

Familles d'équations de Thue–Mahler n'ayant que des solutions triviales

par

CLAUDE LEVESQUE (Québec) et MICHEL WALDSCHMIDT (Paris)

En hommage à André Schinzel

1. Introduction. Les premières familles d'équations de Thue n'ayant que des solutions dites triviales ont été données par E. Thomas en 1990 [13]. D'autres familles ont été trouvées par la suite [10]. Les familles d'équations de Thue étudiées jusqu'à présent font presque toutes intervenir des équations variant avec un paramètre dont dépend un corps de nombres attaché à ladite équation. À date, il n'y avait pas encore de familles d'équations de Thue–Mahler pour lesquelles la finitude du nombre de solutions ait été établie. Notre résultat va permettre d'attacher, à chaque corps de nombres algébriques possédant une infinité d'unités, une famille infinie d'équations de Thue–Mahler n'ayant qu'un nombre fini de solutions non triviales. L'outil diophantien que nous allons mettre en œuvre est le théorème du sous-espace de W. M. Schmidt [5, 1, 14]. Nous poursuivrons ultérieurement ce travail en remplaçant le théorème non effectif du sous-espace par des minorations de formes linéaires de logarithmes, de façon à rendre effectifs nos résultats, au moins dans certains cas particuliers.

2. Résultats connus. Soient K un corps de nombres et S un ensemble fini de places de K contenant les places archimédiennes. Nous notons \mathcal{O}_K l'anneau des entiers algébriques de K , et \mathcal{O}_K^\times le groupe des unités de K (éléments inversibles de \mathcal{O}_K). De plus, pour S , un ensemble fini de places de K contenant les places archimédiennes, \mathcal{O}_S est l'anneau des S -entiers de K , à savoir l'ensemble des éléments x de K tels que $|x|_v \leq 1$ pour toute place $v \notin S$. De plus, \mathcal{O}_S^\times est le groupe des S -unités, c'est-à-dire, des éléments

2010 *Mathematics Subject Classification*: Primary 11D59; Secondary 11D45, 11D61, 11D25, 11J87.

Key words and phrases: diophantine equations, families of Thue–Mahler equations, units of algebraic number fields, Schmidt subspace theorem.

inversibles de O_S , donc des éléments x de K tels que $|x|_v = 1$ pour tout $v \notin S$.

Soient $\mu, \alpha_1, \dots, \alpha_n$ des éléments non nuls de K . On considère pour commencer l'équation diophantienne de Thue–Mahler

$$(2.1) \quad (X - \alpha_1 Y) \cdots (X - \alpha_n Y) = \mu E,$$

où les valeurs prises par les inconnues X et Y sont des éléments x et y de O_S vérifiant $xy \neq 0$, et où les valeurs prises par l'inconnue E sont des éléments ε de O_S^\times .

Si (x, y, ε) est une solution de (2.1), alors pour tout $\eta \in O_S^\times$ le triplet $(\eta x, \eta y, \eta^n \varepsilon)$ est aussi une solution. Selon [6, §2], deux telles solutions sont dites *S-dépendantes*. Autrement, elles sont dites *S-indépendantes*. En voici une formulation équivalente.

DÉFINITION. Deux solutions (x, y, ε) et (x', y', ε') dans $O_S^2 \times O_S^\times$ de l'équation (2.1) sont dites *S-dépendantes* si les points de $\mathbb{P}^1(K)$ de coordonnées projectives $(x : y)$ et $(x' : y')$ sont les mêmes. Autrement, elles sont dites *S-indépendantes*.

Le résultat suivant a été démontré par Parry en 1950 à la suite de travaux de Thue et Mahler notamment (voir par exemple [6, §2], et [12, théorème 5.4]).

THÉORÈME 2.1 (Thue–Mahler–Parry). *Sous l'hypothèse*

$$\text{Card}\{\alpha_1, \dots, \alpha_n\} \geq 3,$$

le nombre maximum de solutions deux à deux S-indépendantes $(x, y, \varepsilon) \in O_S \times O_S \times O_S^\times$ avec $xy \neq 0$ de l'équation (2.1) est fini.

Erdős, Stewart et Tijdeman [4] ont donné des exemples dans lesquels le nombre de solutions de (2.1) est remarquablement grand.

Une conséquence du théorème 2.1 est la suivante.

COROLLAIRE 2.2. *Soit $f(X, Y) \in \mathbb{Z}[X, Y]$ une forme binaire à coefficients dans \mathbb{Z} ayant au moins trois facteurs linéaires deux à deux non proportionnels dans sa factorisation sur \mathbb{C} . Soit $k \in \mathbb{Z} \setminus \{0\}$ et soient p_1, \dots, p_t des nombres premiers. Alors l'équation $f(X, Y) = kp_1^{Z_1} \cdots p_t^{Z_t}$ n'a qu'un nombre fini de solutions (x, y, z_1, \dots, z_t) dans $\mathbb{Z}^2 \times \mathbb{N}^t$ vérifiant $xy \neq 0$ et $\text{pgcd}(xy, p_1 \cdots p_t) = 1$.*

Nous utiliserons la généralisation N_S de la norme, introduite par exemple dans [6] et dont nous rappelons la définition au début du §5. Dans [6, §2], Evertse et Györy font intervenir deux relations d'équivalence : la première concerne les solutions des inéquations de Thue–Mahler

$$(2.2) \quad 0 < N_S(f(x, y)) \leq m.$$

Selon [6], deux solutions (x, y) , (x', y') de (2.2) sont dépendantes s'il existe $\eta \in K^\times$ tel que $x' = \eta x$ et $y' = \eta y$. Voici la seconde relation, qui concerne les formes binaires de $O_S[X, Y]$.

DÉFINITION. Deux formes binaires $f(X, Y)$ et $g(X, Y)$ de $O_S[X, Y]$ sont dites *S-équivalentes* s'il existe $\alpha, \beta, \gamma, \delta$ dans O_S et η dans O_S^\times vérifiant $\alpha\delta - \beta\gamma \in O_S^\times$ et $g(X, Y) = \eta f(\alpha X + \beta Y, \gamma X + \delta Y)$.

Soient K un corps de nombres, S un ensemble fini de places de K contenant les places archimédiennes, et n un entier ≥ 3 . Notons $\mathcal{F}(n, K, S)$ l'ensemble des formes binaires $f \in O_S[X, Y]$ de degré n qui se décomposent en facteurs linéaires dans $K[X, Y]$ et dont la décomposition contient au moins trois facteurs linéaires distincts. Voici la première partie du théorème 2 de [6].

THÉORÈME 2.3 (Evertse et Györy). *Avec les notations ci-dessus, pour tout entier $m > 0$, il n'y a qu'un nombre fini de classes de S-équivalence de formes binaires f dans $\mathcal{F}(n, K, S)$ pour lesquelles il existe plus de deux solutions indépendantes $(x, y) \in O_S \times O_S$ de l'inéquation (2.2).*

Les autres résultats de [6] font intervenir une extension finie L de K , mais pour le théorème 2.3 cela n'apporte pas plus de généralité.

3. Énoncés de nos résultats. Notre résultat principal (théorème 3.1) consiste à remplacer d'une part trois des facteurs $X - \alpha_i Y$ (disons pour $i = 1, 2, 3$) de l'équation (2.1) par des facteurs de la forme $X - \alpha_i E_i Y$, où E_1, E_2, E_3 sont des inconnues supplémentaires prenant des valeurs dans O_S^\times , et à remplacer d'autre part le produit des autres facteurs par Z où l'inconnue Z prend ses valeurs dans l'anneau des S -entiers. On considère donc l'équation plus générale

$$(3.1) \quad (X - \alpha_1 E_1 Y)(X - \alpha_2 E_2 Y)(X - \alpha_3 E_3 Y)Z = \mu E,$$

où les inconnues X, Y et Z sont à valeurs dans O_S et où les inconnues E_1, E_2, E_3, E sont à valeurs dans O_S^\times . On note $(X, Y, Z, E_1, E_2, E_3, E)$ le septuplet formé par les inconnues, et $(x, y, z, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon)$ les septuplets formés par les solutions dans $O_S^3 \times (O_S^\times)^4$.

DÉFINITION. Nous appellerons *triviales* les solutions pour lesquelles $xy = 0$.

Nous supposons que les solutions satisfont

$$\text{Card}\{\alpha_1 \varepsilon_1, \alpha_2 \varepsilon_2, \alpha_3 \varepsilon_3\} = 3.$$

Si $(x, y, z, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon)$ est une solution non triviale de (3.1), alors, pour tout $\eta \in O_S^\times$, les septuplets

$$(\eta x, \eta y, z, \varepsilon_1, \varepsilon_2, \varepsilon_3, \eta^3 \varepsilon), \quad (x, y, \eta z, \varepsilon_1, \varepsilon_2, \varepsilon_3, \eta \varepsilon), \quad (x, \eta^{-1} y, z, \eta \varepsilon_1, \eta \varepsilon_2, \eta \varepsilon_3, \varepsilon)$$

sont aussi des solutions non triviales de (3.1), que l'on qualifera de S^3 -*dépendantes* de la solution initiale.

DÉFINITION. Deux solutions non triviales $(x, y, z, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon)$ et $(x', y', z', \varepsilon'_1, \varepsilon'_2, \varepsilon'_3, \varepsilon')$ de l'équation (3.1) seront dites S^3 -*dépendantes* s'il existe des S -unités η_1, η_2 et η_3 dans O_S^\times telles que

$$x' = x\eta_1, \quad y' = y\eta_1\eta_3^{-1}, \quad z' = z\eta_2, \quad \varepsilon'_i = \varepsilon_i\eta_3 \quad (i = 1, 2, 3), \quad \varepsilon' = \varepsilon\eta_1^3\eta_2.$$

Sinon, ces deux solutions seront dites S^3 -*indépendantes*.

Ceci définit une relation d'équivalence sur l'ensemble des solutions non triviales de (3.1). Quand le groupe des S -unités O_S^\times a un rang ≥ 1 , chaque classe de S^3 -dépendance de solutions non triviales contient une infinité d'éléments.

Le principal but de cet article est de démontrer le résultat suivant, qui généralise le théorème 2.1. Il s'agit apparemment du premier énoncé donnant la finitude du nombre de solutions de familles d'équations de Thue–Mahler.

THÉORÈME 3.1. *Soient K un corps de nombres, S un ensemble fini de places de K contenant les places archimédiennes, et $\mu, \alpha_1, \alpha_2, \alpha_3$ des éléments non nuls de K . Alors l'ensemble des classes de S^3 -dépendance des solutions non triviales $(x, y, z, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon)$ dans $O_S^3 \times (O_S^\times)^4$ de l'équation*

$$(X - \alpha_1 E_1 Y)(X - \alpha_2 E_2 Y)(X - \alpha_3 E_3 Y)Z = \mu E$$

satisfaisant la condition $\text{Card}\{\alpha_1\varepsilon_1, \alpha_2\varepsilon_2, \alpha_3\varepsilon_3\} = 3$ est fini. Le nombre de ces classes est majoré par une constante κ_1 , ne dépendant que de $K, N_S(\mu), \alpha_1, \alpha_2, \alpha_3$ et du rang s du groupe O_S^\times , et dont la valeur est explicitée dans la formule (6.5).

Quitte à agrandir S , on peut supposer $\alpha_1 = \alpha_2 = \alpha_3 = \mu = 1$ (cela augmente le rang de O_S^\times ; il faudrait en tenir compte si on voulait donner une borne explicite). Dans ce cas, les variables E et Z sont redondantes (prendre $\eta_2 = z^{-1}$ dans la définition de la S^3 -dépendance pour se ramener à $z = 1$). De même, il n'y a pas de restriction à supposer $E_3 = 1$ (prendre $\eta_3 = \varepsilon_3^{-1}$). L'équation que l'on considère se ramène donc à

$$(3.2) \quad (X - Y)(X - E_1 Y)(X - E_2 Y) = E,$$

en cinq inconnues, X, Y, E_1, E_2, E . La relation d'équivalence entre les quintuplets dans $O_S^2 \times (O_S^\times)^3$ formés de solutions est essentiellement celle du §2 : nous dirons encore que deux solutions $(x, y, \varepsilon_1, \varepsilon_2, \varepsilon)$ et $(x', y', \varepsilon'_1, \varepsilon'_2, \varepsilon')$ de (3.2) sont S -*dépendantes* s'il existe $\eta \in O_S^\times$ tel que

$$x' = x\eta, \quad y' = y\eta, \quad \varepsilon'_1 = \varepsilon_1, \quad \varepsilon'_2 = \varepsilon_2, \quad \varepsilon' = \varepsilon\eta^3.$$

L'énoncé suivant est donc équivalent au théorème 3.1 (à la valeur près de la borne explicite pour le nombre de classes de solutions, que nous ne précisons pas).

THÉORÈME 3.2. *Le nombre de classes de S -dépendance de solutions de l'équation (3.2) est fini.*

Il est intéressant de noter que nous avons ramené la question de la finitude du nombre de solutions de l'équation de Thue–Mahler en degré quelconque à celle d'une équation cubique (voir à ce sujet [11]).

Pour faire le lien avec le théorème 2.3, montrons que notre théorème 3.1 permet d'établir l'existence d'une infinité de classes de S -équivalence de formes binaires de $\mathcal{F}(n, K, S)$ produisant des inéquations (2.2) dont toutes les solutions sont triviales.

Du théorème 3.2 on déduit facilement l'énoncé suivant.

THÉORÈME 3.3. *Soient K un corps de nombres, S un ensemble fini de places de K contenant les places archimédiennes, n un entier ≥ 3 , $\alpha_1, \dots, \alpha_n$ des éléments de K^\times et $f \in K[X, Y]$ la forme binaire*

$$f(X, Y) = (X - \alpha_1 Y)(X - \alpha_2 Y) \cdots (X - \alpha_n Y).$$

Pour $\underline{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n) \in (O_S^\times)^n$, on note $f_{\underline{\varepsilon}} \in K[X, Y]$ la forme binaire

$$f_{\underline{\varepsilon}}(X, Y) = (X - \alpha_1 \varepsilon_1 Y)(X - \alpha_2 \varepsilon_2 Y) \cdots (X - \alpha_n \varepsilon_n Y).$$

On désigne par \mathcal{E} l'ensemble des éléments $\underline{\varepsilon}$ de $(O_S^\times)^n$ tels que $\varepsilon_1 = 1$ et $\text{Card}\{\alpha_1 \varepsilon_1, \alpha_2 \varepsilon_2, \dots, \alpha_n \varepsilon_n\} \geq 3$. Alors il existe un sous-ensemble fini \mathcal{E}^* de \mathcal{E} tel que, pour tout $\underline{\varepsilon} \in \mathcal{E} \setminus \mathcal{E}^*$ et pour tout $(x, y) \in O_S \times O_S$, la condition

$$f_{\underline{\varepsilon}}(x, y) \in O_S^\times$$

implique $xy = 0$.

Ce théorème 3.3 se déduit du théorème 3.1 avec $\mu = 1$: quitte à renuméroter les racines de $f_{\underline{\varepsilon}}$, on peut supposer $\text{Card}\{\alpha_1 \varepsilon_1, \alpha_2 \varepsilon_2, \alpha_3 \varepsilon_3\} = 3$; on prend alors pour z le produit $(x - \alpha_4 \varepsilon_4 y) \cdots (x - \alpha_n \varepsilon_n y)$.

Au §8, on prouvera la proposition suivante.

PROPOSITION 3.4. *Soit $\underline{\varepsilon} \in \mathcal{E} \setminus \mathcal{E}^*$. Il n'y a qu'un nombre fini d'éléments $\underline{\varepsilon}' \in \mathcal{E} \setminus \mathcal{E}^*$ tels que les deux formes binaires $f_{\underline{\varepsilon}}$ et $f_{\underline{\varepsilon}'}$ soient S -équivalentes.*

On déduit encore du théorème 3.1 le corollaire suivant.

COROLLAIRE 3.5. *Pour chaque $m \in \mathbb{N}$ et pour chaque $\underline{\varepsilon} \in \mathcal{E}$ en dehors d'un sous-ensemble fini (dépendant de m), l'inéquation*

$$0 < N_S(f_{\underline{\varepsilon}}(x, y)) \leq m$$

n'a pas de solution $(x, y) \in O_S \times O_S$ vérifiant $xy \neq 0$.

C'est ainsi que nous obtenons une infinité de classes de S -équivalence de formes binaires donnant lieu à des inéquations de Thue–Mahler (2.2) dont toutes les solutions sont triviales.

Pour énoncer le corollaire 3.6 ci-dessous, nous définissons une famille de formes binaires f_ε , indexée par les S -unités d'un corps de nombres, de la façon suivante. Partons d'une forme

$$f(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_{d-1} Y^{d-1} X + a_d Y^d \in \mathbb{Z}[X, Y]$$

irréductible sur \mathbb{Z} et écrivons

$$f(X, Y) = a_0 (X - \sigma_1(\alpha)Y) \cdots (X - \sigma_d(\alpha)Y),$$

où α est une racine de $f(X, 1)$ et où $\sigma_1, \dots, \sigma_d$ sont les d plongements du corps $K := \mathbb{Q}(\alpha)$ dans \mathbb{C} . Soient p_1, \dots, p_t des nombres premiers et S l'ensemble des places du corps K constitué des places archimédiennes et des places de K au-dessus de p_1, \dots, p_t . Tordons $f(X, Y)$ par une S -unité $\varepsilon \in O_S^\times$ en définissant la forme binaire $f_\varepsilon(X, Y) \in \mathbb{Z}[X, Y]$ de degré d par

$$f_\varepsilon(X, Y) = a_0 (X - \sigma_1(\alpha\varepsilon)Y) \cdots (X - \sigma_d(\alpha\varepsilon)Y).$$

Du théorème 3.1 nous déduisons la généralisation suivante du corollaire 2.2.

COROLLAIRE 3.6. *Soit $k \in \mathbb{Z} \setminus \{0\}$. L'ensemble des $(x, y, \varepsilon, z_1, \dots, z_t)$ dans $\mathbb{Z}^2 \times O_S^\times \times \mathbb{N}^t$ satisfaisant*

$$(3.3) \quad f_\varepsilon(x, y) = kp_1^{z_1} \cdots p_t^{z_t},$$

avec $xy \neq 0$, $\text{pgcd}(xy, p_1 \cdots p_t) = 1$ et $[\mathbb{Q}(\alpha\varepsilon) : \mathbb{Q}] \geq 3$, est fini. Le nombre de ces solutions est majoré par une constante κ_2 , effectivement calculable en fonction de α, k, f et t , dont la valeur est explicitée dans la formule (7.1).

En particulier, lorsque $[\mathbb{Q}(\alpha\varepsilon) : \mathbb{Q}] \geq 3$, l'équation de Thue $f_\varepsilon(X, Y) = \pm 1$, sauf pour un nombre fini de S -unités ε , n'a que des solutions triviales. Un autre cas particulier du corollaire 3.6 s'énonce de la façon suivante : Soient K un corps de nombres de degré ≥ 3 , k un entier non nul et p_1, \dots, p_t des nombres premiers. Pour toute unité ε de K , désignons par $g_\varepsilon(X, Y) \in \mathbb{Z}[X, Y]$ la version homogène du polynôme minimal $g_\varepsilon(X, 1) \in \mathbb{Z}[X]$ de ε . Alors l'ensemble des unités ε de K telles que $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] \geq 3$ et que l'équation $g_\varepsilon(X, Y) = kp_1^{z_1} \cdots p_t^{z_t}$ ait une solution (x, y, z_1, \dots, z_t) dans $\mathbb{Z}^2 \times \mathbb{N}^t$ vérifiant $xy \neq 0$ avec $\text{pgcd}(xy, p_1 \cdots p_t) = 1$ est fini.

Étant donné que nos démonstrations reposent sur le théorème du sous-espace de Schmidt (cf. théorème 5.1), elles ne permettent pas d'obtenir des énoncés effectifs: elles conduisent à des énoncés quantitatifs avec des bornes pour le nombre de solutions, mais pas à des majorations pour les solutions elles-mêmes. Obtenir des résultats effectifs, au moins pour certains cas particuliers du théorème 3.1, sera l'objet de travaux ultérieurs.

4. Lien avec un théorème de Vojta. Le théorème 2.4.1 de Vojta [14] (dont la démonstration repose aussi sur le théorème 5.1) permet de montrer que l'ensemble des solutions de (3.2) est *dégénéré* au sens de [14],

c'est-à-dire, contenu dans un sous-ensemble fermé propre pour la topologie de Zariski. Voici l'énoncé du corollaire 2.4.2 de [14].

THÉORÈME 4.1 (Vojta). *Soit D un diviseur de \mathbb{P}^n ayant au moins $n+2$ composantes distinctes. Alors tout ensemble de points D -entiers de \mathbb{P}^n est dégénéré.*

Montrons comment appliquer ce résultat avec $n = 4$ à l'équation (3.2). Nous avons vu (au §3) que le théorème 3.2 était équivalent au théorème 3.1. Dans le même esprit, quitte à agrandir S , nous pouvons supposer que $\alpha_1 = \alpha_2 = \alpha_3 = \mu = 1$. Si $(x, y, \varepsilon_1, \varepsilon_2, \varepsilon) \in O_S^2 \times (O_S^\times)^3$ est une solution, alors $x - y$, $x - \varepsilon_1 y$ et $x - \varepsilon_2 y$ sont des S -unités.

Introduisons des coordonnées projectives $(X : Y : Z : E_1 : E_2)$ sur $\mathbb{P}^4(K)$ et considérons le diviseur D défini par l'hypersurface

$$ZE_1E_2(X - Y)(XZ - E_1Y)(XZ - E_2Y) = 0$$

qui a six composantes irréductibles. Montrons que chaque solution $\mathbf{p} = (x, y, \varepsilon_1, \varepsilon_2, \varepsilon) \in O_S^2 \times (O_S^\times)^3$ de (3.2) en les inconnues (X, Y, E_1, E_2, E) définit un point entier sur la variété ouverte $\mathbb{P}^4(K) \setminus D$, à savoir le point $\tilde{\mathbf{p}} = (x : y : 1 : \varepsilon_1 : \varepsilon_2)$. En effet, les coordonnées de $\tilde{\mathbf{p}}$ sont dans O_S , et le point $\tilde{\mathbf{p}}$ ne se réduit pas modulo un premier en dehors de S à un point d'un des hyperplans $Z = 0$, $E_1 = 0$, $E_2 = 0$, $X - Y = 0$, ni à un point d'une des hypersurfaces $XZ - E_1Y = 0$, $XZ - E_2Y = 0$, car les nombres ε , ε_1 , ε_2 , $x - y$, $x - \varepsilon_1 y$ et $x - \varepsilon_2 y$ sont des S -unités. Le théorème 4.1 montre que les solutions de (3.2) ne sont pas Zariski denses dans $V = \mathbb{P}^4(K) \setminus D$. En désignant par \mathcal{E} l'ensemble des $(x, y, \varepsilon_1, \varepsilon_2) \in O_S^2 \times (O_S^\times)^2$ qui vérifient

$$(x - y)(x - \varepsilon_1 y)(x - \varepsilon_2 y) \in O_S^\times,$$

cela signifie qu'il existe un polynôme non nul P en les variables X, Y, E_1, E_2 qui s'annule au point $(x : y : \varepsilon_1 : \varepsilon_2)$ chaque fois que $(x, y, \varepsilon_1, \varepsilon_2)$ est dans \mathcal{E} . On peut remarquer que si $(x, y, \varepsilon_1, \varepsilon_2) \in \mathcal{E}$, alors $(x, y, \varepsilon_2, \varepsilon_1)$ et $(y, x, \varepsilon_1, \varepsilon_2)$ sont aussi dans \mathcal{E} , de même que $(tx, ty, \varepsilon_1, \varepsilon_2)$ pour tout t dans O_S^\times . Comme on peut supposer sans perte de généralité que le groupe O_S^\times est infini, on en déduit que le polynôme $P(Tx, Ty, \varepsilon_1, \varepsilon_2) \in K[T]$ est nul. Donc

$$\begin{aligned} P(Tx, Ty, \varepsilon_2, \varepsilon_1) &= P(Ty, Tx, \varepsilon_1, \varepsilon_2) = P(Tx, Ty, \varepsilon_1, \varepsilon_2) \\ &= P(Ty, Tx, \varepsilon_2, \varepsilon_1) = 0. \end{aligned}$$

Il ne semble pas que ces arguments permettent de terminer la démonstration du théorème 3.1 ; pour y parvenir nous allons revenir à la source, à savoir le théorème du sous-espace de Schmidt. Au préalable, rappelons quelques outils diophantiens.

5. Outils diophantiens. Soient K un corps de nombres de degré $d = [K : \mathbb{Q}]$ sur \mathbb{Q} , D_K son discriminant, h_K son nombre de classes, R_K son

régulateur, M_K l'ensemble des places de K et S_∞ l'ensemble des places archimédiennes de K .

Le rang r du groupe des unités de K est $r_1 + r_2 - 1$, où r_1 est le nombre de places réelles de K et r_2 le nombre de places archimédiennes non réelles. On a $d = r_1 + 2r_2$ et on note $d_v = 1$ pour v une place réelle, $d_v = 2$ pour v une place archimédienne non réelle, de sorte que $d = \sum_{v \in S_\infty} d_v$. Nous adopterons la normalisation des valeurs absolues utilisée dans [3] et [9] : pour $\alpha \in K$,

$$|\alpha|_v = \begin{cases} |\sigma(\alpha)| & \text{si } v \text{ est une place archimédienne} \\ & \text{liée à un plongement réel } \sigma : K \rightarrow \mathbb{R}, \\ |\sigma(\alpha)|^2 & \text{si } v \text{ est une place archimédienne} \\ & \text{liée à un plongement non réel } \sigma : K \rightarrow \mathbb{C}, \\ N(\mathfrak{P})^{-\text{ord}_{\mathfrak{P}}(\alpha)} & \text{si } v \text{ est une place ultramétrique} \\ & \text{liée à un idéal premier } \mathfrak{P} \text{ de } \mathcal{O}_K. \end{cases}$$

On notera $h(\alpha)$ la hauteur logarithmique absolue d'un élément α de K (c'est la notation de [9], alors que ce qui est noté $h(\alpha)$ dans [3], [7] et [6] est pour nous $\exp\{h(\alpha)\}$) :

$$h(\alpha) = \frac{1}{d} \sum_{v \in M_K} \log \max\{1, |\alpha|_v\}.$$

On désigne par δ_K un nombre réel positif tel que tout entier algébrique non nul $\alpha \in K$, qui n'est pas une racine de l'unité, vérifie $h(\alpha) \geq \delta_K/d$. Des minoration explicites de δ_K (dues à Blanksby et Montgomery, Dobrowolski et Voutier) sont données dans [3].

Rappelons (cf. [6, §2], ou bien [8, §1]) la définition de la S -norme, notée N_S , associée à un ensemble fini S de places de K contenant les places archimédiennes. Soit $\alpha \in K^\times$. L'idéal principal fractionnaire (α) de \mathcal{O}_K engendré par α s'écrit de manière unique comme un produit $\mathfrak{A}\mathfrak{B}$, où \mathfrak{A} est un idéal fractionnaire de \mathcal{O}_K qui est produit de puissances d'idéaux premiers qui ne sont pas au-dessus des places finies de S , tandis que \mathfrak{B} est un idéal fractionnaire de \mathcal{O}_K qui est produit de puissances d'idéaux premiers au-dessus des places finies de S . Alors $N_S(\alpha)$ est la norme de l'idéal \mathfrak{A} .

Ainsi, par définition, un élément α de K appartient à \mathcal{O}_S si et seulement si l'idéal \mathfrak{A} est un idéal entier de \mathcal{O}_K . De plus, les S -unités de K sont les éléments ε de \mathcal{O}_S qui vérifient $N_S(\varepsilon) = 1$. Si $S = S_\infty$, alors $\mathcal{O}_S = \mathcal{O}_K$, $\mathcal{O}_S^\times = \mathcal{O}_K^\times$ et N_S coïncide avec $|N_{K/\mathbb{Q}}|$.

Quand $K = \mathbb{Q}$, si S est l'ensemble constitué des places archimédiennes et des places au-dessus des nombres premiers p_1, \dots, p_t , pour un nombre rationnel non nul α écrit sous la forme

$$\alpha = \pm \left(\prod_{i=1}^t p_i^{a_i} \right) \left(\prod_{j=t+1}^r p_j^{a_j} \right)$$

avec $a_\ell \in \mathbb{Z}$ ($\ell = 1, \dots, r$) et $p_j \notin \{p_1, \dots, p_t\}$ ($j = t+1, \dots, r$), alors on a

$$N_S(\alpha) = \prod_{j=t+1}^r p_j^{a_j}.$$

On notera s le rang du groupe O_S^\times , ce qui fait que le nombre d'éléments ⁽¹⁾ de S est $s-1$. Si $r = r_1 + r_2 - 1$ est le rang du groupe des unités de K , alors $t = s - 1 - r$ est le nombre d'idéaux premiers $\mathfrak{P}_1, \dots, \mathfrak{P}_t$ de \mathcal{O}_K au-dessus des places ultramétriques de K dans S . On désigne par ν le plus grand des nombres $|N(\mathfrak{P}_i)|$ ($1 \leq i \leq t$), avec $\nu = 1$ si $t = 0$ (c'est-à-dire, si $S = S_\infty$). La norme indice S d'un élément α est

$$N_S(\alpha) = \prod_{v \in S} |\alpha|_v.$$

Nous utiliserons une base w_1, \dots, w_d de l'anneau des entiers de K comme \mathbb{Z} -module :

$$\mathcal{O}_K = \mathbb{Z}w_1 + \dots + \mathbb{Z}w_d.$$

D'après le lemme 5 de [7], il existe une telle base pour laquelle le nombre

$$\theta = \max \left\{ 1, \max_{\sigma: K \rightarrow \mathbb{C}} (|\sigma(w_1)| + \dots + |\sigma(w_d)|) \right\}$$

vérifie la majoration $\theta \leq |D_K|^{1/2}$.

Notons enfin $d(N)$ la fonction *nombre de diviseurs* d'un entier $N > 0$:

$$d(N) := \sum_{d|N} 1.$$

Nous utiliserons le fait banal que pour tout couple (n, N) d'entiers positifs, le nombre de décompositions de N comme produit de n facteurs $m_1 \cdots m_n = N$ est majoré par $d(N)^{n-1}$.

L'outil principal des preuves de nos généralisations de ces résultats, que nous utiliserons plusieurs fois par la suite, est une conséquence du théorème du sous-espace de Schmidt. L'énoncé précis que nous utiliserons est le suivant, dû à Evertse [5], raffiné dans le cas $\ell = 2$ par Beukers et Schlickewei [2].

THÉORÈME 5.1 (Evertse, Beukers–Schlickewei). *Soient K un corps de nombres, $\delta_1, \dots, \delta_\ell$ des éléments non nuls de K et S un ensemble fini de places de K , de cardinal s . Alors les solutions $(x_1, \dots, x_\ell) \in (O_S^\times)^\ell$ de l'équation*

$$\delta_1 X_1 + \delta_2 X_2 + \dots + \delta_\ell X_\ell = 1,$$

pour lesquelles aucune sous-somme stricte

$$\sum_{i \in I} \delta_i x_i \quad (\emptyset \neq I \subset \{1, \dots, \ell\})$$

⁽¹⁾ Dans [3] le nombre d'éléments de S est noté s (et le rang de O_S^\times est bien sûr $s+1$).

ne s'annule, sont en nombre fini majoré par

$$(5.1) \quad \begin{cases} (2^{33}(\ell + 1)^2)^{\ell^3 s} & \text{pour } \ell \geq 3, \\ 2^{8s+24} & \text{pour } \ell = 2, \end{cases}$$

Notons à ce propos qu'un résultat beaucoup plus général a été obtenu par Amoroso et Viada (théorème 6.2 de [1]), qui autorisent K à être un corps de caractéristique nulle et G un sous-groupe de K^\times de rang fini (cette situation plus générale est aussi celle considérée par Beukers et Schlickewei dans [2] pour le cas $\ell = 2$). Leur énoncé raffine un résultat antérieur de Schmidt, Evertse, van der Poorten et Schlickewei, qui comportait une exponentielle de plus. La borne qu'ils obtiennent dans ce cadre bien plus général pour le nombre de solutions est un tout petit peu moins précise que celle du théorème 5.1, puisqu'ils ont $(8\ell)^{4\ell^4(\ell+s+1)}$ à la place de (5.1), et c'est pourquoi nous utilisons le résultat plus ancien d'Evertse.

Nous utiliserons plusieurs fois le théorème 5.1, pour $\ell = 2$ puis pour $\ell = 5$, qui donnent respectivement pour la constante (5.1) les valeurs $\kappa_3 - 1$ et $\kappa_4 - 1$, avec

$$\kappa_3 = 1 + 2^{8s+24} \quad \text{et} \quad \kappa_4 = 1 + (2^{4375}3^{250})^s.$$

Le terme dominant de nos estimations provient du lemme suivant.

LEMME 5.2. *Soient K un corps de nombres et S un ensemble fini de places de K contenant les places archimédiennes. Il existe une constante positive κ_5 , explicitement calculable et ne dépendant que de K et S , telle que, pour tout entier $m > 0$, il existe un sous-ensemble $A_1(m)$ de $O_S \setminus \{0\}$, ayant au plus $\kappa_5 m$ éléments, avec la propriété suivante : pour tout $\beta \in O_S$ vérifiant $N_S(\beta) = m$, il existe $\varepsilon \in O_S^\times$ et $\gamma \in A_1(m)$ satisfaisant $\beta = \varepsilon\gamma$.*

Nous obtiendrons la valeur explicite suivante pour la constante :

$$\kappa_5 = 2^{r+1} \pi^{r_2} |D_K|^{-1/2} e^{c_3 d R_K} \nu^{tdh_K} (1 + \theta)^d$$

avec

$$(5.2) \quad c_3 = \frac{1}{2} r^{r+1} \delta_K^{-(r-1)}.$$

La première étape de la démonstration du lemme 5.2 consistera à utiliser le lemme 9 de [7] que voici.

LEMME 5.3. *Soit $\beta \in O_S$. Il existe $\eta_1 \in O_S^\times$ tel que $\alpha = \eta_1 \beta$ soit dans O_K et vérifie*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \nu^{tdh_K} N_S(\beta).$$

Les liens avec les notations $|\alpha|_K$ et $|\beta|_S$ de [7] sont

$$|\alpha|_K = |N_{K/\mathbb{Q}}(\alpha)|^{1/d} \quad \text{et} \quad |\beta|_S = N_S(\beta)^{1/d}.$$

Notons que le lemme 5.3 est trivial quand $\beta = 0$ avec $\eta_1 = 1$ et $\alpha = 0$.

Nous utiliserons ensuite le résultat suivant qui est un scolie découlant du lemme 2 de [3], avec la constante c_3 introduite en (5.2).

LEMME 5.4. *Soit $\alpha \in \mathcal{O}_K \setminus \{0\}$. Notons $M = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$. Alors il existe $\eta_2 \in \mathcal{O}_K^\times$ tel que, pour tout $v \in S_\infty$, on ait*

$$M^{d_v/d} e^{-c_3 R_K} \leq |\alpha \eta_2|_v \leq M^{d_v/d} e^{c_3 R_K}.$$

Une variante du lemme 5.4 s'obtient comme scolie du lemme 3 de [9], qui fournit le même résultat, mais avec la constante c_3 remplacée par

$$c'_3 = \begin{cases} 0 & \text{si } r = 0, \\ 1/d & \text{si } r = 1, \\ 29e(r!)r\sqrt{r-1} \log d & \text{si } r \geq 2. \end{cases}$$

Le lemme 1 de [6] et le lemme A15 de [12] donnent le même énoncé mais n'explicitent pas c_3 .

LEMME 5.5. *Soit Q un nombre réel ≥ 1 . Alors l'ensemble*

$$\Gamma := \{ \gamma \in \mathcal{O}_K \mid |\gamma|_v \leq Q^{d_v} \text{ pour tout } v \in S_\infty \}$$

est fini et a au plus

$$2^{r+1} \pi^{r^2} (Q + \theta)^d |D_K|^{-1/2}$$

éléments.

Démonstration. Choisissons un ordre sur S_∞ (en numérotant en premier les places réelles et en regroupant une place complexe et sa conjuguée) et notons $\underline{\sigma}$ le plongement canonique de K dans $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$:

$$\underline{\sigma} : K \rightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \quad \alpha \mapsto (\sigma_i(\alpha))_{1 \leq i \leq r_1+r_2},$$

où $\sigma_1, \dots, \sigma_d$ sont les plongements de K dans \mathbb{C} avec $\sigma_{r_1+r_2+j} = \bar{\sigma}_{r_1+j}$ pour $1 \leq j \leq r_2$ ($\bar{\sigma}$ désigne le conjugué complexe du plongement σ). Quand on identifie $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ à \mathbb{R}^d , l'image de \mathcal{O}_K est un réseau de \mathbb{R}^d dont une base est $\underline{\sigma}(w_1), \dots, \underline{\sigma}(w_d)$. Le paralléloétope \mathcal{P} défini par cette base est un domaine fondamental pour le réseau dont le volume est $2^{-r_2} \sqrt{|D_K|}$. La réunion des $\gamma + \mathcal{P}$ quand γ décrit Γ est une réunion disjointe contenue dans le domaine borné

$$\mathcal{B} = \{ (x_v)_{v \in S_\infty} \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |x_v| \leq Q + \theta \ (v \in S_\infty) \}.$$

Le volume de \mathcal{B} est $2^{r_1} \pi^{r_2} (Q + \theta)^d$. Le lemme 5.5 en résulte. ■

Preuve du lemme 5.2. Soit β un élément de \mathcal{O}_S vérifiant $\mathrm{N}_S(\beta) \leq m$. On utilise d'abord le lemme 5.3 pour écrire $\beta = \alpha \eta_1^{-1}$ avec $\alpha \in \mathcal{O}_K$, $\eta_1 \in \mathcal{O}_S^\times$ et

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq \nu^{tdh_K} \mathrm{N}_S(\beta).$$

On utilise ensuite le lemme 5.4 pour écrire $\alpha = \eta_2^{-1} \gamma$ avec $\eta_2 \in \mathcal{O}_K^\times$ et

$$M^{d_v/d} e^{-c_3 R_K} \leq |\alpha \eta_2|_v \leq M^{d_v/d} e^{c_3 R_K} \quad \text{pour tout } v \in S_\infty,$$

avec $M = |\mathbb{N}_{K/\mathbb{Q}}(\alpha)| \leq \nu^{tdh_K} m$. On utilise enfin le lemme 5.5 avec $Q = M^{1/d} e^{c_3 R_K}$ pour dire que l'ensemble

$$\Gamma := \{ \gamma \in \mathcal{O}_K \mid |\gamma|_v \leq Q^{d_v} \text{ pour tout } v \in S_\infty \}$$

est fini et a au plus

$$2^{r+1} \pi^{r_2} (Q + \theta)^d |D_K|^{-1/2}$$

éléments. On majore $Q + \theta$ par $Q(1 + \theta)$: on a

$$2^{r+1} \pi^{r_2} (Q + \theta)^d |D_K|^{-1/2} \leq \kappa_5 m.$$

Enfin, en posant $\varepsilon = \eta_1^{-1} \eta_2^{-1}$, on a $\beta = \varepsilon \gamma$, ce qui complète la démonstration du lemme 5.2. ■

6. Preuve du théorème 3.1. Nous décomposerons la démonstration en plusieurs étapes. Dans la première, nous mettons en évidence des ensembles finis, indépendants d'une solution éventuelle $(x, y, z, \varepsilon, \varepsilon_1, \varepsilon_2, \varepsilon_3) \in \mathcal{O}_S^3 \times (\mathcal{O}_S^\times)^4$ de l'équation diophantienne (3.1).

6.1. Mise en évidence de sous-ensembles finis. Soit K un corps de nombres de degré d sur \mathbb{Q} et soient $\mu, \alpha_1, \alpha_2, \alpha_3$ des éléments non nuls de K . Soit q un entier rationnel positif tel que $q\alpha_i \in \mathcal{O}_S$ pour $i = 1, 2, 3$. Un bon choix pour q est le plus petit commun multiple (ou ppcm) des coefficients directeurs des polynômes irréductibles sur \mathbb{Z} des nombres algébriques $\alpha_1, \alpha_2, \alpha_3$. On a $N_S(q) \leq q^d$. L'existence d'une solution de (3.1) implique $q^3 \mu \in \mathcal{O}_S$. On pose

$$k = N_S(\mu) \quad \text{et} \quad m = N_S(q)^3 k,$$

de sorte que $m = N_S(q^3 \mu)$ est un entier rationnel strictement positif.

L'ensemble A_2 formé des triplets $\underline{k}' = (k'_1, k'_2, k'_3)$ d'entiers positifs satisfaisant $k'_1 k'_2 k'_3 = m$ est fini et a au plus $d(m)^2$ éléments. Soit $\underline{k}' \in A_2$ et soit $i \in \{1, 2, 3\}$. Le lemme 5.2 montre qu'il existe un sous-ensemble fini $A_1(k'_i)$ de $\mathcal{O}_S \setminus \{0\}$, ayant au plus $\kappa_5 k'_i$ éléments, avec la propriété suivante : pour tout $\beta \in \mathcal{O}_S$ vérifiant $N_S(\beta) = k'_i$, il existe $\gamma_i \in A_1(k'_i)$ et $w_i \in \mathcal{O}_S^\times$ tels que $\beta = \gamma_i w_i$.

Pour $\underline{k}' = (k'_1, k'_2, k'_3) \in A_2$, on note $A_1(\underline{k}')$ le sous-ensemble suivant de \mathcal{O}_S^3 :

$$A_1(\underline{k}') = A_1(k'_1) \times A_1(k'_2) \times A_1(k'_3).$$

Le nombre d'éléments de la réunion des $A_1(\underline{k}')$ quand \underline{k}' décrit A_2 est majoré par

$$\sum_{(k'_1, k'_2, k'_3) \in A_2} \kappa_5^3 k'_1 k'_2 k'_3 \leq \kappa_6 \quad \text{avec} \quad \kappa_6 = d(m)^2 \kappa_5^3 m.$$

Soient l un entier ≥ 2 et $\delta_1, \dots, \delta_l$ des éléments de K^\times . Notons $\underline{\delta} = (\delta_1, \dots, \delta_l) \in (K^\times)^l$. Le théorème 5.1 montre qu'il existe un sous-ensemble fini $A_3^{(l)}(\underline{\delta})$

de O_S^\times , contenant 1, ayant un nombre d'éléments majoré par (5.1), tel que, pour toute solution $(x_1, \dots, x_l) \in (O_S^\times)^l$ de l'équation

$$\delta_1 X_1 + \delta_2 X_2 + \dots + \delta_l X_l = 1$$

pour laquelle aucune sous-somme stricte

$$\sum_{i \in I} \delta_i x_i$$

ne s'annule, on ait $x_1 \in A_3^{(l)}(\underline{\delta})$.

Dans la même veine, nous noterons encore $\tilde{A}_3^{(l)}(\underline{\delta})$ l'ensemble formé par les éléments x de O_S^\times tels que l'un au moins des deux éléments x, x^{-1} appartienne à la réunion des ensembles $A_3^{(l)}(\underline{\delta}^\sigma)$ avec $\underline{\delta}^\sigma = (\delta_{\sigma(1)}, \dots, \delta_{\sigma(l)})$, quand σ décrit les transpositions $(1\ i)$ de $\{1, \dots, l\}$.

Soit $\underline{u} = (u_1, u_2, u_3) \in (O_S^\times)^3$ tel que $\text{Card}\{u_1\alpha_1, u_2\alpha_2, u_3\alpha_3\} = 3$. Pour $i = 1, 2, 3$, posons $\alpha'_i = \alpha_i u_i$,

$$\delta_1 = \frac{\alpha'_3 - \alpha'_1}{\alpha'_3 - \alpha'_1}, \quad \delta_2 = \frac{\alpha'_1 - \alpha'_1}{\alpha'_3 - \alpha'_1}, \quad \underline{\delta} = (\delta_1, \delta_2)$$

et $A_4(\underline{u}) = A_3^{(2)}(\underline{\delta})$. Alors $A_4(\underline{u})$ est un sous-ensemble fini de O_S^\times , ayant au plus κ_3 éléments, qui contient 1 et les deux quotients t_2/t_1 et t_3/t_1 quand (t_1, t_2, t_3) est un triplet d'éléments de O_S^\times satisfaisant

$$(6.1) \quad t_1(\alpha'_2 - \alpha'_3) + t_2(\alpha'_3 - \alpha'_1) + t_3(\alpha'_1 - \alpha'_2) = 0.$$

6.2. Utilisation des ensembles finis mis en évidence. Après avoir mis en évidence au lemme 5.2 et à la section 6.1 les sous-ensembles finis $A_1(m), A_2, A_1(\underline{k}'), A_3^{(l)}(\underline{\delta}), \tilde{A}_3^{(l)}(\underline{\delta}), A_4(\underline{u})$, nous pouvons procéder à la démonstration du théorème 3.1 proprement dite.

Partons d'une solution $(x, y, z, \varepsilon, \varepsilon_1, \varepsilon_2, \varepsilon_3) \in O_S^\times \times (O_S^\times)^4$ de l'équation diophantienne (3.1) avec $xy \neq 0$ et prenons pour q le plus petit entier rationnel positif tel que $q\alpha_i \in O_S$ pour $i = 1, 2, 3$. Posons, pour $i = 1, 2, 3$,

$$\tilde{\alpha}_i = \alpha_i \varepsilon_i, \quad \beta_i = x - \tilde{\alpha}_i y, \quad \beta'_i = qx - q\tilde{\alpha}_i y = q\beta_i, \quad k'_i = N_S(\beta'_i),$$

de sorte que $\beta'_1 \beta'_2 \beta'_3 = q^3 \mu \varepsilon$ et $k'_1 k'_2 k'_3 = m$, où $m = N_S(q^3 \mu)$. Comme nous l'avons déjà remarqué, l'existence d'une solution implique $q^3 \mu \in O_S$. Par définition de A_2 , on a $(k'_1, k'_2, k'_3) \in A_2$.

La construction de $A_1(\underline{k}')$ montre qu'il existe $\underline{\gamma} = (\gamma_1, \gamma_2, \gamma_3) \in A_1(\underline{k}')$ et $(w_1, w_2, w_3) \in (O_S^\times)^3$ tels que

$$\beta'_i \gamma_i^{-1} = w_i \quad \text{pour } i = 1, 2, 3.$$

Rappelons maintenant que $\text{Card}\{\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3\} = 3$. Nous allons construire deux sous-ensembles finis $A_3(\underline{\gamma}, i)$ ($i = 2, 3$) de O_S^\times , contenant 1 et ayant au plus κ_4 éléments, tels que $\varepsilon_i/\varepsilon_1 \in A_3(\underline{\gamma}, i)$ pour $i = 2, 3$.

Soit $i \in \{2, 3\}$. On a $\tilde{\alpha}_i \neq \tilde{\alpha}_1$. Soit j tel que $\{i, j\} = \{2, 3\}$. Alors $\tilde{\alpha}_1, \tilde{\alpha}_i, \tilde{\alpha}_j$ sont deux à deux distincts. En éliminant x et y entre les trois équations

$$x - \tilde{\alpha}_1 y = \beta_1, \quad x - \tilde{\alpha}_i y = \beta_i, \quad x - \tilde{\alpha}_j y = \beta_j,$$

c'est-à-dire, en écrivant

$$(x - \tilde{\alpha}_1 y)(\tilde{\alpha}_i - \tilde{\alpha}_j) + (x - \tilde{\alpha}_i y)(\tilde{\alpha}_j - \tilde{\alpha}_1) + (x - \tilde{\alpha}_j y)(\tilde{\alpha}_1 - \tilde{\alpha}_i) = 0,$$

on trouve que le nombre

$$(6.2) \quad \mathcal{T} = \beta_1 \tilde{\alpha}_i - \beta_1 \tilde{\alpha}_j + \beta_i \tilde{\alpha}_j - \beta_i \tilde{\alpha}_1 + \beta_j \tilde{\alpha}_1 - \beta_j \tilde{\alpha}_i$$

est nul.

Pour toute permutation $(j_1, j_2, j_3) = (\sigma(1), \sigma(i), \sigma(j))$ de $(1, i, j)$, nous pouvons écrire l'égalité $\mathcal{T} = 0$, avec \mathcal{T} défini par (6.2), sous la forme

$$(6.3) \quad \text{sgn}(\sigma) \left(\frac{\tilde{\alpha}_{j_3}}{\tilde{\alpha}_{j_2}} - \frac{\beta_{j_2} \tilde{\alpha}_{j_3}}{\beta_{j_1} \tilde{\alpha}_{j_2}} + \frac{\beta_{j_2} \tilde{\alpha}_{j_1}}{\beta_{j_1} \tilde{\alpha}_{j_2}} - \frac{\beta_{j_3} \tilde{\alpha}_{j_1}}{\beta_{j_1} \tilde{\alpha}_{j_2}} + \frac{\beta_{j_3}}{\beta_{j_1}} \right) = 1,$$

où $\text{sgn}(\sigma)$ est la signature de la permutation σ .

6.2.1. Premier cas : *Aucune sous-somme stricte de \mathcal{T} ne s'annule.* Dans ce cas, on prend $l = 5$, on pose

$$\delta_1 = \frac{\alpha_i}{\alpha_1}, \quad \delta_2 = -\frac{\gamma_1 \alpha_i}{\gamma_j \alpha_1}, \quad \delta_3 = \frac{\gamma_1 \alpha_j}{\gamma_j \alpha_1}, \quad \delta_4 = -\frac{\gamma_i \alpha_j}{\gamma_j \alpha_1}, \quad \delta_5 = \frac{\gamma_i}{\gamma_j},$$

et il s'avère que l'on peut prendre l'ensemble $A_3(\underline{\gamma}, i)$ égal à $A_3^{(5)}(\underline{\delta})$ avec $\underline{\delta} = (\delta_1, \dots, \delta_5)$. En effet, cet ensemble a au plus κ_4 éléments, d'après le théorème 5.1. Pour montrer que le quotient $\varepsilon_i/\varepsilon_1$ appartient à $A_3^{(5)}(\underline{\delta})$, on écrit (6.3) avec $(j_1, j_2, j_3) = (j, 1, i)$ sous la forme

$$\delta_1 \frac{\varepsilon_i}{\varepsilon_1} + \delta_2 \frac{w_1}{w_j} \frac{\varepsilon_i}{\varepsilon_1} + \delta_3 \frac{w_1}{w_j} \frac{\varepsilon_j}{\varepsilon_1} + \delta_4 \frac{w_i}{w_j} \frac{\varepsilon_j}{\varepsilon_1} + \delta_5 \frac{w_i}{w_j} = 1.$$

et on utilise la définition de $A_3^{(5)}(\underline{\delta})$.

6.2.2. Deuxième cas : *Au moins une sous-somme stricte s'annule*

6.2.2.1. Preuve que la somme \mathcal{T} ne se décompose pas en trois sous-sommes nulles de deux termes chacune. Pour chacune des 15 partitions de l'ensemble

$$\mathcal{E} = \{(1, i), (1, j), (i, 1), (i, j), (j, 1), (j, i)\}$$

en trois sous-ensembles de deux éléments, disons $\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3$, au moins un des ensembles $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ peut s'écrire $\{(j_1, j_2), (l_1, l_2)\}$ avec

$$j_1 = l_1 \quad \text{ou} \quad j_2 = l_2 \quad \text{ou} \quad (j_1, j_2) = (l_2, l_1).$$

Aucune sous-somme $\pm(\beta_{j_1} \tilde{\alpha}_{j_2} - \beta_{l_1} \tilde{\alpha}_{l_2})$ sur un ensemble à deux termes $\{(j_1, j_2), (l_1, l_2)\}$ avec $j_1 = l_1$ (donc $j_2 \neq l_2$) ne s'annule, car

$$\beta_{j_1}(\tilde{\alpha}_{j_2} - \tilde{\alpha}_{l_2}) \neq 0.$$

De même, aucune sous-somme sur un ensemble $\{(j_1, j_2), (l_1, l_2)\}$ avec $j_2 = l_2$ (donc $j_1 \neq l_1$) ne s'annule, car

$$(\beta_{j_1} - \beta_{l_1})\tilde{\alpha}_{j_2} \neq 0.$$

Enfin, aucune sous-somme sur un ensemble $\{(j_1, j_2), (l_1, l_2)\}$ avec $(j_1, j_2) = (l_2, l_1)$ ne s'annule, car

$$\beta_{j_1}\tilde{\alpha}_{j_2} - \beta_{j_2}\tilde{\alpha}_{j_1} = (\tilde{\alpha}_{j_2} - \tilde{\alpha}_{j_1})x \neq 0.$$

On en déduit que la somme \mathcal{T} de (6.2) ne se décompose pas en trois sous-sommes nulles de deux termes.

6.2.2.2. *Cas où \mathcal{T} se décompose en deux sous-sommes nulles de trois termes.* Supposons $\mathcal{T} = \mathcal{T}_1 + \mathcal{T}_2$ avec \mathcal{T}_1 et \mathcal{T}_2 sous-sommes de trois termes et $\mathcal{T}_1 = \mathcal{T}_2 = 0$. Alors aucune sous-somme stricte de \mathcal{T}_1 ni de \mathcal{T}_2 ne s'annule.

• *Supposons que deux des trois indices des β dans \mathcal{T}_1 sont égaux.* Il existe alors une permutation $(j_1, j_2, j_3) = (\sigma(1), \sigma(i), \sigma(j))$ telle que l'on ait soit

$$\text{sgn}(\sigma)\mathcal{T}_1 = \beta_{j_1}\tilde{\alpha}_{j_2} - \beta_{j_1}\tilde{\alpha}_{j_3} + \beta_{j_3}\tilde{\alpha}_{j_1} \quad \text{et} \quad \text{sgn}(\sigma)\mathcal{T}_2 = \beta_{j_2}\tilde{\alpha}_{j_3} - \beta_{j_2}\tilde{\alpha}_{j_1} - \beta_{j_3}\tilde{\alpha}_{j_2},$$

soit

$$\text{sgn}(\sigma)\mathcal{T}_1 = \beta_{j_1}\tilde{\alpha}_{j_2} - \beta_{j_1}\tilde{\alpha}_{j_3} - \beta_{j_3}\tilde{\alpha}_{j_2} \quad \text{et} \quad \text{sgn}(\sigma)\mathcal{T}_2 = \beta_{j_2}\tilde{\alpha}_{j_3} - \beta_{j_2}\tilde{\alpha}_{j_1} + \beta_{j_3}\tilde{\alpha}_{j_1}.$$

Commençons par le premier cas. Posons $\underline{\delta} = (\delta_1, \delta_2)$ et $\underline{\delta}' = (\delta'_1, \delta'_2)$ avec

$$\delta_1 = \frac{\alpha_{j_2}}{\alpha_{j_3}}, \quad \delta_2 = \frac{\gamma_{j_3}\alpha_{j_1}}{\gamma_{j_1}\alpha_{j_3}}, \quad \delta'_1 = \frac{\alpha_{j_1}}{\alpha_{j_3}}, \quad \delta'_2 = \frac{\gamma_{j_3}\alpha_{j_2}}{\gamma_{j_2}\alpha_{j_3}},$$

de sorte que

$$\delta_1 \frac{\varepsilon_{j_2}}{\varepsilon_{j_3}} + \delta_2 \frac{w_{j_3}}{w_{j_1}} \frac{\varepsilon_{j_1}}{\varepsilon_{j_3}} = \delta'_1 \frac{\varepsilon_{j_1}}{\varepsilon_{j_3}} + \delta'_2 \frac{w_{j_3}}{w_{j_2}} \frac{\varepsilon_{j_2}}{\varepsilon_{j_3}} = 1.$$

Il en résulte que si on définit $\xi_1 := \varepsilon_{j_2}/\varepsilon_{j_3}$ et $\xi_2 := \varepsilon_{j_1}/\varepsilon_{j_3}$, on a $\xi_1 \in A_3^{(2)}(\underline{\delta})$ et $\xi_2 \in A_3^{(2)}(\underline{\delta}')$, tandis que $\xi_1^{-1} = \varepsilon_{j_3}/\varepsilon_{j_2} \in \tilde{A}_3^{(2)}(\underline{\delta})$ et $\xi_2^{-1} = \varepsilon_{j_3}/\varepsilon_{j_1} \in \tilde{A}_3^{(2)}(\underline{\delta}')$. Comme

$$\xi_1 \xi_2^{-1} = \frac{\varepsilon_{j_2}}{\varepsilon_{j_1}} \quad \text{et} \quad \xi_1^{-1} \xi_2 = \frac{\varepsilon_{j_1}}{\varepsilon_{j_2}},$$

l'un des nombres $\xi_1, \xi_2, \xi_1^{-1}, \xi_2^{-1}, \xi_1 \xi_2^{-1}, \xi_1^{-1} \xi_2$ est égal à $\varepsilon_i/\varepsilon_1$. Enfin, comme $1 \in A_3^{(2)}(\underline{\delta}) \cap A_3^{(2)}(\underline{\delta}')$, on pose

$$A_3(\underline{\gamma}, i) = \{\vartheta_1 \vartheta_2 \in O_S^\times \mid \vartheta_1 \in \tilde{A}_3^{(2)}(\underline{\delta}), \vartheta_2 \in \tilde{A}_3^{(2)}(\underline{\delta}')\}.$$

On vérifie encore que $A_3(\underline{\gamma}, i)$ a au plus κ_4 éléments et qu'il contient $\varepsilon_i/\varepsilon_1$.

Passons au deuxième cas. Posons

$$\delta_1 = \frac{\alpha_{j_3}}{\alpha_{j_2}}, \quad \delta_2 = \frac{\gamma_{j_3}}{\gamma_{j_1}}, \quad \delta'_1 = \frac{\alpha_{j_3}}{\alpha_{j_1}}, \quad \delta'_2 = \frac{\gamma_{j_3}}{\gamma_{j_2}}.$$

Nous avons

$$\delta_1 \frac{\varepsilon_{j_3}}{\varepsilon_{j_2}} + \delta_2 \frac{w_{j_3}}{w_{j_1}} = \delta'_1 \frac{\varepsilon_{j_3}}{\varepsilon_{j_1}} + \delta'_2 \frac{w_{j_3}}{w_{j_2}} = 1.$$

Par conséquent, si nous posons $\underline{\delta} = (\delta_1, \delta_2)$, $\underline{\delta}' = (\delta'_1, \delta'_2)$, $\xi_1 := \varepsilon_{j_3}/\varepsilon_{j_2}$ et $\xi_2 := \varepsilon_{j_3}/\varepsilon_{j_1}$, nous avons $\xi_1 \in A_3^{(2)}(\underline{\delta})$, $\xi_2 \in A_3^{(2)}(\underline{\delta}')$, et aussi

$$\xi_1^{-1} = \frac{\varepsilon_{j_2}}{\varepsilon_{j_3}} \in \tilde{A}_3^{(2)}(\underline{\delta}), \quad \xi_2^{-1} := \frac{\varepsilon_{j_1}}{\varepsilon_{j_3}} \in \tilde{A}_3^{(2)}(\underline{\delta}').$$

Enfin

$$\xi_1^{-1} \xi_2 = \frac{\varepsilon_{j_2}}{\varepsilon_{j_1}} \quad \text{et} \quad \xi_1 \xi_2^{-1} = \frac{\varepsilon_{j_1}}{\varepsilon_{j_2}}.$$

Nous posons donc

$$A_3(\underline{\gamma}, i) = \{\vartheta_1 \vartheta_2 \mid \vartheta_1 \in \tilde{A}_3^{(2)}(\underline{\delta}), \vartheta_2 \in \tilde{A}_3^{(2)}(\underline{\delta}')\}.$$

• *Supposons que les trois indices des β dans \mathcal{T}_1 sont distincts mais que deux des trois indices des $\tilde{\alpha}$ dans \mathcal{T}_1 sont égaux.* Il existe alors une permutation $(j_1, j_2, j_3) = (\sigma(1), \sigma(i), \sigma(j))$ telle que

$$\text{sgn}(\sigma)\mathcal{T}_1 = \beta_{j_1} \tilde{\alpha}_{j_2} - \beta_{j_2} \tilde{\alpha}_{j_1} - \beta_{j_3} \tilde{\alpha}_{j_2}, \quad \text{sgn}(\sigma)\mathcal{T}_2 = -\beta_{j_1} \tilde{\alpha}_{j_3} + \beta_{j_2} \tilde{\alpha}_{j_3} + \beta_{j_3} \tilde{\alpha}_{j_1}.$$

Dans ce cas on pose

$$\delta_1 = \frac{\gamma_{j_3}}{\gamma_{j_1}}, \quad \delta_2 = \frac{\gamma_{j_2} \alpha_{j_1}}{\gamma_{j_1} \alpha_{j_2}}, \quad \delta'_1 = \frac{\gamma_{j_2}}{\gamma_{j_1}}, \quad \delta'_2 = \frac{\gamma_{j_3} \alpha_{j_1}}{\gamma_{j_1} \alpha_{j_3}},$$

de sorte que

$$\delta_1 \frac{w_{j_3}}{w_{j_1}} + \delta_2 \frac{w_{j_2}}{w_{j_1}} \frac{\varepsilon_{j_1}}{\varepsilon_{j_2}} = \delta'_1 \frac{w_{j_2}}{w_{j_1}} + \delta'_2 \frac{w_{j_3}}{w_{j_1}} \frac{\varepsilon_{j_1}}{\varepsilon_{j_3}} = 1.$$

Ainsi les S -unités

$$\xi_1 := \frac{w_{j_2}}{w_{j_1}}, \quad \xi_2 := \frac{w_{j_3}}{w_{j_1}}, \quad \xi_3 := \frac{w_{j_2}}{w_{j_1}} \frac{\varepsilon_{j_1}}{\varepsilon_{j_2}}, \quad \xi_4 := \frac{w_{j_3}}{w_{j_1}} \frac{\varepsilon_{j_1}}{\varepsilon_{j_3}}$$

vérifient

$$\xi_1 \in A_3^{(2)}(\underline{\delta}'), \quad \xi_2 \in A_3^{(2)}(\underline{\delta}), \quad \xi_3 \in \tilde{A}_3^{(2)}(\underline{\delta}), \quad \xi_4 \in \tilde{A}_3^{(2)}(\underline{\delta}'),$$

avec $\underline{\delta} = (\delta_1, \delta_2)$, $\underline{\delta}' = (\delta'_1, \delta'_2)$, et on a

$$\begin{aligned} \xi_3 \xi_1^{-1} &= \frac{\varepsilon_{j_1}}{\varepsilon_{j_2}}, & \xi_3^{-1} \xi_1 &= \frac{\varepsilon_{j_2}}{\varepsilon_{j_1}}, & \xi_4 \xi_2^{-1} &= \frac{\varepsilon_{j_1}}{\varepsilon_{j_3}}, \\ \xi_2 \xi_4^{-1} &= \frac{\varepsilon_{j_3}}{\varepsilon_{j_1}}, & \xi_2^{-1} \xi_3^{-1} \xi_1 \xi_4 &= \frac{\varepsilon_{j_2}}{\varepsilon_{j_3}}, & \xi_2 \xi_3 \xi_1^{-1} \xi_4^{-1} &= \frac{\varepsilon_{j_3}}{\varepsilon_{j_2}}. \end{aligned}$$

On pose donc

$$A_3(\underline{\gamma}, i) = \{\vartheta_1 \vartheta_2 \vartheta_3 \vartheta_4 \mid \vartheta_1, \vartheta_2 \in \tilde{A}_3^{(2)}(\underline{\delta}), \vartheta_3, \vartheta_4 \in \tilde{A}_3^{(2)}(\underline{\delta}')\}.$$

• *Supposons que les trois indices des β ainsi que les trois indices des $\tilde{\alpha}$ dans \mathcal{T}_1 sont distincts.* Il existe alors une permutation $(j_1, j_2, j_3) = (\sigma(1), \sigma(i), \sigma(j))$ telle que

$$\text{sgn}(\sigma)\mathcal{T}_1 = \beta_{j_1} \tilde{\alpha}_{j_2} + \beta_{j_2} \tilde{\alpha}_{j_3} + \beta_{j_3} \tilde{\alpha}_{j_1}, \quad \text{sgn}(\sigma)\mathcal{T}_2 = -\beta_{j_1} \tilde{\alpha}_{j_3} - \beta_{j_2} \tilde{\alpha}_{j_1} - \beta_{j_3} \tilde{\alpha}_{j_2}.$$

On pose

$$\delta_1 = -\frac{\gamma_{j_3}\alpha_{j_1}}{\gamma_{j_1}\alpha_{j_2}}, \quad \delta_2 = -\frac{\gamma_{j_2}\alpha_{j_3}}{\gamma_{j_1}\alpha_{j_2}}, \quad \delta'_1 = -\frac{\gamma_{j_2}\alpha_{j_1}}{\gamma_{j_1}\alpha_{j_3}}, \quad \delta'_2 = -\frac{\gamma_{j_3}\alpha_{j_2}}{\gamma_{j_1}\alpha_{j_3}},$$

de sorte que

$$\delta_1 \frac{w_{j_3}}{w_{j_1}} \frac{\varepsilon_{j_1}}{\varepsilon_{j_2}} + \delta_2 \frac{w_{j_2}}{w_{j_1}} \frac{\varepsilon_{j_3}}{\varepsilon_{j_2}} = \delta'_1 \frac{w_{j_2}}{w_{j_1}} \frac{\varepsilon_{j_1}}{\varepsilon_{j_3}} + \delta'_2 \frac{w_{j_3}}{w_{j_1}} \frac{\varepsilon_{j_2}}{\varepsilon_{j_3}} = 1.$$

Ainsi les S -unités

$$\xi_1 := \frac{w_{j_3}}{w_{j_1}} \frac{\varepsilon_{j_1}}{\varepsilon_{j_2}}, \quad \xi_2 := \frac{w_{j_2}}{w_{j_1}} \frac{\varepsilon_{j_3}}{\varepsilon_{j_2}}, \quad \xi_3 := \frac{w_{j_2}}{w_{j_1}} \frac{\varepsilon_{j_1}}{\varepsilon_{j_3}}, \quad \xi_4 := \frac{w_{j_3}}{w_{j_1}} \frac{\varepsilon_{j_2}}{\varepsilon_{j_3}}$$

vérifient

$$\xi_1, \xi_2 \in \widetilde{A}_3^{(2)}(\underline{\delta}), \quad \xi_3, \xi_4 \in \widetilde{A}_3^{(2)}(\underline{\delta}'),$$

avec $\underline{\delta} = (\delta_1, \delta_2)$, $\underline{\delta}' = (\delta'_1, \delta'_2)$, et on a

$$\frac{\xi_3 \xi_4}{\xi_1 \xi_2} = \frac{\varepsilon_{j_2}^3}{\varepsilon_{j_3}^3}, \quad \frac{\xi_1^2 \xi_3}{\xi_2 \xi_4^2} = \frac{\varepsilon_{j_1}^3}{\varepsilon_{j_2}^3}, \quad \frac{\xi_2^2 \xi_4}{\xi_1 \xi_3^2} = \frac{\varepsilon_{j_3}^3}{\varepsilon_{j_1}^3},$$

de sorte que l'on a aussi en mains les inverses de ces trois derniers nombres.

On pose donc

$$A_3(\underline{\gamma}, i) = \left\{ \zeta \in O_S^\times \mid \text{il existe } \vartheta_1, \vartheta_2 \in \widetilde{A}_3^{(2)}(\underline{\delta}) \text{ et } \vartheta_3, \vartheta_4 \in \widetilde{A}_3^{(2)}(\underline{\delta}') \right. \\ \left. \text{tels que } \zeta^3 \in \left\{ \frac{\vartheta_1^2 \vartheta_3}{\vartheta_2 \vartheta_4^2}, \frac{\vartheta_3 \vartheta_4}{\vartheta_1 \vartheta_2} \right\} \right\}.$$

6.2.2.3. *Cas où \mathcal{T} se décompose en exactement deux sous-sommes nulles, l'une de deux termes et l'autre de quatre termes.* D'après ce que nous avons vu au §6.2.2.1, il existe une permutation $(j_1, j_2, j_3) = (\sigma(1), \sigma(i), \sigma(j))$ telle que

$$\text{sgn}(\sigma)\mathcal{T}_1 = \widetilde{\alpha}_{j_2}\beta_{j_1} + \widetilde{\alpha}_{j_3}\beta_{j_2} \quad \text{et} \quad \text{sgn}(\sigma)\mathcal{T}_2 = \beta_{j_3}\widetilde{\alpha}_{j_1} - \beta_{j_1}\widetilde{\alpha}_{j_3} - \widetilde{\alpha}_{j_1}\beta_{j_2} - \widetilde{\alpha}_{j_2}\beta_{j_3}$$

pour laquelle aucune sous-somme stricte de \mathcal{T}_2 ne s'annule, alors que $\mathcal{T}_1 = \mathcal{T}_2 = 0$. On pose

$$\delta_1 = \frac{\alpha_{j_2}}{\alpha_{j_1}}, \quad \delta_2 = \frac{\gamma_{j_1}\alpha_{j_3}}{\gamma_{j_3}\alpha_{j_1}}, \quad \delta_3 = \frac{\gamma_{j_2}}{\gamma_{j_3}}, \quad \underline{\delta} = (\delta_1, \delta_2, \delta_3),$$

de sorte que

$$\delta_1 \frac{\varepsilon_{j_2}}{\varepsilon_{j_1}} + \delta_2 \frac{w_{j_1}}{w_{j_3}} \frac{\varepsilon_{j_3}}{\varepsilon_{j_1}} + \delta_3 \frac{w_{j_2}}{w_{j_3}} = 1.$$

Ainsi les S -unités

$$\xi_1 := \frac{\varepsilon_{j_2}}{\varepsilon_{j_1}}, \quad \xi_2 := \frac{w_{j_1}}{w_{j_3}} \frac{\varepsilon_{j_3}}{\varepsilon_{j_1}} \quad \text{et} \quad \xi_3 := \frac{w_{j_2}}{w_{j_3}}$$

appartiennent à $\widetilde{A}_3^{(3)}(\underline{\delta})$. La relation $\mathcal{T}_1 = 0$ donne

$$\frac{w_{j_1}}{w_{j_2}} \frac{\varepsilon_{j_2}}{\varepsilon_{j_3}} = -\frac{\gamma_{j_2}\alpha_{j_3}}{\gamma_{j_1}\alpha_{j_2}}.$$

On trouve alors

$$\frac{\varepsilon_{j_2}^2}{\varepsilon_{j_3}^2} = -\frac{\gamma_{j_2}\alpha_{j_3}}{\gamma_{j_1}\alpha_{j_2}}\xi_1\xi_2^{-1}\xi_3, \quad \frac{\varepsilon_{j_1}^2}{\varepsilon_{j_3}^2} = -\frac{\gamma_{j_2}\alpha_{j_3}}{\gamma_{j_1}\alpha_{j_2}}\xi_1^{-1}\xi_2^{-1}\xi_3.$$

On pose donc

$$A_3(\underline{\gamma}, i) = \tilde{A}_3^{(3)}(\underline{\delta}) \cup \left\{ \zeta \in O_S^\times \mid \text{il existe } \vartheta_1, \vartheta_2, \vartheta_3 \in \tilde{A}_3^{(3)}(\underline{\delta}) \right. \\ \left. \text{tels que } \zeta^{\pm 2} = -\frac{\vartheta_1\vartheta_2\vartheta_3\gamma_{j_2}\alpha_{j_3}}{\gamma_{j_1}\alpha_{j_2}} \right\}.$$

6.3. Fin de la démonstration. Posons $u_1 = 1$, $u_2 = \varepsilon_2/\varepsilon_1$ et $u_3 = \varepsilon_3/\varepsilon_1$. On a donc $u_i \in A_3(\underline{\gamma}, i)$ pour $i = 1, 2, 3$. On définit $\alpha'_i := \alpha_i u_i$, de sorte que

$$\tilde{\alpha}_i = \alpha_i \varepsilon_i = \varepsilon_1 \alpha_i u_i = \varepsilon_1 \alpha'_i.$$

On pose encore $w = \varepsilon_1 y$. En éliminant x et w entre les trois équations

$$(6.4) \quad \beta_i = x - \alpha'_i w \quad (i = 1, 2, 3),$$

on trouve

$$\beta_1(\alpha'_2 - \alpha'_3) + \beta_2(\alpha'_3 - \alpha'_1) + \beta_3(\alpha'_1 - \alpha'_2) = 0,$$

ce qui signifie que $(\beta_1, \beta_2, \beta_3)$ vérifie la propriété demandée à (t_1, t_2, t_3) dans l'équation (6.1). Il en résulte que les éléments $v_i := \beta_i/\beta_1$ ($i = 1, 2, 3$) appartiennent à $A_4(\underline{u})$.

Posons $\tilde{\eta} = w_1$, $\eta = \varepsilon_1$. On a donc $\beta_1 = q^{-1}\gamma_1\tilde{\eta}$. Soit $i \in \{2, 3\}$. On calcule $y = \eta^{-1}w$ en éliminant x entre deux des équations (6.4) :

$$y = \eta^{-1}\tilde{\eta}y_0, \quad \text{avec} \quad y_0 = \frac{\gamma_1(v_1 - v_i)}{q(\alpha'_i - \alpha'_1)}.$$

On utilise encore une des équations (6.4) pour trouver x :

$$x = \tilde{\eta}x_0, \quad \text{avec} \quad x_0 = q^{-1}\gamma_1 + \alpha'_1 y_0.$$

On pose enfin

$$\varepsilon_0 = \frac{\gamma_1^3 v_2 v_3}{q^n \mu},$$

de sorte que $\varepsilon = \tilde{\eta}^3 \varepsilon_0$, ce qui montre que les solutions $(x, y, z, \varepsilon, \varepsilon_1, \varepsilon_2, \varepsilon_3)$ et $(x_0, y_0, z_0 \varepsilon_0, 1, u_2, u_3)$ sont S^3 -dépendantes.

À une solution $(x, y, z, \varepsilon, \varepsilon_1, \varepsilon_2, \varepsilon_3)$ de l'équation (3.1), nous avons associé un élément \underline{k}' de A_2 , puis un élément $\underline{\gamma}$ de $A_1(\underline{k}')$ (rappelons qu'il y a au plus κ_6 éléments dans la réunion des $A_1(\underline{k}')$ quand \underline{k}' décrit A_2), puis un élément \underline{u} de $\{1\} \times A_3(\underline{\gamma}, 2) \times \cdots \times A_3(\underline{\gamma}, 3)$ (il y en a au plus κ_4^2), et enfin un élément \underline{v} de $A_4(\underline{u})^2$ (il y en a au plus κ_3^2). Nous en avons conclu que la solution de départ était dans la même classe de S^3 -dépendance que

$(x_0, y_0, z_0 \varepsilon_0, 1, u_2, u_3)$. Le théorème 3.1 en résulte, avec

$$(6.5) \quad \kappa_1 = \kappa_6 \kappa_3^2 \kappa_4^2.$$

Comme annoncé, cette constante κ_1 ne dépend que de $K, N_S(\mu), \alpha_1, \alpha_2, \alpha_3$ et du rang s du groupe O_S^\times . Rappelons que

$$\kappa_3 = 1 + 2^{8s+24}, \quad \kappa_4 = 1 + (2^{4375} 3^{250})^s, \quad \kappa_6 = d(m)^2 \kappa_5^3 m$$

avec $m = N_S(q^3 \mu)$, où q est le plus petit entier rationnel positif tel que $q\alpha_i \in O_S$ pour $i = 1, 2, 3$,

$$\kappa_5 = 2^{r+1} \pi^{r_2} |D_K|^{-1/2} e^{c_3 d R_K \nu^{tdh_K} (1 + \theta)^d},$$

où r est le rang du groupe des unités de K , d son degré, D_K son discriminant, h_K son nombre de classes, R_K son régulateur ; ν est le plus grand des nombres $|\mathbb{N}(\mathfrak{P}_i)|$ ($1 \leq i \leq t$) quand $\mathfrak{P}_1, \dots, \mathfrak{P}_t$ sont les idéaux premiers de O_K au-dessus des places ultramétriques de K dans S ,

$$\theta \leq |D_K|^{1/2}, \quad c_3 = \frac{1}{2} r^{r+1} \delta_K^{-(r-1)}$$

et δ_K est la constante (de Blanksby et Montgomery, Dobrowolski et Voutier, cf. [3]) telle que tout entier algébrique non nul $\alpha \in K$ qui n'est pas une racine de l'unité vérifie $h(\alpha) \geq \delta_K/d$. ■

7. Preuve du corollaire 3.6. On utilise le théorème 3.1 avec

$$n = d, \quad \mu = k/a_0, \quad \alpha_i = \sigma_i(\alpha), \quad \varepsilon_i = \sigma_i(\varepsilon) \quad \text{pour } i = 1, \dots, d.$$

L'hypothèse $[\mathbb{Q}(\alpha\varepsilon) : \mathbb{Q}] \geq 3$ du corollaire 3.6 garantit que, quitte à permuter les α_i , l'hypothèse $\text{Card}\{\alpha_1 \varepsilon_1, \alpha_2 \varepsilon_2, \alpha_3 \varepsilon_3\} \geq 3$ du théorème 3.1 est satisfaite.

Soient $(x, y, \varepsilon, z_1, \dots, z_t)$ et $(x', y', \varepsilon', z'_1, \dots, z'_t)$ deux solutions dans $\mathbb{Z}^2 \times O_S^\times \times \mathbb{N}^t$ et S^3 -dépendantes de l'équation (3.3), satisfaisant $\text{pgcd}(xy, p_1 \cdots p_t) = \text{pgcd}(x'y', p_1 \cdots p_t) = 1$. La condition de S^3 -dépendance signifie qu'il existe des S -unités η et $\tilde{\eta}$ dans O_S^\times telles que

$$x' = x\tilde{\eta}, \quad y' = y\eta^{-1}\tilde{\eta}, \quad p_1^{z'_1} \cdots p_t^{z'_t} = p_1^{z_1} \cdots p_t^{z_t} \tilde{\eta}^n, \quad \sigma_i(\varepsilon') = \sigma_i(\varepsilon)\eta \quad (1 \leq i \leq n).$$

La relation $x' = x\tilde{\eta}$ implique que $\tilde{\eta} \in \mathbb{Q} \cap O_S^\times = \{\pm 1\} \times p_1^{\mathbb{Z}} \times \cdots \times p_t^{\mathbb{Z}}$. Comme x et x' sont premiers avec $p_1 \cdots p_t$, on en déduit $\tilde{\eta} = \pm 1$. Ensuite la relation $y' = y\eta^{-1}\tilde{\eta}$ implique, avec les mêmes arguments, que $\eta = \pm 1$. Il en résulte que $\varepsilon' = \eta\varepsilon$ et $(z'_1, \dots, z'_t) = (z_1, \dots, z_t)$. Par conséquent, dans chaque classe de S^3 -dépendance, il y a au plus quatre éléments $(x, y, \varepsilon, z_1, \dots, z_t)$ satisfaisant $f_\varepsilon(x, y) = kp_1^{z_1} \cdots p_t^{z_t}$. On en déduit le corollaire 3.6 avec

$$(7.1) \quad \kappa_2 = 4\kappa_1,$$

où on prend pour paramètres de la constante κ_1 le corps de nombres $K = \mathbb{Q}(\alpha)$, puis $\mu = k$, $\alpha_i = \sigma_i(\alpha)$ ($i = 1, 2, 3$) et $s = t + r + 1$, où r est le rang du groupe des unités de K . ■

8. Preuve de la proposition 3.4. Il s'agit de vérifier que pour tout $\underline{\varepsilon} \in \mathcal{E} \setminus \mathcal{E}^*$, il n'y a qu'un nombre fini de $\underline{\varepsilon}' \in \mathcal{E} \setminus \mathcal{E}^*$ tels que les formes $f_{\underline{\varepsilon}}$ et $f_{\underline{\varepsilon}'}$ soient S -équivalentes. Soient donc $\underline{\varepsilon}$ et $\underline{\varepsilon}'$ deux éléments distincts de $\mathcal{E} \setminus \mathcal{E}^*$ tels que $f_{\underline{\varepsilon}}$ et $f_{\underline{\varepsilon}'}$ soient S -équivalents : il existe $(\alpha, \beta, \gamma, \delta, \eta) \in O_S^4 \times O_S^\times$ tel que $\alpha\delta - \beta\gamma \in O_S^\times$ et

$$f_{\underline{\varepsilon}}(X, Y) = \eta f_{\underline{\varepsilon}'}(\alpha X + \beta Y, \gamma X + \delta Y).$$

Cette relation s'écrit

$$\prod_{j=1}^n (X - \alpha_j \varepsilon_j Y) = \eta \prod_{i=1}^n ((\alpha - \gamma \alpha_i \varepsilon'_i) X + (\beta - \delta \alpha_i \varepsilon'_i) Y),$$

c'est-à-dire,

$$\eta \prod_{i=1}^n (\alpha - \gamma \alpha_i \varepsilon'_i) = 1 \quad \text{et} \quad \prod_{j=1}^n (X - \alpha_j \varepsilon_j Y) = \prod_{i=1}^n \left(X + \frac{\beta - \delta \alpha_i \varepsilon'_i}{\alpha - \gamma \alpha_i \varepsilon'_i} Y \right).$$

Donc il existe une permutation σ de $\{1, \dots, n\}$ pour laquelle on a, pour $i = 1, \dots, n$,

$$\alpha_{\sigma(i)} \varepsilon_{\sigma(i)} (\gamma \alpha_i \varepsilon'_i - \alpha) = \beta - \delta \alpha_i \varepsilon'_i.$$

Soit i un indice dans $\{2, \dots, n\}$ tel que $\alpha_i \varepsilon'_i \neq \alpha_1$ (rappelons que $\varepsilon'_1 = 1$). Nous allons vérifier que ε'_i appartient à un ensemble fini indépendant de $(\alpha, \beta, \gamma, \delta, \eta)$. Soit j un autre indice dans $\{2, \dots, n\}$ tel que les trois nombres $\alpha_1, \alpha_i \varepsilon'_i, \alpha_j \varepsilon'_j$ soient deux à deux distincts.

Comme $f_{\underline{\varepsilon}}(1, 0) = 1$ et $f_{\underline{\varepsilon}'}(\alpha\delta - \beta\gamma, 0) = (\alpha\delta - \beta\gamma)^n$, on a

$$f_{\underline{\varepsilon}'}(\alpha, \gamma) = \eta^{-1} \in O_S^\times \quad \text{et} \quad f_{\underline{\varepsilon}}(\delta, -\gamma) = \eta(\alpha\delta - \beta\gamma)^n \in O_S^\times.$$

Par définition de \mathcal{E}^* , il en résulte que $\alpha\gamma = \delta\gamma = 0$.

Si $(\alpha, \delta) = (0, 0)$, on a $\beta\gamma \neq 0$ et

$$\alpha_{\sigma(i)} \varepsilon_{\sigma(i)} \alpha_i \varepsilon'_i = \alpha_{\sigma(1)} \varepsilon_{\sigma(1)} \alpha_1,$$

ce qui montre qu'il y a au plus $n!$ valeurs possibles pour ε'_i .

Il reste à considérer le cas où $\gamma = 0$. Les trois équations

$$\begin{cases} \alpha \alpha_{\sigma(1)} \varepsilon_{\sigma(1)} - \delta \alpha_1 + \beta = 0, \\ \alpha \alpha_{\sigma(i)} \varepsilon_{\sigma(i)} - \delta \alpha_i \varepsilon'_i + \beta = 0, \\ \alpha \alpha_{\sigma(j)} \varepsilon_{\sigma(j)} - \delta \alpha_j \varepsilon'_j + \beta = 0 \end{cases}$$

montrent que $\alpha_{\sigma(1)} \varepsilon_{\sigma(1)}$, $\alpha_{\sigma(i)} \varepsilon_{\sigma(i)}$ et $\alpha_{\sigma(j)} \varepsilon_{\sigma(j)}$ sont deux à deux distincts. On élimine α , β et δ entre ces trois équations, ce qui donne l'équation aux S -unités à la Siegel

$$\begin{aligned} (\alpha_{\sigma(i)} \varepsilon_{\sigma(i)} - \alpha_{\sigma(j)} \varepsilon_{\sigma(j)}) \alpha_1 + (\alpha_{\sigma(j)} \varepsilon_{\sigma(j)} - \alpha_{\sigma(1)} \varepsilon_{\sigma(1)}) \alpha_i \varepsilon'_i \\ + (\alpha_{\sigma(1)} \varepsilon_{\sigma(1)} - \alpha_{\sigma(i)} \varepsilon_{\sigma(i)}) \alpha_j \varepsilon'_j = 0. \end{aligned}$$

On déduit du théorème 2.3 que ε'_i appartient à un ensemble fini, ce qu'il fallait démontrer. De plus, comme cette dernière équation aux unités n'a que trois termes, le résultat peut être démontré de façon effective: on peut donner une borne pour les hauteurs des $\underline{\varepsilon}' \in \mathcal{E} \setminus \mathcal{E}^*$ tels que les formes $f_{\underline{\varepsilon}}$ et $f_{\underline{\varepsilon}'}$ soient S -équivalentes. ■

Remerciements. Ce projet de recherche est né lors de séances de jogging sur le bord des plages de Rio. Les auteurs expriment leur reconnaissance à ceux qui ont rendu possibles, agréables et productifs leurs séjours communs au Brésil (Instituto Nacional de Matematica Pura e Aplicada (IMPA)), au Népal (Université de Tribhuvan et Université de Kathmandu) et en Inde (Congrès International des Mathématiciens ICM 2010) où ces recherches ont été entreprises et concrétisées. De pertinentes remarques d'Isao Wakabayashi sur une version préliminaire de ce texte nous ont été utiles. Gaël Rémond nous a aidés à faire le lien (qui nous avait été indiqué par un arbitre anonyme) avec le théorème de Vojta.

Références

- [1] F. Amoroso and E. Viada, *Small points on subvarieties of a torus*, Duke Math. J. 150 (2009), 407–442.
- [2] F. Beukers and H. P. Schlickewei, *The equation $x + y = 1$ in finitely generated groups*, Acta Arith. 78 (1996), 189–199.
- [3] Y. Bugeaud and K. Györy, *Bounds for the solutions of Thue–Mahler equations and norm form equations*, *ibid.* 74 (1996), 273–292.
- [4] P. Erdős, C. L. Stewart and R. Tijdeman, *Some Diophantine equations with many solutions*, Compos. Math. 66 (1988), 37–56.
- [5] J.-H. Evertse, *The number of solutions of decomposable form equations*, Invent. Math. 122 (1995), 559–601.
- [6] J.-H. Evertse and K. Györy, *Thue–Mahler equations with a small number of solutions*, J. Reine Angew. Math. 399 (1989), 60–80.
- [7] J.-H. Evertse and K. Györy, *Effective finiteness results for binary forms with given discriminant*, Compos. Math. 79 (1991), 169–204.
- [8] J.-H. Evertse, K. Györy, C. L. Stewart and R. Tijdeman, *S -unit equations and their applications*, in: *New Advances in Transcendence Theory* (Durham, 1986), Cambridge Univ. Press, Cambridge, 1988, 110–174.
- [9] K. Györy and K. Yu, *Bounds for the solutions of S -unit equations and decomposable form equations*, Acta Arith. 123 (2006), 9–41.
- [10] C. Heuberger, *Parametrized Thue equations—a survey*, <http://www.math.tugraz.at/~cheub/thue.html>.
- [11] C. Levesque and M. Waldschmidt, *Some remarks on diophantine equations and diophantine approximation*, 2011, soumis.
- [12] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Math. 87, Cambridge Univ. Press, Cambridge, 1986.
- [13] E. Thomas, *Complete solutions to a family of cubic Diophantine equations*, J. Number Theory 34 (1990), 235–250.

- [14] P. Vojta, *Diophantine Approximations and Value Distribution Theory*, Lecture Notes in Math. 1239, Springer, Berlin, 1987.
- [15] U. Zannier, *Lecture Notes on Diophantine Analysis*, Appunti Scuola Norm. Sup. Pisa 8, Edizioni della Normale, Pisa, 2009.

Claude Levesque
Département de mathématiques
et de statistique
Université Laval
Québec, QC, Canada G1V 0A6
E-mail: Claude.Levesque@mat.ulaval.ca

Michel Waldschmidt
Institut de Mathématiques de Jussieu
Université Pierre et Marie Curie (Paris 6)
4 Place Jussieu
F-75252 Paris Cedex 05, France
E-mail: miw@math.jussieu.fr

*Reçu le 24.6.2011
et révisé le 29.8.2011*

(6743)