Bol. Soc. Paran. Mat. (3s.) **v. 38** 4 (2020): 175–180.
©SPM –ISSN-2175-1188 ON LINE ISSN-00378712 IN PRESS
SPM: www.spm.uem.br/bspm doi:10.5269/bspm.v38i4.40042

On Sextic Integral Bases Using Relative Quadratic Extention

M. Sahmoudi and A. Soullami

ABSTRACT: Let $K = \mathbb{Q}(\theta)$ be a cubic number filed and $P(X) = X^3 - aX - b$ (a, b in $\mathbb{Z}$), the monic irreducible polynomial of θ. In this paper we give a sufficient conditions on a,b which ensure that θ 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.

Contents

1. Introduction

The search of integral bases and Monogenity 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 α 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 $\alpha^2 \in O_K \backslash \mathbb{Z}$, for this we prove that the field L is relatively

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

monogenic over K under the conditions stated above. As a consequence, we obtain a straightforward computation of discriminant $d_{L/\mathbb{Q}}$ given by the formula

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

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

2. Preliminaries

In the following we shall say that an ideal $\mathfrak{a}$ of a dedekind ring R is a square free ideal in R if $\nu_{\mathfrak{p}}(\mathfrak{a}) \leq 1$ for any prime ideal $\mathfrak{p}$ 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 $\mathfrak{p}$ and each non zero algebraic integer m, $\upsilon_p(m)$ 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 $discP$:

$$S_P = \{\, \mathfrak{p} \in specR \mid \mathfrak{p}^2 divides\, discP \,\}.$$

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 α over R. For a fixed prime ideal $\mathfrak{p}$ of R, let the decomposition of P into monic irreducible polynomials in $R/\mathfrak{p}[X]$ take the form*

$$\overline{P(X)} = \prod_{i=1}^{r} \overline{P_i}^{e_i}(X) \in R/\mathfrak{p}[X]. \tag{2.1}$$

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

$$G(X) = \prod_{1\leq i\leq r, e_i\geq 2} P_i(X),\ H(X) = \prod_{i=1}^{r} P_i^{e_i}(X)/G(X), \tag{2.2}$$

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 $a \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then, If $disc_R(P)$ is not square free, then the following are equivalent:

1. *α is a PBG for O_L over R.*
2. *For any prime ideal $\mathfrak{p} \in S_P$, either (P is square free in $R/\mathfrak{p}[X]$) or (P is not square free in $(R/\mathfrak{p})[X]$ and in this case $T \neq 0\, modulo\, \mathfrak{p}$ and $\nu_{\mathfrak{p}}(Res(P, G)) = deg(G)$).*

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 α is a root of a monic irreducible polynomial $P(X) = X^2 - d \in R[X]$. Assume that: for all prime $\mathfrak{p}$ such that $\upsilon_{\mathfrak{p}}(2d) \geq 1$ we have $d - 1 \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then α is a PBG of L/K.*

Proof: Let $\mathfrak{p} \in S_P$. As $\mathrm{disc}_R(P) = 4dR$, then $\mathfrak{p}|4d$ yields $\upsilon_{\mathfrak{p}}(2) + \upsilon_{\mathfrak{p}}(2d) \geq 1$. It is clear that $\upsilon_{\mathfrak{p}}(2d) \geq 1$, This allows us to write $\upsilon_{\mathfrak{p}}(d-1) = 1$, hence by dominance principal theorem that $\upsilon_{\mathfrak{p}}(d) = 0$. By reducing P modulo $\mathfrak{p}$ yields $\overline{X^2 - d} = \overline{(X-1)}^2$. Then, by keeping the notation of Theorem 2.1, we have, $P(X) = G(X)H(X) + a.T(X)$ with $G(X) = H(X) = X-1$ and $T(X) = \frac{2X-1+d}{a}$ for some a in $\mathfrak{p} \setminus \mathfrak{p}^2$. Moreover, $Res_R(X^2 - d, X-1) = (-d+1)R$. Then $\nu_{\mathfrak{p}}(Res_R(X^2 - d, X-1)) = \nu_{\mathfrak{p}}((d-1)R) = 1$. So α 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: $disc_R(P) = ind_R(\alpha)^2 d_{L/K}$. Since α is a PBG, by Theorem 3.1, we have $ind_R(\alpha) = R$ and therefore $disc_R(P) = d_{L/K}$, which suffices to show that $d_{L/K} = 4dR$. □

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

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

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

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

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

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

Proof: The discriminant δ is given by $\delta = 3^2 \prod_{3<p|\delta} p^2$ (See [6]). Let $p \in S_P$, yields the only primes p of $\mathbb{Z}$ such that p^2 divides δ 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, $Res_{\mathbb{Z}}(X^3 - aX - b, X+1) = b - a + 1$. By dominance principal theorem, we check that $\upsilon_3(b-a+1) = \upsilon_3(b-2-(a-3)) = Inf(\upsilon_3(b-2), \upsilon_3(a-3) = 1)$. Then $\nu_3(Res_{\mathbb{Z}}(X^3 - aX - b, X+1) = deg(X+1))$. Secondly, assume now that the prime p in S_p verifies $p \equiv 1 \, mod \, 3$, reducing P modulo p yields, since $\upsilon_p(a) = \upsilon_p(b) = 1$, $P(X) \equiv X^3 \, mod \, p$.

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 $T(X) = -p(\frac{a}{p}X + \frac{b}{p})$. Since $\upsilon_p(a) = 1$, $\overline{T} \not\equiv \overline{0} \, modulo \, p$. The task is now to compute $Res_{\mathbb{Z}}(X^3 - aX - b, X)$, so, by using a computing package, such as (Maple) it can be checked that $Res_{\mathbb{Z}}(X^p - aX - b, X) = b$, hence, $\nu_p(Res_{\mathbb{Z}}(X^3 - aX - b, X)) = \nu_p(b) = deg(G)$, which completes the proof the second case.

□

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 $\alpha^2 \in O_K \backslash \mathbb{Z}$.

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 α is a root of a monic irreducible polynomial $P(X) = X^2 - d \in O_K[X]$. Suppose that for all prime $\mathfrak{p}$ such that $\upsilon_{\mathfrak{p}}(2d) \geq 1$ we have $d - 1 \in \mathfrak{p} \setminus \mathfrak{p}^2$. 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 $\mathcal{B}_c = \{1, \theta, \theta^2\}$ 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. □

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:*

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

Proof: To compute discriminant we use [7, Proposition 13, p. 66], then we have $d_{L/\mathbb{Q}} = 4^3 N_{K/\mathbb{Q}}(dR).\delta^2$. In the rest of this proof, we will give explicitly the norm of d, $N_{K/\mathbb{Q}}(dR)$. Let $m_d : K \mapsto K$ 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:

$$\begin{cases} m_d(1) = u + v\theta + w\theta^2 \\ m_d(\theta) = bw + (aw+u)\theta + v\theta^2 \\ m_d(\theta^2) = vb + (va+wb)\theta + (u+aw)\theta^2 \end{cases}$$

we check that; $det(m_d) = -abvw^2 + b^2w^3 + bv^3 - bv^2w + (aw+v)u^2 + (a^2w^2 - av^2 + (a-2b)vw)u$. □

Remark 4.3. *By considering $d \in \mathbb{Z}$ we see that the discriminant simplifies to $d_{L/\mathbb{Q}} = 4^3d^2\delta^2$, 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 γ is given by:
$F(X) = Irrd(\gamma, \mathbb{Z}) = X^6 + cX^5 + eX^4 + fX^3 + gX^2 + hX + i$, where:

$$\begin{cases} c & = 0, \quad e = -2aw - 2a - 3u, \quad f = -2b - 6bw - 4av \\ g & = a^2w^2 - 2a^2w - 3bvw + 4uwa + a^2 + 3u^2 - v^2a - 9bv \\ h & = 2bw^2a - 4bwa + 6uwb + 2ba - 6v^2b - 6bu + 4uva \\ i & = -ua^2w^2 + 2ua^2w - ua^2 + avw^2b - 2u^2wa - 2avwb + avb + 2au^2 \\ & \quad +uv^2a - b^2w^3 + 3b^2w^2 + 3bvwu - 3b^2w - u^3 - v^3b - 3bvu + b^2 \end{cases}$$

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

$\mathrm{Ind}_{\mathbb{Z}}(\gamma) = \mp\lambda(-3bwvu + u^3 + v^3b + 2wu^2a - uav^2 + ua^2w^2 - aw^2vb + b^2w^3)^{\frac{1}{2}}$ $(-w^6b^2 - 6w^5b^2 + 24w^2bvu - 32wuav^2 - v^2a^2w^4 - 4v^2a^2w^3 + 12v^4u + 40a^3w^3 + 20a^3w - 40a^3w^2 + 7v^2a^2 - 54b^2w + 9b^2w^2 + 28b^2w^3 - 26v^3b + 27b^2 + 64u^3 - 4a^3 - v^6 - 20v^2a^2w + 2w^3v^3b + 4a^3w^5 - 20a^3w^4 - 2av^4 + 72bvu - 54avb - 2w^5avb + 18w^4avb + 12w^3vab + 54wv^3b + 36ua^2 - 96u^2a - 48u^2v^2 + 128wu^2a - 112ua^2w + 32uav^2 + 120ua^2w^2 - 32w^2u^2a + 2w^2v^4a + 24w^3bvu - 48w^3ua^2 + 4w^4ua^2 + 18v^2a^2w^2 - 30w^2v^3b - 120bwvu - 124aw^2vb + 150awvb - 3w^4b^2)$.
Where: $\lambda = (-aw^2vb + b^2w^3 + v^3b - bwv^2 + wu^2a + u^2v + ua^2w^2 - uav^2 + wuva - 2bwvu)^{\frac{1}{2}}$.

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 $Ind_{\mathbb{Z}}(\gamma)^2 = \frac{a-b-1}{a-b}$ hence γ it not a power integral basis.*

References

1. S. Alaca and K. S. Williams, *Introductory Algebraic Number Theory* , ISBN: 9780521540117, Cambridge University Press, 2004.

2. H. Cohen, H. C., *A Course in Computational Algebraic Number theory*, GTM vol. 138, Springer Verlag, Berlin, 1996.

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

4. A. Frohlich, A. F. and M. J. Taylor M. T., *Algebraic number theory* , Cambridge University Press, 1991.

5. M. Sahmoudi, M. S., *Explicit integral basis for a family of sextic field*, Gulf Journal of Mathematics, vol.4, No.4, 2016, 217-222.

6. P. Llorente, P. L. and E. Nart, N. N, *Effective determination of the decomposition of the rational prime in a cubic field*, Proc. American Math. Soc. , 87, (1983), 579-585

7. S. Lang, S. L., *Algebraic Number Theory*, Graduate Texts in Mathematics 110, Springer-Verlag New York , 1986.

8. A. Shahzad, A. S., N. Toru, N. T. and M. H. Sayed, M. S., *Power integral bases for certain pure sextic fields*, International Journal of Number Theory, World Scientific Publishing Company, Vol. 10, No. 8, 2014, 2257-2265.

9. B. K. Spearman, B. S. and K. S. Williams, K. W., *Relative integral bases for quartic fields over quadratic subfields*, Acta Math. Hungar., 70, 1996, 185-192.

Mohammed Sahmoudi,
LAGA Laboratory,
Faculty of Sciences, Dhar El Mahraz,
P. 0. 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. 0. Box 1796, Atlas-Fez
Morocco.
E-mail address: abderazak.soullami@usmba.ac.ma