



Théorie des nombres

Arithmétique d'une famille de corps cubiques

Arithmetic of a family of cubic fields

Ouafae Lahlou, Mohamed El Hassani Charkani

Département de mathématiques, faculté des sciences Dhar-Mahraz, BP 1796, Fes, Maroc

Reçu le 30 juillet 2002 ; accepté après révision le 30 janvier 2003

Présenté par Michel Raynaud

Résumé

Dans cette Note, on étudie la famille de polynômes : $P(X) = X^3 - nX^2 - n$, avec $n = 3^s p_1 \dots p_t$ où $s = 0$ ou 1 et où les p_i pour $1 \leq i \leq t$ sont des nombres premiers deux à deux distincts et distincts de 3 et où $(4n^2 + 27)/9^s$ est sans facteurs carrés. Pour cette famille, on détermine les invariants arithmétiques du corps de nombres $K = \mathbb{Q}(\alpha)$, avec α l'unique racine réelle du polynôme $P(X)$, et on trouve les résultats suivants : $O_K = \mathbb{Z}[\alpha]$ est l'anneau des entiers de K , $d_K = -n^2(4n^2 + 27)$ est le discriminant de K ; $\varepsilon = \alpha^2 + 1$ est l'unité fondamentale de O_K et $R_K = \text{Log}(\alpha^2 + 1)$ est le régulateur de K . **Pour citer cet article : O. Lahlou, M. El Hassani Charkani, C. R. Acad. Sci. Paris, Ser. I 336 (2003).**

© 2003 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS. Tous droits réservés.

Abstract

In this Note, we study the family of polynomials: $P(X) = X^3 - nX^2 - n$, with $n = 3^s p_1 \dots p_t$, where $s = 0$ or 1 and where the p_i , for $1 \leq i \leq t$, are distinct prime numbers and all different from 3 , and $(4n^2 + 27)/9^s$ is squarefree. For this family, we determine the arithmetic invariants of the number field $K = \mathbb{Q}(\alpha)$, where α is the only real root of the polynomial $P(X)$, and we find the following results: $O_K = \mathbb{Z}[\alpha]$ is the ring of integers of K , $d_K = -n^2(4n^2 + 27)$ is the discriminant of K ; $\varepsilon = \alpha^2 + 1$ is the fundamental unit of O_K and $R_K = \text{Log}(\alpha^2 + 1)$ is the regulator of K . **To cite this article: O. Lahlou, M. El Hassani Charkani, C. R. Acad. Sci. Paris, Ser. I 336 (2003).**

© 2003 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS. All rights reserved.

Abridged English version

Let $K \subset \mathbb{R}$ be a complex cubic field. Let L be a free \mathbb{Z} -module of rank 3 of K of basis $\{1, \lambda_1, \lambda_2\}$. We will say that L is a lattice of K and we will denote by $L = \langle 1, \lambda_1, \lambda_2 \rangle$. We denote σ and $\bar{\sigma}$ the not-real embeddings of K .

We first need a few basic results and definitions.

Definitions 0.1. (1) We will say that $\psi_0 \in L$ is a minimal point of L if and only if for every ψ of L such that $0 < \psi < \psi_0$ we have $|\sigma(\psi)| > |\sigma(\psi_0)|$.

Adresses e-mail : l.ouafae@caramail.com (O. Lahlou), mcharkani@excite.com (M. El Hassani Charkani).

(2) Let k be an integer positive. We will say that ψ_{k+1} is the minimal point adjacent to ψ_k of second kind in L if and only if $\psi_{k+1} = \min\{\psi \mid \psi > \psi_k \text{ and } |\sigma(\psi)| < |\sigma(\psi_k)|\}$.

(3) A lattice L is *reduit* if and only if 1 is a minimal point of L .

If L is a lattice *reduit*, we construct an increasing sequence of minimal points adjacent of second kind of the following way: $\psi_0 = 1$ and ψ_{k+1} is the minimal point adjacent to ψ_k of second kind for $k \geq 0$.

By Voronoi [20] we know that this sequence is purely periodic of the form: $\psi_0 = 1, \psi_1, \dots, \psi_{l-1}, \psi_l = \varepsilon, \varepsilon\psi_1, \dots, \varepsilon\psi_{l-1}, \dots$, where ε is the fundamental unit of L upper to 1 and l is the period length.

For construct this sequence, it suffices to know construct the minimal point adjacent to 1 of second kind in a lattice *reduit* L of K (see [21]).

Let $n \geq 2$ be an integer, we consider the polynomial: $P(X) = X^3 - nX^2 - n$.

First, from Proposition 2.1 it is easy to obtain the following theorem:

Theorem 0.1. *Let α be a real root of the polynomial $P(X)$ and $K = \mathbb{Q}(\alpha)$.*

(1) *The sequence of minimal points of $\mathbb{Z}[\alpha]$ is: $\psi_0 = 1, \psi_1 = \alpha, \psi_2 = \alpha^2$ and $\psi_3 = \alpha^3/n$.*

(2) *The fundamental unit of $\mathbb{Z}[\alpha]$ is ψ_3 and the length of Voronoi algorithm is $l = 3$.*

Next, we use Lemmas 3.1–3.3 and 3.4 it is easy to obtain the following theorem:

Theorem 0.2. *Let α be a real root of the polynomial $P(X)$, $K = \mathbb{Q}(\alpha)$ and O_K the ring of integers of K . Let $n = 3^s n'$ where $s \in \mathbb{N}$, $n' \in \mathbb{N}$ and n' and 3 are coprime. If n is squarefree then we have: $O_K = \mathbb{Z}[\alpha]$ if and only if $(4n^2 + 27)/9^s$ is squarefree.*

At the end, we use the last theorems and so we obtain the following corollary:

Corollary 0.1. *With the same notations of Theorem 0.2. If n and $(4n^2 + 27)/9^s$ are squarefree then we have: $O_K = \mathbb{Z}[\alpha]$, $d_K = -n^2(4n^2 + 27)$ and $R_K = \text{Log}(\alpha^2 + 1)$.*

1. Introduction

Il est en général difficile, de déterminer effectivement les principaux invariants arithmétiques d'un corps de nombres K , tels que le discriminant d_K de K , l'anneau des entiers O_K de K , le nombre des classes h_K de K et le régulateur R_K de K .

Dans toute la suite on adopte les notations ci-dessus.

On sait que le produit d'Euler est lié à $h_K R_K$ par la formule analytique du nombre de classes (voir [4], p. 356, et [15], p. 125).

Deux problèmes essentiels se posent alors :

- (1) La détermination d'une base de O_K qui nous permet de calculer d_K .
- (2) La détermination d'un système fondamental d'unités de K qui nous permet de calculer R_K .

Il y a des réponses partielles à ces problèmes que nous citerons ici : l'étude de la monogénéité d'un corps de nombres K , c'est-à-dire la recherche d'un entier algébrique θ de O_K tel que $O_K = \mathbb{Z}[\theta]$, est un problème bien connu et qui a été traité par G. Archinard [2], R. Dedekind [5], D.S. Dummit et H. Kisilevsky [6], Fléckinger [8], M.N. Gras ([9,10] et [11]), K. Györy ([12,13] et [14]), T. Nakahara [18], F. Tanoé [19], etc.

Le développement par l'algorithme de Voronoi [20] est purement périodique et fournit un système fondamental d'unités de tout corps de nombres de degré 3.

2. Notations et rappels

2.1. Algorithme de Voronoi

Soit $K \subset \mathbb{R}$ un corps de nombres cubique à conjugués complexes. Soit L un \mathbb{Z} -module libre de rang 3 de K de base $\{1, \lambda_1, \lambda_2\}$. On dira que L est un réseau de K et on notera $L = \langle 1, \lambda_1, \lambda_2 \rangle$. On note σ et $\bar{\sigma}$ les plongements complexes de K dans \mathbb{C} .

Définition 2.1. (1) On dit que $\psi_0 \in L$ est un point extrémal de L si et seulement si pour tout ψ de L tel que $0 < \psi < \psi_0$ on a $|\sigma(\psi)| > |\sigma(\psi_0)|$.

(2) Soit k un entier positif, on dit que ψ_{k+1} est le point extrémal adjacent à ψ_k de deuxième espèce dans L si et seulement si $\psi_{k+1} = \min\{\psi \mid \psi > \psi_k \text{ et } |\sigma(\psi)| < |\sigma(\psi_k)|\}$.

(3) Un réseau L est réduit si et seulement si 1 est un point extrémal de L .

Si L est un réseau réduit, on construit la suite croissante des points extrémaux adjacents de deuxième espèce de la façon suivante : $\psi_0 = 1$ et ψ_{k+1} est le point extrémal adjacent à ψ_k de deuxième espèce pour $k \geq 0$.

Par Voronoi [20] on sait que cette suite est purement périodique de la forme : $\psi_0 = 1, \psi_1, \dots, \psi_{l-1}, \psi_l = \varepsilon, \varepsilon\psi_1, \dots, \varepsilon\psi_{l-1}, \dots$, où ε est l'unité fondamentale de L supérieure à 1 et l est la longueur de la période.

Pour construire une telle suite, il suffit de savoir construire le point extrémal adjacent à 1 de deuxième espèce dans un réseau réduit L de K . Soit $L_0 = \langle 1, \lambda_1, \lambda_2 \rangle$ un réseau réduit de K (cf. [21]). Soient $\psi_0 = 1$ et ψ_1 le point extrémal adjacent à 1 dans L_0 .

- (a) On choisit un point auxiliaire $\bar{\phi}_1$ tel que $\{\psi_1, \bar{\phi}_1, \psi_0\}$ soit une base de L_0 .
- (b) ψ_2 est le point extrémal adjacent à ψ_1 dans $L_0 = \langle \psi_1, \bar{\phi}_1, \psi_0 \rangle$ équivaut à ψ_2/ψ_1 est le point extrémal adjacent à 1 dans $L_1 = \langle 1, \bar{\phi}_1/\psi_1, \psi_0/\psi_1 \rangle$.

On poursuit ce processus par récurrence.

2.2. Méthode de recherche de points extrémaux

On décrit ici une méthode due à B. Adam [1] qui permet dans certains cas de déterminer une suite croissante de points extrémaux. On sait que pour déterminer une telle suite il suffit de savoir construire le point extrémal adjacent à 1 de deuxième espèce dans un réseau réduit $L = \langle 1, \lambda_1, \lambda_2 \rangle$.

Ainsi on cherche un élément $\psi = x + y\lambda_1 + z\lambda_2$ de L tel que $\psi > 1, |\sigma(\psi)| < 1$ et ψ minimum.

Pour tout $(u, v, w) \in \mathbb{R}^3$ on pose $F(u, v, w) = |u + v\sigma(\lambda_1) + w\sigma(\lambda_2)|^2$.

F définit une forme quadratique à trois variables u, v, w à coefficients réels, positive de rang 2. Dans [1] B. Adam a établi une proposition qui, utilisant un vecteur isotrope de F , lui a permis de restreindre à huit le nombre de choix pour un point extrémal adjacent à 1. Dans [7], on a amélioré la proposition de B. Adam [1] et on a réduit à cinq au maximum le nombre de choix pour un point extrémal adjacent à 1. On supposera dans la suite que $(\gamma_1, 1, \gamma_2)$ est un vecteur isotrope de F et on pose

$$\begin{aligned} \phi_1 &= [\gamma_1] + \lambda_1 + [\gamma_2]\lambda_2, & Q_1 &= ([\gamma_1], 1, [\gamma_2]), \\ \phi_2 &= [\gamma_1] + \lambda_1 + ([\gamma_2] + 1)\lambda_2, & Q_2 &= ([\gamma_1], 1, [\gamma_2] + 1), \\ \phi_3 &= [\gamma_1] + \lambda_1 + ([\gamma_2] - 1)\lambda_2, & Q_3 &= ([\gamma_1], 1, [\gamma_2] - 1), \\ \phi_4 &= [\gamma_1] - 1 + \lambda_1 + [\gamma_2]\lambda_2, & Q_4 &= ([\gamma_1] - 1, 1, [\gamma_2]), \\ \phi_5 &= [\gamma_1] - 1 + \lambda_1 + ([\gamma_2] + 1)\lambda_2, & Q_5 &= ([\gamma_1] - 1, 1, [\gamma_2] + 1), \end{aligned}$$

où $[x]$ désigne la partie entière du réel x .

Lemme 2.1 [1]. Soit F une forme quadratique à trois variables u, v, w à coefficients réels, positive de rang 2 telle que $F(1, 0, 0) = 1$ et $F(0, 0, 1) > 1$. Si F admet un vecteur isotrope $(\gamma_1, 1, \gamma_2)$, alors F s'écrit $F(u, v, w) = a(w - \gamma_2v)^2 + 2b(w - \gamma_2v)(u - \gamma_1v) + (u - \gamma_1v)^2$ avec $a > 1$ et $a > b^2$.

Proposition 2.1 [7]. Si $\gamma_1 > 0$, $\gamma_2 \in \mathbb{R}^*$, $0 < \lambda_1 < 1$, $0 < \lambda_2 < 1$ et $a > \max(1, 2b^2, 2|b|)$ on a :

- (1) Soit $F(Q_1) < 1$.
 - (i) Si $b < 0$, alors le point extrémal adjacent à 1 est ϕ_1, ϕ_3 ou ϕ_4 .
 - (ii) Si $b \geq 0$, alors le point extrémal adjacent à 1 est ϕ_1 ou ϕ_5 .
- (2) Soient $F(Q_1) > 1$, $F(Q_2) < 1$ et $\phi_1 > 1$.
 - (i) Si $b < 0$, alors le point extrémal adjacent à 1 est ϕ_2, ϕ_3 ou ϕ_4 .
 - (ii) Si $b \geq 0$, alors le point extrémal adjacent à 1 est ϕ_2 ou ϕ_5 .

3. Détermination des invariants arithmétiques d'une famille

Soit $n \geq 2$ un entier, on considère le polynôme : $P(X) = X^3 - nX^2 - n$. Levesque et Rhin [17] ont montré que ce type de polynôme est irréductible, admet une racine réelle unique, notée α .

3.1. Recherche de l'unité fondamentale dans $\mathbb{Z}[\alpha]$

Théorème 3.1. Soient α la racine réelle du polynôme $P(X)$ et $K = \mathbb{Q}(\alpha)$.

- (1) La suite des points extrémaux de $\mathbb{Z}[\alpha]$ est : $\psi_0 = 1, \psi_1 = \alpha, \psi_2 = \alpha^2$ et $\psi_3 = \alpha^3/n$.
- (2) L'unité fondamentale dans $\mathbb{Z}[\alpha]$ est ψ_3 et la longueur du développement par l'algorithme de Voronoi est $l = 3$.

Démonstration. A l'aide de la Proposition 2.1 on montre les résultats donnés dans le Tableau 1.

On a noté $\phi_0 = \alpha - n$, $\psi_{-1} = n/\alpha$ et les troisièmes et quatrièmes colonnes du Tableau 1 donnent les coordonnées de ψ_{k+1}/ψ_k et de $\bar{\phi}_{k+1}/\psi_k$ dans le réseau L_k . A l'aide des quotients successifs on peut facilement déterminer la suite des points extrémaux ψ_k de $L_0 = \mathbb{Z}[\alpha]$ (l'égalité $L_0 = \mathbb{Z}[\alpha]$ se déduit de la Proposition 4.7.4, p. 190 [4]). On déduit que $\psi_3 = \alpha^3/n$.

On a $N(\psi_3) = 1$ et $N(\psi_i) \neq 1$ si $1 \leq i \leq 2$. Donc ψ_3 est l'unité fondamentale ε de $\mathbb{Z}[\alpha]$ et la longueur de la période du développement de l'algorithme de Voronoi est $l = 3$.

Remarque 3.1. On note que $\text{Irrd}(\alpha^2 + 1, \mathbb{Q}) = X^3 - (n^2 + 3)X^2 + 3X - 1$.

3.2. Condition nécessaire et suffisante de monogénéité

Théorème 3.2. Soient α la racine réelle du polynôme $P(X)$ et $K = \mathbb{Q}(\alpha)$. Soit $n = 3^s n'$ avec $s \in \mathbb{N}$, $n' \in \mathbb{N}$, et n' et 3 sont premiers entre eux. Si n est sans facteurs carrés alors on a : $O_K = \mathbb{Z}[\alpha]$ si et seulement si $(4n^2 + 27)/9^s$ est sans facteurs carrés.

Pour la démonstration de ce théorème on a besoin des lemmes suivants :

Tableau 1
Résultats

Table 1
Results

k	$L_k = \langle 1, \bar{\phi}_k/\psi_k, \psi_{k-1}/\psi_k \rangle$	ψ_{k+1}/ψ_k	$\bar{\phi}_{k+1}/\psi_k$
0	$\langle 1, \alpha - n, n/\alpha \rangle$	$(n, 1, 0)$	$(0, 0, 1)$
1	$\langle 1, \alpha - n, 1/\alpha \rangle$	$(n, 1, 0)$	$(0, 0, 1)$
2	$\langle 1, 1/\alpha^2, 1/\alpha \rangle$	$(1, 1, 0)$	$(0, 0, 1)$

Lemme 3.1 [16]. Soient $K = \mathbb{Q}(\alpha)$ un corps de nombres de degré n et $P(X) \in \mathbb{Z}[X]$ le polynôme minimal de α . On pose $\delta = P'(\alpha)$ et $D = N(\delta)$. Pour tout nombre premier p et pour tout $a \in \mathbb{Z}$ on note $v_p(a)$ le plus grand entier m tel que $p^m | a$. Alors : $D/\delta = \sum_{i=0}^{n-1} x_i \alpha^i$, $x_i \in \mathbb{Z}$.

En plus s'il existe, pour un nombre premier p , un indice i tel que p ne divise pas x_i on obtient

$$v_p(d_K) = \begin{cases} 1 & \text{si } v_p(D) \text{ est impair,} \\ 0 & \text{si } v_p(D) \text{ est pair} \end{cases}$$

et $v_p(\text{Ind}(\alpha)) = [v_p(D)/2]$, où $\text{Ind}(\alpha)$ désigne l'ordre du groupe additif fini $O_K/\mathbb{Z}[\alpha]$.

Lemme 3.2. En reprenant les notations du Lemme 3.1. Soit $\bar{P}(X) = \bar{g}^e(X)$ avec $e \geq 2$ la factorisation de $P(X)$ modulo p dans $\mathbb{F}_p[X]$ et on pose $T(X) = \frac{P(X) - \bar{g}^e(X)}{p} \in \mathbb{Z}[X]$. Alors les assertions suivantes sont équivalentes :

- (1) p ne divise pas $\text{Ind}(\alpha) = [O_K : \mathbb{Z}[\alpha]]$.
- (2) $(\bar{T}, \bar{g}) = \bar{1}$ dans $\mathbb{F}_p[X]$.
- (3) $\text{Res}(g, P)/p^{\deg(g)} \in \mathbb{Z} - p\mathbb{Z}$, autrement dit $v_p(\text{Res}(g, P)) = \deg(g)$.

Démonstration. Le théorème de Dedekind [4], p. 305, assure qu'il y a équivalence entre (1) et (2). Montrons l'équivalence entre (2) et (3) : D'après le Corollaire 2, p. 73, Iv [3] on a $(\bar{T}, \bar{g}) = \bar{1}$ dans $\mathbb{F}_p[X]$ si et seulement si $\text{Res}(\bar{T}, \bar{g}) \neq \bar{0}$ dans \mathbb{F}_p , d'autre part $\text{Res}(\bar{g}, \bar{T}) = \overline{\text{Res}}(g, T)$ et $\text{Res}(g, T) = \text{Res}(g, P)/p^{\deg(g)}$.

Lemme 3.3. En reprenant les notations du Lemme 3.1 on a : $O_K = \mathbb{Z}[\alpha]$ si et seulement si pour tout nombre premier p tel que p^2 divise $\text{Disc}(P)$ on a p ne divise pas $\text{Ind}(\alpha)$.

Démonstration. Résulte du fait que $O_K = \mathbb{Z}[\alpha]$ si et seulement si $\text{Ind}(\alpha) = 1$, et que $\text{Disc}(P) = (\text{Ind}(\alpha))^2 d_K$ (voir [4], p. 166).

Lemme 3.4. On pose $\delta = P'(\alpha)$, avec $P(X) = \text{Irrd}(\alpha, \mathbb{Q}) = X^3 - nX^2 - n$, et $D = N(\delta)$ on a : $\delta = 3\alpha^2 - 2n\alpha$, $D = n^2(4n^2 + 27)$ et $D/\delta = \sum_{i=0}^2 x_i \alpha^i$ avec $x_0 = -3n^2$, $x_1 = 2n^3 + 9n$ et $x_2 = -2n^2$.

Preuve du Théorème 3.2. Montrons que si $O_K = \mathbb{Z}[\alpha]$ alors $(4n^2 + 27)/9^s$ est sans facteurs carrés : supposons que $O_K = \mathbb{Z}[\alpha]$ et qu'il existe un nombre premier p tel que p^2 divise $(4n^2 + 27)/9^s$, donc p ne divise pas $x_0 = -3n^2$, ainsi d'après le Lemme 3.1 on a $v_p(\text{Ind}(\alpha)) = [v_p(D)/2]$, or $[v_p(D)/2] = [1/2 v_p((4n^2 + 27)/9^s)] \geq 1$, donc p divise $\text{Ind}(\alpha) = 1$, ce qui est impossible.

Inversement, supposons que $(4n^2 + 27)/9^s$ est sans facteurs carrés et montrons que $O_K = \mathbb{Z}[\alpha]$: soit p un nombre premier tel que p^2 divise $\text{Disc}(P) = -n^2(4n^2 + 27)$, donc p divise n et par suite $\bar{P}(X) = \bar{g}(X)^3 \pmod{p}$ avec $g(X) = X$ et $\text{Res}(g, P)/p^{\deg(g)} = P(0)/p = -n/p \in \mathbb{Z} - p\mathbb{Z}$, donc d'après le Lemme 3.2 on a p ne divise pas $\text{Ind}(\alpha)$, ainsi d'après le Lemme 3.3 on a $O_K = \mathbb{Z}[\alpha]$.

3.3. Calcul du discriminant et du régulateur de K

Corollaire 3.1. Avec les mêmes notations que celles du Théorème 3.1. Si n et $(4n^2 + 27)/9^s$ sont sans facteurs carrés alors on a : (1) $O_K = \mathbb{Z}[\alpha]$ et $d_K = -n^2(4n^2 + 27)$; (2) $R_K = \text{Log}(\alpha^2 + 1)$.

Démonstration. (1) Résulte du Théorème 3.2 et de la Proposition 4.4.4, p. 166 [4]. (2) Résulte du Théorème 3.1 et de la Définition 4.9.8, p. 211 [4].

Remarque 3.2. Si on se place dans la situation du Corollaire 3.1, le nombre de classes h_K de K sera donné par la formule :

$$h_K = \frac{n\sqrt{4n^2 + 27}}{2\pi \operatorname{Log}(\alpha^2 + 1)} \prod_{i=1}^3 E_i,$$

où $E_1 = \prod_{\substack{(d_K/p)=1 \\ p \nmid d_K}} E(p)$, $E_2 = \prod_{\substack{p \nmid d_K \\ (d_K/p)=-1}} E(p) = \prod_{\substack{(d_K/p)=-1 \\ p \nmid d_K}} \frac{p^2}{p^2-1}$, $E_3 = \prod_{p \mid d_K} E(p) = \prod_{\substack{p \nmid n \\ p \mid 4n^2+27}} \frac{p}{p-1}$ et $E(p) = (1 - 1/p) / \prod_{\beta \mid p} (1 - 1/N(\beta))$; le produit ci-dessus porte sur l'ensemble des idéaux premiers de O_K au-dessus de p et $N(\beta)$ désigne la norme de l'idéal β .

En effet, on applique le Corollaire 3.1, les résultats de la décomposition des nombres premiers dans les extensions cubiques de \mathbb{Q} (voir [4], p. 351) et la formule analytique du nombre de classes (voir [4], p. 356) on obtient h_K .

4. Cardinalité de la famille des corps $(K_n)_{n \in E}$

Soit $n \geq 1$ un entier, on considère le polynôme : $P_n(X) = X^3 - nX^2 - n$. Le Lemme 1.1 et le Corollaire 1.2, p. 174 [17] montrent que $\forall n \in \mathbb{N}^* \exists \alpha_n \in \mathbb{R}$ tel que $P_n(X) = \operatorname{Irrd}(\alpha_n, \mathbb{Q})$ et $n < \alpha_n < n + 1$. Autrement dit α_n est l'unique racine réelle du polynôme irréductible $P_n(X)$ et si $n \neq m$ alors $\alpha_n \neq \alpha_m$. Considérons l'ensemble $E = \{n \in \mathbb{N} \mid n \text{ et } (4n^2 + 27)/9^{v_3(n)} \text{ sont sans facteurs carrés}\}$ et le corps cubique $K_n = \mathbb{Q}(\alpha_n)$. Donc d'après le Corollaire 3.1 pour tout $n \in E$ le corps K_n est monogène et par suite $R_{K_n} = \operatorname{Log}(\alpha_n^2 + 1)$. Or la fonction $\operatorname{Log}(x^2 + 1)$ est strictement monotone. Donc si $n, m \in E$ et $n \neq m$ alors les corps K_n et K_m sont distincts car leurs régulateurs le sont. Ainsi la famille des corps monogènes $(K_n)_{n \in E}$ est infinie si et seulement si E est infini.

Références

- [1] B. Adam, Développements périodiques de familles paramétrées de nombres algébriques Application à la recherche d'unités, Thèse de doctorat, Univ. Metz, 1995.
- [2] G. Archinard, Extensions cubiques cycliques de \mathbb{Q} dont l'anneau des entiers est monogène, Enseign. Math. 20 (2) (1974) 179–191.
- [3] N. Bourbaki, Algèbre, Masson, 1981, Chapitres 4 à 7.
- [4] H. Cohen, A Course in Computational Algebraic Number Theory, Vol. 138, Springer-Verlag, 1993.
- [5] R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren cyclotimic index, Abh. Akad. Wiss. Göttingen, Math.-Phys. Kl. 23 (1878) 1–23.
- [6] D.S. Dummit, H. Kisilevsky, Indices in cyclic cubic fields, in: Number Theory and Algebra, Academic Press, New York, 1977, pp. 29–42.
- [7] A. Farhane, O. Lahlou, Sur les points extrémaux dans un ordre cubique, à paraître.
- [8] V. Fléckinger, Monogénéité de l'anneau des entiers de certains corps de classes de rayon, Ann. Inst. Fourier (Grenoble) 38 (1) (1988) 17–57.
- [9] M.N. Gras, Sur les corps cubiques cycliques dont l'anneau des entiers est monogène, C. R. Acad. Sci. Paris, Sér. A 278 (1974) 59–62.
- [10] M.N. Gras, \mathbb{Z} -bases d'entiers $1, \theta, \theta^2, \theta^3$ dans les extensions cycliques de degré 4 de \mathbb{Q} , Publ. Math. Fac. Sci. Besançon, Théorie des Nombres (1980/1981), 11 pp.
- [11] M.N. Gras, Non monogénéité des anneaux d'entiers des extensions cycliques de \mathbb{Q} de degré premier $l \geq 5$, J. Number Theory 23 (3) (1986) 347–353.
- [12] K. Györy, On discriminants and indices of integers of an algebraic number field, J. Reine Angew. Math. 324 (1981) 114–126.
- [13] K. Györy, Corps de nombres algébriques d'anneau d'entiers monogène, in : Séminaire Delange–Pisot–Poitou, 20^{ème} année, 1978/79, Théorie des nombres. Exp. n° 26, 7 p.
- [14] K. Györy, Sur les générateurs des ordres monogènes des corps de nombres algébriques, in : Séminaire de Théorie des nombres, 1983/84, Univ. Bordeaux 1, Talence, Exp. n° 32, 12 p.
- [15] G.J. Janusz, Algebraic Number Theory, Academic Press, New York, 1973.
- [16] K. Komatsu, Integral bases in algebraic number fields, Tokyo.
- [17] C. Levesque, G. Rhin, Two families of periodic Jacobi algorithms with period lengths going to infinity, J. Number Theory 37 (2) (1991) 173–180.
- [18] T. Nakahara, On the indices and integral bases of non-cyclic but Abelian biquadratic fields, Arch. Math. 41 (6) (1983) 504–507.
- [19] F. Tanoë, Monogénéité des corps biquadratiques, Thèse de doctorat, Univ. Franche-Comté, 1990.
- [20] G.F. Voronoi, On a generalization of the algorithm of continued fractions, Doctoral Dissertation, Warsaw, 1896 (en Russe).
- [21] H.C. Williams, The period length of Voronoi's algorithm for certain cubic orders, Publ. Math. Debrecen 37 (1990) 245–265.