Corrigendum à l'article
Sur la représentation des entiers par les formes cyclotomiques de grand degré
Bull. Soc. Math. France 148 (2020), no. 2, 253–282.

Étienne Fouvry & Michel Waldschmidt

Au milieu de la page 269 de [**FW**], on donne la liste des homographies, à coefficients rationnels laissant fixe l'ensemble $\mathbb{U}_n$ des racines n–ièmes primitives de l'unité. Cette liste est correcte, elle est d'ailleurs rappelée dans le Lemme 2 ci–dessous, mais la preuve donnée dans [**FW**] est inexacte, puisque partant d'une liste incomplète des homographies, à coefficients complexes fixant le cercle unité $\mathbb{S}^1$ du plan complexe. Notre but est de corriger cette erreur. Nous partons du

Lemme 1. — Soient u_1, u_2, u_3, u_4 des nombres complexes tels que $u_1u_4 - u_2u_3 \neq 0$. Soit $\mathcal{H}$ l'homographie de $\widehat{\mathbb{C}}$ définie par la formule

$$z \in \widehat{\mathbb{C}} \mapsto \mathcal{H}(z) = \frac{u_1z + u_2}{u_3z + u_4}\cdot$$

Les conditions suivantes sont équivalentes:
(i) $\mathcal{H}(\mathbb{S}^1) \subset \mathbb{S}^1$.
(ii) $\mathcal{H}(\mathbb{S}^1) = \mathbb{S}^1$.

(iii) $$|u_1|^2 + |u_2|^2 = |u_3|^2 + |u_4|^2 \quad \text{et} \quad u_1\overline{u}_2 = u_3\overline{u}_4.$$

(iv) $$|u_1| = |u_4|, \quad |u_2| = |u_3| \quad \text{et} \quad u_1\overline{u}_2 = u_3\overline{u}_4.$$

Démonstration. —
• L'équivalence (i)⇔(ii) résulte du fait que toute homographie transforme un cercle–droite de $\widehat{\mathbb{C}}$ en un cercle–droite.
• Montrons (iii)⇒(i). Pour $z \in \mathbb{C}$ on a l'égalité

$$|\mathcal{H}(z)|^2 = \frac{|u_1z|^2 + |u_2|^2 + u_1\overline{u_2}z + \overline{u_1}u_2\overline{z}}{|u_3z|^2 + |u_4|^2 + u_3\overline{u_4}z + \overline{u_3}u_4\overline{z}}\cdot \tag{1}$$

Supposons les conditions (iii) satisfaites. Pour $|z| = 1$, on a

$$|u_3z|^2 + |u_4|^2 = |u_1z|^2 + |u_2|^2,$$

$$u_3\overline{u_4}z = u_1\overline{u_2}z \quad \text{et} \quad \overline{u_3}u_4\overline{z} = \overline{u_1}u_2\overline{z},$$

donc $|\mathcal{H}(z)| = 1$, ce qui prouve $\mathcal{H}(\mathbb{S}^1) \subset \mathbb{S}^1$.
• Montrons (i)⇒(iii). Supposons $\mathcal{H}(\mathbb{S}^1) \subset \mathbb{S}^1$. Pour tout $z \in \mathbb{S}^1$ on a, grâce à (1),

$$|u_1|^2 + |u_2|^2 - |u_3|^2 - |u_4|^2 = 2\,\mathrm{Re}\big((u_1\overline{u_2} - u_3\overline{u_4})z\big).$$

Or étant donné $\xi \in \mathbb{C}$ le nombre réel $\mathrm{Re}(\xi z)$ prend la même valeur pour $z = 1$, $z = -1$, $z = i$ et $z = -i$ si et seulement si $\xi = 0$. D'où les relations (iii).
• Enfin l'équivalence (ii)⇔(iv) résulte de (ii)⇔(iii) pour les homographies $\mathcal{H}$ et

$$\mathcal{H}^{-1}(w) = \frac{u_4w - u_2}{-u_3w + u_1}\cdot$$

□

Il résulte du lemme 1 que pour une homographie $\mathcal{H}(z)$ à coefficients réels, les conditions suivantes sont équivalentes:
(a) $\mathcal{H}(\mathbb{S}^1) = \mathbb{S}^1$.

(b) $$\mathcal{H}(z) = \pm\frac{u_1 z + u_2}{u_2 z + u_1}$$

avec $u_1 \neq \pm u_2$ nombres réels.
(c) On a $\mathcal{H}(\{+1, -1\}) = \{+1, -1\}$.

Voici le résultat utilisé page 269 de [**FW**] pour la démonstration de la proposition 4.6.

Lemme 2. — Soit $\mathbb{U}_n$ l'ensemble des racines primitives n–ièmes de l'unité, avec $n = 5$ ou $n \geqslant 7$. Soit $\mathcal{H}$ une homographie de $\widehat{\mathbb{C}}$ définie par la formule $\mathcal{H}(z) = (u_1 z + u_2)/(u_3 z + u_4)$ où les u_i sont des nombres rationnels tels que $u_1 u_4 - u_2 u_3 \neq 0$ et tels que $\mathcal{H}(\mathbb{U}_n) = \mathbb{U}_n$. Alors $\mathcal{H}$ est nécessairement de la forme

$$\mathcal{H}(z) = \pm z, \text{ ou } \mathcal{H}(z) = \pm 1/z.$$

Remarque: L'hypothèse $n = 5$ ou $n \geqslant 7$ est clairement nécessaire, puisque pour $n \in \{1, 2, 3, 4, 6\}$, l'ensemble $\mathbb{U}_n$ a un ou deux éléments et l'ensemble des homographies $\mathcal{H}$ fixant $\mathbb{U}_n$ est alors infini.

Démonstration. — L'égalité $\mathbb{U}_m = -\mathbb{U}_{2m}$ valable pour tout entier m impair permet de restreindre la preuve de ce lemme aux entiers n satisfaisant

(2) $$n = 5 \text{ ou } n \geqslant 7 \text{ et } n \not\equiv 2 \bmod 4.$$

Les conditions sur n entraînent que $\mathbb{U}_n$ a au moins trois éléments. Puisqu'une homographie conserve tout cercle–droite de $\widehat{\mathbb{C}}$, l'homographie $\mathcal{H}$ conserve globalement le cercle unité $\mathbb{S}^1$. Ainsi $\mathcal{H}$ a la forme (b) avec des u_i maintenant rationnels.

On suppose $u_1 \neq 0$, puisque le cas $u_1 = 0$ est trivial : il conduit à l'homographie $\mathcal{H}(z) = \pm 1/z$. Nous introduisons le nombre rationnel $t = u_2/u_1 (\neq \pm 1)$ et $\mathcal{H}(z)$ devient $\mathcal{H}(z) = \pm(z + t)/(tz + 1)$.

Soit ζ un élément de $\mathbb{U}_n$. Par hypothèse il existe un entier k vérifiant $1 \leqslant k < n$ et $(k, n) = 1$ tel que

(3) $$\mathcal{H}(\zeta) = \zeta^k.$$

Nous exploitons cette égalité en lui appliquant un certain élément σ du groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ défini par $\sigma : \zeta \mapsto \zeta^p$, où p est un nombre premier ne divisant pas n.
• Si n est impair, on choisit $p = 2$. Par action de σ, l'égalité (3) devient

$$\sigma\left(\pm\frac{\zeta + t}{t\zeta + 1}\right) = \pm\frac{\zeta^2 + t}{t\zeta^2 + 1} = \zeta^{2k} = \left(\pm\frac{\zeta + t}{t\zeta + 1}\right)^2.$$

On voit que ζ est racine de l'un des polynômes

(4) $$P_\pm(X) := (X + t)^2(tX^2 + 1) \pm (tX + 1)^2(X^2 + t).$$

Les polynômes $P_\pm$ sont de degrés $\leqslant 4$ et le coefficient de X^4 est $t \pm t^2$. Pour tout $n > 5$ impair, l'entier algébrique ζ est de degré > 4. On obtient ainsi une contradiction à

moins que $t \pm t^2 = 0$, soit $u_2 = 0$ et le Lemme 2 est prouvé pour tout $n > 5$ impair vérifiant (2).

Une étude plus soignée de l'égalité (4) permet de conclure dans le cas $n = 5$. En effet, dans ce cas, le fait que le polynôme $P_\pm$ s'annule en ζ entraîne qu'il est un multiple du polynôme cyclotomique $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$, dont le coefficient dominant et le terme constant coïncident. Il en est de même pour $P_\pm$, d'où l'égalité $t \pm t^2 = t^2 \pm t$, donnant là aussi $t = 0$ soit de nouveau $u_2 = 0$.

• Si n est pair, n est donc divisible par 4 d'après (2). On suppose qu'il existe un nombre premier p tel que

$$p \nmid n \text{ et } 2p - 6 < \varphi(n). \tag{5}$$

Considérons l'élément σ du groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ défini par $\sigma : \zeta \mapsto \zeta^p$, pour l'appliquer à chaque membre de (3). On obtient les égalités

$$\sigma\left(\pm\frac{\zeta + t}{t\zeta + 1}\right) = \pm\frac{\zeta^p + t}{t\zeta^p + 1} = \zeta^{kp} = \left(\pm\frac{\zeta + t}{t\zeta + 1}\right)^p.$$

Puisque p est impair, on voit que ζ est racine du polynôme de $\mathbb{Q}[X]$

$$Q(X) := (X^p + t)(tX + 1)^p - (tX^p + 1)(X + t)^p.$$

Son degré est au plus $2p$, et ζ est un entier algébrique de degré $\varphi(n)$. Donc si $\varphi(n) > 2p$, on obtient une contradiction, à moins que le coefficient du monôme X^{2p} soit nul, c'est–à–dire $t^p - t = 0$ soit encore $t = 0$, puisque $t \neq \pm 1$. La valeur $t = 0$ conduit alors à l'homographie $\mathcal{H}(z) = \pm z$.

On raffine l'étude du polynôme Q précédent en constatant que les six nombres dérivés vérifient $Q^{(\ell)}(\pm 1) = 0$, pour $\ell = 0$, 1 ou 2. Ainsi $Q(X)$ est divisible par $(X + 1)^3(X - 1)^3$ et $Q(X)(X + 1)^{-3}(X - 1)^{-3}$ est un polynôme de degré $2p - 6$ au plus. Le raisonnement précédent s'adapte sous la condition (5).

Il reste à construire, pour chaque n pair, le nombre premier auxiliaire p vérifiant (5). On a

Lemme 3. — Pour tout n vérifiant $n \equiv 0 \bmod 4$, $n \geqslant 8$ et $n \neq 12$, il existe un nombre premier p vérifiant (5).

Démonstration. — La preuve repose sur la décomposition en facteurs premiers de n.

• Si $3 \nmid n$ le nombre $p = 3$ vérifie (5) trivialement.

• Si $n = 2^k \cdot 3 \cdot p_2 \cdots p_{s-1} p_s$ où $k \geqslant 2$, $3 \leqslant p_2 \leqslant \cdots \leqslant p_{s-1} \leqslant p_s$, et $s \geqslant 2$ on a nécessairement $\varphi(n) \geqslant 4(p_s - 1)$. Par le postulat de Bertrand, il existe un nombre premier p tel que $p_s < p < 2p_s$. On a les relations $p \nmid n$ et $2p - 6 < 4(p_s - 1) \leqslant \varphi(n)$. Ainsi p vérifie (5).

• Le seul cas restant est $n = 2^k \cdot 3$ avec $k \geqslant 2$. Si $k \geqslant 3$ le nombre $p = 5$ convient. En revanche, si $n = 12$, il n'existe pas de p vérifiant (5). □

Il reste à prouver le Lemme 2 pour $n = 12$. Dans ce cas $\mathbb{U}_{12} = \{\pm\zeta^{\pm 1}\}$, et la condition $\mathcal{H}(\zeta) \in \mathbb{U}_{12}$, conduit à l'égalité $\pm(u_1\zeta + u_2)/(u_2\zeta + u_1) = \pm\zeta^{\pm 1}$ qui prouverait que ζ est algébrique de degré $\leqslant 2$, à moins que $\mathcal{H}(z) = \pm z$ ou $\pm 1/z$. □

Références

[FW] Étienne Fouvry et Michel Waldschmidt, *Sur la représentation des entiers par des formes cyclotomiques de grand degré,* Bull. Soc. Math. France, **148** 2 (2020), 253-282. arXiv: 1909.01892 [math.NT]. Zbl 1455.11066 MR4124501

Classification MSC 2020
15A04 Linear transformations, semilinear transformations
20B25 Finite automorphism groups of algebraic, geometric, or combinatorial structures

Mots clefs: homographies

Étienne Fouvry, Université Paris–Saclay, CNRS, Laboratoire de Mathématiques d'Orsay, 91405 Orsay, France, E-mail: Etienne.Fouvry@universite-paris-saclay.fr
& Michel Waldschmidt, Sorbonne Université and Université de Paris, CNRS, IMJ–PRG, 75005 Paris, France, E-mail: michel.waldschmidt@imj-prg.fr