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

(3s.) **v. 2025 (43)** : 1–9.
ISSN-0037-8712
doi:10.5269/bspm.63423

Power integral basis for relative extensions of p^n-power Number Fields *

Mohammed Sahmoudi†, Abderazak Soullami, Youness Eraddi

ABSTRACT: Let $L = K(\alpha)$ be an extension of the number field K, where α satisfies the monic irreducible polynomial $f(x) = x^{p^n} - \beta$ of prime power degree belonging to $\mathfrak{o}_K[x]$ and $\mathfrak{o}_K$ is the integral closure of of $\mathbb{Z}$ in K.

The purpose of this paper is to study the monogenity of L/K by using a new version of Dedekind's criterion. So, we give an integral basis of a family of number field of degree $2.p^n$ for some positive integer n. As an illustration, we get a slightly simpler way to compute relative discriminant $d_{L/K}$.

Key Words: Discrete valuation ring(DVR), Dedekind ring, monogenity, relative integral basis.

Contents

1. Introduction

The problem of determining an integral basis of the ring of integral elements in a field is a classical and a hard problem in algebraic number theory. Many works are available in this area (c.f. [1], [3], [?], [14], [8], [11], [12], [15], [16], [17], [20], [18] and others). When R is a principal ideal domain, then $\mathfrak{o}_L$ is a free R-module ($\mathfrak{o}_L$ is the ring of integer of L). An R-basis of $\mathfrak{o}_L$ is called an integral basis of $\mathfrak{o}_L$. We say that L (or $\mathfrak{o}_L$) is monogenic, or has a power relative integral basis, if $\mathfrak{o}_L = R[\alpha]$ for some element α in $\mathfrak{o}_L$.

Testing whether L/K has a relative power integral basis (RPIB for short), is an open problem, and worse still, we don't even know if the integral closure $\mathfrak{o}_L$ of R in L is necessarily a free R-module despite that every fractional ideal of L is finitely generated and torsion-free R-module. So, for cubic relative extensions, [20] give relative integral basis (RIB) for L/K when L is a normal closure of K. This RIB simplifies and completes the one given by [9] (1986), but for relative extensions of degree greater than 4, there are few results on RPIB or RIB and almost published works deal with small dergee or composite extensions. Indeed, the monogenity of number fields and constructing generators of power integral bases (PBG for short) if $R = \mathbb{Z}$ have been intensively studied during the past four decades. mainly by [7], [5], [8], [10] and others.

Throughout this article, unless specifically stated otherwise, Let R be a Dedekind ring of characteristic zero and K its fraction field. Let L/K be a finite separable extension of degree n. We let $Disc_R(f)$ and $D_{L/K}$ denote the discriminant over R, respectively, of the polynomial $f(x)$ and the number field L over

* Moulay Ismail University, Meknes
† Corresponding author

Submitted November 04, 2022. Published December 29, 2024
2010 *Mathematics Subject Classification:* 11Rxx, 11R04, 11R21, 11Y40, 11R16

K. Thus, we will study relative monogenity of $L = K(\alpha)$ over its subfield where α is a root of a monic irreducible polynomial of the form

$$f(x) = x^{p^n} - \beta \in \mathfrak{o}_K[x],\ n \in \mathbb{N}^*. \tag{1.1}$$

This allows to construct an integral basis for a family of extensions $L/\mathbb{Q}$, such that $[L, \mathbb{Q}] = 2.p^n$ ($n \in \mathbb{N}^*$), and compute the discriminant of L/K. As a consequence, we compute the discriminant $d_{L/\mathbb{Q}}$ given by the tower formula:

$$d_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(d_{L/K}).(d_{K/\mathbb{Q}})^{[L:K]}, \tag{1.2}$$

where $N_{K/\mathbb{Q}}$ denote the norm from K to $\mathbb{Q}$ (see [13, Corollary 10. 2] and [6]).

2. Main results

Let us denote by $Spec(R)$, the set of the prime ideals of a commutative ring R. Equipped with the Zariski topology, the closed sets of Spec(R) are the sets:

$$V(\mathfrak{I}) = \{\mathfrak{p} \in Spec\,(R) \mid \mathfrak{I} \subseteq \mathfrak{p}\}$$

Where $\mathfrak{I}$ is an ideal in R. Note also that for any ideal $\mathfrak{I}$ in R and $n \in \mathbb{N}^*$ we have $V(\mathfrak{I}^n) = V(\mathfrak{I})$.

Fix now a non-zero prime ideal $\mathfrak{p} \in Spec\,(R)$. We are also interested in the set of primes $\mathfrak{q}$ in $\mathfrak{o}_L$ with $\mathfrak{p} \subseteq \mathfrak{q}$ −or equivalently $\mathfrak{p} = \mathfrak{q} \cap R$− called the fibre of $\mathfrak{p}$, denoted by $\mathfrak{F}ib_R(\mathfrak{p})$.

With the notation above, for a polynomial f belonging to $R[x]$, $\overline{f}$ will stand for the polynomial over $k = R/\mathfrak{p}$ obtained on replacing each coefficient of f by its residue modulo $\mathfrak{p}$.

2.1. Discrete valuation ring case

The following theorem gives necessary and sufficient conditions on n and β which characterize the monogenity of L/K for some element α in $\mathfrak{o}_L$.

Theorem 2.1 *Let R be a discrete valuation ring with maximal ideal $\mathfrak{p} = \pi R$ and finite residual field k. Let L be a finite separable extension of K, the quotient field of R. Let $\alpha \in L$ be a primitive element of L which be integral over R and $f(x) = x^{p^n} - \beta$ its monic irreducible polynomial in $R[x]$. Let $v_\pi = v_\mathfrak{p}$ be the $\mathfrak{p}-$adic discrete valuation associated to $\mathfrak{p}$. We denote by c_k the characteristic and $m = p^j$ for some integer j; the cardinality of the finite residual field k. Then*

1. *If $v_\mathfrak{p}(\beta) \geq 1$ then α is PBG of $L = K$ if and only if $v_\pi(\beta) = 1$.*
2. *Let r is the smallest positif integer such that $n - rj \leq f$. If $v_\pi(\beta) = 0$, then the following properties hold:*
   (a) *If $c_k = p$, then α is PBG of L/K if and only if*

$$v_\pi(\beta^{m^{r+1}-1} - 1) = 1 \ if\ j < n \ and\ n - rf \leq j \tag{2.1}$$

   (b) *If $c_k \neq p$, then α is PBG of L/K.*

In particular, any one of these conditions guarantees the monogenity of L over K.

The table 1 schematizes our results:

Remark 2.1 *In the case of the characteristic of k not equal to p, we can check that the condition $v_\pi(\beta^m - \beta) = 1$, can be replaced by "$\beta$ is not a p-power modulo π^2."*

Table 1: monogeneity in local case

<table>
<tr><td>$v_{\mathfrak{p}}(\beta) \geq 1$</td><td colspan="3">$\alpha$ is PBG iff $v_{\pi}(\beta) = 1$</td></tr>
<tr><td rowspan="3">$v_{\mathfrak{p}}(\beta) = 0$</td><td>$c_k \neq p$</td><td colspan="2">$c_k = p$</td></tr>
<tr><td rowspan="2">α is PBG</td><td>$j \geq n$</td><td>$j < n$ and $n - rj \leq f$</td></tr>
<tr><td>α is a PBG iff $v_{\pi}(\beta^{m-1} - 1) = 1$</td><td>$\alpha$ is a PGB iff $v_{\pi}(\beta^{m^{r+1}-1} - 1) = 1$</td></tr>
</table>

2.2. Dedekind ring case

Theorem 2.2 *Let R be a Dedekind ring with finite residual field and K its fraction field. Assume that $charK = 0$ and $L = K(\alpha)$ is a finite separable extension of K. Let $f(x) = x^{p^n} - \beta \in R[x]$ be the monic minimal polynomial of α. Then*

1. *If the $\mathfrak{q}-$adic valuation $v_{\mathfrak{q}}(\beta) \geq 1$ for all primes ideals $\mathfrak{q} \in \mathfrak{Fib}_R(p)$, then α is a PBG of L over K if and only if β is square free.*

2. *Let $\mathfrak{Fib}_R(p) - V(\beta R) = \{\mathfrak{p}_1; ...; \mathfrak{p}_h\}$. Let us denote by $(v_i)_{1 \leq i \leq h}$ the $\mathfrak{p}_i - adic$ valuation associated to $\mathfrak{p}_i$ and m_i the cardinality of the residual field $R/\mathfrak{p}_i$. Set $m_i = p^{j_i}$ for some integer j_i when the characteristic of $R/\mathfrak{p}_i$ equal to p. Then α is a PBG of L over K if and only if "β is square free" and for all $i \in \{1; ....; h\}$*

$$v_i(\beta^{m_i - 1} - 1) = 1 \text{ if } j_i \geq n$$

$$v_i(\beta^{m_i^{r_i+1}-1} - 1) = 1 \text{ if } j_i < n \text{ and } n - r_i j_i \leq j_i$$

Where the optimal value of r_i is the smallest integer satisfying the inequality $n \leq (r_i + 1)f_i$ for all $i \in \{1; ....; h\}$ such that $f_i < n$.

3. Preliminaries

In order to prove our main Theorems, we recall some fundamental definitions and results. Let R be a commutative ring, let $\mathfrak{p}$ be a prime ideal in R and $S = R \setminus \mathfrak{p}$. The resulting localization $S^{-1}R$ is usually denoted by $R_{\mathfrak{p}}$ and called the localization of R at the prime ideal $\mathfrak{p}$.

Definition 3.1 *Let R be a Dedekind ring, K its fraction field and υ be a valuation on K. Let $f = b_0 + b_1 x + ... + b_n x^n \in K[x]$, we put:*

$$\upsilon_G(f) = \inf\{\upsilon(b_i) \mid 0 \leq i \leq n\}$$

then υ_G is a valuation on $K[x]$ called the Gauss valuation on $K[x]$ relative to υ.

Proposition 3.1 *Let R be an integrally closed ring and K its quotient field, L is a finite separable extension of K, α is a primitive element of L integral over R. Then $(R[\alpha])_{\mathfrak{p}} = R_{\mathfrak{p}}[\alpha]$ for every prime ideal $\mathfrak{p}$ of R. In particular, $\mathfrak{o}_L = R[\alpha]$ if and only if $R_{\mathfrak{p}}[\alpha]$ is integrally closed for every prime ideal $\mathfrak{p}$ of R if and only if $R[\alpha]$ is integrally closed.*

Proof: We obtain the result from the isomorphism $R[\alpha] = R[x]/ < f(x) >$, the properties of an integrally closed ring and its integral closure, and the properties of a multiplicative closed subset of a ring R, notably, $S^{-1}(R[x]) = (S^{-1}R)[x]$ (see [2]). □

Remark 3.1 *Let us keep all the notations of previous Proposition 3.1. Let B be the integral closure of $R_{\mathfrak{p}}$ in L. Then $B = (\mathfrak{o}_L)_{\mathfrak{p}}$.*

Proposition 3.2 *Let R be a Dedekind ring, K its fraction field, L be a finite separable extension over K and $\mathfrak{o}_L$ be the integral closure of R in L. Let $\alpha \in \mathfrak{o}_L$ be an algebraic integer over R such that $L = K(\alpha)$. Let $\mathfrak{p}$ be a non-zero prime ideal in R and B the integral closure of $R_{\mathfrak{p}}$ in L. Then $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $B = R_{\mathfrak{p}}[\alpha]$.*

Proof: We obtain the result from Lemma 3.1, the properties of ideal index and the fact that any multiplicative closed subset S of a ring R permute with the integral closure, notably, $S^{-1}(\mathfrak{o}_L)$ is equal to the integral closure of $(S^{-1}R)$ in L (see [2]). □

Theorem 3.1 (Dedekind Criterium) *Let R be a Dedekind ring, K its fraction field, L be a finite separable extension over K and $\mathfrak{o}_L$ be the integral closure of R in L. Let $\alpha \in \mathfrak{o}_L$ be an algebraic integer over R such that $L = K(\alpha)$. Let $f = Irrd(\alpha, R) \in R[x]$ be the monic irreducible polynomial of α. Let $\mathfrak{p}$ be a non-zero prime ideal in R and $k := R/\mathfrak{p}$ its residual field. Let $\bar{f}$ be the image of any f in $k[x]$ modulo p and assume that*

$$\bar{f} = \Pi_{i=1}^{r} \bar{f_i}^{l_i}$$

is the primary decomposition of $\bar{f}$ in $k[x]$ with $f_i \in R[x]$ a monic lift of the irreducible polynomial $\overline{f_i}$ for $1 \leq i \leq r$. Let $V_i \in R[x]$ be the remainder of Euclidean division of f by f_i. Let $\upsilon_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Let υ_G be the Gauss valuation on $K[x]$ associated to $\upsilon_{\mathfrak{p}}$. Then $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $\upsilon_G(V_i) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$.

Proof: Let $T \in R[x]$ satisfying $f = \prod_{i=1}^{r} f_i^{l_i} + \pi T$ where π is an uniformizer of R (Any generator π of $\mathfrak{p} \setminus \mathfrak{p}^2$). Let $U_i \in R[x]$ the remainder of the Euclidean division of T by f_i. The uniqueness of the remainder, show that $V_i = \pi U_i$. As $\overline{f}_i$ is irreducible, then $gcd\left(\overline{f}_i, \overline{T}\right) = 1$ if and only if $\overline{U}_i \neq \overline{0}$, which is equivalent to $\upsilon_G(U_i) = 0$ and therefore to $\upsilon_G(V_i) = 1$. Then $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if the element α is PBG of L over $R_{\mathfrak{p}}$ (see Proposition 3.2).

Finally, by Dedekind Criterium (see [19]), the element α is PBG of L over $R_{\mathfrak{p}}$ if and only if $pgcd\left(\overline{f}_i, \overline{T}\right) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$, if and only if $\upsilon_G(V_i) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$. □

4. Proofs of main results

Proof: of Theorem 2.1

1. First, we observe first that in this case $\mathfrak{F}ib_R(p) = \pi R$. Using the fact that $\overline{f} = \overline{x}^{p^n} \ mod\ \mathfrak{p}$, we see immediately that the remainder of the Euclidean division of f by x is $r(x) = \beta$. This complete the proof in this case in view of theorem 3.1.

2. Assume now that $v_{\mathfrak{p}}(\beta) = 0$ and $c_k = p$, then we have $m = p^j$ for some integer j. Hence by reducing f modulo the unique prime ideal πR which lies above pR, yields:

$$\begin{aligned} \overline{f(x)} &= \overline{x}^{p^n} - \overline{\beta}\ mod(\pi R) \\ &= \overline{x}^{p^n} - \overline{\beta}^{p^j}\ mod(\pi R)\ (Since\ \beta^m \equiv \beta\ mod\,\pi\,.) \end{aligned} \tag{4.1}$$

   Hence, We need only consider two cases: $j \geq n$ and $j < n$,

   - If $j \geq n$, the formula 4.1 can be written as:

$$\begin{aligned} \overline{f(x)} &\equiv \overline{x}^{p^n} - \overline{\beta}^{p^j}\, mod(\pi R) \\ &\equiv \left(\overline{x} - \overline{\beta}^{p^{j-n}}\right)^{p^n}\ mod(\pi R). \end{aligned}$$

     Let us denote by $R_1(x)$, the remainder of the Euclidean division of f by $x - \beta^{p^{j-n}}$. Then, $R_1(x) = f(\beta^{p^{j-n}}) = \left(\beta^{p^{j-n}}\right)^{p^n} - \beta = \beta^{p^j} - \beta$. It follows immediately that α is PBG if and only if $v_\pi(\beta^m - \beta) = 1$.

- If $n > j$, let r be the smallest positif integer such that $n - rj \leq j$ then we have:

$$\begin{aligned}
\overline{f(x)} &\equiv \overline{x}^{p^n} - \overline{\beta} \ mod\, \pi R \\
&\equiv \left(\overline{x}^{p^{n-rj}} - \overline{\beta}\right)^{p^{rj}} \ mod\, \pi R \\
&\equiv \left(\overline{x}^{p^{n-rj}} - \overline{\beta}^{p^j}\right)^{p^{rj}} \ mod\, \pi R \\
&\equiv \left(\overline{x} - \overline{\beta}^{p^{j-n+rj}}\right)^{p^{rj}\cdot p^{n-rj}} \ mod\, \pi R \\
&\equiv \left(\overline{x} - \overline{\beta}^{p^{(r+1)j-n}}\right)^{p^n} \ mod\, \pi R.
\end{aligned}$$

  Then $R_2 = \beta^{m^{r+1}} - \beta$, is the remainder of the Euclidean division of f by $x - \beta^{p^{(r+1)j-n}}$. So, α is a PBG if and only if $v_\pi(\beta^{m^{r+1}} - \beta) = 1$, which completes the proof, since $v_\pi(\beta) = 0$.

3. Now if $c_k \neq p$, then from $\beta \in R \setminus \mathfrak{p}$, it follows that f is a separable polynomial. Otherwise, if f has α as a double root, then from $f'(x) = p^n x^{p^n - 1}$ we get $\alpha = 0$ which means that $\beta \in \mathfrak{p}$, hence α is PBG of L/K in this case.

□

Proof: of Theorem 2.2 The index of α is defined as the module index $Ind_R(\alpha) := [\mathfrak{o}_L : \mathfrak{o}_K[\alpha]]$. Obviously, α is a PBG of L over K if and only if $(\mathfrak{o}_L)_\mathfrak{p} = R_\mathfrak{p}[\alpha]$, for all non-zero prime ideal $\mathfrak{p}$ in R if and only if $\mathfrak{p}$ doesn't divide the index ideal, $\mathrm{Ind}_R(\alpha)$. Hence, By using the standard Index formula:

$$Disc_R(P) = Ind_R^2(\alpha).d_{L/K},$$

α is a PBG of L over K if and only if $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ for any prime ideal $\mathfrak{p}$ in S_P ;

$$S_P = \{\, \mathfrak{p} \in specR \mid \mathfrak{p}^2 \ divides \ Disc_R(P) \,\}.$$

Our proof starts with the observation that the discriminant of $f(x)$ is $Disc_R(P) = d_{L/K} = (p^n)^{p^n} \beta^{p^n - 1}$, then the set $S_P = V(\beta R) \cup (\mathfrak{F}ib_R(p) - V(\beta R))$ is a disjoint union, return to the introduction of this section, α is a PBG of L over K if and only if $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ for any prime ideal $\mathfrak{p}$ in S_P. So, let $\mathfrak{p}$ be a prime in S_P by localization at $\mathfrak{p}$, the ring $R_\mathfrak{p}$ is a Discrete valuation ring.

1. Our condition in the first case implies that $S_P = V(\beta R)$. Let $\mathfrak{p} \in V(\beta R)$, then by virtue of the result proved in the third section, α is a PBG of L over K if and only if $v_\mathfrak{p}(\beta) = 1$ which means that β is square free and complete the proof in this case.

2. Let us first note that $S_P = V(\beta R) \cup \{\mathfrak{p}_1, ..., \mathfrak{p}_h\}$. It is clear that $charR/\mathfrak{p}_i = p$ (the characteristic of the field $R/\mathfrak{p}_i$ is equal to p since $pR \subset \mathfrak{p}_i$). According to the result proved in the third section again, we can conclude that $\mathfrak{p}_i$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $v_i(\beta^{m_i^{r_i+1}-1} - 1) = 1$ with $r_i = 0$ if $j_i \geq n$. On the other hand, if $\mathfrak{p} \in V(\beta R)$, $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if β is square free.

□

5. Illustration

Let $K = \mathbb{Q}(\sqrt{d})$ is a quadratic extension of the rational number field and d is square free, we recall that the ring of integers of K is generated by $1; t$ over $\mathbb{Z}$, where

$$t = \begin{cases} \sqrt{d} & if\ d \equiv 2,\ 3\ \ modulo\ \ 4 \\ \frac{1+\sqrt{d}}{2}, & if\ d \equiv 1\ \ modulo\ \ 4. \end{cases} \tag{5.1}$$

And the discriminant is given by:

$$d_{K/\mathbb{Q}} = \begin{cases} 4d, & if\ d \equiv 2,\ 3\ \ modulo\ \ 4 \\ d, & if\ d \equiv 1\ \ modulo\ \ 4. \end{cases} \tag{5.2}$$

Theorem 5.1 *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension such that d is square free and $d \equiv 0$ modulo p. Let $L = K(\alpha)$ such that $\alpha^{p^n} = \beta = u\sqrt{d} + v$ $(n \in \mathbb{N}^*,\ u, v \in \mathbb{Z})$, furthermore we assume that $\upsilon_p(u) = \upsilon_p(v) = 0$ and $\upsilon_p(v^{p^n-1} - 1) > 1$, then L/K is monogenic. In this case we note that:*

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{p^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{p^n-1}\}.$$

is an integral basis of $L/\mathbb{Q}$.

Proof: Firstly, we note that $p\mathfrak{o}_K = \mathfrak{p}^2$, it is known that the cardinality of $\mathfrak{o}_K/\mathfrak{p}$ is p since the residual degree of $\mathfrak{p}$ is $f = 1$ then by Theorem 2.2, α is a power basis generator if and only if $\upsilon_{\mathfrak{p}}(\beta^{p^n-1} - 1) = 1$, then we have

$$\begin{aligned} \beta^{p^n-1} - 1 &= \sum_{k=0}^{p^n-1} \binom{k}{p^n-1} \left(u\sqrt{d}\right)^k v^{p^n-1-k} - 1 \\ &= \sum_{\substack{k=2t \\ t\in\mathbb{N}}} \binom{k}{p^n-1} \left(u\sqrt{d}\right)^k v^{p^n-1-k} - 1 + \sqrt{d}\left(\sum_{\substack{k=2t+1 \\ t\in\mathbb{N}}} \binom{k}{p^n-1} u^k \left(\sqrt{d}\right)^{k-1} v^{p^n-1-k}\right) \end{aligned}$$

Now by property of dominance principle, and using the fact that $\upsilon_p(u) = \upsilon_p(v) = 0$, it is easy to check that

$$\upsilon_{\mathfrak{p}}\left(\sum_{\substack{k=2t+1 \\ t\in\mathbb{N}}} \binom{k}{p^n-1} u^k \left(\sqrt{d}\right)^{k-1} v^{p^n-1-k}\right) = 0,$$

and

$$\upsilon_{\mathfrak{p}}\left(\sum_{\substack{k=2t \\ t\in\mathbb{N}^*}} \binom{k}{p^n-1} u^k \left(\sqrt{d}\right)^{k} v^{p^n-1-k}\right) = 2.$$

Keeping this in mind and using the fact that $\upsilon_p(v^{p^n-1} - 1) > 1$, we see immediatly that

$$\upsilon_{\mathfrak{p}}\left(\beta^{p^n-1} - 1\right) = \min\left(\upsilon_{\mathfrak{p}}\left(\sum_{\substack{k=2t \\ t\in\mathbb{N}^*}} \binom{k}{p^n-1} \left(u\sqrt{d}\right)^k v^{p^n-1-k}\right), \upsilon_{\mathfrak{p}}((v^{p^n-1} - 1)), \upsilon_{\mathfrak{p}}(\sqrt{d})\right) = 1$$

Satisfying the conditions of Theorem 2.2, so that L is monogenic, let denote $\{1; \alpha; \alpha^2; ...; \alpha^{3^n-1}\}$ such RPIB. Using [3, Lemma 3.1] it's obvious that

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{p^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{p^n-1}\}$$

is an integral basis of L over $\mathbb{Q}$ of degree $2 \cdot p^n$. □

Corollary 5.1 *With previous conditions in Theorem 5.1, the discriminant $d_{L/\mathbb{Q}}$ is given by:*

$$d_{L/\mathbb{Q}} = \begin{cases} p^{2.p^n n}(u^2 - v^2 d)^{p^n - 1}(4d)^{p^n} & if\ d \equiv 2,\ 3\ \ modulo\ \ 4 \\ p^{2.p^n n}(d)^{p^n}(u^2 - v^2 d)^{3^n - 1}, & if\ d \equiv 1\ \ modulo\ \ 4. \end{cases}$$

Proof: Since L/K is monogenic we obtain $d_{L/K} = (p^n)^{p^n}\beta^{p^n-1}$, then $N_{K/\mathbb{Q}}(d_{L/K}) = p^{2n.p^n} N_{L/K}(\beta)^{p^n-1}$ and the norm of $u\sqrt{d} + v$ is $N_{K/\mathbb{Q}}(\beta) = u^2 - v^2 d$, by discriminant tower formula 1.2 it follows that:

$$d_{L/\mathbb{Q}} = \begin{cases} p^{2.p^n n}(u^2 - v^2 d)^{p^n - 1}(4d)^{p^n} & if\ d \equiv 2,\ 3\ \text{modulo}\ \ 4 \\ p^{2.p^n n}(d)^{p^n}(u^2 - v^2 d)^{3^n - 1}, & if\ d \equiv 1\ \text{modulo}\ \ 4. \end{cases}$$

□

Theorem 5.2 *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension such that d is square free, $5 \nmid d$. Let $L = K(\alpha)$ such that $\alpha^{5^n} = \beta = \sqrt{d} + 1$ $(n = 1,\ 2)$, furthermore we assume that the ideal $(\sqrt{d} + 1)$ is square free in $\mathfrak{o}_K$ and $p\mathbb{Z}$ is inert in $\mathfrak{o}_K$, then we have :*

- *If $d \equiv 2, 3, 7, 12, 13, 17, 18, 22, 23$ modulo 25, then L/K is monogenic. In this case, we note that:*

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{5^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{5^n-1}\}.$$

  is an integral basis of $L/\mathbb{Q}$.

- *If $d \equiv 8$ modulo 25 Then L/K is not monogenic.*

Proof: Observe first that the ideal $5\mathfrak{o}_K = \mathfrak{p}$ is prime in $\mathfrak{o}_K$.
By Theorem 2.2 it is known that L/K is monogenic if and only if $v_\mathfrak{p}(\beta^{24} - 1) = 1$. We already have that $\beta^{24} - 1 = \sqrt{d}\left(\beta^2 + \beta + 1\right)\left(\beta^{21} + \beta^{18} + \beta^{15} + \beta^{12} + \beta^9 + \beta^6 + \beta^3 + 1\right)$, put $k = \beta^2 + \beta + 1$, Consequently $v_\mathfrak{p}(k) = v_\mathfrak{p}(\beta^2 + \beta + 1) = v_\mathfrak{p}(d + 3\sqrt{d} + 3) = 0$ as $5 \nmid d$. Set now $h = \beta^{21} + \beta^{18} + \beta^{15} + \beta^{12} + \beta^9 + \beta^6 + \beta^3 + 1$ and a ssume that $d \equiv a$ modulo 25 where $a \in \{2, 7, 8, 12, 13, 17, 18, 22, 23\}$ and let k_a be the quotient of h a by $s = d - a$, then we get

$$h = k_a s + u_a + v_a \beta.$$

Now using the fact that $d \equiv a$ modulo 25, we see immediately that $v_\mathfrak{p}(h_1 s) = v_\mathfrak{p}(h_1) + v_\mathfrak{p}(s) \geqslant 2$. Then we have :

1. If $d \equiv 2$ modulo 25, then $h = k_2 s + 17218080 + 41568120\beta$ and hence $v_\mathfrak{p}(h) = 1$ since $v_\mathfrak{p}(17218080 + 41568120) = 2$ and $v_\mathfrak{p}(41568120\sqrt{d}) = 1$. This proves that $v_\mathfrak{p}(\beta^{24} - 1) = 1$, thus L/K is monogenic.
2. If $d \equiv 3$ modulo 25, then $h = k_3 s + 325875485 + 445154190\beta$ and hence $v_\mathfrak{p}(h) = 1$ since $v_\mathfrak{p}(325875485 + 445154190) = 2$ and $v_\mathfrak{p}(445154190\sqrt{d}) = 1$. This proves that $v_\mathfrak{p}(\beta^{24} - 1) = 1$, thus L/K is monogenic.
3. If $d \equiv 7$ modulo 25, then $h = k_7 s + 199236613045 + 121061207890\beta$ and hence $v_\mathfrak{p}(h) = 1$ since $v_\mathfrak{p}(u_7 - 3v_7) = v_\mathfrak{p}(199236613045 - 3.121061207890) = 4$ and $v_\mathfrak{p}(121061207890(4 + \sqrt{d})) = 0$. This proves that $v_\mathfrak{p}(\beta^{24} - 1) = 1$, thus L/K is monogenic.
4. If $d \equiv 12$ modulo 25, then $h = k_{12} s + 15862082187260 + 6437331720060\beta$ and hence $v_\mathfrak{p}(h) = 1$ since $v_\mathfrak{p}(u_{12} - v_{12}) = v_\mathfrak{p}(15862082187260 - 6437331720060) = 2$ and $v_\mathfrak{p}(6437331720060(2 + \sqrt{d})) = 0$. This proves that $v_\mathfrak{p}(\beta^{24} - 1) = 1$, thus L/K is monogenic.
5. If $d \equiv 13$ modulo 25, then $h = k_{13} s + 30993885541465 + 11895524262160\beta$ and hence $v_\mathfrak{p}(h) = 1$ since $v_\mathfrak{p}(30993885541465 + 11895524262160) = 3$ and $v_\mathfrak{p}(11895524262160\sqrt{d}) = 1$. This proves that $v_\mathfrak{p}(\beta^{24} - 1) = 1$, thus L/K is monogenic.

6. If $d \equiv 17$ modulo 25, then $h = k_{17}s + 303216403752225 + 97095649795380\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(303216403752225) = 2$ and $v_{\mathfrak{p}}(97095649795380\sqrt{d}) = 1$. This proves that $v_{\mathfrak{p}}(\beta^{24} - 1) = 1$, thus L/K is monogenic.

7. If $d \equiv 18$ modulo 25, then $h = k_{18}s + 496341807039680 + 153083209946520\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(496341807039680 + 153083209946520) = 2$ and $v_{\mathfrak{p}}(153083209946520\sqrt{d}) = 1$. This provess that $v_{\mathfrak{p}}(\beta^{24} - 1) = 1$, thus L/K is monogenic.

8. If $d \equiv 22$ modulo 25, then $h = k_{22}s + 2851989592814440 + 773025087889600\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(773025087889600) = 2$ and $v_{\mathfrak{p}}(2851989592814440) = 1$. This proves that $v_{\mathfrak{p}}(\beta^{24} - 1) = 1$, thus L/K is monogenic.

9. If $d \equiv 23$ modulo 25, then $h = k_{23}s + 4216875746193045 + 1111301467484130\beta$ and hence $v_{\mathfrak{p}}(h) = 1$ since $v_{\mathfrak{p}}(4216875746193045 + 1111301467484130) = 2$ and $v_{\mathfrak{p}}(1111301467484130\sqrt{d}) = 1$. This proves that $v_{\mathfrak{p}}(\beta^{24} - 1) = 1$, thus L/K is monogenic.

Let denote $\{1; \alpha; \alpha^2; ...; \alpha^{5^n-1}\}$ such RPIB. Using [3, Lemma 3.1] it's obvious that

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{5^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{5^n-1}\}$$

is an integral basis of L over $\mathbb{Q}$ of degree $2 \cdot 5^n$.

If $d \equiv 8$ modulo 25, then $h = h_1 s + 576421380900 + 315255471300\beta$ and hence $v_{\mathfrak{p}}(h) \geqslant 2$ since $v_{\mathfrak{p}}(576421380900) = v_{\mathfrak{p}}(315255471300) = 2$. This proves that $v_{\mathfrak{p}}(\beta^{24}-1) \geqslant 2$, thus L/K is not monogenic. □

Corollary 5.2 *With previous conditions in Theorem 5.2 and $d \not\equiv 8$ modulo 25, the discriminant $d_{L/\mathbb{Q}}$ is given by:*

$$d_{L/\mathbb{Q}} = \begin{cases} 5^{2.5^n n}(1-d)^{p^n-1}(4d)^{5^n} & if\ d \equiv 2, 3\ \ modulo\ \ 4 \\ 5^{2.5^n n}(d)^{5^n}(1-d)^{5^n-1}, & if\ d \equiv 1\ \ modulo\ \ 4. \end{cases}$$

Proof: Since L/K is monogenic we obtain $d_{L/K} = (5^n)^{5^n}\beta^{5^n-1}$, then $N_{K/\mathbb{Q}}(d_{L/K}) = 5^{2n.5^n}N_{L/K}(\beta)^{5^n-1}$ and the norm of $\sqrt{d}+1$ is $N_{K/\mathbb{Q}}(\beta) = 1-d$, by discriminant tower formula 1.2 it follows that:

$$d_{L/\mathbb{Q}} = \begin{cases} 5^{2.5^n n}(1-d)^{5^n-1}(4d)^{5^n} & if\ d \equiv 2, 3\ \ \text{modulo}\ \ 4 \\ 5^{2.5^n n}(d)^{5^n}(1-d)^{5^n-1}, & if\ d \equiv 1\ \ \text{modulo}\ \ 4. \end{cases}$$

□

This work can be generalized to a higher degree of the extension L, knowing that the difficulty of the problem comes from the computation of the relative discriminant. On the other hand, we can be based on the minimal polynomials (see [**?**]) to study the monogenity.

6. Acknowledgements

The author is deeply grateful to the anonymous referees whose valuable comments and suggestions have tremendously improved the quality of this paper.

The authors declare that there is no conflict of interest regarding the publication of this paper

References

1. O. Boughaleb, A. Soullami and M. Sahmoudi, *On relative monogeneity of a family of number fields defined by $X^{p^n} + aX^{p^s} - b$*, Bol. Soc. Mat. Mex. 29 (2023).

2. M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison- Wesley, Massachusetts, 1969.

3. M. E Charkani and M. Sahmoudi, *Sextic Extension with cubic subfield*, JP Journal of Algebra, Number Theory et Applications, 34, no. 2, 139-150, (2014).

4. R. Dedekind, *Uber den zussamenhang zwischen der theorie der ideals und der theorie der hoheren cyclotimy index*, Abh. Akad. Wiss. Gottingen, Math.-Phys. KL **23** 1-23, (1878)

5. J. Didi, M. Sahmoudi and A. Chillali, *A class of number fields without odd rational prime index divisors and applications*, J. Algebra and Related Topics (2024) (In press)

6. A. Frölich and J. Taylor, *Algebraic Number Theory*, Combridge Studies in Advenced Mathematics, 27, Cambridge University Press, (1993).

7. I. Gaál, *An experiment on the monogenity of a family of trinomial,* JP Journal of Algebra Number Theory Appl. 51, no. 1, 97–111 (2021).

8. M. N. Gras, *Non monogénéité de l'anneau des entiers des extensions cycliques de* $\mathbb{Q}$ *de degré premier* $l \geq 5$, J. Number Theory 23, no. 3, 347-353 (1986).

9. M. Haghighi, *Relative integral basis for algebraic number fields*, Int. J. Math. Math. Sci. 9 no. 1, 97-104 (1986).

10. B. Jhorar and S.K. Khanduja, *On power basis of a class of algebraic number fields,* I. J. Number Theory , 12 no. 8, 2317–2321 (2016).

11. M.J. Lavalee and B.K. Sperman, K.S. Williams,*Lifting monogenic cubic fields to monogenic sextic fields*, Kodai math. J. 34, 410-425, (2011).

12. W. Narkizewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, Second Edition, (1999).

13. J. Neukirch, *Algebraic Number Theory*, Springer Publication, (1999).

14. M. Sahmoudi, and M. E Charkani, *On relative pure cyclic fields with power integral bases*, Mathematica Bohemica, 1-12 148 (2022).

15. M. Sahmoudi and A. Soullami, *On monogenicity of relative cubic-power estensions*, Advances in Mathematics: Scientific Journal 9, no.9, 6817–6827 (2020).

16. M. Sahmoudi and A. Soullami, *On Sextic Integral Bases Using Relative Quadratic Extention*, Bol. Soc. Paran. Mat. 38 no.4, 175-180 (2020).

17. M. Sahmoudi, *Explicit integral basis for a family of sextic field*, Gulf J. Math., 4, 217-222 (2016).

18. *A. Soullami, M. Sahmoudi and O. Bughaleb*, On relative power integral bases in a family of Numbers fields, Rocky Mountain Journal of Mathematics, 51 no. 4, 1443-1452 (2021).

19. P. SCHMID, *On criteria by Dedekind and Ore for integral ring extensions*, Arch. Math., 84, 304-310 (2005).

20. B.K. Sperman and K.S. Williams, *Relative integral bases for quartic fields over quadratic subfields*, Acta Math. Hungar., 70, 185-192 (1996).

Mohammed Sahmoudi,
Department of Mathematics,
Moulay Ismail University,
Morocco.
E-mail address: m.sahmoudi@umi.ac.ma

and

Abderazak Soullami,
Department of Mathematics,
Moulay Ismail University,
Morocco.
E-mail address: a.soullami@umi.ac.ma

and

Youness Erradi,
Department of Mathematics,
Moulay Ismail University,
Morocco.
E-mail address: y.erradi@edu.umi.ac.ma