Introduction

EXTENSIONS CUBIQUES CYCLIQUES DE Q DONT L'ANNEAU DES ENTIERS EST MONOGÈNE

par Gabriel ARCHINARD

INTRODUCTION

Soit K/k une extension finie de corps de nombres et O_K et O_k leurs anneaux d'entiers. L'existence d'un élément $\theta \in O_K$ tel que $O_K = \mathbf{Z}[\theta]$ — on dit alors que O_K est monogène — facilite grandement l'étude de l'arithmétique de O_K.

Dans une étude récente, J.-J. Payan obtient des conditions nécessaires pour que O_K soit monogène lorsque k est le corps Q ou un corps quadratique imaginaire et lorsque K/k est cyclique de degré premier impair [6].

Dans le cas où $k = Q$, soit n le degré de K/Q, Δ_K le discriminant de K/Q, $\Delta(\theta)$ le discriminant de l'élément $\theta \in O_K$ et $I(\theta)$ son indice $(\Delta(\theta) = (I(\theta))^2 \Delta_K)$. Alors, la conditions $I(\theta) = \pm 1$ est nécessaire et suffisante pour que $O_K = \mathbf{Z}[\theta]$. $I(\theta)$ pouvant s'exprimer comme forme primitive de degré $\frac{1}{2} n(n-1)$ en $n-1$ variables à valeurs entières, [4], la recherche des générateurs de O_K est équivalente à la résolution de l'équation diophantienne $I(\theta) = \pm 1$. Un cas simple où O_K n'est pas monogène est celui où les nombres $I(\theta)$, $\theta \in O_K$, ont un diviseur commun autre que ± 1. Le critère de Hensel [3], permet de déterminer ces cas en considérant la décomposition des nombres premiers inférieurs à n dans O_K, et Nagell, [5], donne des conditions d'existence de diviseurs communs des indices autres que ± 1, pour les extensions cubiques et pour certaines extensions de degré > 4.

Dans ce travail, j'étudie l'existence d'un générateur de l'anneau des entiers dans le cas des extensions K/Q cubiques cycliques, et j'utilise pour ceci la construction due à A. Châtelet ([1], chap. I à IV) dont l'essentiel est rappelé au chapitre 1. Cette construction établit une application de l'ensemble des couples (θ, σ), formés d'un nombre cubique cyclique θ et d'un générateur de $\mathrm{Gal}(Q(\theta)/Q)$, dans $Q(j) \times Z$, où $j = \frac{1}{2}(-1+i\sqrt{3})$. Si $(\beta, S) \in Q(j) \times Z$ est l'image de (θ, σ) par cette application, S est la trace de θ et on dit que θ est construit avec (β, S) et que β engendre $Q(\theta)$ ($Q(\theta)$

ne dépendant pas de S). De plus, toute extension cubique cyclique K/Q est engendrée par un entier de $Q(j)$ dont la norme est produit de nombres premiers distincts et congrus à 1 (mod 3). Un tel entier est dit canonique et permet la construction de bases d'entiers de K dites aussi canoniques.

Dans le chapitre 2, en utilisant une base canonique de K, j'obtiens pour $I(\theta)$ les formes (2.1) et (2.2), ce qui amène notamment à la propriété suivante:

Propriété 2.3 Soit K le corps engendré par l'entier canonique $a_1 j + a_2 j^2$ ($a_i \in Z$). Alors, 2 est diviseur commun des indices de K si et seulement si $a_1 - a_2$ est pair.

Dans le chapitre 3, j'obtiens le résultat principal de ce travail: des conditions nécessaires et suffisantes sur (β, S) pour que le nombre θ construit avec (β, S) soit générateur de l'anneau des entiers de $Q(\theta)$. Ces conditions, trop longues à énoncer dans cette introduction, sont données par le théorème 3.2. On en déduit aisément les théorèmes suivants:

Théorème 3.3 Soit K/Q une extension cubique cyclique de discriminant m^2. Alors, si O_K est monogène, l'équation diophantienne suivante est soluble:

$$X^2 + 3X + 9 = mY^3 .$$

Théorème 3.4 Soit $m \neq 1$, un produit de nombres premiers et congrus à 1 (mod 3). Alors,

a) si l'équation diophantienne

$$X^2 + 3X + 9 = mY^3$$

est soluble, avec $X \not\equiv 0 \pmod 3$ ou $X \equiv 12 \pmod{27}$, il existe une extension cubique cyclique de Q, modérément ramifiée, de discriminant m^2 et dont l'anneau des entiers est monogène.

b) si l'équation diophantienne

$$X^2 + X + 1 = mY^3$$

est soluble, il existe une extension cubique cyclique de Q, sauvagement ramifiée, de discriminant $81\,m^2$ et dont l'anneau des entiers est monogène.

Ces équations présentent l'avantage de se réduire à des équations du deuxième degré en une variable lorsqu'on fixe la valeur de Y. J'ai utilisé

cette méthode en donnant à Y les valeurs de 1 à 100000 et à m une centaine de valeurs pour chacune des équations a) et b).

Les résultats sont exposés aux chapitres 4 (4.1 et 4.2).

Dans un travail récent [2], M.-N. Gras obtient, par d'autres méthodes, des résultats semblables aux théorèmes 3.3 et 3.4 et donne une liste très fournie de corps cubiques cycliques dont l'anneau est soit monogène, soit non monogène.

MM. les professeurs F. Châtelet et J.-J. Payan m'ont dirigé et aidé dans ce travail; je leur exprime ici ma très vive reconnaissance.

Je remercie aussi M. R. Smadja dont un manuscrit m'a été utile dans la recherche des conditions du théorème 3.2 et M^me M. Archinard, qui a bien voulu se charger de la programmation.

Enfin, je remercie le Centre d'économétrie de l'Université de Genève qui m'a donné accès à l'ordinateur de l'Etat de Genève.

Chapitre 1. — Construction des extensions cubiques cycliques de Q

On rappelle dans ce chapitre la construction donnée par A. Châtelet. ([1], chap. 1 à IV).

1. Notations

Dans la suite, K désigne une extension cubique cyclique du corps Q des rationnels, O_K l'anneau des entiers de K, Δ_K le discriminant de K/Q et $\mathrm{Gal}(K/Q)$ son groupe de Galois. E désigne le corps $Q(j)$, où $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, O_E l'anneau des entiers de E, τ le Q-automorphisme de E défini par $\tau j = j^2$ et β' l'élément $\tau\beta$, pour $\beta \in E$. τ désigne aussi le prolongement de τ à $K(j)$ ayant K comme corps des invariants. σ désigne à la fois un élément non trivial de $\mathrm{Gal}(K/Q)$ et son prolongement à $K(j)$ qui laisse E invariant. E est donc le corps des invariants du groupe cyclique engendré par σ.

θ étant un élément de K, on définit les expressions suivantes (résolvantes de Lagrange).

$$<\theta, \sigma> = \theta + j\sigma\theta + j^2\sigma^2\theta \quad \sigma \in \mathrm{Gal}(K/Q)$$