Vers un théorème de Cobham pour les entiers de Gauss

Georges Hansel Taoufik Safer*

Résumé

Soient p et q deux entiers positifs distincts et soient $\alpha = -p+i$ et $\beta = -q+i$. Sous l'hypothèse que *la conjecture des quatre exponentielles* est vraie, nous montrons que si un ensemble S d'entiers de Gauss est (α, β)-reconnaissable, alors il est syndétique.

Abstract

Let p and q be two distinct positive integers and let $\alpha = -p + i$ and $\beta = -q + i$. Assuming that *the four exponentials conjecture* is true, it is shown that if a set S of Gaussian integers is (α, β)-recognizable, then it is syndetic.

1 Introduction

Soit $p > 1$ un nombre entier ; un sous-ensemble S de l'ensemble $\mathbf{N}$ des entiers naturels est dit *p-reconnaissable* si l'ensemble des mots sur l'alphabet $\{0, 1, \cdots, p-1\}$ qui représentent les éléments de S en base p est une partie reconnaissable du monoïde libre $\{0, 1, \cdots, p-1\}^*$. En 1969, A. Cobham [5] a démontré le résultat fondamental suivant : *Soient p et q deux entiers supérieurs à* 1 *multiplicativement indépendants, (c'est-à-dire tels qu'il n'existe pas de relation de la forme $p^m = q^n$ avec m, n entiers non nuls) et soit S une partie de $\mathbf{N}$. L'ensemble S est à la fois p-reconnaissable et*

*Recherche supportée par le Fonds autrichien pour la promotion de la recherche scientifique (FWF), projet numéro Y96-MAT.

1991 *Mathematics Subject Classification :* 68R15, 68Q45, 11B85.

Key words and phrases : Cobham theorem, automata, p-recognizability, complex bases, four exponentials conjecture.

q-reconnaissable si et seulement si S est ultimement périodique (ou, ce qui revient au même, est, à un ensemble fini près, une réunion finie de progressions arithmétiques).

De nombreux travaux ont été effectués par la suite pour simplifier la démonstration initiale de ce résultat, la généraliser à plusieurs dimensions ou à des systèmes de numération non entiers. On pourra trouver les références de la plupart de ces travaux dans les articles de synthèse [2] et [4].

De manière informelle, la question à l'origine du présent travail est la suivante : y a-t-il un "théorème de Cobham" pour l'ensemble $\mathbf{G}$ des entiers de Gauss, c'est-à-dire l'ensemble des nombres complexes de la forme $a+bi$, $a,b \in \mathbf{Z}$? Précisons-en les termes.

Ainsi que le montrent Kátai et Szabó [9], les seuls systèmes de numération naturels pour les entiers de Gauss sont ceux où la base est de la forme $-p+i$ (ou $-p-i$), avec p entier positif, l'ensemble des chiffres intervenant dans la représentation étant $\{0, 1, \cdots, p^2\}$. Comme on le verra, deux telles bases $\alpha = -p+i$ et $\beta = -q+i$ sont toujours multiplicativement indépendantes. Nous conjecturons alors l'énoncé suivant : *une partie S de $\mathbf{G}$ est à la fois α-reconnaissable et β-reconnaissable si et seulement si c'est une partie périodique de $\mathbf{G}$, à un ensemble fini près*. Signalons qu'un cas particulier de cette conjecture, à savoir $\alpha = -1+i$ et $\beta = -q+i$ est contenu dans la question 9.7 posée par Allouche et *al.* dans [1].

Une direction de cet énoncé est aisée à démontrer (cf. ci-après le théorème 2) : une partie périodique de $\mathbf{G}$ est α-reconnaissable dans toute base complexe $\alpha = -p+i$. La difficulté se concentre donc sur l'autre direction et le but du présent travail est d'obtenir un résultat partiel dans cette voie, résultat dont l'énoncé est suggéré par la manière dont s'obtient le théorème initial de Cobham.

En effet dans toutes les démonstrations connues, le théorème de Cobham s'obtient essentiellement en deux étapes. La première consiste à montrer qu'une partie infinie (p,q)-reconnaissable de $\mathbf{N}$, où p et q sont multiplicativement indépendants, est une partie *syndétique* de $\mathbf{N}$, c'est-à-dire une partie pour laquelle il existe $r \in \mathbf{N}$, tel que $S \cap [n, n+r] \neq \emptyset$ pour tout $n \in \mathbf{N}$. L'équivalent pour les entiers de Gauss s'énonce : *une partie S infinie (α, β)-reconnaissable de $\mathbf{G}$ est syndétique*, c'est-à-dire qu'il existe $r > 0$ telle que toute boule de $\mathbf{C}$ de rayon r rencontre S. Tel est l'énoncé (théorème 3) que nous établissons ici **sous réserve** de la validité d'une conjecture classique de théorie des nombres.

Expliquons cette "réserve". Dans la démonstration du théorème de Cobham, l'indépendance multiplicative des deux bases p et q intervient par le biais de la propriété suivante qui en découle aisément : l'ensemble des rapports p^m/q^n, m,n entiers positifs, est dense dans $\mathbf{R}^+$. Or nous ignorons si la propriété correspondante pour $\mathbf{C}$ (l'ensemble des rapports α^m/β^n est dense dans $\mathbf{C}$) est vraie. Dans la section 3 (théorème 1) nous démontrons cette propriété, mais sous l'hypothèse de la validité de la *conjecture des quatre exponentielles* (rappelée dans la section suivante).

Remerciements. Nous remercions vivement Jean-Claude Lootgieter et Michel Waldschmidt pour l'aide précieuse dont ils nous ont fait bénéficier.

2 Notations, définitions, rappels

On désigne par $\mathbf{G}$ l'ensemble des entiers de Gauss, c'est-à-dire l'ensemble des nombres complexes à coordonnées entières $a+bi$, $a, b \in \mathbf{Z}$. La *norme* de l'entier $a+bi$ est le nombre $N(a+bi) = a^2 + b^2$. Le module de $a+bi$ est noté $|a+bi| = \sqrt{a^2+b^2}$. Soient x et y deux entiers de Gauss. L'anneau $\mathbf{G}$ est euclidien et il existe deux entiers de Gauss q et r (non nécessairement uniques) tels que

$$\begin{aligned} &x = qy + r \\ &N(r) < N(y) \end{aligned}$$

Soit $\alpha = -p + i$, où p est un entier positif ; Kátai et Szabó [9] montrent que le nombre α est base d'un système de numération au sens suivant : pour tout entier de Gauss non nul x, il existe une suite unique d'entiers $\varepsilon_k\varepsilon_{k-1}\ldots\varepsilon_0$ vérifiant les conditions

$$\begin{aligned} &x = \sum_{j=0}^{k} \varepsilon_j \alpha^j \\ &0 \leq \varepsilon_j \leq p^2, j = 0, \ldots, k, \text{ avec } \varepsilon_k \neq 0 \end{aligned}$$

Le mot $\rho_\alpha(x) = \varepsilon_k\varepsilon_{k-1}\ldots\varepsilon_0$ sur l'alphabet $A_\alpha = \{0, 1, \ldots, p^2\}$ est la *représentation de x dans la base complexe α*. On note $l_\alpha(x)$ la *longueur* de $\rho_\alpha(x)$, soit ici $l_\alpha(x) = k+1$. L'ensemble des entiers de Gauss x tels que $l_\alpha(x) \leq k$ est noté G_k. Un calcul simple montre que pour tout $x \in G_k$, on a $|x| \leq 2|\alpha|^{k+1}$.

Inversement soit un mot $u = \varepsilon_k \ldots \varepsilon_0 \in A_\alpha^*$. On note $\omega_\alpha(u)$ la *valeur* de u en base α, c'est-à-dire l'entier de Gauss x donné par la formule (1).

Le résultat suivant sur la longueur de la représentation d'un entier de Gauss nous sera utile par la suite.

Proposition 1 (Grabner et *al.* [7]). *Il existe une constante C_α telle que pour tout $z \in G$,*

$$l_\alpha(z) \leq \log_{|\alpha|} |z| + C_\alpha.$$

Une autre propriété importante des bases complexes $-p+i$ est leur *indépendance multiplicative*. Soient $x, y \in \mathbf{G} \setminus \{0\}$; on dit que x et y sont *multiplicativement indépendants* s'il n'existe pas deux entiers m et n non nuls tels que $x^m = y^n$.

Proposition 2. *Deux bases distinctes $-p+i$ et $-q+i$ sont multiplicativement indépendantes.*

Preuve. Nous utilisons un résultat partiel de V. A. Lebesgue [10] sur la conjecture (récemment démontrée par P. Mihailescu (cf. [11], [3])) de Catalan (1844), selon laquelle l'équation $X^k - Y^l = 1$ n'a pas d'autres solutions entières que $3^2 - 2^3 = 1$: en 1850, Lebesgue a démontré cette conjecture pour $l = 2$.

Supposons qu'on ait une relation de la forme $(-p+i)^m = (-q+i)^n$. On en déduit une relation de la forme $(p^2+1)^m = (q^2+1)^n$ dans laquelle on peut supposer que m et n sont premiers entre eux. En considérant les décompositions de p^2+1 et de q^2+1 en facteurs premiers, on obtient qu'il existe un entier u tel que $p^2+1 = u^n$, contrairement au résultat de Lebesgue. ∎

Un “résultat” important de théorie des nombres, qui à ce jour est encore une conjecture, est la *conjecture des quatres exponentielles* (voir par exemple [12]). Les résultats démontrés dans la suite sont conditionnés par la validité de cette conjecture.

Conjecture. Soient $\{\lambda_1, \lambda_2\}$ et $\{x_1, x_2\}$ deux paires de nombres complexes formées chacune de deux nombres rationnellement indépendants (c'est-à-dire linéairement indépendants sur le corps $\mathbf{Q}$ des rationnels). Alors, l'un des quatres nombres

$$e^{\lambda_1 x_1} \quad e^{\lambda_1 x_2} \quad e^{\lambda_2 x_1} \quad e^{\lambda_2 x_2}$$

est transcendant.[1]

3 Bases complexes et densité

Soient p et q deux nombres entiers (supérieurs à 1) multiplicativement indépendants. Il est bien connu (et facile de montrer) que l'ensemble des rapports $\{p^m/q^n \mid m, n \in \mathbf{N}\}$ est une partie dense de $\mathbf{R}^+$. La propriété correspondante dans $\mathbf{C}$ pour les bases complexes reste un problème ouvert. Dans cette section, nous montrons qu'elle est satisfaite si on suppose vraie la conjecture des quatres exponentielles.

Plus précisément soient $\alpha = -p + i = ae^{i\theta}$ et $\beta = -q + i = be^{i\varphi}$, deux bases complexes distinctes (notées également sous forme trigonométrique). On considère l'ensemble $P_{\alpha,\beta}$ des rapports des puissances de ces deux bases, soit

$$P_{\alpha,\beta} = \left\{ \frac{\alpha^m}{\beta^n} \mid m, n \in \mathbf{N} \right\}. \tag{1}$$

Nous allons montrer que l'ensemble $P_{\alpha,\beta}$ est une partie dense de $\mathbf{C}$.

Lemme 1. *L'ensemble $P_{\alpha,\beta}$ est dense dans $\mathbf{C}$ si les nombres*

$$\frac{\ln b}{\ln a}, \quad \frac{\theta}{2\pi}\frac{\ln b}{\ln a} - \frac{\varphi}{2\pi}, \quad 1$$

sont rationnellement indépendants.

Preuve. L'ensemble $P_{\alpha,\beta}$ est dense dans $\mathbf{C}$ si et seulement si tout nombre complexe $ce^{i\psi}$ est limite d'une suite d'éléments de $P_{\alpha,\beta}$, c'est-à-dire

$$\lim_{k\to\infty} \frac{(ae^{i\theta})^{m_k}}{(be^{i\varphi})^{n_k}} = ce^{i\psi}, \tag{2}$$

pour une certaine suite double d'entiers positifs $(m_k, n_k)_{k\in\mathbf{N}}$.

Le cas $c = 0$ est évident, puisque

$$\lim_{n\to\infty} \frac{1}{(be^{i\varphi})^n} = 0$$

[1] Cette conjecture est elle-même dérivée d'une généralisation du septième problème de Hilbert : des logarithmes de nombres algébriques rationnellement indépendants sont-ils algébriquement indépendants ?

On suppose donc $c \neq 0$. En séparant modules et arguments et en passant aux logarithmes, l'égalité (2) est équivalente aux deux conditions

$$\lim_{k\to\infty} \Big(m_k \ln a - n_k \ln b \Big) = \ln c, \tag{3}$$

$$\lim_{k\to\infty} \Big(m_k \frac{\theta}{2\pi} - n_k \frac{\varphi}{2\pi} \Big) = \frac{\psi}{2\pi} \pmod 1. \tag{4}$$

Les conditions (3) et (4) peuvent encore s'écrire

$$\lim_{k\to\infty} \Big(m_k - n_k \frac{\ln b}{\ln a} \Big) = \frac{\ln c}{\ln a}, \tag{5}$$

$$\lim_{k\to\infty} \Big(\Big(n_k \frac{\ln b}{\ln a} + \frac{\ln c}{\ln a} \Big) \frac{\theta}{2\pi} - n_k \frac{\varphi}{2\pi} \Big) = \frac{\psi}{2\pi} \pmod 1. \tag{6}$$

L'existence de la suite double $(m_k, n_k)_{k\in\mathbf{N}}$ vérifiant (5) et (6) est encore équivalente à celle d'une suite d'entiers positifs $(n_k)_{k\in\mathbf{N}}$ telle que

$$\lim_{k\to\infty} n_k \frac{\ln b}{\ln a} = -\frac{\ln c}{\ln a} \pmod 1,$$

$$\lim_{k\to\infty} n_k \Big(\frac{\theta}{2\pi} \frac{\ln b}{\ln a} - \frac{\varphi}{2\pi} \Big) = \frac{\psi}{2\pi} - \frac{\ln c}{\ln a} \frac{\theta}{2\pi} \pmod 1$$

En vertu du théorème de Kronecker ([8], théorème 443), une telle suite $(n_k)_{k\in\mathbf{N}}$ existe si les nombres

$$\frac{\ln b}{\ln a}, \quad \frac{\theta}{2\pi} \frac{\ln b}{\ln a} - \frac{\varphi}{2\pi}, \quad 1$$

sont rationnellement indépendants. ■

Lemme 2. *Si la "conjecture des* 4 *exponentielles" est vraie, alors les nombres*

$$\frac{\ln b}{\ln a}, \quad \frac{\theta}{2\pi} \frac{\ln b}{\ln a} - \frac{\varphi}{2\pi}, \quad 1$$

sont rationnellement indépendants.

Preuve. Supposons qu'ils ne le sont pas. Il existe alors des entiers r, s et t tels que

$$r \frac{\ln b}{\ln a} + s \Big(\frac{\theta}{2\pi} \frac{\ln b}{\ln a} - \frac{\varphi}{2\pi} \Big) - t = 0$$

Utilisant cette égalité, on définit λ par

$$\lambda = \frac{s\theta + 2\pi r}{\ln a} = \frac{s\varphi + 2\pi t}{\ln b}$$

En multipliant par i et en passant aux exponentielles, on a

$$\begin{cases} e^{is\theta} = e^{i\lambda \ln a} \\ e^{is\varphi} = e^{i\lambda \ln b} \end{cases}$$

Appliquons la conjecture des 4 exponentielles avec les nombres

$$\lambda_1 = i\lambda \quad \lambda_2 = 1 \quad x_1 = \ln a \quad x_2 = \ln b,$$

l'indépendance linéaire de $\ln a$ et $\ln b$ sur $\mathbf{Q}$ étant une conséquence du fait que p^2+1 et q^2+1 sont multiplicativement indépendants.

On en déduit que l'un des nombres

$$e^{i\lambda \ln a} \quad e^{i\lambda \ln b} \quad e^{\ln a} \quad e^{\ln b}$$

est transcendant. Donc évidemment, ou bien $e^{i\lambda \ln a}$, ou bien $e^{i\lambda \ln b}$ est transcendant. Donc, ou bien $e^{is\theta}$, ou bien $e^{is\varphi}$, est transcendant, ce qui est absurde, puisque

$$e^{is\theta} = \left(\frac{-p+i}{\sqrt{p^2+1}}\right)^s \qquad \text{et} \qquad e^{it\varphi} = \left(\frac{-q+i}{\sqrt{q^2+1}}\right)^t.$$

■

Des lemmes 1 et 2 on déduit immédiatement le

Théorème 1. *Soient $\alpha = -p+i$ et $\beta = -q+i$ deux bases complexes distinctes. Si la “conjecture des 4 exponentielles” est vraie, alors l'ensemble*

$$P_{\alpha,\beta} = \left\{\frac{\alpha^m}{\beta^n} \mid m,n \in \mathbf{N}\right\}.$$

est dense dans le plan complexe $\mathbf{C}$.

Remarque. Les nombres c et ψ étant donnés, les conditions (3) et (4) du lemme 1 sont vérifiées séparément sans faire appel à la conjecture des quatre exponentielles (la difficulté est de les obtenir simultanément). La condition (3) résulte déjà de ce que les nombres $\ln a$ et $\ln b$ sont rationnellement indépendants.

De son côté, la condition (4) découle simplement du fait que

$$\frac{\theta}{2\pi} = \frac{\arctan(-1/p)}{2\pi}$$

n'est rationnel que pour $p=1$, et, par conséquent, l'un des deux ensembles

$$\left\{n\frac{\theta}{2\pi} \pmod 1 \mid n \in \mathbf{N}\right\} \quad \text{ou} \quad \left\{n\frac{\varphi}{2\pi} \pmod 1 \mid n \in \mathbf{N}\right\}$$

est dense dans $[0,1]$.

4 Parties α-reconnaissables

Soit $\alpha = -p+i$ une base complexe ; une partie $S \subset \mathbf{G}$ est *α-reconnaissable* si l'ensemble des représentations de ses éléments $\rho_\alpha(S) = \{\rho_\alpha(x) \mid x \in S\}$ est une partie reconnaissable du monoïde libre A_α^*. Par conséquent, l'ensemble S est α-reconnaissable si et seulement si la relation d'équivalence $\mathcal{R}_S^\alpha$ sur A_α^* définie par

$$u\mathcal{R}_S^\alpha v \Leftrightarrow \big(\forall w \in A_\alpha^* : uw \in \rho_\alpha(S) \Leftrightarrow vw \in \rho_\alpha(S)\big)$$

est d'indice fini (cf. [6]).

Comme l'application $x \to \rho_\alpha(x)$ est une bijection de $\mathbf{G} \setminus \{0\}$ sur $(A_\alpha \setminus \{0\})A_\alpha^*$, il revient au même de dire que la relation d'équivalence sur $\mathbf{G}$ notée également $\mathcal{R}_S^\alpha$ et définie par

$$x\mathcal{R}_S^\alpha y \Leftrightarrow \forall w \in A_\alpha^* : \rho_\alpha(x)w \in \rho_\alpha(S) \Leftrightarrow \rho_\alpha(y)w \in \rho_\alpha(S)$$

est d'indice fini.

Proposition 3. *Soit $S \subset \mathbf{G}$ et soient x et y deux entiers de Gauss. Les conditions suivantes sont équivalentes :*

1) $x\mathcal{R}_S^\alpha y$

2) *Pour tout $j \in \mathbf{N}$ et tout $t \in G_j$,*

$$x\alpha^j + t \in S \Leftrightarrow y\alpha^j + t \in S$$

Preuve. 1) $\Rightarrow$ 2) Soient $j \in \mathbf{N}$ et $t \in G_j$ tels que $x\alpha^j + t \in S$. On a

$$\rho_\alpha(x\alpha^j + t) = \rho_\alpha(x)0^m\rho_\alpha(t) \in \rho_\alpha(S)$$

où $m = j - l_\alpha(t)$. Comme $x\mathcal{R}_S^\alpha y$, on a $\rho_\alpha(y)0^m\rho_\alpha(t) \in \rho_\alpha(S)$ et donc $y\alpha^j + t \in S$.

2) $\Rightarrow$ 1) Soit $w \in A_\alpha^*$ tel que $\rho_\alpha(x)w \in \rho_\alpha(S)$. Alors $x\alpha^{|w|} + \omega_\alpha(w) \in S$. Par hypothèse, $y\alpha^{|w|} + \omega_\alpha(w) \in S$ et donc $\rho_\alpha(y)w \in \rho_\alpha(S)$ et par conséquent $x\mathcal{R}_S^\alpha y$. ∎

Une partie $S \subset \mathbf{G}$ est *périodique* s'il existe une *période* $\sigma \in \mathbf{G}$ telle que

$$\forall g \in \mathbf{G} : s \in S \Leftrightarrow s + g\sigma \in S \tag{7}$$

Une partie $S \subset \mathbf{G}$ est *ultimement périodique* s'il existe $\sigma \in \mathbf{G}$ et une partie finie F de $\mathbf{G}$ tels que la relation (7) est vérifiée lorsque s et $s + g\sigma$ n'appartiennent pas à F.

Théorème 2. *Toute partie ultimement périodique S de $\mathbf{G}$ est α-reconnaissable pour toute base complexe $\alpha = -p + i$, $p \in \mathbf{N} \setminus \{0\}$.*

Preuve. On peut supposer que S est périodique.

1) Soit σ une période de S et soient x et y deux entiers de Gauss égaux modulo σ. Montrons qu'alors $x\mathcal{R}_S^\alpha y$.

Soient $j \in \mathbf{N}$ et $t \in G_j$ tels que $x\alpha^j + t \in S$. Soit $g \in \mathbf{G}$ tel que $y = x + g\sigma$. Comme S a pour période σ,

$$y\alpha^j + t = x\alpha^j + t + g\alpha^j\sigma \in S$$

et donc $x\mathcal{R}_S^\alpha y$.

2) Pour tout $x \in \mathbf{G}$, il existe un quotient q et un reste r d'une division euclidienne de x par σ tels que $x = q\sigma + r$ avec $N(r) < N(\sigma)$. Deux entiers de Gauss x et y ayant le même reste r dans une telle division sont égaux modulo σ. Le nombre des classes modulo σ est donc fini et par conséquent, d'après 1), la relation d'équivalence $\mathcal{R}_S^\alpha$ est d'indice fini et S est α-reconnaissable. ∎

Proposition 4. *Soit S une partie α-reconnaissable de* $\mathbf{G}$ *et soit* $g \in \mathbf{G}$.
1) *L'ensemble* $S - g = \{s - g \mid s \in S\}$ *est α-reconnaissable.*
2) *L'ensemble* $S/g = \{x \in \mathbf{G} \mid gx \in S\}$ *est α-reconnaissable.*

Preuve. On note $|\mathcal{R}_S^\alpha|$ l'indice de la relation $\mathcal{R}_S^\alpha$.
1) Soient x et y deux entiers de Gauss tels que $(x+z)\mathcal{R}_S^\alpha(y+z)$ pour tout $z \in \mathbf{G}$ dont le module est majoré par $|g| + 4|\alpha|$. Nous allons montrer qu'alors on a $x\mathcal{R}_{S-g}^\alpha y$, ce qui entraîne que la relation d'équivalence $\mathcal{R}_{S-g}^\alpha$ est d'indice fini (majoré par $|\mathcal{R}_S^\alpha|^{4(|g|+4|\alpha|)^2}$) et donc que $S - g$ est reconnaissable.
Soit $j \in \mathbf{N}$ et $t \in G_j$ tels que

$$x\alpha^j + t \in S - g \tag{8}$$

Il existe $z \in \mathbf{G}$ et $s \in G_j$ tels que

$$t + g \quad = \quad z\alpha^j + s \tag{9}$$

De (9) résulte que

$$|z\alpha^j| \leq |g| + |s| + |t| \leq |g| + 2 \times 2|\alpha^{j+1}|$$

de sorte que $|z| \leq |g| + 4|\alpha|$.
De (8) et (9) résulte que

$$(x+z)\alpha^j + s \in S$$

et donc, par hypothèse sur y,

$$(y+z)\alpha^j + s \in S$$

soit encore $y\alpha^j + t \in S - g$ et par conséquent $x\mathcal{R}_{S-g}y$.
2) Soient x et y deux entiers de Gauss tels que $(xg+z)\mathcal{R}_S^\alpha(yg+z)$ pour tout $z \in \mathbf{G}$ dont le module est majoré par $2(|g|+1)|\alpha|$. Nous allons montrer qu'alors on a $x\mathcal{R}_{S/g}y$, ce qui entraîne que la relation d'équivalence $\mathcal{R}_{S/g}$ est d'indice fini (majoré par $|\mathcal{R}_S|^{4(2(|g|+1)|\alpha|)^2}$) et donc que S/g est reconnaissable.
Soit $j \in \mathbf{N}$ et $t \in G_j$ tels que

$$x\alpha^j + t \in S/g \tag{10}$$

Il existe $z \in \mathbf{G}$ et $s \in G_j$ tels que

$$gt \quad = \quad z\alpha^j + s \tag{11}$$

De (11) résulte que

$$|z\alpha^j| \leq |gt| + |s| \leq 2(|g|+1)|\alpha^{j+1}|$$

de sorte que $|z| \leq 2(|g|+1)|\alpha|$.
De (10) et (11) résulte que

$$(xg+z)\alpha_j + s \in S \tag{12}$$

et donc, par hypothèse sur y,

$$(yg+z)\alpha_j + s \in S$$

soit encore $y\alpha^j + t \in S/g$ et par conséquent $x\mathcal{R}_{S/g}y$. ∎

Proposition 5. *Soit S une partie de $\mathbf{G}$. La relation $\mathcal{R}_S^\alpha$ est "stable" au sens suivant : on a l'implication*

$$x\mathcal{R}_S^\alpha y \Rightarrow \forall j \in \mathbf{N}, \forall t \in G_j : (x\alpha^j + t)\mathcal{R}_S^\alpha(y\alpha^j + t)$$

Preuve. Soient x, y avec $x\mathcal{R}_S^\alpha y$. Soit $j, k \in \mathbf{N}$, $t \in G_j$ et $s \in G_k$. Supposons que

$$(x\alpha^j + t)\alpha^k + s \in S$$

Cela s'écrit encore

$$x\alpha^{j+k} + (t\alpha^k + s) \in S$$

Comme $t\alpha^k + s \in G_{j+k}$, on a

$$y\alpha^{j+k} + (t\alpha^k + s) \in S$$

soit encore

$$(y\alpha^j + t)\alpha^k + s \in S$$

et donc $(x\alpha^j + t)\mathcal{R}_S^\alpha(y\alpha^j + t)$. ∎

Proposition 6. *Soit S une partie infinie α-reconnaissable de $\mathbf{G}$. Il existe deux nombres complexes a et b et un entier $k \in \mathbf{N}$ tels que pour tout $n \in \mathbf{N}$,*

$$a\alpha^{nk} + b \in S$$

Preuve. La démonstration est du type de celle du "lemme de l'étoile" [6]. Soit $x \in S$ tel que $l_\alpha(x) > |\mathcal{R}_S^\alpha|$. La représentation $\rho_\alpha(x)$ peut se factoriser sous la forme $\rho_\alpha(x) = uvw$ avec la condition $u\mathcal{R}_S^\alpha uv$. Par conséquent pour tout $n \in \mathbf{N}$, on a $uv^n w \in \rho_\alpha(S)$. Posons $z_n = \omega_\alpha(uv^n w)$, $n \in N$. On a

$$z_n = \omega_\alpha(w) + \alpha^{|w|}\omega_\alpha(v)\sum_{j=0}^{n-1}\alpha^{j|v|} + \alpha^{|w|+n|v|}\omega_\alpha(u)$$

Un calcul simple montre que $z_n = a\alpha^{nk} + b$ avec $k = |v|$, $a = \alpha^{|w|}(\frac{\omega_\alpha(v)}{\alpha^k - 1} + \omega_\alpha(u))$ et $b = \omega_\alpha(w) - \alpha^{|w|}(\frac{\omega_\alpha(v)}{\alpha^k - 1})$. ∎

5 Parties (α, β)-reconnaissables

Dans cette section, on se donne deux bases distinctes $\alpha = -p + i$ et $\beta = -q + i$ et S une partie infinie de $\mathbf{G}$ reconnaissable dans ces deux bases. Nous supposons que la *conjecture des quatre exponentielles* est vraie.

Proposition 7. *Soit $S' \subset \mathbf{G}$ une classe d'équivalence de la relation $\mathcal{R}_S^\alpha$. Alors S' est reconnaissable dans les deux bases α et β.*

Preuve. 1) Montrons que S' est α-reconnaissable. Il suffit de montrer que la relation $\mathcal{R}_S^\alpha$ est plus fine que la relation $\mathcal{R}_{S'}^\alpha$.

Soient $x, y \in \mathbf{G}$ avec $x\mathcal{R}_S^\alpha y$. Soient $j \in \mathbf{N}$ et $t \in G_j$ tels que $x\alpha^j + t \in S'$. D'après la proposition 5, on a $(y\alpha^j + t)\mathcal{R}_S^\alpha(x\alpha^j + t)$ et comme S' est une classe de $\mathcal{R}_S^\alpha$, on a $y\alpha^j + t \in S'$, et donc $x\mathcal{R}_{S'}^\alpha y$. Par conséquent S' est α-reconnaissable.

2) Montrons que S' est β-reconnaissable. Soit $x_0 \in S'$ et soient $x_1, \ldots, x_m$, des représentants des autres classes de la relation $\mathcal{R}_S^\alpha$. Pour tout $j = 1, 2, \ldots, m$, puisque x_0 et x_j n'appartiennent pas à la même classe, il existe $k_j \in \mathbf{N}$ et $t_j \in G_{k_j}$ tels que, ou bien $x_0\alpha^{k_j} + t_j \in S$ et $x_j\alpha^{k_j} + t_j \notin S$, ou bien $x_0\alpha^{k_j} + t_j \notin S$ et $x_j\alpha^{k_j} + t_j \in S$. Pour tout $j = 1, \ldots, m$, posons

$$S_j = \begin{cases} \{x \in \mathbf{G} \mid x\alpha^{k_j} + t_j \in S\} & \text{si } x_0\alpha^{k_j} + t_j \in S \\ \{x \in \mathbf{G} \mid x\alpha^{k_j} + t_j \in \mathbf{G} \setminus S\} & \text{sinon} \end{cases}$$

La classe S' est donc définie par

$$S' = \bigcap_{j=1}^{m} S_j$$

Comme S est β-reconnaissable, il en est de même de $\mathbf{G} \setminus S$ et par conséquent, en vertu de la proposition 4, S_j est β-reconnaissable pour tout $j = 1, \ldots, m$. Donc S' est β-reconnaissable. ∎

Proposition 8. *Soit S' une classe d'équivalence infinie de la relation $\mathcal{R}_S^\alpha$ et soit $d \in \mathbf{N} \setminus \{0\}$. Il existe un ensemble fini d'entiers positifs F_d tel que pour tout $x \in \mathbf{G}$, il existe $\lambda \in F_d$ et $t \in G_{\lambda d}$ tels que*

$$x\alpha^{\lambda d} + t \in S'$$

Preuve. 1) Montrons d'abord que pour tout $x \in \mathbf{G}$, il existe $\lambda \in \mathbf{N}$ et $t \in G_{\lambda d}$ tels que

$$x\alpha^{\lambda d} + t \in S'$$

D'après la proposition 6, comme S' est β-reconnaissable (proposition 7), il existe $a, b \in \mathbf{C}$ et $k \in \mathbf{N}$ tels que pour tout $n \in \mathbf{N}$,

$$a\beta^{nk} + b \in S'$$

Soit $\varepsilon > 0$. Comme α et β sont multiplicativement indépendants, il en est de même de α^d et β^k et on peut donc, d'après le théorème 1, trouver deux entiers positifs n et λ tels que

$$\frac{a\beta^{nk} + b}{\alpha^{\lambda d}} \in B(x, \varepsilon)$$

où l'on note $B(x, \varepsilon)$ la boule de centre x et de rayon ε pour la norme euclidienne de $\mathbf{C}$. Par conséquent

$$|a\beta^{nk} + b - x\alpha^{\lambda d}| \leq \varepsilon|\alpha^{\lambda d}|$$

En vertu de la proposition 1, on a

$$l_\alpha(a\beta^{nk} + b - x\alpha^{\lambda d}) \leq \lambda d + \log_{|\alpha|} \varepsilon + C_\alpha$$

Donc si ε est choisi assez petit

$$t = a\beta^{nk} + b - x\alpha^{\lambda d} \in G_{\lambda d}$$

2) D'après la proposition 7, S' est α-reconnaissable. Soit $x_1, x_2, \ldots, x_m$ un système de représentants de la relation $\mathcal{R}^{\alpha}_{S'}$ et soient

$$\lambda_1, \ldots, \lambda_m \in \mathbf{N} \text{ et } t_1, \ldots, t_m \in G_{\lambda d}$$

des nombres associés dont l'existence est assurée par ce qui précède. Soit $x \in \mathbf{G}$; soit j tel que $x\mathcal{R}^{\alpha}_{S'}x_j$. Comme $x_j\alpha^{\lambda_j d}+t_j \in S'$, on a aussi $x\alpha^{\lambda_j d}+t_j \in S'$. L'ensemble

$$F_d = \{\lambda_1, \ldots, \lambda_m\}$$

satisfait donc à la condition voulue. ■

Proposition 9. *Soit S' une classe d'équivalence infinie de la relation $\mathcal{R}^{\alpha}_{S}$. Il existe $k \in \mathbf{N}$ et $t \in G_k$ tels que $S'\alpha^k + t \subset S'$.*

Preuve. Soit $x \in S'$; d'après la proposition 8 appliquée avec $d = 1$, il existe $k \in \mathbf{N}$ et $t \in G_k$ tels que

$$x\alpha^k + t \in S'$$

Soit $y \in S'$; on a $y\mathcal{R}^{\alpha}_{S}x$, donc, d'après la proposition 5, on a $(y\alpha^k + t)\mathcal{R}^{\alpha}_{S}(x\alpha^k + t)$ et par conséquent $y\alpha^k + t \in S'$. Donc $S'\alpha^k + t \subset S'$. ■

Théorème 3. *Supposons vraie la conjecture des quatre exponentielles. Soient $\alpha = -p + i$ et $\beta = -q + i$ deux bases complexes différentes et soit S une partie infinie (α, β)-reconnaissable de $\mathbf{G}$; alors S est syndétique.*

Preuve. Soit S' une classe d'équivalence infinie de la relation $\mathcal{R}^{\alpha}_{S}$ contenue dans S. Il suffit de montrer que S' est syndétique.

D'après la proposition 9, il existe $k \in \mathbf{N}$ et $t \in G_k$ tels que

$$S'\alpha^k + t \subset S' \tag{13}$$

Soit F_k l'ensemble fini dont l'existence est assurée par la proposition 8 appliquée avec $d = k$ et posons

$$\overline{\lambda} = \sup\{\lambda \mid \lambda \in F_k\}$$

Soit $x \in \mathbf{G}$; il existe $\lambda \in F_k$ et $t_0 \in G_{\lambda k}$ tels que

$$x\alpha^{\lambda k} + t_0 \in S' \tag{14}$$

Montrons par récurrence que pour tout $n \in \mathbf{N}$, il existe $t_n \in G_{(\lambda+n)k}$ tel que

$$x\alpha^{(\lambda+n)k} + t_n \in S' \tag{15}$$

Pour $n = 0$, t_0 existe d'après (14). Supposons qu'il existe $t_0, t_1, \ldots, t_{n-1}$ vérifiant (15). Il résulte de (13) que

$$(x\alpha^{(\lambda+(n-1))k} + t_{n-1})\alpha^k + t \in S'$$

Comme $t_{n-1} \in G_{(\lambda+(n-1))k}$ et $t \in G_k$, on a $t_{n-1}\alpha^k + t \in G_{(\lambda+n)k}$. La relation (15) est donc vérifiée pour $t_n = t_{n-1}\alpha^k + t$.

Posons $n = \overline{\lambda} - \lambda$; on obtient que pour tout $x \in \mathbf{G}$, il existe $t_x \in G_{\overline{\lambda}k}$ tel que

$$x\alpha^{\overline{\lambda}k} + t_x \in S' \tag{16}$$

Soit $y \in \mathbf{G}$; soient q et r le quotient et le reste d'une division euclidienne de y par $\alpha^{\overline{\lambda}k}$. On a

$$\begin{aligned} y &= q\alpha^{\overline{\lambda}k} + r \\ N(r) &< N(\alpha^{\overline{\lambda}k}) \end{aligned}$$

Or $q\alpha^{\overline{\lambda}k} + t_q \in S'$ et on a

$$|y - (q\alpha^{\overline{\lambda}k} + t_q)| = |r - t_q| < 4|\alpha|^{\overline{\lambda}k+1}$$

Donc pour tout $y \in \mathbf{G}$,

$$B(y, 4|\alpha|^{\overline{\lambda}k+1}) \cap S' \neq \emptyset$$

et par conséquent S' est syndétique. ■

6 Conclusion

Ce travail n'est qu'une première étape vers un théorème de Cobham pour les entiers de Gauss et laisse ouvertes deux questions principales :

a) Peut-on, toujours sous l'hypothèse qu'est vraie la conjecture des quatre exponentielles, montrer qu'un ensemble (α, β)-reconnaissable est non seulement syndétique mais même ultimement périodique ?

b) Peut-on contourner la conjecture des quatre exponentielles pour démontrer que l'ensemble $\left\{ \dfrac{\alpha^m}{\beta^n} \mid m, n \in \mathbf{N} \right\}$ est dense dans $\mathbf{C}$?

Références

[1] J.-P. Allouche, E. Cateland, W.-J. Gilbert, H.-O. Peitgen, J. 0. Shallit, and G. Skordev, Automatic maps on a semiring with digits, *Theory of Computing Systems* **30** (1997), 285-331.

[2] V. Bruyère, G. Hansel, C. Michaux, R. Villemaire, Logic and p-recognizable sets of integers, *Bull. Belg. Math. Soc.* **1** (1994), 191–238.

[3] Y. F. Bilu, Catalan's conjecture (after Mihailescu), *Séminaire Bourbaki*, Exposé 909, 55e année (2002-2003).

[4] V. Bruyère, Automata and numeration systems, *Sém. Lothar. Combin.* **35** (1995) Art. B35b, 19 pages, disponible à `www.mat.univie.ac.at/~slc/wpapers/s35bruyere.pdf`

[5] A. Cobham, On the base-dependence of sets of numbers recognizable by finite automata, *Math. Systems Theory* **3** (1969), 186–192.

[6] S. Eilenberg, *Automata, Languages and Machines*, Vol. A, Academic Press, New-York (1974).

[7] P. Grabner, P. Kirschenhofer and H. Prodinger, The sum-of-digits function for complex bases, *J. London Math. Soc.* (1), **57** (1998), 20-40.

[8] G. B. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford Science Publications, Clarendon Press, Oxford.

[9] I. Kátai and J. Szabó, Canonical number systems for complex integers, *Acta Sci. Math. Hung.* **37** (1975), 255–260.

[10] V. A. Lebesgue, Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$, *Nouv. Ann. de Math.* **9** (1850), 178–181.

[11] P. Mihailescu, Primary units and a proof of Catalan's conjecture, soumis à *Crelle Journal*.

[12] M. Waldschmidt, Diophantine approximation on linear algebraic groups : Transcendence properties of the exponential function in several variables, *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Studies]*, **326** Berlin, New York, Springer, 2000.

Georges Hansel
LIFAR, Université de Rouen
B. P. 67
76130 Mont Saint-Aignan
Email : Georges_Hansel@yahoo.fr

Taoufik Safer
LIAFA, Université Paris-Diderot
Case 7014
2, Place Jussieu
75251 Paris Cedex 05
Email : safer@liafa.jussieu.fr