Générateurs de l’anneau des entiers d’une extension cyclotomique.

GABRIELE RANIERI

Dipartimento di Matematica Leonida Tonelli, Largo Bruno Pontecorvo 5, 56127 Pisa, Italy

Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139, Université de Caen BP 5186, 14032 Caen cedex, France

E-mail : ranieri@mail.dm.unipi.it, ranieri@math.unicaen.fr

Résumé. Soit p un nombre premier impair, soit $q = p^m$, où m est un entier positif ; notons ζ_q une racine primitive q-ième de l'unité et $\mathcal{O}_q$ l'anneau des entiers de $\mathbb{Q}(\zeta_q)$. Dans [3] I. Gaal et L. Robertson montrent que si $(h_q^+, p(p-1)/2) = 1$, où h_q^+ est l'ordre du groupe des classes de $\mathbb{Q}(\zeta_q + \overline{\zeta_q})$, alors si $\alpha \in \mathcal{O}_q$ engendre $\mathcal{O}_q$ (autrement dit $\mathbb{Z}[\alpha] = \mathcal{O}_q$) soit α est un conjugué d'un translaté par un entier de ζ_q soit $\alpha + \overline{\alpha}$ est un entier impair. Dans notre travail nous montrons que nous pouvons éliminer l'hypothèse sur h_q^+. Autrement dit nous prouvons que si α engendre $\mathcal{O}_q$, alors soit α est un conjugué d'un translaté par un entier de ζ_q soit $\alpha + \overline{\alpha}$ est un entier impair.

Abstract. Let p be an odd prime and $q = p^m$, where m is a positive integer. Let ζ_q be a qth primitive root of 1 and $\mathcal{O}_q$ be the ring of integers in $\mathbb{Q}(\zeta_q)$. In [3] I. Gaal and L. Robertson show that if $(h_q^+, p(p-1)/2) = 1$, where h_q^+ is the class number of $\mathbb{Q}(\zeta_q + \overline{\zeta_q})$, then if $\alpha \in \mathcal{O}_q$ is a generator of $\mathcal{O}_q$ (in other words $\mathbb{Z}[\alpha] = \mathcal{O}_q$) either α is equals to a conjugate of an integer translate of ζ_q or $\alpha + \overline{\alpha}$ is an odd integer. In this paper we show that we can remove the hypothesis over h_q^+. In other words we show that if α is a generator of $\mathcal{O}_q$ then either α is a conjugate of an integer translate of ζ_q or $\alpha + \overline{\alpha}$ is an odd integer.

Keywords. Cyclotomic, power bases, Bremner's conjecture.

1 Introduction.

Soit K un corps de nombres et soit $\mathcal{O}_K$ son anneau des entiers. On dit que $\mathcal{O}_K$ admet une base de puissances s'il existe $\alpha \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Il est rare (voir [6]) qu'un corps de nombres admette une base de puissances. Par exemple Gras [4] montre que si d est un entier positif tel que $(d, 6) = 1$, alors il existe seulement un nombre fini d'extensions abéliennes $K/\mathbb{Q}$ de degré d telles que $\mathcal{O}_K$ admette une base de puissances.

Quand l'anneau des entiers $\mathcal{O}_K$ admet une base de puissances le problème de déterminer tous les générateurs de $\mathcal{O}_K$ (autrement dit tous les éléments $\alpha \in \mathcal{O}_K$ tels que $\mathcal{O}_K = \mathbb{Z}[\alpha]$) se pose. Plus précisément, puisque $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha+k]$ pour tout entier k, il est intéressant de déterminer tous les générateurs α de $\mathcal{O}_K$ à translation par entiers près. Dans [5] Györy obtient un important résultat : il montre que, à translation par entiers près, il existe seulement un nombre fini d'éléments qui engendrent l'anneau des entiers de n'importe quel corps de nombres. En outre il y a beaucoup de résultats sur la détermination de bases de puissances de l'anneau des entiers de corps de nombres de petit degré (pour un résumé voir [2]). De toute façon si K est un corps de nombres dont l'anneau des entiers $\mathcal{O}_K$ admet une base de puissances, le problème de déterminer tous les générateurs de $\mathcal{O}_K$ est très difficile.

Les corps cyclotomiques sont une intéressante famille de corps pour notre problème parce que l'anneau des entiers d'un tel corps admet une base de puissances et il y a quelques exemples où nous pouvons trouver tous les générateurs.

Soit n un entier positif et soit ζ_n une racine primitive n-ième de l'unité dans $\mathbb{C}$. Alors il est bien connu que ζ_n engendre l'anneau des entiers de $\mathbb{Q}[\zeta_n]$. Considérons la relation suivante : soit $\alpha \in \mathbb{Z}[\zeta_n]$, nous disons que $\beta \in \mathbb{Z}[\zeta_n]$ est équivalent à α (noté $\alpha \sim \beta$) s'il existe $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{n})/\mathbb{Q})$ et un entier l tel que $\beta = \pm\sigma(\alpha) + l$. Remarquons que si $\beta \sim \alpha$ et α est un générateur de $\mathbb{Z}[\zeta_n]$, alors β engendre $\mathbb{Z}[\zeta_n]$. De plus la relation $\sim$ que nous venons de définir sur les générateurs de $\mathbb{Z}[\zeta_n]$ est une relation d'équivalence.

Soit maintenant p un nombre premier et considérons l'anneau $\mathbb{Z}[\zeta_p]$. Dans ce cas nous connaissons deux classes de générateurs de $\mathbb{Z}[\zeta_p]$: la classe de ζ_p et la classe de $\omega := 1/(\zeta_p + 1)$.

Le nombre ω engendre $\mathbb{Z}[\zeta_p]$ car ω est une unité de norme 1, et par conséquent il existe $a_1, a_2, \ldots, a_{p-1} \in \mathbb{Z}$ tels que :

$$-(a_1 + a_2\omega + \cdots + a_{p-1}\omega^{p-2}) = 1 + \zeta_p.$$

De plus on remarque que ζ_p n'est pas équivalent à ω si $p > 3$ et $\omega + \overline{\omega} = 1$.

Bremner [1] conjecture qu'il n'existe pas d'autres classes de générateurs de $\mathbb{Z}[\zeta_p]$, plus précisément :

Conjecture 1. *Soit p un nombre premier, soit ζ_p une racine p-ième primitive de l'unité et soit $\alpha \in \mathbb{Z}[\zeta_p]$ tel que $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_p]$. Alors soit α est équivalent à ζ_p, soit α est équivalent à $1/(\zeta_p + 1)$.*

Robertson [7] donne une réponse partielle à la conjecture de Bremner :

Théorème 1. *Soit $\alpha \in \mathbb{Z}[\zeta_p]$ tel que $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_p]$. Alors soit α est équivalent à ζ_p soit $\alpha + \overline{\alpha}$ est un entier impair.*

La conjecture 1 se généralise aux corps cyclotomiques engendrés par une racine q-ième de l'unité, où q est la puissance d'un nombre premier, de la façon suivante : soit $\alpha \in \mathbb{Z}[\zeta_q]$ tel que $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_q]$. Alors soit α est équivalent à ζ_q, soit α est équivalent à $1/(\zeta_q + 1)$. Robertson [8] démontre le théorème suivant qui établit une telle conjecture dans le cas où q est une puissance de 2 :

Théorème 2. *Soit m un entier positif et soit α un générateur de $\mathbb{Z}[\zeta_{2^m}]$. Alors $\alpha \sim \zeta_{2^m}$.*

Ensuite, Robertson et Gaál [3] obtiennent un résultat similaire au théorème 1 pour les classes des générateurs de $\mathbb{Z}[\zeta_q]$, où q est la puissance d'un nombre premier p, plus précisément :

Théorème 3. *Soit $\alpha \in \mathbb{Z}[\zeta_q]$ tel que $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_q]$. Alors si $(h_q^+, p(p-1)/2) = 1$, où h_q^+ est l'ordre du groupe des classes de $\mathbb{Q}(\zeta_q + \overline{\zeta_q})$, soit α est équivalent à ζ_q soit $\alpha + \overline{\alpha}$ est un entier impair.*

Dans notre travail nous montrons que l'hypothèse sur h_q^+ dans le théorème 3 n'est pas nécessaire, plus précisément nous obtenons le résultat suivant :

Théorème 4. *Soit $\alpha \in \mathbb{Z}[\zeta_q]$ tel que $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_q]$. Alors soit α est équivalent à ζ_q soit $\alpha + \overline{\alpha}$ est un entier impair.*

Le point de départ de notre démonstration est le lemme 1 où nous montrons une relation assez restrictive (voir (1)) qui lie un générateur α de $\mathbb{Z}[\zeta_q]$ à des éléments de $(\mathbb{Z}/q\mathbb{Z})^*$ notés $b(j, \alpha)$ (ici j est un entier tel que p ne divise pas j et $2 \leq j \leq q-1$). De la relation (1) on déduit la relation (4) sur laquelle la conjugaison complexe agit. Ensuite (lemme 2) nous remarquons que si $\alpha + \overline{\alpha}$ n'est pas un entier alors une telle action n'est pas triviale. Ce fait nous permet d'obtenir une nouvelle relation encore plus restrictive que (1) (voir (5)). D'une telle relation il suit que si i est une racine primitive modulo q, alors la classe de α (dans $\sim$) est bien déterminée par les éléments $b(i, \alpha)$ et $b(i^2, \alpha)$ (proposition 1). Enfin nous terminons la preuve du théorème 4 en montrant que pour tout générateur α de $\mathbb{Z}[\zeta_q]$ tel que $\alpha + \overline{\alpha}$ n'est pas un entier il existe un entier n qui n'est pas divisible par

p tel que $b(i,\alpha) = b(i,\zeta_q^n)$ et $b(i^2,\alpha) = b(i,\zeta_q^n)$, et donc par la proposition 1, $\alpha \sim \zeta_q^n \sim \zeta_q$.

Remerciements. Je tiens à remercier F. Amoroso et R. Dvornicich pour leur aide lors de la réalisation de cet article. Je tiens également à remercier B. Anglès et G. Rhin qui ont relu une version préliminaire de ce travail.

2 Résultats préliminaires.

Soit p un nombre premier, soit m un entier positif et posons $q := p^m$. De plus soit ζ_q une racine primitive q-ième de l'unité, notons $G := \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^*$. Dans ce paragraphe nous déterminons quelques relations satisfaites par les générateurs de $\mathbb{Z}[\zeta_q]$, relations que nous utiliserons dans la preuve du théorème 4.

Lemme 1. *Soit $\alpha \in \mathbb{Z}[\zeta_q]$ tel que $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_q]$. De plus soit $\sigma_j \in G$ tel que $\sigma_j(\zeta_q) = \zeta_q^j$, où $j \in (\mathbb{Z}/q\mathbb{Z})^*$ et $j \not\equiv 1 \mod (q)$. Alors il existe un entier $b(j,\alpha)$ tel que :*

$$\frac{\alpha - \sigma_j(\alpha)}{\overline{\alpha} - \overline{\sigma_j(\alpha)}} = -\zeta_q^{b(j,\alpha)}, \tag{1}$$

Preuve. Soit $\alpha \in \mathbb{Z}[\zeta_q]$ tel que $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_q]$ et soit $\sigma_j \in G$ tel que $\sigma_j(\zeta_q) = \zeta_q^j$, où $j \in (\mathbb{Z}/q\mathbb{Z})^*$ et $j \not\equiv 1 \mod (q)$. Puisque $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_q]$, on a :

$$\delta_{\mathbb{Z}}(\mathbb{Z}[\alpha]) = \delta_{\mathbb{Z}}(\mathbb{Z}[\zeta_q]),$$

où $\delta_{\mathbb{Z}}$ est le discriminant sur $\mathbb{Z}$ (voir [3, Lemme 3.1]). Donc pour tout $j \in (\mathbb{Z}/q\mathbb{Z})^*$ on a que α satisfait la relation suivante :

$$\sigma_j(\alpha) - \alpha = (\zeta_q^j - \zeta_q)\beta(j, \alpha), \tag{2}$$

où $\beta(j, \alpha)$ est une unité. De plus, voir [9, Corollaire 4.13], il existe un entier $c(j, \alpha)$ et il existe une unité réelle $\mu(j, \alpha) \in \mathbb{Q}(\zeta_q + \overline{\zeta_q})$ tels que :

$$\beta(j, \alpha) = \zeta_q^{c(j,\alpha)}\mu(j, \alpha),$$

et donc on obtient la relation :

$$\sigma_j(\alpha) - \alpha = (\zeta_q^j - \zeta_q)\zeta_q^{c(j,\alpha)}\mu(j, \alpha). \tag{3}$$

Par ailleurs on a :

$$\frac{\zeta_q^j - \zeta_q}{\overline{\zeta_q^j} - \overline{\zeta_q}} = -\zeta_q^{j+1}.$$

De cette relation et de (3) nous déduisons que :

$$\frac{\alpha - \sigma_j(\alpha)}{\overline{\alpha} - \overline{\sigma_j(\alpha)}} = \frac{(\zeta_q^j - \zeta_q)\zeta_q^{c(j,\alpha)}\mu(j, \alpha)}{(\overline{\zeta_q^j} - \overline{\zeta_q})\overline{\zeta_q}^{c(j,\alpha)}\mu(j, \alpha)} = -\zeta_q^{j+2c(j,\alpha)+1}.$$

En posant $b(j,\alpha) = j + 2c(j,\alpha) + 1$ on obtient :

$$\frac{\alpha - \sigma_j(\alpha)}{\overline{\alpha} - \overline{\sigma_j(\alpha)}} = -\zeta_q^{b(j,\alpha)}.$$

□

Tout d'abord on remarque que la relation (1) est équivalente à la relation :

$$\alpha + \zeta_q^{b(j,\alpha)}\overline{\alpha} = \sigma_j(\alpha) + \zeta_q^{b(j,\alpha)}\overline{\sigma_j(\alpha)}, \tag{4}$$

qui sera utilisée plusieurs fois dans la suite.

On remarque aussi que si $\alpha \in \mathbb{Z}[\zeta_q]$, alors $\alpha + \overline{\alpha} \in \mathbb{Z}$ si et seulement si pour tout $\sigma_j \in G$, on a :

$$\alpha + \overline{\alpha} = \sigma_j(\alpha) + \overline{\sigma_j(\alpha)}.$$

Donc le théorème 3 nous dit que si α est un générateur de $\mathbb{Z}[\zeta_q]$ qui n'est pas équivalent à ζ_q et si $(h_q^+, p(p-1)/2) = 1$, alors $b(j,\alpha) \equiv 0 \mod (q)$ pour tout $\sigma_j \in G$. Dans la preuve du théorème 4 on montrera que $b(j,\alpha)$ peut être non nul modulo q seulement si α appartient à la classe de ζ_q, en obtenant une généralisation du théorème 3 et du lemme 1.

La remarque élémentaire suivante sera plusieurs fois utilisée dans la preuve du théorème 4.

Remarque 1. *Nous remarquons que si a, b sont entiers tels que $a \geq b \geq 1$, si $p \geq 3$ est un premier et si ϕ est l'homomorphisme*

$$\phi\colon \mathbb{Z}/p^a\mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z}$$

qui envoie la classe de $j \mod (p^a)$ dans la classe de $j \mod (p^b)$, alors si la classe de i engendre $(\mathbb{Z}/p^a\mathbb{Z})^*$ on a :

$$\phi(i) \not\equiv 1 \mod (p^b).$$

De plus si $p \geq 5$ on a :

$$\phi(i) \not\equiv \pm 1 \mod (p^b).$$

Fixons maintenant i une racine primitive modulo q (i.e. un entier tel que sa classe $\mod (q)$ engendre $(\mathbb{Z}/q\mathbb{Z})^*$. Donc σ_i est un générateur de G). Le lemme suivant nous donne une relation entre $b(i,\alpha)$, $b(i^2,\alpha)$ et $\mu(i,\alpha)$ dans le cas $b(i,\alpha) \not\equiv 0 \mod (q)$.

Lemme 2. *Supposons $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta_q]$ et posons (en utilisant les notations du lemme 1) $b(i) := b(i,\alpha)$, $b(i^2) := b(i^2,\alpha)$ et $\mu(i) := \mu(i,\alpha)$. Alors, si $p \geq 3$ et si $b(i) \not\equiv 0 \mod (q)$, on a :*

$$\frac{\sigma_i(\mu(i))}{\mu(i)} = \zeta_q^{ib(i)-b(i^2)-ic(i)+c(i)} \frac{(\zeta_q^i - \zeta_q)}{(\zeta_q^{i^2} - \zeta_q^i)} \frac{(\zeta_q^{b(i^2)-b(i)} - 1)}{(\zeta_q^{ib(i)-b(i^2)} - 1)}, \tag{5}$$

où $c(i) := c(i,\alpha)$ et $2c(i) \equiv b(i) - i - 1 \mod (q)$.

Preuve. Par la relation (4) on a les égalités suivantes :

$$\alpha + \zeta_q^{b(i)}\overline{\alpha} = \sigma_i(\alpha) + \zeta_q^{b(i)}\overline{\sigma_i(\alpha)}, \tag{6}$$

$$\alpha + \zeta_q^{b(i^2)}\overline{\alpha} = \sigma_{i^2}(\alpha) + \zeta_q^{b(i^2)}\overline{\sigma_{i^2}(\alpha)}. \tag{7}$$

En appliquant σ_i aux deux membres de (6) on obtient :

$$\sigma_i(\alpha) + \zeta_q^{ib(i)}\overline{\sigma_i(\alpha)} = \sigma_{i^2}(\alpha) + \zeta_q^{ib(i)}\overline{\sigma_{i^2}(\alpha)}.$$

En soustrayant cette relation à (7) on a :

$$\alpha - \sigma_i(\alpha) + \zeta_q^{b(i^2)}\overline{\alpha} - \zeta_q^{ib(i)}\overline{\sigma_i(\alpha)} = \zeta_q^{b(i^2)}\overline{\sigma_{i^2}(\alpha)} - \zeta_q^{ib(i)}\overline{\sigma_{i^2}(\alpha)}. \tag{8}$$

En additionnant et en soustrayant $\zeta_q^{ib(i)}\overline{\alpha}$ au premier membre de (8) on obtient :

$$\alpha - \sigma_i(\alpha) + (\zeta_q^{b(i^2)} - \zeta_q^{ib(i)})\overline{\alpha} + \zeta_q^{ib(i)}(\overline{\alpha} - \overline{\sigma_i(\alpha)}) = (\zeta_q^{b(i^2)} - \zeta_q^{ib(i)})\overline{\sigma_{i^2}(\alpha)}.$$

En rappelant que, par la relation (1),

$$(\overline{\alpha} - \overline{\sigma_i(\alpha)})\zeta_q^{b(i)} = \sigma_i(\alpha) - \alpha$$

et

$$(\overline{\alpha} - \overline{\sigma_{i^2}(\alpha)})\zeta_q^{b(i^2)} = \sigma_{i^2}(\alpha) - \alpha$$

nous déduisons que

$$\begin{aligned}0 &= \alpha - \sigma_i(\alpha) + \zeta_q^{ib(i)}(\overline{\alpha} - \overline{\sigma_i(\alpha)}) + (\zeta_q^{b(i^2)} - \zeta_q^{ib(i)})(\overline{\alpha} - \overline{\sigma_{i^2}(\alpha)}) \\ &= \alpha - \sigma_i(\alpha) + \zeta_q^{ib(i)-b(i)}(\sigma_i(\alpha) - \alpha) + (\zeta_q^{b(i^2)} - \zeta_q^{ib(i)})\zeta_q^{-b(i^2)}(\sigma_{i^2}(\alpha) - \alpha) \\ &= (\alpha - \sigma_i(\alpha))(1 - \zeta_q^{ib(i)-b(i)}) + (\sigma_{i^2}(\alpha) - \alpha)(1 - \zeta_q^{ib(i)-b(i^2)}),\end{aligned}$$

c'est à dire :

$$(\sigma_i(\alpha) - \alpha)(1 - \zeta_q^{ib(i)-b(i)}) = (\sigma_{i^2}(\alpha) - \alpha)(1 - \zeta_q^{ib(i)-b(i^2)}).$$

Puisque i est une racine primitive modulo q et $p \geq 3$ par la remarque 1 nous avons $i \not\equiv 1 \mod (p)$. Donc $\sigma_i \neq Id$. Alors, $\sigma_i(\alpha) \neq \alpha$, car $\alpha \notin \mathbb{Z}$. De plus $ib(i) - b(i) \not\equiv 0 \mod (q)$ car $i \not\equiv 1 \mod (p)$ et $b(i) \not\equiv 0 \mod (q)$ par hypothèse.

Donc on obtient que $ib(i) - b(i^2) \not\equiv 0 \mod (q)$ et on a :

$$\frac{\sigma_{i^2}(\alpha) - \alpha}{\sigma_i(\alpha) - \alpha} = \frac{\zeta_q^{ib(i)-b(i)} - 1}{\zeta_q^{ib(i)-b(i^2)} - 1},$$

d'où :

$$\frac{\sigma_{i^2}(\alpha) - \sigma_i(\alpha)}{\sigma_i(\alpha) - \alpha} = \frac{\sigma_{i^2}(\alpha) - \alpha}{\sigma_i(\alpha) - \alpha} - 1 = \zeta_q^{ib(i)-b(i^2)} \frac{\zeta_q^{b(i^2)-b(i)} - 1}{\zeta_q^{ib(i)-b(i^2)} - 1}. \qquad (9)$$

Par ailleurs par la relation (3) on a :

$$\sigma_i(\alpha) - \alpha = (\zeta_q^i - \zeta_q)\zeta_q^{c(i)}\mu(i).$$

Donc de cette relation et de (9) il suit que :

$$\frac{(\zeta_q^{i^2}-\zeta_q^i)\zeta_q^{ic(i)}\sigma_i(\mu(i))}{(\zeta_q^i-\zeta_q)\zeta_q^{c(i)}\mu(i)} = \zeta_q^{ib(i)-b(i^2)}\frac{\zeta_q^{b(i^2)-b(i)}-1}{\zeta_q^{ib(i)-b(i^2)}-1},$$

d'où l'assertion. □

Le lemme précédent nous donne une relation entre $\mu(i,\alpha)$, $b(i,\alpha)$ et $b(i^2,\alpha)$. Dans la proposition suivante on verra comment cette relation entraîne que la classe de α est bien déterminée par $b(i,\alpha)$ et $b(i^2,\alpha)$. Cette proposition est le point-clé de la démonstration.

Proposition 1. *Soit i une racine primitive modulo q et soient α_1, α_2 deux générateurs de $\mathbb{Z}[\zeta_q]$. Supposons que $b(i,\alpha_1) \not\equiv 0 \mod (q)$ et que :*

$$b(i,\alpha_1) \equiv b(i,\alpha_2) \mod (q)$$

$$b(i^2,\alpha_1) \equiv b(i^2,\alpha_2) \mod (q);$$

alors $\alpha_1 \sim \alpha_2$.

Preuve. Par le lemme 2,

$$\frac{\sigma_i(\mu(i,\alpha_1))}{\mu(i,\alpha_1)} = \frac{\sigma_i(\mu(i,\alpha_2))}{\mu(i,\alpha_2)}.$$

Puisque σ_i engendre G, il existe un entier h tel que $\mu(i,\alpha_2) = h\mu(i,\alpha_1)$.

De plus, $h = \pm 1$ car $\mu(i, \alpha_1), \mu(i, \alpha_2)$ sont deux unités. Choisissons un entier c tel que $2c \equiv b(i, \alpha_1) - i - 1 \mod (q)$. Par la relation (3) on a :

$$\begin{aligned}\sigma_i(\alpha_1) - \alpha_1 &= (\zeta_q^i - \zeta_q)\zeta_q^c \mu(i, \alpha_1) \\ &= \pm(\zeta_q^i - \zeta_q)\zeta_q^c \mu(i, \alpha_2) \\ &= \pm(\sigma_i(\alpha_2) - \alpha_2);\end{aligned}$$

d'où $\sigma_i(\alpha_1 \pm \alpha_2) = \alpha_1 \pm \alpha_2$ et $\alpha_1 \pm \alpha_2 = k \in \mathbb{Z}$ (car σ_i est un générateur de G). Par conséquent $\alpha_1 \sim \alpha_2$. □

Dans le paragraphe suivant nous allons montrer que si α est un générateur de $\mathbb{Z}[\zeta_q]$ tel que $\alpha + \overline{\alpha}$ n'est pas un entier alors, si nous connaissons $b(i, \alpha)$, $b(i^2, \alpha)$ est aussi bien déterminé. Donc, par la proposition 1, on remarquera que α est seulement déterminé par $b(i, \alpha)$ et il sera facile terminer la démonstration du théorème 4.

3 Preuve du théorème 3.

Robertson [8] montre que la conjecture de Bremner est vraie pour tout corps cyclotomique engendré par une racine de l'unité d'ordre égal à une puissance de 2. De plus, voir [9, Théorème 4.14, Corollaire 10.5, Théorème 11.1], on a que 3 ne divise pas $h_{3^a}^+$ pour tout entier $a \geq 1$. Donc par le théorème 3 nous pouvons

supposer que p soit ≥ 5. De plus par le théorème 1 on peut supposer que q soit égal à p^m, où m est un entier ≥ 2 et donc p^2 divise q.

Soit α un générateur de $\mathbb{Z}[\zeta_q]$ tel que $r := \alpha + \overline{\alpha}$ soit un entier. Si r est pair on a que 2 divise $\alpha - \overline{\alpha}$, car

$$\alpha - \overline{\alpha} = \alpha + \overline{\alpha} - 2\overline{\alpha}.$$

Par ailleurs par la relation (3) on a que l'idéal $(\alpha - \overline{\alpha})$ est engendré par $\overline{\zeta_q} - \zeta_q$. Alors, puisque on peut supposer que $p \geq 5$, on a que (2) est premier avec $\overline{\zeta_q} - \zeta_q$. Donc 2 ne peut pas diviser r et r est un nombre impair.

Soit maintenant α un générateur de $\mathbb{Z}[\zeta_q]$ tel que $\alpha + \overline{\alpha}$ ne soit pas un entier. Pour prouver le théorème nous montrerons que les hypothèses de la proposition 1 sont satisfaites avec $\alpha_1 = \alpha$ et $\alpha_2 = \zeta_q^n$, pour un certain entier n qui n'est pas divisible par p. Donc on aura $\alpha \sim \zeta_q^n \sim \zeta_q$.

Posons, en utilisant les notations du lemme 1, $c(j) := c(j, \alpha)$, $b(j) := b(j, \alpha)$ et $\mu(j) := \mu(j, \alpha)$ pour tout $j \in (\mathbb{Z}/q\mathbb{Z})^*$ (on rappelle que $2c(j) \equiv b(j) - j - 1 \mod (q)$) et soit i une racine primitive modulo q.

On remarque que $b(i) \not\equiv 0 \mod (q)$. En effet si $b(i) \equiv 0 \mod (q)$ alors, par la relation (4), on aurait :

$$\alpha + \overline{\alpha} = \sigma_i(\alpha) + \overline{\sigma_i(\alpha)}$$

et, puisque σ_i engendre G, on obtiendrait :

$$\alpha + \overline{\alpha} = \sigma_j(\alpha) + \overline{\sigma_j(\alpha)} = \sigma_j(\alpha + \overline{\alpha})$$

pour tout $j \in (\mathbb{Z}/q\mathbb{Z})^*$. Donc $\alpha + \overline{\alpha}$ serait un entier car il serait fixé par le groupe G.

Par conséquent on peut appliquer le lemme 2 en obtenant la relation :

$$\frac{\sigma_i(\mu(i))}{\mu(i)} = \zeta_q^{ib(i)-b(i^2)-ic(i)+c(i)} \frac{(\zeta_q^i - \zeta_q)}{(\zeta_q^{i^2} - \zeta_q^i)} \frac{(\zeta_q^{b(i^2)-b(i)} - 1)}{(\zeta_q^{ib(i)-b(i^2)} - 1)}.$$

Par ailleurs puisque

$$\frac{\zeta_q^i - \zeta_q}{\zeta_q^{i^2} - \zeta_q^i} = \frac{\zeta_q^i - \zeta_q}{\sigma_i(\zeta_q^i - \zeta_q)},$$

on obtient :

$$\frac{\sigma_i(\mu(i)(\zeta_q^i - \zeta_q))}{\mu(i)(\zeta_q^i - \zeta_q)} = \zeta_q^{ib(i)-b(i^2)-ic(i)+c(i)} \frac{\zeta_q^{b(i^2)-b(i)} - 1}{\zeta_q^{ib(i)-b(i^2)} - 1}.$$

Nous disons qu'il existe un entier k tel que :

$$\frac{\zeta_q^k}{\sigma_i(\zeta_q^k)} = \zeta_q^{ib(i)-b(i^2)-ic(i)+c(i)}. \tag{10}$$

Cette relation est équivalente à :

$$k(1-i) \equiv ib(i) - b(i^2) - ic(i) + c(i) \mod (q).$$

Puisque $p \geq 5$ on a que $i \not\equiv 1 \mod (p)$ par la remarque 1 et donc $(i-1, q) = 1$.

Donc $(i-1)$ est inversible $\mod (q)$ et il existe k qui satisfait (10).

Par conséquent on a la relation :

$$\frac{\sigma_i(\zeta_q^k\mu(i)(\zeta_q^i-\zeta_q))}{\zeta_q^k\mu(i)(\zeta_q^i-\zeta_q)}=\frac{\zeta_q^{b(i^2)-b(i)}-1}{\zeta_q^{ib(i)-b(i^2)}-1}. \tag{11}$$

Par ailleurs :

$$v_p(b(i^2)-b(i))=v_p(ib(i)-b(i^2)),$$

où v_p est la valuation p-adique. En effet par la remarque 1 on sait que $i-1$ est inversible $\mod(q)$ et donc :

$$\frac{\sigma_i(\zeta_q^k\mu(i)(\zeta_q^i-\zeta_q))}{\zeta_q^k\mu(i)(\zeta_q^i-\zeta_q)}\in\mathbb{Z}[\zeta_q]^*.$$

Par conséquent

$$\frac{\zeta_q^{b(i^2)-b(i)}-1}{\zeta_q^{ib(i)-b(i^2)}-1}\in\mathbb{Z}[\zeta_q]^*$$

et cette relation est vérifiée si et seulement si $v_p(b(i^2)-b(i))=v_p(ib(i)-b(i^2))$.

Maintenant nous voulons déterminer un élément $\beta\in\mathbb{Z}[\zeta_q]$ tel que :

$$\frac{\sigma_i(\beta)}{\beta}=\frac{\zeta_q^{b(i^2)-b(i)}-1}{\zeta_q^{ib(i)-b(i^2)}-1}. \tag{12}$$

Pour cela, on reprend la preuve du théorème 90 de Hilbert. Soit d l'inverse de i $\mod(q)$ et posons

$$\beta_c:=\prod_{l=1}^{c}(\zeta_q^{(b(i^2)-b(i))d^l}-1),$$

où c est un entier et $1\leq c\leq\phi(q)$. Alors on a :

$$\frac{\sigma_i(\beta_c)}{\beta_c}=\frac{\zeta_q^{b(i^2)-b(i)}-1}{\zeta_q^{(b(i^2)-b(i))d^c}-1}.$$

Soit maintenant $\nu \geq 0$ la valuation p-adique de $b(i^2)-b(i)$ et $ib(i)-b(i^2)$. Notons $p^\nu = q/p^e$; l'entier i est une racine primitive modulo p^e et donc il existe un entier c' tel que $1 \leq c' \leq \phi(p^e) \leq \phi(q)$ et :

$$(b(i^2)-b(i))d^{c'} \equiv ib(i)-b(i^2) \mod (q). \tag{13}$$

Donc $\beta_{c'}$ satisfait la relation :

$$\frac{\sigma_i(\beta_{c'})}{\beta_{c'}} = \frac{\zeta_q^{b(i^2)-b(i)}-1}{\zeta_q^{ib(i)-b(i^2)}-1}.$$

Puisque σ_i engendre le groupe G il existe un nombre rationel $h \neq 0$ tel que :

$$\zeta_q^k \mu(i)(\zeta_q^i - \zeta_q) = h\beta_{c'}.$$

Soit maintenant $v_{(\zeta_q-1)}$ la valuation (ζ_q-1)-adique. Puisque ζ_q^k et $\mu(i)$ sont des unités leur valuation (ζ_q-1)-adique est égal à 0, alors que $v_{(\zeta_q-1)}(\zeta_q^i-\zeta_q)=1$ car, comme on l'a plusieurs fois remarqué, p ne divise pas $i-1$. Par ailleurs par construction on a :

$$v_{(\zeta_q-1)}(h\beta_{c'}) = \phi(q)v_p(h) + c'p^{v_p(b(i^2)-b(i))}$$

et donc :

$$1 = \phi(q)v_p(h) + c'p^{v_p(b(i^2)-b(i))}.$$

Supposons par l'absurde $v_p(b(i^2)-b(i)) \geq 1$; puisque p^2 divise q, on obtient la contradiction $1 \equiv 0 \mod (p)$. Donc $v_p(b(i^2)-b(i))=0$ et la relation précédente

devient :

$$1 = \phi(q)v_p(h) + c'.$$

Si $v_p(h) \neq 0$, on a $|\phi(q)v_p(h)| \geq \phi(q)$ alors que $1 \leq c' \leq \phi(q)$; donc on obtient la contradiction $\phi(q)v_p(h) + c' \neq 1$. On a donc $v_p(h) = 0$ et $c' = 1$. Par la relation (13) on a alors :

$$(b(i^2) - b(i))d \equiv ib(i) - b(i^2) \mod (q) \tag{14}$$

et, en multipliant par i,

$$(i+1)b(i^2) \equiv (i^2+1)b(i) \mod (q). \tag{15}$$

Cette dernière relation montre que $b(i^2)$ est déterminé modulo q en fonction de $b(i)$ (puisque $i \not\equiv -1 \mod (p)$, voir la remarque 1) et que $b(i) \not\equiv 0 \mod (p)$ (car sinon $b(i^2) \equiv 0 \mod (p)$ et donc $v_p(b(i^2) - b(i)) \geq 1$).

Soit maintenant $n \in \mathbb{Z}$ tel que $(i+1)n \equiv b(i) \mod (q)$. Alors p ne divise pas n, donc ζ_q^n est un générateur de $\mathbb{Z}[\zeta_q]$ et $\zeta_q^n \sim \zeta_q$. De plus :

$$\frac{\zeta_q^{in} - \zeta_q^n}{\overline{\zeta_q^{in}} - \overline{\zeta_q^n}} = -\zeta_q^{n(i+1)} = -\zeta_q^{b(i)}$$

et donc :

$$b(i, \zeta_q^n) \equiv b(i) \mod (q). \tag{16}$$

Puisque, comme nous venons de le remarquer, ζ_q^n est un générateur de $\mathbb{Z}[\zeta_q]$ et que $\zeta_q^n + \overline{\zeta_q^n}$ n'est évidemment pas un entier, $b(i, \zeta_q^n)$ et $b(i^2, \zeta_q^n)$ satisfont la relation (15). Par conséquent nous obtenons :

$$\begin{aligned}(i+1)b(i^2, \zeta_q^n) &\equiv (i^2+1)b(i, \zeta_q^n) \mod (q) \quad \text{par } (15) \\ &\equiv (i^2+1)b(i, \alpha) \mod (q) \quad \text{par } (16) \\ &\equiv (i+1)b(i^2, \zeta_q^n) \mod (q) \quad \text{par } (15).\end{aligned}$$

Donc :

$$b(i^2, \zeta_q^n) \equiv b(i^2) \mod (q). \tag{17}$$

Mais alors, puisque $b(i, \alpha) \not\equiv 0 \mod (q)$ et par les relations (16) et (17), nous pouvons appliquer la proposition 1 et nous obtenons

$$\alpha \sim \zeta_q^n \sim \zeta_q.$$

□

Références

[1] A. Bremner, On power bases in cyclotomic number fields, J. of Number Theory 28 (1988) 288-298.

[2] I. Gaál, Diophantine equations and power integral bases. New computational methods, Birkhauser, Boston, (2002).

[3] I. Gaál, L. Robertson, Power integral bases in prime-power cyclotomic fields, J. of Number Theory 120 (2006) 372-384.

[4] M. N. Gras, Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$, J. of Number Theory 23, (1986) 347-353.

[5] K. Györy, Sur les polynômes à coefficients entiers et de discriminant donné III, Publ. Math. Debrecen 23, (1976) 141-165.

[6] K. Györy, Corps de nombres algébriques d'anneau d'entiers monogène, Séminaire Delange-Pisot-Poitou 26, Paris (1978-1979).

[7] L. Robertson, Power bases for cyclotomic integer rings, J. of Number Theory 69 (1998) 98-118.

[8] L. Robertson, Power bases for 2-power cyclotomic fields, J. of Number Theory 88 (2001) 196-209.

[9] L. C. Washinghton, Introduction to cyclotomic fields, second ed., Springer-Verlag, New York, 1997.