JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

JEAN COUGNARD
MICHEL VERANT

Monogénéité de l'anneau des entiers de corps de classes de rayon de corps quadratiques

Journal de Théorie des Nombres de Bordeaux, tome 4, n° 1 (1992), p. 53-74

<http://www.numdam.org/item?id=JTNB_1992__4_1_53_0>

Séminaire de Théorie des Nombres,
Bordeaux 4 (1992), 53-74

Monogénéité de l'anneau des entiers de corps de classes de rayon de corps quadratiques.

par JEAN COUGNARD ET MICHEL VERANT

1. Introduction et notations.

L'anneau des entiers d'un corps de nombres F est noté O_F. Si N est une extension finie d'un corps de nombres k, on dit que O_N est O_k-monogène s'il existe un élément θ de O_N tel que $O_N = O_k[\theta]$.

En 1986, M. N. Gras montre que pour un nombre premier $p \geq 5$, l'anneau des entiers d'une extension galoisienne N de Q de degré p est monogène si et seulement si $l = 2p+1$ est premier et N est le sous-corps réel maximal du corps cyclotomique engendré par les racines de l'unité d'ordre l ([Gmn]). En 1988, J. Cougnard montre une condition nécessaire de monogénéité pour les extensions cycliques de degré premier $l \geq 5$ d'un corps quadratique imaginaire ([C1]). Par ailleurs en 1987, Ph. Cassou-Noguès et M. J. Taylor ont démontré que les anneaux d'entiers de $k^{(4\mathfrak{f})}$ et de $k^{(4)}k^{(\mathfrak{f})}$ sont $O_{k^{(4)}}$-monogènes, lorsque k est un corps quadratique imaginaire dans lequel 2 est décomposé et $\mathfrak{f}$ un idéal de O_k premier à 2 ([CN-T1]), où pour un idéal $\mathfrak{l}$ de O_k la notation $k^{(\mathfrak{l})}$ désigne le corps de classes de k de rayon $\mathfrak{l}$. Des résultats analogues ont été obtenus par Ph. Cassou-Noguès et M. J. Taylor, J. Cougnard, V. Fleckinger, R. Schertz, A. Srivastav et S. Venkataraman ([CN-T2], [CN-T3], [C2], [C-F1], [F], [Sc1], [Sc2], [S-V]).

Supposons que k soit un corps quadratique imaginaire, ces résultats conduisaient alors à conjecturer que si H_k est le corps de classes de Hilbert de k et $\mathfrak{f}$ un idéal de O_k, alors l'anneau des entiers de $k^{(\mathfrak{f})}$, est monogène sur celui de H_k sans restriction sur le conducteur.

Un contre-exemple à la conjecture annoncée a été mis en évidence par J. Cougnard et V. Fleckinger ([C-F2]) : ils ont montré, en s'inspirant d'une remarque de M. N. Gras et en utilisant la méthode de Baker, que le corps de classes de $k = \mathbf{Q}(\sqrt{-19})$ de rayon un diviseur premier de 7 dans k a un anneau des entiers non monogène sur celui de k.

Manuscrit reçu le 22 mai 1991.

Il nous a alors paru utile de regarder si des propriétés analogues étaient valables dans le cas d'un corps de base quadratique réel k. L'absence de générateur analytique des corps de classes N de k, l'inexistence d'une construction d'unités canoniques de N (à la manière des unités cyclotomiques ou elliptiques, mises à part celles de H. Stark ([St]), sont autant de raisons qui nous ont conduits à une étude expérimentale sur des corps de petit degré. Pour des raisons de facilité de construction, nous n'avons envisagé que le cas des extensions cycliques d'un corps de nombres k, de degré relatif 4, une seule place, première à 2, étant ramifiée. Nous avons donné des *conditions de monogénéité* pour ce type d'extensions en termes d'unités; la relation obtenue est du type $\epsilon_1 + \epsilon_2 = 1$ qui se ramène aux méthodes théoriquement effectives de A. Baker ([Ba] et [E]). Il faut remarquer que ces méthodes doivent être améliorées avec les récents résultats de M. Waldschmidt ([Wal]).

Suivant une suggestion de R. Schertz, nous en avons profité pour étudier un deuxième *contre-exemple* à la conjecture avec le corps de classes N de $k = \mathbf{Q}(\sqrt{-19})$ de rayon 3 dont tout portait à croire (i.e. des tentatives numériques infructueuses) que son anneau des entiers O_N n'était pas O_k-monogène.

Cet article est issu de la thèse soutenue à Besançon le 11 novembre 1990 ([V]).

Tout au long de ce travail, nous utilisons les notations suivantes:

Soit G un groupe et H un sous-groupe de G,

$(G : H)$ désigne l'indice de H dans G.

Soit L un corps de nombres,

O_L désigne son anneau des entiers,

U_L désigne le groupe des unités de O_L,

h_L désigne le nombre de classes de L.

Soient K/k une extension finie de k et $\alpha \in K$, on désigne par :

$k(\alpha)$, le corps engendré par k et α,

$O_k[\alpha]$, l'anneau engendré par O_k et α (si $\alpha \in O_K$),

$[K : k]$, le degré relatif de K/k,

$T_{K/k}(\alpha)$, la trace de α de K sur k,

$N_{K/k}(\alpha)$, la norme de α de K sur k,

$T_K(\alpha)$, la trace de α de K sur $\mathbf{Q}$,

$N_K(\alpha)$, la norme de α de K sur $\mathbf{Q}$,

$Irr(\alpha, k)(X)$, le polynôme irréductible de α sur k,

$d_{K/k}(\alpha)$, le discriminant du polynôme irréductible de α sur k,

$d_{K/k}$, l'idéal discriminant de K/k,

d_K, l'idéal discriminant de $K/\mathbf{Q}$,

Pour tout plongement de K dans $\mathbf{C}$, l'image de α par σ est notée $\sigma(\alpha)$ ou α^σ et si K/k est galoisienne, Gal(K/k) désigne son groupe de Galois.

CONDITIONS DE MONOGÉNÉITÉ

2. Diviseur commun inessentiel du discriminant

Soient E un corps de nombres et L une extension finie de E. Soit θ un élément entier de L et primitif pour L/E. La norme $N_E(\mathfrak{I})$ d'un idéal $\mathfrak{I}$ de E est le nombre $card(O_E/\mathfrak{I})$. L'idéal engendré par $d_{L/E}(\theta)$ est de la forme $\mathfrak{I}(\theta)^2 d_{L/E}$ et $\mathfrak{I}(\theta)$ est appelé l'indice de θ pour L/E. S'il existe un diviseur premier $\mathfrak{P}$ de $\mathfrak{I}(\theta)$ pour tous les éléments entiers et primitifs θ de L/E, on dit que $\mathfrak{P}$ est un diviseur commun inessentiel du discriminant $d_{L/E}$.

Depuis Dedekind, on sait qu'il peut y en avoir et Hasse a donné un critère que nous allons rappeler. Il nous permet de prendre en défaut la conjecture précédente pour les corps quadratiques réels.

THEORÈME. ([H], ch. 25, §6) *Soient E un corps de nombres et L une extension finie de E. Un diviseur premier $\mathfrak{p}$ de E n'est pas un diviseur commun inessentiel du discriminant de L/E si et seulement si pour tout entier naturel f, le nombre $r(f)$ de diviseurs premiers $\mathfrak{P}$ de $\mathfrak{p}$ dans L de degré relatif f vérifie l'inégalité :*

$$r(f) \leq (1/f) \sum_{d|f} \mu(f/d) N_E(\mathfrak{p})^d,$$

où μ désigne la fonction de Möbius ([La1], Ch.VIII, §3).

Exemple 1. Dans $k = \mathbf{Q}(\sqrt{2})$, on a $113 = N_k(\pi)$ avec $\pi = 11 + 2\omega$ et $\omega = \sqrt{2}$. Notons $\mathfrak{m}$ le module de k de partie finie $\mathfrak{p} = (\pi)$ et de partie infinie $\mathfrak{m}_\infty = \infty_1\infty_2$. Les corps de classes $N = k^{(\mathfrak{m})}$ et $K = k^{(\mathfrak{p})}$ sont respectivement de degrés relatifs 4 et 2 sur k. L'unité fondamentale $\varepsilon = 1 + \omega$ de k étant de norme -1, $k^{(\mathfrak{m}_\infty)}$ est égal à k et K étant le seul corps intermédiaire de $k^{(\mathfrak{m})}/k$, l'extension N/k est cyclique. Le corps K

est engendré par une racine u du polynôme $P(X) = X^2 - (1+\omega)X - 2$ et on a $O_K = O_k[u]$ car $P(X)$ a pour discriminant $11 + 2\omega$. Le polynôme $\overline{P}(X) = X^2 - X = X(X-1)$ est le polynôme réduit de $P(X)$ modulo (ω). L'idéal (ω) se décompose donc dans K ([La2], ch. I, §8, prop. 25). D'après le théorème, ω est un diviseur commun inessentiel du discriminant $d_{N/k}$ de N/k.

Exemple 2. Dans $k = \mathbf{Q}(\sqrt{19})$, on a : $17 = N_k(\pi)$ avec $\pi = 279 + 64\omega$ et $\omega = \sqrt{19}$. Notons $\mathfrak{p}$ l'idéal de O_k engendré par π. Le corps de classes $k^{(\mathfrak{p})}$ de k est de degré relatif 4 sur k. Soit $K = k(u)$ avec pour u une racine du polynôme $P(X) = X^2 - \omega X - 65 - 16\omega$. Le polynôme irréductible de u sur k est $P(X)$. Montrons que K est incluse dans $k(\mathfrak{p})$.

Le discriminant de $P(X)$ est π. L'extension K est réelle car $\pi > 0$. Notons τ un prolongement à K d'un générateur de $Gal(k/\mathbf{Q})$. Le polynôme irréductible de $\tau(u)$ sur k est $X^2 + \omega X - 65 + 16\omega$; son discriminant est aussi positif. K est donc totalement réelle. Par conséquent, K est incluse dans $k(\mathfrak{p})$. De plus on a $O_K = O_k[u]$.

Notons : $\theta = 1 + u + \omega$, $\xi = -18 + 9u + 5\omega - 2u\omega$ et $\alpha = 9 + 2\omega$. Alors on a : $N_{K/k}(\xi) = -1$ et $\theta^2 - 4\alpha = \xi\sqrt{\pi}$. Soit N le corps engendré par une racine v de $X^2 + \theta X + \alpha$.

Montrons que $N = k^{(\mathfrak{p})}$. L'extension N/k est cyclique de degré relatif 4 et $d_{N/k} = \mathfrak{p}^3$. Notons $Q(X) = Irr(v,k)(X)$. Par le calcul, on obtient

$$Q(X) = X^4 + (2+\omega)X^3 - (46 + 11\omega)X^2 + (56 + 13\omega)X + 157 + 36\omega.$$

On vérifie que $Q(X)$ ainsi que son conjugué par τ ont toutes leurs racines réelles. Par conséquent on a $N = k^{(\mathfrak{p})}$. Le calcul du discriminant de $Q(X)$ donne $(9 + 2\omega)^2\pi^3$. D'après le théorème de Hasse, l'entier $9 + 2\omega$, qui est un diviseur de 5 dans O_k, n'est pas un diviseur commun inessentiel du discriminant $d_{N/k}$ de N/k et il ne peut y en avoir d'autres d'après ce qui précède. On va voir dans le §5 que pourtant O_N n'est pas O_k-monogène.

3. Résultats préliminaires.

PROPOSITION 1. *Soit K/k une extension quadratique de corps de nombres, O_k étant principal. Alors O_K est O_k-monogène.*

Démonstration. O_K est un O_k-module libre de rang 2 ([Sa], 2.7, cor. th. 1). Considérons la suite exacte :

$$0 \longrightarrow O_k \longrightarrow O_K \longrightarrow O_K/O_k \longrightarrow 0$$

Le quotient O_K/O_k est un O_k-module. Montrons qu'il est sans torsion, en raisonnant par l'absurde. Supposons qu'il existe : $a \in O_k$ et $x \in O_K - O_k$ tels que $ax \in O_k$. Alors $x = \frac{1}{a}ax$ appartient à $k \cap O_K = O_k$, ce qui est contradictoire; puisque O_k est principal, O_K/O_k étant sans torsion est libre ([La1], ch. XV, th. 2). Il existe donc H sous O_k-module libre de O_K tel que : $O_K = O_k \oplus H$ ([La1], ch. XV, lemme 1). D'où le résultat.

Hypothèses (H_1).

Soient k un corps de nombres, K/k une extension quadratique qui se plonge dans une extension cyclique N/k de degré relatif 4, et σ un générateur de Gal(N/k). On suppose qu'un seul idéal premier p de k est ramifié dans N et qu'il est totalement ramifié et premier à 2 : $\mathfrak{p}$ et $\mathfrak{P}$ sont définis par $pO_K = \mathfrak{p}^2$ et $\mathfrak{p}O_N = \mathfrak{P}^2$.

PROPOSITION 2. *Si h_k est impair et si aucune place infinie de k ne se ramifie dans N, alors h_N est impair, et si p est principal, les idéaux $\mathfrak{P}$ et $\mathfrak{p}$ sont principaux.*

Démonstration : Supposons que h_k est impair et qu'aucune place infinie de k ne se ramifie dans N. Rappelons la formule des classes ambiges ([G], prop. III-1) : le nombre de classes ambiges dans N/k est égal à

$$\frac{h_k\left(\prod e\right)}{[N:k]\left(U_k : U_k \cap N_{K/k}(N^*)\right)},$$

où $\left(\prod e\right)$ est le produit des indices de ramifications dans N des places de k.

Ce nombre est ici impair puisque $\prod e = [N : k] = 4$; donc le groupe des classes ambiges est d'ordre impair, comme le groupe de Galois est un 2-groupe les théorèmes de Sylow ([La1], ch. I, §6, théorème 2) montrent que h_N est impair.

On a $\sigma(\mathfrak{P}) = \mathfrak{P}$ ([Sa], ch. VI, prop. 1), donc la classe de $\mathfrak{P}$ est ambige. Puisque $\mathfrak{P}^4 = pO_N$, l'ordre de la classe de $\mathfrak{P}$ divise quatre. La classe de $\mathfrak{P}$ appartient au 2-groupe des classes ambiges qui est trivial et par suite $\mathfrak{P}$ est principal.

Rappelons le résultat bien connu ([Se], ch. III) :

PROPOSITION 3. *Sous l'hypothèse (H_1), $T_{N/k}(O_N)$ est égal à O_k.*

4. Conditions nécessaires et suffisantes de monogénéité

Hypothèses (H_2).

Supposons qu'il existe $v \in N$ tel que $O_N = O_K[v]$.

Ce sera le cas si K est principal d'après la proposition 1. Posons $x = \sigma^2(v) - v$ et $\rho = x^\sigma/x$. L'idéal $\mathfrak{P}$ est principal, engendré par x (cf. prop. 2), on a alors le résultat suivant :

THÉORÈME. *Sous les hypothèses* (H_1) *et* (H_2), O_N *est* O_k*-monogène si et seulement s'il existe* $\mu \in U_K$ *et* $\varepsilon \in U_N$ *telles que :* $\mu = \rho\varepsilon^\sigma + \varepsilon$.

Démonstration :

1) Supposons qu'il existe $\theta \in N$ tel que $O_N = O_k[\theta]$. L'idéal $\mathfrak{P}$ est donc engendré par $\sigma(\theta) - \theta$. Puisque θ engendre aussi O_N comme O_K-algèbre, $\mathfrak{P}$ est engendré par $\sigma^2(\theta) - \theta$. Il existe donc $\mu \in U_K$, $\varepsilon \in U_N$ telles que :

$$\sigma^2(\theta) - \theta = \mu x \quad \text{et} \quad \sigma(\theta) - \theta = \varepsilon x. \tag{1}$$

De façon élémentaire, on a :

$$\frac{\sigma^2(\theta) - \theta}{\sigma(\theta) - \theta} = \frac{(\sigma(\theta) - \theta)^\sigma}{\sigma(\theta) - \theta} + 1,$$

c'est-à-dire d'après (1) :

$$\mu = \rho\varepsilon^\sigma + \varepsilon. \tag{2}$$

2) Supposons qu'il existe $\mu \in U_K$ et $\varepsilon \in U_N$ telles que (2) soit vérifiée. La définition de x et (2) permettent d'écrire :

$$\sigma^2(x) = -x \quad \text{et} \quad \mu x = (\varepsilon x)^\sigma + \varepsilon x.$$

On en déduit :

$$T_{N/k}(\varepsilon x) = T_{N/K}(\mu x) = \mu T_{N/K}(x) = 0.$$

D'après la proposition 3, il existe $\theta_1 \in O_N$ tel que $T_{N/k}(\theta_1) \in U_k$. Posons $x_1 = \varepsilon x$ et

$$\theta = [x_1\sigma(\theta_1) + (x_1 + \sigma(x_1))\sigma^2(\theta_1) + (x_1 + \sigma(x_1) + \sigma^2(x_1))\sigma^3(\theta_1)]/T_{N/k}(\theta_1),$$

([La1], ch. VIII, §6, th. 90 de Hilbert). On a alors :

$$\theta - \sigma(\theta) = x_1 = \varepsilon x, \tag{3}$$

$$\theta - \sigma^2(\theta) = \theta - \sigma(\theta) + \sigma(\theta - \sigma(\theta)) = (\varepsilon x)^\sigma + \varepsilon x = \mu x, \tag{4}$$

$$\theta - \sigma^3(\theta) = -\sigma^3(\theta - \sigma(\theta))$$

$\mathfrak{P}$ étant ambige, $\theta - \sigma^3(\theta)$ est associé à x (générateur de $\mathfrak{P}$).

Utilisons la formule d'Euler :

$$d_{N/k}(\theta) = N_{N/k}((\theta - \sigma(\theta))(\theta - \sigma^2(\theta))(\theta - \sigma^3(\theta)))$$

p^3 est donc engendré par $d_{N/k}(\theta)$. D'après la formule de Hasse sur les discriminants ([Se], ch. VI, §3), p^3 est égal à $d_{N/k}$; O_N est donc O_k-monogène.

COROLLAIRE. *Si O_N est O_k-monogène, alors il existe $\varepsilon \in U_N$ et $t \in O_k - \{0\}$ tels que $1 + 4N_{N/k}(\varepsilon) = t^2\ N_{N/k}(x)$ avec x défini dans les hypothèses (H_2).*

Démonstration : D'après le théorème, il existe $\mu \in U_K$ et $\varepsilon \in U_N$ telles que : $\mu = \rho\varepsilon^\sigma + \varepsilon$. Reprenons le générateur θ de O_N sur O_k défini dans la deuxième partie de la démonstration du théorème, θ et x vérifient d'après les formules (3) et (4) : $\theta - \sigma(\theta) = \varepsilon x$ et $\theta - \sigma^2(\theta) = \mu x$.

Notons :

$$y_1 = \theta\sigma(\theta) + \sigma^2(\theta)\sigma^3(\theta),$$
$$y_2 = \theta\sigma^2(\theta) + \sigma(\theta)\sigma^3(\theta),$$
$$y_3 = \theta\sigma^3(\theta) + \sigma(\theta)\sigma^2(\theta).$$

On a alors :

$$y_1 = \sigma^2(y_1) \text{ (donc } y_1 \in O_K), \quad y_2 = \sigma(y_2) \text{ (donc } y_2 \in O_k), \quad y_3 = \sigma(y_1),$$

$$y_1 - y_3 = (\theta - \sigma^2(\theta))\sigma(\theta - \sigma^2(\theta)) = N_{K/k}(\mu)x\sigma(x), \tag{1}$$

$$y_3 - y_2 = -(\theta - \sigma(\theta))\sigma^2(\theta - \sigma(\theta)) = -N_{N/K}(\varepsilon x).$$

On en déduit :

$$(y_2 - y_1)(y_2 - y_3) = N_{K/k}(y_3 - y_2) = N_{N/k}(\varepsilon)N_{N/k}(x), \tag{2}$$

$$2y_2 - y_1 - y_3 = T_{K/k}(N_{N/K}(\varepsilon x)). \tag{3}$$

De façon élémentaire, on vérifie l'égalité :

$$4(y_2 - y_1)(y_2 - y_3) = (2y_2 - y_1 - y_3)^2 - (y_1 - y_3)^2.$$

En utilisant (1), (2) et (3), on obtient :

$$4N_{N/k}(\varepsilon)N_{N/k}(x) = T_{K/k}(N_{N/K}(\varepsilon x))^2 - N_{K/k}(\mu)^2(x\sigma(x))^2. \tag{4}$$

De plus on a :

$$N_{N/k}(x) = (x\sigma(x))^2 \text{ et } T_{K/k}(N_{N/K}(\varepsilon x)) \in p.$$

Puisque $N_{N/k}(x)$ engendre p, la relation (4) permet de conclure.

5. Exemples d'application.

Exemple. Reprenons l'exemple 2. Montrons que O_N n'est pas O_k-monogène en raisonnant par l'absurde. Supposons que O_N/O_k est monogène. Il existe $Y \in O_k$ tel que $\pi Y^2 - 1$ soit associé à 4 dans O_k. L'unité fondamentale ε de k est $170 + 39\omega$. Notons $\mathfrak{q}$ l'idéal de O_k engendré par ω. Modulo $\mathfrak{q}$, on a donc les congruences suivantes :

$\varepsilon \equiv -1$, $\pi \equiv 3$, $13 \times 3 \equiv 1$, $13Y^2 \equiv 5$ ou -3, $Y^2 \equiv 15$ ou 10.

Soient $a, b \in \mathbf{Z}$ tels que $Y = a + b\omega$. On a : $Y^2 \equiv a^2$ modulo $\mathfrak{q}$, $\mathfrak{q} \cap \mathbf{Z} = 19\mathbf{Z}$ et, 15 et 10 ne sont pas des carrés modulo 19. On aboutit à une contradiction.

PROPOSITION 4. *Soient k un corps de nombres principal, π un élément irréductible de k, $\omega = \sqrt{\pi}$, $K = k(\omega)$, σ le générateur de $Gal(K/k)$. Supposons qu'il existe $\xi \in U_K$, $\theta \in O_K$ tels que :*

$$\xi + \sigma(\xi) \in U_k, \quad \xi\sigma(\xi) = -1, \quad \text{et} \quad \theta^2 \equiv \xi\omega \ \text{modulo } 4.$$

Alors $N = K(\sqrt{\xi\omega})$, est une extension cyclique de k de degré relatif 4 dont l'anneau des entiers est O_k-monogène.

Démonstration : On peut vérifier que N/k est cyclique de degré relatif 4, que l'idéal p de O_k engendré par π est le seul idéal qui se ramifie dans N et qu'il est totalement ramifié. L'unique relèvement de p dans N est l'idéal $\mathfrak{P}$ engendré par $x = \sqrt{\xi\omega}$.

Une racine v du polynôme $X^2 + \theta X + (\theta^2 - x^2)/4$ est un générateur de O_N sur O_K. Notons encore σ un prolongement de σ à N. Quitte à considérer l'opposé de θ au lieu de θ, on peut supposer que: $\sigma^2(v) - v = x$. Posons $\rho = \sigma(x)/x$. Les hypothèses entraînent :

$$\rho = \pm\sigma(\xi) \text{ et } N_{K/k}(\rho + 1) = \pm(\xi + \sigma(\xi)).$$

D'où le résultat d'après le théorème (avec $\varepsilon = 1$).

Remarque : Regardons le cas où le conducteur est de la forme $\zeta^2 + 4$ avec $\zeta \in U_k$ et faisons les hypothèses suivantes :

Soient n un entier naturel sans facteurs carrés,

m le reste modulo 4 de $(n-1)/4$ si $n \equiv 1$ modulo 4,

$k = \mathbf{Q}(\sqrt{n})$,

$\omega = (1 + \sqrt{n})/2$ si $n \equiv 1$ modulo 4 et $\omega = \sqrt{n}$ sinon,

ε l'unité fondamentale de k,

a un entier tel que $\pi = \varepsilon^{2a} + 4$ soit irréductible,

u la racine positive du polynôme $X^2 - \varepsilon^a X - 1$,

$K = k(u)$.

Une base de l'anneau des entiers de K est $\{1, u, w, uw\}$. On suppose que pour l'une des unités ζ suivantes $\pm u$, $\pm\varepsilon u$, il existe un entier θ de K tel que : $\theta^2 - \zeta\sqrt{\pi} \equiv 0$ modulo 4; des essais montrent que l'existence de θ est assurée dans la majeure partie des cas (voir table numérique dans [V] p. 136-140).

Sous ces hypothèses, le corps N engendré par une racine carrée de $\zeta\sqrt{\pi}$ est cyclique de degré relatif 4 sur k. De plus, N est inclus dans un corps de classes dont la partie finie du rayon est l'idéal (π) et dont on peut facilement préciser la partie infinie en fonction du signe de la norme sur $\mathbf{Q}$ de ε. D'après la proposition, on sait que O_N est O_k-monogène.

PROPOSITION .5. *Soit $k = \mathbf{Q}(\sqrt{n})$, n étant un entier naturel sans facteurs carrés tel que $n \equiv 3$ ou 7 modulo 20. Alors le compositum N de $\mathbf{Q}(\cos(\pi/10))$ et de k est cyclique sur k de degré relatif 4, inclus dans $k^{(5)}$, et son anneau des entiers O_N est O_k-monogène.*

Démonstration : Les symboles de Legendre $\left(\frac{2}{5}\right)$, $\left(\frac{3}{5}\right)$ sont égaux à -1, par suite 5 est inerte dans k ([Sa], ch. V). Notons : $K = k(\sqrt{5})$, $u =$

$\frac{-1+\sqrt{5}}{2}$, $\theta = \sqrt{n}$, $\xi = -1+2u = \sqrt{5}-2$ et x la racine carrée de $\xi\sqrt{5}$. Les corps $\mathbf{Q}(\cos(\pi/10))$ et $\mathbf{Q}(\sqrt{5})$ ayant respectivement pour conducteurs 20 et 5, $\mathbf{Q}(\sqrt{5})$ est inclus dans $\mathbf{Q}(\cos(\pi/10))$, d'où K est inclus dans N. On a alors : $\theta^2 - \xi\sqrt{5} = n+4u-3 \equiv 0$ modulo 4. Soit v une racine du polynôme $X^2 + \theta X + (\theta^2 - x^2)/4$ On vérifie facilement que : $x(u+1)^2 = 2\cos(\pi/10)$, d'où on déduit que N est égal à $k(v)$. Il est facile de voir que N/k est cyclique de degré relatif 4 et que l'idéal p de O_k engendré par 5 est le seul qui se ramifie dans N et qu'il est totalement ramifié. Les conjugués de x étant tous réels, N est totalement réel et est par conséquent inclus dans $k^{(5)}$. Soit σ un générateur de $Gal(K/k)$. Quitte à considérer l'opposé de θ au lieu de θ, on peut supposer que :

$$\sigma^2(v) - v = x.$$

On a alors : $\rho = \pm\sigma(\xi)$. Quitte à considérer σ^3 au lieu de σ, on peut supposer que : $\rho = \sigma(\xi)$. Considérons l'unité de O_K : $\varepsilon = u\sigma(\xi)$, on a : $\rho\varepsilon^\sigma + \varepsilon = -1$, d'où la monogénéité de O_N sur O_k d'après le théorème.

Remarque : D'après le théorème de Dirichlet ([H], ch. 5, §7), le nombre des entiers naturels premiers vérifiant les conditions de la proposition 5 n'est pas fini. On a ainsi une famille infinie non obtenue par extension des scalaires par un corps de discriminant premier à celui de $\mathbf{Q}(\cos(\pi/10))$ et pour laquelle il n'y a pas de monogénéité.

CONTRE-EXEMPLE

6. Construction de $N = k^{(3)}$ corps de classes de rayon 3 du corps $k = \mathbf{Q}(\sqrt{-19})$ et détermination de ses unités.

Notons :

$$\omega = \frac{1+\sqrt{-19}}{2},\ \omega_0 = \frac{1+\sqrt{-3}}{2},\ \omega_1 = \frac{1+\sqrt{57}}{2},$$

$k = \mathbf{Q}(\sqrt{-19})$, $k_0 = \mathbf{Q}(\sqrt{-3})$, $k_1 = \mathbf{Q}(\sqrt{57})$,

$\alpha_0 = \sqrt{-8+7\omega_0}$ et $\alpha_0' = \sqrt{-1-7\omega_0}$ avec $Re(\alpha_0)$, $Re(\alpha_0') > 0$,

$u_0 = (-1-\omega_0+\alpha_0)/2$, $u_0' = (-2+\omega_0+\alpha_0')/2$, $\alpha_1 = \sqrt{13+4\omega_1}$, $\alpha_1' = \sqrt{17-4\omega_1}$, $K = kk_0$, $K_i = \mathbf{Q}(\alpha_i)$ et $K_i' = \mathbf{Q}(\alpha_i')$ pour $i \in \{0,1\}$, $v = (-1+\alpha_1)/2 = (-1+\omega_0^{-1}\alpha_0 + \omega_0\alpha_0')/2$.

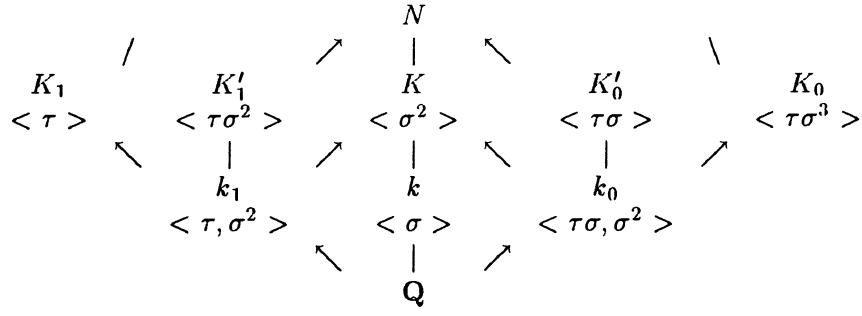
N/k est une extension cyclique de degré relatif 4 et on a : $N = k(v) = \mathbf{Q}(\alpha_0, \alpha_0')$ et $O_N = \mathbf{Z}[\omega, \omega_0, v]$.

Il existe un générateur σ de $Gal(N/k)$ tel que $\sigma(\alpha_0) = -\alpha_0'$ et $\sigma(\alpha_0') = \alpha_0$.

L'extension $N/\mathbf{Q}$ est galoisienne et son groupe de Galois est engendré par σ et la conjugaison complexe notée τ dont les actions sur α_0 et α_0' sont récapitulées dans le tableau suivant :

s	id	σ	σ^2	σ^3	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$
$s(\alpha_0)$	α_0	$-\alpha_0'$	$-\alpha_0$	α_0'	α_0'	$-\alpha_0$	$-\alpha_0'$	α_0
$s(\alpha_0')$	α_0'	α_0	$-\alpha_0'$	$-\alpha_0$	α_0	α_0'	$-\alpha_0$	$-\alpha_0'$

Le schéma ci-dessous récapitule les sous-corps L de $N/\mathbf{Q}$. Pour chacun d'entre eux, $Gal(N/L)$ est indiqué.



On note :

$\varepsilon = -3-4\omega+10\,\omega_0 = -2\sqrt{-19}+5\sqrt{-3}$, $\varepsilon_0 = 2-2\omega_0-u_0\omega_0$, $\varepsilon_0' = \tau(\varepsilon_0) = 2\omega_0 - u_0'(1-\omega_0)$,

$\varepsilon_1 = \sqrt{\varepsilon_0\varepsilon_0'\omega_0}$ avec $Re(\varepsilon_1) > 0$, $\varepsilon_2 = \sqrt{\varepsilon_0\varepsilon}$ avec $Re(\varepsilon_2) > 0$.

U_N est engendré par ω_0, ε_0, $\varepsilon_1$et ε_2.

(Pour le montrer, on utilise les logiciels Kant pour déterminer les unités fondamentales de K, K_0 et K_0', puis, le type de $Gal(N/k_0)$ étant (2,2) la méthode de Wada ([Wad]). $Gal(N/Q)$ agit sur ε_1 et ε_2 de la façon suivante :

s	ϵ_0	ϵ_1	ϵ_2
σ	$\omega_0\epsilon_0\epsilon_1^{-2}$	$\omega_0^3\epsilon_0\epsilon_1^{-1}$	$\omega_0^2\epsilon_0\epsilon_1^{-1}\epsilon_2^{-1}$
σ^2	ϵ_0^{-1}	$\omega_0\epsilon_1^{-1}$	$\epsilon_0^{-1}\epsilon_2$
σ^3	$\omega_0^{-1}\epsilon_0^{-1}\epsilon_1^2$	$\omega_0^2\epsilon_0^{-1}\epsilon_1$	$\omega_0\epsilon_1\epsilon_2^{-1}$
τ	$\omega_0^{-1}\epsilon_0^{-1}\epsilon_1^2$	$\omega_0^5\epsilon_1$	$\omega_0\epsilon_0^{-1}\epsilon_1\epsilon_2$
$\tau\sigma$	ϵ_0^{-1}	$\omega_0^3\epsilon_0^{-1}\epsilon_1$	$\omega_0^3\epsilon_2^{-1}$
$\tau\sigma^2$	$\omega_0\epsilon_0\epsilon_1^{-2}$	ϵ_1^{-1}	$\omega_0^2\epsilon_1^{-1}\epsilon_2$
$\tau\sigma^3$	ϵ_0	$\omega^4\epsilon_0\epsilon_1^{-1}$	$\omega_0^3\epsilon_0\epsilon_2^{-1}$

Signalons les deux lemmes suivants démontrables sans difficultés particulières :

LEMME 1. *Soit $\alpha \in U_N$ tel que pour tout i, $|\sigma^i(\alpha)| \leq 2$. Alors α est une racine 6ème de l'unité.*

LEMME 2. *Les nombres algébriques $|\varepsilon_0|^{2/7}$, $|\varepsilon_2|^{2/7}$ ont pour degré 28 et des hauteurs majorées par 306.*

7. Equation aux unités : notations et lemmes préparatoires.

Notations :

1) Pour tout $\alpha \in U_N$, $\alpha = \omega_0^l \prod_{i=0}^{2} \varepsilon_i^{m_i}$ (§7), on rappelle :

$H(\alpha) = \prod_{i=0}^{3} \max\left(1, |\sigma^i(\alpha)|^{1/4}\right)$ est la hauteur de α,

$h(\alpha) = \ln(H(\alpha))$ est la hauteur logarithmique de α.

$m(\alpha) = \max_{i<3}(|m_i|)$.

2) On note $\mathfrak{R}$ la matrice :

$$\mathfrak{R} = \begin{pmatrix} 1 & \ln(|\varepsilon_0|) & \ln(|\varepsilon|) & \ln(|\varepsilon_2|) \\ 1 & \ln(|\sigma(\varepsilon_0)|) & \ln(|\sigma(\varepsilon_1)|) & \ln(|\sigma(\varepsilon_2)|) \\ 1 & \ln(|\sigma^2(\varepsilon_0)|) & \ln(|\sigma^2(\varepsilon_1)|) & \ln(|\sigma^2(\varepsilon_2)|) \\ 1 & \ln(|\sigma^3(\varepsilon_1)|) & \ln(|\sigma^3(\varepsilon_1)|) & \ln(|\sigma^3(\varepsilon_2)|) \end{pmatrix}$$

elle est inversible; le maximum de la valeur absolue des coefficients de $\mathfrak{R}$ (resp. $\mathfrak{R}^{-1}$) est noté $||\mathfrak{R}||$ (resp. $||\mathfrak{R}^{-1}||$).

3) Pour tout $x \in \mathbf{R}$, on note : $R(x)$ l'un des entiers le plus proche de x et $||x|| = |x - R(x)|$.

Les lemmes suivants sont des adaptations du lemme 5.4 et du théorème 5.5 du chapitre IX de [Si].

LEMME 3. *Quel que soit $\alpha \in U_N$, on a :* $\dfrac{h(\alpha)}{3||\mathfrak{R}||} \leq m(\alpha) \leq 8||\mathfrak{R}^{-1}||h(\alpha)$.

Démonstration : Soit $\alpha \in U_N$, $\alpha = \omega_0^l \prod_{i=0}^{2} \varepsilon_i^{m_i}$ avec $l, m_i \in \mathbf{Z}$. Pour tout $i < 4$, notons $\alpha_i = \ln(|\sigma^i(\alpha)|)$.

1) Montrons la première inégalité. On a $\mathfrak{R}^t(0, m_0, m_1, m_2) = {}^t(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ et par conséquent (cf notations) : $4h(\alpha) \leq \sum_{i=0}^{3} |\alpha_i| \leq 12||\mathfrak{R}||m(\alpha)$.

2) Montrons la deuxième inégalité. On a : $h(\alpha) = h(\alpha^{-1})$ car $\sum_{i=0}^{3} \alpha_i$ est nul ($U_k = \{\pm 1\}$),

$$\forall i \quad \max(0, \alpha_i) + \max(0, -\alpha_i) = |\alpha_i|,$$

et par conséquent :

$$2h(\alpha) = h(\alpha) + h(\alpha^{-1}) = 1/4 \sum_{i=0}^{3} |\alpha_i|.$$

De l'égalité ${}^t(0, m_0, m_1, m_2) = \mathfrak{R}^{-1}{}^t(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$, on déduit donc :

$$m(\alpha) \leq ||\mathfrak{R}^{-1}|| \sum_{i=0}^{3} |\alpha_i| = 8||\mathfrak{R}^{-1}||h(\alpha).$$

LEMME 4. *Quelles que soient α, $\beta \in U_N$ telles que $\alpha + \beta = 1$, on a l'inégalité :*

$|h(\alpha) - h(\beta)| \leq 1$.

Démonstration : Soient α, $\beta \in U_N$ tels que $\alpha+\beta = 1$. On a les inégalités :

$\forall x, y \in [1, +\infty[: \ |\ln(x) - \ln(y)| \leq |x - y|,$

$\forall x, y \in \mathbf{R}_+ \ : \ |\max(x, 1) - \max(y, 1)| \leq |x - y|,$

$\forall x, y \in \mathbf{R} \ : \ ||x| - |y|| \leq |x - y|.$

Pour tout i, on en déduit :

$||\sigma^i(\alpha)| - |\sigma^i(\beta)|| \leq |\sigma^i(\alpha) + \sigma^i(\beta)| = 1,$

$|\max(|\sigma^i(\alpha)|, 1) - \max(|\sigma^i(\beta)|, 1)| \leq ||\sigma^i(\alpha)| - |\sigma^i(\beta)||,$

$|\ln(\max(|\sigma^i(\alpha)|, 1)) - \ln(\max(|\sigma^i(\beta)|, 1))| \leq |\max(|\sigma^i(\alpha)|, 1) - \max(|\sigma^i(\beta)|, 1)| \leq 1.$

On obtient le résultat cherché en sommant sur les i de 1 à 4.

Le lemme suivant permet de ramener l'équation aux unités à des combinaisons de logarithmes et par conséquent d'utiliser la méthode de Baker.

LEMME 5. *Soient α, $\beta \in U_N$, telles que :*

$$\alpha = \prod_{i=0}^{2} |\varepsilon_i|^{m_i}, \quad \beta = \prod_{i=0}^{2} |\varepsilon_i|^{n_i} \text{ avec } m_i, n_i \in \mathbf{Z}, \text{ et } \alpha + \beta = 1,$$

$|\alpha| = \max_{i<4} |\sigma^i(\alpha)|$ et on suppose que $|\alpha| > 2$. Pour tout i, on pose $q_i = m_i - n_i$. Alors il existe une constante a calculable explicitement, indépendante de α et β, telle que :

1) $\max |q_i| \leq a(2h(\alpha) + 1)$,

2) $\left|\sum_{i=0}^{2} q_i \ln(|\varepsilon_i|^{2/7})\right| < \exp\left(-\frac{1}{2a} a(2h(\alpha) + 1)\right)$.

Démonstration :

1) Majorons les q_i en valeur absolue. De façon évidente, on a : $|q_i| \leq |m_i| + |n_i| \leq m(\alpha) + m(\beta)$. D'après les lemmes 3 et 4, on a :

$$m(\alpha) + m(\beta) \leq 8||\mathfrak{R}^{-1}||(h(\alpha) + h(\beta)) \leq 8||\mathfrak{R}^{-1}||(2h(\alpha) + 1).$$

On obtient donc $\max_{i<3} |q_i| \leq a(2h(\alpha) + 1)$, en posant $a > 8||\mathfrak{R}^{-1}||$.

2) Montrons la deuxième inégalité. De façon évidente, on a :

$$\left|\sum_{i=0}^{2} q_i \ln(|\varepsilon_i|)\right| = |\ln(|\alpha|) - \ln(|\beta|)|. \tag{1}$$

Les hypothèses faites sur α et β entraînent :

$$|\alpha|/2 < |\alpha| - 1 \leq |\alpha - 1| = |\beta|, \quad H(\alpha) \leq |\alpha|.$$

En utilisant la convexité de la fonction ln, on a alors :

$$|\ln(|\alpha|) - \ln(|\beta|)| < 2H(\alpha)^{-1}. \tag{2}$$

Puisque $H(\alpha) = \exp(h(\alpha))$ et $4\sqrt{e} < 7$, on obtient :

$$2H(\alpha)^{-1} < 7/2 \exp\left(\frac{-1}{2a} a(2h(\alpha) + 1)\right) \tag{3}$$

Le résultat se déduit de (1), (2) et (3).

Rappelons deux résultats classiques sur les fractions continues.

LEMME 6. *1) Soient $\theta \in \mathbf{R}$ et p/q une approximation rationnelle de θ qui vérifie l'inégalité $|\theta - p/q| < 1/(2q^2)$. Alors p/q est une réduite (ou un convergent) de θ.*

2) Si p_n/q_n est la réduite de rang n dans le développement en fractions continues de θ et a_n le quotient partiel (ou incomplet) de rang n correspondant, alors on a :

$$\frac{1}{(a_n + 2)q_n^2} < \left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{a_n q_n^2}.$$

LEMME 7. *Pour tout $x \in \mathbf{R}$, on a :*

1) $3 \geq 6||x|| \geq ||6x||$

2) $|\sin(x)| = \sin(||x/\pi||\pi)$

3) $\sin(x) \geq (2/\pi)x$ *si* $x \in [0, \pi/2]$.

Démonstration : Soit $x \in \mathbf{R}$. On déduit 1) de l'inégalité suivante :

$|6x - 6R(x)| \geq |6x - R(6x)|$.

On déduit 2) de l'égalité suivante : $x/\pi = R(x/\pi) \pm ||x/\pi||$ et l'inégalité 3) résulte de ce que la restriction de la fonction sinus à $[0, \pi/2]$ est concave.

8. Résolution de l'équation aux unités.

Ce paragraphe suit la méthode expliquée dans [E].

Hypothèses.

Soient α, $\beta \in U_N$, telles que :

$$\alpha = \prod_{i=0}^{2} |\varepsilon_i|^{m_i}, \quad \beta = \prod_{i=0}^{2} |\varepsilon_i|^{n_i} \text{ avec } m_i, n_i \in \mathbf{Z}.$$

On suppose : $\alpha + \beta = 1$, avec $|\alpha| = \max|\sigma^i(\alpha)|$ et $|\alpha| > 2$. Pour tout i, on pose $q_i = m_i - n_i$.

1) Majoration des q_i grâce à la méthode de Baker.

Par le calcul, on trouve : $\|\mathfrak{R}^{-1}\| < 0.6$. Nous sommes dans les conditions d'application du lemme 5, on peut prendre $a = 5$ (voir la démonstration du lemme 5 pour le choix de a). D'après le théorème de Baker ([E]) et le lemme 2, on a donc :

$$5(2h(\alpha) + 1) \leq (4^9 10 \times 28^6 \ln(306))^{49} \leq 10^{780}.$$

C'est-à-dire : $|q_i| \leq 10^{780}$.

2) Transformation de l'inégalité du lemme 5.

Posons $v_i = 2/7 \ln(|\varepsilon_i|)$, $K = \exp(1/10)$, $H = \max(|q_i|)$. D'après le lemme 5, puisque $v_1 = v_0$, on a :

$$|(q_0 + q_1)v_1 + q_2 v_2| < K^{-H}. \tag{1}$$

Posons $q_1' = q_0 + q_1$ et $H' = \max(|q_1'|/2, |q_2|)$. On a alors :

$$|q_1'| \leq 2\max(|q_1|, |q_0|), \quad H' \leq H \text{ et } |q_1' v_1 + q_2 v_2| < K^{-H'}. \tag{2}$$

3) Montrons que si $q_1' q_2 \neq 0$ alors $|q_2| \leq 64$.

Supposons $q_1' q_2 \neq 0$. Posons $\theta = -v_2/v_1$ ($\theta > 0$). La relation (2) devient :

$$\left|\theta - \frac{q_1'}{q_2}\right| < \frac{K^{-|q_2|}}{|v_1||q_2|}. \tag{3}$$

Nous allons montrer que $|q_2| \leq 64$, en raisonnant par l'absurde. Supposons $|q_2| \geq 65$, considérons la fonction f définie par $f(x) = xK^{-x}$, elle est

strictement décroissante sur $[10, +\infty[$ et on a $f(65) < |v_1|/2$. D'après (3), on a alors :

$$|\theta - \frac{q_1'}{q_2}| < \frac{K^{-|q_2|}}{|v_1||q_2|} < \frac{1}{2q_2^2},$$

ce qui entraîne que q_1'/q_2 est un convergent de θ (lemme 6). Nous allons montrer en raisonnant par l'absurde que : $|q_2| < 151$. Supposons $|q_2| \geq 151$. On vérifie, à la machine, que les quotients partiels du développement en fraction continue de θ sont majorés par 6380 pour tous les convergents de dénominateur inférieur à 10^{780} (et même à 2×10^{780}).

Puisque $f(151) < |v_1|/6382$, (3) s'écrit :

$$|\theta - \frac{q_1'}{q_2}| < \frac{K^{-|q_2|}}{|v_1||q_2|} < \frac{1}{6382q_2^2},$$

q_1'/q_2 étant un convergent de θ, il est absurde de supposer $|q_2| \geq 151$, d'après le lemme 6.

La seule réduite p/q de θ telle que $65 \leq q < 151$ est $142/149$. On vérifie que :

$$|\theta - 142/149| > \frac{K^{-149}}{149v_1}.$$

On a donc montré : $|q_2| \leq 64$.

4) Montrons que si $q_1'q_2 \neq 0$ alors $|q_1'| \leq 138$.

Supposons $q_1'q_2 \neq 0$ Posons $\theta' = -v_1/v_2 = 1/\theta$ $(\theta' > 0)$. (1) devient :

$$|\theta' - \frac{q_2}{q_1'}| < \frac{K^{-|q_1'|/2}}{|v_2||q_1'|}. \tag{4}$$

Nous allons montrer que $|q_1'| \leq 138$, en raisonnant par l'absurde. Supposons $|q_1'| > 138$, considérons la fonction g définie par $g(x) = xK^{-x/2}$, elle est strictement décroissante sur $[20, +\infty[$ et on a $g(139) < |v_2|/2$. D'après (4), on a alors :

$$|\theta' - \frac{q_2}{q_1'}| < \frac{K^{-|q_1'|/2}}{|v_2||q_1'|} < \frac{1}{2{q_1'}^2}$$

ce qui entraine que q_2/q_1' est un convergent de θ' (lemme 6). Nous allons montrer que $|q_1'| < 317$, en raisonnant par l'absurde. Supposons $|q_1'| \geq 317$, les deux premières réduites de θ' sont les inverses de celles de θ. Les

quotients partiels du développement en fraction continue de θ' sont donc les mêmes que ceux de θ, c'est-à-dire qu'ils sont aussi majorés par 6380 pour tous les convergents de dénominateur inférieur à 2×10^{780} (cf. **3)**).

Puisque $g(317) < |v_2|/6382$, (4) s'écrit :

$$|\theta' - \frac{q_2}{q_1'}| < \frac{K^{-|q_1'|/2}}{|v_2||q_1'|} < \frac{1}{6382{q_1'}^2},$$

q_2/q_1' étant un convergent de θ', il est absurde de supposer $|q_1'| \geq 317$, d'après le lemme 6. Les seules réduites p/q de θ' telles que $139 \leq q < 317$ sont 149/142 et 213/203. On vérifie dans les deux cas que : $|qv_2 + pv_1| > K^{-p}$. On a donc montré : $|q_1'| \leq 138$.

5) Montrons que si $q_1' = 0$ et $q_2 \neq 0$ alors $|q_1| \leq 2$ et $|q_2| \leq 3$.

Supposons $q_1' = 0$. D'après (1), on a : $|q_2|K^{|q_2|}|v_2| \leq 1$. La fonction qui à x associe $x\exp(x)$ étant strictement croissante sur $\mathbf{R}_+$, on en déduit : $|q_2| \leq 3$. D'après (1), on a aussi : $|q_2||v_2| \leq K^{-|q_1|}$. On en déduit $|q_1| \leq -10\ln(3|v_2|) \leq 2$ car $|q_2| \leq 3$.

6) Montrons que si $q_2 = 0$ et $q_1' \neq 0$ alors $\max(|q_0|, |q_1|) \leq 12$ et $|q_1'| \leq 3$.

Supposons $q_2 = 0$. D'après (1), on a $|v_1| \leq K^{-m}$, où $m = \max(|q_0|, |q_1|)$. On en déduit : $m \leq -10\ln(|v_1|) \leq 12$. D'après (2), on a : $|q_1'|K^{|q_1'|/2}|v_1| \leq 1$. La fonction qui à x associe $x\exp(x)$ étant strictement croissante sur $\mathbf{R}_+$, on en déduit : $|q_1'| \leq 3$.

7) Montrons que si $q_1' = q_2 = 0$ alors $|q_1| \leq 27$.

Supposons $q_1' = q_2 = 0$. Soit $t \in]-\pi, \pi]$ tel que $\varepsilon_1/\varepsilon_0 = e^{it}$. Posons $q = q_1$ et $\gamma = \alpha/\beta$. Il existe $m \in \mathbf{N}$, $0 \leq m \leq 5$, tel que $\gamma = \omega_0^m e^{iqt}$. Quitte à considérer β/α au lieu de α/β, on peut supposer $q > 0$ (car parmi les hypothèses initiales nous n'allons nous servir que de l'égalité $\alpha + \beta = 1$).

L'objectif de ce qui suit est de minorer $\mathfrak{N} = |N_{N/k}(1-\gamma)|$ et d'en déduire une majoration de q sachant que $\mathfrak{N} = 1$.

a) Première minoration de $\mathfrak{N}$.

Notons : $\nu = \ln(|\varepsilon_0|)$, $s = 3t/\pi$, $s' = 1 - s$, $x = qs + m$, $y = qs' + m$. D'après la proposition 7, on a : $|\sigma(\gamma)| = e^{q\nu}$, $|\sigma^3(\gamma)| = e^{-q\nu}$ ainsi que $|\sigma^2(\gamma)| = 1$ et $\arg(\sigma^2(\gamma)) = q(\pi/3 - t) + m\pi/3$. En utilisant les notations précédentes et le lemme 7, on obtient :

$|1-\gamma| = 2|\sin(\pi x/6)| = 2\sin(||x/6||\pi) \geq 4||x/6||,$

$|1-\sigma^2(\gamma)| = 2|\sin(\pi y/6)| = 2\sin(||y/6||\pi) \geq 4||y/6||.$

Puisque $||x|| = ||qs||$ et $||y|| = ||qs'||$, d'après le lemme 7, on a encore :

$|1-\gamma| \geq 2/3||qs||$ et $|1-\sigma^2(\gamma)| \geq 2/3||qs'||$.

$\mathfrak{N}$ est donc minoré par $4/9||qs||||qs'||e^{q\nu}(1-e^{-q\nu})^2$.

b) Minorations de $||qs||$ et de $||qs'||$.

On va montrer que $||qs||$ est minoré par $1/((M+2)q)$, où M est un majorant de tous les quotients partiels (sauf éventuellement le premier car il peut être négatif) correspondant à toutes les réduites p'/q' de s telles que $q' \leq 10^{780}$.

Si $||qs|| \geq 1/(2q)$ alors on a évidemment $||qs|| \geq 1/((M+2)q)$. Si $||qs|| < 1/(2q)$ on a alors : $||qs||/q = |s - R(qs)/q| < 1/(2q^2)$. D'après le lemme 6, $R(qs)/q$ est une réduite de s qui vérifie : $|s - R(qs)/q| > 1/(M+2)q^2$, d'où on déduit la minoration de $||qs||$. Des calculs à la machine permettent de prendre $M = 9987$; c'est aussi un majorant de tous les quotients partiels correspondants à toutes les réduites p'/q' de s' tels que $q' \leq 10^{780}$. De même $||qs'||$ est minoré par $1/((M+2)q)$.

c) Minoration finale de $\mathfrak{N}$.

De a) et b) on déduit : $\mathfrak{N} > 10^{-9}(1-e^{-q\nu})^2 e^{q\nu}/q^2$. Puisque l'on a $\nu > 0.98$ (annexe B), la fonction f définie par $f(x) = 10^{-9}(1-e^{-\nu x})^2 e^{\nu x}/x^2$ est croissante sur $[3, +\infty[$. On vérifie que $f(28) > 1$. Par conséquent q est majoré par 27.

8) Calculs Terminaux.

On a donc montré que :

si $q_1' q_2 \neq 0$ alors $|q_2| \leq 64$ et $|q_1'| \leq 138$,

si $q_1' = 0$ et $q_2 \neq 0$ alors $|q_1| \leq 2$ et $|q_2| \leq 3$,

si $q_2 = 0$ et $q_1' \neq 0$ alors $\max(|q_0|,|q_1|) \leq 12$ et $|q_1'| \leq 3$,

si $q_1' = q_2 = 0$ alors $|q_1| \leq 27$.

Par le calcul on met en évidence que l'équation aux unités $\xi_1 + \xi_2 = 1$ a exactement treize solutions, à permutation près de ξ_1 et de ξ_2, de la forme :

$$\xi_1 = \omega_0^m \varepsilon_0^{q_0} \varepsilon_1^{q_1} \varepsilon_2^{q_2} \text{ et } \xi_2 = \omega_0^{m'} \varepsilon_0^{q_0'} \varepsilon_1^{q_1'} \varepsilon_2^{q_2'}.$$

m	q_0	q_1	q_2	m'	q'_0	q'_1	q'_2
5	2	0	-1	4	-1	3	-1
4	3	-3	0	2	1	-3	1
1	-2	0	1	2	-3	3	0
1	1	-3	1	2	1	0	1
2	0	-3	0	4	-1	0	-1
5	-1	3	-1	4	0	3	0
5	-1	0	-1	1	2	-3	-1
1	-3	3	0	5	-2	3	1
1	1	0	1	5	3	-3	0
4	-2	3	1	2	-2	0	1
5	0	3	0	4	2	0	-1
2	2	-3	-1	1	0	-3	0
1	0	0	0	5	0	0	0

9. Non monogénéité de O_N sur O_k.

THÉORÈME. *L'anneau des entiers du corps de classes N de $k = \mathbf{Q}(\sqrt{-19})$ de rayon 3 n'est pas O_k-monogène.*

Démonstration : L'extension N/k est cyclique de degré 4. Il est facile de se placer dans les conditions du théorème. On a : $O_N = O_K[v]$. Posons $x = \sigma^2(v) - v$ et $\rho = \sigma(x)/x$.

Après des calculs élémentaires, on obtient (cf. §6) : $\rho = -\varepsilon = \omega_0^3 \varepsilon_0^{-1} \varepsilon_2^2$. D'après le théorème du §4, si O_N est O_k-monogène, il existe $\mu \in U_K$ et $\zeta \in U_N$ telles que :

$$\mu/\zeta - \rho\sigma(\zeta)/\zeta = 1. \tag{1}$$

Considérons une solution de l'équation aux unités $\xi_1 + \xi_2 = 1$:

$\xi_1 = \omega_0^m \varepsilon_0^{q_0} \varepsilon_1^{q_1} \varepsilon_2^{q_2}$ et $\xi_2 = \omega_0^{m'} \varepsilon_0^{q'_0} \varepsilon_1^{q'_1} \varepsilon_2^{q'_2}$.

Déterminons les unités ζ de N telles que $-\rho\sigma(\zeta)/\zeta = \xi_1$, et pour chaque unité ζ trouvée calculons $\zeta\xi_2$. Soit $\zeta \in U_N$, ζ et $\zeta\xi_2$ s'écrivent sous la

forme : $\zeta = \omega_0^n \varepsilon_0^{r_0} \varepsilon_1^{r_1} \varepsilon_2^{r_2}$, $\zeta\xi_2 = \omega_0^{n'} \varepsilon_0^{s_0} \varepsilon_1^{s_1} \varepsilon_2^{s_2}$ avec n, n', r_i, s_i entiers. On a $-\rho\sigma(\zeta)/\zeta = \xi_1$ si et seulement si (cf. §6) :

$$(2) \qquad \begin{pmatrix} -2 & 1 & 3 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & -2 & -2 & -1 \\ 0 & 0 & 0 & -2 \end{pmatrix} \begin{pmatrix} n \\ r_0 \\ r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} m \\ q_0 + 1 \\ q_1 \\ q_2 - 2 \end{pmatrix}$$

A partir de (2), connaissant ξ_1, il est facile de résoudre dans U_N l'équation $-\rho\sigma(\zeta)/\zeta = \xi_1$.

Dans le tableau suivant, sont récapitulées les valeurs trouvées pour ξ_1, ξ_2, ζ et $\zeta\xi_2$ en utilisant toutes les solutions de l'équation aux unités (cf. §8) :

m	q_0	q_1	q_2	m'	q_0'	q_1'	q_2'	n	r_0	r_1	r_2	n'	s_0	s_1	s_2
2	-3	3	0	1	-2	0	1	-4	1	-3	1	-3	-1	-3	2
4	0	3	0	5	-1	3	-1	-2	-2	0	1	3	-3	3	0
5	3	-3	0	1	1	0	1	2	-2	3	1	3	-1	3	2
1	0	-3	0	2	2	-3	-1	1	1	0	1	3	3	-3	0

Les valeurs trouvées pour s_1 étant toujours impaires, aucune des unités $\zeta\xi_2$ correspondantes n'est élément de U_K et ne peut jouer le rôle de μ dans (1), O_N n'est donc pas O_k-monogène.

RÉFÉRENCES

[CN-T1] P. CASSOU-NOGUÈS et M. J. TAYLOR, *Elliptic functions and rings of integers*, Progress in Math n°66. Birkhauser.

[CN-T2] P. CASSOU-NOGUÈS et M. J. TAYLOR, *A note on elliptic curves and the monogeneity of rings of integers*, J. London Math. Soc (2) **37** (1988), 63-72.

[CN-T3] P. CASSOU-NOGUÈS et M. J. TAYLOR, *Unités modulaires et monogénéité d'anneaux entiers*, Sém. de Théorie des Nombres de Paris 1986-87. Progress in Math. Birkhauser.

[C1] J. COUGNARD, *Conditions nécessaires de monogénéité. Application aux extensions cycliques de degré premier $\ell > 5$ d'un corps quadratique imaginaire*, J. London Math. Soc. (2) **37** (1988), 73-87.

[C2] J. COUGNARD, *Génération de l'anneau des entiers des corps de classes $\mathbb{Q}(i)$ de rayon impair et points de division de $Y^2 = X^3 - X$*, J. Number Theory, (2) 30 (1988), 140-155.

[C-F1] J. COUGNARD et V. FLECKINGER, *Modèle de Legendre d'une courbe elliptique à multiplication complexe et monogénéité d'anneaux d'entiers II*, Acta Arithmetica **55** (1990), 75-81.

[C-F2] J. COUGNARD et V. FLECKINGER, *Sur la monogénéité de l'anneaux des entiers de certains corps de rayon*, Manuscripta Math. **63** (1989), 365-376.

[E] W. J. ELLISON, *Recipes for solving diophantines problems by Baker's method*, Sém. de Théorie des Nombres de Bordeaux. 1970-71, exp. n°11.

[F] V. FLECKINGER, *Fonctions elliptiques et génération d'anneaux d'entiers*, Thèse de doctorat d'Etat. Université Bordeaux I, 1987.

[G] G. GRAS, *Théorie du corps de classes global*, Cours de Théorie des nombres du D. E. A. Publ. Math. Fac. Sci. Besançon. Théorie des nombres (1979/1980).

[Gmn] M. N. GRAS, *Non monogénéité de l'anneau des entiers des extensions cycliques de degré premier $\ell > 5$.*, J. Number Theory, (2) 23, (1986), 347-353.

[H] H. HASSE, *Number Theory*, Springer-Verlag, 1980.

[La1] S. LANG, *Algebra*, Addison-Wesley, 1971.

[La2] S. LANG, *Algebraic number theory*, Addison-Wesley, 1970.

[Sa] P. SAMUEL, *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[Sc1] R. SCHERTZ, *Konstruktion von Potenzganzheitsbasen in Strahlklassenkörpern über imaginär-quadratischen Zahlkorpern*, J. Reine angew. Math. **398** (1989), 105-129.

[Sc2] R. SCHERTZ, *Zur expliziten Berechnung von Ganzheitsbasen in Strahlklassenkörpern über einem imaginär-quadratischen Zahlkörper*, J. Number Theory, (2) 34, (1990), 41-53.

[Se] J.-P. SERRE, *Corps locaux*, Hermann, Paris 1962.

[Si] J. H. SILVERMAN, *The arithmetic of elliptic curves*, Springer-Verlag 1986.

[St] H. M. STARK, *L-functions at $s = 1$.III. Totally Real Fields and Hilbert's Twelfth Problem*, Advances in Math. **22** (1976), 64-84.

[S-V] A. SRIVASTAV and S. VENKATARAMAN, *On Fueter model and monogeneity of rings of integers*, A paraître.

[V] M. VÉRANT, *Monogénéité de l'anneau des entiers de certains corps de classes de corps quadratiques*, Thèse de doctorat de l'Université de Franche-Comté, 1990.

[Wad] H. WADA, *On the class number and the unit group of certain algebraic number fields*, J. Fac. Sci. Univ. Tokyo **13** (1966), 201-209.

[Wal] M. WALDSCHMIDT, *Nouvelles méthodes pour minorer des combinaisons de logarithmes de nombres algébriques*, Leiden (octobre 1990). A paraître.

J. COUGNARD et M. VÉRANT
U. A. au C. N. R. S. n°741
25030 Besançon Cedex
France