Int. J. Contemp. Math. Sci., Vol. 2, 2007, no. 13, 601 - 606

Computation of a Power Integral Basis of a Pure Cubic Number Field

L houssain EL FADIL

Faculté Polydisciplinaire de Ouarzazat
Ouarzazat-Morocco

Abstract

In this paper, a method to compute an integral basis of $\mathcal{O}$: the integral closure of $K = \mathbb{Q}[\alpha]$, where α a complex root of the irreducible polynomial $T(X) = X^3 - d \in \mathbb{Z}[X]$, is given. A criterion to test if $\mathcal{O}$ is monogenic is given. When $\mathcal{O}$ is monogenic, an algorithm to compute all power integral bases of $\mathcal{O}$ is given.

Introduction

In this paper, let $\mathbb{Q}[\alpha]$ be a pure cubic number field , i.e., α is a root of a polynomial $T = X^3 - d$ and d is a cubic free integer. Let $\mathcal{O}$ be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\alpha]$. We say that $\mathcal{O}$ has a power integral basis if there exists $\theta \in \mathcal{O}$ such that $(1, \theta, \theta^2)$ is a $\mathbb{Z}$- basis of $\mathcal{O}$. In that case, we say that $\mathcal{O}$ is monogenic. An algorithm to compute an integral basis of $\mathcal{O}$ and a criterion to test if $\mathcal{O}$ is monogenic are given. When $\mathcal{O}$ is monogenic, an algorithm to compute all power integral bases of $\mathcal{O}$ is given. We finalize by some examples illustrating this criterion.
The following notations are used: For every prime integer p, denote $\mathbb{F}_p$ the residual field $\mathbb{Z}/p\mathbb{Z}$. For two polynomials P and Q lie in $\mathbb{F}_p[X]$, denote by $D(P, Q))$ their greatest common divisor in $\mathbb{F}_p[X]$.

For two free $\mathbb{Z}$-submodules M and N of $\mathbb{Q}[\alpha]$, with the same rank over $\mathbb{Z}$, there is a nonsingular $\mathbb{Q}$-linear map f with $f(M) = N$. The principal ideal of $\mathbb{Z}$, generated by the determinant of f, depends only of M and N, which will denote by $[M : N]$, i.e., $[M : N] = det(f)\mathbb{Z}$. If $N \subset M$, then $[M : N]$ is called the index of N in M : $[M : N]$ is generated by the cardinal order of the group M/N. Let Λ be a $\mathbb{Z}$-order of $\mathbb{Q}[\alpha]$, i.e., Λ is a unitary sub-ring of $\mathbb{Q}[\alpha]$, finitely generated as $\mathbb{Z}$-module and contains a $\mathbb{Q}$-basis of $\mathbb{Q}[\alpha]$. Since Λ is a finitely generated $\mathbb{Z}$-module, $\Lambda \subset \mathcal{O}$. Let p be a prime integer; we say that Λ is a p-maximal order of $\mathbb{Q}[\alpha]$ if p does not divide $[\mathcal{O} : \Lambda]$. Λ is a maximal order of $\mathbb{Q}[\alpha]$ if Λ is a p-maximal order of $\mathbb{Q}[\alpha]$ for every prime p, i.e., for every

prime p, p does not divide $[\mathcal{O} : \Lambda]$. Thus $\mathcal{O}$ is the only maximal order of $\mathbb{Q}[\alpha]$. Let $(u_1, u_2, u_3) \in \mathbb{Q}[\alpha]^3$; denote $D(u_1, u_2, u_3)$ the discriminant of (u_1, u_2, u_3), i.e., the determinant of the matrix $(T(u_i u_j))_{i,j}$, where T is the trace map of $\mathbb{Q}[\alpha]$. Let (e_1, e_2, e_3) be a $\mathbb{Z}$-basis of $\mathcal{O}$; it's well known that $D(u_1, u_2, u_3) = \lambda^2 D(e_1, e_2, e_3)$, where λ is the determinant of the matrix (x_{ij}), defined by $u_i = \sum_{j=1}^{3} x_{ij} e_j$ for every i. It follows that if (u_1, u_2, u_3) is a $\mathbb{Z}$-basis of Λ, then $D(u_1, u_2, u_3) = [\mathcal{O} : \Lambda]^2 D(e_1, e_2, e_3)$.
The Dedekind criterion allows us to enlarge the $\mathbb{Z}$-order $\mathbb{Z}[\alpha]$, successively, for every prime integer q such that q^2 divides the discriminant δ of $T(X)$, until we obtain the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\alpha]$ as follows: Let $q \in N$ be a prime such that q^2 divides δ. In $\mathbb{F}_q[X]$, let $\bar{T}(X) = \prod_{i=1}^{r} \bar{t}_i(X)^{e_i}$ be the factorization of $\bar{T}(X)$ of irreducible polynomials in $\mathbb{F}_q[X]$, where $t_1(X), ..., t_r(X)$ are monic polynomials lying in $\mathbb{Z}[X]$, $g(X) = \prod_{i=1}^{r} t_i(X)$, $h(X)$ a monic polynomial of $\mathbb{Z}[X]$ such that $\bar{h}(X) = \frac{\bar{T}(X)}{\bar{g}(X)}$ and $f(X) = \frac{gh(X) - T(X)}{q} \in \mathbb{Z}[X]$. If $D(\bar{f}, \bar{g}, \bar{h}) = 1$, then $\mathbb{Z}[\alpha]$ is a q-maximal order of $\mathbb{Z}$ in $\mathbb{Q}[\alpha]$ else, let U be a monic polynomial of $\mathbb{Z}[X]$ lifts of $\bar{U}(X) = \frac{\bar{T}}{D(\bar{f}, \bar{g}, \bar{h})}$ in $\mathbb{F}_q[X]$. Then $\Lambda' = \mathbb{Z}[\alpha] + \frac{1}{q} U(\alpha)\mathbb{Z}[\alpha]$ is a larger $\mathbb{Z}$-order in $\mathbb{Q}[\alpha]$ then $\mathbb{Z}[\alpha]$ (see [1, Th 6.1.4, p 306]).

1 Main results

Let d be a cubic free integer, i.e., $d = ab^2$, where $D(a, b) = 1$, a and b are square free. Let α be a complex root of the irreducible polynomial $T(X) = X^3 - d$ and $\mathcal{O}$ the integral closure of $K = \mathbb{Q}[\alpha]$. In this section, an algorithm to compute an integral basis of $\mathcal{O}$ a criterion to test if $\mathcal{O}$ is monogenic, and then to compute all power integral basis of $\mathcal{O}$ are given.

Theorem 1. 1 *Under these hypotheses, we have that:*
1) If $d^2 = 1$ modulo 9, then $\mathcal{B} = (1, \alpha, \frac{1}{3b}(\alpha - d)^2)$ is an integral basis of $\mathcal{O}$.
2) If $d^2 \neq 1$ modulo 9, then $\mathcal{B} = (1, \alpha, \frac{1}{b}\alpha^2)$ is an integral basis of $\mathcal{O}$.

Proof. Let $\delta = \mp 27 a^2 b^4$ be the discriminant of $T(X)$. Use the Dedekind criterion, it suffices to enlarge successively $\mathbb{Z}[\alpha]$ for every prime p which divides d or $p = 3$.

1. Let p divides a. In $F_p[X]$, we have $g(X) = X$ and $h(X) = X^2$, and then $f(X) = \frac{d}{p}$. Since p^2 does not divide d, $f(0) \neq 0$ modulo p. Therefore, $D(\bar{g}, \bar{h}, \bar{f}) = 1$. Hence $\mathbb{Z}[\alpha]$ is a p-maximal $\mathbb{Z}$ order of $\mathbb{Q}[\alpha]$.

2. Let p divides b. In $\mathbb{F}_p[X]$, we have $g(X) = X$, $h(X) = X^2$ and $f(X) = \frac{d}{p}$. Since p^2 divides d, $f(0) = 0$ modulo p, and then $D(\bar{f}, \bar{g}, \bar{h}) = X$ in

$\mathbb{F}_p[X]$. Therefore, $\bar{U}(X) = \frac{\bar{T}}{D(f,\bar{g},h)} = X^2$ in $\mathbb{F}_p[X]$. Hence $\frac{1}{p}\alpha^2 \in \mathcal{O}$. On the other hand, $X^3 - \frac{d}{p^3}$ is the minimal polynomial of $\frac{\alpha}{p}$ and $X^3 - \frac{d^2}{p^6}$ is the minimal polynomial of $\frac{1}{p^2}\alpha^2$. So, $\frac{1}{p}\alpha$ and $\frac{1}{p^2}\alpha^2$ are not integral over $\mathbb{Z}$. Let $A(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 \in \mathcal{O}$, such that $a_i \in \mathbb{Q}$ and $pA(\alpha) \in \mathbb{Z}[\alpha]$. Then for every i, $pa_i \in \mathbb{Z}$. For every i, let $b_i \in \mathbb{Z}$ such that $a_i = \frac{b_i}{p}$. Then $B(\alpha) = a_0 + a_1\alpha = A(\alpha) - b_2\frac{1}{p}\alpha^2 \in \mathcal{O}$. If $a_1 \neq 0$, consider $X^3 - \frac{3b_0}{p}X^2 + \frac{3b_0^2}{p^2}X - \frac{b_1^3 d + b_0^3}{p^3}$ the minimal polynomial of $B(\alpha)$. Since $B(\alpha) \in \mathcal{O}$, p divides b_0, and then divides b_1. Therefore, $A(\alpha) = a_0 + a_1\alpha + b_2\frac{\alpha^2}{p}$, where $(a_0, a_1, b_2) \in \mathbb{Z}^3$. Consequently, $\mathbb{Z}[\alpha] + \frac{\alpha^2}{p}\mathbb{Z}[\alpha]$ is a p-maximal order of $\mathbb{Q}[\alpha]$

3. $p = 3$ and 3 does not divide d. In $\mathbb{F}_3[X]$, $g(X) = (X - d)$, $h(X) = (X - d)^2$ and $f(X) = \frac{-3dX^2 + 3d^2X - d^3 + d}{3}$. Thus $f(d) = \frac{-d(d^2-1)}{3}$. Hence $f(d) = 0$ modulo 3 if and only if 3^2 divides $d^2 - 1$. Therefore, if $d^2 \neq 1$ modulo 9, then $D(\bar{f}, \bar{g}, \bar{h}) = 1$, and then $\mathbb{Z}[\alpha]$ is a 3-maximal order of $\mathbb{Z}$ in $\mathbb{Q}[\alpha]$. Else, as in the previous case, computing the minimal polynomials of $\frac{1}{3}(\alpha - d)$, $\frac{1}{3}(\alpha - d)^2$ and $\frac{1}{3^2}(\alpha - d)^2$, we show that $\frac{1}{3}(\alpha - d)^2 \in \mathcal{O}$, $\frac{1}{3^2}(\alpha - d)^2$ and $\frac{1}{3}(\alpha - d)$ are not integral over $\mathbb{Z}$. Let $A(\alpha) = a_0 + a_1\alpha + a_2\frac{1}{3}\alpha^2 \in \mathcal{O}$, such that $a_i \in \mathbb{Q}$ and $3A(\alpha) \in \mathbb{Z}[\alpha]$. Then $(3a_0, 3a_1, a_2) \in \mathbb{Z}^3$. Thus $B(\alpha) = a_0 + a_1\alpha \in \mathcal{O}$. If $a_1 = 0$, as $\mathbb{Z}$ is integrally closed, then $a_0 \in \mathbb{Z}$. Else, let $N(X) = X^3 - X^2 b_0 + \frac{b_0^2}{3}X - \frac{b_0^3 + b_1^3 d}{27}b_0^3 + b_1^3 d$ be the minimal polynomial of $B(\alpha)$. Then 3 divides b_0 and b_1. Therefore, $\mathbb{Z}[\alpha] + \frac{(\alpha-d)^2}{3}\mathbb{Z}[\alpha]$ is a 3-maximal $\mathbb{Z}$-order of $\mathbb{Q}[\alpha]$.

Consequently,

1. If 9 does not divide $d^2 - 1$, then $[\mathcal{O} : \mathbb{Z}[\alpha]] = b\mathbb{Z}$. In that case, as $(\frac{1}{b}\alpha^2)^3 = \frac{d^2}{b^3} = a^2 b$, $\frac{1}{b}\alpha^2$ is integral over $\mathbb{Z}$, and then $\mathcal{B} = (1, \alpha, \frac{1}{b}\alpha^2)$ is an integral basis of $\mathcal{O}$.

2. If 9 divides $d^2 - 1$, then $[\mathcal{O} : \mathbb{Z}[\alpha]] = 3b\mathbb{Z}$. Let $X^3 - a^2b^3X^2 + \frac{b^2a^2(2+a^2b^4)}{3}X + \frac{-a^2b(d^2-1)^2}{27}$ be the minimal polynomial of $\frac{1}{3b}(\alpha - d)^2$. Since 9 divides $d^2 - 1$, 3 divides $(2 + a^2b^4)$ and 27 divides $(d^2 - 1)^2$, and then $\frac{1}{3b}(\alpha - d)^2$ is integral over $\mathbb{Z}$. Thus, $\mathcal{B} = (1, \alpha, \frac{1}{3b}(\alpha - d)^2)$ is an integral basis of $\mathcal{O}$. ∎

Corollary 1. 2 *Let $d = ab^2$ be a cubic free integer, a and b are defined above and α a root of $T(X) = X^3 - d$.*

1. *If $d^2 \neq 1$ modulo 9, then $[\mathcal{O} : \mathbb{Z}[\alpha]] = b^2\mathbb{Z}$ and $d_K = -27(ab)^2$ is the discriminant of $K = \mathbb{Q}[\alpha]$.*

2. *If $d^2 = 1$ modulo 9, then $[\mathcal{O} : \mathbb{Z}[\alpha]] = 9b^2\mathbb{Z}$ and $d_K = -3(ab)^2$.*

Now we are ready to give a criterion to test if $\mathcal{O}$ is monogenic.

From Theorem 1.3, let $(s, r) \in \mathbb{Z}^2$ such that $\mathcal{B} = (1, \alpha, \frac{1}{s}(\alpha - r)^2)$ is an integral basis of $\mathcal{O}$. For every $(x, y, z) \in \mathbb{Z}^3$, let $\theta = x + y\alpha + z\frac{1}{s}(\alpha - r)^2$. Then $\theta^2 = f_0(x, y, z) + f_1((x, y, z)\alpha + f_2(x, y, z)\frac{1}{s}(\alpha - r)^2$, where every $f_i(x, y, z)$ is a polynomial of $\mathbb{Z}[x, y, z]$. Define $\lambda(x, y, z)$ the determinant $\lambda(x, y, z) = \begin{vmatrix} y & f_1((x, y, z)) \\ z & f_2((x, y, z)) \end{vmatrix}$.

Lemma 1. 3 *Under the above hypothesis, $\mathcal{O}$ is monogenic if and only if there exists $(x, y, z) \in \mathbb{Z}^3$ such that $\lambda(x, y, z) = \mp 1$.*

Proof. We have $[\mathcal{O} : \mathbb{Z}[\theta]] = \lambda^2\mathbb{Z}$, where $\lambda = \lambda(x, y, z)$. Thus $\mathcal{O} = \mathbb{Z}[\theta]$ if and only if $\lambda^2 = \mp 1$. ∎

Theorem 1. 4 *Let $d = ab^2$ be a cubic free integer, a and b are defined above and α a root of $T(X) = X^3 - d$.*

1. *If $d^2 \neq 1$ modulo 9, then $\mathcal{O}$ is monogenic if and if there exists $(y, z) \in \mathbb{Z}^2$ such that $by^3 - az^3 = \mp 1$.*

2. *If $d^2 = 1$ modulo 9, then $\mathcal{O}$ is monogenic if and only if there exists $(y, z) \in \mathbb{Z}^2$ such that $4yz^2a^2b^3 + 3by^3 - 6y^2zab^2 - \frac{1}{9}z^3a(8a^2b^4 + 1) = \mp 1$.*

Proof. It suffices to compute $\lambda(x, y, z)$ in the following cases:

1. $d^2 \neq 1$ modulo 9. Let $\theta = x + y\alpha + z\frac{1}{b}\alpha^2$. Then $\theta^2 = (2xz/b + y^2)\alpha^2 + (z^2a + 2xy)\alpha + x^2 + 2yzab$. Hence $\lambda(x, y, z) = \begin{vmatrix} y & ((z^2a + 2xy) \\ z & b(2xz/b + y^2) \end{vmatrix} = by^3 - az^3$.

2. $d^2 = 1$ modulo 9. Let $\theta = x + y\alpha + z\frac{1}{3b}(\alpha - d)^2$. Then $f_2(x, y, z) = (\frac{2}{3}(\frac{x+1}{3}za^2b^3)\frac{z}{b} + (y - \frac{2}{3}zab)^2)3b$ and $f_1(x, y, z) = 2(x + \frac{1}{3}za^2b^3)(y - \frac{2}{3}zab) + \frac{1}{9}z^2a + 2d(\frac{2}{3}(x + \frac{1}{3}za^2b^3)\frac{z}{b} + (y - \frac{2}{3}zab)^2)$. Therefore, $\lambda(x, y, z) = \begin{vmatrix} y & f_1(x, y, z) \\ z & f_2(x, y, z) \end{vmatrix} = 4yz^2a^2b^3 + 3by^3 - 6y^2zab^2 - \frac{1}{9}z^3a(8a^2b^4 + 1)$. ∎

Remark that:
(1) Since $\lambda(x, y, z)$ is independent to x, we can assume that $x = 0$.
(2) In the second case, since $d^2 = a^2b^4 = 1$ modulo 9, 9 divides $(8a^2b^4 + 1)$. Thus, $\lambda(x, y, z) \in \mathbb{Z}$.

Corollary 1. 5 *Let d be a cubic free integer such that $d^2 \neq 1$ modulo 9. If $d = \bar{+}n(n+1)^2$ or $d = \mp(n+1)n^2$ or d is square free or $d = \mp b^2$, then $\mathcal{O}$ is monogenic.*

Proof. To compute θ such that $\mathcal{O} = \mathbb{Z}[\theta]$, it suffices to choose suitably $(y, z) \in \mathbb{Z}^2$ such that $\lambda(0, y, z) = \mp 1$.

1. If $d = n(n+1)^2$ or $d = (n+1)n^2$, then $\lambda(0, 1, 1) = \mp 1$.
2. If $d = -n(n+1)^2$ (resp. $d = -(n+1)n^2$), then $\lambda(0, -1, 1) = \mp 1$ (resp. $\lambda(0, 1, -1) = \mp 1$).
3. If d is square free, i.e., $b = \mp 1$. It follows that $\lambda(0, 1, 0) = \mp 1$.
4. If $d = \mp b^2$, then $\lambda(0, 0, \mp 1) = \mp 1$.

Some against examples.

1. Let $d = ab^2$ such that $d^2 \neq 1$ modulo 9.
   (a) If $b^2 \neq 1$ *modulo* 7 *and* $a = 0$ *modulo* 7, then $\mathcal{O}$ is not monogenic. Indeed, let $d = 7ab^2$. If $\mathcal{O}$ is monogenic, then there exists $(y, z) \in \mathbb{Z}^2$ such that $by^3 - 7az^3 = \mp 1$. Thus, in $\mathbb{F}_7$ there exists y such that $by^3 = \mp 1$. Since $\mathbb{F}_7^3 = \{0, 1, -1\}$, if $b^2 \neq 1$ modulo 7, then the equation $by^3 = \mp 1$ has no solution in $\mathbb{F}_7$. Therefore, $\mathcal{O}$ is not monogenic.
   (b) The same of the case where $a^2 \neq 1$ *modulo* 7 *and* $b = 0$ *modulo* 7.
2. Let $d = ab^2$ such that $d^2 = 1$ modulo 9.
   (a) If $b \neq 2$ *and* $b \neq -2$ and 7 divides a, then $\mathcal{O}$ is not monogenic. Indeed, if $\mathcal{O}$ is monogenic, then there exists $(y, z) \in \mathbb{Z}^2$ such that $4yz^2 7^2 a'^2 b^3 + 3by^3 - 42y^2 zab^2 - \frac{7}{9}z^3 a(8a^2b^4 + 1) = \bar{+}1$. So, in F_7 there exists y such that $by^3 = \bar{+}2$.
   (b) If $d = 5a$ and $d^2 = 1$ modulo 9, then $\mathcal{O}$ is not monogenic.
   Indeed, we have $\lambda(0, y, z) = 100yz^2a^2 + 3y^3 - 30y^2za - 5/9(200a^2 + 1)z^3a$. In F_5, $\lambda(0, y, z) = 3y^3$.
   In F_5, $3y^3 = +1$ (resp. $3y^3 = -1$) implies that $y = 2$ (resp. $y = 3$) modulo 5. Replace in $\lambda(0, y, z)$, we will solve in $\mathbb{Z}^2$, $\lambda(0, 5k+2, z) = 375k^3 + (450 - 750za)k^2 + (180 + 500z^2a^2 - 600za)k + 200z^2a^2 - 5/9(200a^2 + 1)z^3a + 24 - 120za = 1$ (resp. $\lambda(0, 5k+3, z) = 375k^3 + (675 - 750za)k^2 + (405 + 500z^2a^2 - 900za)k + 300z^2a^2 - 5/9(200a^2 + 1)z^3a + 81 - 270za = -1$, i.e., we will solve $375k^3 + (450 - 750za)k^2 + (180 + 500z^2a^2 - 600za)k + 200z^2a^2 - 5/9(200a^2 + 1)z^3a + -120za = -23$ (resp. $375k^3 + (675 - 750za)k^2 + (405 + 500z^2a^2 - 900za)k +$

$300z^2a^2 - 5/9(200a^2 + 1)z^3a + -270za = -82$. The first equation implies that 5 divides 3, the second implies that 5 divides 82, which are impossible. Finally, $\mathcal{O}$ is not monogenic.

References

[1] H. Cohen, A course in computational algebraic number theory, GTM 138, Springer-Verlag Berlin Heidelberg, New York, Paris, Tokyo, third, corrected printing 1996.

[2] L. El fadil, Computational of the integral closure. (to appear in International Journal of Commutative Rings)

[3] L. El Fadil and M. Charkani. Generalization of the discriminant and applications, The Arabian Journal for Science and Engineering, (1A)29, 2004, 93-98.

[4] A. Fröhlich and M. Taylor, Algebraic number theory, Combridge Studies in Advenced Mathematics 27,CUP, 1992.

[5] L.C. Washington. Introduction to cyclotomic fields, Springer-Verlag, Berlin, Heidelberg, New York, 1982.

Received: June 11, 2006