



HAL
open science

Vers une version explicite d'une conjecture de Schinzel

Francesco Amoroso, Njaka Andriamandratanana

► **To cite this version:**

Francesco Amoroso, Njaka Andriamandratanana. Vers une version explicite d'une conjecture de Schinzel. 2023. hal-04109813

HAL Id: hal-04109813

<https://hal.science/hal-04109813>

Preprint submitted on 30 May 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Vers une version explicite d'une conjecture de Schinzel

Francesco AMOROSO et Njaka Harilala ANDRIAMANDRATOMANANA

*Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139
Université de Caen Normandie, Campus II, BP 5186
14032 Caen Cedex, France*

In memory of Andrzej Schinzel

1 Introduction

En 2008, M. Filaseta, A. Granville et A. Schinzel [11] ont montré qu'il existe un algorithme qui permet de calculer le pgcd de deux polynômes $f, g \in \mathbb{Z}[x]$ de degré au plus $D \geq 2$ en $^1 \tilde{\mathcal{O}}_{N,h}(\log D)$ opérations binaires sous l'hypothèse qu'au moins l'un des f et g n'ait pas de facteur cyclotomique. La constante implicite dans $\tilde{\mathcal{O}}$ dépend du nombre N des coefficients non nuls de f et g et du maximum H de la valeur absolue de leur coefficients. L'hypothèse que f ou g n'est pas divisible par un polynôme cyclotomique est cruciale, comme a été déjà remarqué dans [11, p. 157]. Soient a et b deux entiers naturels premiers entre eux. Alors on a :

$$\text{pgcd}\left(x^{ab} - 1, (x^a - 1)(x^b - 1)\right) = \frac{(x^a - 1)(x^b - 1)}{x - 1}.$$

Ensuite 2015, F. Amoroso, L. Leroux et M. Sombra [4] ont précisé l'algorithme de [11]. Ils ont montré qu'il existe un algorithme qui permet de déterminer la partie non-cyclotomique du pgcd de f et g en au plus $\tilde{\mathcal{O}}_{N,h}(\log D)$ opérations binaires, même si f et g ont des facteurs cyclotomiques. On va énoncer leur résultat. On note $V(f, g)$ l'ensemble des racines communes de f, g dans $\overline{\mathbb{Q}}$. Le symbole μ_∞ désigne l'ensemble des racines de l'unité de $\overline{\mathbb{Q}}$.

Théorème 1.1. [4, Theorem 4.5] Soient $f, g \in \mathbb{Z}[x]$. Il existe un algorithme qui permet de calculer deux polynômes $p_1, p_2 \in \mathbb{Z}[x]$ tels que :

$$\begin{aligned} p_1 \mid \text{pgcd}(f, g), \quad V(p_1) \setminus \mu_\infty &= V(\text{pgcd}(f, g)) \setminus \mu_\infty \quad \text{et} \\ V(p_2) &= V(\text{pgcd}(f, g)) \cap \mu_\infty, \end{aligned}$$

1. Pour deux fonctions de la variable réel $F \geq 0$ et $G > 0$ on utilise la notation $F = \tilde{\mathcal{O}}(G)$ dès que $F \leq c_1 G (\log(1 + G))^{c_2}$ avec $c_1 > 0$ et $c_2 \geq 0$.

en au plus $\tilde{\mathcal{O}}_{N,h}(\log D)$ opérations binaires.

L'algorithme correspondant au théorème 1.1 se compose de deux procédures :

- 1) la recherche de la partie non-cyclotomique p_1 ;
- 2) la recherche de la partie cyclotomique p_2 .

L'algorithme est décrit et analysé dans [4, Algorithm 4.3]. Sa complexité est de au plus $\tilde{\mathcal{O}}_{N,h}(\log D)$ opérations binaires. Si la dépendance en N et h de la complexité de la recherche de la partie cyclotomique est explicite et peut être déduite du théorème 2.2 de L. Leroux dans [13], celle qui concerne la recherche de la partie non-cyclotomique utilise une estimation non explicite qui provient d'une ex-conjecture de Schinzel [18, Conjecture 1].

Théorème 1.2. *Soit $n \geq 1$ un entier. Soient $F, G \in \mathbb{Z}[x_1, \dots, x_n]$ tels que $\text{pgcd}(F, G) = 1$. Alors il existe $B(F, G) > 0$ satisfaisant la propriété suivante. Soient $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$, $\boldsymbol{\zeta} = (\zeta_1, \dots, \zeta_n) \in \boldsymbol{\mu}_\infty^n$ et $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$. Si*

$$F(\zeta_1 \xi^{a_1}, \dots, \zeta_n \xi^{a_n}) = G(\zeta_1 \xi^{a_1}, \dots, \zeta_n \xi^{a_n}) = 0$$

alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^n$ orthogonal à \mathbf{a} de norme L_∞ satisfaisant :

$$\|\mathbf{b}\|_\infty \leq B(F, G).$$

A. Schinzel [18, Theorem 45] avait énoncé et donné une preuve de cette conjecture dans le cas particulier $n \leq 3$ (et pour $\zeta_1 = \dots = \zeta_n = 1$). Ensuite, elle a été démontré pour n quelconque (mais toujours pour $\zeta_1 = \dots = \zeta_n = 1$) par E. Bombieri et U. Zannier [18, Appendix] et, avec une méthode partiellement différent et en toute généralité, par E. Bombieri, D. Masser et U. Zannier [7, Theorem 1.6]. Ces preuves sont effectives mais pas explicites (voir la discussion après [11, Theorem 2]). Une preuve qui explicite la dépendance de $B(F, G)$ permettrait de rendre effectif l'algorithme du théorème 1.1 pour la partie non-cyclotomique.

On présente ici une nouvelle méthode pour démontrer le théorème 1.2 en explicitant la dépendance en le degré et en la taille des coefficient de F et G . Le résultat obtenu n'est cependant pas explicite en n . Cette méthode s'inspire de l'approche de S. Checcoli, F. Veneziano et E. Viada dans [8], où les auteurs ont démontré un théorème analogue au théorème 1.2 dans le cas de produit de courbes elliptiques. L'idée principale consiste à utiliser le théorème de Bézout arithmétique de P. Philippon et une version fonctorielle du théorème de Dobrowolski généralisé.

Pour $F \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$ on note $\|F\|_1$ la norme L_1 de son vecteur des coefficients. Notre résultat principal est le théorème suivant :

Théorème 1.3. *Soient $n \geq 2$ et $s \geq 2$ deux entiers positifs et $\varepsilon \in]0, 1]$. Soient $F_1, \dots, F_s \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$, $\mathbf{a} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, $\xi \in \overline{\mathbb{Q}}^*$ et $\zeta \in \mu_\infty^n$. On suppose que la sous-variété V de \mathbb{G}_m^n définie par $F_1 = \dots = F_s = 0$ soit de codimension au moins 2 en $\alpha := \zeta \xi^{\mathbf{a}}$. Alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^n$ orthogonal à \mathbf{a} tel que :*

$$\xi^{\langle \mathbf{a}, \mathbf{b} \rangle} = 1, \quad \text{et} \quad \|\mathbf{b}\|_\infty \leq c(n, \varepsilon) \max(h_1/D^n, 1)^{1+\varepsilon} D^{2n^2},$$

où $c(n, \varepsilon) > 0$,

$$D = \max_{1 \leq i \leq s} \deg(F_i) \quad \text{et} \quad h_1 = \max_{1 \leq i \leq s} \log \|F_i\|_1.$$

Pour expliciter la dépendance en n et ε de $c(n, \varepsilon)$, il faudrait expliciter la méthode de transfert de G. Rémond [17] qui permet de déduire cette version fonctorielle du théorème de Dobrowolski généralisé à partir de la version relative de E. Delsinne [10].

2 Hauteurs, théorèmes de Bézout et de Dobrowolski généralisé

Dans cette section on énonce les définitions et les résultats de géométrie diophantienne qui nous seront utiles. Dans la sous-section 2.1 on rappellera la définition de hauteur projective, et dans la sous-section 2.2 le théorème de Bézout arithmétique. La sous-section 2.3 sera consacrée au rappel de la définition de hauteur normalisée. Dans ces trois sous-sections, on suivra l'approche développée par P. Philippon dans [14], [15] et [16]. Enfin, dans la sous-section 2.4, on donnera une version effective et fonctorielle du théorème de Dobrowolski généralisé (théorème 2.6) qui provient des travaux de F. Amoroso, S. David, E. Delsinne, G. Rémond et U. Zannier.

2.1 Hauteur projective

Rappelons d'abord la notion de hauteur de Weil dans l'espace projectif \mathbb{P}^n . Soit $\alpha = (\alpha_0 : \alpha_1 : \dots : \alpha_n) \in \mathbb{P}^n$ et soit \mathbb{K} un corps de nombre qui contient les α_j . On pose :

$$h(\alpha) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_v n_v \log |\alpha|_v \quad (2.1)$$

où la somme est sur les places (finies et infinies) de \mathbb{K} , $n_v = [\mathbb{K}_v : \mathbb{Q}_v]$ est le degré local et $|\alpha|_v = \max(|\alpha_0|_v, \dots, |\alpha_n|_v)$. Cette définition ne dépend pas du choix de \mathbb{K} ni du choix de coordonnées projective de α .

Soit V une sous-variété géométriquement irréductible de \mathbb{P}^n . P. Philippon dans [14], [15] et [16], définit à l'aide de la théorie des formes éliminantes, une

notion de hauteur de V , notée $h_{\mathbb{P}^n}(V)$. La définition de hauteur d'une variété s'étend par additivité à un cycle de Chow $S = \sum [l_i]V_i$ (V_i irréductibles) à coefficients $l_i \in \mathbb{N}$, par : $h_{\mathbb{P}^n}(S) = \sum_i l_i h_{\mathbb{P}^n}(V_i)$.

Nous remarquons que dans [16] l'auteur considère des sous-variétés projectives définies sur un corps de nombre K et qui sont implicitement supposée K -irréductibles (au moins on peut se réduire à ce cas en considérant le cycle des conjugués galoisiens de chaque variété). Ici, nous utiliserons le mot *sous-variété de \mathbb{P}^n* pour se référer à une intersection ensembliste de sous-variétés géométriquement irréductibles de \mathbb{P}^n . Comme on le fait usuellement, nous noterons aussi par $V \cap W$ l'intersection ensembliste de V et W . Soient I et J les idéaux homogènes définissant V et W ; on peut alors identifier cette intersection au cycle $ZR(I+J)$ (voir [16], dernière paragraphe à p. 347) supporté sur les composantes irréductibles de l'intersection et avec coefficients 1. Remarquons que dans *op. cit.* en revanche le cycle $V \cap W = Z(I+J)$ n'est pas en général réduit et qui peut même avoir des composantes immergées.

Pour un point $\alpha = (\alpha_0 : \alpha_1 : \dots : \alpha_n) \in \mathbb{P}^n$, la hauteur de la sous-variété projective $V = \{\alpha\}$ coïncide avec la hauteur " L_2 " de α , définie en prenant dans (2.1)

$$\|\alpha\|_v = (|\alpha_0|_v^2 + \dots + |\alpha_n|_v^2)^{1/2}$$

au places archimédienne à la place de $|\alpha|_v$. Comme pour les points, on dispose également d'une formule explicite pour la hauteur $h_{\mathbb{P}^n}(V)$ d'une hypersurface V . Soit \mathbb{K} un corps de nombres et soit $F \in \mathbb{K}[\mathbf{x}]$. En suivant P. Philippon ([16], p. 346, en particulier le dernière paragraphe en prenant $p = 1$ et $m_1 = m$) on définit une hauteur de F par

$$h(F) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_v [\mathbb{K}_v : \mathbb{Q}_v] \log \tilde{M}_v(F) + \frac{\deg(P)}{2} \sum_{i=1}^n \frac{1}{i} \quad (2.2)$$

où $\tilde{M}_v(F)$ est le maximum des valeurs absolues v -adique des coefficients de F si v est finie, et $\tilde{M}_v(F) = \tilde{M}(\sigma_v(F))$ si v est infinie associée au plongement σ_v de \mathbb{K} dans \mathbb{C} , où, pour un polynôme homogène $P \in \mathbb{C}[x_0, \dots, x_n]$,

$$\log \tilde{M}(P) = \int_{S_{n+1}} \log |P| \sigma_n. \quad (2.3)$$

Ici σ_n désigne la mesure invariante de masse totale 1 sur la sphere S_{n+1} de rayon 1 de $\mathbb{C}^n \simeq \mathbb{R}^{n+1}$. Soit maintenant Z une hypersurface de \mathbb{P}^n définie par l'équation $F = 0$, où $F \in \overline{\mathbb{Q}}[x_0, \dots, x_n]$ est homogène. On a alors ([16, p. 347]),

$$h_{\mathbb{P}^n}(Z) = h(F) + \frac{\deg(F)}{2} \sum_{i=1}^{n-1} \sum_{j=1}^i \frac{1}{j}. \quad (2.4)$$

2.2 Théorème de Bézout

Nous utiliserons la version suivante du théorème de Bézout (géométrique et arithmétique) de P. Philippon ([16, théorème 3]).

Théorème 2.1. *Soient V et W deux sous-variétés de \mathbb{P}_n définie sur un corps de nombre K et K -irréductibles. Notons X_1, \dots, X_g les composantes irréductibles (isolées) de l'intersection ensembliste $V \cap W$. On a alors :*

$$\sum_{i=1}^g \deg(X_i) \leq \deg(V) \deg(W)$$

$$\sum_{i=1}^g h_{\mathbb{P}_n}(X_i) \leq h_{\mathbb{P}_n}(V) \deg(W) + h_{\mathbb{P}_n}(W) \deg(V) + c \deg(V) \deg(W)$$

où

$$c = \frac{1}{2} \sum_{i=0}^{\dim V} \sum_{j=0}^{\dim W} \frac{1}{i+j+1} + \frac{\log 2}{2} (\operatorname{codim}(V) + \operatorname{codim}(W)).$$

Démonstration. On considère le cycle intersection $V.W$, son degré et son hauteur (voir [16, sous-section B), p. 353]). Toute composante irréductible (isolée) de $V \cap W$ apparaît comme composante isolée du cycle intersection $V.W$ (cf. *op. cit.*, paragraphe avant l'énoncé du théorème 3), et donc, par définition de degré et hauteur du cycle intersection, $\sum_{i=1}^g \deg(X_i) \leq \deg(V.W)$ et $h_{\mathbb{P}_n}(\sum_{i=1}^g \deg(X_i)) \leq h_{\mathbb{P}_n}(V.W)$. On applique alors [16, théorème 3].

On pourra également se référer à [12, Theorem 3, p. 455], où cependant la valeur de la constante c est moins précise. \square

Le corollaire suivant permet de majorer la hauteur d'une variété en fonction de la hauteur et du degré de ses générateurs.

Corollaire 2.2. *Soient $l \geq 1$ un entier et Z_1, \dots, Z_l des hypersurfaces définies sur un corps de nombre K . Soit V une composante K -irréductible (isolée) de $Z_1 \cap \dots \cap Z_l$. Alors,*

$$\deg(V) \leq D^{\operatorname{codim}(V)}$$

et

$$h_{\mathbb{P}_n}(V) \leq nhD^{\operatorname{codim}(V)-1} + \frac{n}{2} \left(\sum_{i=1}^n \sum_{j=1}^i \frac{1}{j} \right) D^{\operatorname{codim}(V)},$$

où

$$D = \max_{1 \leq i \leq s} \deg(Z_i) \quad \text{et} \quad h = \max_{1 \leq i \leq s} h(Z_i).$$

Démonstration. On applique [16, Corollaire 5, p. 357] avec $S = \mathbb{P}_n$, $\delta = D$ et $\eta = h$, en tenant compte des notations introduites au milieu de *op. cit.* p. 347. Notons cependant que dans *op. cit.* Z_i est supposée définie sur un corps de nombre K et K -irréductible; on peut se réduire à cette situation par linéarité et en négligeant les éventuelles multiplicités. On a alors, en tenant compte du fait que $\deg(P_n) = 1$ et $h_{\mathbb{P}_n}(\mathbb{P}^n) = \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^i \frac{1}{j}$ (cf [16], avant-dernière paragraphe),

$$d(S_l; D) \leq d(\mathbb{P}_n; D) = D^n;$$

$$h(S_l; D) \leq h(\mathbb{P}_n; D) + nh d(\mathbb{P}_n; D) = \frac{1}{2} \left(\sum_{i=1}^n \sum_{j=1}^i \frac{1}{j} \right) D^{n+1} + nhD^n.$$

Les composantes irréductibles V_i de $Z_1 \cap \dots \cap Z_l$ sont des composante irréductibles du cycle intersection S_l . En particulier, en négligeant les multiplicités d'intersection et les composantes de codimension $\neq k$,

$$d(S_l; D) \geq \sum_i \deg(V_i) D^{\deg(V_i)} \geq \deg(V) D^{\dim(V)};$$

$$d(S_l; D) \geq \sum_i h_{\mathbb{P}_n}(V_i) D^{\dim(V)+1} \geq h_{\mathbb{P}_n}(V) D^{\dim(V)+1}.$$

□

2.3 Hauteur normalisée dans $\mathbb{G}_m^n \hookrightarrow \mathbb{P}^n$

On considère le plongement $\iota_n : \mathbb{G}_m^n \hookrightarrow \mathbb{P}^n$ défini par

$$\iota_n(\alpha_1, \dots, \alpha_n) = (1 : \alpha_1 : \dots : \alpha_n).$$

Soit V une sous-variété de \mathbb{G}_m^n . Par abus de notation, on note $h_{\mathbb{P}_n}(V)$ la hauteur de la clôture de Zariski de $\iota_n(V)$ dans \mathbb{P}^n . D'après [16], on définit la hauteur normalisée de V (par rapport au plongement ι_n) par :

$$\widehat{h}(V) = \lim_{m \rightarrow +\infty} \frac{h_{\mathbb{P}_n}([m]V) \deg(V)}{m \deg([m]V)} \quad (2.5)$$

où $[m]$ est le morphisme de multiplication par m définie par $[m](x_1, \dots, x_n) = (x_1^m, \dots, x_n^m)$. On peut vérifier que la hauteur $\widehat{h}(\alpha)$ de $\alpha \in \mathbb{G}_m^n$ coïncide avec la hauteur de Weil $h(\iota_n(\alpha))$ de l'image de α dans \mathbb{P}_n . Rappelons également ([21]) qu'une variété géométriquement irréductible est de hauteur normalisée nulle si et seulement si elle est une *variété de torsion*, i.e. un translaté d'un sous-tore de \mathbb{G}_m^n par un point de torsion.

D'après [9, Proposition 2.1, p. 497], on a la relation suivante entre $\widehat{h}(V)$ et $h_{\mathbb{P}_n}(V)$:

$$\left| \widehat{h}(V) - h_{\mathbb{P}_n}(V) \right| \leq \frac{7}{2} (\dim V + 1) \deg(V) \log(n + 1). \quad (2.6)$$

On définit ensuite le minimum essentiel de V , noté $\hat{\mu}^{\text{ess}}(V)$, par :

$$\hat{\mu}^{\text{ess}}(V) = \inf \left\{ \theta > 0 \mid \overline{V(\theta)} = V \right\}$$

où $V(\theta) = \{\alpha \in V(\overline{\mathbb{Q}}^*) \mid \hat{h}(\alpha) \leq \theta\}$. Le minimum essentiel de V est donc le seuil de la hauteur à partir duquel les points de V deviennent denses dans V .

La hauteur normalisée et le minimum essentiel sont liées par des inégalités de S. Zhang [22, théorème 5.2] :

$$\frac{\hat{h}(V)}{(\dim(V) + 1) \deg(V)} \leq \hat{\mu}^{\text{ess}}(V) \leq \frac{\hat{h}(V)}{\deg(V)}. \quad (2.7)$$

2.4 Théorème de Dobrowolski généralisé

Le problème de Lehmer et le théorème de Dobrowolski se généralisent en dimension supérieure. On dit que V est une *variété de torsion* si V est une réunion finie de translatés de sous-tores de \mathbb{G}_m^n par des points de torsion. Rappelons que $\hat{\mu}^{\text{ess}}(V) = 0$ si et seulement si V est une variété de torsion. Le problème de déterminer de bonne minoration pour le minimum essentiel d'une variété qui n'est pas de torsion a donné lieu à plusieurs travaux.

Dans ce but, F. Amoroso et S. David ([3, Définition 1.1, p. 337]) ont introduit la notion d'*indice d'obstruction* :

Definition 2.3 (Indice d'obstruction). *Soient $V \subsetneq W$ deux sous-variétés irréductibles de \mathbb{G}_m^n et soit $\mathbb{K} \subseteq \overline{\mathbb{Q}}$ un corps. On appelle indice d'obstruction de V relatif à W sur \mathbb{K} , noté $\omega_{\mathbb{K}}(V, W)$, le minimum de²*

$$\left(\frac{\deg(Z)}{\deg(W)} \right)^{1/\text{codim}_W(Z)}$$

où Z parcourt les sous-variétés strictes de W définies sur \mathbb{K} et contenant V . Lorsque $\mathbb{K} = \overline{\mathbb{Q}}$, on omet l'indice $\overline{\mathbb{Q}}$ et lorsque $W = \mathbb{G}_m^n$, on notera simplement $\omega_{\mathbb{K}}(V)$ l'indice d'obstruction $\omega_{\mathbb{K}}(V, \mathbb{G}_m^n)$.

On peut maintenant énoncer une des généralisations de la conjecture de Lehmer en dimension supérieure.

Conjecture 2.4 ([3, Conjecture 1.10, p. 342]). *Soit V une sous-variété irréductible de \mathbb{G}_m^n . Soit $W \subseteq \mathbb{G}_m^n$ la plus petite sous-variété de torsion contenant V . Alors³ on a :*

$$\hat{\mu}^{\text{ess}}(V) \geq \frac{c(n)}{\omega_{\mathbb{Q}}(V, W)}.$$

2. où $\text{codim}_W(Z) = \dim(W) - \dim(Z)$

3. Dans *op. cit.* V est supposé \mathbb{Q} -irréductible et W est une réunion de variétés de torsion. On vérifie facilement que les deux énoncés sont équivalents.

Dans le cas d'une sous-variété irréductible V *faiblement transverse* (i.e. qui n'est contenue dans aucune sous-variété de torsion stricte de \mathbb{G}_m^n) cette conjecture est démontrée à un ε près ([2, corollaire 1.2 p. 239]). En généralisant l'approche de [1] et [5], E. Delsinne [10] a montré (toujours à un ε près) une version *relative* de la conjecture 2.4, toujours pour V faiblement transverse, en remplaçant l'indice d'obstruction sur \mathbb{Q} par celui sur \mathbb{Q}^{ab} , extension maximale abélienne de \mathbb{Q} . Nous énonçons une version simplifiée de son résultat principal (*op. cit.*, Corollaire 1.7) :

Théorème 2.5. *Soit V une sous-variété irréductible de \mathbb{G}_m^n . On suppose que V est faiblement transverse. Alors, pour tout $\varepsilon > 0$, on a :*

$$\hat{\mu}^{\text{ess}}(V) \geq \frac{c(\varepsilon, n)}{\omega_{\mathbb{Q}^{\text{ab}}}(V)^{1+\varepsilon}}$$

où $c(n, \varepsilon) > 0$ est explicite.

On s'intéresse maintenant à la version fonctorielle du théorème 2.5 qui consiste à enlever l'hypothèse faiblement transverse, quitte à faire intervenir dans l'indice d'obstruction la plus petite variété de torsion contenant V . Le théorème suivant a été déduit par G. Rémond à partir du résultat de E. Delsinne :

Théorème 2.6 ([17], Théorème 3.7, p. 261). *Soit V une sous-variété irréductible de \mathbb{G}_m^n . Soit $W \subseteq \mathbb{G}_m^n$ la plus petite sous-variété de torsion contenant V . Alors, pour tout $\varepsilon > 0$, il existe une constante $c(n, \varepsilon) > 0$ tel que :*

$$\hat{\mu}^{\text{ess}}(V) \geq \frac{c(n, \varepsilon)}{\omega_{\mathbb{Q}^{\text{ab}}}(V, W)^{1+\varepsilon} \deg(W)^\varepsilon}.$$

3 Résultats auxiliaires

Dans cette section on démontre les résultats auxiliaires dont nous aurons besoin pour la preuve de notre résultat principal.

Comme conséquence du théorème 2.1 et du corollaire 2.2, on obtient une majoration de la hauteur de l'intersection d'une sous-variété de \mathbb{G}_m^n avec une sous-variété de torsion de \mathbb{G}_m^n , i.e. un translatés d'un sous-tore par un point de torsion.

Proposition 3.1. *Soient $F_1, \dots, F_s \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$ et notons*

$$D = \max_{1 \leq i \leq s} \deg(F_i) \quad \text{et} \quad h_1 = \max_{1 \leq i \leq s} \log \|F_i\|_1.$$

Soit V une composante \mathbb{Q} -irréductible de la sous-variété de \mathbb{G}_m^n définie par $F_1 = \dots = F_s = 0$ et soit $B \subseteq \mathbb{G}_m^n$ une sous-variété de torsion. Notons

par X_1, \dots, X_g les composantes $\overline{\mathbb{Q}}$ -irréductibles de l'intersection ensembliste $V \cap B$. On a alors :

$$\begin{aligned} \sum_{i=1}^g \deg(X_i) &\leq D^{\text{codim}(V)} \deg(B) \\ \sum_{i=1}^g h_{\mathbb{P}^n}(X_i) &\leq (nh_1/D + c) D^{\text{codim}(V)} \deg(B) \end{aligned}$$

où

$$\begin{aligned} c = \frac{1}{2} \sum_{i=0}^{\dim V} \sum_{j=0}^{\dim B} \frac{1}{i+j+1} + \frac{\log 2}{2} (\text{codim}(V) + \text{codim}(B)) \\ + n \left(\sum_{i=1}^n \sum_{j=1}^i \frac{1}{j} \right) + \frac{7}{2} (\dim B + 1) \log(n+1). \end{aligned}$$

Démonstration. On applique le théorème 2.1, en choisissant comme K le corps de définition de B . On en déduit : $\sum_{i=1}^g \deg(X_i) \leq \deg(V) \deg(B)$ et

$$\sum_{i=1}^g h_{\mathbb{P}^n}(X_i) \leq h_{\mathbb{P}^n}(V) \deg(B) + h_{\mathbb{P}^n}(B) \deg(V) + c_0 \deg(V) \deg(B) \quad (3.1)$$

où

$$c_0 = \frac{1}{2} \sum_{i=0}^{\dim V} \sum_{j=0}^{\dim B} \frac{1}{i+j+1} + \frac{\log 2}{2} (\text{codim}(V) + \text{codim}(B)). \quad (3.2)$$

On majore $\deg(V)$ et $h_{\mathbb{P}^n}(V)$ à l'aide du corollaire 2.2. On peut supposer les polynômes F_i dans $\mathbb{Z}[\mathbf{x}]$; en choisissant comme Z_i les hypersurfaces définies par les homogénéisés des F_i on obtient alors :

$$\deg(V) \leq D^{\text{codim}(V)} \quad (3.3)$$

et

$$h_{\mathbb{P}^n}(V) \leq nhD^{\text{codim}(V)-1} + \frac{n}{2} \left(\sum_{i=1}^n \sum_{j=1}^i \frac{1}{j} \right) D^{\text{codim}(V)},$$

où $h = \max_{1 \leq i \leq s} h(Z_i)$. On en déduit en particulier la majoration annoncée pour la somme des degrés des X_i . Pour montrer celle pour la somme des hauteurs, on remarque que, pour $P \in \mathbb{C}[x_1, \dots, x_n]$ et en notant hP son homogénéisé, $\widehat{M}({}^hP) \leq \|P\|_1$ (cf définition (2.3)). Donc, en tenant compte des définitions (2.2), (2.4) et du fait que F_i est à coefficients entiers,

$$h(F_i) \leq \log \|F_i\|_1 + \frac{\deg(F_i)}{2} \sum_{i=1}^n \frac{1}{i},$$

et

$$h \leq \max_{1 \leq i \leq s} \left(h(F_i) + \frac{\deg(F_i)}{2} \sum_{i=1}^{n-1} \sum_{j=1}^i \frac{1}{j} \right) \leq h_1 + \frac{D}{2} \sum_{i=1}^n \sum_{j=1}^i \frac{1}{j}.$$

On a alors :

$$h_{\mathbb{P}^n}(V) \leq nh_1 D^{\text{codim}(V)-1} + n \left(\sum_{i=1}^n \sum_{j=1}^i \frac{1}{j} \right) D^{\text{codim}(V)}. \quad (3.4)$$

Par ailleurs $\widehat{h}(B) = 0$ et donc, par (2.6),

$$h_{\mathbb{P}^n}(B) \leq \frac{7}{2} (\dim B + 1) \deg(B) \log(n + 1). \quad (3.5)$$

En mettant ensemble les inégalités (3.1), (3.2), (3.3), (3.4) et (3.5) on déduit la majoration annoncée pour la somme des hauteurs des X_i . \square

Le lemme suivant permet de déterminer explicitement les équations de translatsés de sous-tores contenus dans une sous-variété de \mathbb{G}_m^n . La preuve repose sur [19, Lemma 4]. Soit $F \in \overline{\mathbb{Q}}[\mathbf{x}^{\pm 1}]$. On note $\text{Supp}(F) \subset \mathbb{Z}^n$ le support de F i.e. l'ensemble des exposants des monômes de F correspondant aux coefficients non nuls. On note également :

$$\mathcal{D}(F) = \{\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2 \mid \boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \text{Supp}(F)\}.$$

Lemme 3.2. *Soient $F_1, \dots, F_s \in \overline{\mathbb{Q}}[\mathbf{x}^{\pm 1}]$ et V la sous-variété de \mathbb{G}_m^n définie par $F_1 = \dots = F_s = 0$. Soit $\boldsymbol{\alpha}T$ un translatsé de sous-tore contenu dans V , de codimension $\text{codim}(T) = r < n$, maximale par rapport à l'inclusion parmi les translatsés vérifiant cette propriété. Alors il existe $\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_n$ formant une base de \mathbb{Z}^n telle que $\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_r$ est une base du réseau définissant T et :*

$$\begin{cases} \text{pour } k = 1, \dots, r : \\ \boldsymbol{\mu}_k = c_{k,1}\boldsymbol{\lambda}_1 + c_{k,2}\boldsymbol{\lambda}_2 + \dots + c_{k-1,1}\boldsymbol{\lambda}_{k-1} + c_k\boldsymbol{\lambda}_k, \\ \text{pour } k = r+1, \dots, n : \\ \boldsymbol{\mu}_k = c_{k,1}\boldsymbol{\lambda}_1 + \dots + c_{k,r}\boldsymbol{\lambda}_r + c_{k,r+1}\mathbf{f}_{r+1} + \dots + c_{k,k-1}\mathbf{f}_{k-1} + c_k\mathbf{f}_k, \end{cases} \quad (3.6)$$

où $\boldsymbol{\lambda}_1, \dots, \boldsymbol{\lambda}_r \in \bigcup_i \mathcal{D}(F_i)$ et $\mathbf{f}_{r+1}, \dots, \mathbf{f}_n$ sont des vecteurs de la base standard $(1, 0, \dots, 0), \dots, (0, \dots, 0, 1)$ de \mathbb{Z}^n , et où :

$$\begin{aligned} &\text{les } c_{k,i} \text{ (} k = 1, \dots, n; i = 1, \dots, k-1 \text{) et les } c_k \text{ (} k = 1, \dots, n \text{)} \\ &\text{sont des nombres rationnels tels que } c_{k,i} \in [-1/2, 1/2[\text{ et } c_k \in]0, 1]. \end{aligned} \quad (3.7)$$

Démonstration. Le fait que $\boldsymbol{\alpha}T \subseteq V$ est maximal implique que $T \subset \boldsymbol{\alpha}^{-1}V$ est maximal. La variété $\boldsymbol{\alpha}^{-1}V$ est définie par les équations $G_i(\mathbf{x}) = 0$ avec $G_i(\mathbf{x}) := F_i(\boldsymbol{\alpha}\mathbf{x})$ pour $i = 1, \dots, s$. On a alors $\text{Supp}(G_i) = \text{Supp}(F_i)$ pour

tout $i = 1, \dots, s$. Soit Λ le sous-groupe saturé de \mathbb{Z}^n de rang r qui définit T . Comme $T \subseteq \alpha^{-1}V$ est maximal, d'après [19, Lemme 4], Λ est engendré par $\lambda_1, \dots, \lambda_r \in \mathbb{Z}^n$ avec $\lambda_j \in \mathcal{D}(F_{i_j})$ pour un certain $i_j \in \{1, \dots, s\}$. Par le théorème de la base incomplète, ils existent des vecteurs $\mathbf{f}_{r+1}, \dots, \mathbf{f}_n$ de la base standard de \mathbb{Z}^n tels que $\lambda_1, \lambda_2, \dots, \lambda_r, \mathbf{f}_{r+1}, \dots, \mathbf{f}_n$ soient linéairement indépendants. D'après [20, Theorem 18], il existe des vecteurs $\mu_1, \dots, \mu_n \in \mathbb{Z}^n$ formant une base de \mathbb{Z}^n tels que (3.6) et (3.7) soient satisfaites.

Le sous-groupe M de \mathbb{Z}^n engendré par les vecteurs μ_1, \dots, μ_r est primitif car les vecteurs μ_1, \dots, μ_n forment une base de \mathbb{Z}^n . Les vecteurs μ_1, \dots, μ_r appartiennent à $\mathbb{Q}\Lambda$ car les vecteurs $\lambda_1, \dots, \lambda_r \in \Lambda$ et les coefficients $c_{k,i}, c_k$ sont des nombres rationnels. On a alors $M \subseteq \Lambda^{\text{sat}} = \Lambda$. Comme $\text{rang}(\Lambda) = \text{rang}(M)$, on en déduit que $\Lambda = M$. \square

4 Preuve du résultat principal.

Soient $n \geq 2$ et $s \geq 2$ deux entiers. Soient $F_1, \dots, F_s \in \mathbb{Z}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$. On note W la sous-variété de \mathbb{G}_m^n définie par $F_1 = \dots = F_s = 0$. Soient $\mathbf{a} \in \mathbb{Z}^n$ un vecteur primitif et $\zeta \in \mu_\infty^n$. On note T_1 le sous-tore de dimension 1 défini par :

$$T_1 = \{\xi^{\mathbf{a}} = (\xi^{a_1}, \dots, \xi^{a_n}) \in \mathbb{G}_m^n, \xi \in \mathbb{G}_m\}. \quad (4.1)$$

On s'intéresse aux points $\alpha \in W \cap \zeta T$ qui ne sont pas de torsion et tels que W est de dimension au plus $n - 2$ en α . On se propose de montrer que pour tout tel point α , il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^n$ orthogonal à \mathbf{a} et dont la norme est majorée par une constante ne dépendant que de n et des F_i . On note W^a la réunion des translatés de sous-tores de \mathbb{G}_m^n contenus dans W et $W^o = W \setminus W^a$.

Pour démontrer théorème 1.3, on suppose d'abord, dans la proposition 4.1, $\alpha \in W^o$. On se réduira ensuite à ce cas dans la preuve du théorème par un procédé qui reprend l'approche de [7, preuve du théorème 4.1, p.21].

Proposition 4.1. *Soient $n \geq 2$ et $s \geq 2$ deux entiers positifs et $\varepsilon \in]0, 1]$. Soient $F_1, \dots, F_s \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$. On note W la sous-variété de \mathbb{G}_m^n définie par $F_1 = \dots = F_s = 0$. Soient $\mathbf{a} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, $\zeta \in \mu_\infty^n$ et $\xi \in \overline{\mathbb{Q}}^*$. On note $\alpha = \zeta \xi^{\mathbf{a}}$. Si W est de codimension ≥ 2 en α et $\alpha \in W^o$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^n$ tel que :*

$$\xi^{\langle \mathbf{a}, \mathbf{b} \rangle} = 1, \quad \text{et} \quad \|\mathbf{b}\|_\infty \leq c(n, \varepsilon) \max(h_1/D, 1)^{1+\varepsilon} D^{2n},$$

où $c(n, \varepsilon) > 0$ et où l'on a noté :

$$D = \max_{1 \leq i \leq s} \deg(F_i) \quad \text{et} \quad h_1 = \max_{1 \leq i \leq s} \log \|F_i\|_1.$$

Démonstration. On définit T_1 comme dans (4.1) et on note V la composante \mathbb{Q}^{ab} -irréductible de W qui passe par α , qui est de codimension $k \geq 2$. On a alors $\alpha \in V \cap \zeta T_1$. On note dans la suite c_1, \dots des fonctions strictement positives qui dépendront des variables indiqués.

Soit $\{\mathbf{b}_1, \dots, \mathbf{b}_{n-1}\}$ une base réduite de \mathbf{a}^\perp telle que $\|\mathbf{b}_1\|_2 \leq \|\mathbf{b}_2\|_2 \leq \dots \leq \|\mathbf{b}_{n-1}\|_2$. Pour $i \in \{1, \dots, n-1\}$, le sous-groupe de \mathbb{Z}^n engendré par les vecteurs $\mathbf{b}_1, \dots, \mathbf{b}_i$ est primitif. On note T^i le sous-tore de \mathbb{G}_m^n de codimension i défini par :

$$T^i = \{\mathbf{x} \in \mathbb{G}_m^n \mid \mathbf{x}^{\mathbf{b}_1} = \dots = \mathbf{x}^{\mathbf{b}_i} = 1\}.$$

On pose aussi $T^0 = \mathbb{G}_m^n$. On a donc la suite de sous-tores suivante :

$$T_1 = T^{n-1} \subset T^{n-2} \subset \dots \subset T^1 \subset T^0 = \mathbb{G}_m^n.$$

D'après [6], le degré de T^i est égal au maximum des valeurs absolues des déterminants des mineurs $i \times i$ de la matrice formée par les vecteurs $\mathbf{b}_1, \dots, \mathbf{b}_i$. Comme $\{\mathbf{b}_1, \dots, \mathbf{b}_{n-1}\}$ est une base réduite, pour $i = 1, \dots, n-2$ on a :

$$c_1(n) \prod_{j=1}^i \|\mathbf{b}_j\|_2 \leq \deg(T^i) \leq c_2(n) \prod_{j=1}^i \|\mathbf{b}_j\|_2 \quad (4.2)$$

où $\|\star\|_2$ désigne la norme L_2 . Pour U sous-variété de \mathbb{G}_m^n on note aussi $\dim_\alpha(U)$ la dimension de la réunion des composantes irréductibles de U passant par α . Pour $i \in \{0, 1, \dots, n-2\}$, on a $\dim_\alpha(V \cap \zeta T^{i+1}) \leq \dim(\zeta T^{i+1}) = n - i - 1$. Si $\dim_\alpha(V \cap \zeta T^{i+1}) = n - i - 1$ alors $\zeta T^{i+1} \subseteq V$ et ceci contredit le fait que $\alpha \in V^\circ$. Ainsi, pour $i \in \{0, 1, \dots, n-2\}$, on a :

$$\dim_\alpha(V \cap \zeta T^{i+1}) \leq n - i - 2. \quad (4.3)$$

En particulier pour $i = n-2$, on a $\dim_\alpha(V \cap \zeta T^{n-1}) = 0 = n - i - 2$. On peut donc définir $m \in \{0, \dots, n-2\}$ comme le plus petit entier vérifiant :

$$\dim_\alpha(V \cap \zeta T^{m+1}) = n - m - 2.$$

Par minimalité de m , on a $\dim_\alpha(V \cap \zeta T^i) \leq n - i - 2$ pour $i \in \{1, \dots, m\}$ et cela est aussi vrai pour $i = 0$ car $\dim(V) \leq n - 2$. En particulier,

$$\dim_\alpha(V \cap \zeta T^{m+1}) = \dim_\alpha(V \cap \zeta T^m) = n - m - 2. \quad (4.4)$$

Soit Y une composante $\overline{\mathbb{Q}}$ -irréductible de $V \cap \zeta T^{m+1}$ de dimension $n - 2 - m$ et contenant α . D'après l'égalité (4.4), Y est également une composante irréductible de $V \cap \zeta T^m$. On note $\mathbb{Q}^{\text{ab}}(Y)$ le corps de définition de Y sur \mathbb{Q}^{ab} et $[\mathbb{Q}^{\text{ab}}(Y) : \mathbb{Q}^{\text{ab}}]$ son degré sur \mathbb{Q}^{ab} . Pour tout $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\text{ab}})$ on a :

$$\sigma(Y) \subseteq \sigma(V \cap \zeta T^m) \subseteq V \cap \zeta T^m$$

car V et T^m sont définis sur \mathbb{Q} et $\zeta \in \mathbb{Q}^{\text{ab}}$. On obtient alors :

$$\hat{Y} := \bigcup_{\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\text{ab}})} \sigma(Y) \subseteq V \cap \zeta T^m. \quad (4.5)$$

D'après (4.5) et la Proposition 3.1, on a :

$$\deg(\hat{Y}) = [\mathbb{Q}^{\text{ab}}(Y) : \mathbb{Q}^{\text{ab}}] \deg(Y) \leq D^k \deg(T^m) \quad (4.6)$$

$$h_{\mathbb{P}^n}(\hat{Y}) = [\mathbb{Q}^{\text{ab}}(Y) : \mathbb{Q}^{\text{ab}}] h_{\mathbb{P}^n}(Y) \leq (nh_1/D + c_3(n)) D^k \deg(T^m). \quad (4.7)$$

On va minorer $\hat{\mu}^{\text{ess}}(Y)$ en utilisant le théorème 2.6 et ensuite appliquer les inégalités de Zhang pour majorer $\hat{\mu}^{\text{ess}}(Y)$ en fonction de $h_{\mathbb{P}^n}(Y)$.

Soit $T \subsetneq \mathbb{G}_m^n$ la plus petite sous-variété de torsion contenant Y . On a alors $Y \subseteq T \subseteq \zeta T^{m+1}$. De plus, $\dim(Y) = n - m - 2$ par choix de Y et $\dim(\zeta T^{m+1}) = n - m - 1$ par définition de T^{m+1} . Par ailleurs, Y n'est pas de torsion car $\alpha \in Y$ et $\alpha \in V^o$. On en déduit que $T = \zeta T^{m+1}$.

Par définition, l'indice d'obstruction de Y par rapport à ζT^{m+1} sur \mathbb{Q}^{ab} est :

$$\omega_{\mathbb{Q}^{\text{ab}}}(Y, \zeta T^{m+1}) = \min_Z \left(\frac{\deg(Z)}{\deg(T^{m+1})} \right)^{1/\text{codim}_{\zeta T^{m+1}}(Z)}$$

où Z parcourt les sous-variétés strictes de ζT^{m+1} , définies sur \mathbb{Q}^{ab} et contenant Y . La variété \hat{Y} définie dans (4.5) est une sous-variété de ζT^{m+1} définie sur \mathbb{Q}^{ab} et de dimension $= n - m - 2$. Comme $\dim(\zeta T^{m+1}) = n - m - 1$, l'inclusion $\hat{Y} \subset \zeta T^{m+1}$ est stricte. On a donc :

$$\omega_{\mathbb{Q}^{\text{ab}}}(Y, \zeta T^{m+1}) \leq \frac{\deg(\hat{Y})}{\deg(T^{m+1})}.$$

On pose :

$$\varepsilon' = \frac{\varepsilon}{1 + (n-2)(1+\varepsilon)}. \quad (4.8)$$

Soit $\varepsilon \in]0, 1]$ comme dans l'énoncé. D'après le théorème 2.6, il existe une constante $c_4(n, \varepsilon)$ strictement positive telle que :

$$\hat{\mu}^{\text{ess}}(Y) \geq \frac{c_4(n, \varepsilon)}{\omega_{\mathbb{Q}^{\text{ab}}}(V, \zeta T^{m+1})^{1+\varepsilon'} \deg(T^{m+1})^{\varepsilon'}} \geq c_4(n, \varepsilon) \frac{\deg(T^{m+1})}{\deg(\hat{Y})^{1+\varepsilon'}}.$$

En utilisant les inégalités de Zhang (2.7), on majore le minimum essentiel de Y en fonction de la hauteur normalisée :

$$c_4(n, \varepsilon) \frac{\deg(T^{m+1})}{\deg(\hat{Y})^{1+\varepsilon'}} \leq \hat{\mu}^{\text{ess}}(Y) \leq \frac{\hat{h}(Y)}{\deg(Y)}.$$

À l'aide de la relation (2.6), on majore $\hat{h}(Y)$ en fonction de $h(Y)$:

$$c_4(n, \varepsilon) \frac{\deg(T^{m+1})}{\deg(\hat{Y})^{1+\varepsilon'}} \leq \frac{h_{\mathbb{P}^n}(Y)}{\deg(Y)} + \frac{7}{2} (\dim Y + 1) \log(n+1).$$

On majore $h_{\mathbb{P}^n}(Y)$ à l'aide de l'inégalité (4.7) :

$$c_4(n, \varepsilon) \frac{\deg(T^{m+1})}{\deg(\hat{Y})^{1+\varepsilon'}} \leq \frac{(nh_1/D + c_3(n))D^k}{[\mathbb{Q}^{\text{ab}}(Y) : \mathbb{Q}^{\text{ab}}] \deg(Y)} \deg(T^m) + \frac{7}{2} (n-2) \log(n+1)$$

En simplifiant par $\deg(\hat{Y}) = [\mathbb{Q}^{\text{ab}}(Y) : \mathbb{Q}^{\text{ab}}] \deg(Y)$, on a :

$$c_4(n, \varepsilon) \deg(T^{m+1}) \leq (nh_1/D + c_3(n))D^k \deg(\hat{Y})^{\varepsilon'} \deg(T^m) + \frac{7}{2} (n-2) \log(n+1).$$

On majore ensuite $\deg(\hat{Y})$ par l'inégalité (4.6) :

$$\deg(T^{m+1}) \leq c_5(n, \varepsilon)(h_1/D + 1)D^{(1+\varepsilon')D^k} \deg(T^m)^{1+\varepsilon'}.$$

Par l'inégalité (4.2) on a :

$$\deg(T_m) \leq c_2(n) \prod_{i=1}^m \|\mathbf{b}_i\|_2 \quad \text{et} \quad \deg(T^{m+1}) \geq c_1(n) \prod_{i=1}^{m+1} \|\mathbf{b}_i\|_2.$$

En simplifiant par $\prod_{i=1}^m \|\mathbf{b}_i\|_2$ et en majorant ensuite $\prod_{i=1}^m \|\mathbf{b}_i\|_2$ par $\|\mathbf{b}_{m+1}\|_2^m$, on obtient donc :

$$\|\mathbf{b}_{m+1}\|_2^{1-m\varepsilon'} \leq c_6(n, \varepsilon)(h_1/D + 1)D^{k(1+\varepsilon')}.$$

Comme $m \leq n-2$ et par définition (4.8) de ε' on a

$$1 - m\varepsilon' \geq 1 - (n-2)\varepsilon' = \frac{n-1}{1 + (n-2)(1+\varepsilon)} > 0.$$

Donc :

$$\|\mathbf{b}_{m+1}\|_2^{1-(n-2)\varepsilon'} \leq c_6(n, \varepsilon)(h_1/D + 1)D^{k(1+\varepsilon')}.$$

Toujours par définition (4.8) de ε' , on a :

$$\frac{1}{1 - (n-2)\varepsilon'} = 1 + \frac{n-2}{n-1}\varepsilon \leq 1 + \varepsilon, \quad \frac{1 + \varepsilon'}{1 - (n-2)\varepsilon'} = 1 + \varepsilon \leq 2.$$

Donc

$$\begin{aligned} \|\mathbf{b}_{m+1}\|_2 &\leq c_7(n, \varepsilon) \left((h_1/D + 1)D^{k(1+\varepsilon')} \right)^{1/(1-(n-2)\varepsilon')} \\ &= c_7(n, \varepsilon)(h_1/D + 1)^{\frac{1}{1-(n-2)\varepsilon'}} D^{\frac{k(1+\varepsilon')}{1-(n-2)\varepsilon'}} \\ &\leq c_7(n, \varepsilon)(h_1/D + 1)^{1+\varepsilon} D^{2n}. \end{aligned}$$

Enfin, puisque $\zeta \xi^{\mathbf{a}} \in \zeta T_1 \subseteq \zeta T^{m+1}$, on a $\xi^{\mathbf{a}} \in T^{m+1}$ et donc $\xi^{(\mathbf{a}, \mathbf{b}_{m+1})} = 0$.
On choisit donc $\mathbf{b} = \mathbf{b}_{m+1}$. \square

Démonstration du théorème 1.3. Soit $\varepsilon \in (0, 1)$. Si $\alpha \in V^o$ alors, d'après la proposition 4.1, il existe $c(n, \varepsilon) > 0$, et un vecteur $\mathbf{b} \in \mathbb{Z}^n$ orthogonal à \mathbf{a} tels que :

$$\|\mathbf{b}\|_\infty \leq c(n, \varepsilon)(h_1/D + 1)^{1+\varepsilon} D^{2n}.$$

ce qui donne une majoration plus précis de celle annoncé.

Supposons donc $\alpha \in V^a$. On note dans la suite c_1, \dots des fonctions strictement positives qui dépendront des variables indiqués. Par hypothèse, il existe un sous-tore T de \mathbb{G}_m^n de dimension non nulle tel que $\alpha T \subseteq V$. On choisit un tel T de maximale et on note r sa codimension. On va construire un automorphisme φ de \mathbb{G}_m^n tel que $\varphi(T) = \{\mathbf{y} \in \mathbb{G}_m^n \mid y_1 = \dots = y_r = 1\}$.

D'après le lemme 3.2, il existe n vecteurs μ_1, \dots, μ_n formant une base de \mathbb{Z}^n tels que T est défini par $\mathbf{x}^{\mu_1} - 1 = \dots = \mathbf{x}^{\mu_r} - 1 = 0$ et

$$\max_{1 \leq i \leq n} \|\mu_i\|_\infty \leq n \max_{1 \leq j \leq s} \deg(F_j) \leq nD. \quad (4.9)$$

On note M la matrice dont les colonnes sont formées par les vecteurs μ_1, \dots, μ_n . Par construction, $M \in \text{GL}_n(\mathbb{Z})$. On considère l'automorphisme φ de \mathbb{G}_m^n défini par :

$$\begin{aligned} \varphi : \mathbb{G}_m^n &\longrightarrow \mathbb{G}_m^n \\ \mathbf{x} &\mapsto \mathbf{x}^M = (\mathbf{x}^{\mu_1}, \dots, \mathbf{x}^{\mu_n}). \end{aligned}$$

On a alors, toujours par construction,

$$\varphi(T) = \{\mathbf{y} \in \mathbb{G}_m^n \mid y_1 = \dots = y_r = 1\}.$$

Maintenant, on effectue le changement de variable $\mathbf{x} = \varphi^{-1}(\mathbf{y}) = \mathbf{y}^{M^{-1}}$ et on écrit pour $i \in \{1, \dots, s\}$:

$$F_i(\varphi^{-1}(\mathbf{y})) = \sum_{j=1}^t F_{i,j}(y_1, \dots, y_r) y_{r+1}^{\theta_{j,r+1}} \dots y_n^{\theta_{j,n}} \quad (4.10)$$

pour certains $F_{i,j} \in \mathbb{Z}[y_1^{\pm 1}, \dots, y_r^{\pm 1}]$, pour certains $\theta_{j,r+1}, \dots, \theta_{j,n} \in \mathbb{Z}$ et $t \in \mathbb{N}$. On renomme les polynômes $F_{i,j}$ par :

$$\{F_{i,j} \mid i \in \{1, \dots, s\}, j \in \{1, \dots, t\}\} = \{G_1, \dots, G_{s'}\}.$$

On considère la sous-variété W de \mathbb{G}_m^r définie par :

$$W = \{(y_1, \dots, y_r) \in \mathbb{G}_m^r \mid G_j(y_1, \dots, y_r) = 0, \forall j \in \{1, \dots, s'\}\}.$$

On vérifie que :

$$W = \{(y_1, \dots, y_r) \in \mathbb{G}_m^r \mid \forall (y_{r+1}, \dots, y_n) \in \mathbb{G}_m^{n-r}, (y_1, \dots, y_n) \in \varphi(V)\}.$$

On note ensuite β l'image de α par φ i.e. $\beta = \varphi(\alpha) = (\zeta^{\mu_1} \xi^{\mathbf{a}\mu_1}, \dots, \zeta^{\mu_n} \xi^{\mathbf{a}\mu_n})$ et on pose $\beta' = (\zeta^{\mu_1} \xi^{\mathbf{a}\mu_1}, \dots, \zeta^{\mu_r} \xi^{\mathbf{a}\mu_r})$. On a alors :

$$\{\beta'\} \times \mathbb{G}_m^{n-r} = \beta\varphi(T) = \varphi(\alpha T) \subseteq \varphi(V).$$

Donc $\beta' \in W$.

Supposons qu'il existe un sous-tore $T' \subseteq \mathbb{G}_m^r$ de dimension non nulle tel que $\beta'T' \subseteq W$. On a alors $\beta(T' \times \mathbb{G}_m^{n-r}) \subseteq W \times \mathbb{G}_m^{n-r} \subseteq \varphi(V)$. Cela implique que α est contenu dans un translaté de sous-tore de dimension $\geq n - r + 1$ contenu dans V et contredit le fait que $\alpha T \subseteq V$ est maximal dans V . Donc $\beta' \in W^o$. Par ailleurs $W \times \mathbb{G}_m^{n-r} \subseteq \varphi(V)$. D'où :

$$\dim_{\beta'}(W) + n - r = \dim_{\beta}(W \times \mathbb{G}_m^{n-r}) \leq \dim_{\beta}(\varphi(V)) = \dim_{\alpha}(V) \leq n - 2.$$

Cela implique que $W \subseteq \mathbb{G}_m^r$ est de codimension $k' \geq 2$ en β' .

On remarque également que si $\mathbf{a}\mu_1 = 0$ alors on a la conclusion de la proposition avec $\mathbf{b} = \mu_1$ car $\|\mu_1\|_{\infty} \leq nD$ d'après (4.9). On suppose dorénavant que $\mathbf{a}\mu_1 \neq 0$. Ainsi le vecteur $(\mathbf{a}\mu_1, \dots, \mathbf{a}\mu_r)$ est non nul. Puisque $\beta = (\zeta^{\mu_1} \xi^{\mathbf{a}\mu_1}, \dots, \zeta^{\mu_r} \xi^{\mathbf{a}\mu_r})$ et ξ n'est pas une racine de l'unité, d'après la Proposition 4.1, il existe une constante $c_1(n, \varepsilon)$, qui ne dépend que de ε et n , et un vecteur non nul $\eta \in \mathbb{Z}^r$ orthogonal à $(\mathbf{a}\mu_1, \dots, \mathbf{a}\mu_r)$ tels que :

$$\|\eta\|_2 \leq c_1(n, \varepsilon) \max(h_1/D'^n, 1)^{1+\varepsilon} D'^{2(n-1)} \quad (4.11)$$

où

$$D' = \max_{1 \leq i \leq s'} \deg(G_i) \quad \text{et} \quad h'_1 = \max_{1 \leq i \leq s'} \log \|G_i\|_1.$$

On considère ensuite le vecteur \mathbf{b} défini par $\mathbf{b} = \eta_1 \mu_1 + \dots + \eta_r \mu_r$. Puisque (η_1, \dots, η_r) est non nul et μ_1, \dots, μ_r sont linéairement indépendants, \mathbf{b} est aussi non nul. Comme $(\eta_1, \dots, \eta_r) \in \mathbb{Z}^r$ est orthogonal à $(\mathbf{a}\mu_1, \dots, \mathbf{a}\mu_r)$, on a $\mathbf{a}\mathbf{b} = 0$. On va déterminer une majoration de la norme de \mathbf{b} en fonction de D et h .

Les exposants des monômes de G_j sont donnés par les vecteurs $M^{-1}\nu$ où ν parcourt $\text{Supp}(F_i)$. D'après l'inégalité de Hadamard, la valeur absolue des coefficients de M^{-1} est majorée par :

$$(n-1)^{(n-1)/2} \max_{1 \leq i \leq n} \|\mu_i\|_{\infty}^{n-1} \leq n^{3(n-1)/2} D^{n-1}.$$

Par suite, on a :

$$D' \leq n^{(3n-1)/2} D^n.$$

Par ailleurs :

$$h'_1 \leq \max_{1 \leq i \leq s} \|F_i\|_1 = h_1.$$

En remplaçant D' et h'_1 par ces majorations dans (4.11) (on remarquera que le membre de droite dans (4.11) est une fonction croissante de D') on obtient :

$$\|\boldsymbol{\eta}\|_2 \leq c_2(n, \varepsilon) \max(h_1/D^n, 1)^{1+\varepsilon} D^{2n(n-1)}.$$

Par définition de \mathbf{b} et par (4.9),

$$\|\mathbf{b}\|_2 \leq \|\boldsymbol{\eta}\|_2 \cdot \|\boldsymbol{\mu}\|_2 \leq n^{3/2} D \|\boldsymbol{\eta}\|_2.$$

Donc, en majorant $2n(n-1) + 1$ par $2n^2$,

$$\|\mathbf{b}\|_2 \leq c_3(n, \varepsilon) \max(h_1/D^n, 1)^{1+\varepsilon} D^{2n^2}.$$

□

Références

- [1] F. Amoroso and S. David. Le problème de Lehmer en dimension supérieure. *J. Reine Angew. Math.*, 513 :145–179, 1999.
- [2] F. Amoroso and S. David. Densité des points à coordonnées multiplicativement indépendantes. *Ramanujan J.*, 5(3) :237–246, 2001.
- [3] F. Amoroso and S. David. Minoration de la hauteur normalisée dans un tore. *Journal of the Institute of Mathematics of Jussieu*, 2(3) :335–381, 2003.
- [4] F. Amoroso, L. Leroux, and M. Sombra. Overdetermined systems of sparse polynomial equations. *Foundations of Computational Mathematics*, 15(1) :53–87, 2015.
- [5] F. Amoroso and U. Zannier. A relative Dobrowolski lower bound over abelian extensions. *Annali della Scuola Normale Superiore di Pisa-Classe di Scienze*, 29(3) :711–727, 2000.
- [6] D. Bertrand and P. Philippon. Sous-groupes algébriques de groupes algébriques commutatifs. *Illinois journal of mathematics*, 32(2) :263–280, 1988.
- [7] E. Bombieri, D. Masser, and U. Zannier. Anomalous subvarieties-structure theorems and applications. *International Mathematics Research Notices*, 2007, 2007.
- [8] S. Checcoli, F. Veneziano, and E. Viada. On torsion anomalous intersections. *Accounts Lincei-Mathematics and Applications*, 25(1) :1–36, 2014.
- [9] S. David and P. Philippon. Minorations des hauteurs normalisées des sous-variétés des tores. *Annali della Scuola Normale Superiore di Pisa-Classe di Scienze*, 28(3) :489–543, 1999.

- [10] E. Delsinne. Le probleme de lehmer relatif en dimension supérieure. In *Annales scientifiques de l'École normale supérieure*, volume 42, pages 981–1028, 2009.
- [11] M. Filaseta, A. Granville, and A. Schinzel. Irreducibility and greatest common divisor algorithms for sparse polynomials. *London Mathematical Society Lecture Note Series*, 352 :155, 2008.
- [12] P. Habegger. Intersecting subvarieties of \mathbf{G}_m^n with algebraic subgroups. *Mathematische Annalen*, 342(2) :449–466, 2008.
- [13] L. Leroux. Computing the torsion points of a variety defined by lacunary polynomials. *Mathematics of Computation*, 81(279) :1587–1607, 2012.
- [14] P. Philippon. Sur des hauteurs alternatives. I. *Mathematische Annalen*, 289(1) :255–283, 1991.
- [15] P. Philippon. Sur des hauteurs alternatives. II. *Ann. Inst. Fourier (Grenoble)*, 44(4) :1043–1065, 1994.
- [16] P. Philippon. Sur des hauteurs alternatives III. *Journal de mathématiques pures et appliquées*, 74(4) :345–365, 1995.
- [17] G. Rémond. Généralisations du problème de Lehmer et applications à la conjecture de Zilber-Pink. *Around the Zilber–Pink Conjecture/Autour de la conjecture de Zilber–Pink*, *Panor. Synthèses*, 52 :243–284, 2017.
- [18] A. Schinzel. *Polynomials with special regard to reducibility. With an appendix by Umberto Zannier.*, volume 77. Cambridge University Press, 2000.
- [19] W. M. Schmidt. Heights of points on subvarieties of \mathbf{G}_m^n . *Number Theory (Paris, 1993–1994)*. *London Mathematical Society Lecture Notes Series*, 235 :157–187, 1996.
- [20] C. L. Siegel. *Lectures on the Geometry of Numbers*. Springer Science & Business Media, 2013.
- [21] S. Zhang. *Positive line bundles on arithmetic surfaces*. Columbia University, 1991.
- [22] S. Zhang. Positive line bundles on arithmetic varieties. *Journal of the American Mathematical Society*, 8(1) :187–221, 1995.