On Sextic Integral Bases Using Relative Quadratic Extension

M. Sahmoudi and A. Soullami

Abstract: Let $K = \mathbb{Q}(\theta)$ be a cubic number field and $P(X) = X^3 - aX - b$ ($a, b \in \mathbb{Z}$), the monic irreducible polynomial of $\theta$. In this paper we give sufficient conditions on $a, b$ which ensure that $\theta$ is a power basis generator, also we give conditions on relative quadratic extension to be monogenic. As a consequence of this theoretical result we can reach an integral basis of some sextic fields which Neither algebraically split nor arithmetically split.

Key Words: Dedekind ring, Monogenicity, Relative power integral basis, Integral basis.

1. Introduction

The search of integral bases and Monogeneity are classical topic of algebraic number theory c.f. [3], [9] and [8]. Let $K \subseteq L$ be algebraic number fields with $[L : K] = n$, denote by $O_K$ and $O_L$ the rings of integers of $K$ and $L$, respectively. The field $L$ possess a power basis generator (PBG) if there exists an algebraic integer $\alpha$ such that: $\{1, \alpha, ..., \alpha^{n-1}\}$ forms a basis of $O_L$, so, $L$ is called monogenic relative over $K$ (for $K \neq \mathbb{Q}$).

The main result of this paper is a generalization of sufficient condition given by Dedekind for quadratic number field to relative quadratic number field (Theorem 3.1). As well we give a simplest sufficient condition for cubic number field to have monogenic basis (Theorem 3.3). As a consequence, if $K$ is a cubic field and $L = K(\alpha)$ with $\alpha^2 \in \mathbb{Z}$ it has proved that the rings of integers of $L$ admits an integral basis over $\mathbb{Z}$ See [3]. we want to solve the same problem for a family of sextic fields with $\alpha^2 \in O_K \setminus \mathbb{Z}$, for this we prove that the field $L$ is relatively

2010 Mathematics Subject Classification: 35B40, 35L70.
Submitted October 16, 2017. Published December 28, 2017

Typeset by 2SPM style.
© Soc. Paran. de Mat.
monogenic over $K$ under the conditions stated above. As a consequence, we obtain a straightforward computation of discriminant $d_{L/Q}$ given by the formula

$$d_{L/Q} = N_{K/Q}(d_{L/K})(d_{K/Q})^{[L:K]}$$

where $N_{K/Q}$ denote the norm from $K$ over $Q$.

2. Preliminaries

In the following we shall say that an ideal $a$ of a Dedekind ring $R$ is a square free ideal in $R$ if $\nu_p(a) \leq 1$ for any prime ideal $p$ in $R$. An element $d$ of a Dedekind ring $R$ is said a square free element in $R$ if the ideal $dR$ is a square free ideal of $R$. This implies that $d \in R - R^2$.

For each prime $p$ and each non zero algebraic integer $m$, $\nu_p(m)$ denotes the greatest nonnegative integer $l$ such that $p^l$ divides $m$.

For any polynomial $P$, we denote by $S_P$ the set of prime square divisors of $\text{disc}P$:

$$S_P = \{ p \in \text{spec}R \mid p^2 \text{divides } \text{disc}P \}.$$  

The set $S_P$ is very useful to use Dedekind Criterium in order to know whether the ring of integers of $L$ has a power basis generators over $K$ or not.

Hereinafter, we recall the result that gives necessary and sufficient conditions for an extension $L/K$ to be monogenic.

**Theorem 2.1.** [5, Theorem 2.1.]. Let $R$ be a Dedekind ring, $K$ its quotient field, $L$ a finite separable extension of $K$, $O_L$ the integral closure of $R$ in $L$, $\alpha \in O_L$ a primitive element of $L$, and $P(X) \in R[X]$ the monic irreducible polynomial of $\alpha$ over $R$. For a fixed prime ideal $p$ of $R$, let the decomposition of $P$ into monic irreducible polynomials in $R/p[X]$ take the form

$$P(X) = \prod_{i=1}^{r} P_i^{e_i}(X) \in R/p[X].$$  

(2.1)

For $i = 1, \ldots, r$, let $P_i \in R[X]$ be a monic lift of $P_i$, set

$$G(X) = \prod_{1 \leq i \leq r, e_i \geq 2} P_i(X), \quad H(X) = \prod_{i=1}^{r} P_i^{e_i}(X)/G(X),$$  

(2.2)

where the empty product is to mean that $G(X) = 1$, and let $P(X) = G(X)H(X) + aT(X)$ for some $T(X) \in R[X]$ and $a \in p \setminus p^2$. Then, If $\text{disc}_R(P)$ is not square free, then the following are equivalent:

1. $\alpha$ is a PBG for $O_L$ over $R$.

2. For any prime ideal $p \in S_P$, either ($P$ is square free in $R/p[X]$) or ($P$ is not square free in $(R/p)[X]$ and in this case $T \equiv 0 \mod p$ and $\nu_p(\text{Res}(P,G)) = \deg(G)$).
3. Relative and absolute monogenicity

Our first main result study monogenicity of relative quadratic extension. For the second, we give sufficient condition for a extension to have a PBG.

**Theorem 3.1.** Let $R$ be a Dedekind ring with quotient field $K$. Let $L = K(\alpha)$ be a pure quadratic extension of $K$, where $\alpha$ is a root of a monic irreducible polynomial $P(X) = X^2 - d \in R[X]$. Assume that: for all prime $p$ such that $v_p(2d) \geq 1$ we have $d - 1 \in p \setminus p^2$. Then $\alpha$ is a PBG of $L/K$.

**Proof:** Let $p \in S_P$. As $\text{disc}_R(P) = 4dR$, then $p\vert 4d$ yields $v_p(2) + v_p(2d) \geq 1$. It is clear that $v_p(2d) \geq 1$, This allows us to write $v_p(d - 1) = 1$, hence by dominance principal theorem that $v_p(d) = 0$. By reducing $P$ modulo $p$ yields $X^2 - d = (X - 1)^2$. Then, by keeping the notation of Theorem 2.1, we have, $P(X) = G(X)H(X) + aT(X)$ with $G(X) = H(X) = X - 1$ and $T(X) = \frac{2X - 1 + d}{a}$ for some $a \in p \setminus p^2$. Moreover, $\text{Res}_R(X^2 - d, X - 1) = (-d + 1)R$. Then $v_p(\text{Res}_R(X^2 - d, X - 1)) = v_p((d - 1)R) = 1$. So $\alpha$ is a PBG of $L/K$. □

**Corollary 3.2.** Let $L = K(\alpha)$, using the notations of theorem 3.1, the discriminant $d_{L/K}$ of $L$ is given by: $d_{L/K} = 4dR$.

**Proof:** The proof is based on the index formula: $\text{disc}_R(P) = \text{ind}_R(\alpha)^2d_{L/K}$. Since $\alpha$ is a PBG, by Theorem 3.1, we have $\text{ind}_R(\alpha) = R$ and therefore $\text{disc}_R(P) = d_{L/K}$, which suffices to show that $d_{L/K} = 4dR$. □

Let $K = \mathbb{Q}(\theta)$ be a cubic field, where $\theta$ is a root of the monic irreducible polynomial

$$X^3 - aX - b = 0, \quad a, b \in \mathbb{Z}.$$ 

The discriminant of $\theta$ is $\delta = 4a^3 - 27b^2$ and $\delta = \text{ind}_\mathbb{Z}(\theta)^2d(K/\mathbb{Q})$, where $d(K/\mathbb{Q})$ denotes the discriminant of $K$, and $\text{ind}_\mathbb{Z}(\theta)$ is the index of $\theta$.

**Theorem 3.3.** Under the assumptions above and in addition, we may assume that:

1. $3 \nmid b, \quad a = 3 + 3^2A; \quad b = 2 + 3B$ with $3 \nmid AB$,
2. If $p \equiv 1 \mod 3$ and $p \mid \delta$, then $v_p(a) = v_p(b) = 1$.
3. $\delta$ is square without prime divisors congruent to $2 \mod 3$.

Then, $\theta$ is a power basis generator of $K/\mathbb{Q}$.

**Proof:** The discriminant $\delta$ is given by $\delta = 3^2 \prod_{3 < p \mid \delta} p^2$ (See [6]). Let $p \in S_P$, yields the only primes $p$ of $\mathbb{Z}$ such that $p^2$ divides $\delta$ are $p = 3$ or $p \equiv 1 \mod 3$. Let us first examine the case $p = 3$. Reducing $P$ modulo $3$, yields $P(X) \equiv X^3 - b \mod 3$. Since $b \equiv 2 \mod 3$. Hence, $P(X) \equiv (X + 1)^3 \mod 3$. Letting $P(X) = (X + 1)^3 - 3X^2 - (3 + a)X - (b + 1)$, we put $b + 1 = 3b'$ and $3 + a = 3(1 + a')$, then
$P(X) = (X + 1)^3 + 3T(X)$ with $T(X) = -X^2 - (1 + a')X - b'$. Hence, $\overline{T} \not\equiv \overline{0}$ modulo 3 as desired. Moreover, $Res_Z(X^3 - aX - b, X + 1) = b - a + 1$. By dominance principal theorem, we check that $v_3(b - a + 1) = v_3(b - 2 - (a - 3)) = Inf(v_3(b - 2), v_3(a - 3)) = 1$. Then $\nu_3(Res_Z(X^3 - aX - b, X + 1)) = deg(X + 1))$. Secondly, assume now that the prime $p$ in $S_p$ verifies $p \equiv 1 \mod 3$, reducing $P$ modulo $p$ yields, since $v_p(a) = v_p(b) = 1$, $P(X) \equiv X^3 \mod p$.

Then, by keeping the notation of Theorem 2.1, we have, $P(X) = G(X)H(X) + p.T(X)$ with $G(X) = X$, $H(X) = X^2$ and $T(X) = -p(\frac{2}{p} X + \frac{2}{p})$. Since $v_p(a) = 1$, $\overline{T} \not\equiv \overline{0}$ modulo $p$. The task is now to compute $Res_Z(X^3 - aX - b, X)$, so, by using a computing package, such as (Maple) it can be checked that $Res_Z(X^p - aX - b, X) = b$, hence, $v_p(Res_Z(X^3 - aX - b, X)) = v_p(b) = deg(G)$, which completes the proof the second case.

\[ \Box \]

4. Illustration

4.1. Integral basis of sextic extension

In [3] it was considered sextic fields that are composites of subfields. In the following case we consider the sextic field $L$. Neither algebraically split nor arithmetically split see ([4, III.2.13]).

Let $\alpha \in O_L$ be a primitive element of $L/K$ ($L = K(\alpha)$) with $\alpha^2 \in O_K \setminus \mathbb{Z}$.

**Theorem 4.1.** Let $K = \mathbb{Q}(\theta)$ be a cubic field as in Theorem 3.3. Let $L = K(\alpha)$ a pure quadratic extension of $K$, where $\alpha$ is a root of a monic irreducible polynomial $P(X) = X^2 - d \in O_K[X]$. Suppose that for all prime $p$ such that $v_p(2d) \geq 1$ we have $d - 1 \in p \setminus p^2$. Then the sextic fields $L = \mathbb{Q}(\alpha; \theta)$ has integral basis given by : \[ \{1, \theta, \theta^2, \alpha, \alpha\theta, \alpha\theta^2\}. \]

**Proof:** of Theorem 4.1 we know that $\mathcal{B}_L = \{1, \theta, \theta^2\}$ is an integral basis of $K$ over $\mathbb{Q}$. According to the Theorem 3.1 and Lemma [3, Lemma 3.1.], it is easily seen that $\{1, \theta, \theta^2, \alpha, \alpha\theta, \alpha\theta^2\}$ is an integral basis of $L$. $\Box$

**Corollary 4.2.** Under the assumptions and suppositions of Theorem 4.1. Let $d = u + v\theta + w\theta^2$, $(u, v, w) \in \mathbb{Z}^3$. The discriminant of the sextic field $L$ over $\mathbb{Q}$ is given by:

\[ d_{L/\mathbb{Q}} = 4^3(-abvw^3 + b^2w^2 + bu^3 + bu^3 - bw^2w + (aw + v)u^2 + (a^2w^2 - av^2 + (a - 2b)vw)u).\delta^2. \]

**Proof:** To compute discriminant we use [7, Proposition 13, p. 66 ], then we have $d_{L/\mathbb{Q}} = 4^3N_{K/\mathbb{Q}}(dR).\delta^2$. In the rest of this proof, we will give explicitly the norm of $d$, $N_{K/\mathbb{Q}}(dR)$. Let $m_d : K \rightarrow K$ the left multiplication by $d$ i.e., a $K$-linear transformation, we know that $N_{K/\mathbb{Q}}(dR) = det(m_d)$. To compute this norm, we will need in particular to compute explicitly $m_d(1)$, $m_d(\theta)$ and $m_d(\theta^2)$. Then by
using a computer algebra package (such as Maple) it can be checked that:

\[
\begin{align*}
m_d(1) &= u + v\theta + w\theta^2 \\
m_d(\theta) &= bw + (aw + w)\theta + v\theta^2 \\
m_d(\theta^2) &= vb + (aw + wb)\theta + (u + aw)\theta^2
\end{align*}
\]

we check that: \( \det(m_d) = -abvw^2 + b^2w^3 + bv\gamma - bv^2w + (aw + v)u^2 + (a^2w^2 - au^2 + (a - 2b)ew)u. \)

Remark 4.3. By considering \( d \in \mathbb{Z} \) we see that the discriminant simplifies to \( d_{L/Q} = 4^3d^2\delta^3 \), which has been proved in [3].

4.2. Monogenicity of sextic extension

We keep the same notation of Theorem 3.3 and Theorem 3.1. Like previous sections let \( L = \mathbb{Q}(\theta, \alpha) \). Set \( \gamma = \alpha + \theta \), using a computing package previously cited, we can checked that the minimal polynomial of \( \gamma \) is given by:

\[
F(X) = \text{Irrd}(\gamma, \mathbb{Z}) = X^6 + cX^5 + eX^4 + fX^3 + gX^2 + hX + i, \text{ where:}
\]

\[
\begin{align*}
c &= 0, \quad e = -2aw - 2a - 3u, \quad f = -2b - 6bw - 4av \\
g &= a^2w^2 - 2a^2w - 3bvw + 4uwa + a^3 + 3u^2 - v^2a - 9bv \\
h &= 2bw^2a - 4bwa + 6awb + 2ba - 6v^2b - 6bu + 4uwa \\
i &= -ua^2w^2 + 2ua^2w - ua^4 + avu^2b - 2u^2wa - 2avwb + avb + 2a^2u \\
&\quad +uv^2a - b^2w^3 + 3b^2w^2 - 3bwvu - 3b^2w - u^3 - v^3b - 3bv + b^2
\end{align*}
\]

Then \( L = \mathbb{Q}(\gamma) \) and hence the index is:

\[
\text{Ind}_{\mathbb{Z}}(\gamma) = \frac{\pi\lambda(-3bwvu + u^3 + v^3b + 2wu^2a - uav^2 + ua^2w^2 - aw^2vb + b^2w^3)}{(-w^6b^2 - 6w^5b^2 + 24w^4bvu - 32wuav^2 - v^4a^2w^4 - 4v^2aw^3 + 12v^4u + 40aw^3 + 20a^3w - 40aw^3 + 7a^2u^2 - 54b^2w + 9b^2w^2 + 28b^2w^3 - 26b^2 + 27b^2 + 64u^3 - 4aw^3 - v^2 - 20u^2a^2w + 2awv^2b + 4aw^2u^2 - 20u^2a^2 - 2uv^2 + 72bvu - 54uavb - 2u^3vb + 18u^4avb + 12uw^2ab + 54uv^3b + 36u^2a^2 - 96a^2 - 48u^2v^2 + 128uw^2a - 112au^2w + 32uav^2 + 120uv^2 - 32w^2ua^2 + 2uw^2a + 24w^3bvu - 48uv^2a^2 + 4u^4a^2 + 18u^2a^2w - 30w^2v^3b - 12buvvu - 124uw^2vb + 150uavvb - 3u^4b^2).}
\]

Where: \( \lambda = (aw^2vb + b^2w^3 + v^2b - buvw^2 + wuva + u^2 + u^2w^2 - uaw^2 + uwva - 2bwvu)^{2}. \)

Remark 4.4. The presented method permits to check whether a particular element generates a power basis of \( L \) over \( \mathbb{Q} \). For example, by the particular case where \( d = \theta + \theta^2 \), we get \( \text{Ind}_{\mathbb{Z}}(\gamma)^2 = \frac{aw^2v + b^2w^3 + v^2b - buvw^2 + wuva + u^2 + u^2w^2 - uaw^2 + uwva - 2bwvu}{2} \) hence \( \gamma \) it not a power integral basis.

References


Mohammed Sahmoudi,
LAGA Laboratory,
Faculty of Sciences, Dhar El Mahraz,
P. O. Box 1796, Atlas-Fez
Morocco.
E-mail address: mohamed-sahmoudi@usmba.ac.ma

and

Soullami Abderazak,
Department of Mathematics,
Faculty of Sciences, Dhar El Mahraz,
P. O. Box 1796, Atlas-Fez
Morocco.
E-mail address: abderazak.soullami@usmba.ac.ma