Gulf Journal of Mathematics
Vol 4, Issue 4 (2016) 217-222

EXPLICIT INTEGRAL BASIS FOR A FAMILY OF SEXTIC FIELD

M. SAHMOUDI[1*]

Abstract. Let L be a sextic number field which is a relative quadratic over cyclic cubic subfield K. In this paper, we will explicitly construct an integral basis under appropriate technical hypotheses where L isn't split arithmetically. As a consequence of this theoretical result the discriminant $d_{L/\mathbb{Q}}$ of L will be straightforwardly computed.

1. Introduction

The search of an integral bases and Monogenity are classical topic of algebraic number theory c.f. [6], [3], [11], [12]. 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 is said to possess a power integral basis generator (PBG) if there exists an element $\alpha \in O_K$ such that: $O_L = O_K.1 + O_K.\alpha + ... + O_K.\alpha^{n-1}$, then the field L is called monogenic relative over K. Every quadratic number field is monogenic. There are many algorithms for deciding monogenity and determining generators of power integral basis. These procedures heavily depend on the degree and other properties of number fields, see [7]. It has already been proved that if $L = KE$ (we say that L split algebraically), without necessarily split arithmetically, with $K = \mathbb{Q}(\beta)$ and $E = \mathbb{Q}(\alpha)$, α satisfying $\alpha^2 \in \mathbb{Z}$, the ring O_L in L admits an integral basis over the ring $\mathbb{Z}$ of rational integers [3]. The purpose of this paper is to solve the same problem for a family of sextic fields. Namely, we give sufficient conditions on sextic field, $L = K(\alpha)$, which is a relative quadratic over cyclic cubic subfield K, with $\alpha^2 \in O_K \backslash \mathbb{Z}$, to admits an integral basis. We prove that the L is relatively monogenic over cyclic cubic subfield K under the conditions stated above. On the other hand, since K is cyclic cubic field, Gras [8], [9] and Archinard [1] have given necessary and sufficient conditions for K to be monogenic. In the present paper we utilize integral basis given in [4], to construct an integral basis for L. As a consequence, we obtain a straightforward computation of discriminant $d_{L/\mathbb{Q}}$ given by the formula

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

Date: Accepted: Oct 24, 2016.
* Corresponding author.
2010 *Mathematics Subject Classification.* 11R04, 11R11, 11R32, 11Y40.
Key words and phrases. Dedekind ring, monogenicity, relative integral basis, sextic extension
.

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

Definition 1.1. Let $k \subseteq K \subseteq L$ be a tower of number fields.

(1) We say that $L/K/k$ is algebraically split if there exists an extension E/k such that $L = KE$ over k,
(2) We say that $L/K/k$ is arithmetically split if there exists an extension E/k such that $L = KE$ and E is arithmetically disjoint from K over k, or equivalently, $(d_{K/k}, d_{E/k}) = O_k$ and K is linearly disjoint from E over k see (III.2.13 [5]).

2. Monogenicity of relative quadratic extension

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 $d \in R - R^2$. The converse is false.
Let n be an integer ($n \neq 0$) and a,b tow elements in a Dedekind ring R. We define the binary relation: $a \equiv b$ modulo n, if $a - b \in nR$.

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 $discP$:

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

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 integral basis generators over K or not.

Hereinafter, we recall the result that gives necessary and sufficient conditions for L to be monogenic.

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 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 $a \in p \setminus p^2$. 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* $R/\mathfrak{p}[X][X]$ *and in this case* $T \neq 0 \, modulo \, \mathfrak{p}$ *and* $\nu_{\mathfrak{p}}(Res(P,G)) = deg(G)$).

Proof. See (Theorem 3.1. [2]). □

We begin with a general result in witch we give a sufficient condition to have PBG for relative quadratic extension.

Theorem 2.2. *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* $P(X) = X^2 - d \in R[X]$. *Suppose that* $\upsilon_{\mathfrak{p}}(d) = 1$ *for all prime divisors* $\mathfrak{p}$ *such that* $\mathfrak{p}/2d$. *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 $\upsilon_{\mathfrak{p}}(2R)+\upsilon_{\mathfrak{p}}(2dR) \geq 1$. It is clear that $\upsilon_{\mathfrak{p}}(2dR) \geq 1$ otherwise, we must have $\upsilon_{\mathfrak{p}}(2R) \geq 1$ which contradicts the fact that $\mathfrak{p}$ does not divides $2dR$ and hence $\mathfrak{p}|2d$. Now with the supposition $\upsilon_{\mathfrak{p}}(d) = 1$, reducing P modulo $\mathfrak{p}$ yields $\overline{P(X)} = \overline{X^2}$. Then, by keeping the notation of Theorem 2.1, we have, $P(X) = G(X)H(X)+d.T(X)$ with $G(X) = H(X) = X$ and $T(X) = 1$. Moreover, $Res_R(X^2 - d, X) = dR$. Then $\nu_{\mathfrak{p}}(Res_R(X^2 - d, X)) = \nu_{mathfrakp}(dR) = 1$. So α is a PBG of O_L over O_K. □

Corollary 2.3. *Let* $L = K(\alpha)$, *using the notations of theorem 2.2, 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 2.2, we have $ind_R(\alpha) = R$ and therefore $disc_R(P) = d_{L/K}$, which suffices to show that $d_{L/K} = 4dR$. □

3. Integral basis of sextic extension with cyclic cubic subfield

Every cyclic cubic field K over the rational field $\mathbb{Q}$, which the prime 3 is ramified in K can be given in the form

$$K = \mathbb{Q}(\beta), \quad \beta^3 - 3e\beta + eu = 0 \tag{3.1}$$

where $e = \frac{u^2+3v^2}{4}$, $u \equiv 2 \, mod \, 3$, $3 \nmid v$, $3u \equiv v \, mod \, 2$, $v > 0$ and e is equal to a product of distinct primes congruent to 1 modulo 3 such that the polynomial $P(X) = X^3 - 3eX + eu$ is irreducible in $\mathbb{Q}[X]$ and its discriminant is equal to $81e^2v^2$, (Theorem 6.4.6. [4]) and (Corollary 6.4.8. [4]).
The Galois group of K has, apart from its identity element, two other elements which are inverses. We denote them by σ and $\sigma^{-1} = \sigma^2$, then the conjugates of β are given by the formulas

$$\begin{cases} \sigma(\beta) = \frac{-2e}{v} - \frac{u+v}{2v}\beta + \frac{1}{v}\beta^2, \\ \sigma^2(\beta) = \frac{2e}{v} + \frac{u-v}{2v}\beta - \frac{1}{v}\beta^2. \end{cases} \tag{3.2}$$

With our additional assumption on K (3 is ramified in K), which is equivalent to $3 \nmid v$, the family $\mathcal{B}_c = \{1, \beta, \sigma(\beta)\}$ form an integral basis of K and the discriminant of K is equal to $(9e)^2$.

Let L/K be a relative quadratic extension, we denote the ring of integers of L and K, by O_L and O_K respectively. In this note we obtain an explicit integral basis of $L/\mathbb{Q}$. More precisely, we prove that under appropriate technical hypotheses, the existence of an integral basis in the upper layer of a tower $Q \subseteq K \subseteq L$ where L cannot be algebraically split and gives an explicit description of this one.

In [3] it was considered sextic fields that are composites of subfields with coprime discriminants or not. View as sextic field over cubic subfield. According to the title in our case the fields we consider L is not composites of subfields i.e., not algebraically split.

Let $\alpha \in O_L$ be a primitive element of L/K $(L = K(\alpha))$ with $\alpha^2 \in O_K \backslash \mathbb{Z}$. We can now formulate our main result.

Theorem 3.1. *Let $K = \mathbb{Q}(\beta)$ be a cyclic cubic field in which the prime integer 3 is ramified. Let $L = K(\alpha)$ be a pure quadratic extension of K, where α is a root of a monic irreducible polynomial $P(X) = X^2 - d \in O_K[X]$. Suppose that $\upsilon_{\mathfrak{p}}(d) = 1$ for all prime $\mathfrak{p}$ in O_k such that $\mathfrak{p}/2d$. Then the sextic fields $L = \mathbb{Q}(\alpha; \beta)$ has an integral basis given by :*

$$\{1, \beta, \sigma(\beta), \alpha, \beta\alpha, \sigma(\beta)\alpha\}.$$

To show this theorem, we utilize the following lemma.

Lemma 3.2. *Let $A \subseteq B \subseteq C$ be rings. If B is finitely generated as an A-module, and C is finitely generated as a B-module, then C is finitely generated as an A-module. Moreover if $\{\alpha_1, ..., \alpha_n\}$ is a basis for B as an A-module, and $\{\beta_1, ..., \beta_m\}$ is a basis for C as a B-module, then $\{\alpha_i\beta_k \, 1 \leq i \leq n \, ; 1 \leq j \leq m$ form a basis of C as an A-module.*

Proof. To show that is finitely generated module over A, see (2.3 page 28 [10]). Let $\sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j}\alpha_i\beta_j = 0$ for some $a_{i,j}$ in $\mathbb{Z}$, we write $\sum_{j=1}^{m}(\sum_{i=1}^{n} a_{i,j}\alpha_i)\beta_j = 0$ then for each j $\sum_{i=1}^{n} a_{i,j}\alpha_i = 0$ ($\{\beta_1, ..., \beta_m\}$ is a basis for C as a B-module) so what $a_{i,j} = 0$ for all i and j for the same reason. □

Proof. of Theorem 3.1 we know that $\mathcal{B}_c = \{1, \beta, \sigma(\beta)\}$ is an integral basis of K over $\mathbb{Q}$. According to the Theorem 2.2 and Lemma 3.2 it is easily seen that $\{1, \beta, \sigma(\beta), \alpha, \beta\alpha, \sigma(\beta)\alpha\}$ is an integral basis of L. □

Corollary 3.3. *under the assumptions and suppositions of Theorem 3.1. The discriminant of the sextic field $L = \mathbb{Q}(\alpha; \beta)$ over $\mathbb{Q}$ is given by:*

$$d_{L/\mathbb{Q}} = 4^3 N_{K/\mathbb{Q}}(dR).(9e)^2.$$

where $N_{K/\mathbb{Q}}(d) = (-\frac{1}{8}cb^2 + (1/4)b^3)u^3 + (\frac{1}{2}cb^2 - \frac{3}{4}bc^2 + \frac{1}{2}abc + \frac{3}{8}cvb^2 - \frac{3}{4}ab^2 + \frac{1}{4}c^3)u^2 + ((\frac{3}{4}b^3 - \frac{3}{8}cb^2)v^2 - \frac{1}{2}abc - \frac{1}{2}a^2c)u + \frac{9}{8}cv^3b^2 + (\frac{3}{2}abc + \frac{3}{2}cb^2 - \frac{9}{4}bc^2 - \frac{9}{4}ab^2 + \frac{3}{4}c^3)v^2 + (\frac{1}{2}a^2c + \frac{1}{2}abc - ac^2)v + a^3 - a^2c$

Proof. To compute discriminant we use (Proposition 13 page 66 [13]), then we have

$$\begin{aligned} d_{L/\mathbb{Q}} = N_{K/\mathbb{Q}}(d_{L/K}).(d_{K/\mathbb{Q}})^{[L:K]} &= N_{K/\mathbb{Q}}(4dR).(9e)^2 \\ &= 4^3 N_{K/\mathbb{Q}}(dR).(9e)^2 \end{aligned}$$

In the rest of this proof, we will give explicitly the norm of d, $N_{K/\mathbb{Q}}(dR)$. Let $d = a + b\beta + c\sigma(\beta)$, $(a, b, c) \in \mathbb{Z}^2$. 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 $m_d(1)$, $m_d(\beta)$ and $m_d(\sigma(\beta))$. Then by using a computer algebra package (such as Maple) it can be checked that:

$$\begin{cases} m_d(1) = a + b\beta + c\sigma(\beta) \\ m_d(\beta) = \frac{1}{4v}[(-2cuv + 4bv^2 - 2cv^2)\sigma(\beta) + (4va + 2vbu + 2bv^2 + 4ce - cu^2 - \\ 2cuv - cv^2)\beta + (8bev - 4cve)] \\ m_d(\sigma(\beta)) = (a - c + \frac{1}{4v}b(-2uv - 2v^2))\sigma(\beta) + (-c + \frac{1}{4v}b(-u^2 - 2uv + 4e - v^2))\beta \\ -be \end{cases}$$

Write now $e = \frac{u^2+3v^2}{4}$, we check that; $det(m_d) = (-\frac{1}{8}cb^2 + (1/4)b^3)u^3 + (\frac{1}{2}cb^2 - \frac{3}{4}bc^2 + \frac{1}{2}abc + \frac{3}{8}cvb^2 - \frac{3}{4}ab^2 + \frac{1}{4}c^3)u^2 + ((\frac{3}{4}b^3 - \frac{3}{8}cb^2)v^2 - \frac{1}{2}abc - \frac{1}{2}a^2c)u + \frac{9}{8}cv^3b^2 + (\frac{3}{2}abc + \frac{3}{2}cb^2 - \frac{9}{4}bc^2 - \frac{9}{4}ab^2 + \frac{3}{4}c^3)v^2 + (\frac{1}{2}a^2c + \frac{1}{2}abc - ac^2)v + a^3 - a^2c$

□

Remark 3.4.

(1) The calculation of the discriminant of a composite of couple of fields is known when the discriminants of fields are coprime. In the above corollary, we compute the discriminants of field L, without the need for the coprimeness of discriminants of $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$,

(2) By considering $d \in \mathbb{Z}$ we see that the expression of discriminant simplifies to $d_{L/\mathbb{Q}} = 4^3.d^3.(9e)^2$ which was proved in other article.

4. Conclusion

In this work, we have extended the results of existence of an integral basis of sextic extension L, which split arithmetically. we have explicitly construct an integral basis where L is not split algebraically.

5. ACKNOWLEDGMENT

The author is very very grateful to Professor A. Chillali and would like to thank Sidi Mohamed Ben Abdellah Univercity (USMBA), LSI and FP of Taza in MOROCCO for their valued supports.

References

1. G. Archinard, *Extensions cubiques cycliques de $\mathbb{Q}$ dont l'anneau des entiers est monogène*, Enseignement Math. 20, (1974), 179203.
2. M. E. Charkani and A. Deajim, *Generating a Power Basis over a Dedekind Ring*, J. Number Theory 132, No. 10, (2012), 2267-2276.
3. M. E. Charkani and M. Sahmoudi, *Sextic Extension with cubic subfield*, JP Journal of Algebra, Number Theory et Applications, vol.34,no.2, (2014), 139-150.
4. H. Cohen, *A Course in Computational Algebraic Number theory*, GTM vol. 138, Springer Verlag, Berlin, (1996).
5. A. Fröhlich and M. J. Taylor, *Algebraic number theory*, CambridgeStudies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, (1993).
6. I. Gaàl, P. Olajos, M. Pohst, *Power Integral Bases in Orders of Composite Fields* , Experimental Mathematics, Vol. 11, no. 1, (2002).
7. I. Gaàl, *Diophantine equations and power integral bases*, Boston, Birkhäuser, (2002).
8. M. N. Gras, *Sur les corps cubiques cycliques dont lanneau des entiers est monogne*, Ann. Sci. Univ. Besançon 3, No. 6, (1973).
9. M. N. Gras, *Lien entre le groupe des unités et la monogéneité des corps cubiques cycliques*, Ann. Sci. Univ. Besançon No. 1, (1975-76).
10. A. Fröhlich and M. Taylor, *Algebraic Number Theory*, Combridge Studies in Advenced Mathematics 27, (1993).
11. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer, Berlin, (1974).
12. B. K. Spearman and K. S. Williams, *Relative integral bases for quartic fields over quadratic subfields*, Acta Math. Hungar., 70, (1996), 185-192.
13. S. Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics 110, Springer-Verlag New York, (1986).

[1] LAGA Laboratory, Faculty of Sciences Dhar elmahraz. P. 0. Box 1796, Atlas-Fez, Morocco.
E-mail address: mohamed-sahmoudi@usmba.ac.ma

A. Chillali, Sidi Mohamed Ben Abdellah University, FP, LSI, Taza, Morocco.
E-mail address: abdelhakim.chillali@usmba.ac.ma