Un anneau d'entiers stablement libre et non libre

Jean Cougnard

TABLE DES MATIÈRES

L'anneau des entiers $\mathcal{O}_N$ d'une extension galoisienne $N/\mathbb{Q}$ modérément ramifiée de groupe de Galois G est $\mathbb{Z}[G]$-projectif. Il existe une condition nécessaire et suffisante pour que la somme $\mathcal{O}_N \oplus \mathbb{Z}[G]$ soit isomorphe à $\mathbb{Z}[G]^2$. On donne un premier exemple où cette condition n'implique pas que $\mathcal{O}_N$ soit $\mathbb{Z}[G]$ libre.

The ring of integers $\mathcal{O}_N$ of a tame Galois extension $N/\mathbb{Q}$ with Galois group G is $\mathbb{Z}[G]$-projective. There exists a necessary and sufficient condition for $\mathcal{O}_N \oplus \mathbb{Z}[G]$ and $\mathbb{Z}[G]^2$ to be isomorphic. We give a first example where this condition does not imply that $\mathcal{O}_N$ is free over $\mathbb{Z}[G]$.

1. INTRODUCTION

Pour chaque corps de nombres M, l'anneau des entiers se note $\mathcal{O}_M$.

Soit N/K une extension galoisienne de corps de nombres de groupe de Galois G, modérément ramifiée (c'est-à-dire les idéaux ramifiés ont des indices de ramification premiers à la caractéristique de leurs corps résiduels). On sait qu'alors l'anneau des entiers $\mathcal{O}_N$ est un $\mathcal{O}_K[G]$ (et par restriction un $\mathbb{Z}[G]$) module projectif.

Un théorème de M. J. Taylor [1981], répondant à une conjecture de A. Fröhlich, lie la classe de $\mathcal{O}_N$ dans $\mathrm{Cl}(G)$ (le groupe des classes des $\mathbb{Z}[G]$-modules projectifs) aux constantes des équations fonctionnelles des fonctions L d'Artin (pour un exposé complet, voir [Fröhlich 1983] et sa bibliographie). Dans de nombreux cas, le théorème de Taylor permet de savoir si $\mathcal{O}_N$ est $\mathbb{Z}[G]$-libre ou non. Il reste toutefois une famille d'extensions pour laquelle il ne permet pas de se prononcer : ce sont les extensions galoisiennes de $\mathbb{Q}$ dont l'algèbre sur $\mathbb{Z}$ du groupe de Galois ne possède pas la propriété de simplification.

1058-6458/96 \$0.50 per page

Le théorème permet alors au mieux d'affirmer soit que :

$$\mathcal{O}_N \oplus \mathcal{O}_N \approx \mathbb{Z}[G] \oplus \mathbb{Z}[G]$$

soit que :

$$\mathcal{O}_N \oplus \mathbb{Z}[G] \approx \mathbb{Z}[G] \oplus \mathbb{Z}[G].$$

On dit dans ce dernier cas que le $\mathbb{Z}[G]$-module $\mathcal{O}_N$ est stablement libre, sans que l'on puisse en déduire qu'il est libre (c'est-à-dire que $\mathcal{O}_N \approx \mathbb{Z}[G]$). Une telle situation se produit avec le groupe H_{32}, groupe quaternionien d'ordre 32, et c'est Swan qui le premier a construit un $\mathbb{Z}[H_{32}]$-module stablement libre et non-libre [Swan 1962] ; on peut trouver de plus amples renseignements sur ce problème dans [Vigneras 1975; Swan 1981].

Dans le cas des extensions modérément ramifiées à groupe de Galois quaternionien d'ordre 32, Fröhlich [1980] a prouvé que leur anneau des entiers est toujours stablement libre. La question se pose de savoir si ces anneaux d'entiers sont ou non libres. On construit ici une extension de $\mathbb{Q}$, modérément ramifiée, de groupe de Galois H_{32}, et prouve que son anneau des entiers n'est pas libre. Les calculs ont été effectués au moyen du logiciel Pari [Batut et al. 1992].

Une autre question, qui reste ouverte, est la suivante : Lorsqu'un élément x de $\mathrm{Cl}(G)$ représente un anneau d'entiers, est-ce que toutes les classes d'isomorphismes de $\mathbb{Z}[G]$ modules de rang 1 de cette classe peuvent être réalisées par des anneaux d'entiers ? Dans le cas de H_{32}, il y a trois telles classes d'isomorphisme [Swan 1981], et l'on aimerait savoir si le résultat de cet article s'étend aux deux autres classes.

2. CHOIX DU CORPS

Une extension galoisienne modérément ramifiée de $\mathbb{Q}$ à groupe de Galois quaternionien d'ordre 32 contient un corps quadratique réel $\mathbb{Q}(\sqrt{d})$ avec $d \equiv 1 \bmod 4$; ce corps se plonge d'une infinité de façons dans une extension diédrale de $\mathbb{Q}$ de degré 32, modérément ramifiée, et d'une infinité de manières dans une extension cyclique de $\mathbb{Q}$ de degré 4, modérément ramifiée. On peut choisir une des extensions diédrales, la composer avec une des extensions cycliques de degré 4 ; le compositum contient alors une extension quaternionienne de degré 32. Réciproquement la composée de deux extensions, l'une quaternionienne de degré 32, l'autre cyclique de degré 4, contenant un même sous-corps quadratique réel contient une extension cyclique de degré 16 de ce corps quadratique réel, diédrale sur $\mathbb{Q}$ [Damey et Martinet 1973]. Les changements de corps diédraux et cycliques permettent de varier la ramification.

Il faut partir d'un corps quadratique réel $k = \mathbb{Q}(\sqrt{d})$ avec $d \equiv 1 \bmod 4$ et chercher les groupes de classes généralisés possédant un quotient cyclique d'ordre 16, invariant par la conjugaison du corps quadratique. Plutôt que de faire une telle étude, il a paru plus rapide de regarder dans les tables de groupes de classes de B. Oriat [19 ? ?] les $\mathbb{Q}(\sqrt{p_1p_2})$ avec p_1 et $p_2 \equiv 1 \bmod 4$, ce qui assure que le 2-groupe des classes est cyclique, et de prendre le premier exemple dont le nombre de classes est divisible par 16 : $K_0 = \mathbb{Q}(\sqrt{5 \times 461})$. On engendre un idéal entier de norme 2305 dans K_0 par $u = 2305 + 48\sqrt{2305}$, et $\mathbb{Q}(\sqrt{2305 + 48\sqrt{2305}})$ est une extension M_0 cyclique de degré 4 de $\mathbb{Q}$ dans laquelle 5 et 461 sont totalement ramifiés. Par ailleurs le corps de classes de Hilbert de K_0 est l'extension cyclique non ramifiée de degré 16 de K_0 diédrale sur $\mathbb{Q}$.

On a la tour cyclique non ramifiée maximale de 2-extensions :

$$K_0 = \mathbb{Q}(\sqrt{2305}) \subset K_1 = \mathbb{Q}(\sqrt{5}, \sqrt{461}) \subset K_2 \subset K_3 \subset K_4,$$

où K_i est diédrale de degré 2^{1+i} sur $\mathbb{Q}$. Le composé de K_i et M_0 est noté M_i. Le corps M_4 est une extension biquadratique de K_3. Le sous-corps N de M_4, quadratique sur K_3 et distinct de K_4 et de M_3, est une extension quaternionienne de $\mathbb{Q}$ contenant K_0, modérément ramifiée (voir [Damey et Martinet 1973, § II]). C'est l'anneau des entiers $\mathcal{O}_N$ de ce corps de nombres qui fournit l'exemple cherché.

3. UNE ALGÈBRE DE QUATERNIONS

Pour exposer le principe de la preuve, supposons construit l'anneau des entiers $\mathcal{O}_N$, connue une $\mathbb{Z}$-base et l'action des éléments du groupe de Galois sur cette base. On suit la démarche habituelle qui consiste, dans un premier temps, à faire une extension des scalaires de $\mathbb{Z}[G]$ à un ordre maximal $\mathcal{M}$ le contenant, c'est-à-dire à étudier $\mathcal{M}\mathcal{O}_N$. Un tel ordre maximal est produit direct d'ordres maximaux de chacun des facteurs simples de $\mathbb{Q}[G]$ et on regarde d'abord des modules sur un ordre maximal d'une algèbre centrale simple. On a, par conséquent, besoin de quelques renseignements sur l'algèbre $\mathbb{Q}[H_{32}]$.

Définissons le groupe $G = H_{32}$ par générateurs et relations : $\{\sigma, \tau \mid \sigma^{16} = e;\ \tau^2 = \sigma^8;\ \tau\sigma\tau^{-1} = \sigma^{-1}\}$. Les facteurs simples de $\mathbb{Q}[G]$ sont en bijection avec les classes de conjugaison de caractères à valeurs dans $\mathbb{Q}$. Les méthodes classiques [Serre 1971, ch. 13] nous donnent :

- 4 facteurs simples isomorphes à $\mathbb{Q}$ provenant des représentations de degré 1 de H_{32} ;
- 2 facteurs simples isomorphes à une algèbre de matrices 2×2 à cœfficients l'une dans $\mathbb{Q}$, l'autre dans $\mathbb{Q}(\sqrt{2})$, et qui correspondent aux représentations irréductibles de degré 2 du groupe diédral d'ordre 16 quotient de H_{32} par son centre ; avec les notations du § 1 ce groupe est le groupe de Galois de $K_3/\mathbb{Q}$.
- Un facteur $A = \mathbb{Q}[H_{32}]/(\tau^2 + 1)$ qui s'identifie à une $\mathbb{Q}$-sous-algèbre $\mathbb{H}$ du corps des quaternions usuels $\mathbb{R}[i, j, k]$ (avec les relations $i^2 = j^2 = k^2 = ijk = -1$). Si ζ est une racine primitive 16-ème de l'unité, $t = \zeta + \zeta^{-1}$ est réel et A est la sous-algèbre engendrée par ζ et j.

On reprend les indications données dans [Swan 1962, § 2]. On peut choisir la racine de l'unité ζ de sorte que $t = \sqrt{2 + \sqrt{2}}$, un de ses conjugués galoisiens est $t' = \tau^{-1}\sqrt{2} = \sqrt{2 - \sqrt{2}}$. On pose

$$\alpha = \frac{\sqrt{2} + 1 + i}{\sqrt{2}\tau},$$

on construit un homomorphisme de $\mathbb{Z}[H_{32}]$ dans A en envoyant σ sur α et τ sur j, et l'on note $\mathcal{O}$ son image. Pour les calculs effectués dans l'algèbre de quaternions, on choisit comme base les éléments α^r et $\alpha^s j$, où $0 \le r, s \le 7$. Le centre de $\mathcal{O}$ est le sous-anneau R engendré par t.

Soit $\beta = (1 + j)/t'$. Le R-module Λ engendré par 1, α, β et $\alpha\beta$ est un sous-anneau de A et on peut prouver que c'est un ordre maximal de A qui contient $\mathcal{O}$. Un autre ordre maximal Λ' est donné par une R-base

$$1,\ \frac{1+i}{\sqrt{2}},\ \frac{1+j}{\sqrt{2}},\ \frac{1+i+j+k}{2}.$$

Soit $\mathcal{I}$ un Λ-idéal à gauche ; c'est un Λ-module projectif. S'il est libre, c'est-à-dire de la forme Λm, son ordre à droite, c'est-à-dire l'ensemble des λ de A tels que $\mathcal{I}\lambda \subset \mathcal{I}$, est l'ordre maximal $m^{-1}\Lambda m$. On a ainsi la notion d'ordres conjugués.

On peut démontrer ([Swan 1962] par exemple) que l'ordre Λ possède 2 classes d'isomorphismes d'idéaux à gauche et que dans A existent deux classes de conjugaison d'ordre maximaux Vigneras 1972, ch. II, § 3. Il en résulte [Swan 1962] qu'un Λ-idéal à gauche est libre si et seulement si son ordre à droite est conjugué de Λ, et n'est pas libre si et seulement si son ordre à droite est conjugué de Λ'. Une manière de distinguer entre ces deux classes de conjugaison consiste à regarder les unités de l'ordre maximal. Deux ordres conjugués ont des groupes d'unités isomorphes et seuls les ordres conjugués de Λ' possèdent un élément d'ordre 3.

Remarque. Un idéal à gauche d'un ordre maximal étant donné, on peut construire explicitement son ordre à droite en un nombre fini d'étapes ; par ailleurs, un ordre d'un corps de quaternions totalement défini étant donné, la remarque 2 de [Swan 1962] montre qu'il existe un algorithme permettant de déterminer ses éléments de norme réduite 1 et donc son groupe de torsion.

Un travail de Vignéras [1975, § 4, th. 5, lemmes 3 et 4, th. 6) permet de décrire le groupe des unités de Λ : le sous-groupe des unités de Λ^* de norme 1 est le groupe H_{32} [Swan 1962, § 2] ; par ailleurs les éléments de la forme $(1+\alpha)x$ avec $x \in R$ ont une norme différente de 1. C'est que Λ^* est engendré par le groupe des unités de R et par l'image de H_{32}. D'où :

Lemme. *Les groupes des unités Λ^* et $\mathcal{O}^*$ sont les mêmes.*

4. PRINCIPE DE LA DÉMONSTRATION

On démontre maintenant que l'anneau $\mathcal{O}_N$ n'est pas libre.

Comme ordre maximal $\mathcal{M}$ contenant $\mathbb{Z}[H_{32}]$, on choisit un ordre de la forme $\mathcal{M}' \times \Lambda$ où $\mathcal{M}'$ est un ordre maximal de l'algèbre du groupe diédral d'ordre 16 et Λ l'ordre maximal décrit dans le paragraphe précédent. L'idempotent central $\frac{1}{2}(1-\sigma^8)$ est tel que $\frac{1}{2}(1-\sigma^8)\mathcal{M} = \Lambda$. On suppose que $\mathcal{O}_N$ est $\mathbb{Z}[H_{32}]$-libre, et on essaie d'obtenir une contradiction. Sous cette hypothèse,

$$\Bigl(\frac{1-\sigma^8}{2}\Bigr)^2\mathcal{M}\mathcal{O}_N \approx \Bigl(\frac{1-\sigma^8}{2}\Bigr)\mathcal{M}(1-\sigma^8)\mathcal{O}_N$$

est Λ-libre. Ceci fait apparaître $(1-\sigma^8)\mathcal{O}_N$ le noyau de la trace dans N/K_3, qui est, toujours parce que $\mathcal{O}_N$ est $\mathbb{Z}[H_{32}]$-libre, un module libre sur

$$\mathbb{Z}[H_{32}]/(1+\sigma^8)$$

isomorphe à l'image $\mathcal{O}$ de $\mathbb{Z}[H_{32}]$ dans A.

Soit a une $\mathcal{O}$-base de $\ker \mathrm{Tr}_{N/K_3}$ et b une base de $\Lambda(\ker \mathrm{Tr}_{N/K_3})$. Il existe donc une unité $\varepsilon \in \Lambda$ telle que $b = \varepsilon a$; or on a vu à la fin du § 3 que $\Lambda^* = \mathcal{O}^*$, donc $b = \varepsilon a$ est aussi une $\mathcal{O}$-base de $\ker \mathrm{Tr}_{N/K_3}$. Autrement dit toutes les bases de $\Lambda(\ker \mathrm{Tr}_{N/K_3})$ sont dans $\ker \mathrm{Tr}_{N/K_3}$.

Dans les calculs qui vont suivre, on met en évidence une Λ-base de $\Lambda(\ker \mathrm{Tr}_{N/K_3})$ qui n'appartient pas à $\ker \mathrm{Tr}_{N/K_3}$, ce qui nous donne la contradiction recherchée.

Construction des extensions et des anneaux d'entiers

Comme nous l'avons annoncé, nous commençons par construire le corps de classes de Hilbert de $K_0 = \mathbb{Q}(\sqrt{2305})$ et son anneau des entiers en précisant l'action du groupe de Galois sur cette base. Ceci a été exposé en détail dans [Cougnard 1992b]. On pose $\omega = \frac{1}{2}(1+\sqrt{5})$; son conjugué est $\omega_1 = 1-\omega$, et le composé K_1 de $L_1 = \mathbb{Q}(\omega)$ et K_0 est le corps des genres de K_0. Le nombre $\omega + 21$, congru à ω^2 modulo 4, est générateur totalement positif d'un idéal principal de norme 461. Posons

$$a = \frac{\omega + \sqrt{\omega+21}}{2},$$

et $L_2 = L_1(a)$. L'anneau des entiers de L_2 est engendré sur celui de L_1 par 1 et a ; le composé K_2 de L_2 et K_0 est une extension cyclique non ramifiée de degré 4 de K_0. Les conjugués de a sont :

$$\begin{aligned} a_1 &= \sigma(a) = \frac{\omega_1 + \sqrt{\omega_1+21}}{2}, \\ a_p &= \sigma^2(a) = \omega - a, \\ a_{1p} &= \sigma^3(a) = \frac{\omega - \sqrt{\omega+21}}{2}. \end{aligned}$$

Dans L_2, l'élément $15+7\omega+(1-5\omega)a$, congru à $1+(1+\omega)a)^2$ modulo 4, a pour norme 461 et est totalement positif. On construit le corps

$$L_3 = L_2(\sqrt{15+7\omega+(1-5\omega)a});$$

son anneau des entiers est engendré sur celui de L_2 par 1 et

$$b = \frac{1+(1+\omega)a + \sqrt{15+7\omega+(1-5\omega)a}}{2}.$$

On vérifie que $1+(1+\omega)a$ est une unité et donc que l'anneau des entiers de L_3 possède une base normale relativement à celui de L_2. Le composé de L_3 et K_0 est une extension cyclique non ramifiée de degré 8 de K_0. On peut prolonger σ par théorie de Kummer en vérifiant que :

$$\begin{aligned} 461\frac{\sigma(15+7w_1+(1-5w_1)a_1)}{15+7w_1+(1-5w_1)a_1} &= (-190a_1\omega a + 34a_p\omega_1 a_1 + 140a_{1p}\omega a_p \\ &\quad + 1271a\omega_1 a_{1p} + 190a_{1p}\omega a + 112a\omega_1 a_1 \\ &\quad - 140a_1\omega a_p + 888a_p\omega_1 a_{1p})^2. \end{aligned}$$

Les conjugués de b sont les $\sigma^k(b)$, pour $0 \le k < 8$. En ordre de k ascendant, ce sont :

$$
\begin{aligned}
b &= \frac{-1-(1+\omega)a+\sqrt{15+7\omega+(1-5\omega)a}}{2},\\
b_1 &= \frac{-1-(1+\omega_1)a_1+\sqrt{15+7\omega_1+(1-5\omega_1)a_1}}{2},\\
b_p &= \frac{-1-(1+\omega)a_p+\sqrt{15+7\omega+(1-5\omega)a_p}}{2},\\
b_{1pt} &= -1-(1+\omega_1)a_{1p}-b_{1p},\\
b_t &= -1-(1+\omega)a-b,\\
b_{1t} &= -1-(1+\omega_1)a_1-b_1,\\
b_{pt} &= -1-(1+\omega)a_p-b_p,\\
b_{1p} &= \frac{-1-(1+\omega_1)a_{1p}+\sqrt{15+7\omega_1+(1-5\omega_1)a_{1p}}}{2}.
\end{aligned}
$$

L'élément

$$
\begin{aligned}
y = 76 - 38\omega + (20-15\omega)a \\
+ (-24+13\omega+(-33+21\omega)a)b
\end{aligned}
$$

de L_3 est totalement positif, de norme 461, congru modulo 4 à

$$(3+2\omega+\omega a+(-3+3\omega+(2-\omega)a)b)^2$$

carré d'une unité de L_3. On en déduit donc que le corps K_4 composé de K_0 et de

$$L_4 = L_3(\sqrt{y})$$

est une extension cyclique non ramifiée de degré 16 de K_0, c'est donc le corps de classes de Hilbert de K_0. L'anneau des entiers de L_4 est engendré sur celui de L_3 par 1 et

$$c = \frac{3+2\omega+\omega a+(-3+3\omega+(2-\omega)a)b+\sqrt{y}}{2}.$$

Les conjugués de c sont :

$$
\begin{aligned}
c &= \tfrac{1}{2}\Big(3+2\omega+\omega a+(-3+3\omega+(2-\omega)a)b+\sqrt{76-38\omega+(20-15\omega)a+(-24+13\omega+(-33+21\omega)a)b}\Big)\\
c_1 &= \tfrac{1}{2}\Big(3+2\omega_1+\omega_1 a_1+(-3+3\omega_1+(2-\omega_1)a_1)b_1+\sqrt{76-38\omega_1+(20-15\omega_1)a_1+(-24+13\omega_1+(-33+21\omega_1)a_1)b_1}\Big)\\
c_p &= \tfrac{1}{2}\Big(3+2\omega+\omega a_p+(-3+3\omega+(2-\omega)a_p)b_p+\sqrt{76-38\omega+(20-15\omega)a_p+(-24+13\omega+(-33+21\omega)a_p)b_p}\Big)\\
c_{1ptu} &= \tfrac{1}{2}\Big(3+2\omega_1+\omega_1 a_{1p}+(-3+3\omega_1+(2-\omega_1)a_{1p})b_{1pt}-\sqrt{76-38\omega_1+(20-15\omega_1)a_{1p}+(-24+13\omega_1+(-33+21\omega_1)a_{1p})b_{1pt}}\Big)\\
c_{tu} &= \tfrac{1}{2}\Big(3+2\omega+\omega a+(-3+3\omega+(2-\omega)a)b_t-\sqrt{76-38\omega+(20-15\omega)a+(-24+13\omega+(-33+21\omega)a)b_t}\Big)\\
c_{1tu} &= \tfrac{1}{2}\Big(3+2\omega_1+\omega_1 a_1+(-3+3\omega_1+(2-\omega_1)a_1)b_{1t}-\sqrt{76-38\omega_1+(20-15\omega_1)a_1+(-24+13\omega_1+(-33+21\omega_1)a_1)b_{1t}}\Big)\\
c_{pt} &= \tfrac{1}{2}\Big(3+2\omega+\omega a_p+(-3+3\omega+(2-\omega)a_p)b_{pt}+\sqrt{76-38\omega+(20-15\omega)a_p+(-24+13\omega+(-33+21\omega)a_p)b_{pt}}\Big)\\
c_{1pu} &= \tfrac{1}{2}\Big(3+2\omega_1+\omega_1 a_{1p}+(-3+3\omega_1+(2-\omega_1)a_{1p})b_{1p}-\sqrt{76-38\omega_1+(20-15\omega_1)a_{1p}+(-24+13\omega_1+(-33+21\omega_1)a_{1p})b_{1p}}\Big)\\
c_u &= \tfrac{1}{2}\Big(3+2\omega+\omega a+(-3+3\omega+(2-\omega)a)b-\sqrt{76-38\omega+(20-15\omega)a+(-24+13\omega+(-33+21\omega)a)b}\Big)\\
c_{1u} &= \tfrac{1}{2}\Big(3+2\omega_1+\omega_1 a_1+(-3+3\omega_1+(2-\omega_1)a_1)b_1-\sqrt{76-38\omega_1+(20-15\omega_1)a_1+(-24+13\omega_1+(-33+21\omega_1)a_1)b_1}\Big)\\
c_{pu} &= \tfrac{1}{2}\Big(3+2\omega+\omega a_p+(-3+3\omega+(2-\omega)a_p)b_p-\sqrt{76-38\omega+(20-15\omega)a_p+(-24+13\omega+(-33+21\omega)a_p)b_p}\Big)\\
c_{1pt} &= \tfrac{1}{2}\Big(3+2\omega_1+\omega_1 a_{1p}+(-3+3\omega_1+(2-\omega_1)a_{1p})b_{1pt}+\sqrt{76-38\omega_1+(20-15\omega_1)a_{1p}+(-24+13\omega_1+(-33+21\omega 1)a_{1p})b_{1pt}}\Big)\\
c_t &= \tfrac{1}{2}\Big(3+2\omega+\omega a+(-3+3\omega+(2-\omega)a)b_t+\sqrt{76-38\omega+(20-15\omega)a+(-24+13\omega+(-33+21\omega)a)b_t}\Big)\\
c_{1t} &= \tfrac{1}{2}\Big(3+2\omega_1+\omega_1 a_1+(-3+3\omega_1+(2-\omega_1)a_1)b_{1t}+\sqrt{76-38\omega_1+(20-15\omega_1)a_1+(-24+13\omega_1+(-33+21\omega_1)a_1)b_{1t}}\Big)\\
c_{ptu} &= \tfrac{1}{2}\Big(3+2\omega+\omega a_p+(-3+3\omega+(2-\omega)a_p)b_{pt}-\sqrt{76-38\omega+(20-15\omega)a_p+(-24+13\omega+(-33+21\omega)a_p)b_{pt}}\Big)\\
c_{1p} &= \tfrac{1}{2}\Big(3+2\omega_1+\omega_1 a_{1p}+(-3+3\omega_1+(2-\omega_1)a_{1p})b_{1p}+\sqrt{76-38\omega_1+(20-15\omega_1)a_{1p}+(-24+13\omega_1+(-33+21\omega_1)a_{1p})b_{1p}}\Big)
\end{aligned}
$$

Pour préciser l'action du prolongement de σ, on renvoie à [Cougnard 1992b], où l'on prouve qu'il peut être pris tel que les $\sigma^k(c)$, pour $0 \leq k < 16$, soient les conjugués de c dans l'ordre donné ci-dessus.

On sait que l'extension K_4/L_2 est diédrale de degré 8 ; puisque

$$3 + \omega + \omega a + (-3 + 3\omega + (2 - \omega)a)b$$

est une unité, l'anneau des entiers de L_4 possède une base normale relativement à celui de L_3. Il en est donc de même pour le L_2 conjugué de L_4 et les discriminants de ces deux extensions sont conjugués relativement à L_2 et premiers entre eux. Ceci acquis, on a donc une base normale dans K_4/L_2 que l'on construit comme dans [Cougnard 1992a], soit

$$u = c\sigma^4(c)b,\ \sigma^4(c)\sigma^8(c)b_t,\ \sigma^8(c)\sigma^{12}(c)b,\ \sigma^{12}(c)cb_t,$$
$$c\sigma^{12}(c)b,\ \sigma^4(c)cb_t,\ \sigma^8(c)\sigma^4(c)b,\ \sigma^{12}(c)\sigma^8(c)b_t.$$

On en déduit une base sur $\mathbb{Z}$ de $\mathcal{O}_{K_4}$ obtenue en multipliant successivement les éléments de cette base par $a\omega$, $a_p\omega$, $a\omega_1$, $a_p\omega_1$.

Les renseignements donnés au fur et à mesure, ainsi que la structure du groupe diedral d'ordre 32, permettent de connaître les conjugués de chacun des éléments de la base des entiers de K_4.

Le corps composé de K_4 et M_0 a un groupe de Galois Γ qui est produit semi-direct d'un groupe cyclique distingué d'ordre 16, engendré par un élément que l'on note encore σ (dont le corps des invariants est M_0) et d'un groupe cyclique d'ordre 4 engendré par un élément que l'on note τ (dont le corps des invariants est L_4) et vérifiant la relation $\tau\sigma\tau^{-1} = \sigma^{-1}$; ces notations sont choisies de sorte que le groupe de Galois de $K_4/\mathbb{Q}$ soit le quotient de Γ par le sous-groupe distingué engendré par τ^2 et que les générateurs de $\mathrm{Gal}(K_4/\mathbb{Q})$ soient les restrictions à K_4 de σ et τ. Le corps N formé des éléments de M_4 invariants par $\tau^2\sigma^8$ est une extension de $\mathbb{Q}$ de groupe de Galois quaternionien d'ordre 32.

Puisque $2304 + 48\sqrt{2305}$ est divisible par 4, on a une base normale relative des entiers de M_0 qui consiste des éléments $e = \frac{1}{2}\bigl(1+\sqrt{2305 + 48\sqrt{2305}}\bigr)$ et $\tau^2(e) = e_2 = 1 - e$ dont les autres conjugués sur $\mathbb{Q}$ sont $\tau(e) = e_1 = \frac{1}{2}\bigl(1 + \sqrt{2305 - 48\sqrt{2305}}\bigr)$ et $\tau^3(e) = e_3 = 1 - e_1$.

L'extension quadratique M_0/K_0 étant ramifiée et K_4/K_0 ne l'étant pas, e et e_2 forment une base de l'anneau des entiers de M_4 sur celui de K_4. L'extension M_4/N étant modérément ramifiée, l'anneau des entiers $\mathcal{O}_N$ de N est la trace de celui de M_4 ; l'extension N/K_3 étant modérément ramifiée, le noyau de la trace dans N/K_3 est l'image de $\mathcal{O}_N$ par $1 - \sigma^8$. Ces calculs sont facilités par les remarques précédentes : l'anneau des entiers de K_4 est un module libre sur l'algèbre du groupe H_8 à cœfficients dans l'anneau des entiers de L_2 ; par restriction, c'est un module libre de rang 4 sur l'algèbre du groupe de Galois de K_4/K_3 à cœfficients dans les entiers de L_2 et on en déduit une base de la précédente. Avec cette base et les éléments e et e_2 on construit une base de l'anneau des entiers de M_4 relativement à l'anneau des entiers de L_2 sur laquelle on connaît l'action du groupe de Galois de M_4/K_3. On en déduit que les nombres suivants :

$$e u + \tau^2(e)\sigma^8(u) - e\sigma^8(u) - \tau^2(e)u,$$
$$e\sigma^4(u) + \tau^2(e)\sigma^{12}(u) - e\sigma^{12}(u) - \tau^2(e)\sigma^4(u),$$
$$e\tau(u) + \tau^2(e)\sigma^8\tau(u) - e\sigma^8\tau(u) - \tau^2(e)\tau(u),$$
$$e\sigma^4\tau(u) + \tau^2(e)\sigma^{12}\tau(u) - e\sigma^{12}\tau(u) - \tau^2(e)\sigma^4\tau(u)$$

forment une base du noyau de la trace dans N/K_3, restreinte aux entiers de L_2. On en déduit une $\mathbb{Z}$-base en multipliant chacun de ces éléments successivement par $a\omega$, $a_p\omega$, $a\omega_1$, $a_p\omega_1$.

Pour les calculs numériques, on utilise le plongement géométrique du corps au moyen des $\mathbb{Q}$-isomorphismes de N dans $\mathbb{R}$ (le corps est totalement réel) ; on prend dans l'ordre les σ^i puis les $\sigma^i\tau$ $(0 \leq i \leq 15)$, chaque élément de N étant identifié à son image, laquelle est représentée par un vecteur colonne. On a donné au fur et à mesure les indications permettant de calculer les conjugués de chacun des nombres algébriques. (Le détail des calculs peut être demandé par courrier à l'auteur.)

$$
\begin{pmatrix}
375 & 105 & -1075 & -457 & 580 & 1118 & -279 & -456 & 700 & -654 & -289 & 252 & -222 & 981 & 294 & 961 \\
180 & 3 & -550 & -217 & 284 & 544 & -129 & -269 & 403 & -311 & -173 & 157 & -93 & 530 & 155 & 486 \\
83 & -51 & -558 & -213 & 239 & 417 & 100 & -465 & 496 & -74 & -374 & 243 & 51 & 578 & 153 & 445 \\
29 & -154 & -329 & -83 & 111 & 190 & 70 & -347 & 398 & -8 & -264 & 205 & 68 & 406 & 102 & 253 \\
-71 & -349 & -243 & -495 & 700 & 33 & -551 & -101 & 277 & -516 & -618 & 618 & -2116 & -1770 & -1033 & -856 \\
-100 & -243 & -109 & -266 & 326 & -45 & -230 & -145 & 193 & -235 & -366 & 333 & -1036 & -914 & -503 & -375 \\
-319 & -422 & -76 & -319 & 289 & -118 & -31 & -407 & 264 & -162 & -366 & 345 & -735 & -875 & -414 & -166 \\
-328 & -395 & -13 & -218 & 96 & -218 & 92 & -452 & 282 & -29 & -344 & 246 & -344 & -542 & -187 & 41 \\
323 & 17 & -637 & -542 & 849 & 570 & -765 & 70 & 342 & -764 & -561 & 541 & -2111 & -1132 & -822 & -544 \\
208 & 105 & -319 & -262 & 434 & 327 & -389 & 117 & 96 & -376 & -238 & 230 & -1045 & -543 & -412 & -306 \\
368 & 367 & -256 & -130 & 296 & 310 & -378 & 343 & -61 & -261 & -166 & 82 & -870 & -304 & -297 & -342 \\
310 & 433 & -138 & -49 & 184 & 275 & -219 & 385 & -221 & -129 & 20 & -56 & -445 & -114 & -167 & -269 \\
-343 & -201 & 753 & 212 & -211 & -938 & 173 & 258 & -430 & 526 & -123 & 95 & -526 & -1384 & -657 & -1217 \\
-145 & -95 & 345 & 115 & -83 & -419 & 82 & 139 & -208 & 258 & -42 & 57 & -241 & -626 & -326 & -616 \\
-126 & -34 & 122 & 40 & 8 & -232 & 249 & -52 & -80 & 345 & -177 & 126 & -52 & -309 & -246 & -463 \\
0 & -8 & -10 & 46 & 59 & -1 & 113 & 3 & -26 & 168 & -40 & 89 & 24 & -\;8 & -126 & -271
\end{pmatrix}
$$

TABLEAU 1. Matrice de changement de base obtenue par l'algorithme LLL.

Lors des calculs préliminaires on s'est aperçu, tout comme dans [Cougnard 1992a; 1992b], que cette base "naturelle" n'était pas forcément la plus adaptée. On utilise donc la structure euclidienne associée au noyau de la trace dans une extension quadratique totallement réelle : si x et y sont deux éléments du noyau de la trace de N/K_3, le produit xy est un entier de K_3 et l'application

$$x \mapsto \mathrm{Tr}_{K_3/\mathbb{Q}}(x^2)$$

définit sur le noyau de la trace une structure euclidienne [Martinet 1971]. On utilise alors l'algorithme LLL pour en donner une base aussi proche que possible d'une base orthonormée. La matrice de changement de base est donnée sur le Tableau 1.

Soit v le dernier vecteur de cette base ; on construit le $\mathbb{Z}[H_{32}]$-module engendré par v et ses conjugués. Comme $v \in \ker \mathrm{Tr}_{N/K_3}$, il suffit de prendre les images par σ^i et par $\sigma^i\tau$ $(0 \leq i \leq 7)$. On vérifie que ces nombres sont linéairement indépendants sur $\mathbb{Z}$. C'est donc, avec les notations du § 2, un $\mathcal{O}$-module libre, donc $\mathcal{O}$-isomorphe à $\mathcal{O}$ comme $\mathcal{O}$-module à gauche. L'isomorphisme se prolonge en un $\mathbb{H}$-isomorphisme de $\mathbb{H}$-espace vectoriel à gauche de dimension 1 entre le noyau de la trace de N sur K_3 et $\mathbb{H}$. On connaît une $\mathbb{Z}$-base de Λ, ce qui permet de construire Λv.

La restriction de l'isomorphisme au noyau de $\mathrm{Tr}_{N/K_3}(\mathcal{O}_N)$ l'identifie à un $\mathcal{O}$-idéal à gauche fractionnaire $\mathcal{J}$ et on en connaît une base. Comme annoncé dans le § 1, on étend ce $\mathcal{O}$-module à l'ordre maximal Λ ; pour cela, on considère les vecteurs de bases de $\mathcal{J}$ et leurs produits par β et par $\alpha\beta$, ce qui donne 48 générateurs à l'aide desquels on construit une $\mathbb{Z}$-base. Pour n'utiliser que des cœfficients entiers, on préfère étudier $\mathcal{J}' = 2\Lambda\mathcal{J}$. L'invariant relatif de $\mathcal{J}'$ et de Λ est une puissance de 2. On compare 2Λ et $\Lambda\mathcal{J}'(\zeta + \zeta^{-1})$; on constate que ces deux réseaux sont identiques. C'est donc que l'on a un isomorphisme $\Lambda(2/\theta) \sim \Lambda\mathcal{J}'$, et le Λ-module $\Lambda\mathcal{J}'$ est donc libre. On vérifie alors que $2\theta^{-1}$ n'est pas dans l'image de $\mathcal{J}'$.

BIBLIOGRAPHIE

[Cougnard 1992a] J. Cougnard, "Bases normales pour des extensions diédrales de degré 8", prépublication du Séminaire de théorie des nombres de Caen 1992–93.

[Cougnard 1992b] J. Cougnard, "Base normale dans un corps de classes de Hilbert", publications mathématiques de la faculté des sciences de Besançon 1992–93 (Besançon, F 25030 Cedex, France).

[Damey et Martinet 1973] P. Damey et J. Martinet, "Plongement d'une extension quadratique dans une extension quaternionienne", *J. reine angew. Math.* **262** (1973), 323–338.

[Fröhlich 1983] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Ergebnisse der Math. (3. Folge) **1**, Springer, Berlin, 1983.

[Fröhlich 1980] A. Fröhlich, "Galois module structure and rootnumbers for quaternion extensions of degree 2^n", *J. Number Theory* **12** (1980), 499–518.

[Martinet 1971] J. Martinet, "Modules sur l'algèbre de groupe quaternionien", *Ann. Sci. Ec. Norm. Sup. Paris* (4e série) **4** (1971), 399–408.

[Oriat 1987] B. Oriat, "Groupes des Classes des Corps Quadratiques Réels $\mathbb{Q}(\sqrt{d})$, $d < 10000$", publications mathématiques de la faculté des sciences de Besançon **2** 1986–87 (Besançon, F 25030 Cedex, France).

[Batut et al. 1992] C. Batut, D. Bernardi, H. Cohen et M. Olivier, *User's Guide to PARI-GP* (version 1.37.2). Ce manuel fait partie de la distribution du programme, qui peut être obtenu par ftp sur le serveur pari@ceremab.u-bordeaux.fr.

[Serre 1967] J.-P. Serre, *Corps Locaux*, seconde édition, Hermann, Paris, 1967.

[Serre 1971] J.-P. Serre, *Représentations linéaires des groupes finis*, seconde édition, Hermann, Paris, 1971.

[Swan 1962] R. G. Swan, "Projective modules over group rings and maximal orders", *Ann. Math.* **76** (1962), 55–61.

[Swan 1981] R. G. Swan, "Projective modules over binary polyhedral groups", *J. reine angew. Math.* **342** (1981), 66–172.

[Taylor 1981] M. J. Taylor, "On Fröhlich's conjecture for rings of integers of tame extensions", *Inv. Math.* **63** (1981), 41–79.

[Vigneras 1972] M. F. Vigneras, "Corps de quaternions sur un corps de nombres algébriques", Thèse de troisième cycle, Université de Bordeaux I, 1972.

[Vigneras 1975] M. F. Vigneras, "Simplification pour les ordres des corps de quaternions totalement définis", *J. reine angew. Math.*, **286** (1975), 257–277.

Jean Cougnard, Section Mathématiques et Mécanique, Équipe A3, Université de Caen, Esplanade de la Paix, 14032 Caen Cedex (cougnard@univ-caen.fr)

Received February 14, 1994; accepted August 13