ADV MATH
SCI JOURNAL

Advances in Mathematics: Scientific Journal **9** (2020), no.9, 6817–6827
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.9.40

ON MONOGENICITY OF RELATIVE CUBIC-POWER PURE EXTENSIONS

M. SAHMOUDI[1] AND A. SOULLAMI

ABSTRACT. Let K be a number field and $L = K(\alpha)$ where α satisfies the monic irreducible polynomial $P(X) = X^{3^n} - \beta$ in $\mathcal{O}_K[X]$ ($\mathcal{O}_K$ is the ring of integer of K). In this paper we characterize the monogeneity of L over K by a simple and efficient version of Dedekind's criterion. As illustration, we construct an integral basis of a family of number field of degree equal to $2 \cdot 3^n$ for a positive integer n. As a consequence, we obtain a straightforward computation of discriminant $D_{L/K}$.

1. INTRODUCTION

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.

If R is a principal ideal domain, every finitely generated torsion-free R-module has integral basis; so, any fractional ideal in a number field has an integral basis.

The problem of monogeneity (more generally existence of an integral basis) is a classical topic of algebraic number theory. It was originally examined by Dedekind [5] and since many number theorists have been attracted (c.f. [1–3, 8–10, 13, 15, 17, 20] and others). Indeed, Testing whether L/K has a relative monogenic integral basis (RMIB for short) is a hard open problem, worse still,

[1] *corresponding author*

2010 *Mathematics Subject Classification.* 11Rxx, 11R04, 11R21, 11Y40, 11R16.

Key words and phrases. Discrete valuation ring; Dedekind ring; monogenetic; relative integral basis.

we don't even know if the integral closure $\mathcal{O}_L$ of R in L is necessarily a free R-module despite that every fractional ideals of L is finitely generated and torsion-free R-module. In the best case, we say that L/K is *monogenic* or α is a PBG of L/K, or equivalently, $\{1,\ \alpha,\ \alpha^2,\ \dots,\ \alpha^{n-1}\}$ for some α of $\mathcal{O}_L$, is a basis for $\mathcal{O}_L$ over R which is denoted more briefly by $\mathcal{O}_L = R[\alpha]$.

The authors of [7, 14], have given examples of quadratic extensions of imaginary quadratic number fields for which there exists no relative integral basis and by using a theorem of Artin, [21] gives necessary and sufficient conditions for certain quadratic extensions of imaginary quadratic fields to have relative integral bases. Hereafter, [3, 17], studies monogeneity in general quadratic cases.

For cubic relative extension, [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 [11] (1986), but for relative extensions of degree greater than 4, there is few results on RMIB or RIB and almost published works deal with decomposable extensions (which are composite of two pure subfields).

Throughout this article, we let $Disc_R(P)$ and $D_{L/K}$ denote the discriminants over R, respectively, of the polynomial $P(X)$ and the number field L over K.

In this note, we study relative monogeneity of $L = K(\alpha)$ over its subfield where α is a root of a monic irreducible polynomial of the form

$$P(X) = X^{3^n} - \beta \in \mathcal{O}_K[X],\ n \in \mathbb{N}^*.$$

This allow to construct an integral basis for a family of extensions $L/\mathbb{Q}$, such that $[L, \mathbb{Q}] = 2 \cdot 3^n$ ($n \in \mathbb{N}^*$), and compute the discriminant of L/K. As a consequence, we compute the discriminant $D_{L/\mathbb{Q}}$ given by the tower formula:

$$D_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(D_{L/K}).(D_{K/\mathbb{Q}})^{[L:K]}, \tag{1.1}$$

where $N_{K/\mathbb{Q}}$ denote the norm from K to $\mathbb{Q}$ (see [16, Corollary 10. 2] and [6]).

The following result allows us to explicite necessary and sufficient conditions for a relative extension to admit a power integral basis:

Let R be a Dedekind ring, K its fraction field and v be a valuation on K. Let L be a finite separable extension over K and $\alpha \in \mathcal{O}_L$ be an algebraic integer over R such that $L = K(\alpha)$. Let $P = Irrd(\alpha,\ R) \in R[X]$ be the monic irreducible polynomial of α. Let $P = a_0 + a_1 X + \dots + a_n X^n \in K[X]$. We put $v_G(P) = \inf\{v(a_i) \mid 0 \leq i \leq n\}$, then v_G is a valuation on $K[X]$ called the Gauss valuation on $K[X]$ relative to v. Let $\mathfrak{p}$ be a non zero prime ideal in R

and $k := R/\mathfrak{p}$ its residual field. Let $\bar{P}$ be the image in $k[X]$ of P and assume that $\bar{P} = \Pi_{i=1}^{r}\bar{P_i}^{l_i}$ is the primary decomposition of $\bar{P}$ in $k[X]$ with $P_i \in R[X]$ a monic lift of the irreducible polynomial $\overline{P_i}$ for $1 \leq i \leq r$. Let $V_i \in R[X]$ be the remainder of Euclidean division of P by P_i. Let $\upsilon_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$.

Then, by Dedekind Criterium (see [18], [12] or [19]), the element α is PBG of L over $R_{\mathfrak{p}}$ if and only if $gcd\left(\overline{P}_i,\ \overline{T}\right) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$. So, the latest condition can be changed by the simplest one $\upsilon_G(V_i) = 1$ for all $i = 1, \cdots, r$ such that $l_i \geq 2$.

2. Monogeneity of relative cubic-power pure extension - local case

Since we are going to apply the Dedekind Criterium recalled in introduction, we begin by formulate our first main result in case of discrete valuation ring as part of simplifying the general case.

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 $P(X) = X^{3^n} - \beta$ its monic irreducible polynomial in $R[X]$. Let $\upsilon_\pi = \upsilon_{\mathfrak{p}}$ be the $\mathfrak{p} - adic$ discrete valuation associated to $\mathfrak{p}$. We denote by c_k the characteristic and m the cardinality of the finite residual field k. Then*

1. *If $\upsilon_{\mathfrak{p}}(\beta) \geq 1$ then α is PBG of $L = K$ if and only if $\upsilon_\pi(\beta) = 1$.*
2. *If $\upsilon_\pi(\beta) = 0$, then the following properties hold:*
   (a) *If $c_k = 3$, then α is PBG of L/K if and only if*

$$\upsilon_\pi(\beta^{m-1} - 1) = 1 \ if \ f \geq n \tag{2.1}$$

$$\upsilon_\pi(\beta^{m^{r+1}-1} - 1) = 1 \ if \ f < n \ and \ n - rf \leq f \tag{2.2}$$

Where r is the smallest positif integer such that $n - rf \leq f$.

   (b) *If $c_k \neq 3$, then α is PBG of L/K.*

Proof. (1) First we note that $\overline{P} = \overline{X}^{3^n}$ $modulo$ $\mathfrak{p}$, then the remainder of the Euclidean division of P by X is $r(X) = \beta$. So, α is a PBG if and only if $\upsilon_\pi(\beta) = 1$.

(2) We assume that $\upsilon_{\mathfrak{p}}(\beta) = 0$.

(a) Since $c_k = 3$, we have $m = 3^f$ for some integer f. Now by reducing P modulo the unique prime ideal πR which lies above $3R$, yields:

$$\begin{aligned} \overline{P(X)} &= \overline{X}^{3^n} - \overline{\beta}\ mod(\pi R) \\ &= \overline{X}^{3^n} - \overline{\beta}^{3^f} mod(\pi R)\ (Since\, \beta^m \equiv \beta\ modulo\, \pi\ .) \end{aligned} \tag{2.3}$$

Hence, we need only consider two cases: $f \geq n$ and $f < n$,

- If $f \geq n$, the formula (2.3) can be written as:

$$\begin{aligned} \overline{P(X)} &\equiv \overline{X}^{3^n} - \overline{\beta}^{3^f} mod(\pi R) \\ &\equiv \left(\overline{X} - \overline{\beta}^{3^{f-n}}\right)^{3^n} mod(\pi R). \end{aligned}$$

  Let us denote by R_1, the remainder of the Euclidean division of P by $X - \beta^{3^{f-n}}$. Then, $R_1 = P(\beta^{3^{f-n}}) = \left(\beta^{3^{f-n}}\right)^{3^n} - \beta = \beta^{3^f} - \beta$. It follows immediately that α is PBG if and only if $v_\pi(\beta^{m-1} - 1) = 1$.

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

$$\begin{aligned} \overline{P(X)} &\equiv \overline{X}^{3^n} - \overline{\beta}\ mod\, \pi R \\ &\equiv \left(\overline{X}^{3^{n-rf}} - \overline{\beta}\right)^{3^{rf}} mod\, \pi R \\ &\equiv \left(\overline{X}^{3^{n-rf}} - \overline{\beta}^{3^f}\right)^{3^{rf}} mod\, \pi R \\ &\equiv \left(\overline{X} - \overline{\beta}^{3^{f-n+rf}}\right)^{3^{rf}.3^{n-rf}} mod\, \pi R \\ &\equiv \left(\overline{X} - \overline{\beta}^{3^{(r+1)f-n}}\right)^{3^n} mod\, \pi R. \end{aligned}$$

  Then $R_2 = \beta^{m^{r+1}} - \beta$, is the remainder of the Euclidean division of P by $X - \beta^{3^{(r+1)f-n}}$. So, α is a PBG if and only if $v_\pi(\beta^{m^{r+1}} - \beta) = 1$, which completes the proof, since $v_\pi(\beta) = 0$.

(b) For the second case: from $\beta \in R \setminus \mathfrak{p}$, it follows that P is a separable polynomial. Otherwise, if P has α as a double root, then from $P'(X) = 3^n X^{3^n - 1}$ we get $\alpha = 0$ which means that $\beta \in \mathfrak{p}$ and complete the proof in this case.

□

We are going in table 1 to schematizes our results:

TABLE 1. monogeneity in local case

$v_{\mathfrak{p}}(\beta)\ \geq\ 1$	α is PBG iff $v_\pi(\beta)=1$		
$v_{\mathfrak{p}}(\beta)=0$	$c_k\ \neq\ 3$	$c_k=3$	
	α is PBG	$f\geq n$	$f<n$ and $n-rf\leq f$
		α is a PBG iff $v_\pi(\beta^{m-1}-1)=1$	α is a PGB iff $v_\pi(\beta^{m^{r+1}-1}-1)=1$

Remark 2.1. (1) *We can replace the two properties* (2.1) *and* (2.2) *with the following:*

$$v_\pi(\beta^{m^{r+1}-1}-1)=1\,,$$

where r is the smallest positif integer such that $n-rf\leq f$.

(2) *In the case of the characteristic of k equal to 3, we can checks that the condition $v_\pi(\beta^{m-1}-1)=1$, is equivalent to: β is not a 3-power modulo π^2*

3. MONOGENEITY OF RELATIVE CUBIC-POWER PURE EXTENSION - DEDEKIND CASE

Let R be a Dedekind ring, K its fraction field, L a finite separable extension over K and $\mathcal{O}_L$ the integral closure of R in L. Let $\alpha\in\ \mathcal{O}_L$ be an algebraic integer over R such that $L=K(\alpha)$. Let $P\in R[X]$ be the monic minimal polynomial of α.

The index of α is defined as the module index $Ind_R(\alpha)\ :=\ [\mathcal{O}_L\ :\ \mathcal{O}_K[\alpha]]$. Obviously, α is a PBG of L over K if and only if $(\mathcal{O}_L)_{\mathfrak{p}}=R_{\mathfrak{p}}[\alpha]$, 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 ;

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

We 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 $V(\mathfrak{I}^n) = V(\mathfrak{I})$.

Now, fix a non-zero prime ideal $\mathfrak{p} \in Spec\,(R)$. We are also interested in the set of primes $\mathfrak{q}$ in $\mathcal{O}_L$ with $\mathfrak{p} \subseteq \mathfrak{q}$ $-$or equivalently $\mathfrak{p} = \mathfrak{q}\,\cap R-$ and we call that set for the fibre over $\mathfrak{p}$, denoted by $\mathfrak{F}ib_R(\mathfrak{p})$.

Theorem 3.1. *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 $P = X^{3^n} - \beta \in R[X]$ 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 $\mathfrak{q} \in \mathfrak{F}ib_R(3)$, then α is a PBG of L over K if and only if β is square free.*
2. *Let $\mathfrak{F}ib_R(3) - V(\beta R) = \{\mathfrak{p}_1; ...; \mathfrak{p}_h\}$. 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 $R/\mathfrak{p}_i$. Then α is a PBG of L over K if and only if " β is square free" and for all $i \in \{1; ....; h\}$*

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

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

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 $f_i < n$.

Proof. Our proof starts with the observation that the discriminant of $P(X)$ is $Disc_R(P) = 27^{p^2}\beta^{3^p-1}$, then the set $S_P = V(\beta\, R) \cup (\mathfrak{F}ib_R(3) - V(\beta\, R))$ 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. We may then use Theorem 2.1.

(1) Our condition in the first case implies that $S_P = V(\beta\, R)$. Let $\mathfrak{p} \in V(\beta R)$, then by Theorem 2.1, 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 $charR/\mathfrak{p}_i = 3$ (the characteristic of the field $R/\mathfrak{p}_i$ is equal to 3 since $3R \subset \mathfrak{p}_i$). According to the second case in Theorem 2.1, 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 $f_i \geq n$. 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.

□

Remark 3.1. *Theorem 3.1 is a generalization in relative case of p-power extension for $p = 3$, studied in [4] Theorem 4.2.*

4. 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 $\mathcal{O}_K$ of K is $\mathcal{O}_K = \mathbb{Z}[t]$ such that:

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

And the discriminant is given by:

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

Theorem 4.1. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension such that d is square free $d \equiv 0$ modulo 3. Let $L = K(\alpha)$ such that $\alpha^{3^n} = b = \sqrt{d} + 1$ ($n \in \mathbb{N}^*$), furthermore we assume that the ideal $(\sqrt{d} + 1)$ is square free in $\mathcal{O}_K$, then L/K is monogenic. In this case we note that:*

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{3^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{3^n-1}\}.$$

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

Proof. First of all we note that $v_{\mathfrak{p}}(b) = 0$ where $3O_K = \mathfrak{p}^2$, it is known that the cardinality of $\mathcal{O}_K/\mathfrak{p}$ is 3 since the residual degree of $\mathfrak{p}$ is $f = 1$ then two cases arises:

(1) If $n = 1$, then by Theorem 3.1, L/K is monogenic if and only if $v_{\mathfrak{p}}(b^2 - 1) = 1$, we have $b^2 - 1 = d + 2\sqrt{d} = \sqrt{d}(\sqrt{d}+2)$. Since $v_3(d) = 1$ (d square free and $d \equiv 0 \mod 3$) then, $v_{\mathfrak{p}}(\sqrt{d}) = \frac{1}{2}v_{\mathfrak{p}}(d) = \frac{1}{2}e_{K/\mathbb{Q}}v_3(d) = 1$. Since otherwise by property of dominance principle $v_{\mathfrak{p}}(\sqrt{d}+2) = 0$. So, we can deduce that $v_{\mathfrak{p}}(b^2 - 1) = 1$.

(2) If $n \geq 2$, it follows by Theorem 3.1, that α is a power basis generator if and only if $v_{\mathfrak{p}}(b^{3^n-1} - 1) = 1$ we have that

$$b^{3^n-1} - 1 = \sum_{k=1}^{3^n-1} \binom{k}{3^n - 1}(\sqrt{d})^k = \sqrt{d}\left(\sum_{k=1}^{3^n-1} \binom{k}{3^n - 1}(\sqrt{d})^{k-1}\right),$$

by property of dominance principle, it is easy to check that

$$v_{\mathfrak{p}}(\sum_{k=1}^{3^n-1} \binom{k}{3^n - 1}(\sqrt{d})^{k-1}) = 0$$

and so,

$$v_{\mathfrak{p}}(b^{3^n-1} - 1) = v_{\mathfrak{p}}(\sqrt{d}) + v_{\mathfrak{p}}(\sum_{k=1}^{3^n-1} \binom{k}{3^n - 1}(\sqrt{d})^{k-1}) = 1.$$

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

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{3^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{3^n-1}\}$$

is an integral basis of L over $\mathbb{Q}$ of degree $2 \cdot 3^n$. □

Theorem 4.2. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension such that d is square free, $3 \nmid d$ and $d \equiv 2$ modulo 9. Let $L = K(\alpha)$ such that $\alpha^{3^n} = b = \sqrt{d} + 1$ ($n = 1, 2$), furthermore we assume that the ideal $(\sqrt{d} + 1)$ is square free in $\mathcal{O}_K$ and $3\mathbb{Z}$ is inert in $\mathcal{O}_K$, then L/K is monogenic. In this case we note that:*

$$\mathfrak{B} = \{1; \alpha; \alpha^2; ...; \alpha^{3^n-1}; t; t\alpha; t\alpha^2; ...; t\alpha^{3^n-1}\}.$$

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

Proof. The ideal $3\mathcal{O}_K = \mathfrak{p}$ is prime in $\mathcal{O}_K$. We claim that $v_{\mathfrak{p}}(b + 1) = 0$, we have $v_{\mathfrak{p}}(b^2 - 2b - 1) = v_{\mathfrak{p}}(d - 2) \geq 1$ then $v_{\mathfrak{p}}(b^2 - 2b) = 0$ and $v_{\mathfrak{p}}(b - 2) = 0$ (since $v_{\mathfrak{p}}(b) = 0$), therefore $v_{\mathfrak{p}}(b + 1) = v_{\mathfrak{p}}(b - 2 + 3) = inf(v_{\mathfrak{p}}(b - 2), v_{\mathfrak{p}}(3)) = 0$.
By Theorem 3.1 it is known that L/K is monogenic if and only if $v_{\mathfrak{p}}(b^8 - 1) = 1$.

we already have that $b^8-1=\sqrt{d}(b^7+b^6+b^5+\ldots+1)$, put $h=b^7+b^6+b^5+\ldots+1$, expressing h as a polynomial in $\alpha=d-2$, we get

$$h=\underbrace{(b+7)\alpha^3}_{A}+\underbrace{(34b+70)\alpha^2}_{B}+\underbrace{(194b+182)\alpha}_{C}+\underbrace{(288b+120)}_{D}.$$

we calculate the valuation of every term of h,

- $v_{\mathfrak{p}}(D)=1$ since $v_{\mathfrak{p}}(120)=1$ and $v_{\mathfrak{p}}(288b)=2$.
- $v_{\mathfrak{p}}(C)=v_{\mathfrak{p}}(\alpha)+v_{\mathfrak{p}}(194(b+1)-9)=v_{\mathfrak{p}}(\alpha)$ since $v_{\mathfrak{p}}(9)=2$ and $v_{\mathfrak{p}}(194(b+1))=0$.
- $v_{\mathfrak{p}}(B)=2v_{\mathfrak{p}}(\alpha)+v_{\mathfrak{p}}(34(b+1)+36)=2v_{\mathfrak{p}}(\alpha)+0$ since $v_{\mathfrak{p}}(36)=2$ and $v_{\mathfrak{p}}(34(b+1))=0$.
- $v_{\mathfrak{p}}(A)=3v_{\mathfrak{p}}(\alpha)+v_{\mathfrak{p}}((b+1)+6)=3v_{\mathfrak{p}}(\alpha)+0$ since $v_{\mathfrak{p}}(b+1)=0$ and $v_{\mathfrak{p}}(6)=1$.

As we assumed that $d\equiv 2$ modulo 9, $v_{\mathfrak{p}}(\alpha)\geq 2$ which means that $3v_{\mathfrak{p}}(\alpha)>2v_{\mathfrak{p}}(\alpha)>v_{\mathfrak{p}}(\alpha)>v_{\mathfrak{p}}(D)$ then $v_{\mathfrak{p}}(A)>v_{\mathfrak{p}}(B)>v_{\mathfrak{p}}(C)>v_{\mathfrak{p}}(D)=1$, as a result we get $v_{\mathfrak{p}}(b^8-1)=1$, thus L/K is monogenic.
Let denote $\{1;\alpha;\alpha^2;...;\alpha^{3^n-1}\}$ such RMIB. Using [3, Lemma 3.1] it's obvious that

$$\mathfrak{B}=\{1;\alpha;\alpha^2;...;\alpha^{3^n-1};t;t\alpha;t\alpha^2;...;t\alpha^{3^n-1}\}$$

is an integral basis of L over $\mathbb{Q}$ of degree $2\cdot 3^n$. □

Corollary 4.1. *With previous conditions in Theorem 4.1 and Theorem 4.2, the discriminant $D_{L/\mathbb{Q}}$ is given by:*

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

Proof. Since L/K is monogenic we obtain $D_{L/K}=(3^n)^{3^n}\beta^{3^n-1}$, then $N_{K/\mathbb{Q}}(D_{L/K})=3^{2n.3^n}N_{L/K}(\beta)$ and the norm of $\sqrt{d}+1$ is $N_{K/\mathbb{Q}}(\beta)=1-d$, by discriminant tower formula (1.1) it follows that:

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

□

Remark 4.1. *The number field $L/\mathbb{Q}$ is not seen as composite fields which split algebraically or arithmetically.*

ACKNOWLEDGMENT

The authors would like to thank the Department of Computer Science, Logistics and Mathematics, Ensa-Kenitra, Ibn Tofail University, MOROCCO, Department of Mathematics, FSDMFES, Sidi Mohamed Ben Abdellah University, MOROCCO and especially professor M. E. Charkani for its valued support.

REFERENCES

[1] P. H. CASSOU-NOGUÉS, M. J. TAYLOR: *A Note on elliptic curves and the monogeneity of rings of integers*, J. London Math. Soc., **37** (2) (1988), 63–72.

[2] P. H. CASSOU-NOGUÈS, M. J. TAYLOR: *Uniés Modulaires et monogénéité d'anneaux d'entiers*, Séminaire de Théorie des nombres, Paris, **75**(3) (1989), 347–353.

[3] M. E. CHARKANI, M. SAHMOUDI: *Sextic Extension with cubic subfield*, JP Journal of Algebra, Number Theory et Applications, **34**(2) (2014), 139–150.

[4] M. E. CHARKANI, O. LAHLOU: *On Dedekind's criterion and monogenicity over Dedekind rings*, Int. J. of Math. and Math. Sci. **2003** (2003), 4455–4464.

[5] 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** (1878), 1–23.

[6] A. FRÖHLICH, M. J. TAYLOR: *Algebraic number Theory*, Combridge Studies in Advenced Mathematics, **27**, Cambridge University Press, 1993.

[7] G. FUJISAKI: *Some examples of number fields without relative integral bases*, J. Fac. Sei. Univ. Tokyo Sect. **21** (1974), 92–95.

[8] M. N. GRAS: *Lien entre le groupe des unités et la monogénéité des corps cubiques cycliques*, Publ. Math. Fac. Sci. Besançon Théorie des nombres, (1975/1976) 19..

[9] 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**(3) (1986), 347–353.

[10] M. N. GRAS: *Conditions nécessaire de monogénéité de l'anneau des entiers d'une extension abélienne de Q*, "Séminaire de Théorie des nombres, Paris 1984-85", **63** (1986), 97–107.

[11] M. HAGHIGHI: *Relative integral basis for algebraic number fields*, Int. J. Math. Math. Sci., **6**(1) (1986), 97–104.

[12] M. KUMAR, S. KHANDUJA: *A Generalization of Dedekind Criterion*, Communication in Algebra, **35** (2007), 1479–1486.

[13] M. J. LAVALLEE, B. K. SPEARMAN, K. S. WILLIAMS: *Lifting Monogenic Cubic Fields to Monogenic Sextic Fields*, Kodai Math. J. **34** (2011), 410–425.

[14] R. MACKENZIE, J. SCHEUNEMAN: *A Number Field Without a Relative Integral Basis*, Amer. Math. Monthly, **78** (1971), 882–883.

[15] W. NARKIEWICZ: *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, Second Edition, 1990.

[16] J. NEUKIRCH: *Algebraic number theory*, SPRINGER PUBLICATION, 1999.

[17] M. Sahmoudi, A. Soullami: *On Sextic Integral Bases Using Relative Quadratic Extention*, Bol. Soc. Paran. Mat., **38**(4) (2020), 175–180.

[18] M. Sahmoudi: *Explicit integral basis for a family of sextic field*, Gulf J. Math., **4** (2016), 217–222.

[19] P. Schmid: *On criteria by Dedekind and Ore for integral ring extensions*, Arch. Math. **84** (2005), 304–310.

[20] B. K. Spearman, K. S. Williams: *Relative integral bases for quartic fields over quadratic subfields*, Acta Math. Hungar., **76** (1996), 185–192.

[21] L. C. Washington: *Relative integral bases*, Proceedings of the American Mathemtical Society, **56**, 1976.

Department of Computer Science, Logistics and Mathematics
Ibn Tofail University, Ensa
Kenitra, Morocco
Email address: mohammed.sahmoudi@uit.ac.ma

Department of Mathematics, FSDMFES, LSI
Sidi Mohamed Ben Abdellah University
Fez, Morocco
Email address: abderazak.soullami@usmba.ac.ma