

Bulletin

de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

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

Tome 154
Fascicule 2

2026

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

pages 547-550

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel
de la Société Mathématique de France.

Fascicule 2, tome 154, juin 2026

Comité de rédaction

Boris ADAMCZEWSKI
Valeria BANICA
Julie DÉSERTI
Gabriel DOSPINESCU
Dorothee FREY

Youness LAMZOURI
Wendy LOWEN
Ludovic RIFFORD
Erwan ROUSSEAU
Béatrice de TILIÈRE

François DAHMANI (Dir.)

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
commandes@smf.emath.fr

AMS
P.O. Box 6248
Providence RI 02940
USA
www.ams.org

Tarifs

Vente au numéro : 50 € (\$ 75)

Abonnement électronique : 175 € (\$ 262),

avec supplément papier : Europe 266 €, hors Europe 307 € (\$ 460)

Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Bulletin de la SMF

Bulletin de la Société Mathématique de France

Société Mathématique de France

Institut Henri Poincaré, 11, rue Pierre et Marie Curie

75231 Paris Cedex 05, France

Tél : (33) 1 44 27 67 99

• Fax : (33) 1 40 46 90 96

bulletin@smf.emath.fr

• smf.emath.fr

© Société Mathématique de France 2026

Tous droits réservés (article L 122-4 du Code de la propriété intellectuelle). Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'éditeur est illicite. Cette représentation ou reproduction par quelque procédé que ce soit constituerait une contrefaçon sanctionnée par les articles L 335-2 et suivants du CPI.

ISSN 0037-9484 (print) 2102-622X (electronic)

Directrice de la publication : Isabelle GALLAGHER

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

PAR ÉTIENNE FOUVRY & MICHEL WALDSCHMIDT

Au milieu de la page 269 de [1], 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 [1] 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. — *On considère des nombres complexes u_1, u_2, u_3, u_4 vérifiant la relation*

$$u_1 u_4 - u_2 u_3 \neq 0.$$

Soit $\mathcal{H}$ l'homographie de $\widehat{\mathbb{C}}$ définie par la formule

$$z \in \widehat{\mathbb{C}} \mapsto \mathcal{H}(z) = \frac{u_1 z + u_2}{u_3 z + u_4}.$$

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) $|u_1|^2 + |u_2|^2 = |u_3|^2 + |u_4|^2$ et $u_1 \bar{u}_2 = u_3 \bar{u}_4$.
- (iv) $|u_1| = |u_4|$, $|u_2| = |u_3|$ et $u_1 \bar{u}_2 = u_3 \bar{u}_4$.

Texte reçu le 1^{er} juin 2025, accepté le 6 octobre 2025.

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, Université de Paris, CNRS, IMJ-PRG, 75005 Paris, France • *E-mail* : michel.waldschmidt@imj-prg.fr

Classification mathématique par sujets (2020). — 15A04, 20B25.

Mots clefs. — Homographies.

Démonstration. — • L'équivalence (i) $\Leftrightarrow$ (ii) résulte du fait que toute homographie transforme un cercle-droite de $\widehat{\mathbb{C}}$ en un cercle-droite.

- Montrons (iii) $\Rightarrow$ (i). Pour $z \in \mathbb{C}$ on a l'égalité

$$(1) \quad |\mathcal{H}(z)|^2 = \frac{|u_1 z|^2 + |u_2|^2 + u_1 \overline{u_2} z + \overline{u_1} u_2 \bar{z}}{|u_3 z|^2 + |u_4|^2 + u_3 \overline{u_4} z + \overline{u_3} u_4 \bar{z}}.$$

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

$$|u_3 z|^2 + |u_4|^2 = |u_1 z|^2 + |u_2|^2, \\ u_3 \overline{u_4} z = u_1 \overline{u_2} z \quad \text{et} \quad \overline{u_3} u_4 \bar{z} = \overline{u_1} u_2 \bar{z},$$

donc $|\mathcal{H}(z)| = 1$, ce qui prouve $\mathcal{H}(\mathbb{S}^1) \subset \mathbb{S}^1$.

- Montrons (i) $\Rightarrow$ (iii). Supposons $\mathcal{H}(\mathbb{S}^1) \subset \mathbb{S}^1$. Pour tout $z \in \mathbb{S}^1$ on a, grâce à (1),

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

Or étant donné $\xi \in \mathbb{C}$ le nombre réel $\operatorname{Re}(\xi z)$ 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) $\Leftrightarrow$ (iv) résulte de (ii) $\Leftrightarrow$ (iii) pour les homographies $\mathcal{H}$ et

$$\mathcal{H}^{-1}(w) = \frac{u_4 w - u_2}{-u_3 w + u_1}. \quad \square$$

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 [1] 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 $n \geq 7$. 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 $n \geq 7$ 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 $\mathcal{H}$, à coefficients rationnels, 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

$$(2) \quad n = 5 \text{ ou } n \geq 7 \text{ et } n \not\equiv 2 \pmod{4}.$$

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 $1 \leq k < n$ et $(k, n) = 1$ tel que

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

Nous exploitons cette égalité en lui appliquant un certain élément σ du groupe de Galois $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ 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

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

Les polynômes $P_{\pm}$ sont de degrés ≤ 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 $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$. On en déduit que tous les coefficients de P_+ sont égaux entre eux ainsi que tous les coefficients de P_- . Ceci n'est possible que dans le cas de P_- avec la valeur $t = 0$, 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

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

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