sum_{i=1}^{t}\left(m_i \cdot \sum_{j=1}^{l_i} \lfloor y_{ij} \rfloor\right).$$

Our method is based on calculating a q-integral basis for every rational prime q dividing $\Delta(F)$. Once the q-integral bases are calculated for every rational prime q dividing $\Delta(F)$, the following theorem allows to recover an integral basis of $\mathbb{Z}_K$ from the q-integral bases (see for instance [1, Theorem 1.3.6]) by applying: $\nu_q(\text{ind}(\alpha)) = \sum_{i=1}^{t} \text{ind}_{\phi_i}(F)$ if and only if $\text{ind}_2(F) = 0$ for every $i = 1, \ldots, t$.

Theorem 3.4. *([1, Theorem 1.3.6])*
Let $K = \mathbb{Q}(\alpha)$ be the number field generated by α a root of a monic ireductible polynomial $F(x) \in \mathbb{Z}[x]$ of degree n. Let $p_1, p_2, \dots, p_s$ be the distinct rational prime integers dividing $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ and

$$\left\{1, \frac{x_{r0}^{(1)} + \alpha}{p_r^{k_{r1}}}, \frac{x_{r0}^{(2)} + x_{r1}^{(2)}\alpha + \alpha^2}{p_r^{k_{r2}}}, \dots, \frac{x_{r0}^{(n-1)} + x_{r1}^{(n-1)}\alpha + \dots + x_{r\,n-2}^{(n-1)}\alpha^{n-2} + \alpha^{n-1}}{p_r^{k_{r\,n-1}}}\right\}$$

a p_r-integral basis of K for every $r = 1, 2, \dots, s$. Define the integers $X_i^{(j)}$ $(i = 1, 2, \dots, j-1; j = 1, 2, \dots, n-1)$ by

$$X_i^{(j)} \equiv x_{ri}^{(j)} \ (mod\ p_r^{k_{rj}}) \qquad (r = 1, 2, \dots, s),$$

and let

$$T_j = \prod_{r=1}^{s} p_r^{k_{rj}} \quad (j = 1, 2, \dots, n-1).$$

Then

$$\left\{1, \frac{X_0^{(1)} + \alpha}{T_1}, \frac{X_0^{(2)} + X_1^{(2)}\alpha + \alpha^2}{T_2}, \dots, \frac{X_0^{(n-1)} + X_1^{(n-1)}\alpha + \dots + X_{n-2}^{(n-1)}\alpha^{n-2} + \alpha^{n-1}}{T_{n-1}}\right\}$$

is an integral basis of $\mathbb{Z}_K$.

Recall that the requirement, $F(x)$ is p-regular is only a sufficient condition to have equality in theorem of index of Ore and not necessarily.

If a factor of $F(x)$ provided by Hensel's lemma and refined by Newton polygon (in the context of Ore program) is not irreducible over $\mathbb{Q}_p$, then in order to complete the factorization of $F(x)$ in $\mathbb{Q}_p[x]$, Guardia, Montes, and Nart introduced the notion of higher order Newton polygon [12]. They showed, thanks to a theorem of index [12, Theorem 4.18], that after a finite number of iterations, the process provides all monic irreducible factors of $F(x)$, all prime ideals of $\mathbb{Z}_K$ lying above a rational prime p, the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$, and the absolute discriminant of K. We recall some fundamental techniques of Newton polygon of high order. For more details, we refer to [12] and [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, with $H = \prod_{i=0}^{r-2} f_i$ and $f_i = \deg(\psi_i(x))$, satisfying the following recursive properties:

(0) $\mathbb{F}_0$ is the finite field of p elements.

(1) $g_1(x)$ is irreducible modulo p, $\psi_0(y) \in \mathbb{F}_0[y]$ $(\mathbb{F}_0 = \mathbb{F}_p)$ is the polynomial obtained by reducing $g_1(x)$ 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 side of slope $-\lambda_i$.

(3) For every $i = 1, \dots, r-1$, the residual polynomial of i^{th} order, $R_i(g_{i+1})(y) = \psi_i(y) \in \mathbb{F}_i[y]$ is a monic irreducible polynomial in $\mathbb{F}_i[y]$, and $\mathbb{F}_{i+1} = \mathbb{F}_i[y]/(\psi_i(y))$.

(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 $\mathbb{F}_r = \mathbb{F}_{r-1}[y]/(\psi_{r-1}(y))$.

Thus, $\mathbb{F}_0 \subset \mathbb{F}_1 \subset \dots \subset \mathbb{F}_r$ is a tower of finite fields, here the field $\mathbb{F}_i$ should not be confused with the finite field of i elements. 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 $\mathbb{F}_i[y]$, and by the theorem of the product in order i, the polynomial $g_i(x)$ is irreducible in $\mathbb{Z}_p[x]$. Let $\omega_0 = [\nu_p, x, 0]$ be the Gauss's extension of ν_p to $\mathbb{Q}_p(x)$. According to MacLane's terminology ([21]), g_{i+1} is a key polynomial of ω_i, and it induces a valuation on $\mathbb{Q}_p(x)$, denoted by $\omega_{i+1} = e_i[\omega_i, g_i, \lambda_i]$, 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 and λ_i and defined over $\mathbb{Q}_p[x]$ as

$$\omega_{i+1}(F(x)) = \min\left\{e_i\omega_i(a_j^i(x)) + j(e_i\omega_i(g_i) + h_i),\ j = 0, \dots, n_i\right\}, \tag{3.1}$$

where $F(x) = \sum_{j=0}^{n_i} a_j^i(x) g_i^j(x)$ is the g_i-expansion of $F(x)$. According to the terminology in [12], 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 is the lower boundary convex envelope of the set of points $\{(i, \mu_i), i = 0, \dots, n_r\}$ in the Euclidean plane, where $\mu_i = \omega_r(a_i^r(x) g_r^i(x)))$. The relevant theorems from Montes-Guardia-Nart's work are theorem of the product, theorem of the polygon and theorem of the residual polynomial in high order Newton polygon (see [12, Theorems 2.26, 3.1, 3.7]).

4 Proofs of main results

Proof. (**of Theorem** 2.1.)
Since $\Delta(F) = \pm p^{rp^r} \cdot a^{p^r-1}$ is the discriminant of $F(x)$ and thanks to the formula linking $\Delta(F)$, d_K, and $\text{ind}(\alpha)$, we need to calculate a q-integral basis of $\mathbb{Z}_K$ for every rational prime q such that $q = p$ or q divides a.

(i) If q divides a and $q \neq p$, then $F(x) \equiv x^{p^r} \pmod{q}$. Let $\phi = x$. Then $N_\phi(F) = S_1$ has a single side of slope $-\lambda_1 = \frac{-\nu_q(a)}{p^r}$, length $l = p^r$, and $\text{ind}_1(F) = \text{ind}_\phi(F) = \sum_{i=1}^{p^r-1} \lfloor i\frac{i\nu_q(a)}{p^r} \rfloor$. By [12, Theorem 4.18], $\nu_q((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \text{ind}_1(F)$ if and only if $\text{ind}_2(F) = 0$, where $\text{ind}_2(F)$ is the index of the second order of Newton polygon.

a. If $\gcd(p, \nu_q(a)) = 1$, then $d(S_1) = 1$; that is $R_{\lambda_1}(F)(y)$ is irreducible, and so by Theorem 3.3, $\nu_q(\text{ind}(\alpha)) = \text{ind}_\phi(F) = \sum_{j=0}^{p^r-1} \lfloor y_j \rfloor = \sum_{j=1}^{p^r-1} \lfloor \frac{(p^r-j)\nu_q(a)}{p^r} \rfloor$.

b. If p divides $\nu_q(a)$, then let $t = \nu_p(\nu_q(a))$, $e = p^{r-t}$, and $d(S_1) = p^t$ is the degree of S_1. Thus $R_{\lambda_1}(F)(y) = y^{p^t} - a_q \in \mathbb{F}_\phi[y]$, where $a_q \equiv \frac{a}{q^{\nu_q(a)}} \pmod{(q, \phi(x))}$. As $p \neq q$, $R_{\lambda_1}(F)(y)$ is separable over $\mathbb{F}_\phi$, and so by Theorem 3.3, $\nu_q(\text{ind}(\alpha)) = \text{ind}_\phi(F) = \sum_{j=1}^{p^r-1} \lfloor y_j \rfloor = \sum_{j=1}^{p^r-1} \lfloor \frac{(p^r-j)\nu_q(a)}{p^r} \rfloor$.

In both cases, $F(x)$ is q-regular. By Theorem 3.3, $\left(\frac{q_j(\alpha)}{q^{\lfloor y_j \rfloor}}, j = 1, \dots, p^r\right)$ is a q-integral basis of $\mathbb{Z}_K$, where $\lfloor y_j \rfloor = \lfloor \frac{p^r-j}{p^r}\nu_q(a) \rfloor$ for every $j = 1, \dots, p^r$ and $\lfloor y \rfloor$ is the integral part of y; the greatest integer b satisfying $b \leq y$. Thus

$$\left(1, \frac{\alpha}{q^{\lfloor \frac{\nu_q(a)}{p^r} \rfloor}}, \frac{\alpha^2}{q^{\lfloor \frac{2\nu_q(a)}{p^r} \rfloor}}, \dots, \frac{\alpha^{p^r-1}}{q^{\lfloor \frac{(p^r-1)\nu_q(a)}{p^r} \rfloor}}\right) \text{ is a } q\text{-integral basis of } \mathbb{Z}_K.$$

(ii) If $q = p$, then we have the following cases:

a. If p divides a, then $F(x) \equiv x^{p^r} \pmod{p}$. Let $\phi = x$. Then $N_\phi(F) = S_1$ joining $(0, \nu_p(a))$ and $(p^r, 0)$. Thus $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) \geq \text{ind}_\phi(F)$. More precisely, if p divides a and p does not divide $\nu_p(a)$, then $d(S_1) = 1$, and so its attached residual polynomial is irreducible. Therefore $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = \text{ind}_\phi(F)$ and

$$\left(1, \frac{\alpha}{p^{\lfloor \frac{\nu_p(a)}{p^r} \rfloor}}, \frac{\alpha^2}{p^{\lfloor \frac{2\nu_p(a)}{p^r} \rfloor}}, \dots, \frac{\alpha^{p^r-1}}{p^{\lfloor \frac{(p^r-1)\nu_p(a)}{p^r} \rfloor}}\right)$$

is a p-integral basis of $\mathbb{Z}_K$.
If p divides $\nu_p(a)$, then by Remark 4.1, $\nu_p((\mathbb{Z}_K : \mathbb{Z}[\alpha])) > \text{ind}_\phi(F)$ and

$$\left(1, \frac{\alpha}{p^{\lfloor \frac{\nu_p(a)}{p^r} \rfloor}}, \frac{\alpha^2}{p^{\lfloor \frac{2\nu_p(a)}{p^r} \rfloor}}, \dots, \frac{\alpha^{p^r-1}}{p^{\lfloor \frac{(p^r-1)\nu_p(a)}{p^r} \rfloor}}\right)$$

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

b. If p does not divide a, then $F(x) \equiv x^{p^r} - a \pmod{p} \equiv (x-a)^{p^r} \pmod{p}$. Let $\phi = x - a$. Then

$$\begin{array}{rcl} F(x) & = & (x-a+a)^{p^r} - a \\ & = & \sum_{k=0}^{p^r} \binom{p^r}{k} a^k \phi^{p^r-k} - a \\ & = & \phi^{p^r} + \binom{p^r}{1} a\phi^{p^r-1} + \cdots + \binom{p^r}{p^r-1} a^{p^r-1}\phi + a^{p^r} - a \end{array} \tag{4.1}$$

If $\nu_p(a^{p-1}-1) = 1$, then $N_\phi(F) = S_1$ has a single side of height 1. Hence, by Corollary 3.2, $\nu_p(\mathrm{ind}(\alpha)) = 0$.

We conclude, using Theorem 2.1, that $\left(1, \alpha, \frac{\alpha^2}{C_2}, \ldots, \frac{\alpha^{p^r-1}}{C_{p^r-1}}\right)$ is a $\mathbb{Z}$-integral basis of $\mathbb{Z}_K$ if and only if p divides a and p does not divide $\nu_p(a)$ or p does not divide a and $\nu_p(a^{p-1}-1) = 1$.

□

Remark 4.1. If p divides $\nu_p(a)$, then a natural question is "**under which conditions we get** $\nu_p(\mathrm{ind}(\alpha)) = \mathrm{ind}_\phi(F)$**, and so** $\mathcal{B}_1$ **is an integral basis of** $\mathbb{Z}_K$ **?** The answer is negative, that means if p divides $\nu_p(a)$, then $\mathrm{ind}_2(F) \geq 1$. For this reason, let $\nu_p(a) = bp^s$, with $\nu_p(b) = 0$ and $s < r$. Thus $a = p^{bp^s} \cdot A$ such that p does not divide A. Then $F(x) = x^{p^r} - p^{bp^s} A \equiv x^{p^r} \pmod{p}$. Let $\phi(x) = x$. Then $N_\phi(F) = S_1$ joining $(0, bp^s)$ and $(p^r, 0)$ (see Figure 1), with slope $-\lambda_1 = \frac{-b}{p^{r-s}}$. Its attached residual polynomial is $R_{\lambda_1}(F)(y) = y^{p^s} - A = (y-A)^{p^s} \in \mathbb{F}_\phi[y]$. In this case, we have to use second order Newton polygon.

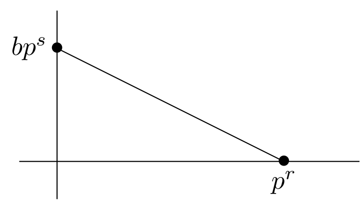

Figure 1. $N_\phi(F)$

Let us take the example $s = 1$. Let $\mathbf{t} = (x, \lambda_1, \psi_1)$, with $\psi_1 = y - A$. We have also $f_1 = m_1 = 1$ and $e_1 = p^{r-1}$ are the data of first order Newton polygon. Let $\omega_2 = p^{r-1}[\nu_p, \phi, b/p^{r-1}]$ be the valuation of second order Newton polygon and $g_2 = x^{p^{r-1}} - p^b A$ the key polynomial of ω_2, where $[\nu_p, \phi, b/p^{r-1}]$ is the augmented valuation of ν_p with respect to ϕ and $\lambda_1 = b/p^{r-1}$. Let

$$F(x) = g_2^p + \sum_{k=1}^{p-1} \binom{p}{k} (p^b A)^{p-k} g_2^k + p^{bp}(A^p - A)$$

be the g_2-expansion of $F(x)$. By (3.1), we have $\omega_2(x) = 1, \omega_2(g_2) = bp^{r-1}, \omega_2\left(\binom{p}{k} g_2^k (p^b A)^{p-k}\right) = bp^r + p^{r-1}$, and $\omega_2(p^{bp}(A^p - A)) \geq bp^r + p^{r-1}$. Hence, according to $\nu_p(A^p - A) = 1$ or $\nu_p(A^p - A) \geq 2$, the Newton polygon of second order is given by the following figure (Figure 2):

In both cases $\mathrm{ind}_2(F) \geq m_1 \cdot f_1 \cdot \mathrm{ind}(N_2(F))$ and $\mathrm{ind}(N_2(F)) \geq 1$ because its length is $p^{r-1} \geq 2$ and its height is greater than $e_1 \geq 2$.

Proof. (**of Theorem** 2.2)
In order to prove this theorem we need to calculate a p-integral basis when p does not divide a and $\nu_p(a^{p-1}-1) \geq 2$, and then collect it with the other q-integral bases when $q \neq p$ divides a, found in the proof of Theorem 2.1.

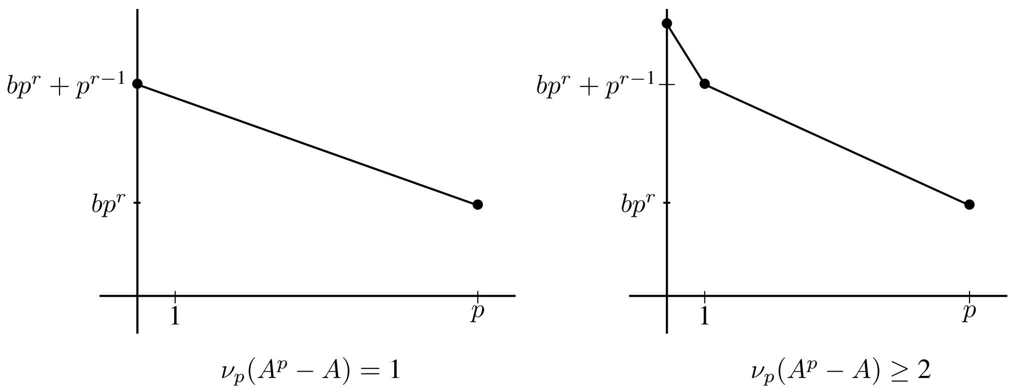

Figure 2. $N_2(F)$

p does not divide a implies that $F(x) \equiv x^{p^r} - a \pmod{p} \equiv (x-a)^{p^r} \pmod{p}$. Let $\phi = x - a$ as the lift to $\mathbb{Z}[x]$ to the irreducible factor of $F(x)$ modulo p. Then

$$\begin{array}{rcl} F(x) & = & (x-a+a)^{p^r} - a, \\ & = & \sum_{k=0}^{p^r} \binom{p^r}{k} a^k \phi^{p^r-k} - a, \\ & = & \phi^{p^r} + \binom{p^r}{1} a \phi^{p^r-1} + \cdots + \binom{p^r}{p^r-1} a^{p^r-1}\phi + a^{p^r} - a, \end{array}$$

Let $v = \nu_p(a^{p-1} - 1)$, then the number of sides of the Newton polygon depends on v. Two cases arise:

(i) If $v \geq r+2$, then $N_\phi^+(F) = S_1 + \cdots + S_{r+1}$ has $r+1$ sides joining $(0, v)$, $(1, r)$, $(p, r-1), \ldots, (p^{r-1}, 1)$, and $(p^r, 0)$. Thus every side has degree 1 (see Figure 3, $v \geq r+2$). So, for every $i = 1, \ldots, r+1$, the residual polynomial $R_{\lambda_i}(F)(y)$ attached to S_i is irreducible over $\mathbb{F}_\phi$ as it is of degree 1. Hence $F(x)$ is p-regular, and by Theorem 3.3,

$$\left(\frac{q_i(\alpha)}{p^{\lfloor y_i \rfloor}}, 1 \leq i \leq p^r \right),$$

is a p-integral basis of $\mathbb{Z}_K$, with $\lfloor y_i \rfloor = r - t_i - 1$, where $t_i \in \{0, \ldots, r-1\}$ is the smallest positive integer such that $i - p^{t_i+1} \leq 0$ for every $i = 0, \ldots, p^r$. Since $q_{p^r}(x) \in \mathbb{Z}$ and $\lfloor y_{p^r} \rfloor = 0$, then

$$\left(1, \frac{q_i(\alpha)}{p^{\lfloor y_i \rfloor}}, 1 \leq i \leq p^r - 1 \right),$$

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

Likewise, let $p_1, \ldots, p_s$ be the distinct rational primes whose dividing a. So, for every $j = 1, \ldots, s$

$$\left(1, \frac{\alpha}{p_j^{\lfloor \frac{t_j}{p^r} \rfloor}}, \frac{\alpha^2}{p_j^{\lfloor \frac{2t_j}{p^r} \rfloor}}, \ldots, \frac{\alpha^{p^r-1}}{p_j^{\lfloor \frac{(p^r-1)t_j}{p^r} \rfloor}} \right) \text{ is a } p_j\text{-integral basis of } \mathbb{Z}_K.$$

By Theorem 3.4, we get that

$$\left(1, \frac{q_i(\alpha)}{p^{\lfloor y_i \rfloor} C_{p^r-i}}, 1 \leq i \leq p^r - 1 \right),$$

is a $\mathbb{Z}$-basis of K, with $q_i(\alpha)$ and $\lfloor y_i \rfloor$ are defined above.

(ii) If $v \leq r+1$, then two cases arise.

a. If $p \neq 2$, then $N_\phi(F) = S_1 + \cdots + S_v$ has v sides joining $(0, v)$, $(p^{r-v+1}, v-1), \ldots, (p^{r-1}, 1)$, and $(p^r, 0)$. Thus every side has degree 1 (see Figure 3, $v \leq r+1$). So, for every $i = 1, \ldots, v$, $R_{\lambda_i}(F)(y)$ is irreducible over $\mathbb{F}_\phi$ as it is of degree 1.

b. If $p=2$, $N_\phi(F) = S_1+\cdots+S_{v-1}$ has $v-1$ sides joining $(0,v)$, $(p^{r-v+2}, v-2)$, $(p^{r-v+3}, v-3), \dots, (p^{r-1}, 1)$, and $(p^r, 0)$ with $d(S_i)=1$ for every $i=2,\dots v$, and the residual polynomial attached to S_1 is $R_{\lambda_1}(F)(y) = y^2+y+1$ which is irreducible over $\mathbb{F}_\phi$.

In both cases $F(x)$ is p-regular, and by Theorem 3.3,

$$\left(1, \frac{q_i(\alpha)}{p^{\lfloor y_i \rfloor}}, 1 \le i \le p^r-1\right) \text{ is a } p\text{-integral basis of } \mathbb{Z}_K,$$

$$\text{with } \lfloor y_i \rfloor = \begin{cases} v-1 & \text{if } \ i \le p^{r-v+1}, \\ r-t_i-1 & \text{if } \ i \ge p^{r-v+1}, \end{cases}$$

where $t_i \in \{0,\dots,r-1\}$ is the smallest positive integer such that $i - p^{t_i+1} \le 0$ for every $i = 0,\dots,p^r$. Using the same process, we get that

$$\left(1, \frac{q_i(\alpha)}{p^{\lfloor y_i \rfloor} C_{p^r-i}}, 1 \le i \le p^r-1\right),$$

is a $\mathbb{Z}$-basis of K, with the $q_i(\alpha)$ and the $\lfloor y_i \rfloor$ are defined above.

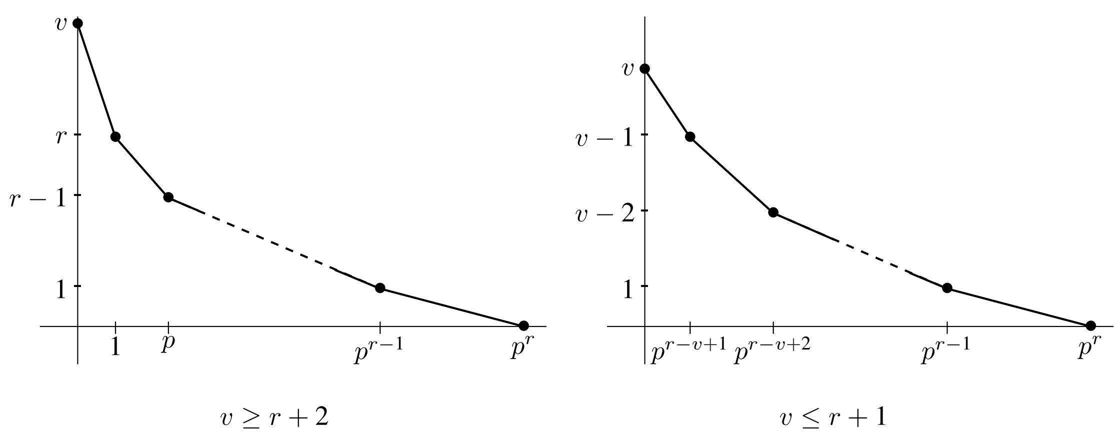

Figure 3. $N_\phi^+(F)$

□

Proof. (**of Corollary** 2.3)
According to the bases given in Theorems 2.1 and 2.2, we conclude that $\mathbb{Z}[\alpha]$ is the ring of integers of K if and only if $\nu_p(a^p-a)=1$ and $C_i=1$ for every $i=2,\dots,p^r-1$, which means that $\nu_p(a^p-a)=1$ and a is square-free. □

The index of a number field K is defined by

$$i(K) = \gcd\{(\mathbb{Z}_K : \mathbb{Z}[\theta]) \mid K = \mathbb{Q}(\theta) \text{ and } \theta \in \mathbb{Z}_K\}.$$

A rational prime p dividing $i(K)$ is called a prime common index divisor of K. If $\mathbb{Z}_K$ has a power integral basis, then $i(K)=1$. Therefore a field having a prime common index divisor is not monogenic.

For the proof of Theorem 2.2, we need the following lemma, which characterizes the rational primes dividing $i(K)$.

Lemma 4.2. (*[27, Theorem 2.2]*)
Let p be a rational prime and K a number field. For every positive integer f, let $\mathcal{P}_f$ be the number of distinct prime ideals of $\mathbb{Z}_K$ lying above p with residue degree f and $\mathcal{N}_f$ the number of monic irreducible polynomials of $\mathbb{F}_p[x]$ of degree f. Then p divides the index $i(K)$ if and only if $\mathcal{P}_f > \mathcal{N}_f$ for some positive integer f.

Remark 4.3. In order to prove Theorem 2.4 we do not need to determine the factorization of $p\mathbb{Z}_K$ explicitly. But according to Lemma 4.2, we need only to show that $\mathcal{P}_f > \mathcal{N}_f$ for an adequate positive integer f. So in practice the second point of Theorem 3.1, could replaced by the following: if $l_i = 1$ or $d_{ij} = 1$ or $a_{ijk} = 1$ for some (i, j, k) according to notation of Theorem 3.1, then ψ_{ijk} provides a prime ideal $\mathfrak{p}_{ijk}$ of $\mathbb{Z}_K$ lying above p with residue degree $f_{ijk} = m_i \cdot t_{ijk}$, where $t_{ijk} = \deg(\psi_{ijk})$ and $p\mathbb{Z}_K = \mathfrak{p}_{ijk}^{e_{ij}} I$, where the factorization of the ideal I can be derived from the other factors of each residual polynomial of $F(x)$.

Proof. (**of Theorem** 2.4).
Let $v = \nu_p(a^p - a)$ and recall that $F(x) = \phi^{p^r} \pmod p$, where $\phi = x - a$. By the above ϕ-expansion (4.1) of $F(x)$, $N_\phi^+(F)$ is the lower boundary convex envelope of the set of points $\{(0, v)\} \cup \{(p^r, r - j),\ 0 \le j \le r\}$ in the Euclidean plane. More precisely, if $v \ge r + 2$, then $N_\phi^+(F)$ is the polygon joining the points $\{(0, v), (1, r), (p, r-1) \dots, (p^r, 0)\}$ and if $v \le r + 1$, then $N_\phi^+(F)$ is the polygon joining the points $\{(0, v), (p^{r-v+1}, v - 1), \dots, (p^r, 0)\}$.

(i) If p is an odd rational prime, then $N_\phi^+(F) = S_1 + \cdots + S_g$ has g sides of degree 1 each, with $g \ge \min\{v, r + 1\} \ge p + 1$. So, $R_{\lambda_i}(F)(y)$ is irreducible over $\mathbb{F}_\phi$ for every $i = 1, \dots, g$. Then $F(x)$ is p-regular and by Theorem 3.1, there are at least $p + 1$ distinct prime ideals of $\mathbb{Z}_K$ lying above p with residue degree 1 each ideal factor. As there are just p monic irreducible polynomials of degree 1 over $\mathbb{F}_p$, by Lemma 4.2, p divides $i(K)$. Hence K is not monogenic.

(ii) If $p = 2$, $r = 2$, and $v \ge 4$, then $N_\phi^+(F) = S_1 + S_2 + S_3$ has 3 sides of degree one each. So, $R_{\lambda_i}(F)(y)$ is irreducible over $\mathbb{F}_\phi$ for every $i = 1, 2, 3$. Hence there are three distinct prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each ideal factor. As it is known, there are just two monic irreducible polynomials of degree 1 over $\mathbb{F}_2$, by Lemma 4.2, 2 divides $i(K)$. Hence K is not monogenic.

(iii) If $p = 2$, $r \ge 3$, and $v \ge 5$, then $N_\phi^+(F) = S_1 + \cdots + S_g$ has at least $g - 1$ sides of degree 1 each, with $g \ge \min\{v, r + 1\} \ge 4$. So, there are at least $g - 1 \ge 3$ prime ideals of $\mathbb{Z}_K$ lying above 2 with residue degree 1 each ideal factor. By the same reason, 2 divides $i(K)$ and so K is not monogenic.

□

5 Examples

Let $K = \mathbb{Q}(\alpha)$ be a number field generated by a root α of a monic irreducible polynomial $F(x) = x^{p^r} - a \in \mathbb{Z}[x]$, where p is a rational prime and r a positive integer.

(i) For $r = 1$, Theorems 2.1 and 2.2 generalize the results given in [18].

(ii) For a is square-free, Theorems 2.1 and 2.2 generalize the results given in [26].

(iii) For a is a square-free integer, then Theorem 2.4 generalizes the results given in [3].

(iv) For $p = 3$ and a a square-free integer, Theorem 2.4 generalizes the results given in [4].

(v) For $p = 2$ and $r = 3$, the main Theorems generalize the results given in [7].

(vi) For $p = 2$, $r = 3$ and a a square-free integer, Corollary 2.3 and Theorem 2.4 generalize the results given in [14].

(vii) For $p = 2$ and a a square-free integer, our Corollary 2.3 and Theorem 2.4, show that the results given in [16] hold.

(viii) For $p = 7$ and $a = 15$, we have $\nu_5(a^6 - 1) = 1$ and a is square-free, then by Corollary 2.3, $(1, \alpha, \dots, \alpha^{7^r - 1})$ is an integral basis of $\mathbb{Z}_K$ for every positive integer r. Hence K is monogenic.

(ix) For $p = 5$, $r = 2$, and $a = 150$, we have $\nu_5(a) = 2$, which is coprime with 5. By Theorem 2.1, $\left(1, \alpha, \dots, \alpha^{12}, \frac{\alpha^{13}}{5}, \frac{\alpha^{14}}{5}, \dots, \frac{\alpha^{24}}{5}\right)$ is an integral basis of K.

(x) For $p = 3$, $r = 2$, and $a = 80$, we have $\nu_3(a^2 - 1) = 4$ and $\nu_2(a) = 4$, then by Theorem 2.2,

$$\left(1, \alpha, \alpha^2, \frac{q_6(\alpha)}{2}, \frac{q_5(\alpha)}{2}, \frac{q_4(\alpha)}{4}, \frac{q_3(\alpha)}{12}, \frac{q_2(\alpha)}{24}, \frac{q_1(\alpha)}{72}\right)$$

is an integral basis of $\mathbb{Z}_K$, where $q_6(\alpha) = \alpha^3 - 6\alpha^2 + 21\alpha - 56$, $q_5(\alpha) = \alpha^4 - 5\alpha^3 + 15\alpha^2 - 35\alpha + 70$, $q_4(\alpha) = \alpha^5 - 4\alpha^4 + 10\alpha^3 - 202\alpha^2 + 35\alpha - 56$, $q_3(\alpha) = \alpha^6 - 3\alpha^5 + \alpha^4 - 10\alpha^3 + 15\alpha^2 - 21\alpha + 28$, $q_2(\alpha) = \alpha^7 - 2\alpha^6 + 3\alpha^5 - 4\alpha^4 + 5\alpha^3 - 6\alpha^2 + 7\alpha - 8$, and $q_1(\alpha) = \sum_{i=0}^{8} (-1)^i \alpha^i$.

(xi) If $p = 2$, $r = 4$, and $a = 1800$, we have $\nu_2(a) = 3$, which is coprime with 2. By Theorem 2.1, $\left(1, \alpha, \dots \alpha^5, \frac{\alpha^6}{2}, \frac{\alpha^7}{2}, \frac{\alpha^8}{30}, \frac{\alpha^9}{30}, \frac{\alpha^{10}}{30}, \frac{\alpha^{11}}{60}, \dots, \frac{\alpha^{15}}{60}\right)$ is an integral basis of $\mathbb{Z}_K$.

(xii) If $p = 2$, $r = 7$, and $a = 1050625$, we have $r \geq 3$ and $\nu_2(a - 1) = 11 \geq 5$, then by Theorem 2.4, K is not monogenic.

(xiii) If $p = 5$, $r = 8$, and $a = 11602921876$, we have $r \geq 6$ and $\nu_5(a^4 - 1) = 6$, then by Theorem 2.4, K is not monogenic.

(xiv) If $p = 11$, $r = 20$, and $a = 6044929680708$, we have $r \geq 11$ and $\nu_{11}(a^{10} - 1) = 12 > 11$, then by Theorem 2.4, K is not monogenic.

Competing interests

There are non-financial competing interests to report.

References

[1] S. Alaca, *p-Integral bases of algebraic number fields*, Utilitas Math., 56 (1999), 97–106.

[2] M. Bauer, *Über die außerwesentlichen Diskriminantenteiler einer Gattung*, Math. Ann. 64(4) (1907), 573–576. doi: 10.1007/BF01450065

[3] H. Ben Yakou and L. El Fadil, *On power integral bases for certain pure number fields defined by* $x^{p^r} - m$, Int. J. Number Theory, 17(10) (2021), 2235–2242.

[4] H. Ben Yakou and O. Kchit, *on power integral bases for certain pure number fields defined by* $x^{3^r} - m$. São Paulo J. Math. Sci., 16 (2022), 1072–1079. https://doi.org/10.1007/s40863-021-00251-2

[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 and I. Gaál, *On integral bases and monogenity of pure octic number fields with non-square-free parameters*. arXiv:2202.04417

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

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

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

[11] T. A. Gassert, *A note on the monogeneity of power maps*, Albanian J. Math., 11(1) (2017), 3–12.

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

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

[14] A. Hameed and T. Nakahara, *Integral bases and relative monogeneity of pure ocitc fields*, Bull. Math. Soc. Sci. Math. Répub. Soc. Roum., 58(106) No. 4 (2015), 419–433.

[15] A. Hameed, T. Nakahara, and S. Ahmad, *Non-monogenity of an infinite family of pure octic fields*, J. Elixir Appl. Math., 113 (2017), 49328–49333.

[16] A. Hameed, T. Nakahara, S. M. Husnine, and S. Ahmad, *On existence of canonical number system in certain classes of pure algebraic number fields*, J. of Prime Research in Math., 7 (2011), 19–24.

[17] K. Hensel, *Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung*, J. Reine Angew. Math., (1894), 113:128-160. ISSN 0075-4102. doi: 10.1515/crll.1894.113.128.

[18] A. Jakhar and N. Sangwan, *Integral basis of pure prime degree number fields*, Indian J. Pure Appl. Math., 50(2) (2019), 309–314.

[19] A. Jakhar, S. K. Khanduja, and N. Sangwan, *On integral basis of pure number fields*, Mathematika, 67(1) (2021), 187–195.

[20] O. Kchit, *A note on monogenity of certain pure number fields defined by $x^{p^r} - a$ with non-square-free parameter*, Mosc. J. Comb. Number Theory, 12(2) (2023), 147–164. https://doi.org/10.2140/moscow.2023.12.147

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

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

[23] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Third Edition, Springer, (2004).

[24] J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin, (1999).

[25] O. Ore, *Newtonsche polygone in der Theorie der algebraischen Korper*, Math. Ann., 99(1928) 84–117.

[26] L. Remete, *Integral bases of pure fields with square-free parameter*, Studia Sci. Math. Hungarica 57(1) (2020), 91–115.

[27] H. Smith, *The monogeneity of radical extensions*. Acta Arith., 198(3) (2021), 313–327.

[28] J. Westlund, *On the fundamental number of the algebraic number field $k(\sqrt[p]{m})$*, Trans. Amer. Math. Soc. 11 (1910), 388–392.

Author information

Omar Kchit, Faculty of Sciences Dhar El Mahraz, P.O. Box 1874 Atlas-Fes, Sidi Mohamed ben Abdellah University, Morocco.
E-mail: omar.kchit@usmba.ac.ma, orcid: 0000.0002.0844.5034

Received: 2023-01-17
Accepted: 2023-11-10