Conjecture de Schinzel et algorithmique des polynômes lacunaires

Njaka Harilala Andriamandratomanana

Normandie Université

UNIVERSITÉ CAEN NORMANDIE

THÈSE

Pour obtenir le diplôme de doctorat

Spécialité MATHEMATIQUES

Préparée au sein de l'Université de Caen Normandie

Conjecture de Schinzel et algorithmique des polynômes lacunaires

Présentée et soutenue par
NJAKA HARILALA ANDRIAMANDRATOMANANA

Thèse soutenue le 26/06/2023 devant le jury composé de		
M. FRANCESCO PAPPALARDI	Professeur des universités, Universita Roma Tre	Rapporteur du jury
MME SARA CHECCOLI	Maître de conférences, Institut Fourier	Membre du jury
M. MARTIN SOMBRA	Chercheur, ICREA	Membre du jury
M. FABIEN PAZUKI	Professeur des universités, COPENHAGUE - UNIVERSITE DE COPENHAGUE	Président du jury
M. FRANCESCO AMOROSO	Professeur des universités, Université de Caen Normandie	Directeur de thèse
M. DENIS SIMON	Professeur des universités, Université de Caen Normandie	Co-directeur de thèse

Thèse dirigée par FRANCESCO AMOROSO (Laboratoire de Mathématiques 'Nicolas Oresme' (Caen)) et DENIS SIMON (Laboratoire de Mathématiques 'Nicolas Oresme' (Caen))

MIS

LMNO

Remerciements

Durant ma thèse, j'ai eu l'opportunité de côtoyer de nombreuses personnes qui ont grandement contribué à rendre ces trois années à la fois enrichissantes et agréables. Je tiens donc à exprimer ici ma profonde gratitude envers eux.

Mes remerciements vont tout d'abord à mes directeurs de thèse, Francesco Amoroso et Denis Simon, pour m'avoir offert la chance de travailler sur un sujet fascinant. Je souhaite également exprimer ma gratitude envers leur bienveillance, d'autant plus pendant la période difficile de la pandémie de Covid-19.

Je tiens à exprimer ma gratitude envers les membres du jury qui ont consacré leur temps à évaluer ma thèse, et en particulier à Fabien Pazuki et Francesco Pappalardi pour leurs rapports détaillés et élogieux. Leurs précieuses expertises et remarques constructives ont contribué à améliorer la qualité de mon travail de recherche.

Je tiens également remercier tous ceux qui, à différents niveaux, font du LMNO un environnement de travail fantastique. Je remercie tous les membres de l'équipe de Théorie des nombres et Géométrie arithmétique pour les séminaires et les rencontres enrichissantes. Mes remerciements vont également aux membres administratifs. Un grand remerciement à tous les collègues doctorants du LMNO, avec qui j'ai partagé des moments inoubliables : Alexis (qui me doit un match de tennis), Etienne (on le trouve toujours entrain d'arroser ses plantes), Édouard (j'espère que tu n'auras plus l'air fatigué après avoir terminé ta thèse), Francesco (qui est, selon Etienne, le roi du Stima, mais qui est aussi connu pour sa capacité à modifier constamment les règles de jeux à son avantage), Hugo (l'homme en feux car on le trouve souvent entouré de fumée), Joaquim (le seul qui a peur de manger au RU), Manu (l'homme sans soucis qui détient le record mondial en tant que plus grand mangeur de mayo), Nhuan (le seul qui peut gagner au Stima avec une technique infaillible).

Je tiens également à remercier les personnes qui ont visité le labo et avec lesquelles j'ai eu le privilège de faire connaissance : Velibor, Giada, Ilaria, Neha, Raquel et les autres stagiaires. Merci à Romain et Charlotte pour les soirées et les sorties. Toute ma gratitude envers les anciens : Angelot, Coumba, Dorian, Étienne, Tiphaine, Thien, Stavroula et les autres, pour m'avoir chaleureusement accueilli lorsque j'étais en première année.

Je tiens également à exprimer ma gratitude envers toutes les personnes que j'ai rencontrées en dehors du laboratoire. Je tiens à remercier l'association FMPA Caen, où j'ai véritablement eu le sentiment d'appartenir à une communauté. Un spécial remerciement aux membres actifs de la STK pour les soirées, les sorties et les repas partagés, ainsi que les moments de partage, qui ont été des expériences inoubliables : Iavo, Miora, Anika, Miary, Tsitsi, Nanou, Tiaray, Elodie, Setra, Tsiky, Anja, Tahiana, famille Pascal, famille Jean-Jacques et à tous les autres membres.

Je conclus mes remerciements en exprimant ma gratitude envers ma famille, que je ne peux que remercier d'être toujours présente. Je tiens à remercier mes parents tout particulièrement pour leurs prières inlassables. Je souhaite adresser mes meilleurs voeux à ma mère, qui a toujours été préoccupée par mon bien-être. Un grand merci à ma grand-mère pour son soutien indéfectible afin que je puisse poursuivre mes études à l'étranger. Je suis reconnaissant envers mon oncle pasteur et ma tante pour leur soutien précieux tout au long de mes études universitaires. Mes remerciements vont également à mes frères, soeurs, cousins, cousines, oncles et tantes, que j'aimerais revoir plus souvent. Je souhaite dédier ceci de manière spéciale à ma mère et à mon petit Aiko, et enfin, je tiens à exprimer un remerciement particulier à ma chérie Tantely avec beaucoup d'affection. Misaotra !

Table des matières

Introduction

Soient f et g deux polynômes à une variable et à coefficients dans $\mathbb{Z}$, ayant un nombre de coefficients relativement petit par rapport à leur degré. De tels polynômes sont appelés *polynômes lacunaires* ou *creux*.

Ensuite, en 2008, M. Filaseta, A. Granville et A. Schinzel [23] ont montré qu'il existe un algorithme qui permet de calculer le pgcd de f et g de degré au plus D en $\widetilde{\mathcal{O}}_{N,h}(\log D)$ opérations binaires sous l'hypothèse qu'au moins l'un des f et g n'ait pas de facteur cyclotomique. Ici, N désigne le nombre de coefficients non nuls de f et g et h la taille de leurs coefficients. La notation $\widetilde{\mathcal{O}}_{N,h}(\log D)$ signifie une borne supérieure dont l'ordre de grandeur est $\log(D)$ à des facteurs $\log\log(D)$ près et à une constante près qui ne dépend que de N et h. Leur résultat implique que si f ou g n'est pas divisible par un polynôme cyclotomique alors le pgcd de f et g contient au plus $c(N,h)$ coefficients non nuls où $c(N,h)$ est une constante non nulle, positive et ne dépendant que de N et h. L'hypothèse que f ou g n'est pas divisible par un polynôme cyclotomique est cruciale. L'exemple suivant, démontrant ce fait, a déjà été noté par A. Schinzel [41]. Soient a et b deux entiers naturels premiers entre eux. Alors on a :

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

Ce polynôme contient $2\min(a,b)$ coefficients non nuls. Ainsi, pour deux entiers a,b *relativement grands*, les deux polynômes $x^{ab}-1$ et $(x^a-1)(x^b-1)$ sont lacunaires mais pas leur pgcd.

En 2015, F. Amoroso, L. Leroux et M. Sombra [4] ont amélioré l'algorithme de M. Filaseta, A. Granville et A. Schinzel [23]. Ils ont montré qu'il existe un algorithme qui permet de trouver *une approximation* du pgcd de f et g en au plus $\widetilde{\mathcal{O}}_{N,h}(\log D)$ opérations binaires en autorisant f et g à avoir des facteurs cyclotomiques. On va énoncer leur résultat. On note $V(f,g)$ l'ensemble des racines communes de f,g dans le corps des nombres algébriques $\overline{\mathbb{Q}}$. Le symbole $\boldsymbol{\mu}_\infty$ désigne l'ensemble des racines de l'unité de $\overline{\mathbb{Q}}$.

Théorème 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 :*

$$p_1\mid\mathrm{pgcd}(f,g),\quad V(p_1)\setminus\boldsymbol{\mu}_\infty=V(\mathrm{pgcd}(f,g))\setminus\boldsymbol{\mu}_\infty\quad\text{et}\quad V(p_2)=V(\mathrm{pgcd}(f,g))\cap\boldsymbol{\mu}_\infty,$$

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

L'algorithme correspondant au Théorème 1 est divisé en deux procédures :

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

L'algorithme pour la recherche de la partie cyclotomique est décrit et analysé dans [4, Algorithm 4.3]. La complexité de cette première procédure est au plus $\widetilde{\mathcal{O}}_{N,h}(\log D)$ opérations binaires. En outre, la dépendance en N et h de cette complexité peut être déduite du Théorème 2.2 de L. Leroux dans [30].

L'algorithme pour la recherche de la partie non-cyclotomique est aussi décrit et analysé dans [4, Algorithm 4.2] et a une complexité en au plus $\widetilde{\mathcal{O}}_{N,h}(\log D)$ opérations binaires. Toutefois, cet algorithme n'est pas effectif car il utilise une constante non explicite dont l'existence est donnée par la *Conjecture de Schinzel* [40, Conjecture 1]. Cette conjecture concerne l'intersection d'une sous-variété de codimension au moins 2 dans une puissance du tore multiplicatif $\overline{\mathbb{Q}}^{*n}$ avec un translaté de sous-tore de dimension 1 par un point de torsion. Cette conjecture est maintenant un théorème.

Théorème 2 (Conjecture de Schinzel). *Soit $n \geqslant 2$ un entier. Soient $F, G \in \mathbb{Z}[x_1, \cdots, x_n]$ tels que $\mathrm{pgcd}(F, G) = 1$. Alors il existe une constante $B(F, G)$ satisfaisant la propriété suivante. Soient $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{Z}^n$, $\boldsymbol{\zeta} = (\zeta_1, \cdots, \zeta_n) \in \boldsymbol{\mu}_\infty^n$ et $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$. Si $F(\zeta_1 \xi^{a_1}, \cdots, \zeta_n \xi^{a_n}) = G(\zeta_1 \xi^{a_1}, \cdots, \zeta_n \xi^{a_n}) = 0$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^n$ orthogonal à $\mathbf{a}$ tel que :*

$$\max_{1 \leqslant i \leqslant n} |b_i| \leqslant B(F, G).$$

Ce théorème a été démontré par plusieurs auteurs : par A. Schinzel [40, Theorem 45] en 1989 (seulement dans le cas $2 \leqslant n \leqslant 3$ et pour $\zeta_1 = \cdots = \zeta_n = 1$), puis, pour n quelconque, par E. Bombieri et U. Zannier [40, Appendix] en 1998 (à nouveau pour $\zeta_1 = \cdots = \zeta_n = 1$), et par E. Bombieri, D. Masser et U. Zannier [11, Theorem 1.6] en 2007 (pour $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ quelconque). Un résultat similaire dans le cas d'un produit de courbes elliptiques a été réalisé par S. Checcoli, F. Veneziano et E. Viada [15] en 2016.

Dans le cas torique qui nous intéresse, les preuves de ce théorème sont effectives mais pas explicites. Le sujet de cette thèse consiste à expliciter la constante du Théorème 2 et à rendre effectif l'algorithme correspondant du Théorème 1 pour la partie non-cyclotomique. Les résultats principaux de cette thèse donnent des constantes explicites pour les deux cas $n = 2$ et $n = 3$ et un résultat partiel pour n quelconque (explicite en le degré et la taille des coefficients de F et G mais pas explicite en n).

La suite de cette introduction présente les résultats principaux des différents chapitres.

Dans le Chapitre 2, on présente les notions de relation de dépendance multiplicative faible et forte entre des nombres algébriques. Ces relations ont un intérêt indépendant mais apparaissent également dans la démonstration explicite du Théorème 2. On applique la notion de relation de dépendance multiplicative faible pour démontrer l'analogue de la Conjecture de Schinzel pour les variétés qui sont des translatés de sous-tores. On donne ensuite des algorithmes pour calculer l'ensemble des relations de dépendance multiplicative faible. Pour le cas des nombres rationnels, l'algorithme consiste à faire la factorisation en des nombres qui sont premiers entre eux grâce à l'Algorithme de Bernstein [8]. On pourrait adapter cette méthode pour le cas des nombres algébriques, mais cette opération s'avère coûteuse. On a ainsi proposé une autre méthode qui est basée sur l'approximation diophantienne et les fractions continues, mais qui, cette fois-ci, ne s'applique qu'au cas de deux nombres algébriques. À l'aide de cet algorithme, on en déduit un algorithme pour calculer l'ensemble des relations de dépendance multiplicative faible entre n nombres algébriques lorsque cet ensemble est de codimension au plus 1. On note que c'est ce cas-là qui est utile pour la Conjecture de Schinzel.

Le Chapitre 3 contient une version explicite du Théorème 2 dans le cas $n = 2$. Étant donné $\mathbf{a} \in \mathbb{Z}^2$, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^2$ et $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$, on montre que si $\boldsymbol{\alpha} = \boldsymbol{\zeta} \xi^{\mathbf{a}}$ est un point isolé de la variété V définie par $F = G = 0$ alors la norme de $\mathbf{a}$ est majorée par cDh où $c > 0$ est une constante explicite strictement positive, D est le maximum entre entre le degré de F et G et h le maximum entre le logarithme de la mesure de Mahler de F et G. Pour déduire un vecteur $\mathbf{b}$ satisfaisant les propriétés du Théorème 2, il suffit de considérer $\mathbf{b} = (-a_2, a_1)$. La preuve consiste d'une part à majorer la hauteur des points isolés dans V en utilisant le résultant et d'autre part, à minorer la hauteur de ξ par un théorème de E. Dobrowolski [21] sur la minoration de la hauteur des nombres algébriques non nuls et différents des racines de l'unité, en utilisant une version explicite par P. Voutier [45]. Ce théorème de Dobrowolski est un résultat partiel dans la direction de la Conjecture de Lehmer. Le résultat que l'on a obtenu permet de montrer l'existence ou non de facteurs communs non-cyclotomiques de deux polynômes f et g à une variable lorsqu'ils sont spécialisations de deux polynômes à deux variables. L'algorithme suggéré par le Théorème 1 consiste à tester tous les vecteurs $\mathbf{b}$ plus petits que la borne du Théorème 2. Dans

le Chapitre 3, on propose également un algorithme plus efficace, dans le cas où $n = 2$, qui consiste à construire les vecteurs $\mathbf{b}$ en utilisant le résultant.

Dans le Chapitre 4, on présente une version explicite du Théorème 2 dans le cas $n = 3$, basée sur une amélioration de la preuve de A. Schinzel [40, Theorem 45]. L'approche de A. Schinzel consiste à considérer deux vecteurs linéairement indépendants $\mathbf{u}_1, \mathbf{u}_2$ tels que $\mathbf{a} \in \langle \mathbf{u}_1, \mathbf{u}_2 \rangle$ et tels que $\|\mathbf{u}_1\|_\infty \|\mathbf{u}_2\|_\infty$ est minimal. Ensuite, on pose $H(y_1, y_2) = \mathrm{pgcd}(F(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}), G(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}))$ et on considère deux cas selon le cas où H est un monôme ou non. Si H n'est pas un monôme alors on montre l'existence d'un vecteur $\mathbf{b}$ satisfaisant les propriétés requises en utilisant un théorème d'Ostrowski sur le polytope de Newton de l'ensemble de support de F et G. En revanche, si H est un monôme alors on montre que le degré de ξ peut être contrôlé par $\|\mathbf{a}\|^{1/2}$ (le fait que cet exposant soit strictement inférieur à 1 est crucial). En séparant encore en deux sous-cas suivant la nature du polytope de Newton de F et de G, soit on montre que la norme de $\mathbf{a}$ est majorée par une constante explicite à l'aide du Théorème de Dobrowolski, soit on trouve directement un vecteur $\mathbf{b}$ dont la norme est majorée par F et G.

Dans le Chapitre 5, toujours dans le cas particulier $n = 3$, on suit une approche inspirée de la preuve de E. Bombieri et U. Zannier dans [40, Appendix] et de celle de E. Bombieri, D. Masser et U. Zannier dans [11, Theorem 1.6]. Cette approche consiste à construire un sous-tore auxiliaire T_2 de dimension 2 contenant $\boldsymbol{\alpha} = \boldsymbol{\zeta}\boldsymbol{\xi}^{\mathbf{a}}$. Ensuite, on sépare trois cas. Dans le premier cas, on suppose que $\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$. Dans ce cas, on majore la hauteur de $\boldsymbol{\alpha}$ en explicitant un théorème de U. Zannier [40, Appendix]. En minorant la hauteur de ξ avec le Théorème de Dobrowolski relatif [5], on montre que la norme de $\mathbf{a}$ est majorée par une constante ne dépendant que de D et h. Dans le deuxième cas, on suppose que $\boldsymbol{\alpha}$ n'est pas un point isolé et que $\boldsymbol{\alpha}$ n'appartient pas à un translaté de sous-tore de dimension non nulle contenu dans V. Dans ce deuxième cas, on peut conclure par un argument de dimension. Enfin, dans le dernier cas, si $\boldsymbol{\alpha}$ est contenu dans un translaté de sous-tore contenu dans V, alors on fait un changement de variable pour se ramener au cas $n = 2$.

Dans le Chapitre 6, on présente une nouvelle approche, encore dans le cas $n = 3$, que l'on développe ensuite dans le Chapitre 8 pour n quelconque. Le début de la preuve est similaire à celui du Chapitre 5. On construit un tore auxiliaire T_2 de dimension 2 et on sépare trois cas comme dans le Chapitre 5. Dans le premier cas, on suppose que $\boldsymbol{\alpha} = \boldsymbol{\zeta}\boldsymbol{\xi}^{\mathbf{a}}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$. Dans ce cas, la nouveauté de la preuve consiste à utiliser une majoration de type Bézout Arithmétique que l'on obtient, dans ce cas particulier ($n = 3$), à l'aide du résultant. Dans le deuxième et le troisième cas, on procède comme dans le Chapitre 5. Dans le même chapitre, pour n quelconque, on décrit également un algorithme qui permet de calculer l'ensemble des sous-tores de $\mathbb{G}_{\mathrm{m}}^n$ dont un translaté est contenu dans V et y est maximal. En combinant ces algorithmes avec ceux du Chapitre 2, on a un algorithme qui permet de résoudre la Conjecture de Schinzel dans le cas où $\boldsymbol{\alpha}$ appartient à un translaté de sous-tore contenu dans V lorsque $n = 3$.

Le Chapitre 7 contient des comparaisons des bornes obtenues suivant les différentes approches décrites dans les chapitres précédents. Dans chaque approche, le schéma de la preuve est divisé en trois cas, mais ce n'est pas toujours le même schéma. Pour pouvoir les comparer, on divise en quatre cas. On note V^{a} la réunion des translatés de sous-tores de dimension non nulle contenus dans V et V^{o} le complémentaire de V^{a} dans V. Le tableau suivant résume les différentes bornes obtenues en omettant les puissances de $\log$:

On observe que l'approche décrite dans le Chapitre 6 donne une borne plus précise, en particulier dans le cas où $\boldsymbol{\alpha}$ est un point isolé. En utilisant ces bornes, on explicite l'algorithme correspondant au Théorème 1 pour le calcul de la partie non-cyclotomique du pgcd de deux polynômes $f, g \in \mathbb{Z}[x]$ qui sont des spécialisations de deux polynômes F et G à (seulement) trois variables.

Hypothèses	Chapitre 4	Chapitre 5	Chapitre 6
$\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$	ND^4	$N^3D^5h^2$	Dh
$\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{a}}$	D^5h	D^4h	Dh
$\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$	D^6	D^4	D^4
$\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{a}}$	D^5h	D^4h	D^4h
Maximum	D^6h	$N^3D^5h^2$	D^4h

Tableau 1 – Ordre de grandeur des bornes suivant les différentes approches

Enfin, dans le Chapitre 8, on présente une nouvelle méthode pour démontrer le Théorème 2 pour n quelconque en explicitant la dépendance en D et h. 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 [15], où ils ont démontré un théorème analogue au Théorème 2 dans le cas des courbes elliptiques. L'idée principale consiste à utiliser le Théorème de Bézout Arithmétique et une version fonctorielle du Théorème de Dobrowolski généralisé. Pour expliciter la dépendance en n de notre résultat, il faudrait expliciter la méthode de transfert de G. Rémond [39] qui permet de déduire une version fonctorielle du Théorème de Dobrowolski généralisé à partir de la version relative de E. Delsinne [20]. Le tableau suivant résume la dépendance en D et h des bornes obtenues pour n quelconque et pour tout $\varepsilon > 0$.

Hypothèses	Bornes
$\boldsymbol{\alpha} \in V^{\mathrm{o}}$	$(hD + D^2)^{1+\varepsilon}$
$\boldsymbol{\alpha} \in V^{\mathrm{a}}$	$(hD^{(n-1)^2} + D^{(n-1)^2+n})^{1+\varepsilon}$

Tableau 2 – Ordre de grandeur des bornes pour n quelconque

Dans le cas où $\boldsymbol{\alpha} \in V^{\mathrm{o}}$, on a utilisé le Théorème de Bézout Arithmétique qui donne une majoration de type $hD^{k-1} + D^k$ pour la hauteur des sous-variétés de codimension k de $\mathbb{G}_{\mathrm{m}}^n$. On remarque que, dans le Chapitre 3, on a montré une majoration de même type sans le terme en D^k pour le cas des sous-variétés de dimension 0 dans $\mathbb{G}_{\mathrm{m}}^2$. Il serait ainsi intéressant d'avoir une majoration du type hD^{k-1} pour n et k quelconques. Une telle majoration permettrait de :

— remplacer le terme $hD + D^2$ par hD dans le cas où $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ et pour n quelconque ;
— remplacer le terme $hD^{(n-1)^2} + D^{(n-1)^2+n}$ par $hD^{(n-1)^2}$ dans le cas où $\boldsymbol{\alpha} \in V^{\mathrm{a}}$ et pour n quelconque ;
— remplacer le terme D^4 par hD dans le cas où $\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ pour $n = 3$.

Dans le cas où $\boldsymbol{\alpha} \in V^{\mathrm{a}}$, on applique une stratégie semblable à celle du Chapitre 6 qui consiste à se ramener à une situation du type $\boldsymbol{\alpha} \in W^{\mathrm{o}}$ pour une sous-variété W contenue dans $\mathbb{G}_{\mathrm{m}}^{r}$ où $r < n$.

Enfin, on a reporté à l'annexe les preuves de certains résultats auxiliaires.

1. Préliminaires

1.1 Notations

Soit $n > 0$ un entier.

Norme d'un vecteur

Soit $\mathbf{a} \in \mathbb{C}^n$. On note par $\|\mathbf{a}\|_i$ la norme L_i de $\mathbf{a}$ pour $i \in \{1, 2, \infty\}$. Par exemple, $\|\mathbf{a}\|_\infty$ désigne le maximum des valeurs absolues des coordonnées de $\mathbf{a}$. Soit, de plus, $\mathbf{b} \in \mathbb{C}^n$. La notation $\mathbf{ab}$ désigne le produit scalaire entre $\mathbf{a}$ et $\mathbf{b}$ et on considère implicitement que $\mathbf{a}$ est un vecteur ligne et $\mathbf{b}$ est un vecteur colonne.

Polynômes

Soit $\mathbb{K}$ un corps. Soient $x_1, \cdots, x_n$ des indéterminées. On note $\mathbf{x} = (x_1, \cdots, x_n)$ et $\mathbb{K}[\mathbf{x}^{\pm 1}]$ l'anneau des polynômes de Laurent à coefficients dans $\mathbb{K}$ en ces indéterminées. On note $\mathbb{Z}[\mathbf{x}^{\pm 1}]$ l'anneau des polynômes de Laurent à coefficients dans $\mathbb{Z}$ en ces indéterminées.

Soit $F \in \mathbb{K}[\mathbf{x}^{\pm 1}]$. On note $\mathrm{Supp}(F) \subset \mathbb{Z}^n$ le support de F i.e. l'ensemble des exposants des monômes de F correspondant aux coefficients non nuls. Le polynôme F peut s'écrire sous la forme $F(\mathbf{x}) = x_1^{a_1} \cdots x_n^{a_n} \widetilde{F}(\mathbf{x})$ où $(a_1, \cdots, a_n) \in \mathbb{Z}^n$ et $\widetilde{F} \in \mathbb{K}[\mathbf{x}]$ tels que $\mathrm{pgcd}(\widetilde{F}, x_1 \cdots x_n) = 1$. Le polynôme $\widetilde{F}$ est uniquement déterminé par F et on l'appellera le *polynôme associé à* F. On définit alors :

- $\deg_{x_i}(F)$ le degré partiel de $\widetilde{F}$ par rapport à x_i ;
- $\deg_\infty(F)$ le maximum des degrés partiels de $\widetilde{F}$;
- $\deg_1(F)$ la somme des degrés partiels de $\widetilde{F}$;
- $\deg(F)$ le degré total de $\widetilde{F}$.

Si $G \in \mathbb{K}[\mathbf{x}^{\pm 1}]$ alors le résultant de F et G par rapport à x_i est le résultant de $\widetilde{F}$ et $\widetilde{G}$ par rapport à x_i. Si $F, G \in \mathbb{C}[\mathbf{x}^{\pm 1}]$ alors on désigne par $\|F\|_i$ la norme L_i du vecteur formé par les coefficients non nuls de F.

Tore algébrique

L'ensemble $\mathbb{G}_{\mathrm{m}}^n = (\overline{\mathbb{Q}}^*)^n$ est appelé *le tore algébrique de dimension* n. C'est un groupe pour la multiplication coordonnée par coordonnée :

$$(x_1, \cdots, x_n)(y_1, \cdots, y_n) = (x_1 y_1, \cdots, x_n y_n).$$

Un élément d'ordre fini dans $\mathbb{G}_{\mathrm{m}}^n$ est appelé un *point de torsion*. On note $\boldsymbol{\mu}_\infty^n$ l'ensemble des points de torsion de $\mathbb{G}_{\mathrm{m}}^n$. Si $\mathbb{K}$ est un corps de nombres alors on note $\boldsymbol{\mu}_{\mathbb{K}}^n$ l'ensemble de points de torsion de $\mathbb{G}_{\mathrm{m}}^n$ qui sont définis sur $\mathbb{K}$. Par exemple, on a $\boldsymbol{\mu}_{\mathbb{Q}}^n = \{\pm 1\}^n$. Si $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ alors on note $\mathbb{Q}(\boldsymbol{\alpha})$ le corps de définition de $\boldsymbol{\alpha}$ i.e. le plus petit sous-corps de $\overline{\mathbb{Q}}$ contenant tous les α_i pour $0 \leqslant i \leqslant n$.

Soient $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{G}_{\mathrm{m}}^n$ et $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbb{Z}^n$. On note :

$$\boldsymbol{\alpha}^{\mathbf{a}} \coloneqq \alpha_1^{a_1} \cdots \alpha_n^{a_n}.$$

Si $\xi \in \mathbb{G}_{\mathrm{m}}$ alors on note :

$$\xi^{\mathbf{a}} \coloneqq (\xi^{a_1}, \cdots, \xi^{a_n}).$$

Soit $m, l > 0$ deux autres entiers. On note $M_{n,m}(\mathbb{Z})$ l'ensemble des matrices de taille $n \times m$ à coefficients entiers et $\mathrm{GL}_n(\mathbb{Z})$ le groupe des matrices de taille $n \times n$ à coefficients entiers dont le déterminant vaut ± 1.

Soit $A \in M_{n,m}(\mathbb{Z})$ une matrice dont les colonnes sont les coordonnées de $\mathbf{a}_1, \cdots, \mathbf{a}_m$ par rapport à la base canonique de $\mathbb{Z}^n$. On pose :

$$\boldsymbol{\alpha}^A = (\boldsymbol{\alpha}^{\mathbf{a}_1}, \cdots, \boldsymbol{\alpha}^{\mathbf{a}_m}).$$

Soit $B \in M_{m,l}(\mathbb{Z})$. Alors on a :

$$(\boldsymbol{\alpha}^A)^B = \boldsymbol{\alpha}^{AB}. \tag{1.1.1}$$

En effet, en notant $\mathbf{b}_i = (b_{i1}, \cdots, b_{im})$ pour $1 \leqslant i \leqslant l$, on a :

$$(\boldsymbol{\alpha}^A)^B = (\boldsymbol{\alpha}^{\mathbf{a}_1}, \cdots, \boldsymbol{\alpha}^{\mathbf{a}_m})^B = (\boldsymbol{\alpha}^{b_{11}\mathbf{a}_1 + \cdots + b_{1m}\mathbf{a}_m}, \cdots, \boldsymbol{\alpha}^{b_{l1}\mathbf{a}_1 + \cdots + b_{lm}\mathbf{a}_m}) = \boldsymbol{\alpha}^{AB}.$$

Pour toute matrice A, on notera $A^\top$ sa *transposée*.

Sous-variété de $\mathbb{G}_{\mathrm{m}}^n$

On fixe le plongement naturel :

$$\begin{aligned} \iota_n : \mathbb{G}_{\mathrm{m}}^n &\hookrightarrow \mathbb{P}^n \\ (\alpha_1, \cdots, \alpha_n) &\mapsto (1 : \alpha_1 : \cdots : \alpha_n). \end{aligned}$$

Ainsi, les sous-ensembles algébriques de $\mathbb{G}_{\mathrm{m}}^n$ peuvent être vus comme des ensembles algébriques de $\mathbb{P}^n$ en considérant leur adhérence de Zariski dans $\mathbb{P}^n$.

On dit qu'un ensemble algébrique (ou un fermé de Zariski) est défini sur un corps $\mathbb{K} \subseteq \overline{\mathbb{Q}}$ s'il est stable sous l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$. En d'autres termes, cela signifie que son idéal de définition peut être engendré par des polynômes à coefficients dans le corps $\mathbb{K}$. Le corps de définition d'un ensemble algébrique sera le plus petit sous-corps de $\overline{\mathbb{Q}}$ sur lequel il est défini. Une variété désignera un ensemble algébrique et irréductible sur son corps de définition.

Soit V une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$. Le degré de V, notée $\deg(V)$, est le degré de la clôture de Zariski de $\iota_n(V)$ dans $\mathbb{P}^n$. La dimension de V, notée $\dim(V)$, est la longueur maximale d d'une suite :

$$V_0 \subset V_1 \subset \cdots \subset V_d,$$

telles que les V_i sont des sous-variétés algébriques de V, non-vides, irréductibles et distinctes. Si $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ alors on définit $\dim_{\boldsymbol{\alpha}}(V)$ comme la dimension maximale des composantes irréductibles sur $\overline{\mathbb{Q}}$ de V contenant $\boldsymbol{\alpha}$. Dans la suite, toute variété irréductible est implicitement définie sur $\overline{\mathbb{Q}}$.

Si $F_1, \cdots, F_s \in \overline{\mathbb{Q}}[\mathbf{x}^{\pm 1}]$ alors on note $V(F_1, \cdots, F_s)$ la sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie par $F_1 = \cdots = F_s = 0$.

1.2 Mesure de Mahler, Hauteur de Weil et Conjecture de Lehmer

Dans cette section, on rappelle les définitions de la mesure de Mahler d'un polynôme et la hauteur de Weil d'un nombre algébrique. On évoque également la Conjecture de Lehmer sur le problème de minoration de la hauteur.

1.2.1 Mesure de Mahler et Hauteur de Weil

En 1962, K. Mahler a introduit dans [31] une mesure pour la complexité les polynômes (qui portera plus tard son nom). Soit $F \in \mathbb{C}[x]$ un polynôme non nul. La *mesure de Mahler* de F est définie par :

$$M(F) = \exp\left(\int_0^1 \log|F(e^{2\pi i\theta})|d\theta\right).$$

De manière équivalente, en écrivant F sous la forme :

$$F(x) = a_d \prod_{i=1}^{d}(x - \alpha_i),$$

où d est le de degré de F, a_d son coefficient dominant et α_i ses racines complexes, on a :

$$M(F) = |a_d| \prod_{i=1}^{d} \max(1, |\alpha_i|).$$

L'équivalence des deux définitions découle de la formule de Jensen :

$$\int_0^1 \log|e^{2\pi i\theta} - \alpha|d\theta = \log^+|\alpha|,$$

où $\log^+ x = \max(0, \log x)$.

Soit α un nombre algébrique. Soit $P_\alpha \in \mathbb{Z}[x]$ son polynôme minimal (i.e. irréductible sur $\mathbb{Q}$ et primitif). On définit :

$$M(\alpha) = M(P_\alpha).$$

Soit $\mathbb{K}$ un corps de nombres contenant α. D'après [10, Proposition 1.4.7], il est possible de choisir un ensemble $M_\mathbb{K}$ de représentants des classes d'équivalence de valeurs absolues sur $\mathbb{K}$ de telle sorte que pour tout $x \in \mathbb{K}^*$, on ait la formule du produit :

$$\prod_{v \in M_\mathbb{K}} |x|_v^{n_v} = 1,$$

où $n_v = [\mathbb{K}_v : \mathbb{Q}_v]$ est le degré local en v. D'après [10, Proposition 1.6.5], la quantité

$$h(\alpha) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_K} n_v \log^+|\alpha|_v$$

est appelée *hauteur de Weil de* α. Elle ne dépend pas du choix du corps $\mathbb{K}$ qui contient α. D'après [10, Proposition 1.6.6], on a la relation :

$$h(\alpha) = \frac{\log M(\alpha)}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}.$$

Cette hauteur vérifie les propriétés suivantes :

— $h(\alpha) \geqslant 0$ et de plus, $h(\alpha) = 0$ si et seulement si $\alpha \in \{0\} \cup \boldsymbol{\mu}_\infty$ (Théorème de L. Kronecker [26]),
— $h(\zeta\alpha) = h(\alpha)$ si $\zeta \in \boldsymbol{\mu}_\infty$,

— $h(1/\alpha) = h(\alpha)$ et plus généralement, $h(\alpha^m) = |m|h(\alpha)$ pour tout $m \in \mathbb{Z}$ et avec $\alpha \neq 0$,
— $h(\sigma(\alpha)) = h(\alpha)$ pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

La notion de mesure de Mahler d'un polynôme se généralise à un polynôme à plusieurs variables. Soit $n > 0$ un entier et soit $F \in \mathbb{C}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$ non nul. La *mesure de Mahler* de F est définie par :

$$M(F) = \exp\left(\int_{[0,1]^n} \log|F(e^{2\pi i\theta_1}, \cdots, e^{2\pi i\theta_n})| d\theta_1 \cdots d\theta_n\right).$$

On remarque que la mesure de Mahler est multiplicative i.e. si $F, G \in \mathbb{C}[\mathbf{x}^{\pm 1}]$ sont non nuls alors on a :

$$M(FG) = M(F)M(G).$$

En outre, on a aussi les inégalités suivantes :

$$M(F) \leqslant \|F\|_1 \leqslant 2^{\deg_1(F)} M(F). \tag{1.2.1}$$

La première inégalité se déduit directement de la définition. La seconde inégalité se déduit de [40, Corollary 11]. Remarquons que cette deuxième inégalité est atteinte. Par exemple, si $d \in \mathbb{N}$ et $F = (x-1)^d$ alors on a $\|F\|_1 = 2^d$ et $2^{\deg_1(F)} M(F) = 2^d$.

Si $0 \neq F \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$ alors on a $M(F) \geqslant 1$ (voir par exemple [40, Lemma 15 avec $\sigma = 0$]). De plus, d'après [40, Corollary 17], $M(F) = 1$ si et seulement si F est primitif et égal à un produit de monômes et de polynômes cyclotomiques généralisés (un polynôme cyclotomique généralisé est un polynôme de la forme $\phi_d(\mathbf{x}^{\boldsymbol{\mu}})$ où $\boldsymbol{\mu} \in \mathbb{Z}^n$ et ϕ_d est un polynôme cyclotomique).

Calcul de la mesure de Mahler

Soit $n > 0$ un entier et soit $0 \neq F \in \mathbb{C}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$. Si $n = 1$ alors, grâce à la formule de Jensen, on peut calculer la mesure de Mahler de F en utilisant ses racines. Si $n \geqslant 2$ alors le calcul de la mesure de Mahler F peut être difficile puisque on n'a pas une version analogue de la formule de Jensen. Cependant, en utilisant une approche basée sur la méthode de Graeffe, on peut déterminer un encadrement de la mesure de Mahler de F. La méthode suivante est celle décrite par D. Boyd dans [13]. On commence par définir une opération τ sur F par la formule suivante :

$$\tau(F)(x_1, \cdots, x_n) = \prod F(\pm x_1^{1/2}, \cdots, \pm x_n^{1/2}),$$

où le produit est sur l'ensemble de 2^n choix des signes. Ce polynôme est bien défini. En effet, le polynôme $G(y_1, \cdots, y_n) = \prod F(\pm y_1, \cdots, \pm y_n)$ est invariant pour tout changement de variables y_j en $-y_j$. Ainsi G est une fonction paire pour chaque variable y_i et donc $\tau(F)$ est bien un polynôme. Il est immédiat que $\deg_{x_i} \tau(F) = 2^{n-1} \deg_{x_i}(F)$. De plus, par la multiplicativité de la mesure de Mahler, on a $M(\tau(F)) = M(G) = M(F)^{2^n}$ puisque chacun des polynômes $F(\pm y_1, \cdots, \pm y_k)$ a pour mesure de Mahler $M(F)$.

Soit $m > 0$ un entier. On définit $\tau^m(F)$ comme étant le résultat de m applications de l'opération τ à F. On a alors :

$$M(\tau^m(F)) = M(F)^{2^{mn}} \quad \text{et} \quad \deg_{x_i} \tau^m(F) = 2^{(n-1)m} \deg_{x_i}(F).$$

D'après (1.2.1), on en déduit que :

$$M(F)^{2^{mn}} \leqslant \|\tau^m(F)\|_1 \leqslant 2^{2^{(n-1)m} \deg_1(F)} M(F)^{2^{nm}}.$$

Ainsi, on obtient l'encadrement :

$$\left(\frac{\|\tau^m(F)\|_2}{2^{2(n-1)m\deg_1(F)}}\right)^{1/2^{mn}} \leqslant M(F) \leqslant \|\tau^m(F)\|_1^{1/2^{mn}}. \tag{1.2.2}$$

On a aussi $M(F) \leqslant \|F\|_2$ d'après [40, Corollary 11]. Cela permet de remplacer la norme L_1 dans (1.2.2) par la norme L_2 qui est plus fine.

Remarques. $(\mathbf{1})$ On note que dans cet encadrement, plus m est grand, plus les deux bornes obtenues sont plus précises. Cependant, cela aura un impact dans le coût des calculs.

$(\mathbf{2})$ En observant sur quelques exemples, la minoration ne fournit pas une bonne approximation de la mesure de Mahler. En revanche, avec la majoration, on obtient une bonne approximation de celle-ci.

1.2.2 Conjecture de Lehmer

La *Conjecture de Lehmer* (connue aussi sous le nom de *Problème de Lehmer*) peut être formulée comme suit :

Conjecture 1.2.2.1 (Conjecture de Lehmer)**.** *Il existe une constante absolue c telle que $M(\alpha) \geqslant c > 1$ pour tout $\alpha \in \overline{\mathbb{Q}}$ non nul et différent des racines de l'unité.*

L'hypothèse que α est non nul et n'est pas une racine de l'unité est nécessaire car sinon on a $M(\alpha) = 1$. Cette conjecture reste encore ouverte dans toute sa généralité. La meilleure borne connue sans condition supplémentaire est due à E. Dobrowolski [21] en 1979 :

Théorème 1.2.2.2. *[21, Theorem 1] Pour tout réel $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tout nombre algébrique non nul α qui n'est pas une racine de l'unité, on a :*

$$[\mathbb{Q}(\alpha) : \mathbb{Q}]^{1+\varepsilon} h(\alpha) \geqslant c(\varepsilon).$$

En 1996, P. Voutier a donné une version explicite de ce théorème. Dans [45], il a montré :

Théorème 1.2.2.3. *[45, Theorem, p. 83] Soit $\alpha \neq 0$ un nombre algébrique de degré d qui n'est pas une racine de l'unité. Si $d \geqslant 3$ alors on a :*

$$\log M(\alpha) \geqslant \frac{1}{4}\left(\frac{\log\log d}{\log d}\right)^3$$

et

$$\log M(\alpha) \geqslant \frac{2}{(\log(3d))^3}.$$

La deuxième minoration est plus fine pour $3 \leqslant d \leqslant 184$.

Si $d \geqslant 1$ est un entier alors on définit $\ell(d)$ la borne supérieure de l'ensemble des réels $1/\log M(\alpha)$ où α parcourt les nombres algébriques non nuls et différents des racines de l'unité de degré $\leqslant d$ i.e.

$$\ell(d) = \sup\left\{(\log M(\alpha))^{-1}, \alpha \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty \ , \deg(\alpha) \leqslant d\right\}. \tag{1.2.3}$$

Remarquons que cette fonction ℓ est croissante. D'après [12] et [34], on connaît les valeurs exactes de $\ell(d)$ pour $1 \leqslant d \leqslant 55$:

$$\begin{aligned}
&\ell(1) = (\log 2)^{-1} \leqslant 1,44270,\\
&\ell(2) = (\log \alpha)^{-1} \leqslant 2,07809,\\
&\ell(d) = (\log M(P_3))^{-1} \leqslant 3,55620 \text{ pour } d = 3,4,5,6,7,\\
&\ell(d) = (\log M(P_8))^{-1} \leqslant 4,04272 \text{ pour } d = 8,9,\\
&\ell(d) = (\log M(P_{10}))^{-1} \leqslant 6,15925 \text{ pour } 10 \leqslant d \leqslant 55,
\end{aligned}$$

où

— $\alpha = (1+\sqrt{5})/2$ est le nombre d'or
— $P_3 = x^3 - x - 1$,
— $P_8 = x^8 + x^5 - x^4 + x^3 + 1$
— $P_{10} = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$.

Enfin, d'après le Théorème 1.2.2.3, on a $\ell(d) \leqslant 4(\log d/\log\log d)^3$ pour tout entier $d \geqslant 3$. Il existe également une conjecture de Lehmer dite *forte* :

Conjecture 1.2.2.4 (Conjecture de Lehmer Forte)**.** *Soit $\alpha \in \overline{\mathbb{Q}}^*$ qui n'est pas une racine de l'unité. Alors on a :*

$$M(\alpha) \geqslant M(P_{10}) \approx 1,176280818\cdots$$

1.2.3 Version relative de la Conjecture de Lehmer

F. Amoroso et U. Zannier ont proposé une version relative de la Conjecture de Lehmer en remplaçant le degré de α sur $\mathbb{Q}$ par le degré « non abélien » de α sur un corps de nombres $\mathbb{K}$, i. e. le degré de α sur une extension abélienne de $\mathbb{K}$. Ils ont montré dans [5] un analogue du Théorème de Dobrowolski dans le cas relatif :

Théorème 1.2.3.1. *[5, Theorem 1.1] Soit $\mathbb{K}$ un corps de nombres. Il existe une constante $c(\mathbb{K})$ strictement positive ne dépendant que de $\mathbb{K}$ et vérifiant la propriété suivante. Pour tout nombre algébrique non nul α qui n'est pas une racine de l'unité et pour toute extension abélienne $\mathbb{L}$ de $\mathbb{K}$, on a :*

$$h(\alpha) \geqslant \frac{c(\mathbb{K})}{D}\left(\frac{\log\log 5D}{\log 2D}\right)^{13}$$

où $D = [\mathbb{L}(\alpha) : \mathbb{L}]$.

Dans notre situation, on a besoin d'une version explicite de $c(\mathbb{Q})$. Un des résultats dans cette direction est le théorème du premier auteur et E. Delsinne. Ils ont donné la dépendance en $\mathbb{K}$ de la constante $c(\mathbb{K})$ qui dépend d'une part du degré du corps $\mathbb{K}$ et d'autre part de son discriminant. Ils ont montré dans [3] le résultat suivant.

Théorème 1.2.3.2. *[3, Théorème 1.3] Soit $\mathbb{K}$ un corps de nombres de degré δ et discriminant Δ. Soit α un nombre algébrique non nul qui n'est pas une racine de l'unité. Alors pour toute extension abélienne $\mathbb{L}$ de $\mathbb{K}$, on a :*

$$h(\alpha) \geqslant \frac{(2g(\delta)\Delta)^{-c}}{d}\frac{\log\log(5d)^3}{\log(2d)^4}$$

où c est une constante absolue strictement positive, $d = [\mathbb{L}(\alpha) : \mathbb{L}]$ et $g(\delta) = 1$ s'il existe une tour d'extensions :

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \mathbb{K}_m = \mathbb{K}$$

avec $\mathbb{K}_i/\mathbb{K}_{i-1}$ est normale pour $i = 1, \cdots, m$ et $g(\delta) = \delta!$ sinon.

E. Delsinne a montré dans [20] une généralisation du Théorème 1.2.3.2, dont la borne est explicite. Pour $n = 3$, cette borne fait intervenir une constante $c_1(3) > \exp(16 \times 10^{13})$ qui est beaucoup trop grande pour être utilisée dans des applications algorithmiques. Par conséquent, on a choisi de garder le Théorème 1.2.3.2 pour nos applications plus tard.

1.3 Sous-groupes de $\mathbb{Z}^n$ et sous-groupes algébriques de $\mathbb{G}_{\mathrm{m}}^n$

Dans cette section, on fixe un entier $n > 0$. On rappelle ici la définition d'un sous-groupe saturé de $\mathbb{Z}^n$ et ses propriétés. Ensuite, on présente la correspondance entre les sous-groupes de $\mathbb{Z}^n$ et les sous-groupes algébriques de $\mathbb{G}_{\mathrm{m}}^n$.

1.3.1 Sous-groupes de $\mathbb{Z}^n$

On dit qu'un sous-groupe Λ de $(\mathbb{R}^n, +)$ est discret si chaque point de Λ est isolé dans $\mathbb{R}^n$ muni de la topologie usuelle. Par exemple, les sous-groupes $\{\mathbf{0}\}$ et le réseau $\mathbb{Z}^n$ sont des sous-groupes discrets de $\mathbb{R}^n$. Cette définition implique que tout sous-groupe d'un sous-groupe discret est discret. Donc, tout sous-groupe de $\mathbb{Z}^n$ est un sous-groupe discret. On pose :

$$\mathbb{Q}\Lambda = \{x\boldsymbol{\lambda}, x \in \mathbb{Q}, \boldsymbol{\lambda} \in \Lambda\} \quad \text{et} \quad \mathbb{R}\Lambda = \{x\boldsymbol{\lambda}, x \in \mathbb{R}, \boldsymbol{\lambda} \in \Lambda\}$$

La proposition suivante montre que les sous-groupes discrets de $\mathbb{R}^n$ sont isomorphes à $\mathbb{Z}^r$, pour un certain entier $0 \leqslant r \leqslant n$.

Proposition 1.3.1.1. *[46, Theorem 4.20, p.168] Tout sous-groupe discret Λ de $\mathbb{R}^n$ admet une $\mathbb{Z}$-base finie formée par des vecteurs $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_r$ qui sont linéairement indépendants sur $\mathbb{R}$. De plus on a $r = \dim_{\mathbb{Q}}(\mathbb{Q}\Lambda) = \dim_{\mathbb{R}}(\mathbb{R}\Lambda)$.*

On va s'intéresser aux sous-groupes de $\mathbb{Z}^n$. Soit $\Lambda \subset \mathbb{Z}^n$ un sous-groupe. Le *rang* de Λ, noté $\mathrm{rang}(\Lambda)$, est la dimension de l'espace vectoriel $\mathbb{R}\Lambda$ sur $\mathbb{R}$. On l'appelle aussi la *dimension* de Λ que l'on note $\dim(\Lambda)$. D'après la Proposition 1.3.1.1, on a $\mathrm{rang}(\Lambda) = \dim_{\mathbb{Q}}(\mathbb{Q}\Lambda)$.

Le *saturé* de Λ, noté Λ^{sat}, est défini par :

$$\Lambda^{\mathrm{sat}} = \mathbb{Q}\Lambda \cap \mathbb{Z}^n.$$

Ainsi, Λ^{sat} est un sous-groupe de $\mathbb{Z}^n$ contenant Λ et l'index $[\Lambda^{\mathrm{sat}} : \Lambda]$ est fini car Λ^{sat} et Λ ont le même rang. On dit que Λ est *saturé* ou *primitif* si $\Lambda^{\mathrm{sat}} = \Lambda$.

L'*orthogonal* $\Lambda^{\perp}$ de Λ est le sous-groupe de $\mathbb{Z}^n$ contenant les vecteurs orthogonaux à Λ. On remarque que $\Lambda^{\perp}$ est saturé (l'hypothèse $m\boldsymbol{\lambda} \in \Lambda^{\perp}$ implique $\boldsymbol{\lambda} \in \Lambda^{\perp}$ pour $\boldsymbol{\lambda} \in \mathbb{Z}^n$ et $m \in \mathbb{Z}$). Il s'ensuit que si Λ est saturé alors $\Lambda^{\perp\perp} = \Lambda$.

Dans la suite, si $m > 0$ est un entier et si $M \in M_{n,m}(\mathbb{Z})$ alors la notation $\langle M \rangle$ désigne le sous-groupe de $\mathbb{Z}^n$ engendré par les m vecteurs colonnes de M.

La proposition suivante donne des conditions équivalentes à la primitivité de Λ.

Proposition 1.3.1.2. *[46, Proposition 4.2] Soit Λ un sous-groupe de $\mathbb{Z}^n$ de rang r. Les propriétés suivantes sont équivalentes.*

1. *Λ est saturé.*
2. *$\mathbb{Z}^n/\Lambda$ est sans torsion.*
3. *Il existe un sous-groupe Λ_c de $\mathbb{Z}^n$ tel que $\Lambda \oplus \Lambda_c = \mathbb{Z}^n$, i.e., toute base de Λ peut se compléter en une base de $\mathbb{Z}^n$.*
4. *$\dim_{\mathbb{F}_p}(\Lambda(p)) = rang(\Lambda)$ pour tout nombre premier p et où $\Lambda(p)$ est l'image de Λ dans $\mathbb{F}_p^n$ par la réduction modulo p dans $\mathbb{Z}^n$.*
5. *Soit $\{\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_r\}$ une $\mathbb{Z}$-base de Λ. Alors, le pgcd des déterminants des mineurs d'ordre r de la matrice $(\boldsymbol{\lambda}_{ij})$ vaut 1.*

Dans nos applications, on utilisera principalement les propriétés **1**, **3** et **5** de cette proposition. La proposition suivante permet de construire une base d'un sous-groupe de $\mathbb{Z}^n$ à partir d'un système de vecteurs linéairement indépendants de rang maximal.

Proposition 1.3.1.3. *[44, Theorem 18] Soit Λ un sous-groupe de $\mathbb{Z}^n$ de rang r et soient $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_r \in \Lambda$ des vecteurs linéairement indépendants sur $\mathbb{R}$. Alors il existe des vecteurs $\boldsymbol{\mu}_1, \cdots, \boldsymbol{\mu}_r \in \Lambda$ formant une base de Λ et qui sont définis comme suit :*

$$\begin{aligned}
\boldsymbol{\mu}_1 &= c_1\boldsymbol{\lambda}_1, \\
\boldsymbol{\mu}_2 &= c_{2,1}\boldsymbol{\lambda}_1 + c_2\boldsymbol{\lambda}_2, \\
&\vdots \\
\boldsymbol{\mu}_r &= c_{r,1}\boldsymbol{\lambda}_1 + c_{r,2}\boldsymbol{\lambda}_2 + \cdots + c_{r,r-1}\boldsymbol{\lambda}_{r-1} + c_r\boldsymbol{\lambda}_r,
\end{aligned}$$

où les coefficients $c_{i,j}$ (pour $i = 2, \cdots, r$ et $j = 1, \cdots, i-1$) et c_k (pour $i = 1, \cdots, r$) sont des nombres rationnels avec :

$$0 \leqslant c_{i,j} < 1 \quad \text{et} \quad 0 < c_k \leqslant 1.$$

Par translation, on peut aussi prendre $-1/2 \leqslant c_{i,j} < 1/2$.

1.3.2 Sous-groupes algébriques de $\mathbb{G}_{\mathrm{m}}^n$

Un *sous-groupe algébrique* de $\mathbb{G}_{\mathrm{m}}^n$ est à la fois une sous-variété et un sous-groupe de $\mathbb{G}_{\mathrm{m}}^n$. Un *sous-tore* de $\mathbb{G}_{\mathrm{m}}^n$ est un sous-groupe algébrique qui est irréductible sur $\overline{\mathbb{Q}}$ en tant que variété. Si Λ est un sous-groupe de $\mathbb{Z}^n$, alors l'ensemble

$$H_\Lambda = \{\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n \mid \boldsymbol{\alpha}^{\boldsymbol{\lambda}} = 1, \ \forall\ \boldsymbol{\lambda} \in \Lambda\} \tag{1.3.1}$$

est un sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^n$ défini sur $\mathbb{Q}$. Il existe une bijection entre les sous-groupes de $\mathbb{Z}^n$ et les sous-groupes algébriques de $\mathbb{G}_{\mathrm{m}}^n$. En effet, d'après [42, Lemma 2], tout sous-groupe algébrique de

$\mathbb{G}_{\mathrm{m}}^n$ est de la forme (1.3.1) et $\dim H_\Lambda = n - \mathrm{rang}(\Lambda)$. D'après [10, Corollary 3.2.8], H_Λ est un sous-tore si et seulement si Λ est primitif. Si H est un sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^n$ et s'il existe un sous-groupe Λ de $\mathbb{Z}^n$ tel que $H = H_\Lambda$ alors on dit que H est défini par Λ.

Un *translaté de sous-groupe algébrique (resp. translaté de sous-tore)* est une sous-variété de la forme $\boldsymbol{\alpha}H$ (resp. $\boldsymbol{\alpha}T$) où $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ et H un sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^n$ (resp. T est un sous-tore de $\mathbb{G}_{\mathrm{m}}^n$).

Soit V une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$. Un translaté de sous-groupe algébrique $\boldsymbol{\alpha}H \subset V$ (resp. un translaté de sous-tore $\boldsymbol{\alpha}T$) est dit *maximal* si aucun translaté de sous-groupe algébrique $\boldsymbol{\beta}H'$ (resp. aucun translaté de sous-tore $\boldsymbol{\beta}T'$) ne vérifie $\boldsymbol{\alpha}H \subsetneq \boldsymbol{\beta}H' \subset V$ (resp. $\boldsymbol{\alpha}T \subsetneq \boldsymbol{\beta}T' \subset V$).

On note V^{a} la réunion des translatés de sous-tores de dimension non nulle contenus dans V et V^{o} le complémentaire de V^{a} dans V i.e. $V^{\mathrm{o}} = V \setminus V^{\mathrm{a}}$.

On va énoncer quelques résultats concernant les translatés de sous-groupes de $\mathbb{G}_{\mathrm{m}}^n$. La proposition suivante donne une paramétrisation d'un translaté de sous-tore par un point de torsion.

Proposition 1.3.2.1. *Soit T un sous-tore de $\mathbb{G}_{\mathrm{m}}^n$ de dimension d défini par un sous-groupe saturé Λ de $\mathbb{Z}^n$. Soit $A \in M_{d,n}(\mathbb{Z})$ une matrice dont les lignes forment une base de $\Lambda^\perp$. Soit $\boldsymbol{\eta} \in \boldsymbol{\mu}_\infty^n$. Si $\boldsymbol{\alpha} \in \boldsymbol{\eta}T$ alors il existe $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ et $\boldsymbol{\xi} \in \mathbb{G}_{\mathrm{m}}^d$ tels que $\boldsymbol{\alpha} = \boldsymbol{\zeta}\boldsymbol{\xi}^A$ et $\mathbb{Q}(\boldsymbol{\zeta}, \boldsymbol{\xi}) = \mathbb{Q}(\boldsymbol{\alpha})$. De plus, on a $\boldsymbol{\alpha} \in \boldsymbol{\mu}_\infty^n$ si et seulement si $\boldsymbol{\xi} \in \boldsymbol{\mu}_\infty^d$. Enfin, si $\boldsymbol{\eta} = \mathbf{1}$ alors $\boldsymbol{\zeta} = \mathbf{1}$.*

Démonstration. On note $\mathbf{a}_1, \cdots, \mathbf{a}_d \in \mathbb{Z}^n$ les lignes de A. Comme $\Lambda^\perp$ est primitif, il existe $\mathbf{a}_{d+1}, \cdots, \mathbf{a}_n \in \mathbb{Z}^n$ tels que $\{\mathbf{a}_1, \cdots, \mathbf{a}_n\}$ est une base de $\mathbb{Z}^n$. On note $\bar{A}$ la matrice dont les lignes sont $\mathbf{a}_{d+1}, \cdots, \mathbf{a}_n$ et M la matrice dont les lignes sont $\mathbf{a}_1, \cdots, \mathbf{a}_n$. On a alors :

$$M = \begin{pmatrix} A \\ \bar{A} \end{pmatrix} \in \mathbf{GL}_n(\mathbb{Z}).$$

On note $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_n$ les colonnes de la matrice M^{-1}. On a alors :

$$\boldsymbol{\alpha} = (\boldsymbol{\alpha}^{M^{-1}})^M = \left(\boldsymbol{\alpha}^{\boldsymbol{\lambda}_1}, \cdots, \boldsymbol{\alpha}^{\boldsymbol{\lambda}_n}\right)^M = (\boldsymbol{\alpha}^{\boldsymbol{\lambda}_1}, \cdots, \boldsymbol{\alpha}^{\boldsymbol{\lambda}_d})^A (\boldsymbol{\alpha}^{\boldsymbol{\lambda}_{d+1}}, \cdots, \boldsymbol{\alpha}^{\boldsymbol{\lambda}_n})^{\bar{A}}.$$

On pose $\boldsymbol{\xi} = (\boldsymbol{\alpha}^{\boldsymbol{\lambda}_1}, \cdots, \boldsymbol{\alpha}^{\boldsymbol{\lambda}_d})$ et $\boldsymbol{\zeta} = (\boldsymbol{\alpha}^{\boldsymbol{\lambda}_{d+1}}, \cdots, \boldsymbol{\alpha}^{\boldsymbol{\lambda}_n})^{\bar{A}}$. Par construction, on a $\boldsymbol{\alpha} = \boldsymbol{\zeta}\boldsymbol{\xi}^A$ et $\boldsymbol{\zeta}, \boldsymbol{\xi} \in \mathbb{Q}(\boldsymbol{\alpha})$. On a aussi $\boldsymbol{\alpha} \in \mathbb{Q}(\boldsymbol{\zeta}, \boldsymbol{\xi})$ (car $\boldsymbol{\alpha} = \boldsymbol{\zeta}\boldsymbol{\xi}^A$) et donc $\mathbb{Q}(\boldsymbol{\zeta}, \boldsymbol{\xi}) = \mathbb{Q}(\boldsymbol{\alpha})$.

Montrons que $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$. Comme $MM^{-1} = I_n$, on déduit que $\langle \boldsymbol{\lambda}_{d+1}, \cdots, \boldsymbol{\lambda}_n \rangle = (\Lambda^\perp)^\perp = \Lambda$. Comme $\boldsymbol{\alpha} \in \boldsymbol{\eta}T$, il existe $\boldsymbol{\tau} \in T$ tel que $\boldsymbol{\alpha} = \boldsymbol{\eta}\boldsymbol{\tau}$. En particulier, on a $\boldsymbol{\tau}^{\boldsymbol{\lambda}_i} = 1$ pour $d+1 \leqslant i \leqslant n$. On a alors :

$$\boldsymbol{\zeta} = ((\boldsymbol{\eta}\boldsymbol{\tau})^{\boldsymbol{\lambda}_{d+1}}, \cdots, (\boldsymbol{\eta}\boldsymbol{\tau})^{\boldsymbol{\lambda}_n})^{\bar{A}} = (\boldsymbol{\eta}^{\boldsymbol{\lambda}_{d+1}}, \cdots, \boldsymbol{\eta}^{\boldsymbol{\lambda}_n})^{\bar{A}}.$$

Ainsi, on a $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$. On déduit également que si $\boldsymbol{\eta} = \mathbf{1}$ alors $\boldsymbol{\zeta} = \mathbf{1}$. De plus, comme $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$, il est immédiat de voir que $\boldsymbol{\alpha} \in \boldsymbol{\mu}_\infty^n$ si et seulement si $\boldsymbol{\xi} \in \boldsymbol{\mu}_\infty^d$. □

On a la réciproque de la Proposition 1.3.2.1 dans le cas où $\boldsymbol{\zeta} = \mathbf{1}$.

Proposition 1.3.2.2. *Soit T un sous-tore de $\mathbb{G}_{\mathrm{m}}^n$ de dimension d défini par un sous-groupe saturé Λ de $\mathbb{Z}^n$. Soit $A \in M_{d,n}(\mathbb{Z})$ une matrice dont les lignes forment une base de $\Lambda^\perp$. Alors on a :*

$$T = \left\{\xi^A, \xi \in \mathbb{G}_{\mathrm{m}}^d\right\}.$$

Démonstration. Notons T' l'ensemble du second membre. D'après la Proposition 1.3.2.1, on a $T \subseteq T'$. Réciproquement, si $\xi^A \in T'$ alors on a $\xi^{A\boldsymbol{\lambda}} = 1$ pour tout $\boldsymbol{\lambda} \in \Lambda$. □

Si $F \in \mathbb{C}[\mathbf{x}^{\pm 1}]$ alors on note :

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

La proposition suivante permet de déterminer explicitement les équations de translatés de sous-tores contenus dans une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$. La preuve repose essentiellement sur le Lemma 4 de W. Schmidt [42].

Proposition 1.3.2.3. *Soit $s > 0$ un entier et soient $F_1, \cdots, F_s \in \mathbb{Z}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$. Soit $\boldsymbol{\alpha}T$ un translaté maximal de sous-tore contenu dans $V(F_1, \cdots, F_s)$ et de dimension non nulle. On pose $r = n - \dim T$. Alors il existe $\{\boldsymbol{\mu}_1, \cdots, \boldsymbol{\mu}_n\}$ formant une base de $\mathbb{Z}^n$ telle que $\{\boldsymbol{\mu}_1, \cdots, \boldsymbol{\mu}_r\}$ est une base du réseau définissant T. De plus, ces vecteurs peuvent être définis comme suit :*

— *pour $k = 1, \cdots, r$, on a :*

$$\boldsymbol{\mu}_k = c_{k,1}\boldsymbol{\lambda}_1 + c_{k,2}\boldsymbol{\lambda}_2 + \cdots + c_{k-1,1}\boldsymbol{\lambda}_{k-1} + c_k\boldsymbol{\lambda}_k,$$

— *pour $k = r+1, \cdots, n$, on a :*

$$\boldsymbol{\mu}_k = c_{k,1}\boldsymbol{\lambda}_1 + \cdots + c_{k,r}\boldsymbol{\lambda}_r + c_{k,r+1}\mathbf{e}_{i_{r+1}} + \cdots + c_{k,k-1}\mathbf{e}_{i_{k-1}} + c_k\mathbf{e}_{i_k},$$

où

- *$\boldsymbol{\lambda}_k \in \bigcup_i \mathcal{D}(F_i)$ pour tout k,*
- *les $\mathbf{e}_i$ sont des vecteurs de la base standard de $\mathbb{Z}^n$,*
- *les $c_{k,i}$ (pour $k = 1, \cdots, n$ et $i = 1, \cdots, k-1$) et les c_k (pour $k = 1, \cdots, n$) sont des nombres rationnels tels que $-1/2 \leqslant c_{k,i} < 1/2$ et $0 < c_k \leqslant 1$.*

Démonstration. On note $V = V(F_1, \cdots, F_s)$. 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 $i = 1, \cdots, s$. On a alors $\mathrm{Supp}(G_i) = \mathrm{Supp}(F_i)$ pour tout $i = 1, \cdots, s$. Comme T est un sous-tore de $\mathbb{G}_{\mathrm{m}}^n$, T est défini par un sous-groupe saturé Λ de $\mathbb{Z}^n$. Comme $H_\Lambda = T \subseteq \boldsymbol{\alpha}^{-1}V$ est maximal, d'après [42, Lemme 4], Λ est engendré par l vecteurs $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_l \in \mathbb{Z}^n$ (pour un certain entier $l \geqslant r$) tels que les $\boldsymbol{\lambda}_j \in \mathcal{D}(F_{i_j})$ pour un certain $i_j \in \{1, \cdots, s\}$. Comme $\mathrm{rang}(\Lambda) = r$, Λ contient r vecteurs linéairement indépendants que l'on note encore $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_r \in \mathbb{Z}^n$.

Posons $m = n - r = \dim T$. Si $m = 1$ alors il existe un vecteur $\mathbf{e}_{i_{r+1}}$ (avec $1 \leqslant i_{r+1} \leqslant n$) appartenant à la base canonique de $\mathbb{Z}^n$, tel que $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_r, \mathbf{e}_{i_{r+1}}$ soient linéairement indépendants sur $\mathbb{R}$. En raisonnant par récurrence, il existe des vecteurs $\mathbf{e}_{i_{r+1}}, \cdots, \mathbf{e}_{i_n}$ appartenant à la base canonique de $\mathbb{Z}^n$ tels que les vecteurs $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \cdots, \boldsymbol{\lambda}_r, \mathbf{e}_{i_{r+1}}, \cdots, \mathbf{e}_{i_n}$ soient linéairement indépendants sur $\mathbb{R}$. D'après la Proposition 1.3.1.3, il existe des vecteurs $\boldsymbol{\mu}_1, \cdots, \boldsymbol{\mu}_r, \boldsymbol{\mu}_{r+1}, \cdots, \boldsymbol{\mu}_n \in \mathbb{Z}^n$ formant une base de $\mathbb{Z}^n$, tels que :

— pour $k = 1, \cdots, r$, on a :

$$\boldsymbol{\mu}_k = c_{k,1}\boldsymbol{\lambda}_1 + c_{k,2}\boldsymbol{\lambda}_2 + \cdots + c_{k-1,1}\boldsymbol{\lambda}_{k-1} + c_k\boldsymbol{\lambda}_k,$$

— pour $k = r+1, \cdots, n$, on a :

$$\boldsymbol{\mu}_k = c_{k,1}\boldsymbol{\lambda}_1 + \cdots + c_{k,r}\boldsymbol{\lambda}_r + c_{k,r+1}\mathbf{e}_{i_{r+1}} + \cdots + c_{k,k-1}\mathbf{e}_{i_{k-1}} + c_k\mathbf{e}_{i_k},$$

— les $c_{k,i}$ (pour $k = 1, \cdots, n$ et $i = 1, \cdots, k-1$) et les c_k (pour $k = 1, \cdots, n$) sont des nombres rationnels avec $-1/2 \leqslant c_{k,i} < 1/2$ et $0 < c_k \leqslant 1$.

On note M le sous-groupe de $\mathbb{Z}^n$ engendré par les vecteurs $\boldsymbol{\mu}_1, \cdots, \boldsymbol{\mu}_r$. M est primitif car les vecteurs $\boldsymbol{\mu}_1, \cdots, \boldsymbol{\mu}_n$ forment une base de $\mathbb{Z}^n$. Les vecteurs $\boldsymbol{\mu}_1, \cdots, \boldsymbol{\mu}_r$ appartiennent à $\mathbb{Q}\Lambda$ car les vecteurs $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_r \in \Lambda$ et les coefficients $c_{k,i}, c_k$ sont des nombres rationnels. On a alors $M \subseteq \Lambda^{\mathsf{sat}} = \Lambda$. Comme $\mathrm{rang}(\Lambda) = \mathrm{rang}(M)$, on en déduit que $\Lambda = M$. □

1.4 Géométrie des nombres

Dans cette section, on fixe un entier $n \geqslant 2$. On rappelle ici les définitions sur les minimas successifs, la constante d'Hermite et la constante de Rankin. On énonce également le Second Théorème de Minkwoski. Pour une application ultérieure, on donne également un lemme qui affirme qu'étant donné un vecteur non nul $\mathbf{a} \in \mathbb{Z}^n$, il est possible de trouver deux vecteurs linéairement indépendants (sur $\mathbb{R}$) $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}^n$ tels que $\mathbf{a} \in \langle \mathbf{u}_1, \mathbf{u}_2 \rangle$ et dont leur déterminant est contrôlé par $\|\mathbf{a}\|_2^{(n-2)/(n-1)}$ (Lemme 1.4.2).

Minima successifs

Soit Λ un sous-groupe de $\mathbb{Z}^n$ de dimension d. Pour $1 \leqslant i \leqslant d$, *le i-ème minimum successif* de Λ, noté par $\lambda_i(\Lambda)$, est défini par :

$$\lambda_i(\Lambda) = \inf_{\substack{\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_i \in \Lambda \\ \text{lin. indep.}}} \max_{1 \leqslant j \leqslant i} \|\boldsymbol{\lambda}_j\|_2.$$

En d'autres termes, $\lambda_i(\Lambda)$ est le rayon de la plus petite boule dans $\mathbb{R}^n$ qui contient i vecteurs de Λ linéairement indépendants.

Déterminants

Si $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_d \in \mathbb{Z}^n$ alors on définit :

$$\det(\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_d) = |\det(U^\top U)|^{1/2}.$$

où U est la matrice dont les colonnes sont les coordonnées des vecteurs $\boldsymbol{\lambda}_i$ dans la base canonique de $\mathbb{Z}^n$. Si $d = n$ alors $\det(\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_n)$ est la valeur absolue du déterminant classique.

Soit Λ un sous-groupe de $\mathbb{Z}^n$ de dimension d et soit $\{\mathbf{u}_1, \cdots, \mathbf{u}_d\}$ une base de Λ. On définit le *déterminant* de Λ par :

$$\det(\Lambda) = \det(\mathbf{u}_1, \cdots, \mathbf{u}_d).$$

Si Λ est primitif alors on a $\det(\Lambda^\perp) = \det(\Lambda)$.

Constante d'Hermite

Soit d un entier positif non nul. *La constante d'Hermite* de dimension d est définie par :

$$\gamma_d = \sup_{\dim \Lambda = d} \left(\frac{\lambda_1(\Lambda)^2}{\det(\Lambda)^{2/d}} \right).$$

D'après [35, p.15], la valeur exacte de γ_d est connue seulement pour $r \leqslant 8$ et $r = 24$.

d	1	2	3	4	5	6	7	8	24
γ_d^d	1	4/3	2	4	8	64/3	64	2^8	4^{24}

Tableau 1.1 – Constantes d'Hermite

Toutefois, pour tout entier d, on a la majoration suivante [35, p.17] :

$$\gamma_d \leqslant 1 + \frac{d}{4}.$$

Le Second Théorème de Minkowski donne une majoration des minima successifs d'un sous-groupe de $\mathbb{Z}^n$.

Théorème 1.4.1. *[44, Theorem 16](Second Théorème de Minkowski) Soit Λ un sous-groupe de $\mathbb{Z}^n$ de dimension d. Si $1 \leqslant r \leqslant d$ alors on a :*

$$\left(\prod_{i=1}^{r} \lambda_i(\Lambda)\right)^{1/r} \leqslant \sqrt{\gamma_d}\,\det(\Lambda)^{1/d}.$$

Constante de Rankin

En 1953, R. Rankin [38] a introduit une généralisation de la constante d'Hermite. Soit Λ un sous-groupe de $\mathbb{Z}^n$ de dimension d. Soit $1 \leqslant r \leqslant d$, *l'invariant de Rankin* de Λ, noté $\gamma_{d,r}(\Lambda)$, est défini par :

$$\gamma_{d,r}(\Lambda) = \inf_{\substack{\boldsymbol{\lambda}_1,\cdots,\boldsymbol{\lambda}_r \in \Lambda \\ \det(\boldsymbol{\lambda}_1,\cdots,\boldsymbol{\lambda}_r)\neq 0}} \left(\frac{\det(\boldsymbol{\lambda}_1,\cdots,\boldsymbol{\lambda}_r)}{\det(\Lambda)^{r/d}}\right)^2 = \inf_{\substack{L \text{ sous-groupe de } \Lambda \\ \dim(L)=r}} \left(\frac{\det(L)}{\det(\Lambda)^{r/d}}\right)^2.$$

En considérant une famille de vecteurs linéairement indépendants atteignant simultanément tous les minima et en utilisant le Théorème 1.4.1, on obtient :

$$\gamma_{d,r}(\Lambda) \leqslant \left(\frac{\prod_{i=1}^{r} \lambda_i(\Lambda)}{\det(\Lambda)^{r/d}}\right)^2 \leqslant \gamma_d^r.$$

Ainsi, *la constante de Rankin*, notée par $\gamma_{d,r}$, est bien définie :

$$\gamma_{d,r} = \sup_{\dim \Lambda = d} \gamma_{d,r}(\Lambda),$$

où Λ parcourt les sous-groupes de $\mathbb{Z}^n$ de dimension d. De plus, on a $\gamma_{d,r} \leqslant \gamma_d^r$.

Étant donné un vecteur $\mathbf{a} \in \mathbb{Z}^n$, le lemme suivant permet de construire un sous-groupe saturé de $\mathbb{Z}^n$ de dimension 2, contenant $\mathbf{a}$ et de déterminant contrôlé par $\|\mathbf{a}\|_2^{(n-2)/(n-1)}$.

Lemme 1.4.2. *Soit $\mathbf{a} \in \mathbb{Z}^n$ un vecteur non nul. Alors il existe deux vecteurs linéairement indépendants $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}^n$ tels que $\langle \mathbf{u}_1, \mathbf{u}_2 \rangle$ est saturé, contient $\mathbf{a}$ et vérifie :*

$$\gamma_2^{-1}\|\mathbf{u}_1\|_2\|\mathbf{u}_2\|_2 \leqslant \det(\mathbf{u}_1, \mathbf{u}_2) \leqslant \gamma_{n-1}^{1/2}\|\mathbf{a}\|_2^{(n-2)/(n-1)}.$$

Démonstration. Remarquons que $\mathbf{a}^\perp$ est de dimension $n-1$ et $\det(\mathbf{a}^\perp) \leqslant \|\mathbf{a}\|_2$ (avec égalité si $\mathbf{a}$ est primitif). Par définition, il existe un sous-groupe Λ de $\mathbf{a}^\perp$ de dimension $n-2$ tel que

$$\det(\Lambda) = \sqrt{\gamma_{n-1,n-2}(\mathbf{a}^\perp)}\det(\mathbf{a}^\perp)^{(n-2)/(n-1)}.$$

Par minimalité, Λ est saturé. D'après [35, p.18], on a :

$$\gamma_{n-1,n-2}(\mathbf{a}^\perp) \leqslant \gamma_{n-1,n-2} = \gamma_{n-1,1} = \gamma_{n-1}.$$

Par suite, on obtient :

$$\det(\Lambda) \leqslant \sqrt{\gamma_{n-1}}\|\mathbf{a}\|_2^{(n-2)/(n-1)}.$$

Soit $\{\mathbf{u}_1, \mathbf{u}_2\}$ une base réduite de $\Lambda^\perp$ au sens de Lagrange [35, Definition 17, p.22]. On a :

$$\det(\mathbf{u}_1, \mathbf{u}_2) = \det(\Lambda^\perp) = \det(\Lambda).$$

Ainsi, on en déduit la deuxième inégalité :

$$\det(\mathbf{u}_1, \mathbf{u}_2) \leqslant \gamma_{n-1}^{1/2}\|\mathbf{a}\|_2^{(n-2)/(n-1)}.$$

Comme $\{\mathbf{u}_1, \mathbf{u}_2\}$ est une base réduite de $\Lambda^\perp$, d'après [35, Theorem 7, p.22], on a $\lambda_1(\Lambda^\perp) = \|\mathbf{u}_1\|_2$ et $\lambda_2(\Lambda^\perp) = \|\mathbf{u}_2\|_2$. D'après le Théorème 1.4.1, on a la première inégalité :

$$\|\mathbf{u}_1\|_2\|\mathbf{u}_2\|_2 \leqslant \gamma_2 \det(\mathbf{u}_1, \mathbf{u}_2).$$

□

1.5 Géométrie convexe

Cette section contient les notions de *polytope de Newton* et *polynôme de facette* d'un polynôme. Soient $n \geqslant m > 0$ deux entiers. Soit $0 \neq F \in \mathbb{C}[\mathbf{x}^{\pm 1}]$. On écrit

$$F(\mathbf{x}) = \sum_{\boldsymbol{\lambda} \in \mathrm{Supp}(F)} f_{\boldsymbol{\lambda}} \mathbf{x}^{\boldsymbol{\lambda}},$$

où les $f_{\boldsymbol{\lambda}}$ sont les coefficients non nuls de F correspondants à $\boldsymbol{\lambda} \in \mathrm{Supp}(F)$. Soit $\mathcal{L}$ une application linéaire de $\mathbb{Z}^n$ sur $\mathbb{Z}^m$. On munit $\mathbb{Z}^m$ d'un ordre total (ordre lexicographique). On définit :

$$\mathrm{d}(F) = \sup_{\boldsymbol{\lambda} \in \mathrm{Supp}(F)} \mathcal{L}(\boldsymbol{\lambda}) \quad \text{et} \quad F_{\mathcal{L}}(\mathbf{x}) = \sum_{\boldsymbol{\lambda} \in \mathrm{Supp}(F) | \mathcal{L}(\boldsymbol{\lambda}) = \mathrm{d}(F)} f_{\boldsymbol{\lambda}} \mathbf{x}^{\boldsymbol{\lambda}}.$$

Le polynôme $F_{\mathcal{L}}$ est appelé le *polynôme de facette* de F suivant $\mathcal{L}$. Le lemme suivant généralise la propriété selon laquelle le degré d'un produit de polynômes à une variable est la somme des degrés et que le coefficient dominant du produit est égal au produit des coefficients dominants.

Lemme 1.5.1. *Soient $F, G \in \mathbb{C}[\mathbf{x}^{\pm 1}]$ deux polynômes non nuls. Alors on a :*

$$\mathrm{d}(FG) = \mathrm{d}(F) + \mathrm{d}(G) \quad \textit{et} \quad (FG)_{\mathcal{L}} = F_{\mathcal{L}} G_{\mathcal{L}}.$$

En particulier, si F divise G alors $F_{\mathcal{L}}$ divise $G_{\mathcal{L}}$.

Démonstration. On écrit :

$$F(\mathbf{x}) = \sum_{\boldsymbol{\lambda}\in \mathrm{Supp}(F)} f_{\boldsymbol{\lambda}}\mathbf{x}^{\boldsymbol{\lambda}} \quad \text{et} \quad G(\mathbf{x}) = \sum_{\boldsymbol{\lambda}\in \mathrm{Supp}(G)} g_{\boldsymbol{\lambda}}\mathbf{x}^{\boldsymbol{\lambda}},$$

où les $f_{\boldsymbol{\lambda}}$ et $g_{\boldsymbol{\lambda}}$ sont les coefficients non nuls de F et G correspondants à $\boldsymbol{\lambda}$.

Comme $F_{\mathcal{L}}$ et $G_{\mathcal{L}}$ sont non nuls, on a $F_{\mathcal{L}}G_{\mathcal{L}} \neq 0$ et donc $\mathrm{Supp}(F_{\mathcal{L}}G_{\mathcal{L}}) \neq \emptyset$. Par définition de $F_{\mathcal{L}}$ et $G_{\mathcal{L}}$, on a $\mathcal{L}(\boldsymbol{\lambda}) = \mathrm{d}(F) + \mathrm{d}(G)$ pour tout $\boldsymbol{\lambda} \in \mathrm{Supp}(F_{\mathcal{L}}G_{\mathcal{L}})$. Donc on a :

$$\mathrm{d}(F_{\mathcal{L}}G_{\mathcal{L}}) = \mathrm{d}(F) + \mathrm{d}(G).$$

On considère les polynômes :

$$F_{\overline{\mathcal{L}}}(\mathbf{x}) = \sum_{\boldsymbol{\lambda}\in \mathrm{Supp}(F)\mid \mathcal{L}(\boldsymbol{\lambda})\neq \mathrm{d}(F)} f_{\boldsymbol{\lambda}}\mathbf{x}^{\boldsymbol{\lambda}} \quad \text{et} \quad G_{\overline{\mathcal{L}}}(\mathbf{x}) = \sum_{\boldsymbol{\lambda}\in \mathrm{Supp}(G)\mid \mathcal{L}(\boldsymbol{\lambda})\neq \mathrm{d}(G)} g_{\boldsymbol{\lambda}}\mathbf{x}^{\boldsymbol{\lambda}}.$$

On peut alors écrire :

$$F = F_{\mathcal{L}} + F_{\overline{\mathcal{L}}} \quad \text{et} \quad G = G_{\mathcal{L}} + G_{\overline{\mathcal{L}}}.$$

On a donc :

$$FG = F_{\mathcal{L}}G_{\mathcal{L}} + F_{\mathcal{L}}G_{\overline{\mathcal{L}}} + F_{\overline{\mathcal{L}}}G_{\mathcal{L}} + F_{\overline{\mathcal{L}}}G_{\overline{\mathcal{L}}}.$$

On remarque que l'on a $\mathrm{d}(F_{\mathcal{L}}) = \mathrm{d}(F)$ et $\mathrm{d}(F_{\overline{\mathcal{L}}}) < \mathrm{d}(F)$. On a des inégalités similaires pour G. Comme $\mathrm{Supp}(F_{\mathcal{L}}G_{\overline{\mathcal{L}}}) \subseteq \mathrm{Supp}(F_{\mathcal{L}}) + \mathrm{Supp}(G_{\overline{\mathcal{L}}})$ et $\mathcal{L}$ est linéaire, on a :

$$\mathrm{d}(F_{\mathcal{L}}G_{\overline{\mathcal{L}}}) \leqslant \mathrm{d}(F_{\mathcal{L}}) + \mathrm{d}(G_{\overline{\mathcal{L}}}) < \mathrm{d}(F) + \mathrm{d}(G).$$

Similairement, on a :

$$\mathrm{d}(F_{\overline{\mathcal{L}}}G_{\mathcal{L}}) < \mathrm{d}(F) + \mathrm{d}(G)$$
$$\mathrm{d}(F_{\overline{\mathcal{L}}}G_{\overline{\mathcal{L}}}) < \mathrm{d}(F) + \mathrm{d}(G).$$

Ainsi, on en déduit que $(FG)_{\mathcal{L}} = F_{\mathcal{L}}G_{\mathcal{L}}$ et $\mathrm{d}(FG) = \mathrm{d}(F) + \mathrm{d}(G)$. La dernière propriété s'ensuit facilement. □

Si $0 \neq F \in \mathbb{C}[\mathbf{x}^{\pm 1}]$ alors le *polytope de Newton* de F, noté $\mathrm{Newt}(F)$, est défini comme l'enveloppe convexe de $\mathrm{Supp}(F)$. On rappelle le résultat suivant, connu sous le nom de Théorème d'Ostrowski [36].

Théorème 1.5.2. *(Théorème d'Ostrowski) Soient $F, G \in \mathbb{C}[\mathbf{x}^{\pm 1}]$ deux polynômes non nuls. Alors on a $Newt(FG) = Newt(F) + Newt(G)$.*

1.6 Hauteurs et Théorèmes de Bézout

On fixe un entier $n \geqslant 1$. Dans la sous-section 1.6.1, on rappelle deux définitions de hauteurs des points de $\mathbb{G}_{\mathrm{m}}^n$. Dans la sous-section 1.6.2, on rappelle la définition de hauteur d'une variété, notamment celle d'une hypersurface et ainsi que le Théorème de Bézout Arithmétique établi par P. Philippon [37, III]. On y rappelle également le Théorème de Bézout Géométrique.

1.6.1 Hauteurs d'un point de $\mathbb{G}_{\mathrm{m}}^n$

On commence avec la notion de hauteurs dans l'espace projectif $\mathbb{P}^n$. Soit $\boldsymbol{\alpha} = (\alpha_0 : \alpha_1 : \cdots : \alpha_n) \in \mathbb{P}^n$. On rappelle que $\mathbb{Q}(\boldsymbol{\alpha})$ est le corps de définition de $\boldsymbol{\alpha}$. On définit :

— *la hauteur de Weil* de $\boldsymbol{\alpha}$ par :

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

où la somme est sur les places finies et infinies de $\mathbb{Q}(\boldsymbol{\alpha})$, $n_v = [\mathbb{Q}(\boldsymbol{\alpha})_v : \mathbb{Q}_v]$ est le degré local et

$$|\boldsymbol{\alpha}|_v = \max(|\alpha_0|_v, \ldots, |\alpha_n|_v).$$

— *la hauteur "ℓ_2"* de $\boldsymbol{\alpha}$ par :

$$h_2(\boldsymbol{\alpha}) = \frac{1}{[\mathbb{Q}(\boldsymbol{\alpha}) : \mathbb{Q}]} \sum_v n_v \log \|\boldsymbol{\alpha}\|_v$$

où cette fois-ci

$$\|\boldsymbol{\alpha}\|_v = \begin{cases} \max(|\alpha_0|_v, \ldots, |\alpha_n|_v) & , \text{ si } v \nmid \infty \\ (|\alpha_0|_v^2 + \cdots + |\alpha_n|_v^2)^{1/2} & , \text{ si } v \mid \infty. \end{cases}$$

Par la formule du produit, ces deux hauteurs sont indépendantes du choix des coordonnées et elles sont positives. On a les relations suivantes entre ces deux hauteurs :

Lemme 1.6.1.1. *Soit $\boldsymbol{\alpha} \in \mathbb{P}^n$. On a :*

$$h(\boldsymbol{\alpha}) \leqslant h_2(\boldsymbol{\alpha}) \leqslant h(\boldsymbol{\alpha}) + \frac{1}{2}\log(n+1).$$

Démonstration. Ces inégalités se déduisent en comparant les termes locaux dans leurs définitions et en remarquant, de plus, que $\sum_{v \in M_{\mathbb{Q}(\boldsymbol{\alpha})}^{\infty}} n_v = [\mathbb{Q}(\boldsymbol{\alpha}) : \mathbb{Q}]$ pour la deuxième inégalité. □

On rappelle le plongement $\iota_n : \mathbb{G}_{\mathrm{m}}^n \hookrightarrow \mathbb{P}^n$ défini par $\iota_n(\alpha_1, \cdots, \alpha_n) = (1 : \alpha_1 : \cdots : \alpha_n)$. Ce morphisme induit une hauteur $h_{\iota_n} : \mathbb{G}_{\mathrm{m}}^n(\overline{\mathbb{Q}}) \to \mathbb{R}_+$ en posant $h_{\iota_n}(\boldsymbol{\alpha}) = h(\iota_n(\boldsymbol{\alpha}))$. Pour simplifier la notation, on note simplement $h(\boldsymbol{\alpha})$ la hauteur de Weil de $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$.

On mentionne également une autre définition de la hauteur. Si $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ alors on peut définir :

$$h_1(\boldsymbol{\alpha}) = \sum_{i=1}^n h(\alpha_i).$$

Cette définition correspond en effet au plongement $\varphi_n : \mathbb{G}_{\mathrm{m}}^n \hookrightarrow \mathbb{P}^1 \times \cdots \times \mathbb{P}^1$ défini par $\varphi_n(\alpha_1, \cdots, \alpha_n) = ((1 : \alpha_1), \cdots, (1 : \alpha_n))$. On a la relation entre $h(\boldsymbol{\alpha})$ et $h_1(\boldsymbol{\alpha})$ suivante :

Lemme 1.6.1.2. *Soit $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$. On a :*

$$h(\boldsymbol{\alpha}) \leqslant h_1(\boldsymbol{\alpha}).$$

Démonstration. On pose $\mathbb{K} = \mathbb{Q}(\boldsymbol{\alpha})$. Soit $M_{\mathbb{K}}$ l'ensemble des places de $\mathbb{K}$ de telle sorte que pour tout $\alpha \in \mathbb{K}^{\times}$, on ait la formule du produit :

$$\prod_{v \in M_{\mathbb{K}}} |\alpha|_v^{n_v} = 1,$$

où n_v est le degré local en v. Il suffit de remarquer que pour tout $v \in M_{\mathbb{K}}$, on a : :

$$\max(1, |\alpha_1|_v, \cdots, |\alpha_n|_v) \leqslant \max(1, |\alpha_1|_v) \cdots \max(1, |\alpha_n|_v).$$

Par suite, on a $h(\boldsymbol{\alpha}) \leqslant h(\alpha_1) + \cdots + h(\alpha_n)$. □

Enfin, on énonce le lemme suivant qui donne des relations entre $h(\xi)$ et $h(\boldsymbol{\zeta}\xi^{\mathbf{a}})$ où $\boldsymbol{\zeta} \in \boldsymbol{\mu}_{\infty}$.

Lemme 1.6.1.3. *Soient* $\mathbf{a} \in \mathbb{Z}^n$, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_{\infty}^n$ *et* $\xi \in \overline{\mathbb{Q}}^*$. *On pose* $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$. *On a les relations suivantes :*

$$\|\mathbf{a}\|_{\infty} h(\xi) \leqslant h(\boldsymbol{\alpha}) \leqslant 2\|\mathbf{a}\|_{\infty} h(\xi).$$

Démonstration. On pose :

$$\mathbf{a}_+ = (\max(a_1, 0), \cdots, \max(a_n, 0)) \quad \text{et} \quad \mathbf{a}_- = (-\min(a_1, 0), \cdots, -\min(a_n, 0)).$$

Soit v une place de $\mathbb{Q}(\boldsymbol{\alpha})$. On a alors $|\zeta_i \xi|_v = |\xi|_v$ et par suite :

$$\max\left(1, |\xi|_v^{\|\mathbf{a}_+\|_{\infty}}\right) \leqslant \max(1, |\zeta_1\xi|_v^{a_1}, \cdots, |\zeta_n\xi|_v^{a_n})$$

et

$$\max\left(1, |\xi^{-1}|_v^{\|\mathbf{a}_-\|_{\infty}}\right) \leqslant \max(1, |\zeta_1\xi|_v^{a_1}, \cdots, |\zeta_n\xi|_v^{a_n}).$$

En prenant le logarithme et en faisant la somme sur v, on en déduit que $\|\mathbf{a}_+\|_{\infty} h(\xi) \leqslant h(\boldsymbol{\alpha})$ et $\|\mathbf{a}_-\|_{\infty} h(\xi^{-1}) \leqslant h(\boldsymbol{\alpha})$. Comme $h(\xi^{-1}) = h(\xi)$, on a la première inégalité.

Soit $i \in \{1, \cdots, n\}$ et soit v une place de $\mathbb{Q}(\boldsymbol{\alpha})$. On a :

$$\max(1, |\zeta_i\xi|_v^{a_i}) = \max(1, |\xi|_v^{a_i}) \leqslant \max\left(\max(1, |\xi|_v^{\|\mathbf{a}_+\|_{\infty}}), \max(1, |\xi^{-1}|_v^{\|\mathbf{a}_-\|_{\infty}})\right).$$

On a alors :

$$\max(1, |\zeta_1\xi|_v^{a_1}, \cdots |\zeta_n\xi|_v^{a_n}) \leqslant \max\left(\max(1, |\xi|_v^{\|\mathbf{a}_+\|_{\infty}}), \max(1, |\xi^{-1}|_v^{\|\mathbf{a}_-\|_{\infty}})\right),$$

et par conséquent :

$$\log\max(1, |\zeta_1\xi|_v^{a_1}, \cdots |\zeta_n\xi|_v^{a_n}) \leqslant \log\max(1, |\xi|_v^{\|\mathbf{a}_+\|_{\infty}}) + \log\max(1, |\xi^{-1}|_v^{\|\mathbf{a}_-\|_{\infty}}).$$

En faisant la somme sur v, on en déduit que $h(\boldsymbol{\alpha}) \leqslant \|\mathbf{a}_+\|_{\infty} h(\xi) + \|\mathbf{a}_-\|_{\infty} h(\xi^{-1})$. Comme $h(\xi^{-1}) = h(\xi)$, on déduit la deuxième inégalité. □

1.6.2 Hauteurs d'une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ et Théorèmes de Bézout

Soit V une sous-variété de $\mathbb{P}^n$. Soient $Z_1, \cdots, Z_g$ les composantes irréductibles de V, où $g \geqslant 1$ un entier. On dit que V est de dimension pure si toutes les Z_i ont la même dimension. Dans ce cas, on a $\deg(V) = \sum_{i=1}^{g} \deg(Z_i)$ (voir [18, Chapitre III, 2.2]). En général, on a seulement l'inégalité $\deg(V) \leqslant \sum_{i=1}^{g} \deg(Z_i)$. Les variétés irréductibles et les hypersurfaces sont de dimension pure. On a besoin du Théorème de Bézout (Géométrique) sous la forme suivante :

Théorème 1.6.2.1. *(Théorème de Bézout Géométrique) Soit $s \geqslant 2$ un entier. Soient $V_1, \cdots, V_s$ des variétés de dimension pure dans $\mathbb{P}^n$. Soient $g \geqslant 1$ un entier et $Z_1, \cdots, Z_g$ les composantes irréductibles de $V_1 \cap \cdots \cap V_s$. Alors on a :*

$$\sum_{i=1}^{g} \deg(Z_i) \leqslant \prod_{j=1}^{s} \deg(V_j).$$

Démonstration. Voir Proposition dans la page 10 de [24]. □

L'analogue pour la hauteur de ce théorème est appelé Théorème de Bézout Arithmétique. Soit V une sous-variété irréductible de $\mathbb{P}^n$. La hauteur projective de V, notée $h_{\mathbb{P}^n}(V)$, est celle définie par Philippon dans [37, III]. Par exemple, si $V = \{\boldsymbol{\alpha}\}$ alors la hauteur de $\boldsymbol{\alpha}$ en tant que variété de $\mathbb{P}^n$ est la hauteur $h_2(\boldsymbol{\alpha})$. Si V est réductible et si $Z_1, \cdots, Z_g$ sont les composantes irréductibles de V alors on a :

$$h_{\mathbb{P}^n}(V) \leqslant \sum_{i=1}^{g} h_{\mathbb{P}^n}(Z_i).$$

Si V est une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ alors la hauteur de V, notée $h(V)$, est la hauteur de la clôture de Zariski de $\iota_n(V)$ dans $\mathbb{P}^n$.

Le cas d'une hypersurface :

Soit $\mathbb{K}$ un corps de nombres et soit $F \in \mathbb{K}[\mathbf{x}]$. D'après Philippon [37, III], *la hauteur de F*, notée $h(F)$, est définie par :

$$h(F) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v} [\mathbb{K}_v : \mathbb{Q}_v] \log M_v(F) \tag{1.6.1}$$

où v parcourt l'ensemble des places de $\mathbb{K}$ tels que :

— si v est finie alors $M_v(F)$ est le maximum des valeurs absolues v-adique des coefficients de F,
— si v est infinie associée au plongement σ_v de $\mathbb{K}$ dans $\mathbb{C}$ alors

$$\log M_v(F) = \widehat{m}_v(F) + \deg(F) \sum_{i=1}^{n} \frac{1}{2i},$$

où $\widehat{m}_v(F)$ est une variante du logarithme de la mesure de Mahler :

$$\widehat{m}_v(F) = \int_{S_n(1)} \log |\sigma_v(F)| \sigma_n,$$

$S_n(1)$ désignant la sphère unité de $\mathbb{C}^n$ et σ_n la mesure invariante de masse totale 1 sur $S_n(1)$.

Soit V l'hypersurface de $\mathbb{G}_{\mathrm{m}}^n$ définie par $F = 0$. D'après la définition [37, p. 347, III], on a :

$$h(V) = h(F) + \frac{1}{2}\deg(F)\sum_{i=1}^{n-1}\sum_{j=1}^{i}\frac{1}{j}.$$

On appelle *hauteur de Gauss-Mahler* de F, notée $h_{\mathrm{GM}}(F)$, la hauteur logarithmique obtenue en effectuant la somme des logarithmes de la norme de Gauss aux places ultramétriques et de la mesure de Mahler aux places archimédiennes i.e.

$$h_{\mathrm{GM}}(F) = \frac{1}{[\mathbb{K}:\mathbb{Q}]}\sum_{v}[\mathbb{K}_v:\mathbb{Q}_v]\log M_v(F)$$

où v parcourt l'ensemble des places de $\mathbb{K}$ et tels que :

— si v est finie alors $M_v(F)$ est le maximum des valeurs absolues v-adique des coefficients de F,
— si v est infinie associée au plongement σ_v de $\mathbb{K}$ dans $\mathbb{C}$ alors $M_v(F)$ est la mesure de Mahler de $\sigma_v(F)$ (le polynôme dont les coefficients sont les conjugués des coefficients de F par σ_v).

Puisque la hauteur de Gauss-Mahler fait intervenir la mesure de Mahler, elle possède des propriétés plus intéressantes. Par exemple, si $F \in \mathbb{Z}[\mathbf{x}]$ est primitive (i.e. de contenu 1) alors on a $h_{\mathrm{GM}}(F) = \log M(F)$ car il n'y a que la place infinie qui contribue à la hauteur. En utilisant un résultat de P. Lelong [28], on en déduit la proposition suivante qui donne une majoration de la hauteur d'une hypersurface en fonction de la hauteur de Gauss-Mahler. Pour un entier $d \geqslant 1$, on note $\phi(d) = \sum_{i=1}^{d}\sum_{j=1}^{i}\frac{1}{j}$ et on pose $\phi(0) = 0$.

Proposition 1.6.2.2. *Soit $\mathbb{K}$ un corps de nombres et soit $F \in \mathbb{K}[\mathbf{x}^{\pm 1}]$. On note V l'hypersurface de $\mathbb{G}_{\mathrm{m}}^n$ définie par $F = 0$. Alors, on a :*

$$h(V) \leqslant h_{GM}(F) + \frac{1}{2}\deg(F)\phi(n).$$

En particulier, si $F \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$ alors on peut remplacer $h_{GM}(F)$ par $\log M(F)$.

Démonstration. Quitte à remplacer F par son polynôme associé, on peut supposer que $F \in \mathbb{K}[\mathbf{x}]$. Par définition, on a :

$$h(V) = h(F) + \frac{1}{2}\deg(F)\sum_{i=1}^{n-1}\sum_{j=1}^{i}\frac{1}{j}.$$

On va donner une majoration de $h(F)$ en fonction de $h_{\mathrm{GM}}(F)$. Soit v une place infinie associée au plongement σ_v de $\mathbb{K}$ dans $\mathbb{C}$. D'après le Théorème 2 de [28, p. 140], on a :

$$\widehat{m}_v(F) \leqslant \log M(\sigma_v(F)).$$

En remplaçant $\hat{m}_v(F)$ par cette majoration dans la définition (1.6.1) de $h(F)$, on déduit que :

$$h(F) \leqslant h_{\mathrm{GM}}(F) + \frac{1}{2}\deg(F)\sum_{i=1}^{n}\frac{1}{i}.$$

En remplaçant $h(F)$ par cette majoration dans la définition de $h(V)$, on a :

$$h(V) \leqslant h_{\mathrm{GM}}(F) + \frac{1}{2}\deg(F)\sum_{i=1}^{n}\frac{1}{i} + \frac{1}{2}\deg(F)\sum_{i=1}^{n-1}\sum_{j=1}^{i}\frac{1}{j}.$$

En remarquant que

$$\sum_{i=1}^{n-1}\sum_{j=1}^{i}\frac{1}{j}+\sum_{i=1}^{n}\frac{1}{i}=\sum_{i=1}^{n}\sum_{j=1}^{i}\frac{1}{j}=\phi(n),$$

on en déduit la première assertion.

Maintenant supposons que F est à coefficients dans $\mathbb{Z}$. On note C_F le contenu de F. Comme $V(F)=V(F/C_F)$, d'après la première assertion, on a :

$$h(V)\leqslant h_{\mathrm{GM}}(F/C_F)+\frac{1}{2}\deg(F)\phi(n).$$

Or $h_{\mathrm{GM}}(F/C_F)=\log M(F/C_F)\leqslant \log M(F)$ et la dernière assertion s'ensuit. □

La majoration de la Proposition (1.6.2.2) permet de déduire des majorations plus simples (en fonction de la mesure de Mahler) du Théorème de Bézout Arithmétique dû à Philippon ([37, III]) pour l'intersection d'une variété avec une hypersurface. Le Théorème de Bézout Arithmétique, établi par Philippon, est formulé de manière plus générale, mais on va l'énoncer dans le contexte qui nous intéresse (voir aussi [25, Theorem 3]).

Théorème 1.6.2.3. *(Théorème de Bézout Arithmétique) Soit V une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie sur $\overline{\mathbb{Q}}$. Soit $F\in\overline{\mathbb{Q}}[\mathbf{x}^{\pm 1}]$ et soit W l'hypersurface de $\mathbb{G}_{\mathrm{m}}^n$ définie par $F=0$. Soient $g\geqslant$ un entier et $Z_1,\cdots,Z_g$ les composantes irréductibles de $V\cap W$. Alors on a :*

$$\sum_{i=1}^{g}h(Z_i)\leqslant h(V)\deg(F)+h_{GM}(F)\deg(V)+\frac{1}{2}\left(\log(n+1)+\sum_{i=1}^{n}\frac{1}{i}\right)\deg(V)\deg(F).$$

En particulier, si $F\in\mathbb{Z}[\mathbf{x}^{\pm 1}]$ alors on peut remplacer $h_{GM}(F)$ par $\log M(F)$.

Démonstration. Quitte à remplacer F par son polynôme associé, on peut supposer que $F\in\overline{\mathbb{Q}}[\mathbf{x}]$. D'après la Proposition 4 de ([37, III]), on a :

$$\sum_{i=1}^{g}h(Z_i)\leqslant h(V)\deg(F)+h_V(F)\deg(V),$$

où $h_V(F)$ est une quantité majorée par :

$$h_V(F)\leqslant h(W)+\frac{1}{2}\left(\log(n+1)-\phi(n-1)\right)\deg(W).$$

D'après la Proposition (1.6.2.2), on a :

$$h(W)\leqslant h_{\mathrm{GM}}(F)+\frac{1}{2}\deg(F)\phi(n).$$

En combinant ces inégalités, on a :

$$\begin{aligned}\sum_{i=1}^{g}h(Z_i)&\leqslant h(V)\deg(F)+\left(h_{\mathrm{GM}}(F)+\frac{1}{2}\deg(F)\phi(n)+\frac{1}{2}\left(\log(n+1)-\phi(n-1)\right)\deg(F)\right)\deg(V)\\&=h(V)\deg(F)+h_{\mathrm{GM}}(F)\deg(V)+\frac{1}{2}\left(\phi(n)+\log(n+1)-\phi(n-1)\right)\deg(F)\deg(V).\end{aligned}$$

En remarquant que

$$\phi(n) - \phi(n-1) = \sum_{i=1}^{n} \frac{1}{i},$$

on en déduit le résultat requis. □

Comme conséquence du Théorème 1.6.2.3, on obtient une majoration de la hauteur d'une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie par des polynômes $F_i \in \mathbb{Z}[\mathbf{x}^{\pm}]$ en fonction de leur degré et de leur mesure de Mahler. Pour une application plus tard, on va considérer le cas de deux polynômes.

Corollaire 1.6.2.4. *Soient $F_1, F_2 \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$. Soient $g \geqslant 1$ un entier et $Z_1, \cdots, Z_g$ les composantes irréductibles de la sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie par $F_1 = F_2 = 0$. Alors on a :*

$$\sum_{i=1}^{g} h(Z_i) \leqslant \log M(F_1)\deg(F_2) + \log M(F_2)\deg(F_1) + \frac{1}{2}\left(\phi(n) + \log(n+1) + \sum_{i=1}^{n}\frac{1}{i}\right)\deg(F_1)\deg(F_2).$$

Démonstration. On applique le Théorème 1.6.2.3 à $V = V(F_1)$ et $W = V(F_2)$:

$$\sum_{i=1}^{g} h(Z_i) \leqslant h(V)\deg(F_2) + \log M(F_2)\deg(V) + \frac{1}{2}\left(\log(n+1) + \sum_{i=1}^{n}\frac{1}{i}\right)\deg(V)\deg(F_2). \quad (1.6.2)$$

D'après la Proposition 1.6.2.2, on a :

$$h(V) \leqslant \log M(F_1) + \frac{1}{2}\deg(F_1)\phi(n).$$

En rempaçant $h(V)$ par cette majoration dans (1.6.2) et en tenant compte du fait que $\deg(V) = \deg(F_1)$, on obtient :

$$\begin{aligned}\sum_{i=1}^{g} h(Z_i) &\leqslant \left(\log M(F_1) + \frac{1}{2}\deg(F_1)\phi(n)\right)\deg(F_2) + \log M(F_2)\deg(F_1) + \\ &\quad \frac{1}{2}\left(\log(n+1) + \sum_{i=1}^{n}\frac{1}{i}\right)\deg(F_1)\deg(F_2) \\ &= \log M(F_1)\deg(F_2) + \log M(F_2)\deg(F_1) + \frac{1}{2}\left(\phi(n) + \log(n+1) + \sum_{i=1}^{n}\frac{1}{i}\right)\deg(F_1)\deg(F_2).\end{aligned}$$

□

On désigne par $\mathbb{Q}^{\mathrm{ab}}$ l'extension abélienne maximale de $\mathbb{Q}$. D'après le Théorème de Kronecker-Weber, $\mathbb{Q}^{\mathrm{ab}}$ est la réunion de toutes les extensions cyclotomiques de $\mathbb{Q}$.

On va aussi énoncer une variante du Théorème 1.6.2.3 en remplaçant W par une variété définie par des polynômes de la forme $\mathbf{x}^{\mathbf{b}} - \boldsymbol{\zeta}^{\mathbf{b}}$ où $\mathbf{b} \in \mathbb{Z}^n$.

Corollaire 1.6.2.5. *Soit V une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie sur $\mathbb{Q}$. Soit $m > 0$ un entier. Soient $\mathbf{b}_1, \cdots, \mathbf{b}_m \in \mathbb{Z}^n$ et $\boldsymbol{\zeta}_1, \cdots, \boldsymbol{\zeta}_m \in \boldsymbol{\mu}_\infty^n$. On pose $G_i(\mathbf{x}) = \mathbf{x}^{\mathbf{b}_i} - \boldsymbol{\zeta}_i^{\mathbf{b}_i}$ pour $i \in \{1, \cdots, m\}$ et on note W la sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie par $G_1 = \cdots = G_m = 0$. Soient $g \geqslant 1$ un entier et $Z_1, \cdots, Z_g$ les composantes irréductibles de $V \cap W$. Alors on a :*

$$\sum_{i=1}^{g} h(Z_i) \leqslant \left(h(V) + \frac{m}{2} \left(\log(n+1) + \sum_{i=1}^{n} \frac{1}{i} \right) \deg(V) \right) \prod_{i=1}^{m} \deg(G_i)$$

Démonstration. On remarque tout d'abord que l'on a $h_{\mathrm{GM}}(G_i) = 0$. En effet, soit v une place de $\mathbb{Q}^{\mathrm{ab}}$. Si v est finie alors on a $M_v(G_i) = \max(1, |\boldsymbol{\zeta}_i^{\mathbf{b}_i}|_v) = 1$ (car $\boldsymbol{\zeta}_i \in \boldsymbol{\mu}_\infty^n$). Si v est une place infinie associée au plongement de $\mathbb{Q}^{\mathrm{ab}}$ dans $\mathbb{C}$ alors on a :

$$M_v(G_i) = M(\sigma_v(G_i)) = M(G_i(\sigma_v(\boldsymbol{\zeta}_i)\mathbf{x})) = M(\mathbf{x}^{\mathbf{b}_r} - \sigma_v(\boldsymbol{\zeta}_i^{\mathbf{b}_i})).$$

D'après [40, Theorem 42, p. 253], on a $M(\mathbf{x}^{\mathbf{b}_r} - \sigma_v(\boldsymbol{\zeta}_i^{\mathbf{b}_i})) = 1$ et ainsi $M_v(G_i) = 1$.

Montrons maintenant le résultat par récurrence sur m. On note W_m la sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie $G_1 = \cdots = G_m = 0$. On note g_m le nombre des composantes irréductibles de $V \cap W_m$ et $Z_{m,1}, \cdots, Z_{m,g_m}$ ses composantes irréductibles. Si $m = 1$ alors, d'après le Théorème 1.6.2.3, on a :

$$\sum_{i=1}^{g_1} h(Z_{1,i}) \leqslant h(V)\deg(G_1) + \frac{1}{2}\left(\log(n+1) + \sum_{i=1}^{n} \frac{1}{i} \right) \deg(V)\deg(G_1),$$

car $h_{\mathrm{GM}}(G_1) = 0$. Supposons que, jusqu'au rang $m-1$, on a :

$$\sum_{i=1}^{g_{m-1}} h(Z_{m-1,i}) \leqslant \left(h(V) + \frac{(m-1)}{2} \left(\log(n+1) + \sum_{i=1}^{n} \frac{1}{i} \right) \deg(V) \right) \prod_{i=1}^{m-1} \deg(G_i).$$

Au rang m, on note Y l'hypersurface définie par $G_m = 0$. On a alors $V \cap W_m = V \cap W_{m-1} \cap Y$. En appliquant le Théorème 1.6.2.3 à $V \cap W_{m-1} \cap Y$, on a :

$$\sum_{i=1}^{g_m} h(Z_{m,i}) \leqslant h(V \cap W_{m-1})\deg(G_m) + \frac{1}{2}\left(\log(n+1) + \sum_{i=1}^{n} \frac{1}{i} \right) \deg(V \cap W_{m-1})\deg(G_m),$$

car $h_{\mathrm{GM}}(G_m) = 0$. D'après le Théorème 1.6.2.1, on a :

$$\deg(V \cap W_{m-1}) \leqslant \deg(V) \prod_{i=1}^{m-1} \deg(G_i).$$

D'après l'hypothèse de récurrence, on a :

$$\sum_{i=1}^{g_m} h(Z_{m,i}) \leqslant \left(h(V) + \frac{(m-1)}{2} \left(\log(n+1) + \sum_{i=1}^{n} \frac{1}{i} \right) \deg(V) \right) \prod_{i=1}^{m} \deg(G_i) + \frac{1}{2}\left(\log(n+1) + \sum_{i=1}^{n} \frac{1}{i} \right) \deg(V) \prod_{i=1}^{m} \deg(G_i).$$

Par suite, on a :

$$\sum_{i=1}^{g_m} h(Z_{m,i}) \leqslant \left(h(V) + \frac{m}{2} \left(\log(n+1) + \sum_{i=1}^{n} \frac{1}{i} \right) \deg(V) \right) \prod_{i=1}^{m} \deg(G_i).$$

Ainsi, on obtient l'inégalité voulue au rang m. Par le principe de récurrence, on a bien le résultat du corollaire. □

Le corollaire suivant permet de majorer le degré et la hauteur de V en fonction de degré des F_i, leur mesure de Mahler et la codimension de V. On rappelle que $\phi(d) = \sum_{i=1}^{d} \sum_{j=1}^{i} \frac{1}{j}$ pour tout entier $d > 0$ et $\phi(0) = 0$.

Corollaire 1.6.2.6. *Soit $s \geqslant 1$ un entier et soient $F_1, \cdots, F_s \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$. On note V la sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie par $F_1 = \cdots = F_s = 0$ et k sa codimension. Alors on a :*

$$\deg(V) \leqslant D^k \quad \textit{et} \quad h(V) \leqslant \left(\frac{1}{2}\phi(n) + nh\right) D^{k-1} + \frac{n}{2}\phi(n) D^k,$$

où

$$D = \max_{1 \leqslant i \leqslant s} \deg(F_i) \quad \textit{et} \quad h = \max_{1 \leqslant i \leqslant s} \log M(F_i).$$

Démonstration. Pour $i \in \{1, \cdots, s\}$, on note W_i l'hypersurface de $\mathbb{G}_{\mathrm{m}}^n$ définie par $F_i = 0$. En appliquant [37, Corollaire 5, p. 357] (avec $S = \mathbb{P}^n$, $Z_i = W_i$ et $\boldsymbol{\delta} = D$), on obtient :

$$D^d \deg(V) \leqslant \deg(\mathbb{P}^n) D^n.$$

Par suite, on en déduit que $\deg(V) \leqslant D^k$. Par ailleurs, pour la hauteur, on obtient :

$$D^{d+1} h(V) \leqslant h(\mathbb{P}^n) D^n + n \left(\max_{1 \leqslant i \leqslant s} h(W_i)\right) \deg(\mathbb{P}^n) D^n. \tag{1.6.3}$$

D'après la Proposition 1.6.2.2 et en tenant compte que les F_i ont des coefficients dans $\mathbb{Z}$, on a :

$$h(W_i) \leqslant \log M(F_i) + \frac{1}{2} \deg(F_i) \phi(n).$$

En majorant $\log M(F_i)$ par h et $\deg(F_i)$ par D, on a :

$$h(W_i) \leqslant h + \frac{1}{2} D \phi(n).$$

En remplaçant $h(W_i)$ dans (1.6.3) par cette dernière majoration et en tenant compte du fait que $h(\mathbb{P}^n) = \frac{1}{2}\phi(n)$, on obtient :

$$\begin{aligned} h(V) &\leqslant \frac{1}{2}\phi(n) D^{n-d-1} + n\left(h + \frac{1}{2}\phi(n) D\right) D^{n-d-1} \\ &\leqslant \frac{1}{2}\phi(n) D^{k-1} + nh D^{k-1} + \frac{n}{2}\phi(n) D^k. \end{aligned}$$

□

2. Relations de dépendance multiplicative

Ce chapitre vise à étudier l'ensemble des relations de dépendance multiplicative entre des nombres algébriques et utiliser cette notion pour démontrer l'analogue de la Conjecture de Schinzel dans le cas des sous-variétés qui sont des translatés de sous-tores de $\mathbb{G}_{\mathrm{m}}^n$.

Dans la Section 2.1, on introduit les notions de dépendance multiplicative faible et forte. On montre que l'ensemble des relations de dépendance multiplicative faible est le saturé de l'ensemble des relations de dépendance multiplicative forte. Dans la Section 2.2, on applique la notion de relations de dépendance multiplicative faible pour démontrer l'analogue de la Conjecture de Schinzel pour les sous-variétés qui sont des translatés de sous-tores de $\mathbb{G}_{\mathrm{m}}^n$. La Section 2.3 contient un algorithme pour calculer les relations de dépendance multiplicative faible dans le cas des nombres rationnels (pour un nombre quelconque de rationnels) et un exemple d'application à la Conjecture de Schinzel. Dans la Section 2.4, on donne un algorithme pour calculer l'ensemble des relations de dépendance multiplicative faible pour un nombre algébrique, en d'autres termes, qui reconnaît les racines de l'unité. Dans la Section 2.5, on donne un algorithme pour calculer les relations de dépendance multiplicative faible dans le cas de deux nombres algébriques et on en déduit un algorithme pour calculer l'ensemble des relations de dépendance multiplicative faible de n nombres algébriques lorsque celui-ci est codimension au plus 1. On note que c'est ce dernier cas qui est utile pour la Conjecture de Schinzel. Enfin, dans la Section 2.6, on donne une procédure permettant de calculer l'ensemble des relations de dépendance multiplicative forte à partir des relations de dépendance multiplicative faible.

Les différents algorithmes présentés dans cette section sont implémentés en le langage du calcul formel PARI/GP et sont exécutés sur un ordinateur ayant les spécifications suivantes :

— Processeur : ® Core™ i5-8265U CPU @1.60GHz× 8
— RAM : 16GB.

Dans toute la suite, on fixe $n \geqslant 1$ un entier (sauf indication du contraire).

2.1 Relations de dépendance multiplicative faible et forte

Soient $\alpha_1, \cdots, \alpha_n \in \overline{\mathbb{Q}}^*$. On appelle une *relation de dépendance multiplicative faible entre* $\alpha_1, \cdots, \alpha_n$ une relation de la forme :

$$\boldsymbol{\alpha}^{\mathbf{b}} = \mu \quad \text{où} \quad \mathbf{b} \in \mathbb{Z}^n \quad \text{et} \quad \mu \in \boldsymbol{\mu}_\infty.$$

Si, de plus, $\mu = 1$ alors on dit que la relation de dépendance multiplicative entre $\alpha_1, \cdots, \alpha_n$ est *forte*. On dit que $\alpha_1, \cdots, \alpha_n$ sont *multiplicativement indépendants* si aucun vecteur non nul $\mathbf{b} \in \mathbb{Z}^n$ ne satisfait $\boldsymbol{\alpha}^{\mathbf{b}} \in \boldsymbol{\mu}_\infty$.

On note $R_f(\boldsymbol{\alpha})$ (respectivement $R_F(\boldsymbol{\alpha})$) l'ensemble des vecteurs $\mathbf{b} \in \mathbb{Z}^n$ vérifiant une relation de dépendance multiplicative faible (respectivement forte) entre $\alpha_1, \cdots, \alpha_n$. Ces deux ensembles sont des sous-groupes de $\mathbb{Z}^n$ et de plus, $R_F(\boldsymbol{\alpha}) \subseteq R_f(\boldsymbol{\alpha})$. Le lemme suivant montre que $R_f(\boldsymbol{\alpha}) = R_F^{\mathrm{sat}}(\boldsymbol{\alpha})$.

Lemme 2.1.1. *Soit $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$. Alors $R_f(\boldsymbol{\alpha})$ est saturé et $R_F^{\mathrm{sat}}(\boldsymbol{\alpha}) = R_f(\boldsymbol{\alpha})$.*

Démonstration. Montrons que $R_f(\boldsymbol{\alpha})$ est saturé. Soit $\mathbf{b} \in \mathbb{Z}^n$ et $m \in \mathbb{N}$ tels que $m\mathbf{b} = (mb_1, \cdots, mb_n) \in R_f(\boldsymbol{\alpha})$. Il existe donc $\mu \in \boldsymbol{\mu}_\infty$ tel que $\boldsymbol{\alpha}^{m\mathbf{b}} = \mu$. On a alors $(\boldsymbol{\alpha}^{\mathbf{b}})^m = \mu$ et donc $\boldsymbol{\alpha}^{\mathbf{b}} \in \boldsymbol{\mu}_\infty$. Par suite, $R_f(\boldsymbol{\alpha})$ est saturé.

Montrons que $R_f(\boldsymbol{\alpha})$ est le saturé de $R_F(\boldsymbol{\alpha})$. Il est évident que $R_F(\boldsymbol{\alpha}) \subseteq R_f(\boldsymbol{\alpha})$. Soit d la dimension de $R_f(\boldsymbol{\alpha})$ et soient $\{\mathbf{b}_1, \cdots, \mathbf{b}_d\}$ une $\mathbb{Z}$-base de $R_f(\boldsymbol{\alpha})$. Pour $i \in \{1, \cdots, d\}$, on note $\mu_i = \boldsymbol{\alpha}^{\mathbf{b}_i} \in \boldsymbol{\mu}_\infty$ et d_i l'ordre de μ_i. Soit N le plus petit commun multiple des d_i et soit B la matrice associée à $\{\mathbf{b}_1, \cdots, \mathbf{b}_d\}$ (i.e. les colonnes de B sont les coordonnées des $\mathbf{b}_i$ exprimés dans la base canonique de $\mathbb{Z}^n$). On a alors $\boldsymbol{\alpha}^{NB} = \mathbf{1}$ et donc $NR_f(\boldsymbol{\alpha}) \subseteq R_F(\boldsymbol{\alpha})$. On obtient ainsi les relations $NR_f(\boldsymbol{\alpha}) \subseteq R_F(\boldsymbol{\alpha}) \subseteq R_f(\boldsymbol{\alpha})$. Comme $R_f(\boldsymbol{\alpha})$ est saturé, on en déduit que $R_F^{\mathrm{sat}}(\boldsymbol{\alpha}) = R_f(\boldsymbol{\alpha})$. □

D'après ce lemme, on peut déduire $R_f(\boldsymbol{\alpha})$ à partir de $R_F(\boldsymbol{\alpha})$. En effet, on peut calculer le saturé de $R_F(\boldsymbol{\alpha})$ à l'aide de l'Algorithme 15. Réciproquement, on peut également déduire $R_F(\boldsymbol{\alpha})$ à partir de $R_f(\boldsymbol{\alpha})$ comme on verra plus tard (voir Algorithme 9). On va alors s'intéresser aux relations de dépendance multiplicative faible.

Lemme 2.1.2. *Soit $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$. On note $d = \dim R_f(\boldsymbol{\alpha})$. Soit $A \in M_{n-d,n}(\mathbb{Z})$ la matrice dont les lignes forment une base de $R_f(\boldsymbol{\alpha})^\perp$. Alors il existe $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ et $\boldsymbol{\xi} \in \mathbb{G}_{\mathrm{m}}^{n-d}$ tels que $\boldsymbol{\alpha} = \boldsymbol{\zeta}\boldsymbol{\xi}^A$ et $\mathbb{Q}(\boldsymbol{\zeta}, \boldsymbol{\xi}) = \mathbb{Q}(\boldsymbol{\alpha})$. De plus, on a $R_f(\boldsymbol{\xi}) = \{\mathbf{0}\}$ i.e. $\xi_1, \cdots, \xi_{n-d}$ sont multiplicativement indépendants.*

Démonstration. Soit $\{\mathbf{b}_1, \cdots, \mathbf{b}_d\}$ une $\mathbb{Z}$-base de $R_f(\boldsymbol{\alpha})$. Pour $i \in \{1, \cdots, d\}$, on note $\mu_i = \boldsymbol{\alpha}^{\mathbf{b}_i} \in \boldsymbol{\mu}_\infty$ et d_i l'ordre de μ_i. Soit N le plus petit commun multiple des d_i et soit B la matrice associée à $\{\mathbf{b}_1, \cdots, \mathbf{b}_d\}$. On a alors $\boldsymbol{\alpha}^{NB} = \mathbf{1}$ et donc $\boldsymbol{\alpha}^N = (\alpha_1^N, \cdots, \alpha_n^N)$ appartient au sous-groupe algébrique $H_{R_f(\boldsymbol{\alpha})}$ défini par $R_f(\boldsymbol{\alpha})$. Comme $R_f(\boldsymbol{\alpha})$ est saturé, $H_{R_f(\boldsymbol{\alpha})}$ est un sous-tore de $\mathbb{G}_{\mathrm{m}}^n$. D'après la Proposition 1.3.2.1, il existe $\boldsymbol{\zeta}' \in \boldsymbol{\mu}_\infty^n$ et $\boldsymbol{\xi}' \in \mathbb{G}_{\mathrm{m}}^d$ tels que $\boldsymbol{\alpha}^N = \boldsymbol{\zeta}'\boldsymbol{\xi}'^A$. Soit $\boldsymbol{\xi}'' \in \mathbb{G}_{\mathrm{m}}^{n-d}$ tel que $\boldsymbol{\xi}''^N = \boldsymbol{\xi}'$. On a alors $\boldsymbol{\alpha} = \boldsymbol{\zeta}''\boldsymbol{\xi}''^A \in H_{R_f(\boldsymbol{\alpha})}$ où $\boldsymbol{\zeta}'' \in \boldsymbol{\mu}_\infty^n$. De nouveau, d'après la Proposition 1.3.2.1, il existe $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ et $\boldsymbol{\xi} \in \mathbb{G}_{\mathrm{m}}^{n-d}$ tels que $\boldsymbol{\alpha} = \boldsymbol{\zeta}\boldsymbol{\xi}^A$ et $\mathbb{Q}(\boldsymbol{\zeta}, \boldsymbol{\xi}) = \mathbb{Q}(\boldsymbol{\alpha})$.

Soit $r = \dim R_f(\boldsymbol{\xi})$. Il reste à montrer $R_f(\boldsymbol{\xi}) = \{\mathbf{0}\}$ i.e. $r = 0$. Soit $\tilde{A} \in M_{n-d-r,n-d}(\mathbb{Z})$ la matrice dont les lignes forment une base de $R_f(\boldsymbol{\xi})^\perp$. En appliquant le résultat précédent à $\boldsymbol{\xi} \in \mathbb{G}_{\mathrm{m}}^{n-d}$, il existe $\tilde{\boldsymbol{\zeta}} \in \boldsymbol{\mu}_\infty^{n-d}$ et $\tilde{\boldsymbol{\xi}} \in \mathbb{G}_{\mathrm{m}}^{n-d-r}$ tels que $\boldsymbol{\xi} = \tilde{\boldsymbol{\zeta}}\tilde{\boldsymbol{\xi}}^{\tilde{A}}$. On a alors $\boldsymbol{\alpha} = \boldsymbol{\zeta}\tilde{\boldsymbol{\zeta}}^A\tilde{\boldsymbol{\xi}}^{\tilde{A}A}$. On a alors $(\tilde{A}A)^\perp \subseteq R_f(\boldsymbol{\alpha})$. Comme la matrice $\tilde{A}A$ est de rang au plus $n-d-r$, on a $d + r \leqslant d$. Cela implique $r = 0$. □

2.2 Conjecture de Schinzel pour les translatés de sous-tores

On s'intéresse ici à une version analogue du Théorème 2 dans le cas où la variété $V(F, G)$ est remplacée par un translaté $\boldsymbol{\beta}T$ de sous-tore de $\mathbb{G}_{\mathrm{m}}^n$. Pour cela, on considère le problème suivant :

Soit $\boldsymbol{\beta}T$ un translaté de sous-tore de $\mathbb{G}_{\mathrm{m}}^n$. Pour quelles valeurs de $\mathbf{a} \in \mathbb{Z}^n$, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ et $\xi \in \mathbb{G}_{\mathrm{m}} \setminus \boldsymbol{\mu}_\infty$, a-t-on $\boldsymbol{\zeta}\xi^{\mathbf{a}} \in \boldsymbol{\beta}T$?

Grâce à la Proposition 1.3.2.1, cette question peut être reformulée comme suit : étant donné $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$ et $\Lambda \subseteq \mathbb{Z}^n$ un sous-groupe primitif de rang d, existe-il $(\boldsymbol{\gamma}, \xi, \boldsymbol{\zeta}, \mathbf{a}) \in \mathbb{G}_{\mathrm{m}}^d \times \mathbb{G}_{\mathrm{m}} \times \boldsymbol{\mu}_\infty^n \times \mathbb{Z}^n$ tel que $\xi \notin \boldsymbol{\mu}_\infty$ vérifiant :

$$\boldsymbol{\beta}\boldsymbol{\gamma}^\Delta = \boldsymbol{\zeta}\xi^{\mathbf{a}} \tag{2.2.1}$$

où $\Delta \in M_{d,n}(\mathbb{Z})$ est la matrice dont les lignes forment une base de Λ ?

On montre facilement que $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp \subseteq \mathbf{a}^\perp$ est une condition nécessaire. En particulier, dans ce cas, tous les vecteurs $\mathbf{b} \in R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$ satisfont les propriétés requises du Théorème 2 i.e. que $\mathbf{b}$ est orthogonal à $\mathbf{a}$ et ne dépend que de $\boldsymbol{\beta}$ et T.

On va ainsi donner une condition nécessaire et suffisante pour l'équation (2.2.1) ait une solution (Proposition 2.2.2). On commence par le lemme suivant.

Lemme 2.2.1. *Soient $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$, $\Lambda \subseteq \mathbb{Z}^n$ un sous-groupe saturé de rang d et $\mathbf{a} \in \mathbb{Z}^n$. On définit la propriété suivante :*

$$R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = \mathbf{a}^\perp \cap \Lambda^\perp. \tag{2.2.2}$$

(1) Si la propriété (2.2.2) est satisfaite alors on a $n-d-1 \leqslant \dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) \leqslant n-d$.

(2) Si $\dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) = n-d-1$ alors la propriété (2.2.2) est satisfaite si et seulement si $\mathbf{a} \in (R_f(\boldsymbol{\beta})^\perp + \Lambda)^{\mathrm{sat}} \setminus \Lambda$. Dans ce cas, on a $\Lambda \not\subseteq R_f(\boldsymbol{\beta})$.

(3) Si $\dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) = n-d$ alors la propriété (2.2.2) est satisfaite si et seulement si $\mathbf{a} \in \Lambda$. Dans ce cas, on a $\Lambda \subseteq R_f(\boldsymbol{\beta})$.

Démonstration. (1) On a $\dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) \leqslant \dim(\Lambda^\perp) = n-d$. Par ailleurs, on a :

$$\dim(\mathbf{a}^\perp \cap \Lambda^\perp) = \dim \mathbf{a}^\perp + \dim \Lambda^\perp - \dim(\mathbf{a}^\perp + \Lambda^\perp) \geqslant \dim \mathbf{a}^\perp + \dim \Lambda^\perp - n \geqslant n-d-1.$$

Ainsi, si on a $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = \mathbf{a}^\perp \cap \Lambda^\perp$ alors on a $n-d-1 \leqslant \dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) \leqslant n-d$.

(2) Supposons que $\dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) = n-d-1$. Supposons que la propriété (2.2.2) est satisfaite. Dans ce cas, on a $\dim(\mathbf{a}^\perp \cap \Lambda^\perp) = \dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) = n-d-1$ et donc $\mathbf{a} \notin \Lambda$. D'après la relation $\mathbf{a}^\perp \cap \Lambda^\perp = R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$, on en déduit que $\mathbf{a} \in (R_f(\boldsymbol{\beta})^\perp + \Lambda)^{\mathrm{sat}}$. Réciproquement, supposons que $\mathbf{a} \in (R_f(\boldsymbol{\beta})^\perp + \Lambda)^{\mathrm{sat}} \setminus \Lambda$. Comme $\mathbf{a} \notin \Lambda$, $\dim(\mathbf{a}^\perp \cap \Lambda^\perp) = n-d-1$. Puisque $\mathbf{a} \in (R_f(\boldsymbol{\beta})^\perp + \Lambda)^{\mathrm{sat}}$, on a aussi $(\mathbb{Z}\mathbf{a} + \Lambda)^{\mathrm{sat}} \subseteq (R_f(\boldsymbol{\beta})^\perp + \Lambda)^{\mathrm{sat}}$. En passant à l'orthogonal, on a $(R_f(\boldsymbol{\beta})^\perp + \Lambda)^\perp \subseteq (\mathbb{Z}\mathbf{a} + \Lambda)^\perp$. Cela est équivalent à $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp \subseteq \mathbf{a}^\perp \cap \Lambda^\perp$. Puisque $R_f(\boldsymbol{\beta}), \mathbf{a}^\perp$ et $\Lambda^\perp$ sont saturés, alors il est en de même pour leur intersection. Enfin, comme $\dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) = n-d-1 = \dim(\mathbf{a}^\perp \cap \Lambda^\perp)$, on a l'égalité $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = \mathbf{a}^\perp \cap \Lambda^\perp$.

(3) Supposons que $\dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) = n-d$. Si la propriété (2.2.2) est satisfaite alors on a $\dim(\mathbf{a}^\perp \cap \Lambda^\perp) = \dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) = n-d = \dim(\Lambda^\perp)$ et donc $\mathbf{a} \in \Lambda^{\mathrm{sat}} = \Lambda$. Réciproquement, si $\mathbf{a} \in \Lambda$ alors on a $\mathbf{a}^\perp \cap \Lambda^\perp = \Lambda^\perp$. Puisque $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp \subseteq \Lambda^\perp$ est de dimension $n-d$, on a $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = \Lambda^\perp$. □

On donne maintenant une réponse à la question (2.2.1) précédente.

Proposition 2.2.2. *Soient $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$ et $\Lambda \subseteq \mathbb{Z}^n$ un sous-groupe primitif de rang d. On note $\Delta \in M_{d,n}(\mathbb{Z})$ la matrice dont les lignes forment une base de Λ. Alors (2.2.1) possède une solution $(\boldsymbol{\gamma}, \xi, \boldsymbol{\zeta}, \mathbf{a}) \in \mathbb{G}_{\mathrm{m}}^d \times \mathbb{G}_{\mathrm{m}} \times \boldsymbol{\mu}_\infty^n \times \mathbb{Z}^n$ telle que $0 \neq \xi \notin \boldsymbol{\mu}_\infty$ si et seulement si $\mathbf{a}^\perp \cap \Lambda^\perp = R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$.*

Démonstration. Supposons qu'il existe un quadruplet $(\boldsymbol{\gamma}, \xi, \boldsymbol{\zeta}, \mathbf{a}) \in \mathbb{G}_{\mathrm{m}}^d \times \mathbb{G}_{\mathrm{m}} \times \boldsymbol{\mu}_\infty^n \times \mathbb{Z}^n$ tels que $0 \neq \xi \notin \boldsymbol{\mu}_\infty$ et vérifiant (2.2.1). Montrons que $\mathbf{a}^\perp \cap \Lambda^\perp = R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$. Soit $\mathbf{b} \in \mathbb{Z}^n$ un vecteur (colonne). En mettant (2.2.1) à la puissance $\mathbf{b}$, on a :

$$\boldsymbol{\beta}^{\mathbf{b}} \boldsymbol{\gamma}^{\Delta \mathbf{b}} = \boldsymbol{\zeta}^{\mathbf{b}} \xi^{\mathbf{a}\mathbf{b}}. \tag{2.2.3}$$

Si $\mathbf{b} \in \mathbf{a}^\perp \cap \Lambda^\perp$ alors on obtient $\boldsymbol{\beta}^{\mathbf{b}} = \boldsymbol{\zeta}^{\mathbf{b}}$. Comme $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty$, on a $\boldsymbol{\beta}^{\mathbf{b}} \in \boldsymbol{\mu}_\infty$ et donc $\mathbf{b} \in R_f(\boldsymbol{\beta})$. Ainsi, on a l'inclusion $\mathbf{a}^\perp \cap \Lambda^\perp \subseteq R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$. Inversement, si $\mathbf{b} \in R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$ alors, d'après (2.2.3), on obtient cette fois-ci $\boldsymbol{\beta}^{\mathbf{b}} = \boldsymbol{\zeta}^{\mathbf{b}} \xi^{\mathbf{a}\mathbf{b}}$ car $\mathbf{b} \in \Lambda^\perp$. Comme $\mathbf{b} \in R_f(\boldsymbol{\beta})$, on a $\boldsymbol{\beta}^{\mathbf{b}} \in \boldsymbol{\mu}_\infty$ et par suite, on a

$\xi^{\mathbf{ab}} = \boldsymbol{\beta}^{\mathbf{b}}\boldsymbol{\zeta}^{-\mathbf{b}} \in \boldsymbol{\mu}_\infty$. Puisque $\xi \notin \boldsymbol{\mu}_\infty$, on en déduit que $\mathbf{ab} = 0$ et donc $\mathbf{b} \in \mathbf{a}^\perp$. Ainsi, on a aussi l'autre inclusion $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp \subseteq \mathbf{a}^\perp \cap \Lambda^\perp$.

Réciproquement, soit $\mathbf{a} \in \mathbb{Z}^n$ tel que $\mathbf{a}^\perp \cap \Lambda^\perp = R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$. D'après le Lemme 2.2.1, on a $n-d-1 \leqslant \dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) \leqslant n-d$. On considère ainsi les deux cas suivants.

1er cas : $\dim R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = n-d-1$.

Soit $\{\mathbf{b}_1, \cdots, \mathbf{b}_{n-d-1}\}$ une base de $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$. Comme $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$ est saturé dans $\Lambda^\perp$, il existe un vecteur $\mathbf{b}_{n-d} \in \mathbb{Z}^n$ tels que $\{\mathbf{b}_1, \cdots, \mathbf{b}_{n-d}\}$ soit une base de $\Lambda^\perp$. Comme $\Lambda^\perp$ est saturé dans $\mathbb{Z}^n$, il existe des vecteurs $\mathbf{b}_{n-d+1}, \cdots, \mathbf{b}_n \in \mathbb{Z}^n$ tel que $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ soit une base de $\mathbb{Z}^n$. Notons B la matrice dont les colonnes sont les vecteurs $\mathbf{b}_1, \cdots, \mathbf{b}_n$. En mettant l'équation (2.2.1) à la puissance B qui est inversible, on en déduit que cette équation est équivalente au système :

$$\begin{cases} \boldsymbol{\beta}^{\mathbf{b}_1} = \boldsymbol{\zeta}^{\mathbf{b}_1} \\ \vdots \\ \boldsymbol{\beta}^{\mathbf{b}_{n-d-1}} = \boldsymbol{\zeta}^{\mathbf{b}_{n-d-1}} \\ \boldsymbol{\beta}^{\mathbf{b}_{n-d}} = \boldsymbol{\zeta}^{\mathbf{b}_{n-d}} \xi^{\mathbf{ab}_{n-d}} \\ \boldsymbol{\beta}^{\mathbf{b}_{n-d+1}} \boldsymbol{\gamma}^{\Delta\mathbf{b}_{n-d+1}} = \boldsymbol{\zeta}^{\mathbf{b}_{n-d+1}} \xi^{\mathbf{ab}_{n-d+1}} \\ \vdots \\ \boldsymbol{\beta}^{\mathbf{b}_n} \boldsymbol{\gamma}^{\Delta\mathbf{b}_n} = \boldsymbol{\zeta}^{\mathbf{b}_n} \xi^{\mathbf{ab}_n}, \end{cases}$$

en utilisant le fait que $\mathbf{b}_1, \cdots, \mathbf{b}_{n-d} \in \Lambda^\perp$ et $\mathbf{b}_1, \cdots, \mathbf{b}_{n-d-1} \in R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = \mathbf{a}^\perp \cap \Lambda^\perp$. Comme $\mathbf{b}_1, \cdots, \mathbf{b}_{n-d-1} \in R_f(\boldsymbol{\beta})$, on a $(\boldsymbol{\beta}^{\mathbf{b}_1}, \cdots, \boldsymbol{\beta}^{\mathbf{b}_{n-d-1}}) \in \boldsymbol{\mu}_\infty^{n-d-1}$. Comme $\mathbf{b}_1, \cdots, \mathbf{b}_{n-d-1}$ sont linéairement indépendants (sur $\mathbb{R}$), on peut donc trouver $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ satisfaisant les $n-d-1$ premières équations. On fixe un tel $\boldsymbol{\zeta}$. À la $n-d$-ième équation, on a $\mathbf{ab}_{n-d} \neq 0$ (sinon on aurait $\mathbf{b}_{n-d} \in \mathbf{a}^\perp \cap \Lambda^\perp = R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$ et $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$ serait de dimension $n-d$). On en déduit donc qu'il existe $\xi \in \mathbb{G}_{\mathrm{m}}$ tel que $\xi^{\mathbf{ab}_{n-d}} = \boldsymbol{\beta}^{\mathbf{b}_{n-d}}\boldsymbol{\zeta}^{-\mathbf{b}_{n-d}}$. Par suite, $\xi \notin \boldsymbol{\mu}_\infty$ sinon $\mathbf{b}_{n-d} \in R_f(\boldsymbol{\beta})$ et $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$ serait de dimension $n-d$. Pour $n-d+1 \leqslant i \leqslant n$, on a $\Delta\mathbf{b}_i \neq 0$. Par construction des $\mathbf{b}_{n-d+1}, \cdots, \mathbf{b}_n$, les vecteurs $\Delta\mathbf{b}_{n-d+1}, \cdots, \Delta\mathbf{b}_n$ sont linéairement indépendants sur $\mathbb{R}$. Ainsi il existe $\boldsymbol{\gamma} \in \mathbb{G}_{\mathrm{m}}^d$ satisfaisant les d dernières équations. Donc l'équation (2.2.1) a une solution $(\boldsymbol{\gamma}, \xi, \boldsymbol{\zeta}, \mathbf{a})$ avec $\xi \notin \boldsymbol{\mu}_\infty$.

2ème cas : $\dim R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = n-d$.

Dans ce cas, on a $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = \Lambda^\perp$. D'après le Lemme 2.2.1, on a $\mathbf{a} \in \Lambda$. Soit $\{\mathbf{b}_1, \cdots, \mathbf{b}_{n-d}\}$ une base de $\Lambda^\perp$. Comme $\Lambda^\perp$ est saturé dans $\mathbb{Z}^n$, il existe des vecteurs $\mathbf{b}_{n-d+1}, \cdots, \mathbf{b}_n \in \mathbb{Z}^n$ tels que $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ soit une base de $\mathbb{Z}^n$. Notons encore B la matrice dont les colonnes sont les vecteurs $\mathbf{b}_1, \cdots, \mathbf{b}_n$. En mettant l'équation (2.2.1) à la puissance B qui est inversible, on en déduit que l'équation (2.2.1) est équivalente au système :

$$\begin{cases} \boldsymbol{\beta}^{\mathbf{b}_1} = \boldsymbol{\zeta}^{\mathbf{b}_1} \\ \vdots \\ \boldsymbol{\beta}^{\mathbf{b}_{n-d}} = \boldsymbol{\zeta}^{\mathbf{b}_{n-d}} \\ \boldsymbol{\beta}^{\mathbf{b}_{n-d+1}} \boldsymbol{\gamma}^{\Delta\mathbf{b}_{n-d+1}} = \boldsymbol{\zeta}^{\mathbf{b}_{n-d+1}} \xi^{\mathbf{ab}_{n-d+1}} \\ \vdots \\ \boldsymbol{\beta}^{\mathbf{b}_n} \boldsymbol{\gamma}^{\Delta\mathbf{b}_n} = \boldsymbol{\zeta}^{\mathbf{b}_n} \xi^{\mathbf{ab}_n}, \end{cases}$$

en utilisant le fait que $\mathbf{b}_1, \cdots, \mathbf{b}_{n-d} \in R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = \mathbf{a}^\perp \cap \Lambda^\perp$. On a $(\boldsymbol{\beta}^{\mathbf{b}_1}, \cdots, \boldsymbol{\beta}^{\mathbf{b}_{n-d}}) \in \boldsymbol{\mu}_\infty^{n-d}$ car

$\mathbf{b}_1, \cdots, \mathbf{b}_{n-d} \in R_f(\boldsymbol{\beta})$. Comme $\mathbf{b}_1, \cdots, \mathbf{b}_{n-d}$ sont linéairement indépendants sur $\mathbb{R}$, on peut trouver $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ satisfaisant les $n-d$ premières équations. On fixe un tel $\boldsymbol{\zeta}$. On choisit $\xi \in \mathbb{G}_{\mathrm{m}} \setminus \boldsymbol{\mu}_\infty$ arbitrairement. De nouveau, par construction des $\mathbf{b}_{n-d+1}, \cdots, \mathbf{b}_n$, les vecteurs $\Delta\mathbf{b}_{n-d+1}, \cdots, \Delta\mathbf{b}_n$ sont linéairement indépendants sur $\mathbb{R}$. Cela permet de trouver un $\boldsymbol{\gamma} \in \mathbb{G}_{\mathrm{m}}^d$ satisfaisant les d dernières équations. Donc (2.2.1) possède une solution $(\boldsymbol{\gamma}, \xi, \boldsymbol{\zeta}, \mathbf{a})$ avec $\xi \notin \boldsymbol{\mu}_\infty$. □

On va présenter ensuite une autre reformulation de la proposition précédente en utilisant la notion de dépendance multiplicative. Soit $m > 0$ un entier. Si $A \in M_{n,m}(\mathbb{Z})$ et E un ensemble de vecteurs (colonnes) de $\mathbb{Z}^m$ alors on note AE l'ensemble des vecteurs de la forme $A\boldsymbol{\lambda}$ dans $\mathbb{Z}^n$ où $\boldsymbol{\lambda}$ parcourt E.

Corollaire 2.2.3. *Soient $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$ et $\Lambda \subseteq \mathbb{Z}^n$ un sous-groupe saturé de rang d. On note $\Delta \in M_{d,n}(\mathbb{Z})$ la matrice dont les lignes forment une base de Λ et $K \in M_{n,n-d}(\mathbb{Z})$ le noyau à droite de Δ. Alors (2.2.1) possède une solution $(\boldsymbol{\gamma}, \xi, \boldsymbol{\zeta}, \mathbf{a}) \in \mathbb{G}_{\mathrm{m}}^d \times \mathbb{G}_{\mathrm{m}} \times \boldsymbol{\mu}_\infty^n \times \mathbb{Z}^n$ telle que $\xi \notin \boldsymbol{\mu}_\infty$ si et seulement si $\operatorname{codim} R_f(\boldsymbol{\beta}^K) \leqslant 1$ dans $\mathbb{Z}^{n-d}$. Dans ce cas, on a $KR_f(\boldsymbol{\beta}^K) = \mathbf{a}^\perp \cap \Lambda^\perp$.*

Démonstration. Remarquons d'abord que l'on a :

$$R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = KR_f(\boldsymbol{\beta}^K). \tag{2.2.4}$$

En effet, on a :

$$\mathbf{b} \in R_f(\boldsymbol{\beta}) \cap \Lambda^\perp \iff \begin{cases} \mathbf{b} = K\boldsymbol{\lambda} \text{ où } \boldsymbol{\lambda} \in \mathbb{Z}^{n-d} \\ \boldsymbol{\beta}^{K\boldsymbol{\lambda}} \in \boldsymbol{\mu}_\infty \end{cases} \iff \begin{cases} \mathbf{b} = K\boldsymbol{\lambda} \text{ où } \boldsymbol{\lambda} \in \mathbb{Z}^{n-d} \\ \boldsymbol{\lambda} \in R_f(\boldsymbol{\beta}^K) \end{cases} \iff \mathbf{b} \in KR_f(\boldsymbol{\beta}^K).$$

De plus, comme K est de rang $n-d$, on a :

$$\dim(KR_f(\boldsymbol{\beta}^K)) = \dim R_f(\boldsymbol{\beta}^K). \tag{2.2.5}$$

Supposons que $(\boldsymbol{\gamma}, \xi, \boldsymbol{\zeta}, \mathbf{a}) \in \mathbb{G}_{\mathrm{m}}^d \times \mathbb{G}_{\mathrm{m}} \times \boldsymbol{\mu}_\infty^n \times \mathbb{Z}^n$ telle que $\xi \notin \boldsymbol{\mu}_\infty$ est une solution de (2.2.1). D'après la Proposition 2.2.2, on a $\mathbf{a}^\perp \cap \Lambda^\perp = R_f(\boldsymbol{\beta}) \cap \Lambda^\perp$. D'après l'assertion $(\mathbf{1})$ du Lemme 2.2.1, on a $n-d-1 \leqslant \dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) \leqslant n-d$. D'après (2.2.4) et (2.2.5), on a $\dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) = \dim KR_f(\boldsymbol{\beta}^K) = \dim R_f(\boldsymbol{\beta}^K)$ et donc :

$$n-d-1 \leqslant \dim R_f(\boldsymbol{\beta}^K) \leqslant n-d.$$

Réciproquement, supposons que $\operatorname{codim} R_f(\boldsymbol{\beta}^K) \leqslant 1$. D'après (2.2.4) et (2.2.5), on a :

$$n-d-1 \leqslant \dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) \leqslant n-d.$$

Si $\dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) = n-d$ alors, en choisissant $\mathbf{a} \in \Lambda$, d'après l'assertion $(\mathbf{3})$ du Lemme 2.2.1, on a $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = \mathbf{a}^\perp \cap \Lambda^\perp$. D'après la Proposition 2.2.2, (2.2.1) possède une solution $(\boldsymbol{\gamma}, \xi, \boldsymbol{\zeta}, \mathbf{a}) \in \mathbb{G}_{\mathrm{m}}^d \times \mathbb{G}_{\mathrm{m}} \times \boldsymbol{\mu}_\infty^n \times \mathbb{Z}^n$ telle que $\xi \notin \boldsymbol{\mu}_\infty$.

Supposons que $\dim(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp) = n-d-1$. Puisque $\Lambda^\perp$ est de dimension $n-d$, on a $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp \neq \Lambda^\perp$. En passant à l'orthogonal, $(R_f(\boldsymbol{\beta}) \cap \Lambda^\perp)^\perp \setminus \Lambda = (R_f(\boldsymbol{\beta})^\perp + \Lambda)^{\mathrm{sat}} \setminus \Lambda$ est non vide. En choisissant $\mathbf{a} \in (R_f(\boldsymbol{\beta})^\perp + \Lambda)^{\mathrm{sat}} \setminus \Lambda$, d'après l'assertion $(\mathbf{2})$ du Lemme 2.2.1, on a $R_f(\boldsymbol{\beta}) \cap \Lambda^\perp = \mathbf{a}^\perp \cap \Lambda^\perp$ et on conclut de nouveau par la Proposition 2.2.2.

La dernière assertion suit directement de la Proposition 2.2.2 et en tenant compte de (2.2.4). □

Remarque. On va donner dans la section suivante un exemple (Exemple 2.3.2) pour illustrer une application de ce corollaire à la Conjecture de Schinzel.

2.3 Relations de dépendance multiplicative faible sur $\mathbb{Q}^*$

Soient $\alpha_1, \cdots, \alpha_n \in \mathbb{Q}^*$. L'algorithme suivant permet de trouver une base de $R_f(\boldsymbol{\alpha})$. Cet algorithme repose sur la factorisation des entiers en produits de nombres premiers entre eux.

Algorithme 1 : Relations de dépendance multiplicative faible sur $\mathbb{Q}^*$

Entrée : $\alpha_1, \cdots, \alpha_n \in \mathbb{Q}^*$.

Sortie : Une base de $R_f(\boldsymbol{\alpha})$.

1 Si $|\alpha_1| = \cdots = |\alpha_n| = 1$ alors renvoyer $\{I_n\}$.

2 Écrire les $|\alpha_i|$ en produits de nombres $p_1, \cdots, p_r \neq 1$ premiers entre eux :

$$|\alpha_i| = \mathbf{p}^{\mathbf{u}_i} \text{ où } \mathbf{u}_i \in \mathbb{Z}^r$$

3 Noter $U \in M_{r,n}(\mathbb{Z})$ la matrice dont la i-ème colonne est le vecteur $\mathbf{u}_i$ et calculer B une base du noyau entier (à droite) de U.

4 Renvoyer B.

Remarque. À l'étape 2, on peut utiliser l'Algorithme de Bernstein [8] pour décomposer les $|\alpha_i|$ en produit de nombres premiers entre eux en temps *« essentiellement »* linéaire. Pour notre implémentation, on utilise une autre version qui est plus simple à implémenter mais dont la complexité n'est plus linéaire mais quadratique et effectue au plus $O(\log(\max_i |\alpha_i|)^2)$ opérations élémentaires [6].

Proposition 2.3.1. *L'Algorithme 1 est correct.*

Démonstration. Si $|\alpha_1| = \cdots = |\alpha_n| = 1$ alors c'est trivial. Supposons donc qu'il existe $i \in \{1, \cdots, n\}$ tel que $|\alpha_i| \neq 1$. Dans ce cas, $r \geqslant 1$. Par suite, on a $|\boldsymbol{\alpha}| = \mathbf{p}^U$ et donc :

$$\mathbf{b} \in R_f(\boldsymbol{\alpha}) \iff \boldsymbol{\alpha}^{\mathbf{b}} = \pm 1 \iff \mathbf{p}^{U\mathbf{b}} = 1 \iff U\mathbf{b} = 0 \iff \mathbf{b} \in \ker U.$$

D'où le résultat. □

Remarque. L'algorithme de Bernstein peut être adapté au cas des nombres algébriques en utilisant la décomposition en idéaux premiers entre eux. Cependant, cette opération s'avère coûteuse, en particulier pour le calcul de la base de l'anneau des entiers qui nécessite la factorisation du discriminant [16, Algorithm 6.1.8, p. 305]. En outre, une telle décomposition ne donne pas directement une relation de dépendance multiplicative faible sur $\overline{\mathbb{Q}}^*$ à cause du fait que les idéaux sont définis à des unités près. Pour remédier à cela, on va décrire un algorithme plus efficace mais s'applique seulement au cas de deux nombres algébriques.

Exemple 2.3.2. On va appliquer le Corollaire 2.2.3 pour trouver explicitement un vecteur non nul $\mathbf{b} \in \mathbb{Z}^n$ satisfaisant la Conjecture de Schinzel dans le cas où la sous-variété considérée est un translaté de sous-tore de $\mathbb{G}_{\mathrm{m}}^n$. On se place dans le cas $n = 5$ et $d = 3$. On considère :

$$\boldsymbol{\beta} = (2^4 3^3 5^0, 2^3 3^2 5^0, 2^0 3^4 5^4, 2^2 3^1 5^2, 2^0 3^3 5^4) = (432, 72, 50625, 300, 16875).$$

En appliquant l'Algorithme 1, on trouve une base B de $R_f(\boldsymbol{\beta})$:

$$B = \begin{pmatrix} 14 & 3 \\ -20 & -4 \\ -1 & -1 \\ 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

On considère ensuite le sous-groupe $\Lambda \subseteq \mathbb{Z}^5$ dont les lignes de la matrice Δ suivante forment une base :

$$\Delta = \begin{pmatrix} 2 & 1 & 0 & -4 & 3 \\ 3 & 2 & -2 & -2 & -5 \\ -1 & 0 & -8 & 3 & 3 \end{pmatrix}.$$

Le noyau K à droite de Δ est :

$$K = \begin{pmatrix} 9 & 14 \\ 5 & -20 \\ 3 & -1 \\ 8 & 2 \\ 3 & 0 \end{pmatrix}.$$

On considère donc le translaté de sous-tore $\boldsymbol{\beta}T$ de $\mathbb{G}_{\mathrm{m}}^5$ où T est paramétré par :

$$T = \left\{ \boldsymbol{\gamma}^{\Delta}, \boldsymbol{\gamma} \in \mathbb{G}_{\mathrm{m}}^3 \right\}.$$

Soient maintenant $\mathbf{a} \in \mathbb{Z}^n$, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty$ et $\xi \in \mathbb{G}_{\mathrm{m}} \setminus \boldsymbol{\mu}_\infty$ comme dans les hypothèses du Théorème 2. Si $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}} \in \boldsymbol{\beta}T$ alors, d'après le Corollaire 2.2.3, on a $\operatorname{codim}(R_f(\boldsymbol{\beta}^K)) \leqslant 1$ et $KR_f(\boldsymbol{\beta}^K) \subseteq \mathbf{a}^{\perp}$. Or on a :

$$\boldsymbol{\beta}^K = (2^{67}3^{66}5^{40}, 1) \in \mathbb{G}_{\mathrm{m}}^2$$

et donc

$$R_f(\boldsymbol{\beta}^K) = \left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle \quad \text{et} \quad KR_f(\boldsymbol{\beta}^K) = \left\langle \begin{pmatrix} 14 \\ -20 \\ -1 \\ 2 \\ 0 \end{pmatrix} \right\rangle.$$

Ainsi, on peut donc prendre $\mathbf{b} = \begin{pmatrix} 14 \\ -20 \\ -1 \\ 2 \\ 0 \end{pmatrix} \in \mathbf{a}^{\perp}$.

Cet exemple montre qu'il est intéressant de savoir calculer l'ensemble des relations de dépendance multiplicative faible entre des nombres algébriques, au moins dans le cas où sa codimension est au plus 1 (Algorithme 7).

2.4 Relations de dépendance multiplicative d'un nombre algébrique

Avant de chercher l'ensemble des relations dépendance multiplicative faible sur $\mathbb{G}_{\mathrm{m}}^n$, il faut une procédure permettant de reconnaître une racine de l'unité. Cela revient à calculer $R_f(\alpha)$ pour $\alpha \in \mathbb{G}_{\mathrm{m}}$.

La première procédure ci-après (Algorithme 2) permet de trouver un multiple de l'ordre du groupe de torsion d'un corps de nombres. En utilisant cette procédure, on donnera un algorithme (Algorithme 3) qui permet de vérifier si un nombre algébrique donné est une racine de l'unité.

Algorithme 2 : Multiple de l'ordre du groupe de torsion d'un corps de nombres

Entrée : Un polynôme irréductible $P \in \mathbb{Z}[x]$ définissant un corps $\mathbb{K} = \mathbb{Q}[x]/P$.

Sortie : Un entier strictement positif N tel que $\boldsymbol{\mu}_{\mathbb{K}} \subseteq \boldsymbol{\mu}_N$.

1 Noter d, a_d et a_0 le degré, le coefficient dominant et le coefficient constant de P.
2 Si d est impair ou $a_0 a_d < 0$ ou $a_d P(1) < 0$ ou $a_d P(-1) < 0$ alors renvoyer 2.
3 Calculer la liste D des diviseurs de d et l'ensemble $\mathcal{P} = \{p \in \mathbb{N} \mid p \text{ premier et } p-1 \in D\}$.
4 Renvoyer $N = \prod_{p \in \mathcal{P}} p^{v_p(d)+1}$.

Proposition 2.4.1. *L'Algorithme 2 est correct.*

Démonstration. Si $n \in \mathbb{N}^*$ alors on note ζ_n une racine n-ième de l'unité et $\varphi(n)$ la fonction indicatrice d'Euler. Remarquons qu'on a toujours $\zeta_1, \zeta_2 \in \boldsymbol{\mu}_{\mathbb{K}}$.

Soient d, a_d et a_0 les entiers définis à l'étape 1. Si d est impair ou $a_0 a_d < 0$ ou $a_d P(1) < 0$ ou $a_d P(-1) < 0$ alors P a une racine réelle. Cela implique qu'il existe un plongement réel $\sigma : \mathbb{K} \hookrightarrow \mathbb{R}$ et donc $\boldsymbol{\mu}_{\mathbb{K}} \subseteq \boldsymbol{\mu}_{\mathbb{R}}$. Cela implique $\boldsymbol{\mu}_{\mathbb{K}} = \{\pm 1\}$ et ainsi, l'algorithme termine et renvoie 2 à l'étape 2.

Soit $n \in \mathbb{N}^*$ tel que $\zeta_n \in \mathbb{K}$. On écrit $n = \prod_p p^{e_p}$ où p parcourt l'ensemble des nombres premiers. En particulier, on a $\zeta_{p^{e_p}} \in \mathbb{K}$ et donc $[\mathbb{Q}(\zeta_{p^{e_p}}) : \mathbb{Q}]$ divise $[\mathbb{K} : \mathbb{Q}]$ i.e. $\varphi(p^{e_p}) = (p-1)p^{e_p - 1}$ divise d. En particulier, on a $p - 1 \mid d$ et $e_p - 1 \leqslant v_p(d)$. Ainsi, l'entier N défini à l'étape 4 est un multiple de n et donc $\zeta_n^N = 1$. □

Remarque. On pourrait aussi utiliser le fait que le discriminant $\mathbb{Q}(\zeta_p^{e_p})$ divise celui de $\mathbb{K}$. Cette stratégie aurait permis d'obtenir une estimation plus précise de N, mais le calcul du discriminant demeure une opération coûteuse.

La procédure suivante permet de vérifier si un nombre algébrique est une racine de l'unité.

Algorithme 3 : Racine de l'unité

Entrée : Un polynôme irréductible $P \in \mathbb{Z}[x]$, $\alpha \in \mathbb{K} = \mathbb{Q}[x]/P$ et un entier N tel que $\boldsymbol{\mu}_{\mathbb{K}} \subseteq \boldsymbol{\mu}_N$.

Sortie : 1 si $\alpha \in \boldsymbol{\mu}_{\mathbb{K}}$ et 0 sinon.

1 Si $\alpha = \pm 1$ alors renvoyer 1.
2 Si $N = 2$ alors renvoyer 0.
3 Si $\alpha^2 + 1 \in \{0, \pm\alpha\}$ alors renvoyer 1.
4 Si $N \leqslant 6$ alors renvoyer 0.
5 Noter A le relevé de α^2 dans $\mathbb{Q}[x]$ tel que $\deg(A) < \deg(P)$.
6 Choisir aléatoirement un nombre premier p tel que p ne divise pas le contenu de $P - P(0)$ et p ne divise pas le dénominateur de A.
7 Noter $\bar{P}$ l'image de P dans $\mathbb{F}_p[x]$ et $\bar{A}$ la réduction de A dans $\mathbb{F}_p[x]/\bar{P}$.
8 Si $\bar{A}^{N/2} \neq 1$ alors renvoyer 0.
9 Si $(\alpha^2)^{N/2} = 1$ dans $\mathbb{K}$ alors renvoyer 1.
10 Renvoyer 0.

Remarques. (**1**) Il est fréquent qu'un corps de nombres $\mathbb{K}$ ne contienne que les deux points de torsion -1 et 1. Dans ce cas, l'algorithme s'arrête à l'étape 2 et est particulièrement rapide. Le cas où $\boldsymbol{\mu}_{\mathbb{K}} = \boldsymbol{\mu}_4$ ou $\boldsymbol{\mu}_{\mathbb{K}} = \boldsymbol{\mu}_6$ est déterminé par l'algorithme à l'étape 3 ou l'étape 4.

(**2**) Il suffit de calculer α^2 une seule fois tout au long de l'algorithme.

(**3**) On peut utiliser l'Algorithme 2 pour calculer un entier N vérifiant $\boldsymbol{\mu}_{\mathbb{K}} \subseteq \boldsymbol{\mu}_N$ si celui-ci n'a pas été donné dans l'entrée.

Proposition 2.4.2. *L'Algorithme 3 est correct.*

Démonstration. Les étapes 1 et 2 sont triviales. L'étape 3 consiste à vérifier si α est égal à ζ_4, ζ_3 ou ζ_6. Comme $\boldsymbol{\mu}_{\mathbb{K}} \subseteq \boldsymbol{\mu}_N$, N est pair. Ainsi, si $N \leqslant 6$ alors $N \in \{2, 4, 6\}$. Le cas $N = 2$ est déterminé à l'étape 2 et les deux autres cas sont déterminés à l'étape 4.

Puisque $\alpha^2 \in \mathbb{K}$, A est le polynôme vérifiant $\alpha^2 = A(\xi)$ où $P(\xi) = 0$ et $\deg(A) < \deg(P)$. Soit p un nombre premier vérifiant les deux conditions de l'étape 6. La première condition implique que le polynôme $P(X)$ n'est pas constant modulo p et donc $\mathbb{F}_p[x]/\bar{P} \neq \mathbb{F}_p[x]$. La deuxième condition implique que $\bar{A}$ est bien défini dans $\mathbb{F}_p[x]/\bar{P}$.

Si $\alpha^N = 1$ alors on a $\bar{A}^{N/2} = 1$ (ainsi l'algorithme termine à l'étape 8) et $(\alpha^2)^{N/2} = 1$ (et donc l'algorithme termine à l'étape 9). □

Remarque. Une autre méthode pour déterminer si un nombre algébrique α est une racine de l'unité consiste à calculer sa mesure de Mahler. En effet, on a $\alpha \in \boldsymbol{\mu}_\infty$ si et seulement si $M(\alpha) = 1$. Toutefois, comme le calcul des racines du polynôme minimal de α dans $\mathbb{C}$ implique l'utilisation de valeurs approchées, il est préférable de ne pas s'en servir, d'où la nécessité de l'Algorithme 3.

2.5 Relations de dépendance multiplicative faible entre deux nombres algébriques

Soit $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^2$. Afin de donner l'algorithme qui calcule une base de $R_f(\boldsymbol{\alpha})$ (Algorithme 6), on a besoin de quelques procédures préliminaires.

On souhaite établir un algorithme permettant de vérifier si $\boldsymbol{\alpha}^{\mathbf{b}} \in \boldsymbol{\mu}_\infty$ pour un vecteur $\mathbf{b} \in \mathbb{Z}^2$ donné. Une méthode simple consiste à calculer directement $\boldsymbol{\alpha}^{\mathbf{b}}$ et vérifier si le nombre obtenu est une racine de l'unité ou non. L'inconvénient de cette méthode est que le calcul peut être coûteux en termes de taille. Par exemple, soit $\xi \in \overline{\mathbb{Q}}$ dont le polynôme minimal vaut $P = 109x^{123} + 17x^5 + 14x + 2$ et soit $\mathbb{K} = \mathbb{Q}[x]/P$. Soit $(\alpha_1, \alpha_2) = (\xi^{43}, \xi^{100})$. On veut vérifier si $\alpha_1^{100}\alpha_2^{-43} \in \boldsymbol{\mu}_\infty$. Pour écrire α_1^{100}, on a déjà besoin d'un polynôme de degré 122, ayant beaucoup de coefficients non nuls, et dont la taille est plus de 100 chiffres chacun. Sans même compter les calculs, la complexité en taille vaut au moins $O(\|\mathbf{b}\|h(\xi))$. L'algorithme suivant (Algorithme 4) utilise la réduction modulo p pour éviter cette explosion des coefficients.

Algorithme 4 : Vérification d'une relation de dépendance multiplicative faible

Entrée : Un polynôme irréductible $P \in \mathbb{Z}[x]$, $\boldsymbol{\alpha} \in \mathbb{K}^{*2}$ où $\mathbb{K} = \mathbb{Q}[x]/P$ et $\mathbf{b} \in \mathbb{Z}^2$.

Sortie : 1 si $\boldsymbol{\alpha}^{\mathbf{b}} \in \boldsymbol{\mu}_{\mathbb{K}}$ et 0 sinon.

1 Si $\mathbf{b} = \mathbf{0}$ alors renvoyer 1.

2 Pour $i = 1, 2$: si $b_i < 0$ alors faire

$$b_i \leftarrow -b_i \quad \text{et} \quad \alpha_i \leftarrow \alpha_1^{-i}.$$

3 Noter A_i le relevé de α_i dans $\mathbb{Q}[x]$ tel que $\deg(A_i) < \deg(P)$ pour $i = 1, 2$.

4 Choisir aléatoirement un nombre premier p tel que p ne divise pas le contenu de $P - P(0)$ et p ne divise pas le dénominateur de A_1 ni de A_2.

5 Noter $\bar{P}$ l'image de P dans $\mathbb{F}_p[x]$ et $\bar{A}_1$ (resp. $\bar{A}_2$) la réduction de A_1 (resp. A_2) dans $\mathbb{F}_p[x]/\bar{P}$.

6 Si $\bar{A}_1^{b_1}\bar{A}_2^{b_2} \neq 1$ alors renvoyer 0.

7 Tant que $b_2 \neq 0$:

8 calculer $m, r \in \mathbb{Z}$ tels que $b_1 = b_2 m + r$ où $0 \leqslant r < b_2$;

9 faire :

$$(b_1, b_2) \leftarrow (b_2, r) \quad \text{et} \quad (\alpha_1, \alpha_2) \leftarrow (\alpha_2\alpha_1^m, \alpha_1).$$

10 Renvoyer 1 si $\alpha_1 \in \boldsymbol{\mu}_{\mathbb{K}}$ et 0 sinon, en appliquant l'Algorithme 3.

Proposition 2.5.1. *L'Algorithme 4 est correct.*

Démonstration. La première étape est triviale. On peut supposer donc que $\mathbf{b}$ est non nul. Quitte à remplaçer α_i par α_i^{-1} à l'étape 2, on peut supposer que b_1 et b_2 sont positifs.

Soient A_1 et A_2 les deux polynômes définis à l'étape 3 et soit p un nombre premier vérifiant les conditions de l'étape 4. La première condition sur p implique que le polynôme $P(X)$ n'est pas constant modulo p et donc $\mathbb{F}_p[x]/\bar{P} \neq \mathbb{F}_p[x]$. Les deux autres conditions impliquent que la réduction de A_1 et celle de A_2 sont bien définies dans $\mathbb{F}_p[x]/\bar{P}$. Maintenant si $\boldsymbol{\alpha}^{\mathbf{b}} \in \boldsymbol{\mu}_\infty$ alors on a $\bar{A}_1^{b_1}\bar{A}_2^{b_2} = 1$. Ainsi si $\bar{A}_1^{b_1}\bar{A}_2^{b_2} \neq 1$ alors on a $\boldsymbol{\alpha}^{\mathbf{b}} \notin \boldsymbol{\mu}_\infty$; et dans ce cas, l'algorithme termine et renvoie 0 à l'étape 6.

Soit k le nombre d'étapes dans la division euclidienne de b_1 par b_2. On pose $\mu = \boldsymbol{\alpha}^{\mathbf{b}}$ et on note $\alpha_{1,i}$, $\alpha_{2,i}$, m_i et r_i les valeurs respectives de α_1, α_2, m et r après i itérations de la boucle « Tant que ». On a donc $r_1, \cdots, r_k \in \mathbb{Z}$, $0 = r_k < r_{k-1} < \cdots < r_1 < b_2$ et

$$\begin{cases} b_1 = b_2 m_1 + r_1 \\ b_2 = r_1 m_2 + r_2 \\ r_1 = r_2 m_3 + r_3 \\ \vdots \\ r_{k-3} = r_{k-2} m_{k-1} + r_{k-1} \\ r_{k-2} = r_{k-1} m_k + r_k. \end{cases}$$

Supposons d'abord $\operatorname{pgcd}(b_1, b_2) = 1$. Il existe donc $(u_1, u_2) \in \mathbb{Z}^2$ tel que $u_1 b_1 + u_2 b_2 = 1$. En posant $\xi = \alpha_1^{u_2}\alpha_2^{-u_1}$, on a $\xi^{b_2} = \alpha_1^{u_2 b_2}\alpha_2^{-u_1 b_2} = \alpha_1 \mu^{-u_1}$ et donc $\alpha_1 = \mu^{u_1}\xi^{b_2}$. Similairement, on a $\alpha_2 =$

$\mu^{u_2}\xi^{-b_1}$. Par suite, il existe $\eta_1 = u_1, \eta_2, \cdots, \eta_{k-1}, \eta_k \in \mathbb{Z}$ tels que :

$$\begin{cases} \alpha_{1,1} = \mu^{\eta_1}\xi^{b_2} \\ \alpha_{1,2} = \mu^{\eta_2}\xi^{-r_1} \\ \vdots \\ \alpha_{1,k-1} = \mu^{\eta_{k-1}}\xi^{\mp r_{k-1}} \\ \alpha_{1,k} = \mu^{\eta_k}. \end{cases} \tag{2.5.1}$$

Cela montre que si $\mu \in \boldsymbol{\mu}_\infty$ alors $\alpha_{1,k} \in \boldsymbol{\mu}_\infty$ et donc l'algorithme termine et renvoie 1 à l'étape 10.

Enfin, si $\operatorname{pgcd}(b_1, b_2) \neq 1$ alors la boucle « Tant que » finit en une seule étape. Dans ce cas, l'algorithme termine à l'étape 10. □

On s'intéresse maintenant au problème suivant. Soient $\alpha_1, \alpha_2 \in \overline{\mathbb{Q}}^{*2}$ deux unités algébriques qui ne sont pas des racines de l'unité. Comment peut-on calculer une base de $R_f(\boldsymbol{\alpha})$? L'Algorithme 5 permet de traiter ce type de problème. L'idée consiste à utiliser les plongements de $\mathbb{K}$ dans $\mathbb{C}$. On a besoin du lemme suivant qui donne une majoration des vecteurs $\mathbf{b}$ vérifiant $\boldsymbol{\alpha}^{\mathbf{b}} \in \boldsymbol{\mu}_\infty$. On rappelle que la fonction ℓ est définie à l'équation (1.2.3) à la page 5, à la fin de la Section 1.2.2 du Chapitre 1.

Lemme 2.5.2. *Soit $\boldsymbol{\alpha} \in \overline{\mathbb{Q}}^{*2}$ qui n'est pas de torsion et soit $\mathbf{b} \in \mathbb{Z}^2$. Si $\boldsymbol{\alpha}^{\mathbf{b}} \in \boldsymbol{\mu}_\infty$ alors on a :*

$$\frac{|b_1|}{\operatorname{pgcd}(b_1, b_2)} \leqslant d\ell(d)h(\alpha_2) \quad \text{et} \quad \frac{|b_2|}{\operatorname{pgcd}(b_1, b_2)} \leqslant d\ell(d)h(\alpha_1),$$

où $d = [\mathbb{Q}(\boldsymbol{\alpha}) : \mathbb{Q}]$.

Démonstration. Si $\mathbf{b} = 0$ alors c'est trivial. On peut supposer donc que $\mathbf{b}$ est non nul. Supposons d'abord $\operatorname{pgcd}(b_1, b_2) = 1$. On a alors $\dim R_f(\boldsymbol{\alpha}) = 1$ car $\boldsymbol{\alpha}$ n'est pas un point de torsion. Ainsi, $\mathbf{b}$ est un générateur de $R_f(\boldsymbol{\alpha})$. D'après le Lemme 2.1.2, on a $\boldsymbol{\alpha} = (\zeta_1\xi^{b_2}, \zeta_2\xi^{-b_1})$ où $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^2$, $\xi \in \overline{\mathbb{Q}}^*$ tel que $R_f(\xi) = \{0\}$ et $\mathbb{Q}(\boldsymbol{\alpha}) = \mathbb{Q}(\boldsymbol{\zeta}, \xi)$. On a alors :

$$h(\alpha_1) = h(\zeta_1\xi^{b_2}) = h(\xi^{b_2}) = |b_2|h(\xi).$$

Puisque $0 \neq \xi \notin \boldsymbol{\mu}_\infty$, on a $h(\xi) \neq 0$. Par suite, on a :

$$|b_2| = \frac{h(\alpha_1)}{h(\xi)} = \frac{[\mathbb{Q}(\xi) : \mathbb{Q}]}{\log M(\xi)} h(\alpha_1).$$

En utilisant la fonction ℓ et comme $\xi \in \mathbb{Q}(\boldsymbol{\alpha})$, on obtient :

$$|b_2| \leqslant [\mathbb{Q}(\boldsymbol{\alpha}) : \mathbb{Q}]\ell([\mathbb{Q}(\boldsymbol{\alpha}) : \mathbb{Q}])h(\alpha_1).$$

Si $\operatorname{pgcd}(b_1, b_2) \neq 1$ alors il suffit de faire le calcul précédent en remplaçant respectivement b_1 et b_2 par $b_1/\operatorname{pgcd}(b_1, b_2)$ et $b_2/\operatorname{pgcd}(b_1, b_2)$. Par symétrie, on a la majoration pour $|b_1|/\operatorname{pgcd}(b_1, b_2)$. □

Algorithme 5 : Relations de dépendance multiplicative faible entre deux unités algébriques $\alpha_1, \alpha_2 \notin \boldsymbol{\mu}_\infty$

Entrée : Un polynôme irréductible $P \in \mathbb{Z}[x]$ définissant un corps de nombres $\mathbb{K} = \mathbb{Q}[x]/P$, deux unités algébriques $\alpha_1, \alpha_2 \notin \boldsymbol{\mu}_\infty$.

Sortie : Une base de $R_f(\boldsymbol{\alpha})$.

1 Calculer l'ensemble Σ des plongements σ de $\mathbb{K}$ dans $\mathbb{C}$.
2 Noter d le degré de P.
3 Calculer un majorant H de $h(\alpha_2) = \frac{1}{d}\sum_{\sigma\in\Sigma} \log\max(1, |\sigma(\alpha_2)|)$.
4 Calculer $B = d\ell(d)H$.
5 Choisir $\sigma \in \Sigma$ tel que $\max_{\sigma'\in\Sigma} |\sigma'(\alpha_2)| = |\sigma(\alpha_2)|$.
6 Calculer $r = \dfrac{\log(|\sigma(\alpha_1)|)}{\log(|\sigma(\alpha_2)|)}$ à $1/(4B^2)$ précision près.
7 En utilisant l'algorithme de la fraction continue de r, calculer la réduite (p_n/q_n) telle que $q_n \leqslant B$ est maximal et poser $(b_1, b_2) = (p_n, q_n)$.
8 Appliquer l'Algorithme 4 à $\boldsymbol{\alpha}$ et $\{\begin{pmatrix} -b_2 \\ b_1 \end{pmatrix}\}$.
9 Si l'Algorithme 4 renvoie 1 alors renvoyer $\{\begin{pmatrix} -b_2 \\ b_1 \end{pmatrix}\}$.
10 Sinon renvoyer $\{\}$.

Proposition 2.5.3. *L'Algorithme 5 est correct.*

Démonstration. Supposons qu'il existe $\mathbf{b}' \in \mathbb{Z}^2$ primitif tel que $\boldsymbol{\alpha}^{\mathbf{b}'} \in \boldsymbol{\mu}_\infty$. On peut supposer $b'_1 < 0$. D'après le Lemme 2.5.2, on a $|b'_1| \leqslant d\ell(d)h(\alpha_2)$. Ainsi, la borne B construite à l'étape 4 est un majorant de $|b'_1|$. On a $\dim R_f(\boldsymbol{\alpha}) = 1$ car $\boldsymbol{\alpha}$ n'est pas un point de torsion. Ainsi, $\mathbf{b}'$ est un générateur de $R_f(\boldsymbol{\alpha})$. D'après le Lemme 2.1.2, on a $\boldsymbol{\alpha} = (\zeta_1\xi^{b'_2}, \zeta_2\xi^{-b'_1})$ où $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^2$ et $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$. Soit σ le plongement défini à l'étape 5. Puisque $\alpha_2 \notin \boldsymbol{\mu}_\infty$, on a $|\sigma(\alpha_2)| > 1$ et on peut donc faire le calcul du quotient r à l'étape 6. Par construction, on a :

$$\left| r - \frac{b'_2}{-b'_1} \right| \leqslant \frac{1}{4B^2} \leqslant \frac{1}{b'^2_1}.$$

Cette inégalité montre que $b'_2/-b'_1$ est une réduite de r. Soit (b_1, b_2) le vecteur défini à l'étape 7. Par maximalité de b_2, on a $-b'_1 \leqslant b_2$.

Montrons ensuite que l'on a $(b_1, b_2) = (b'_2, -b'_1)$. Supposons $|b_2 r - b_1| < |-b'_1 r - b'_2|$. Comme $-b'_1 \leqslant b_2$, on obtient :

$$\left| r - \frac{b_1}{b_2} \right| < \left| r - \frac{b'_2}{-b'_1} \right| \leqslant \frac{1}{4B^2}.$$

Par suite, on a :

$$\frac{1}{B^2} \leqslant \frac{1}{-b_2 b'_1} \leqslant \left| \frac{b_1}{b_2} - \frac{b'_2}{-b'_1} \right| \leqslant \left| \frac{b_1}{b_2} - r \right| + \left| r - \frac{b'_2}{-b'_1} \right| \leqslant \frac{1}{4B^2} + \frac{1}{4B^2} = \frac{1}{2B^2}.$$

D'où on a une contradiction et donc $|b_2 r - b_1| \geqslant |-b'_1 r - b'_2|$. Puisque b_1/b_2 est une meilleure approximation de r (car réduite) et $-b'_1 \leqslant b_2$, on en déduit $b_1/b_2 = b'_2/b'_1$ et donc $(b_1, b_2) = (b'_2, -b'_1)$. Ainsi, l'algorithme est correct. □

Remarque. Il semble possible de généraliser la méthode utilisée dans l'Algorithme 5 pour n unités algébriques (avec n quelconque) quitte à bien gérer les précisions.

Soit $\mathbb{K}$ un corps de nombres et soit $\alpha \in \mathbb{K}$. On note Σ l'ensemble des plongements σ de $\mathbb{K}$ dans $\mathbb{C}$. On note $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha) \in \mathbb{Q}$ la norme et $\chi^{\alpha}_{\mathbb{K}/\mathbb{Q}}(x) \in \mathbb{Z}[x]$ le polynôme caractéristique (dans $\mathbb{Z}[x]$ et primitif) de α i.e.

$$\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha) = \prod_{\sigma\in\Sigma} \sigma(\alpha) \quad \text{et} \quad \chi^{\alpha}_{\mathbb{K}/\mathbb{Q}}(x) = c_\alpha \prod_{\sigma\in\Sigma} (x - \sigma(\alpha)) \quad \text{où} \quad c_\alpha \in \mathbb{Z}.$$

Il est connu que si $\alpha_1, \alpha_2 \in \mathbb{K}$ alors on a :

$$\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_1\alpha_2) = \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_1)\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_2).$$

On note $\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha)$ la valeur absolue du coefficient dominant de $\chi^{\alpha}_{\mathbb{K}/\mathbb{Q}}(x)$ i.e. $\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha) = |c_\alpha|$. On a la propriété suivante.

Lemme 2.5.4. *Soit $\mathbb{K}$ un corps de nombres et soit $\alpha \in \mathbb{K}$. Si $0 \neq n \in \mathbb{N}$ alors on a $\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha^n) = \mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha)^n$.*

Démonstration. Soit Σ l'ensemble des plongements σ de $\mathbb{K}$ dans $\mathbb{C}$. On note $d = [\mathbb{K} : \mathbb{Q}]$. Pour simplifier les notations, si $n \in \mathbb{N}$ alors on désigne par χ_n le polynôme caractéristique de α^n i.e.

$$\chi_n(x) = c_n \prod_{\sigma\in\Sigma} (x - \sigma(\alpha^n)).$$

On va alors montrer $|c_n| = |c_1|^n$. Soit $\zeta \in \boldsymbol{\mu}_\infty$ tel que $\zeta^n = 1$. On a :

$$\begin{aligned}
\chi_n(x^n) &= c_n \prod_{\sigma\in\Sigma} (x^n - \sigma(\alpha)^n) \\
&= c_n \prod_{i=0}^{n-1} \prod_{\sigma\in\Sigma} (x - \zeta^i\sigma(\alpha)) \\
&= c_n(-1)^{(n-1)d} \prod_{i=0}^{n-1} \frac{\chi_1(\zeta^{-i}x)}{c_1} \\
&= \frac{(-1)^{(n-1)d}c_n}{c_1^n} \prod_{i=0}^{n-1} \chi_1(\zeta^{-i}x).
\end{aligned}$$

Puisque $\chi_1 \in \mathbb{Z}[x]$, on en déduit que :

$$\prod_{i=0}^{n-1} \chi_1(\zeta^{-i}x) \in \mathbb{Q}[x] \cap \mathbb{Z}[\zeta][x] = \mathbb{Z}[x].$$

Puisque χ_1 est primitif et ζ est une unité algébrique, $\chi_1(\zeta^{-i}x)$ est primitif dans $\mathbb{Z}[\zeta][x]$. Puisque $\mathbb{Z}[\zeta]$ est intégralement clos, d'après le Lemme de Gauss, $\prod_{i=0}^{n-1} \chi_1(\zeta^{-i}x)$ est primitif dans $\mathbb{Z}[\zeta][x]$ et donc dans $\mathbb{Z}[x]$. Par suite, on en déduit que $c_n = \pm c_1^n$ et donc $|c_n| = |c_1|^n$. □

On peut utiliser ces deux outils pour déduire une relation de dépendance multiplicative entre α_1 et α_2. Par exemple, s'il existe une relation de dépendance entre leur norme alors on peut vérifier si le même

vecteur donne une relation entre α_1 et α_2 en utilisant l'Algorithme 4. On a aussi une propriété similaire pour le coefficient dominant.

En combinant ces différentes procédures, on obtient un algorithme pour calculer une base de l'ensemble des relations de dépendance multiplicative faible entre deux nombres algébriques α_1 et α_2.

Algorithme 6 : Relations de dépendance multiplicative faible dans $\mathbb{G}_{\mathrm{m}}^2$

Entrée : Un polynôme irréductible $P \in \mathbb{Z}[x]$ définissant un corps de nombres $\mathbb{K} = \mathbb{Q}[x]/P$, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2) \in \mathbb{K}^{*2}$.

Sortie : Une base de $R_f(\boldsymbol{\alpha})$.

1 Appliquer l'Algorithme 3 à α_1 et α_2 successivement.
2 Si $\alpha_1 \in \boldsymbol{\mu}_{\mathbb{K}}$ et $\alpha_2 \in \boldsymbol{\mu}_{\mathbb{K}}$ alors renvoyer $\{I_2\}$.
3 Si $\alpha_1 \in \boldsymbol{\mu}_{\mathbb{K}}$ alors renvoyer $\{\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\}$.
4 Si $\alpha_2 \in \boldsymbol{\mu}_{\mathbb{K}}$ alors renvoyer $\{\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)\}$.
5 Appliquer l'Algorithme 1 à $(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_1), \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_2))$ et noter B_1 la base renvoyée.
6 Si $B_1 = \{\}$, renvoyer $\{\}$.
7 Si $B_1 = \{\mathbf{b}\}$ alors :
8 appliquer l'Algorithme 4 à $\boldsymbol{\alpha}$ et $\mathbf{b}$;
9 si $\boldsymbol{\alpha}^{\mathbf{b}} \in \boldsymbol{\mu}_{\mathbb{K}}$ alors renvoyer $\{\mathbf{b}\}$;
10 sinon renvoyer $\{\mathbf{0}\}$.
11 Appliquer l'Algorithme 1 à $(\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_1), \mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_2))$ et noter B_2 la base renvoyée.
12 Si $B_2 = \{\}$ alors renvoyer $\{\}$.
13 Si $B_2 = \{\mathbf{b}\}$ alors :
14 appliquer l'Algorithme 4 à $\boldsymbol{\alpha}$ et $\mathbf{b}$;
15 si $\boldsymbol{\alpha}^{\mathbf{b}} \in \boldsymbol{\mu}_{\mathbb{K}}$ alors renvoyer $\{\mathbf{b}\}$;
16 appliquer l'Algorithme 4 à $\boldsymbol{\alpha}$ et $\mathbf{b}^* = \left(\begin{smallmatrix} b_1 \\ -b_2 \end{smallmatrix}\right)$;
17 si $\boldsymbol{\alpha}^{\mathbf{b}^*} \in \boldsymbol{\mu}_{\mathbb{K}}$ alors renvoyer $\{\mathbf{b}^*\}$ et sinon renvoyer $\{\}$.
18 Appliquer l'Algorithme 5 à (α_1, α_2) et noter B la base renvoyée.
19 Renvoyer B.

Proposition 2.5.5. *L'Algorithme 6 est correct.*

Démonstration. L'étape 1 consiste à vérifier si α_1 ou α_2 est une racine de l'unité. Si tel est le cas, la base de R_f est triviale.

À l'étape 5, on a $\alpha_1, \alpha_2 \notin \boldsymbol{\mu}_\infty$. Cela implique en particulier que $R_f(\boldsymbol{\alpha})$ est au plus de dimension 1. Remarquons que l'on a $R_f(\boldsymbol{\alpha}) \subseteq R_f(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_1), \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_2))$.

Si $R_f(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_1), \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_2)) = \{\mathbf{0}\}$ alors $R_f(\boldsymbol{\alpha}) = \{\mathbf{0}\}$ et donc l'algorithme termine à l'étape 6.

Si $\dim R_f(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_1), \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_2)) = 1$ alors $0 \leqslant \dim R_f(\boldsymbol{\alpha}) \leqslant 1$. Si $\dim R_f(\boldsymbol{\alpha}) = 1$ alors on a $R_f(\boldsymbol{\alpha}) = R_f(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_1), \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_2))$ (car ils sont saturés) et donc l'algorithme termine à l'étape 9. Si $\dim R_f(\boldsymbol{\alpha}) = 0$ alors l'algorithme termine à l'étape 10.

À l'étape 11, on a $\dim R_f(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_1), \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_2)) = 2$ et donc $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_1) = \pm\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_2) = \pm 1$. Cela implique que $\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_i) = \mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_i^{-1})$ pour $i = 1, 2$. En effet, soit P le polynôme caractéristique de α_i. On note $a_{i,d}$ (resp. $a_{i,0}$) le coefficient dominant de P (resp. son coefficient constant) et d_i son degré. Alors on a $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_i) = \pm a_{i,0}/a_{i,d} = \pm 1$ et donc $\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_i) = |a_{i,d}| = |a_{i,0}| = \mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_i^{-1})$.

Maintenant, soit $\mathbf{b} \in R_f(\boldsymbol{\alpha})$. On a donc $\boldsymbol{\alpha}^{\mathbf{b}} \in \boldsymbol{\mu}_\infty$. Il existe alors $0 \neq m \in \mathbb{N}$ tel que $\alpha_1^{b_1 m}\alpha_2^{mb_2} = 1$. D'après le Lemme 2.5.4, on en déduit que $\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_1)^{|b_1|}\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_2)^{-|b_2|} = 1$. Ainsi, on a $R_f(\boldsymbol{\alpha}) \subseteq R_f(\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_1), \mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_2))$ ou $R_f(\boldsymbol{\alpha}) \subseteq R_f(\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_1), \mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_2))$. Les arguments pour les étapes 11 à 17 sont les mêmes que ceux de 5 à 10.

À l'étape 18, on a $\dim R_f(\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_1), \mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_2)) = 2$ et donc α_1 et α_2 sont des unités algébriques car $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_1) = \pm\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_2) = \pm 1$ et $\mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_1) = \mathcal{C}_{\mathbb{K}/\mathbb{Q}}(\alpha_2) = 1$. De plus, $\alpha_1, \alpha_2 \notin \boldsymbol{\mu}_\infty$ et donc on peut appliquer l'Algorithme 5 à l'étape 18. □

Relations de dépendance multiplicative faible de codimension au plus 1

Soit $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$. L'algorithme suivant calcule une base de $R_f(\boldsymbol{\alpha})$ si $\mathrm{codim} R_f(\boldsymbol{\alpha}) \leqslant 1$.

Algorithme 7 : Relations de dépendance multiplicative faible de codimension au plus 1

Entrée : Un polynôme irréductible $P \in \mathbb{Z}[x]$ définissant un corps de nombres $\mathbb{K} = \mathbb{Q}[x]/P$, $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{K}^{*n}$.

Sortie : Une base de $R_f(\boldsymbol{\alpha})$ ou $\emptyset$.

1 Appliquer l'Algorithme 3 à $\alpha_1, \cdots, \alpha_n$ successivement.
2 Si $(\alpha_1, \cdots, \alpha_n) \in \boldsymbol{\mu}_{\mathbb{K}}^n$ alors renvoyer $\{I_n\}$.
3 Soit α_j le premier nombre algébrique différent des racines de l'unité parmi les $\alpha_1, \cdots, \alpha_n$.
4 Échanger α_1 et α_j de telle sorte que $\alpha_1 \notin \boldsymbol{\mu}_{\mathbb{K}}$.
5 Pour $i \in \{2, \cdots, n\}$:
6 appliquer l'Algorithme 6 à (α_1, α_i) ;
7 si $\dim R_f(\alpha_1, \alpha_i) = 0$ alors renvoyer $\emptyset$;
8 si $\dim R_f(\alpha_1, \alpha_i) = 1$ alors noter $\mathbf{b}_i = \begin{pmatrix} b_{i,1} \\ b_{i,2} \end{pmatrix}$ la base renvoyée ;
9 Noter $U \in M_{n,n-1}(\mathbb{Z})$ la matrice :

$$U = \begin{pmatrix} b_{2,1} & b_{3,1} & \cdots & b_{n,1} \\ b_{2,2} & 0 & \cdots & 0 \\ 0 & b_{3,2} & \mathbf{0} & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & b_{n,2} \end{pmatrix}.$$

10 Échanger la première colonne et la j-ème colonne de U.
11 Renvoyer une base B de $\langle U \rangle^{\mathrm{sat}}$.

Proposition 2.5.6. *Soit $P \in \mathbb{Z}[x]$ un polynôme irréductible définissant un corps de nombres $\mathbb{K} = \mathbb{Q}[x]/P$ et $\boldsymbol{\alpha} \in \mathbb{K}^{*n}$. Si $\mathrm{codim} R_f(\boldsymbol{\alpha}) \leqslant 1$ alors l'Algorithme 7 renvoie une base de $R_f(\boldsymbol{\alpha})$, sinon il renvoie $\emptyset$.*

Démonstration. Si $\mathrm{codim} R_f(\boldsymbol{\alpha}) = 0$ alors $\boldsymbol{\alpha}$ est un point de torsion et donc l'algorithme termine à l'étape 2 et renvoie $\{I_n\}$.

Sans perte de généralité, on peut supposer qu'à l'étape 3, α_1 est le premier nombre algébrique différent des racines de l'unité parmi les $\alpha_1, \cdots, \alpha_n$.

Supposons que l'algorithme renvoie $\emptyset$. Donc il existe $i \geqslant 2$ tel que $\dim R_f(\alpha_1, \alpha_i) = 0$. Cela signifie que α_1 et α_i sont multiplicativement indépendants et donc la codimension est au moins 2.

Supposons que cet algorithme ne renvoie pas $\emptyset$. Par construction de U, son rang est égal à $n-1$ et $\boldsymbol{\alpha}^U \in \boldsymbol{\mu}_\infty^{n-1}$. On a donc $\langle U \rangle \subseteq R_f(\boldsymbol{\alpha})$ et donc $R_f(\boldsymbol{\alpha})$ est de codimension 1 (car $\boldsymbol{\alpha}$ n'est pas de torsion). En prenant le saturé et en tenant compte du fait que $R_f(\boldsymbol{\alpha})$ est saturé, on a :

$$\langle U \rangle^{\mathrm{sat}} \subseteq R_f(\boldsymbol{\alpha}).$$

Par un argument de dimension, on a l'égalité $\langle U \rangle^{\mathrm{sat}} = R_f(\boldsymbol{\alpha})$. □

2.6 Calcul des relations de dépendance forte à partir des relations de dépendance faible

Maintenant que l'on dispose d'un algorithme (Algorithme 6) pour calculer $R_f(\boldsymbol{\alpha})$ pour $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^2$, on va décrire un algorithme qui permet d'obtenir $R_F(\boldsymbol{\alpha})$ à partir de $R_f(\boldsymbol{\alpha})$. Pour cela, on a besoin d'une procédure qui permet de calculer une base de l'ensemble des relations de dépendance multiplicative forte entre des racines de l'unité. Les deux algorithmes qui suivent s'appliquent au cas où $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ mais pas seulement au cas où $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^2$.

Algorithme 8 : Relations de dépendance multiplicative forte entre racines de l'unité

Entrée : Un polynôme irréductible $P \in \mathbb{Z}[x]$ définissant un corps de nombres $\mathbb{K} = \mathbb{Q}[x]/P$ et $\boldsymbol{\alpha} \in \boldsymbol{\mu}_{\mathbb{K}}^n$.

Sortie : Une base de $R_F(\boldsymbol{\alpha})$.

1 Calculer un entier positif N tel que $\boldsymbol{\mu}_{\mathbb{K}} \subseteq \boldsymbol{\mu}_N$ en appliquant l'Algorithme 2
2 Choisir un plongement σ de $\mathbb{K}$ dans $\mathbb{C}$.
3 Calculer le vecteur $\mathbf{a} \in \mathbb{Z}^n$ où la coordonnée a_k de $\mathbf{a}$ est l'entier positif vérifiant $\sigma(\alpha_k) = \exp(2\pi i a_k/N)$.
4 Calculer le noyau $K \subseteq \mathbb{Z}^n$ de l'application $\mathbf{x} \in \mathbb{Z}^n \mapsto \mathbf{a}\mathbf{x} \mod N \in \mathbb{Z}/N\mathbb{Z}$.
5 Renvoyer une base de K.

Proposition 2.6.1. *L'Algorithme 8 est correct.*

Démonstration. Soit $\{\mathbf{b}_1, \cdots, \mathbf{b}_d\}$ une $\mathbb{Z}$-base de K. Pour $j \in \{1, \cdots, d\}$, on a :

$$\mathbf{b}_j \in K \iff \mathbf{a}\mathbf{b}_j = 0 \mod N \iff \exp(2\pi i/N)^{\mathbf{a}\mathbf{b}_j} = 1 \iff \sigma(\boldsymbol{\alpha})^{\mathbf{b}_j} = 1 \iff \boldsymbol{\alpha}^{\mathbf{b}_j} = 1.$$

□

On en déduit l'algorithme qui permet de déduire $R_F(\boldsymbol{\alpha})$ à partir de $R_f(\boldsymbol{\alpha})$.

Algorithme 9 : Relations de dépendance multiplicative forte entre nombres algébriques

Entrée : Un polynôme irréductible $P \in \mathbb{Z}[x]$ définissant un corps de nombres $\mathbb{K} = \mathbb{Q}[x]/P$, $\boldsymbol{\alpha} \in \mathbb{K}^{*n}$ et une base B de $R_f(\boldsymbol{\alpha})$.

Sortie : Une base de $R_F(\boldsymbol{\alpha})$.

1 Calculer $\boldsymbol{\beta} = (\beta_1, \cdots, \beta_m) = \boldsymbol{\alpha}^B$ où $m = \dim R_f(\boldsymbol{\alpha})$.
2 Appliquer l'Algorithme 8 à $\boldsymbol{\beta}$ et noter U la base renvoyée.
3 Renvoyer BU.

Proposition 2.6.2. *L'Algorithme 9 est correct.*

Démonstration. À l'étape 1, B est une base de $R_f(\boldsymbol{\alpha})$ et donc on a :

$$\boldsymbol{\beta} = \boldsymbol{\alpha}^B \in \boldsymbol{\mu}_\infty^m.$$

Ainsi, on peut appliquer l'Algorithme 8 à $\boldsymbol{\beta}$. À l'étape 2, comme U est une base de $R_F(\boldsymbol{\beta})$, d'après la propriété (1.1.1), on a :

$$(\boldsymbol{\alpha}^B)^U = \boldsymbol{\alpha}^{BU} = \mathbf{1}.$$

Ainsi, on a $\langle BU \rangle \subseteq R_F(\boldsymbol{\alpha})$. Réciproquement, soit $\mathbf{b} \in R_F(\boldsymbol{\alpha})$. On a alors $\boldsymbol{\alpha}^{\mathbf{b}} = 1$ et donc $\mathbf{b} \in R_f(\boldsymbol{\alpha})$. Ainsi, il existe un vecteur (colonne) $\mathbf{u} \in \mathbb{Z}^m$ tel que $\mathbf{b} = B\mathbf{u}$. On a alors $(\boldsymbol{\alpha}^B)^{\mathbf{u}} = 1$ et donc $\mathbf{u} \in R_f(\boldsymbol{\beta})$. Ainsi, il existe un vecteur (colonne) $\mathbf{v} \in \mathbb{Z}^r$ où $r = \dim R_F(\boldsymbol{\beta})$ tel que $\mathbf{u} = U\mathbf{v}$. D'où on a $\mathbf{b} = BU\mathbf{v}$ et donc $\mathbf{b} \in \langle BU \rangle$. □

3. Cas $n = 2$

Dans ce chapitre, on va donner une version explicite du Théorème 2 pour $n = 2$ (Théorème 3.2.1). Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}]$. Soient $\mathbf{a} \in \mathbb{Z}^2$ un vecteur primitif, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^2$ et $\xi \in \mathbb{G}_{\mathrm{m}} \setminus \boldsymbol{\mu}_\infty$. On pose $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$. Quitte à remplacer ξ par $\xi^{\mathrm{pgcd}(a_1,a_2)}$, on peut supposer que $\mathbf{a}$ est primitif. On va montrer que si $\boldsymbol{\alpha}$ est un point isolé de $V(F, G)$ alors la norme de $\mathbf{a}$ est majorée par une constante explicite ne dépendant que de F et G. Pour déduire un vecteur $\mathbf{b}$ satisfaisant les propriétés du Théorème 2, il suffit de prendre $(b_1, b_2) = (a_2, -a_1)$.

Pour majorer la norme de $\mathbf{a}$, la preuve se passe en deux étapes : d'une part, on minore la hauteur de Weil de ξ par une version explicite du Théorème de Dobrowolski montrée par Voutier (Théorème 1.2.2.3) et d'autre part, on majore la hauteur de Weil de α_i par une majoration de type Bézout Arithmétique (Proposition 3.1.6) que l'on obtient à l'aide du résultant.

On note qu'il est possible de trouver une majoration pour la hauteur de $\boldsymbol{\alpha}$ en utilisant le Théorème de Bézout Arithmétique (Théorème 1.6.2.3) ainsi qu'un autre résultat du même type fait par M. César [32]. Bien que ces résultats soient applicables à notre situation ainsi qu'à des contextes plus généraux, la majoration obtenue à l'aide de la Proposition 3.1.6 est plus précise dans le cas particulier $n = 2$.

Dans la Section 3.1, on donne la majoration de type Bézout Arithmétique que l'on obtient à l'aide du résultant. Ensuite, dans la Section 3.2, on donne une version explicite du Théorème 2 pour $n = 2$. La Section 3.3 contient des exemples et des applications, notamment le calcul de facteurs communs non-cyclotomiques de deux polynômes à une variable lorsque ceux-ci sont des spécialisations de deux polynômes à deux variables. Enfin, dans la Section 3.4, on décrit un algorithme plus efficace qui permet de calculer explicitement les vecteurs $\mathbf{a}$ du Théorème 3.2.1 sans passer par la recherche exhaustive basée sur la borne obtenue.

3.1 Majoration de type Bézout Arithmétique par le résultant

Si A est un anneau et si $F, G \in A[x]$ alors on note $\mathrm{Res}(F, G)$ leur résultant par rapport à x. En utilisant la majoration de Hadamard pour le déterminant de la matrice de Sylvester de F et G, on peut montrer le lemme classique suivant :

Lemme 3.1.1. *Soient $F, G \in \mathbb{C}[x]$ deux polynômes non nuls de degré respectif d_F et d_G. On a :*

$$|\mathrm{Res}(F, G)| \leqslant \|F\|_2^{d_G} \|G\|_2^{d_F}.$$

Dans notre situation, cette inégalité n'est pas suffisante car la norme L_2 ne se comporte pas bien par rapport au produit des polynômes. Rappelons que si $0 \neq F \in \mathbb{C}[\mathbf{x}^{\pm 1}]$ alors $M(F)$ désigne la mesure de Mahler de F et $\|F\|_1$ la norme L_1 du vecteur correspondant aux coefficients non nuls de F. Le lemme ci-après permet de majorer le résultant de deux polynômes à une variable en fonction de la mesure de Mahler et de la norme L_1.

Lemme 3.1.2. *Soient $F, G \in \mathbb{C}[x]$ deux polynômes non nuls de degré respectif d_F et d_G. On a :*

$$|\mathrm{Res}(F, G)| \leqslant M(F)^{d_G} \|G\|_1^{d_F}.$$

Démonstration. On écrit :

$$F(x)=\sum_{i=0}^{d_F} a_i x^i = a_{d_F}\prod_{i=1}^{d_F}(x-\alpha_i) \quad \text{et} \quad G(x)=\sum_{j=0}^{d_G} b_j x^j = b_{d_G}\prod_{j=1}^{d_G}(x-\beta_j).$$

Pour tout $z\in\mathbb{C}$, on a :

$$|G(z)|\leqslant \sum_{j=0}^{d_G}|b_j|\max(1,|z|)^{d_G}=\|G\|_1\max(1,|z|)^{d_G}.$$

Donc :

$$|\mathrm{Res}(F,G)|=|a_{d_F}^{d_G}\prod_{i=1}^{d_F}G(\alpha_i)|\leqslant\left(|a_{d_F}|\prod_{i=1}^{d_F}\max(1,|\alpha_i|)\right)^{d_G}\|G\|_1^{d_F}=M(F)^{d_G}\|G\|_1^{d_F}.$$

□

Remarque. Il aurait été bien pratique d'avoir la mesure de Mahler $M(G)$ à la place de la norme $\|G\|_1$ dans le Lemme 3.1.2. Cependant, cela n'est pas vrai en général. Par exemple, si $d,e\in\mathbb{N}$, $F(x)=(x-1)^d$ et $G(x)=(x+1)^e$ alors on a $\mathrm{Res}(F,G)=2^{de}$ et $M(F)=M(G)=1$.

Soit $\mathbb{K}$ un corps de nombre de degré d. Soient $\sigma_1,\cdots,\sigma_d$ les plongements de $\mathbb{K}$. Si $F\in\mathbb{K}[x]$ alors on note $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(F)$ la norme de F sur $\mathbb{Q}$ i.e.

$$\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(F)=\prod_{i=1}^{d}\sigma_i(F).$$

Les trois lemmes qui suivent sont utiles pour obtenir une majoration pour la mesure de Mahler des points isolés de $V(F,G)$.

Lemme 3.1.3. *Soient $F,G\in\mathbb{K}[x_1,x_2]$ tels que $\mathrm{pgcd}(F,G)=1$. On note R_i le résultant de F et G par rapport à x_i. Soit $\boldsymbol{\alpha}=(\alpha_1,\alpha_2)\in V(F,G)$. Pour $i=1,2$, on note $P_i\in\mathbb{Z}[x_i]$ le polynôme minimal de α_i. Alors :*

(i) *$P_1^{[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{Q}(\alpha_1)]}$ divise $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(R_2)$ (sur $\mathbb{Q}$).*
(ii) *$P_2^{[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{Q}(\alpha_2)]}$ divise $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(R_1)$ (sur $\mathbb{Q}$).*
(iii) *$[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{K}]\leqslant\min(\deg_{x_1}(R_2),\deg_{x_2}(R_1))$.*

Démonstration. Notons $P_{1,\mathbb{K}}$ le polynôme minimal de α_1 sur $\mathbb{K}$. Puisque α_1 annule $R_2\in\mathbb{K}[x_1]$ alors $P_{1,\mathbb{K}}$ divise R_2. On va tout d'abord montrer que $P_{1,\mathbb{K}}^{[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{K}(\alpha_1)]}$ divise R_2. Les deux polynômes $F(\alpha_1,x_2)$ et $G(\alpha_1,x_2)$ ne sont pas tous les deux nuls sinon F et G ont comme diviseur commun $P_{1,\mathbb{K}}$. Ainsi le polynôme $\widehat{H}(x_2)=\mathrm{pgcd}(F(\alpha_1,x_2),G(\alpha_1,x_2))\in\mathbb{K}(\alpha_1)[x_2]$ est non nul. Il existe $\widehat{F}_1(x_2)\in\mathbb{K}(\alpha_1)[x_2]$ tel que $\widehat{H}(x_2)\widehat{F}_1(x_2)=F(\alpha_1,x_2)$. Soit $H\in\mathbb{K}[x_1,x_2]$ un relevé de $\widehat{H}$ tel que $H(\alpha_1,x_2)=\widehat{H}(x_2)$ et $\deg_{x_2}(H)=\deg_{x_2}(\widehat{H})$. On choisit de même un relevé F_1 de $\widehat{F}_1$. Ainsi, le polynôme $F-HF_1\in\mathbb{K}[x_1,x_2]$ s'annule en $x_1=\alpha_1$. Par suite, il existe $F_2\in\mathbb{K}[x_1,x_2]$ tel que $F=HF_1+P_{1,\mathbb{K}}F_2$. De même, il existe $G_1,G_2\in\mathbb{K}[x_1,x_2]$ tels que $G=HG_1+P_{1,\mathbb{K}}G_2$. On a alors $\langle F,G\rangle\subset\langle H,P_{1,\mathbb{K}}\rangle$ en tant qu'idéaux dans $\mathbb{K}[x_1,x_2]$. D'après [27, Lemma 3.12, p. 398], on en déduit que $\mathrm{Res}_{x_2}(H,P_{1,\mathbb{K}})$ divise $\mathrm{Res}_{x_2}(F,G)=R_2$. Comme $P_{1,\mathbb{K}}$ est indépendant de x_2, on a $\mathrm{Res}_{x_2}(H,P_{1,\mathbb{K}})=P_{1,\mathbb{K}}^{\deg_{x_2}(H)}$. Puisque $[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{K}(\alpha_1)]$ est le

degré du polynôme minimal de α_2 sur $\mathbb{K}(\alpha_1)$ et que $\widehat{H}(\alpha_2) = 0$, on a $[\mathbb{K}(\boldsymbol{\alpha}) : \mathbb{K}(\alpha_1)] \leqslant \deg_{x_2}(\widehat{H})$. D'où $P_{1,\mathbb{K}}^{[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{K}(\alpha_1)]}$ divise R_2.

Par la multiplicativité de la norme, $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P_{1,\mathbb{K}})^{[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{K}(\alpha_1)]}$ divise $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(R_2)$ sur $\mathbb{Q}$. Comme α_1 annule $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P_{1,\mathbb{K}})$, P_1 divise $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P_{1,\mathbb{K}})$ qui est donc une puissance de P_1. En comparant les degrés de ces polynômes, on trouve :

$$\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P_{1,\mathbb{K}}) = P_1^{[\mathbb{K}(\alpha_1):\mathbb{Q}(\alpha_1)]}.$$

Comme $\mathcal{N}(P_{1,\mathbb{K}})^{[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{K}(\alpha_1)]}$ divise $\mathcal{N}(R_2)$ sur $\mathbb{Q}$, il en est de même pour $P_1^{[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{Q}(\alpha_1)]}$. D'où on a (**i**) et similairement on a aussi (**ii**). Enfin, on a :

$$[\mathbb{K}(\boldsymbol{\alpha}) : \mathbb{K}] = [\mathbb{K}(\boldsymbol{\alpha}) : \mathbb{K}(\alpha_1)][\mathbb{K}(\alpha_1) : \mathbb{K}] = [\mathbb{K}(\boldsymbol{\alpha}) : \mathbb{K}(\alpha_1)] \deg(P_{1,\mathbb{K}}).$$

Comme $P_{1,\mathbb{K}}^{[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{K}(\alpha_1)]}$ divise R_2, on en déduit $[\mathbb{K}(\boldsymbol{\alpha}) : \mathbb{K}] \leqslant \deg_{x_1}(R_2)$ et d'où on a (**iii**). □

Si $\boldsymbol{\alpha}$ est un point isolé d'une variété V de $\mathbb{G}_{\mathrm{m}}^2$ alors le lemme suivant fournit une méthode permettant de trouver une variété de dimension nulle dans V contenant $\boldsymbol{\alpha}$.

Lemme 3.1.4. *Soit $\mathbb{K}$ un corps de nombres. Soit $s \geqslant 1$ un entier et soient $F_1, \cdots, F_s \in \mathbb{K}[x_1^{\pm 1}, x_2^{\pm 1}]$. Si $\boldsymbol{\beta}$ est un point isolé de $V(F_1, \cdots, F_s)$ alors pour tout $i \in \{1, \cdots, s\}$, il existe un facteur irréductible S_i de F_i et $j \in \{1, \cdots, s\}$, $j \neq i$, tels que $\boldsymbol{\alpha} \in V(S_i, F_j)$ et $\operatorname{pgcd}(S_i, F_j) = 1$.*

Démonstration. On note $G = \operatorname{pgcd}(F_1, \cdots, F_s)$. Comme $\boldsymbol{\alpha}$ est un point isolé de $V(F_1, \cdots, F_s)$, on a $G(\boldsymbol{\alpha}) \neq 0$ et donc $(F_i/G)(\boldsymbol{\alpha}) = 0$. Il existe donc un facteur irréductible S_i de (F_i/G) tel que $S_i(\boldsymbol{\alpha}) = 0$. Par suite, on a $S_i \nmid G$. Par ailleurs, il existe $j \neq i$ tel que $S_i \nmid (F_j/G)$. On a alors $S_i \nmid (F_j/G)G = F_j$ et en particulier $\operatorname{pgcd}(S_i, F_j) = 1$. On a aussi $(F_j/G)(\boldsymbol{\alpha}) = 0$. □

Remarque. Il est nécessaire de prendre des facteurs irréductibles de F_i car parmi ces derniers, il n'existe pas nécessairement deux F_i qui sont premiers entre eux. Pour illustrer cela, on peut considérer l'exemple suivant : $F_1(x_1, x_2) = (x_1 - 1)(x_2 - 1)$, $F_2(x_1, x_2) = (x_1 - 1)(x_1 - x_2)$ et $F_3(x_1, x_2) = (x_1 - x_2)(x_2 - 1)$ avec $\boldsymbol{\alpha} = \mathbf{1}$.

Le résultat suivant est un lemme technique qui ne sert que comme outil de démonstration pour les deux propositions qui suivent.

Lemme 3.1.5. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$ non nuls. Soient $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ et $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}^n$ deux vecteurs linéairement indépendants. On pose $P(\mathbf{y}) = F(\boldsymbol{\zeta} y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})$ et $Q(\mathbf{y}) = G(\boldsymbol{\zeta} y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}) \in \mathbb{Z}[\boldsymbol{\zeta}][y_1, y_2]$. Si $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^2$ est un point isolé de $V(P, Q)$ alors on a :*

$$M(\beta_1)^{[\mathbb{K}(\boldsymbol{\beta}):\mathbb{Q}(\beta_1)]} \leqslant M(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P))^{\deg_{y_2}(Q)} \|G\|_1^{\deg_{y_2}(P)[\mathbb{K}:\mathbb{Q}]},$$

$$M(\beta_2)^{[\mathbb{K}(\boldsymbol{\beta}):\mathbb{Q}(\beta_2)]} \leqslant M(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P))^{\deg_{y_1}(Q)} \|G\|_1^{\deg_{y_1}(P)[\mathbb{K}:\mathbb{Q}]}$$

et

$$[\mathbb{K}(\boldsymbol{\beta}) : \mathbb{K}] \leqslant \deg_{y_1}(P) \deg_{y_2}(Q) + \deg_{y_1}(Q) \deg_{y_2}(P),$$

où $\mathbb{K} = \mathbb{Q}(\boldsymbol{\zeta})$.

Démonstration. Quitte à remplacer F et G par leurs polynômes associés $\widetilde{F}$ et $\widetilde{G}$, on peut supposer $F, G \in \mathbb{Z}[\mathbf{x}]$. Comme $\boldsymbol{\beta}$ est un point isolé de $V(P,Q)$, d'après le Lemme 3.1.4, il existe un facteur irréductible $S \in \mathbb{K}[y_1, y_2]$ de P tel que $\boldsymbol{\beta} \in V(S,Q)$ et $\operatorname{pgcd}(S,Q) = 1$. Comme $\mathbb{Z}[\boldsymbol{\zeta}]$ est intégralement clos, on peut supposer $S \in \mathbb{Z}[\boldsymbol{\zeta}][y_1, y_2]$. On note $R_2 \in \mathbb{Z}[\boldsymbol{\zeta}][y_1]$ le résultant de S et Q par rapport à la variable y_2. Soit $z \in \mathbb{C}$ tel que z ne soit pas un zéro du coefficient dominant de S ni de Q par rapport à la variable y_2. On note $d = [\mathbb{K} : \mathbb{Q}]$. Soient $\sigma_1, \cdots, \sigma_d$ sont les plongements de $\mathbb{K}$ dans $\mathbb{C}$. En appliquant le Lemme 3.1.2 à $\sigma_i(S)(z, y_2)$ et $\sigma_i(Q)(z, y_2)$, on a :

$$|\sigma_i(R_2)(z)| \leqslant M(\sigma_i(S)(z, y_2))^{\deg_{y_2}(Q)} \|\sigma_i(Q)(z, y_2)\|_1^{\deg_{y_2}(S)}. \tag{3.1.1}$$

On note P_1 le polynôme minimal de β_1 sur $\mathbb{Q}$. D'après le Lemme 3.1.3 (**i**), $P_1^{[\mathbb{K}(\boldsymbol{\beta}):\mathbb{Q}(\beta_1)]}$ divise $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(R_2)$ sur $\mathbb{Q}$. Comme $R_2 \in \mathbb{Z}[\boldsymbol{\zeta}][y_1]$, on a $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(R_2) \in \mathbb{Z}[y_1]$. Puisque $P_1 \in \mathbb{Z}[y_1]$ est primitif, la divisibilité reste vraie sur $\mathbb{Z}$. Par la multiplicativité de la mesure de Mahler, on en déduit que :

$$M(\beta_1)^{[\mathbb{K}(\boldsymbol{\beta}):\mathbb{Q}(\beta_1)]} \leqslant M(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(R_2)) = \exp\left(\int_0^1 \log\left(|\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(R_2)(e^{2\pi i\theta_1})|\right) d\theta_1\right).$$

Les valeurs de $z = e^{2\pi i\theta_1}$ qui sont des racines du coefficient dominant de S ou de Q par rapport à la variable x_2 sont en nombre fini. D'après (3.1.1), on a :

$$\begin{aligned} M(\beta_1)^{[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{Q}(\beta_1)]} \leqslant \exp\left(\deg_{y_2}(Q)\int_0^1 \log\prod_{i=1}^d M\left(\sigma_i(S)(e^{2\pi i\theta_1}, y_2)\right) d\theta_1\right) \times \\ \exp\left(\deg_{y_2}(S)\int_0^1 \log\prod_{i=1}^d \|\sigma_i(Q)(e^{2\pi i\theta_1}, y_2)\|_1 \, d\theta_1\right). \end{aligned}$$

D'une part, on a :

$$\begin{aligned} \int_0^1 \log\prod_{i=1}^d M\left(\sigma_i(S)(e^{2\pi i\theta_1}, y_2)\right) d\theta_1 &= \int_0^1\int_0^1 \log|\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(S)(e^{2\pi i\theta_1}, e^{2\pi i\theta_1})| \, d\theta_1 d\theta_2 \\ &= \log M(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(S)) \\ &\leqslant \log M(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P)), \end{aligned}$$

où, dans la dernière inégalité, on a utilisé le fait que $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(S)$ divise $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P)$ et ces polynômes ont des coefficients dans $\mathbb{Z}$.

D'autre part, on a :

$$\int_0^1 \log\prod_{i=1}^d \|\sigma_i(Q)(e^{2\pi i\theta_1}, y_2)\|_1 \, d\theta_1 \leqslant \log\prod_{i=1}^d \max_{|z|=1} \|\sigma_i(Q)(z, y_2)\|_1 \leqslant \log\prod_{i=1}^d \|\sigma_i(Q)\|_1 \leqslant \log\|G\|_1^d.$$

En combinant ces inégalités et le fait que $\deg_{y_2}(S) \leqslant \deg_{y_2}(P)$, on a :

$$M(\beta_1)^{[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{Q}(\beta_1)]} \leqslant M(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P))^{\deg_{y_2}(Q)} \|G\|_1^{\deg_{y_2}(P)[\mathbb{K}:\mathbb{Q}]}.$$

Enfin, d'après le Lemme 3.1.3 (**iii**), on a :

$$[\mathbb{K}(\boldsymbol{\beta}) : \mathbb{K}] \leqslant \min(\deg_{y_1}(R_2), \deg_{y_2}(R_1)).$$

En utilisant la matrice de Sylvester pour le calcul du résultant, on en déduit que :

$$\begin{aligned} [\mathbb{K}(\boldsymbol{\beta}) : \mathbb{K}] &\leqslant \deg_{y_1}(S)\deg_{y_2}(Q) + \deg_{y_1}(Q)\deg_{y_2}(S) \\ &\leqslant \deg_{y_1}(P)\deg_{y_2}(Q) + \deg_{y_1}(Q)\deg_{y_2}(P). \end{aligned}$$

□

La proposition suivante donne une majoration du type Bézout Arithmétique dans le cas de deux polynômes à deux variables.

Proposition 3.1.6. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}]$. Si $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^2$ est un point isolé de $V(F,G)$ alors on a :*

$$M(\beta_1)^{[\mathbb{Q}(\boldsymbol{\beta}):\mathbb{Q}(\beta_1)]} \leqslant M(F)^{\deg_{x_2}(G)} \|G\|_1^{\deg_{x_2}(F)},$$

$$M(\beta_2)^{[\mathbb{Q}(\boldsymbol{\beta}):\mathbb{Q}(\beta_2)]} \leqslant M(F)^{\deg_{x_1}(G)} \|G\|_1^{\deg_{x_1}(F)}$$

et

$$[\mathbb{Q}(\boldsymbol{\beta}) : \mathbb{Q}] \leqslant \deg_{x_1}(F)\deg_{x_2}(G) + \deg_{x_1}(G)\deg_{x_2}(F).$$

Démonstration. Il suffit d'appliquer le Lemme 3.1.5 à $\boldsymbol{\zeta} = \mathbf{1}$, $\{\mathbf{u}_1, \mathbf{u}_2\}$ la base canonique de $\mathbb{Z}^2$, $P = F$ et $Q = G$. □

Pour une utilisation ultérieure (dans le Chapitre 6), on donne la proposition suivante qui est une variante de la Proposition 3.1.6. On note que la borne dans la Proposition 3.1.6 est plus précise que celle dans la Proposition 3.1.7 dans le cas où $n = 2$ et $\{\mathbf{u}_1, \mathbf{u}_2\}$ la base canonique de $\mathbb{Z}^2$.

Proposition 3.1.7. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$. Soit $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$. On note $\mathbb{K} = \mathbb{Q}(\boldsymbol{\zeta})$. Soient $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}^n$ deux vecteurs linéairement indépendants. Si $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^2$ est un point isolé de $V(F(\boldsymbol{\zeta} y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}), G(\boldsymbol{\zeta} y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}))$ alors on a :*

$$M(\beta_1)^{[\mathbb{K}(\boldsymbol{\beta}):\mathbb{Q}(\beta_1)]} \leqslant \left(\|F\|_1^{\deg_\infty(G)} \|G\|_1^{\deg_\infty(F)}\right)^{\|\mathbf{u}_2\|_1 [\mathbb{K}:\mathbb{Q}]},$$

$$M(\beta_2)^{[\mathbb{K}(\boldsymbol{\beta}):\mathbb{Q}(\beta_2)]} \leqslant \left(\|F\|_1^{\deg_\infty(G)} \|G\|_1^{\deg_\infty(F)}\right)^{\|\mathbf{u}_1\|_1 [\mathbb{K}:\mathbb{Q}]}$$

et

$$[\mathbb{K}(\boldsymbol{\beta}) : \mathbb{K}] \leqslant 2\deg_\infty(F)\deg_\infty(G)\|\mathbf{u}_1\|_1\|\mathbf{u}_2\|_1.$$

Démonstration. On pose $P(\mathbf{y}) = F(\boldsymbol{\zeta} y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})$ et $Q(\mathbf{y}) = G(\boldsymbol{\zeta} y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}) \in \mathbb{Z}[\boldsymbol{\zeta}][y_1, y_2]$. D'après le Lemme 3.1.5, on a :

$$M(\beta_1)^{[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{Q}(\beta_1)]} \leqslant M(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P))^{\deg_{y_2}(Q)} \|G\|_1^{\deg_{y_2}(P)[\mathbb{K}:\mathbb{Q}]},$$

et

$$[\mathbb{K}(\boldsymbol{\beta}) : \mathbb{K}] \leqslant \deg_{y_1}(P)\deg_{y_2}(Q) + \deg_{y_1}(Q)\deg_{y_2}(P).$$

On note $d = [\mathbb{K} : \mathbb{Q}]$. Soient $\sigma_1, \cdots, \sigma_d$ les plongements de $\mathbb{K}$ dans $\mathbb{C}$. On a :

$$M(\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P)) \leqslant \|\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(P)\|_1 \leqslant \prod_{i=1}^{d} \|\sigma_i(P)\|_1 \leqslant \|F\|_1^d.$$

On a aussi les majorations suivantes sur les degrés :

$$\deg_{y_2}(P) \leqslant \|\mathbf{u}_1\|_1 \deg_\infty(F) \quad \text{et} \quad \deg_{y_2}(Q) \leqslant \|\mathbf{u}_2\|_1 \deg_\infty(G).$$

En combinant ces inégalités, on obtient :

$$M(\beta_1)^{[\mathbb{K}(\boldsymbol{\beta}):\mathbb{Q}(\beta_1)]} \leqslant \|F\|_1^{\deg_\infty(G)\|\mathbf{u}_2\|_1[\mathbb{K}:\mathbb{Q}]}\|G\|_1^{\deg_\infty(F)\|\mathbf{u}_2\|_1[\mathbb{K}:\mathbb{Q}]}.$$

Par symétrie, on a aussi l'inégalité pour $M(\beta_2)^{[\mathbb{K}(\boldsymbol{\beta}):\mathbb{Q}(\beta_2)]}$. Enfin, on a :

$$\begin{aligned}[\mathbb{K}(\boldsymbol{\alpha}):\mathbb{K}] &\leqslant \deg_{y_1}(P)\deg_{y_2}(Q) + \deg_{y_1}(Q)\deg_{y_2}(P)\\ &\leqslant 2\deg_\infty(F)\deg_\infty(G)\|\mathbf{u}_1\|_1\|\mathbf{u}_2\|_1.\end{aligned}$$

□

Dans la suite, on va donner une autre approche permettant de déterminer une majoration du degré des points isolés de $V(F,G)$ à l'aide du *volume mixte* et le Théorème de Bernstein-Kushnirenko [7] sur le nombre de racines communes dans $\mathbb{G}_{\mathrm{m}}^n$ (Corollaire 3.1.9). Le résultat obtenu permet de retrouver une majoration très similaire à celle de la Proposition 3.1.7.

Si E est un ensemble compact dans $\mathbb{R}^n$ alors on définit $\mathrm{diam}_2(E) = \sup_{\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2\in E}\|\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2\|_2$. Si $F \in \mathbb{C}[\mathbf{x}^{\pm 1}]$ alors on note $\mathrm{diam}_2(F) = \mathrm{diam}_2(\mathrm{Supp}(F))$. On a donc $\mathrm{diam}_2(F) \leqslant \sqrt{n}\deg_\infty(F)$. Pour montrer le Corollaire 3.1.9, on a besoin de la proposition suivante qui majore le nombre de racines communes de deux polynômes à deux variables qui sont de la forme $F(\mathbf{y}^U)$ et $G(\mathbf{y}^U)$.

Proposition 3.1.8. *Soient $F, G \in \mathbb{C}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$ non nuls. Soient $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}^n$ deux vecteurs linéairement indépendants et U la matrice dont les lignes sont $\mathbf{u}_1$ et $\mathbf{u}_2$. On suppose que $F(\mathbf{y}^U)$ et $G(\mathbf{y}^U)$ sont non nuls. On note $H(\mathbf{y}) = \mathrm{pgcd}(F(\mathbf{y}^U), G(\mathbf{y}^U))$, $P(\mathbf{y}) = F(\mathbf{y}^U)/H$ et $Q(\mathbf{y}) = G(\mathbf{y}^U)/H$. On pose :*

$$\mathcal{Z}_U = \left\{\mathbf{y} \in \mathbb{G}_{\mathrm{m}}^2 \mid P(\mathbf{y}) = Q(\mathbf{y}) = 0\right\}.$$

Alors on a :

$$\#\mathcal{Z}_U \leqslant \frac{\pi}{4}\mathrm{diam}_2(F)\mathrm{diam}_2(G)|\det(UU^\top)|^{1/2}.$$

Démonstration. Si $k > 0$ est un entier alors on désigne par Mvol_k et vol_k respectivement le volume mixte et le volume usuel dans $\mathbb{R}^k$. Pour plus de détails sur la preuve des propriétés du volume mixte mentionnées ci-dessus, on se réfère à [22]. Dans la suite, si A et B sont deux ensembles alors $A + B = \{a + b, a \in A, b \in B\}$ désigne est la somme de Minkowski. Si B n'a qu'un seul élément b alors on note par $A + b$ la somme $A + \{b\}$.

D'après le Théorème de Bernstein-Kushnirenko [7] sur le nombre de racines communes dans $\mathbb{G}_{\mathrm{m}}^2$, on a :

$$\#\mathcal{Z}_U \leqslant \mathrm{Mvol}_2\left(\mathrm{Newt}(P), \mathrm{Newt}(Q)\right).$$

Soit $\boldsymbol{\lambda}_H \in \mathrm{Newt}(H)$. On a $\mathrm{Newt}(P) + \boldsymbol{\lambda}_H \subset \mathrm{Newt}(P) + \mathrm{Newt}(H)$ où la somme est prise au sens de la somme de Minkwoski. On a donc $\mathrm{Newt}(P) + \boldsymbol{\lambda}_H \subset \mathrm{Newt}(F(\mathbf{y}^U))$. Similairement, on a $\mathrm{Newt}(Q) + \boldsymbol{\lambda}_H \subset \mathrm{Newt}(G(\mathbf{y}^U))$. Comme le volume mixte est invariant par translation, on a :

$$\mathrm{Mvol}_2\left(\mathrm{Newt}(P), \mathrm{Newt}(Q)\right) = \mathrm{Mvol}_2\left(\mathrm{Newt}(P) + \boldsymbol{\lambda}_H, \mathrm{Newt}(Q) + \boldsymbol{\lambda}_H\right).$$

Comme $\mathrm{Newt}(P)+\boldsymbol{\lambda}_H \subset \mathrm{Newt}(F(\mathbf{y}^U))$ et $\mathrm{Newt}(Q)+\boldsymbol{\lambda}_H \subset \mathrm{Newt}(G(\mathbf{y}^U))$, par monotonie du volume mixte, on en déduit que :

$$\mathrm{Mvol}_2\left(\mathrm{Newt}(P),\mathrm{Newt}(Q)\right) \leqslant \mathrm{Mvol}_2\left(F(\mathbf{y}^U),G(\mathbf{y}^U)\right).$$

Ainsi, on obtient :

$$\#\mathcal{Z}_U \leqslant \mathrm{Mvol}_2\left(\mathrm{Newt}(F(\mathbf{y}^U)),\mathrm{Newt}(G(\mathbf{y}^U))\right).$$

Comme $\mathrm{Newt}(F(\mathbf{y}^U)) \subseteq U\mathrm{Newt}(F)$ et $\mathrm{Newt}(G(\mathbf{y}^U)) \subseteq U\mathrm{Newt}(G)$, de nouveau par monotonie du volume mixte, on a :

$$\mathrm{Mvol}_2\left(\mathrm{Newt}(F(\mathbf{y}^U)),\mathrm{Newt}(G(\mathbf{y}^U))\right) \leqslant \mathrm{Mvol}_2\left(U\mathrm{Newt}(F),U\mathrm{Newt}(G)\right) \tag{3.1.2}$$

On pose $M = UU^\top \in M_2(\mathbb{Z})$. Comme U est de rang 2 alors $\det M \neq 0$. D'après le procédé d'orthonormalisation de Gram-Schmidt, il existe $W \in M_2(\mathbb{R})$ telle que $WMW^\top = I_2$. Par suite, on a :

$$\mathrm{Mvol}_2\left(U\mathrm{Newt}(F),U\mathrm{Newt}(G)\right) = |\det(W)|^{-1}\mathrm{Mvol}_2\left(WU\mathrm{Newt}(F),WU\mathrm{Newt}(G)\right). \tag{3.1.3}$$

Si $r>0$ et $\mathbf{c}\in\mathbb{R}^2$ alors on note $D(\mathbf{c},r)$ le disque de centre $\mathbf{c}$ et de rayon r. Comme $WU\mathrm{Newt}(F)$ est compact, alors il existe un réel $r_F>0$ et un vecteur $\mathbf{c}_F\in\mathbb{R}^2$ tels que $WU\mathrm{Newt}(F)$ est inclus dans le disque $D_F = D(\mathbf{c}_F,r_F)$. De même il existe un réel $r_G>0$ et $\mathbf{c}_G\in\mathbb{R}^2$ tels que $WU\mathrm{Newt}(G)\subseteq D_G = D(\mathbf{c}_G,r_G)$. En termes de la somme de Minkwoski, on peut écrire $D(\mathbf{c}_F,r_F) = \mathbf{c}_F + D(O,r_F)$ et $D(\mathbf{c}_G,r_G) = \mathbf{c}_G + D(O,r_G)$ où O est le point à l'origine $(0,0)$. On note $D_1 = D(O,1)$ le disque unité. On a alors $D(O,r_F) = r_F D(O,1)$ et $D(O,r_G) = r_G D(O,1)$. Par monotonie et invariance par translation du volume mixte, on a :

$$\begin{aligned}
\mathrm{Mvol}_2\left(WU\mathrm{Newt}(F),WU\mathrm{Newt}(G)\right) &\leqslant \mathrm{Mvol}_2\left(D_F,D_G\right)\\
&= \mathrm{Mvol}_2\left(D(O,r_F),D(O,r_G)\right)\\
&= \mathrm{Mvol}_2\left(r_F D_1, r_G D_1\right)\\
&= r_F r_G \mathrm{Mvol}_2\left(D_1,D_1\right)\\
&= r_F r_G \mathrm{vol}_2\left(D_1\right).
\end{aligned}$$

Or on a $\mathrm{vol}_2\left(D_1\right) = \pi$. Par définition, on a la majoration :

$$r_F \leqslant \frac{1}{2}\mathrm{diam}_2(WU\mathrm{Supp}(F)).$$

Comme $WMW^\top = I_2$, on a $(WU)(WU)^\top = I_2$. Ainsi WU est une isométrie et donc on a :

$$r_F \leqslant \frac{1}{2}\mathrm{diam}_2(WU\mathrm{Supp}(F)) = \frac{1}{2}\mathrm{diam}_2(F).$$

Similairement, on a le même résultat pour G. Ainsi, on obtient :

$$\mathrm{Mvol}_2\left(WU\mathrm{Newt}(F),WU\mathrm{Newt}(G)\right) \leqslant \frac{\pi}{4}\mathrm{diam}_2(F)\mathrm{diam}_2(G). \tag{3.1.4}$$

Par ailleurs, on a $\det(W)^2\det(M) = 1$ et $\det(M) = \det(UU^\top)$. On en déduit que

$$\det(W)^{-1} = |\det(UU^\top)|^{1/2}.$$

En combinant cette dernière équation avec (3.1.3) et (3.1.4), la relation (3.1.2) devient :

$$\mathrm{Mvol}_2\left(\mathrm{Newt}(F(\mathbf{y}^U)),\mathrm{Newt}(G(\mathbf{y}^U))\right) \leqslant \frac{\pi}{4}|\det(UU^\top)|^{1/2}\mathrm{diam}_2(F)\mathrm{diam}_2(G).$$

Ainsi, on a :

$$\#\mathcal{Z}_U \leqslant \frac{\pi}{4}\mathrm{diam}_2(F)\mathrm{diam}_2(G)|\det(UU^\top)|^{1/2}.$$

□

Corollaire 3.1.9. *Soient $F,G\in\mathbb{Z}[x_1^{\pm1},\cdots,x_n^{\pm1}]$. Soit $\boldsymbol{\zeta}\in\boldsymbol{\mu}_\infty^n$. On note $\mathbb{K}=\mathbb{Q}(\boldsymbol{\zeta})$. Soient $\mathbf{u}_1,\mathbf{u}_2\in\mathbb{Z}^n$ deux vecteurs linéairement indépendants. Soit U la matrice dont les lignes sont $\mathbf{u}_1$ et $\mathbf{u}_2$. Si $\boldsymbol{\beta}\in\mathbb{G}_{\mathrm{m}}^2$ est un point isolé de $V(F(\boldsymbol{\zeta}\mathbf{y}^U),G(\boldsymbol{\zeta}\mathbf{y}^U))$ alors on a :*

$$[\mathbb{K}(\boldsymbol{\beta}):\mathbb{K}] \leqslant \frac{\pi}{4}\mathrm{diam}_2(F)\mathrm{diam}_2(G)|\det(UU^\top)|^{1/2}.$$

Démonstration. On note $H(\mathbf{y})=\mathrm{pgcd}(F(\mathbf{y}^U),G(\mathbf{y}^U))$, $P(\mathbf{y})=F(\mathbf{y}^U)/H$ et $Q(\mathbf{y})=G(\mathbf{y}^U)/H$. Comme $\boldsymbol{\beta}$ un point isolé de $V(F(\boldsymbol{\zeta}\mathbf{y}^U),G(\boldsymbol{\zeta}\mathbf{y}^U))$ alors on a $P(\boldsymbol{\beta})=Q(\boldsymbol{\beta})=0$. D'après la Proposition 3.1.8, on a :

$$\#V\left(F(\boldsymbol{\zeta}\mathbf{y}^U),G(\boldsymbol{\zeta}\mathbf{y}^U)\right) \leqslant \frac{\pi}{4}\mathrm{diam}_2(F)\mathrm{diam}_2(G)|\det(UU^\top)|^{1/2}.$$

Comme tous les conjugués de $\boldsymbol{\beta}$ sur $\mathbb{K}$ appartiennent à $V(F(\boldsymbol{\zeta}\mathbf{y}^U),G(\boldsymbol{\zeta}\mathbf{y}^U))$, on a :

$$[\mathbb{K}(\boldsymbol{\beta}):\mathbb{K}] \leqslant \frac{\pi}{4}\mathrm{diam}_2(F)\mathrm{diam}_2(G)|\det(UU^\top)|^{1/2}.$$

□

Remarque. En observant que $\det(UU^\top)^{1/2}\leqslant\|\mathbf{u}_1\|_2\|\mathbf{u}_2\|_2$, on retrouve une majoration similaire à celle de la Proposition 3.1.7 pour $[\mathbb{K}(\boldsymbol{\beta}):\mathbb{K}]$.

3.2 Version explicite de la Conjecture de Schinzel

En combinant les résultats précédemment obtenus, on peut maintenant établir une version explicite de la Conjecture de Schinzel pour le cas $n=2$. On rappelle que la fonction ℓ est définie à l'équation (1.2.3) à la page 5, à la fin de la Section 1.2.2 du Chapitre 1.

Théorème 3.2.1. *Soient $F,G\in\mathbb{Z}[x_1^{\pm1},x_2^{\pm1}]$. Soient $\mathbf{a}\in\mathbb{Z}^2$ un vecteur primitif, $\boldsymbol{\zeta}\in\boldsymbol{\mu}_\infty^2$ et $\xi\in\overline{\mathbb{Q}}^*\backslash\boldsymbol{\mu}_\infty$. On note $\boldsymbol{\alpha}=\boldsymbol{\zeta}\xi^{\mathbf{a}}$ et $d=[\mathbb{Q}(\boldsymbol{\alpha}):\mathbb{Q}]$. Si $\boldsymbol{\alpha}$ est un point isolé de $V(F,G)$ alors on a :*

$$|a_1| \leqslant \left(\deg_{x_2}(G)\log M(F)+\deg_{x_2}(F)\log\|G\|_1\right)\ell(d),$$

$$|a_2| \leqslant \left(\deg_{x_1}(G)\log M(F)+\deg_{x_1}(F)\log\|G\|_1\right)\ell(d)$$

et

$$d \leqslant \deg_{x_1}(F)\deg_{x_2}(G)+\deg_{x_1}(G)\deg_{x_2}(F).$$

Remarques. (**1**) Si $\mathbf{a}$ n'est pas primitif alors ces majorations restent vraies en remplaçant a_i par $a_i/\operatorname{pgcd}(a_1,a_2)$. Cela correspond à remplacer ξ par $\xi^{\operatorname{pgcd}(a_1,a_2)}$ dans la preuve.

(**2**) D'après la Proposition 1.3.2.1, on peut supposer $\boldsymbol{\zeta},\xi\in\mathbb{Q}(\boldsymbol{\alpha})$. Comme $[\mathbb{Q}(\boldsymbol{\alpha}):\mathbb{Q}]$ est majoré par une constante ne dépendant que de F et G, il est en de même pour $[\mathbb{Q}(\boldsymbol{\zeta}):\mathbb{Q}]$. Par suite, il n'y a qu'un nombre fini de $\boldsymbol{\zeta}\in\boldsymbol{\mu}_\infty^2$ à considérer.

Démonstration. On a $\boldsymbol{\alpha}=(\zeta_1\xi^{a_1},\zeta_2\xi^{a_2})$. D'après la Proposition 1.3.2.1, on peut supposer $\xi\in\mathbb{Q}(\boldsymbol{\alpha})$. Comme $\zeta_1\in\boldsymbol{\mu}_\infty$, on a :

$$h(\alpha_1)=h(\zeta_1\xi^{a_1})=h(\xi^{a_1})=|a_1|h(\xi).$$

Puisque $0\neq\xi\notin\boldsymbol{\mu}_\infty$, on a $h(\xi)\neq 0$. Par suite, on a :

$$|a_1|=\frac{h(\alpha_1)}{h(\xi)}=\frac{[\mathbb{Q}(\xi):\mathbb{Q}]}{\log M(\xi)}\frac{\log M(\alpha_1)}{[\mathbb{Q}(\alpha_1):\mathbb{Q}]}.$$

Comme $\xi\in\mathbb{Q}(\boldsymbol{\alpha})$, on a :

$$[\mathbb{Q}(\xi):\mathbb{Q}]\leqslant[\mathbb{Q}(\boldsymbol{\alpha}):\mathbb{Q}].$$

On obtient donc :

$$|a_1|\leqslant[\mathbb{Q}(\boldsymbol{\alpha}):\mathbb{Q}(\alpha_1)]\log M(\alpha_1)\frac{1}{\log M(\xi)}. \tag{3.2.1}$$

Puisque $\boldsymbol{\alpha}$ est un point isolé de $V(F,G)$, d'après la Proposition 3.1.6, on a :

$$[\mathbb{Q}(\boldsymbol{\alpha}):\mathbb{Q}(\alpha_1)]\log M(\alpha_1)\leqslant\deg_{x_2}(G)\log M(F)+\deg_{x_2}(F)\log\|G\|_1 \tag{3.2.2}$$

et

$$[\mathbb{Q}(\boldsymbol{\alpha}):\mathbb{Q}]\leqslant\deg_{x_1}(F)\deg_{x_2}(G)+\deg_{x_1}(G)\deg_{x_2}(F).$$

Comme la fonction ℓ est croissante, on a :

$$\frac{1}{\log M(\xi)}\leqslant\ell([\mathbb{Q}(\xi):\mathbb{Q}])\leqslant\ell(d). \tag{3.2.3}$$

En combinant (3.2.2) et (3.2.3), l'inégalité (3.2.1) devient :

$$|a_1|\leqslant\left(\deg_{x_2}(G)\log M(F)+\deg_{x_2}(F)\log\|G\|_1\right)\ell(d).$$

On a l'inégalité similaire pour $|a_2|$. □

Remarques. (**1**) Comme déjà remarqué par Schinzel, la borne pour le vecteur $\mathbf{a}$ ne peut pas dépendre uniquement des degrés de F et G. Par exemple, si $F(x_1,x_2)=x_1-2$, $G(x_1,x_2)=x_2-2^a$ et $\boldsymbol{\alpha}=(2,2^a)$ alors $\mathbf{a}=(a,-1)$ et en particulier, $\|\mathbf{a}\|_\infty=a$.

(**2**) On remarque que si la conjecture de Lehmer forte (Conjecture 1.2.2.4) est vraie alors pour tout $\alpha\in\overline{\mathbb{Q}}^*\setminus\boldsymbol{\mu}_\infty$, on a :

$$M(\alpha)\geqslant M(x^{10}+x^9-x^7-x^6-x^5-x^4-x^3+x+1)\approx 1,176280818...$$

Cela permettrait de remplacer $\ell(d)$ par $\ell(10) \leqslant 6,15925$ dans le Théorème 3.2.1. Si on ne s'intéresse qu'aux $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^2$ dont les coordonnées ne sont pas des unités algébriques (donc ξ n'est pas non plus une unité algébrique) alors on a $M(\xi) \geqslant 2$. Cela permet de remplacer $\ell(d)$ par $\ell(1) \leqslant 1,44270$.

(**3**) En utilisant le Théorème de Bernstein-Kushnirenko [7] qui affirme que le nombre de racines communes de F et G dans $\mathbb{C}^{*2}$ est égal au volume mixte des polygones de Newton de F et G, on peut remplacer la majoration obtenue pour d par ce volume mixte.

Une version explicite du Théorème 2 pour $n = 2$ peut se déduire directement à partir du corollaire suivant.

Corollaire 3.2.2. *Soient $F_1, \ldots, F_s \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}]$. Soient $\mathbf{a} \in \mathbb{Z}^2$ un vecteur non nul, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^2$ et $\xi \in \mathbb{G}_{\mathrm{m}} \setminus \boldsymbol{\mu}_\infty$. Si $\boldsymbol{\zeta}\xi^{\mathbf{a}}$ est un point isolé de $V(F_1, \cdots, F_s)$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^2$ orthogonal à $\mathbf{a}$ tel que :*

$$\|\mathbf{b}\|_\infty \leqslant 2Dh\ell(2D^2),$$

où

$$D = \max_{1 \leqslant i \leqslant s} \deg_\infty(F_i) \quad \textit{et} \quad h = \max_{1 \leqslant i \leqslant s} \log \|F_i\|_1.$$

Démonstration. On pose $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$ et $d = [\mathbb{Q}(\boldsymbol{\alpha}) : \mathbb{Q}]$. Comme $\boldsymbol{\alpha}$ est un point isolé de $V(F_1, \cdots, F_s)$, d'après le Lemme 3.1.4, il existe $i \neq j \in \{1, \cdots, s\}$ et un facteur irréductible S_i de F_i tels que $\boldsymbol{\alpha} \in V(S_i, F_j)$ et $\operatorname{pgcd}(S_i, F_j) = 1$. D'après le Théorème 3.2.1, on a :

$$\frac{|a_1|}{\operatorname{pgcd}(a_1, a_2)} \leqslant \left(\deg_{x_2}(F_j) \log M(S_i) + \deg_{x_2}(S_i) \log \|F_j\|_1\right) \ell(d)$$

et

$$\frac{|a_1|}{\operatorname{pgcd}(a_1, a_2)} \leqslant \left(\deg_{x_1}(F_j) \log M(S_i) + \deg_{x_1}(S_i) \log \|F_j\|_1\right) \ell(d)$$

avec

$$d \leqslant \deg_{x_1}(S_i) \deg_{x_2}(F_j) + \deg_{x_1}(F_j) \deg_{x_2}(S_i).$$

On note $\mathbf{b}$ le vecteur dont les coordonnées sont définies par :

$$b_1 = \frac{a_2}{\operatorname{pgcd}(a_1, a_2)} \quad \text{et} \quad b_2 = \frac{-a_1}{\operatorname{pgcd}(a_1, a_2)}.$$

Par construction, $\mathbf{b}$ est orthogonal à $\mathbf{a}$. Puisque S_i divise F_i, d'après la majoration (1.2.1), on a :

$$M(S_i) \leqslant M(F_i) \leqslant \|F_i\|_1.$$

On obtient :

$$\|\mathbf{b}\|_\infty \leqslant 2Dh\ell(d)$$

et

$$d \leqslant \deg_{x_1}(F_i) \deg_{x_2}(F_j) + \deg_{x_1}(F_j) \deg_{x_2}(F_i) \leqslant 2D^2.$$

On a la majoration voulue car ℓ est croissante. □

3.3 Exemples et applications

Les exemples ci-après illustrent quelques applications du Théorème 3.2.1 pour le calcul du pgcd de deux polynômes qui sont des spécialisations en une variable deux polynômes à deux variables.

Les calculs suivants sont faits en Pari/GP et sur un ordinateur ayant les caractéristiques suivantes :

— Processeur : ® Core™ i5-8265U CPU @1.60GHz× 8
— RAM : 16GB.

Exemple 3.3.1. On considère les deux polynômes lacunaires F et G :

$$F(x_1,x_2) = 2606 + 2023x_1^{2543}x_2^{567} + 1010x_1^{5321}x_2^{4560} - 2020x_1^{1234}x_2^{2789},$$
$$G(x_1,x_2) = 6062 + 3202x_1^{5427}x_2^{2345} + 1001x_1^{3123}x_2^{4321}.$$

On choisit $\mathbf{a} = (800000000, -1234567) \in \mathbb{Z}^2$. On cherche à déterminer si les deux polynômes f et g suivants :

$$f(t) = F(t^{\mathbf{a}}) = 2606 + 2023t^{202740000511} + 1010t^{420050374480} - 2020t^{95276792637},$$
$$g(t) = G(t^{\mathbf{a}}) = 6062 + 3202t^{431264940385} + 1001t^{244505435993}.$$

ont un facteur commun non cyclotomique. On a $\mathrm{pgcd}(a_1,a_2) = 1$. Pour utiliser le Théorème 3.2.1, il faut montrer $\mathrm{pgcd}(F,G) = 1$. On note $D = \mathrm{pgcd}(F,G)$. D'après le Lemme 1.5.1, toute arête de $\mathrm{Newt}(D)$ est parallèle à une arête de $\mathrm{Newt}(F)$ et à une arête de $\mathrm{Newt}(G)$. Ainsi, si D n'est pas un monôme alors $\mathrm{Newt}(F)$ a une arête qui est parrallèle à une arête de $\mathrm{Newt}(G)$. En traçant ces deux polygones dans le plan (voir Figure 3.3.1), on observe que ce n'est pas le cas et ainsi $\mathrm{pgcd}(F,G) = 1$.

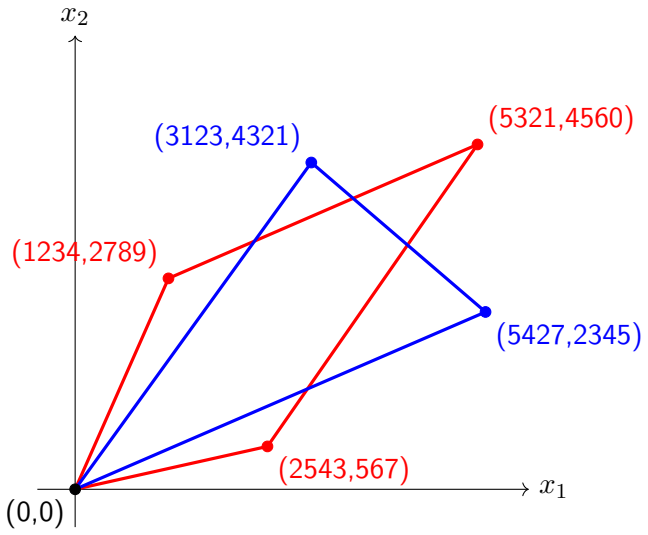

FIGURE 3.3.1 – Polygônes de Newton de F (en rouge) et G (en bleu)

Maintenant, d'après le Théorème 3.2.1, si $F(t^{\mathbf{a}})$ et $G(t^{\mathbf{a}})$ ont un facteur commun non-cyclotomique alors $|a_1| \leqslant 75341516$ et $|a_2| \leqslant 91126127$. Puisque $|a_1| > 75341516$, on en déduit que f et g n'ont aucun facteur commun non cyclotomique.

Exemple 3.3.2. On définit les deux polynômes F et G :

$$F(x_1, x_2) = -1 + 27x_2^3 + 27x_1^3x_2^3 + 27x_1x_2^2,$$
$$G(x_1, x_2) = -3 - x_1 + 9x_2 - 6x_1x_2 - 3x_1^2x_2.$$

On cherche à déterminer les vecteurs $(u, v) \in \mathbb{Z}^2$ pour lesquels les deux polynômes suivants :

$$f_{u,v}(t) = F(t^u, t^v) = -1 + 27t^{3v} + 27t^{3u+3v} + 27t^{u+2v},$$
$$g_{u,v}(t) = G(t^u, t^v) = -3 - t^u + 9t^v - 6t^{u+v} - 3t^{2u+v}$$

ont un facteur commun non-cyclotomique.

En calculant sur Pari/GP (ou en utilisant le Théorème d'Ostrowski comme dans l'exemple précédent), on trouve $\mathrm{pgcd}(F, G) = 1$. D'après le Théorème 3.2.1, le problème est réduit à calculer le pgcd de $f_{u,v}$ et $g_{u,v}$ pour tout vecteur primitif $(u, v) \in \mathbb{Z}^2$ vérifiant $|u| \leqslant 52$ et $|v| \leqslant 66$. En faisant ce calcul sur Pari/GP, on déduit qu'aucun vecteur ne donne un pgcd non trivial en environ 0,9s.

On cherche ensuite à déterminer les points de torsion $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^2$ pour lesquels les deux polynômes $F(\zeta_1 t^u, \zeta_2 t^v)$ et $G(\zeta_1 t^u, \zeta_2 t^v)$ ont un facteur commun non-cyclotomique. Si tel est le cas alors, de nouveau d'après le Théorème 3.2.1 et la remarque qui le suit, les bornes pour u et v restent les mêmes et de plus, on a $[\mathbb{Q}(\boldsymbol{\zeta}) : \mathbb{Q}] \leqslant 9$ (en particulier, il n'y a qu'un nombre fini de $\boldsymbol{\zeta}$ à considérer). Le Tableau 3.1 suivant donne quelques exemples de points de torsion $\boldsymbol{\zeta}$ et de vecteurs (u, v) primitifs pour lesquels ces deux polynômes ont un facteur commun non-cyclotomique.

$\boldsymbol{\zeta}$	(u, v)	pgcd	Temps de calcul
$(1, -1)$	$\pm(1, -2)$	$t^2 - 3t + 3$	0,9s
$(-1, -1)$	$\pm(1, -2)$	$t^2 + 3t + 3$	0,9s
$(i, 1)$	$\pm(1, -2)$	$t^2 + 3it - 3$	6,4s

Tableau 3.1 – Quelques points de torsion

3.4 Algorithme

Au lieu de passer par une recherche exhaustive en utilisant la borne, on propose ici un algorithme permettant de calculer explicitement les vecteurs $\mathbf{a}$ vérifiant les propriétés requises en utilisant les zéros communs de F et G.

Algorithme 10 :

Entrée : $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}]$ tels que $\gcd(F,G) = 1$.

Sortie : une liste finie $A \subset (\mathbb{G}_{\mathrm{m}}^2 \setminus \boldsymbol{\mu}_\infty^2) \times \mathbb{Z}^2$.

Résoudre dans $\mathbb{G}_{\mathrm{m}}^2$ le système $F(\boldsymbol{\alpha}) = G(\boldsymbol{\alpha}) = 0$ et noter $V(F,G)$ l'ensemble des solutions.
Pour chaque $\boldsymbol{\alpha} \in V(F,G)$:
    calculer une base $R_f(\boldsymbol{\alpha})$ en appliquant l'Algorithme 6 ;
    si $\dim(R_f(\boldsymbol{\alpha})) = 1$ alors :
        noter $\mathbf{b} \in \mathbb{Z}^2$ un générateur de $R_f(\boldsymbol{\alpha})$ et poser $\mathbf{a} = (b_2, -b_1)$;
        mettre $(\boldsymbol{\alpha}, \mathbf{a})$ dans A.
Renvoyer A.

Remarque. Pour le calcul de $V(F,G)$, on utilise la méthode standard avec le résultant. On commence par calculer le résultant $R_1(x_2)$ de F et G par rapport à x_1. On factorise R_1 dans $\mathbb{Q}[x_2]$. Pour chaque facteur irréductible $P_i \in \mathbb{Z}[x_2]$ de R_1, on note $\alpha_{2,i}$ le nombre algébrique dont le polynôme minimal est P_i et on calcule $D_i = \gcd(F(x_1, \alpha_{2,i}), G(x_1, \alpha_{2,i}))$. On factorise D_i dans $\mathbb{Q}(\alpha_{2,i})[x_1]$. Pour chaque facteur $Q_{i,j} \in \mathbb{Q}(\alpha_{2,i})[x_1]$ de D_i, on note $\alpha_{1,i,j}$ le nombre algébrique dont le polynôme minimal sur $\mathbb{Q}(\alpha_{2,i})$ est $Q_{i,j}$. Ainsi, on trouve $V(F,G) = \bigcup_{i,j}(\alpha_{1,i,j}, \alpha_{2,i})$. L'Algorithme 10 a été implémenté en PARI/GP.

Proposition 3.4.1. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}]$ tels que $\gcd(F,G) = 1$. L'Algorithme 10 termine et renvoie une liste finie $A \subset (\mathbb{G}_{\mathrm{m}}^2 \setminus \boldsymbol{\mu}_\infty^2) \times \mathbb{Z}^2$ vérifiant la propriété suivante : $(\boldsymbol{\alpha}, \pm\mathbf{a}) \in A$ si et seulement si $\boldsymbol{\alpha} \in V(F,G)$ et $\boldsymbol{\alpha}$ est de la forme $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$ où $\mathbf{a} \in \mathbb{Z}^2$ est primitif, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^2$ et $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$.*

Démonstration. Comme $\gcd(F,G) = 1$, $V(F,G)$ est fini et donc cet algorithme termine après un nombre fini d'étapes. Montrons que la sortie vérifie les propriétés annoncées.

Supposons que $(\boldsymbol{\alpha}, \mathbf{a}) \in A$. Posons $\boldsymbol{\zeta} = \mu^{\mathbf{u}}$ et $\xi = \alpha_1^{u_2}\alpha_2^{-u_1}$ où $\mu = \boldsymbol{\alpha}^{\mathbf{b}} \in \boldsymbol{\mu}_\infty$, $\mathbf{u} = (u_1, u_2) \in \mathbb{Z}^2$ tel que $u_1 b_1 + u_2 b_2 = 1$ et $\mathbf{b} = (-a_2, a_1)$. On a :

$$\begin{aligned}
\boldsymbol{\zeta}\xi^{\mathbf{a}} &= (\mu^{u_1}\xi^{a_1}, \mu^{u_2}\xi^{a_2}) \\
&= \left((\alpha_1^{b_1}\alpha_2^{b_2})^{u_1}(\alpha_1^{u_2}\alpha_2^{-u_1})^{b_2}, (\alpha_1^{b_1}\alpha_2^{b_2})^{u_2}(\alpha_1^{u_2}\alpha_2^{-u_1})^{-b_1}\right) \\
&= \left(\alpha_1^{b_1u_1+u_2b_2}\alpha_2^{b_2u_1-u_1b_2}, (\alpha_1^{b_1u_2-u_2b_1}\alpha_2^{b_2u_2+u_1b_1}\right) \\
&= \boldsymbol{\alpha} \quad \text{car} \quad u_1b_1 + u_2b_2 = 1.
\end{aligned}$$

Réciproquement, si $\boldsymbol{\alpha} \in V(F,G)$ de la forme $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$ où $\mathbf{a} \in \mathbb{Z}^2$ est primitif, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^2$ et $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$ alors on a $R_f(\boldsymbol{\alpha}) = \mathbf{a}^\perp$. □

Remarque. En observant cette démonstration, on a $\mathbb{Q}(\boldsymbol{\zeta}, \xi) = \mathbb{Q}(\boldsymbol{\alpha})$ comme annoncé dans la Proposition 1.3.2.1.

Exemple 3.4.2. On reprend les deux polynômes F et G définis dans l'Exemple 3.3.2 :

$$\begin{aligned}
F(x_1, x_2) &= -1 + 27x_2^3 + 27x_1^3x_2^3 + 27x_1x_2^2, \\
G(x_1, x_2) &= -3 - x_1 + 9x_2 - 6x_1x_2 - 3x_1^2x_2.
\end{aligned}$$

On cherche à déterminer l'ensemble des couples $(\boldsymbol{\alpha}, \pm\mathbf{a}) \in A$ tels que $\mathbf{a} \in \mathbb{Z}^2$ est primitif et $\boldsymbol{\alpha} \in V(F,G)$ de la forme $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$ où $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^2$ et $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$. En appliquant l'Algorithme 10, on trouve $A = \{(\alpha_1, \alpha_2), \pm(1,-2)\}$ où α_1 est le nombre algébrique dont le polynôme minimal est $P_1 = x^2 - 3x + 3$ et α_2 celui dont le polynôme minimal est $P_2 = 9x^2 + 3x + 1$ en 2ms.

Exemple 3.4.3. On considère les deux polynômes F et G :

$$F(x_1, x_2) = -123 + 456x_2^{13} + 789x_1^3x_2^5 + 10123x_1x_2^2,$$
$$G(x_1, x_2) = -90807 - x_1^7 + 605x_2^3 - 403x_1x_2 - 201x_1^2x_2^7;.$$

On cherche à déterminer l'ensemble des couples $(\boldsymbol{\alpha}, \pm\mathbf{a}) \in A$ tels que $\mathbf{a} \in \mathbb{Z}^2$ est primitif et $\boldsymbol{\alpha} \in V(F,G)$ de la forme $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$ où $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^2$ et $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$. En appliquant l'Algorithme 10, on trouve $A = \emptyset$ en 0,7s.

Si on avait utilisé la méthode avec les bornes, on aurait calculé le $\gcd$ de $F(t^{\mathbf{a}})$ et $G(t^{\mathbf{a}})$ pour tout vecteur primitif $\mathbf{a}$ vérifiant $|a_1| \leqslant 20978$ et $|a_2| \leqslant 9728$. Avec ces bornes, le temps de calcul prend environ 328h (soit 13jours et une demi-journée) sur notre machine.

Remarque. En essayant sur plusieurs exemples, on remarque que l'essentiel du temps passé par l'Algorithme 10 se trouve dans le calcul des racines communes de F et G, et plus précisément dans l'étape où on effectue un calcul de $\gcd$ de deux polynômes sur un corps de nombres.

4. Cas $n = 3$: approche S

Dans ce chapitre, on présente une version explicite du Théorème 2 dans le cas où $n = 3$ et $\boldsymbol{\zeta} = \mathbf{1}$ (Théorème 4.4.1), basée sur une amélioration de la preuve de A. Schinzel [40, Theorem 45], que l'on appelle *approche S*.

4.1 Présentation de l'approche

Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\mathrm{pgcd}(F, G) = 1$. Soient $\mathbf{a} \in \mathbb{Z}^3$ et $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$ tels que $F(\xi^{\mathbf{a}}) = G(\xi^{\mathbf{a}}) = 0$. Soient $\mathbf{u}_1, \mathbf{u}_2$ deux vecteurs linéairement indépendants tels que $\mathbf{a} \in \langle \mathbf{u}_1, \mathbf{u}_2 \rangle$ (on peut appliquer le Lemme 1.4.2 pour montrer l'existence de tels vecteurs). On suppose de plus que $\|\mathbf{u}_1\|_\infty \|\mathbf{u}_2\|_\infty$ est minimal. On note $H(y_1, y_2) = \mathrm{pgcd}(F(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}), G(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}))$. On commence par considérer les deux cas suivants : H est un monôme ou H n'est pas un monôme.

Si H n'est pas un monôme alors, grâce au Lemme 1.5.1, on montre qu'il existe un vecteur $\mathbf{b}$ satisfaisant les propriétés requises (Proposition 4.2.1).

En revanche, si H est un monôme alors cela implique que le degré de ξ peut être contrôlé par $\|\mathbf{a}\|^{1/2}$ (Proposition 4.3.1). Le fait que cette puissance de $\|\mathbf{a}\|_2$ est strictement inférieure à 1 est crucial. Pour trouver un vecteur $\mathbf{b}$ vérifiant les propriétés requises, on fait une *décomposition* de F et G suivant la construction suivante.

Matrice associée à un polynôme

Si $0 \neq P \in \mathbb{C}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$ alors on écrit :

$$P = p_{\boldsymbol{\lambda}_1} \mathbf{x}^{\boldsymbol{\lambda}_1} + \cdots + p_{\boldsymbol{\lambda}_{n_P}} \mathbf{x}^{\boldsymbol{\lambda}_{n_P}},$$

où les $p_{\boldsymbol{\lambda}_i}$ sont les coefficients non nuls de P, $n_P = \#\mathrm{Supp}(P)$ et les vecteurs $\boldsymbol{\lambda}_i \in \mathrm{Supp}(P)$ sont ordonnés suivant l'ordre lexicographique : $\boldsymbol{\lambda}_1 < \cdots < \boldsymbol{\lambda}_{n_P}$. La matrice $\mathcal{M}(P)$ associée à P est définie par :

$$\mathcal{M}(P) = (\boldsymbol{\lambda}_{i,j} - \boldsymbol{\lambda}_{1,j})_{\substack{2 \leqslant i \leqslant n_P \\ 1 \leqslant j \leqslant n}} \in M_{n, n_P - 1}(\mathbb{Z}).$$

Matrice associée à une décomposition de F et G

Une *décomposition σ de F et G suivant $\xi^{\mathbf{a}}$* est une représentation de F et G sous la forme :

$$\sigma : \ F = \sum_{i=1}^{p} F_i \quad \text{et} \quad G = \sum_{j=1}^{q} G_i, \tag{4.1.1}$$

tels que

- les F_i et les G_j sont non nuls,
- $\mathrm{Supp}(F_i) \cap \mathrm{Supp}(F_j) = \mathrm{Supp}(G_i) \cap \mathrm{Supp}(G_j) = \emptyset$ pour $i \neq j$,
- $F_i(\xi^{\mathbf{a}}) = G_j(\xi^{\mathbf{a}}) = 0$ pour $1 \leqslant i \leqslant p$ et $1 \leqslant j \leqslant q$.

On associe à σ la matrice $\mathcal{M}_\sigma$ définie par :

$$\mathcal{M}_\sigma = \begin{pmatrix} \mathcal{M}(F_1) & \cdots & \mathcal{M}(F_p) & \mathcal{M}(G_1) & \cdots & \mathcal{M}(G_q) \end{pmatrix} \in M_{3,m}(\mathbb{Z}),$$

où $m = (n_{F_1} - 1) + \cdots (n_{F_p} - 1) + (n_{G_1} - 1) + \cdots + (n_{G_q} - 1)$.

On considère une telle décomposition σ de F et G telle que p et q soient maximaux. Dans ce cas, on dit que la décomposition est maximale. On note r_σ le rang du sous groupe Λ de $\mathbb{Z}^3$ engendré par les vecteurs colonnes de $\mathcal{M}_\sigma$. On considère les deux cas : $r_\sigma = 3$ et $r_\sigma \leqslant 2$.

Si $r_\sigma = 3$ et sous l'hypothèse que le degré de ξ est contrôlé par $\|\mathbf{a}\|_2^{1/2}$, on montre que la norme de $\mathbf{a}$ est majorée par une constante ne dépendant que de F et G (Proposition 4.3.3). Ensuite, pour déduire un vecteur $\mathbf{b}$ ayant les propriétés requises, il suffit d'appliquer le Théorème 1.4.1 à $\mathbf{a}^\perp$.

Si $r_\sigma \leqslant 2$ alors, en se ramenant au cas $n = 2$, on montre qu'il existe un vecteur $\mathbf{b}$ ayant les propriétés requises (Proposition 4.3.4). Dans cette proposition, l'hypothèse que le degré de ξ est contrôlé par $\|\mathbf{a}\|_2^{1/2}$ n'est pas nécessaire.

Le Tableau 4.1 suivant récapitule le schéma de la preuve :

Hypothèses	$r_\sigma = 3$	$r_\sigma \leqslant 2$
H est un monôme	Proposition 4.3.3	Proposition 4.3.4
H n'est pas un monôme	Proposition 4.2.1	Proposition 4.2.1 ou Proposition 4.3.4

Tableau 4.1 – Schéma de l'approche S

On note :

$$\begin{aligned} D &= \max\left(\deg_\infty(F), \deg_\infty(G)\right) \\ h &= \max(\log \|F\|_1, \log \|G\|_1) \\ N &= \max(\#\mathrm{Supp}(F), \#\mathrm{Supp}(G)). \end{aligned}$$

Le Tableau 4.2 donne asymptotiquement l'ordre de grandeur des bornes associées aux différents cas.

Hypothèses	$r_\sigma = 3$	$r_\sigma \leqslant 2$
H est un monôme	ND^4	D^5h
H n'est pas un monôme	D^6	D^6 ou D^5h

Tableau 4.2 – Ordre de grandeur des bornes suivant l'approche S

Dans la Section 4.2 et la Section 4.3, on traite respectivement les deux cas : H n'est pas un monôme puis H est un monôme. Dans la Section 4.4, on donne une version explicite du Théorème 2 dans le cas $n = 3$.

4.2 Cas 1 : $H(\mathbf{y})$ n'est pas un monôme

La proposition suivante montre que si H n'est pas un monôme alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ et dont la norme est majorée par une constante ne dépendant que de $\deg(F)$ et $\deg(G)$.

Proposition 4.2.1. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\operatorname{pgcd}(F, G) = 1$. Soient $\mathbf{a} \in \mathbb{Z}^3$ un vecteur primitif et $\xi \in \overline{\mathbb{Q}} \setminus \boldsymbol{\mu}_\infty$ tels que $F(\xi^{\mathbf{a}}) = G(\xi^{\mathbf{a}}) = 0$. Soient $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}^3$ deux vecteurs linéairement indépendants tels que $\mathbf{a} \in \langle \mathbf{u}_1, \mathbf{u}_2 \rangle$ et $\|\mathbf{u}_1\|_\infty \|\mathbf{u}_2\|_\infty$ est minimal. Si $\operatorname{pgcd}(F(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}), G(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}))$ n'est pas un monôme alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :*

$$\|\mathbf{b}\|_\infty \leqslant 48 \left(\deg_\infty(F) \deg_\infty(G) \min\left(\deg_\infty(F), \deg_\infty(G)\right)\right)^2.$$

Démonstration. Quitte à renuméroter les $\mathbf{u}_i$, on peut supposer que $\|\mathbf{u}_1\|_\infty \leqslant \|\mathbf{u}_2\|_\infty$. On note $H(y_1, y_2) = \operatorname{pgcd}(F(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}), G(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}))$. Comme H n'est pas un monôme, $\operatorname{Newt}(H)$ possède une arête A. On note L la droite qui passe par cette arête et $(c_1, c_2) \in \mathbb{Z}^2$ un vecteur normal à L. On écrit :

$$F(\mathbf{x}) = \sum_{\boldsymbol{\lambda} \in \operatorname{Supp}(F)} f_{\boldsymbol{\lambda}} \mathbf{x}^{\boldsymbol{\lambda}} \quad \text{et} \quad H(\mathbf{y}) = \sum_{\boldsymbol{\alpha} \in \operatorname{Supp}(H)} h_{\boldsymbol{\alpha}} \mathbf{y}^{\boldsymbol{\alpha}}.$$

On définit les deux polynômes de facette (suivant L) :

$$F_{\mathrm{L}}(\mathbf{y}) = \sum_{\boldsymbol{\lambda} \in \operatorname{Supp}(F) \mid (\mathbf{u}_1 \boldsymbol{\lambda}, \mathbf{u}_2 \boldsymbol{\lambda}) \in \mathrm{L}} f_{\boldsymbol{\lambda}} y_1^{\mathbf{u}_1 \boldsymbol{\lambda}} y_2^{\mathbf{u}_2 \boldsymbol{\lambda}} \quad \text{et} \quad H_{\mathrm{L}}(\mathbf{y}) = \sum_{\boldsymbol{\alpha} \in \operatorname{Supp}(H) \cap \mathrm{L}} h_{\boldsymbol{\alpha}} \mathbf{y}^{\boldsymbol{\alpha}}.$$

En considérant l'application linéaire $\mathcal{L}(z_1, z_2) = c_1 z_1 + c_2 z_2$ et en utilisant le Lemme 1.5.1, H_{L} divise $F_{\mathrm{L}}(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})$ car H divise $F(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})$. Comme L contient au moins deux points de $\operatorname{Supp}(H)$, H_{L} possède au moins deux monômes. Ainsi, il en est de même pour F_{L}. Par suite, il existe $\boldsymbol{\lambda}_1 \neq \boldsymbol{\lambda}_2 \in \operatorname{Supp}(F)$ tels que $c_1 \mathbf{u}_1 (\boldsymbol{\lambda}_2 - \boldsymbol{\lambda}_1) + c_2 \mathbf{u}_2 (\boldsymbol{\lambda}_2 - \boldsymbol{\lambda}_1) = 0$. En posant $\mathbf{v}_1 = \boldsymbol{\lambda}_2 - \boldsymbol{\lambda}_1$, on a :

$$c_1 \mathbf{u}_1 \mathbf{v}_1 + c_2 \mathbf{u}_2 \mathbf{v}_1 = 0 \quad \text{et} \quad 0 < \|\mathbf{v}_1\|_\infty \leqslant \deg_\infty(F). \tag{4.2.1}$$

Puisque H divise $G(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})$, on a aussi des propriétés similaires avec G. Ainsi, on peut remplacer $\deg_\infty(F)$ par $\deg_\infty(G)$ dans (4.2.1).

Comme $\mathbf{v}_1 \neq \mathbf{0}$, alors il existe $k \in \{1, 2, 3\}$ tel que $v_{1k} \neq 0$. Pour alléger les notations, on suppose $k = 3$. Notons R le résultant de F et G par rapport à la variable x_3. Comme $\operatorname{pgcd}(F, G) = 1$, on a $R \neq 0$. En utilisant la matrice de Sylvester pour le calcul du résultant, on en déduit :

$$\deg_\infty(R) \leqslant 2 \deg_\infty(F) \deg_\infty(G).$$

De plus, il existe $R_1, R_2 \in \mathbb{Q}[x_1, x_2, x_3]$ tels que $R = R_1 F + R_2 G,$. Puisque H divise $F(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})$ et $G(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})$, donc il divise $R(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})$. En appliquant la même procédé, il existe deux vecteurs $\boldsymbol{\lambda}'_1 \neq \boldsymbol{\lambda}'_2 \in \operatorname{Supp}(R)$ tels que $c_1 \mathbf{u}_1 (\boldsymbol{\lambda}'_2 - \boldsymbol{\lambda}'_1) + c_2 \mathbf{u}_2 (\boldsymbol{\lambda}'_2 - \boldsymbol{\lambda}'_1) = 0$. La 3ème coordonnée de $\boldsymbol{\lambda}'_1$ et celle de $\boldsymbol{\lambda}'_2$ sont nulles car $\deg_{x_3}(R) = 0$. En posant $\mathbf{v}_2 = \boldsymbol{\lambda}'_2 - \boldsymbol{\lambda}'_1$, on a :

$$c_1 \mathbf{u}_1 \mathbf{v}_2 + c_2 \mathbf{u}_2 \mathbf{v}_2 = 0 \quad \text{et } 0 < \|\mathbf{v}_2\|_\infty \leqslant \deg_\infty(R) \leqslant 2 \deg_\infty(F) \deg_\infty(G). \tag{4.2.2}$$

En combinant (4.2.1) et (4.2.2), on obtient la relation :

$$(\mathbf{u}_1 \mathbf{v}_1)(\mathbf{u}_2 \mathbf{v}_2) = (\mathbf{u}_2 \mathbf{v}_1)(\mathbf{u}_1 \mathbf{v}_2). \tag{4.2.3}$$

Par ailleurs, les vecteurs $\mathbf{v}_1$ et $\mathbf{v}_2$ sont linéairement indépendants car si $d_1 \mathbf{v}_1 + d_2 \mathbf{v}_2 = 0$ où $d_1, d_2 \in \mathbb{Z}$ alors $d_1 = 0$ ($v_{23} = 0$ et $v_{13} \neq 0$) et $d_2 = 0$ ($\mathbf{v}_2 \neq \mathbf{0}$).

En résumé, il existe deux vecteurs $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{Z}^n$ linéairement indépendants tels que :

$$0 < \|\mathbf{v}_1\|_\infty \leqslant \min\left(\deg_\infty(F), \deg_\infty(G)\right), \tag{4.2.4}$$

$$0 < \|\mathbf{v}_2\|_\infty \leqslant 2 \deg_\infty(F) \deg_\infty(G). \tag{4.2.5}$$

On pose :

$$\mathbf{c} = (c_1, c_2), \quad U = \begin{pmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \end{pmatrix} \quad \text{et} \quad V = \begin{pmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{pmatrix}.$$

D'après (4.2.2) et (4.2.3), on a :

$$\mathbf{c}UV = 0 \quad \text{et} \quad \det(UV) = 0.$$

Comme $\mathbf{c}$ est non nul, sans perte de généralité, on peut supposer $c_2 \neq 0$. Supposons d'abord $\mathbf{u}_1\mathbf{v}_1 = 0$. Comme $\mathbf{c}UV = 0$ et $c_2 \neq 0$, on en déduit $\mathbf{u}_2\mathbf{v}_1 = 0$. Donc on a $\mathbf{a}\mathbf{v}_1 = (\eta_1\mathbf{u}_1 + \eta_2\mathbf{u}_2)\mathbf{v}_1 = 0$. En prenant $\mathbf{b} = \mathbf{v}_1$, on a $\mathbf{ab} = 0$ et $\|\mathbf{b}\|_\infty \leqslant \min(\deg_\infty(P), \deg_\infty(Q))$; d'où le résultat.

Supposons maintenant $\mathbf{u}_1\mathbf{v}_1 \neq 0$. Posons $\mathbf{b} = (\mathbf{u}_1\mathbf{v}_1)\mathbf{v}_2 - (\mathbf{u}_1\mathbf{v}_2)\mathbf{v}_1$. On a $\mathbf{b} \neq 0$ car $\mathbf{v}_1$ et $\mathbf{v}_2$ sont linéairement indépendants. Il est évident que $\mathbf{u}_1\mathbf{b} = 0$. De plus, on a $\mathbf{u}_2\mathbf{b} = 0$ car $\det(UV) = 0$. Ainsi, on en déduit que $\mathbf{ab} = 0$. Enfin, déterminons une majoration explicite de $\|\mathbf{b}\|_\infty$ en fonction de F et G. Comme $\mathbf{b} = (\mathbf{u}_1\mathbf{v}_1)\mathbf{v}_2 - (\mathbf{u}_1\mathbf{v}_2)\mathbf{v}_1$, on a :

$$\|\mathbf{b}\|_\infty \leqslant 2\|\mathbf{v}_1\|_\infty\|\mathbf{v}_2\|_\infty\|\mathbf{u}_1\|_1. \tag{4.2.6}$$

On peut écrire $\mathbf{b} = (\mathbf{v}_1 \wedge \mathbf{v}_2) \wedge \mathbf{u}_1$. Comme $\mathbf{a}$ est orthogonal à $\mathbf{b}$, on peut écrire $\mathbf{a}$ de la façon suivante :

$$\mathbf{a} = d_1(\mathbf{v}_1 \wedge \mathbf{v}_2) + d_2\mathbf{u}_1, \quad \text{avec } d_1, d_2 \in \mathbb{Q}.$$

Les deux vecteurs $\mathbf{v}_1 \wedge \mathbf{v}_2$ et $\mathbf{u}_1$ sont linéairement indépendants. En effet, supposons qu'on a $\alpha_1(\mathbf{v}_1 \wedge \mathbf{v}_2) + \alpha_2\mathbf{u}_1 = 0$ avec $\alpha_1, \alpha_2 \in \mathbb{R}$. Si $\mathbf{u}_1\mathbf{v}_1 = \mathbf{u}_1\mathbf{v}_2 = 0$ alors on fait le produit vectoriel avec $\mathbf{v}_2$; dans ce cas, on obtient $\alpha_2 = 0$ et aussi $\alpha_1 = 0$ (car $\mathbf{v}_1 \wedge \mathbf{v}_2 \neq \mathbf{0}$). Sinon, on fait le produit vectoriel avec $\mathbf{u}_1$; dans ce cas, on obtient $\alpha_1 = 0$ et aussi $\alpha_2 = 0$ (car $\mathbf{u}_1 \neq \mathbf{0}$).

Notons Λ le sous-groupe de $\mathbb{Z}^3$ engendré par $\mathbf{v}_1 \wedge \mathbf{v}_2$ et $\mathbf{u}_1$. On a $\mathbf{a} \in \mathbb{Z}^3 \cap \mathbb{Q}\Lambda = \Lambda^{\text{sat}}$. En appliquant le Lemme 1.3.1.3 à Λ^{sat}, il existe deux vecteurs linéairement indépendants $\mathbf{u}_3, \mathbf{u}_4 \in \mathbb{Z}^3$ tels que :

$$\mathbf{a} = \eta_3\mathbf{u}_3 + \eta_4\mathbf{u}_4, \text{ avec } \eta_3, \eta_4 \in \mathbb{Z} \quad \text{et} \quad \|\mathbf{u}_3\|_\infty\|\mathbf{u}_4\|_\infty \leqslant \frac{3}{2}\|\mathbf{v}_1 \wedge \mathbf{v}_2\|_\infty\|\mathbf{u}_1\|_\infty.$$

Puisque $\|\mathbf{u}_1\|_\infty\|\mathbf{u}_2\|_\infty$ est minimal, on a :

$$\|\mathbf{u}_1\|_\infty\|\mathbf{u}_2\|_\infty \leqslant \|\mathbf{u}_3\|_\infty\|\mathbf{u}_4\|_\infty \leqslant \frac{3}{2}\|\mathbf{v}_1 \wedge \mathbf{v}_2\|_\infty\|\mathbf{u}_1\|_\infty \leqslant 3\|\mathbf{v}_1\|_\infty\|\mathbf{v}_2\|_\infty\|\mathbf{u}_1\|_\infty.$$

Par suite, on a :

$$\|\mathbf{u}_1\|_\infty \leqslant \|\mathbf{u}_2\|_\infty \leqslant 3\|\mathbf{v}_1\|_\infty\|\mathbf{v}_2\|_\infty.$$

L'inégalité (4.2.6) devient :

$$\|\mathbf{b}\|_\infty \leqslant 4\|\mathbf{v}_1\|_\infty\|\mathbf{v}_2\|_\infty(3\|\mathbf{v}_1\|_\infty\|\mathbf{v}_2\|_\infty) = 12\left(\|\mathbf{v}_1\|_\infty\|\mathbf{v}_2\|_\infty\right)^2.$$

Enfin, d'après (4.2.4) et (4.2.5), on en déduit que :

$$\|\mathbf{b}\|_\infty \leqslant 48\left(\deg_\infty(F)\deg_\infty(G)\min(\deg_\infty(F), \deg_\infty(G))\right)^2.$$

□

4.3 Cas 2 : $H(\mathbf{y})$ est un monôme

La proposition suivante montre que si H est un monôme alors le degré de $\xi \in \overline{\mathbb{Q}} \setminus \boldsymbol{\mu}_\infty$ vérifiant $F(\xi^{\mathbf{a}}) = G(\xi^{\mathbf{a}}) = 0$ est contrôlé par $\|\mathbf{a}\|_2^{1/2}$.

Proposition 4.3.1. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\operatorname{pgcd}(F, G) = 1$. Soient $\mathbf{a} \in \mathbb{Z}^3$ un vecteur primitif et $\xi \in \overline{\mathbb{Q}} \setminus \boldsymbol{\mu}_\infty$ tels que $F(\xi^{\mathbf{a}}) = G(\xi^{\mathbf{a}}) = 0$. Soient $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}^3$ deux vecteurs linéairement indépendants tels que $\mathbf{a} \in \langle \mathbf{u}_1, \mathbf{u}_2 \rangle$ et $\|\mathbf{u}_1\|_\infty \|\mathbf{u}_2\|_\infty$ est minimal. Si $\operatorname{pgcd}(F(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}), G(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}))$ est un monôme alors on a :*

$$[\mathbb{Q}(\xi) : \mathbb{Q}] \leqslant 6\gamma_2^{3/2} \deg_\infty(F) \deg_\infty(G) \|\mathbf{a}\|_2^{1/2}, \tag{4.3.1}$$

où $\gamma_2 = 2/\sqrt{3}$ est la constante d'Hermite de dimension 2.

Démonstration. On note $H(\mathbf{y}) = \operatorname{pgcd}(F(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}), G(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}))$. On considère les deux polynômes $P(\mathbf{y}) = F(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})/H(\mathbf{y})$ et $Q(\mathbf{y}) = F(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})/H(\mathbf{y})$. On note R le résultant de P et Q par rapport à la variable y_2. On a donc $R \neq 0$. Soit E l'ensemble des racines communes de P et Q dans $\overline{\mathbb{Q}}^2$:

$$E = \left\{ \boldsymbol{\alpha} \in \overline{\mathbb{Q}}^2 \mid P(\boldsymbol{\alpha}) = Q(\boldsymbol{\alpha}) = 0 \right\}.$$

On a $\#E \leqslant \deg_\infty(R)$. En utilisant la matrice de Sylvester pour majorer $\deg_\infty(R)$ et en utilisant l'inégalité de Cauchy-Schwarz pour majorer $\deg_{y_i} P$ et $\deg_{y_i} Q$, on en déduit :

$$\begin{aligned} \#E &\leqslant \deg_{y_1}(P) \deg_{y_2}(Q) + \deg_{y_2}(P) \deg_{y_1}(Q) \\ &\leqslant 2\|\mathbf{u}_1\|_1 \|\mathbf{u}_2\|_1 \deg_\infty(F) \deg_\infty(G). \end{aligned}$$

D'après l'hypothèse, il existe $\boldsymbol{\eta} \in \mathbb{Z}^2$ tel que $\mathbf{a} = \eta_1 \mathbf{u}_1 + \eta_2 \mathbf{u}_2$. Comme $F(\xi^{\mathbf{a}}) = G(\xi^{\mathbf{a}})$ et ξ n'est pas une racine de l'unité, on a $\xi^{\boldsymbol{\eta}} \in E$. Puisque $\mathbf{a}$ primitif, il en est de même pour $\boldsymbol{\eta}$ et donc ξ est uniquement déterminé par $\xi^{\boldsymbol{\eta}}$. Comme chaque conjugué de $\xi^{\boldsymbol{\eta}}$ appartient à E, on a :

$$[\mathbb{Q}(\xi) : \mathbb{Q}] \leqslant 2\|\mathbf{u}_1\|_1 \|\mathbf{u}_2\|_1 \deg_\infty(F) \deg_\infty(G).$$

D'après le Lemme 1.4.2, il existe deux vecteurs linéairement indépendants $\mathbf{u}_1', \mathbf{u}_2' \in \mathbb{Z}^n$ tels que $\mathbf{a} \in \langle \mathbf{u}_1', \mathbf{u}_2' \rangle$ et

$$\|\mathbf{u}_1'\|_2 \|\mathbf{u}_2'\|_2 \leqslant \gamma_2^{3/2} \|\mathbf{a}\|_2^{1/2}.$$

Puisque $\|\mathbf{u}_1\|_\infty \|\mathbf{u}_2\|_\infty$ est minimal, on a :

$$\|\mathbf{u}_1\|_\infty \|\mathbf{u}_2\|_\infty \leqslant \|\mathbf{u}_1'\|_\infty \|\mathbf{u}_2'\|_\infty \leqslant \gamma_2^{3/2} \|\mathbf{a}\|_2^{1/2}.$$

Ainsi, on a :

$$[\mathbb{Q}(\xi) : \mathbb{Q}] \leqslant 2\gamma_2^{3/2} \deg_\infty(F) \deg_\infty(G) \|\mathbf{a}\|_2^{1/2}.$$

□

Sous l'hypothèse que le degré de ξ est contrôlé par $\|\mathbf{a}\|_2^{1/2}$ et $r_\sigma = 3$, on va appliquer la Proposition 4.3.3 pour montrer que la norme de $\mathbf{a}$ est majorée par une constante ne dépendant que de F et G. Pour montrer cette proposition, on a besoin d'un lemme de U. Zannier sur la hauteur des zéros d'un polynôme lacunaire.

Lemme 4.3.2. *[40, Lemme 1, p.524] Soit $n \geqslant 1$ un entier. Soient $\alpha_1, \cdots, \alpha_n \in \overline{\mathbb{Q}}^{*n}$ tels que $\alpha_1 \cdots \alpha_n \neq 0$. Soient $m_1 > m_2 > \cdots > m_n$ des entiers naturels et soit ξ un nombre algébrique non nul satisfaisant :*

$$\sum_{i=1}^{n} \alpha_i \xi^{m_i} = 0 \quad \text{et} \quad \sum_{i=1}^{k} \alpha_i \xi^{m_i} \neq 0 \quad \text{pour tout} \quad k = 1, \cdots, n-1.$$

Alors on a :

$$(m_1 - m_n) \log M(\xi) \leqslant (n-1)\left(\log(n-1) + h_1(\boldsymbol{\alpha})\right)[\mathbb{Q}(\xi) : \mathbb{Q}].$$

On note τ la fonction définie par $\tau(x) = 4\left(\log(x)/\log\log(x)\right)^3$ pour tout $x > e$. On rappelle que la fonction ℓ est définie à l'équation (1.2.3) à la page 5, à la fin de la Section 1.2.2 du Chapitre 1. Si $F \in \mathbb{C}[\mathbf{x}^{\pm 1}]$ alors on note $H(F)$ la somme de logarithmes des valeurs absolues des coefficients non nuls de F. On note aussi :

$$\begin{aligned} D &= \max\left(\deg_\infty(F), \deg_\infty(G)\right) \\ h &= \max\left(\log\|F\|_1, \log\|G\|_1\right) \\ N &= \max\left(\#\mathrm{Supp}(F), \#\mathrm{Supp}(G)\right) \\ H &= \max\left(H(F), H(G)\right). \end{aligned}$$

Proposition 4.3.3. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\mathrm{pgcd}(F, G) = 1$. Soient $\mathbf{a} \in \mathbb{Z}^3$ un vecteur primitif et $\xi \in \overline{\mathbb{Q}} \setminus \boldsymbol{\mu}_\infty$ de degré vérifiant (4.3.1) tels que $F(\xi^{\mathbf{a}}) = G(\xi^{\mathbf{a}}) = 0$. Soit σ la décomposition maximale de F et G définie par (4.1.1). Si $r_\sigma = 3$ alors on a :*

$$\|\mathbf{a}\|_\infty^{1/2} \leqslant 3\sqrt{864} D^4 H(N-1)\log(N-1)\tau(1152 D^6 H(N-1)\log(N-1)).$$

En particulier, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_2 \leqslant 125 D^4 H(N-1)\log(N-1)\tau(1152 D^6 H(N-1)\log(N-1)).$$

Démonstration. Par hypothèse, σ est une décomposition maximale de F et G définie par (4.1.1) :

$$\sigma : \ F = \sum_{i=1}^{p} F_i \quad \text{et} \quad G = \sum_{j=1}^{q} G_i,$$

tels que

- les F_i et les G_j sont non nuls,
- $\mathrm{Supp}(F_i) \cap \mathrm{Supp}(F_j) = \mathrm{Supp}(G_i) \cap \mathrm{Supp}(G_j) = \emptyset$ pour $i \neq j$,
- $F_i(\xi^{\mathbf{a}}) = Q_j(\xi^{\mathbf{a}}) = 0$ pour $1 \leqslant i \leqslant p$ et $1 \leqslant j \leqslant q$.

On rappelle que la matrice $\mathcal{M}_\sigma$ est définie par :

$$\mathcal{M}_\sigma = \begin{pmatrix} \mathcal{M}(F_1) & \cdots & \mathcal{M}(F_p) & \mathcal{M}(G_1) & \cdots & \mathcal{M}(G_q) \end{pmatrix} \in M_{n,m}(\mathbb{Z}),$$

où $m = (n_{F_1} - 1) + \cdots (n_{F_p} - 1) + (n_{G_1} - 1) + \cdots + (n_{G_q} - 1)$. Comme la décomposition σ est maximale, les entiers p et q sont maximaux.

Quitte à faire une somme sur les coefficients, on peut supposer que pour tout i, j, aucun couple de vecteurs distincts $(\boldsymbol{\lambda}, \boldsymbol{\mu}) \in \mathrm{Supp}(F_i)^2 \cup \mathrm{Supp}(G_j)^2$ vérifie $\mathbf{a}\boldsymbol{\lambda} = \mathbf{a}\boldsymbol{\mu}$.

Soit $i \in \{1, \cdots, p\}$. Pour $\boldsymbol{\lambda}_k \in \mathrm{Supp}(F_i)$, on pose $m_k = \mathbf{a}\boldsymbol{\lambda}_k$. Quitte à renuméroter les m_k, on peut supposer $m_1 > \cdots > m_{n_{F_i}}$. Puisque p est maximal, aucune sous-somme de F_i s'annule en $\xi^{\mathbf{a}}$. D'après le Lemme 4.3.2, on en déduit que :

$$(m_1 - m_{n_{F_i}}) \log M(\xi) \leqslant (n_{F_i} - 1)\,(\log(n_{F_i} - 1) + H(F_i))\,[\mathbb{Q}(\xi) : \mathbb{Q}].$$

où $H(F_i)$ est la somme des logarithmes des valeurs absolues des coefficients non nuls de F_i. Comme $\mathrm{Supp}(F_i) \cap \mathrm{Supp}(F_j) = \emptyset$ pour $i \neq j$, on a les majorations $n_{F_i} \leqslant n_F$ et $H(F_i) \leqslant H(F)$. On a alors :

$$(m_1 - m_{n_{F_i}}) \log M(\xi) \leqslant (n_F - 1)\,(\log(n_F - 1) + H(F))\,[\mathbb{Q}(\xi) : \mathbb{Q}]. \tag{4.3.2}$$

On a une inégalité similaire pour G_j.

Par ailleurs, comme $r_\sigma = 3$, il existe trois vecteurs linéairement indépendants $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in \mathbb{Z}^3$ tels que chaque $\mathbf{v}_i$ (pour $i = 1, 2, 3$) correspond à une des colonnes de $\mathcal{M}_\sigma$. On a alors $\|\mathbf{v}_i\|_\infty \leqslant \max(\deg_\infty(F), \deg_\infty(G))$. Sans perte de généralité, on peut supposer que $\mathbf{v}_1$ correspond à une des colonnes de $\mathcal{M}(F_i)$. D'après la construction de m_1 et $m_{n_{F_i}}$ ci-dessus, on en déduit :

$$|\mathbf{a}\mathbf{v}_1| \leqslant m_1 - m_{n_{F_i}}. \tag{4.3.3}$$

On rappelle $\gamma_2 = 2/\sqrt{3}$ la constante d'Hermite de dimension 2. On note :

$$d = 6\gamma_2^{3/2} \deg_\infty(F) \deg_\infty(G) \|\mathbf{a}\|_2^{1/2}.$$

En combinant les deux inégalités (4.3.3) et (4.3.2) et en utilisant le fait que $(\log M(\xi))^{-1} \leqslant \ell(d)$, on obtient :

$$|\mathbf{a}\mathbf{v}_1| \leqslant m_1 - m_{n_{F_i}} \leqslant (n_F - 1)\,(\log(n_F - 1) + H(F))\,d\ell(d).$$

En appliquant cette procédé à $\mathbf{v}_2$ et $\mathbf{v}_3$, on a des inégalités similaires. Ainsi, pour $i \in \{1, 2, 3\}$, on a :

$$\begin{aligned} &\|\mathbf{v}_i\|_\infty \leqslant D \\ &|\mathbf{a}\mathbf{v}_i| \leqslant (N-1)\,(\log(N-1) + H)\,d\ell(d). \end{aligned}$$

En écrivant

$$\begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix} \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{v}_3 \end{pmatrix} = \begin{pmatrix} \mathbf{a}\mathbf{v}_1 \\ \mathbf{a}\mathbf{v}_2 \\ \mathbf{a}\mathbf{v}_3 \end{pmatrix}$$

et utilisant les formules de Cramer, on en déduit que :

$$\|\mathbf{a}\|_\infty \leqslant 2\|\mathbf{v}_1\|_\infty\, \|\mathbf{v}_2\|_\infty\, \|\mathbf{v}_3\|_\infty \sum_{i=1}^{3} \frac{|\mathbf{a}\mathbf{v}_i|}{\|\mathbf{v}_i\|_\infty} \leqslant 6D^2(N-1)\log(N-1)Hd\ell(d).$$

Comme ℓ est croissante et en remplaçant d par son expression, on obtient :

$$\|\mathbf{a}\|_\infty^{1/2} \leqslant \sqrt{864}D^4(N-1)\log(N-1)H\ell\left(\sqrt{96}D^2\|\mathbf{a}\|_\infty^{1/2}\right).$$

En multipliant par $\sqrt{96}D^2$ cette inégalité, on obtient :

$$X \leqslant C\ell(X)$$

où

$$X = \sqrt{96}D^2\|\mathbf{a}\|_\infty^{1/2} \quad \text{et} \quad C = \sqrt{82944}D^6(N-1)\log(N-1)H.$$

D'après le Théorème 1.2.2.3, on a $\ell(X) \leqslant \tau(X)$ car $X \geqslant 3$. Comme $C \geqslant 2$ et $3 \leqslant X \leqslant C\tau(X)$, d'après le Lemme A.2.2, on a :

$$X \leqslant 3C\tau(4C).$$

En remplaçant X et C par leur expression, on en déduit que la majoration de $\|\mathbf{a}\|_\infty$ voulue :

$$\|\mathbf{a}\|_\infty^{1/2} \leqslant 3\sqrt{864}D^4(N-1)\log(N-1)H\tau(1152D^6H(N-1)\log(N-1)).$$

D'après le Théorème 1.4.1, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_2 \leqslant \gamma_2^{1/2}\|\mathbf{a}\|_2^{1/2}.$$

Par suite, on a :

$$\|\mathbf{b}\|_2 \leqslant 125D^4(N-1)\log(N-1)L\tau(1152D^6H(N-1)\log(N-1)).$$

□

Enfin, si $r_\sigma \leqslant 2$, on applique la proposition suivante pour trouver un vecteur $\mathbf{b}$ vérifiant les propriétés requises. On note que l'hypothèse que la décomposition σ soit maximale n'est plus nécessaire. On note encore :

$$D = \max\left(\deg_\infty(F), \deg_\infty(G)\right) \quad \text{et} \quad h = \max\left(\log\|F\|_1, \log\|G\|_1\right)$$

Proposition 4.3.4. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\operatorname{pgcd}(F,G) = 1$. Soient $\mathbf{a} \in \mathbb{Z}^3$ un vecteur primitif et $\xi \in \overline{\mathbb{Q}} \setminus \boldsymbol{\mu}_\infty$ tels que $F(\xi^{\mathbf{a}}) = G(\xi^{\mathbf{a}}) = 0$. Soit σ la décomposition de F et G définie par (4.1.1). Si $r_\sigma \leqslant 2$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :*

$$\|\mathbf{b}\|_\infty \leqslant 30D^3(6D^2\log 2 + h)\ell(18D^4).$$

Démonstration. On va faire un changement de variables pour se ramener au cas $n = 2$. On rappelle que la matrice $\mathcal{M}_\sigma$ est définie par :

$$\mathcal{M}_\sigma = \begin{pmatrix} \mathcal{M}(F_1) & \cdots & \mathcal{M}(F_p) & \mathcal{M}(G_1) & \cdots & \mathcal{M}(G_q) \end{pmatrix} \in M_{3,m}(\mathbb{Z}),$$

où $m = (n_{F_1} - 1) + \cdots (n_{F_p} - 1) + (n_{G_1} - 1) + \cdots + (n_{G_q} - 1)$.

On commence par montrer qu'il existe deux matrices $U \in M_{3,2}(\mathbb{Z})$ et $A \in M_{2,N}(\mathbb{Z})$ vérifiant les propriétés suivantes :

- $\mathcal{M}_\sigma = UA$
- $\operatorname{rang}(U) = 2$
- les normes des vecteurs colonnes de U sont majorées par une constante ne dépendant que de F et de G

• Si $r_\sigma = 0$ alors $\mathcal{M}_\sigma$ est la matrice nulle et ainsi on prend A la matrice nulle et

$$U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

• Supposons $r_\sigma = 1$. Dans ce cas, le sous-groupe Λ engendré les vecteurs colonnes de $\mathcal{M}_\sigma$ est de rang 1. Ainsi, Λ est engendré par un vecteur non nul $\mathbf{u}_1 \in \mathrm{Supp}(F) \cup \mathrm{Supp}(G)$. D'après le Théorème 1.4.1, il existe un vecteur non nul $\mathbf{u}_2 \in \mathbb{Z}^3$ orthogonal à $\mathbf{u}_1$ et tel que :

$$\|\mathbf{u}_2\|_2 \leqslant \gamma_2^{1/2} \|\mathbf{u}_1\|_2^{1/2}.$$

On peut alors écrire M_σ de la façon suivante :

$$M_\sigma = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 \end{pmatrix} \begin{pmatrix} \mathbf{c} \\ \mathbf{0} \end{pmatrix} \quad \text{où} \quad \mathbf{c} \in \mathbb{Z}^m.$$

La matrice U dont les colonnes sont $\mathbf{u}_1$ et $\mathbf{u}_2$ est de rang 2 car ces deux vecteurs sont orthogonaux. De pus, on a

$$\|\mathbf{u}_1\|_\infty \leqslant \max\left(\deg_\infty(F), \deg_\infty(G)\right) \quad \text{et} \quad \|\mathbf{u}_2\|_\infty \leqslant \sqrt{2} \max\left(\deg_\infty(F), \deg_\infty(G)\right)^{1/2}.$$

• Supposons $r_\sigma = 2$. Soit $\{\mathbf{u}_1, \mathbf{u}_2\}$ une base de Λ et soit U la matrice dont les colonnes sont ces deux vecteurs. Il existe donc une matrice entière $A \in M_{2,m}(\mathbb{Z})$ telle que :

$$\mathcal{M}_\sigma = UA.$$

Par construction, on a bien $\mathrm{rang}(U) = 2$. D'après la Proposition 1.3.1.3, on peut choisir $\mathbf{u}_1$ et $\mathbf{u}_2$ tels que $\mathbf{u}_1 = c_1 \boldsymbol{\mu}_1$ et $\mathbf{u}_2 = c_{2,1}\boldsymbol{\mu}_1 + c_2\boldsymbol{\mu}_2$ où $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2 \in \mathrm{Supp}(F) \cup \mathrm{Supp}(G)$, $|c_i| \leqslant 1$ (pour $i = 1, 2$) et $|c_{2,1}| \leqslant 1/2$. En particulier, on a

$$\|\mathbf{u}_1\|_\infty \leqslant \max\left(\deg_\infty(F), \deg_\infty(G)\right) \quad \text{et} \quad \|\mathbf{u}_2\|_\infty \leqslant (3/2) \max\left(\deg_\infty(F), \deg_\infty(G)\right).$$

On en conclut que, dans chaque cas, il existe deux matrices $U \in M_{3,2}(\mathbb{Z})$ de rang 2 et une matrice $A \in M_{2,m}(\mathbb{Z})$ vérifiant $M_\sigma = UA$ et telles

$$\|\mathbf{u}_1\|_\infty \leqslant \max\left(\deg_\infty(F), \deg_\infty(G)\right) \quad \text{et} \quad \|\mathbf{u}_2\|_\infty \leqslant (3/2) \max\left(\deg_\infty(F), \deg_\infty(G)\right). \tag{4.3.4}$$

Maintenant, pour i, j, on écrit F_i et G_j sous la forme :

$$F_i(\mathbf{x}) = \mathbf{x}^{\mathbf{p}_i} F_i^*(\mathbf{x}^U) \quad \text{et} \quad G_j(\mathbf{x}) = \mathbf{x}^{\mathbf{q}_j} G_j^*(\mathbf{x}^U),$$

où $\mathbf{p}_i, \mathbf{q}_j \in \mathbb{Z}^3$ et tels que $F_i^*, G_j^* \in \mathbb{Z}[y_1, y_2]$ sont uniquement déterminés par :

$$\mathrm{pgcd}\left(F_i^*, y_1 y_2\right) = 1 \quad \text{et} \quad \mathrm{pgcd}\left(G_j^*, y_1 y_2\right) = 1.$$

Puisque F_i et G_j s'annulent en $\xi^{\mathbf{a}}$, on a :

$$F_i^*(\xi^{\mathbf{a}\cdot\mathbf{u}_1}, \xi^{\mathbf{a}\cdot\mathbf{u}_2}) = G_j^*(\xi^{\mathbf{a}\cdot\mathbf{u}_1}, \xi^{\mathbf{a}\cdot\mathbf{u}_2}) = 0.$$

On pose :

$$R_\sigma = \operatorname{pgcd}(F_1^*, \cdots, F_p^*) \quad \text{et} \quad F_i^{**} = F_i^*/R_\sigma \quad \text{pour } i \in \{1, \cdots, p\},$$
$$S_\sigma = \operatorname{pgcd}(G_1^*, \cdots, G_q^*) \quad \text{et} \quad G_j^{**} = G_j^*/S_\sigma \quad \text{pour } j \in \{1, \cdots, q\}.$$

On a $\operatorname{pgcd}(R_\sigma, S_\sigma) = 1$ car $\operatorname{pgcd}(F, G) = 1$. Par construction, on a aussi $\operatorname{pgcd}(F_1^{**}, \cdots, F_p^{**}) = \operatorname{pgcd}(G_1^{**}, \cdots, G_q^{**}) = 1$. On est alors dans l'un des trois cas suivants :

$$\begin{cases} R_\sigma(\xi^{\mathbf{a}\cdot\mathbf{u}_1}, \xi^{\mathbf{a}\cdot\mathbf{u}_2}) = S_\sigma(\xi^{\mathbf{a}\cdot\mathbf{u}_1}, \xi^{\mathbf{a}\cdot\mathbf{u}_2}) = 0 \\ F_i^{**}(\xi^{\mathbf{a}\cdot\mathbf{u}_1}, \xi^{\mathbf{a}\cdot\mathbf{u}_2}) = 0 \text{ pour tout } i \in \{1, \cdots, p\} \\ G_j^{**}(\xi^{\mathbf{a}\cdot\mathbf{u}_1}, \xi^{\mathbf{a}\cdot\mathbf{u}_2}) = 0 \text{ pour tout } j \in \{1, \cdots, q\} \end{cases} \tag{4.3.5}$$

Soit $\mathcal{F}$ un ensemble fini de polynômes. On pose :

$$B(\mathcal{F}) = 2D_\mathcal{F} h_\mathcal{F} \ell(2D_\mathcal{F}^2),$$

où

$$D_\mathcal{F} = \max_{P \in \mathcal{F}} \deg_\infty(P) \quad \text{et} \quad h_\mathcal{F} = \max_{P \in \mathcal{F}} \log \|P\|_1.$$

On note :

$$B_{\max} = \max\left(B(R_\sigma, S_\sigma), B(F_1^{**}, \cdots, F_p^{**}), B(G_1^{**}, \cdots, G_q^{**})\right).$$

En appliquant le Corollaire 3.2.2 aux trois cas (4.3.5), il existe un vecteur non nul $\boldsymbol{\eta} \in \mathbb{Z}^2$ orthogonal à $(\mathbf{a}\cdot\mathbf{u}_1, \mathbf{a}\cdot\mathbf{u}_2)$ tel que

$$\|\mathbf{c}\|_\infty \leqslant B.$$

On prend $\mathbf{b} = \eta_1\mathbf{u}_1 + \eta_2\mathbf{u}_2$. Puisque $\mathbf{u}_1$ et $\mathbf{u}_2$ sont linéairement indépendants et $\boldsymbol{\eta}$ est non nul, $\mathbf{b}$ est non nul. Comme $\boldsymbol{\eta}$ orthogonal à $(\mathbf{a}\cdot\mathbf{u}_1, \mathbf{a}\cdot\mathbf{u}_2)$, $\mathbf{b}$ est orthogonal à $\mathbf{a}$. En utilisant (4.3.4), on a :

$$\|\mathbf{b}\|_\infty \leqslant 5B_{\max} \max\left(\deg_\infty(F), \deg_\infty(G)\right). \tag{4.3.6}$$

Il reste à déterminer une majoration de $B_{\max}$ en fonction de F et G. Comme $F_i^{**}R_\sigma = F_i^*$, on a $\deg_\infty(F_i^{**}) \leqslant \deg_\infty(F_i^*)$. Puisque $F_i(\mathbf{x}) = \mathbf{x}^{\mathbf{p}_i} F_i^*(\mathbf{x}^U)$ et U est de rang 2, pour tout $\boldsymbol{\mu} \in \operatorname{Supp}(F_i^*)$, il existe $\boldsymbol{\lambda} \in \operatorname{Supp}(F_i)$ tel que $\mu_1\mathbf{u}_1 + \mu_2\mathbf{u}_2 = \boldsymbol{\lambda}$. D'après les formules de Cramer, on en déduit que :

$$\deg_\infty(F_i^*) \leqslant 2\deg_\infty(F_i) \max\left(\|\mathbf{u}_1\|_\infty, \|\mathbf{u}_2\|_\infty\right)$$

En utilisant (4.3.4), on en déduit que :

$$\deg(F_i^{**}) \leqslant \deg_\infty(F_i^*) \leqslant 3D^2.$$

Par ailleurs, d'après la majoration (1.2.1) de la mesure de Mahler par la norme L_1 et la multiplicativité de la mesure de Mahler, on a :

$$\|F_i^{**}\|_1 \leqslant 2^{2\deg_\infty(F_i^{**})} M(F_i^{**}) \leqslant 2^{2\deg_\infty(F_i^{**})} M(F_i^*) \leqslant 2^{2\deg_\infty(F_i^{**})} \|F_i\|_1 \leqslant 2^{6D^2} \|F\|_1.$$

Ainsi, on a :

$$\deg(F_i^{**}) \leqslant 3D^2 \quad \text{et} \quad \log\|F_i^{**}\|_1 \leqslant 6D^2\log 2 + h.$$

Par suite, on a :

$$B(F_1^{**}, \cdots, F_p^{**}) \leqslant 6D^2(6D^2\log 2 + h)\ell(18D^4).$$

De même, $B(G_1^{**}, \cdots, G_q^{**})$ et $B(R_\sigma, S_\sigma)$ sont majorées par cette borne. Enfin, (4.3.6) devient :

$$\|\mathbf{b}\|_\infty \leqslant 5B_{\max}D \leqslant 30D^3(6D^2\log 2 + h)\ell(18D^4).$$

□

4.4 Version explicite de la Conjecture de Schinzel

On donne maintenant une version explicite du Théorème 2 pour $n = 3$ suivant l'approche S. Si $F \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$ alors on note $H(F)$ est la somme de logarithmes des valeurs absolues des coefficients non nuls de F. Pour $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$, on pose :

$$\begin{aligned} D &= \max\left(\deg_\infty(F), \deg_\infty(G)\right) \\ h &= \max\left(\log\|F\|_1, \log\|G\|_1\right) \\ N &= \max\left(\#\mathrm{Supp}(F), \#\mathrm{Supp}(G)\right) \\ H &= \max\left(H(F), H(G)\right). \end{aligned}$$

Théorème 4.4.1. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\mathrm{pgcd}(F, G) = 1$. Soient $\mathbf{a} \in \mathbb{Z}^3$ un vecteur primitif et $\xi \in \overline{\mathbb{Q}} \setminus \boldsymbol{\mu}_\infty$. Si $F(\xi^{\mathbf{a}}) = G(\xi^{\mathbf{a}}) = 0$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :*

$$\|\mathbf{b}\|_2 \leqslant 120 D^4 (6D^2 \log 2 + h) HN \log N \left(\frac{\log(1152 D^6 HN \log N)}{\log\log(18D^4)}\right)^3.$$

Démonstration. Soient $\mathbf{u}_1, \mathbf{u}_2$ deux vecteurs linéairement indépendants tels que $\mathbf{a} \in \langle \mathbf{u}_1, \mathbf{u}_2 \rangle$ et $\|\mathbf{u}_1\|_\infty \|\mathbf{u}_2\|_\infty$ est minimal. On note $H(y_1, y_2) = \mathrm{pgcd}(F(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}), G(y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}))$. Si H n'est pas un monôme alors, d'après la Proposition 4.2.1, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_\infty \leqslant 48 D^6. \tag{4.4.1}$$

Si H est un monôme alors, d'après la Proposition 4.3.1, on a :

$$[\mathbb{Q}(\xi) : \mathbb{Q}] \leqslant 6\gamma_2^{3/2} \deg_\infty(F) \deg_\infty(G) \|\mathbf{a}\|_2^{1/2}.$$

Soit σ une décomposition maximale de F et G suivant $\xi^{\mathbf{a}}$. On note $\mathcal{M}_\sigma$ la matrice associée à σ et r_σ le rang du sous groupe de $\mathbb{Z}^3$ engendré par les vecteurs colonnes de $\mathcal{M}_\sigma$.

Si $r_\sigma = 3$ alors d'après la Proposition 4.3.3, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_2 \leqslant 125 D^4 H(N-1)\log(N-1)\tau(1152 D^6 H(N-1)\log(N-1)).$$

Comme $\tau(x)$ est croissante pour $x > e^e$, on a :

$$\tau(1152 D^6 H(N-1)\log(N-1)) \leqslant 4\left(\frac{\log(1152 D^6 HN \log N)}{\log\log(1152 D^6 HN \log N)}\right)^3.$$

Donc on a :

$$\|\mathbf{b}\|_2 \leqslant 500 D^4 HN \log N \left(\frac{\log(1152 D^6 HN \log N)}{\log\log(1152 D^6 HN \log N)}\right)^3. \tag{4.4.2}$$

Si $r_\sigma \leqslant 2$ alors d'après la Proposition 4.3.4, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_\infty \leqslant 30 D^3 (6D^2 \log 2 + h)\ell(18D^4).$$

Par le Théorème 1.2.2.3, on a $\ell(d) \leqslant \tau(d)$ pour $d \geqslant 3$, donc on a :

$$\ell(18D^4) \leqslant 4\left(\frac{\log(18D^4)}{\log\log(18D^4)}\right)^3.$$

Donc on a :

$$\|\mathbf{b}\|_\infty \leqslant 120D^3(6D^2\log 2 + h)\left(\frac{\log(18D^4)}{\log\log(18D^4)}\right)^3. \tag{4.4.3}$$

En prenant le maximum entre les bornes de (4.4.1), (4.4.2) et (4.4.3), on obtient :

$$\|\mathbf{b}\|_2 \leqslant 120D^4(6D^2\log 2 + h)HN\log N\left(\frac{\log(1152D^6HN\log N)}{\log\log(18D^4)}\right)^3.$$

□

5. Cas $n = 3$: approche BMZ

Dans ce chapitre, on va décrire une autre approche, que l'on appelle approche BMZ et qui s'inspire de la preuve de E. Bombieri, D. Masser et U. Zannier dans [11] et celle de U. Zannier dans [40, Appendix]. Cette approche permet aussi d'obtenir une version explicite du Théorème 2 dans le cas $n = 3$ (Théorème 5.5.1).

5.1 Présentation de l'approche

Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\mathrm{pgcd}(F, G) = 1$. Soient $\mathbf{a} \in \mathbb{Z}^3$ un vecteur primitif et $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^3$. On note :

$$V = V(F, G) \quad \text{et} \quad T_1 = \left\{ \xi^{\mathbf{a}} \in \mathbb{G}_{\mathrm{m}}^3,\ \xi \in \overline{\mathbb{Q}}^* \right\}.$$

On s'intéresse aux points $\boldsymbol{\alpha} \in V \cap \boldsymbol{\zeta} T_1$ qui ne sont pas de torsion. On a alors :

$$\boldsymbol{\alpha} \in V \cap \boldsymbol{\zeta} T_1 \neq \emptyset.$$

On aurait pu s'attendre à une intersection vide car $\dim(V) + \dim(\boldsymbol{\zeta} T_1) - n = 1 + 1 - 3 = -1$. Il s'agit de ce que Zilber [49] appelle une *intersection atypique*. On cherche à déterminer un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ et dont la norme est majorée par une constante ne dépendant que de F et G.

À l'aide du Théorème de H. Minkwoski, on construit un sous-tore auxiliaire T_2 de $\mathbb{G}_{\mathrm{m}}^3$ de dimension 2 contenant T_1 et tel que $\deg(T_2) \ll \deg(T_1)^{1/2}$. Plus précisément, d'après le Théorème 1.4.1, il existe un vecteur non nul $\mathbf{u} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{u}\|_2 \leqslant \sqrt{\gamma_2} \|\mathbf{a}\|_2^{1/2}, \tag{5.1.1}$$

où $\gamma_2 = 2/\sqrt{3}$ est la constante d'Hermite en dimension 2. Quitte à diviser $\mathbf{u}$ par son pgcd, on peut supposer que $\mathbf{u}$ est primitif. On note T_2 le sous-tore de $\mathbb{G}_{\mathrm{m}}^3$ défini par le vecteur $\mathbf{u}$ i.e.

$$T_2 = \{ \boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^3 \mid \boldsymbol{\alpha}^{\mathbf{u}} = 1 \}. \tag{5.1.2}$$

On rappelle que V^{a} est la réunion des translatés de sous-tores de dimension non nulle contenus dans V et $V^{\mathrm{o}} = V \setminus V^{\mathrm{a}}$. On est alors dans l'un des trois cas suivants :

Cas 1 : $\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ (Proposition 5.4.1). Dans ce cas, on montre que la norme de $\mathbf{a}$ est majorée uniquement en fonction de F et G. En écrivant $\boldsymbol{\alpha} = \boldsymbol{\zeta} \xi^{\mathbf{a}}$, l'idée consiste d'une part à minorer la hauteur de $h(\xi)$ soit en utilisant la minoration du Théporème Dobrowolski soit sa version relative établi par F. Amoroso et U. Zannier et d'autre part à majorer la hauteur de $\boldsymbol{\alpha}$ en utilisant une majoration de type *Bounded Height Conjecture*. Ensuite, pour déduire un vecteur $\mathbf{b}$ ayant les propriétés requises, il suffit d'appliquer le Théorème 1.4.1 à $\mathbf{a}^{\perp}$.

Cas 2 : $\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ (Proposition 5.4.2). Dans ce cas, à l'aide d'une certaine variété $V^{-1}V$ construite à partir de V, on montre qu'il existe un vecteur $\mathbf{b}$ vérifiant les propriétés requises.

Cas 3 : $\boldsymbol{\alpha} \notin V^{\mathrm{o}}$ (Proposition 5.4.3). Dans ce cas, on fait un changement de variable pour se ramener au cas $n = 2$.

On note que cette approche est semblable à celle de Bombieri, Masser et Zannier [11] sauf dans le **Cas 2**. Dans ce cas, on a pu simplifier leur approche car on est dans une situation particulière.

On peut aussi faire l'analogie avec l'approche S décrite dans le Chapitre 4. Avec les notations du Chapitre 6, le fait que H n'est pas un monôme correspond au cas où $\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$. Le fait que H est un monôme correspond au cas où $\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$. Le cas où $r_\sigma \leqslant 2$ et $r = 3$ correspondent respectivement au cas où $\boldsymbol{\alpha} \in V^{\mathrm{a}}$ et où $\boldsymbol{\alpha} \in V^{\mathrm{o}}$.

Le Tableau 5.1 récapitule le schéma de la preuve.

Hypothèses	$\boldsymbol{\alpha} \in V^{\mathrm{o}}$	$\boldsymbol{\alpha} \in V^{\mathrm{a}}$
$\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$	Proposition 5.4.1	Proposition 5.4.3
$\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$	Proposition 5.4.2	Proposition 5.4.3

Tableau 5.1 – Schéma de la preuve de l'approche BMZ

On note :

$$\begin{aligned} D &= \max\left(\deg_\infty(F), \deg_\infty(G)\right) \\ h &= \max(\log \|F\|_1, \log \|G\|_1) \\ N &= \max(\#\mathrm{Supp}(F), \#\mathrm{Supp}(G)). \end{aligned}$$

Le Tableau 5.2 donne asymptotiquement l'ordre de grandeur des bornes associées aux différents cas suivant l'approche BMZ.

Hypothèses	$\boldsymbol{\alpha} \in V^{\mathrm{o}}$	$\boldsymbol{\alpha} \in V^{\mathrm{a}}$
$\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$	$N^3 D^5 h^2$	$D^4 h$
$\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$	D^4	$D^4 h$

Tableau 5.2 – Ordre de grandeur des bornes suivant l'approche BMZ

Dans la Section 5.2, on va définir et donner des propriétés de la variété $V^{-1}V$ construite à partir de V. Ensuite, dans la Section 5.3, on donne la majoration du type *Bounded Height Conjecture*. La Section 5.4 contient la démonstration de chaque proposition dans les trois cas mentionnés ci-dessus. Enfin, dans la Section 5.5, on donne une version explicite de la Conjecture de Schinzel (Théorème 5.5.1) suivant l'approche BMZ.

5.2 La sous-variété $V^{-1}V$

On fixe un entier $n \geqslant 1$. Soit V est une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$. L'objectif de cette section est d'étudier des conditions (Proposition 5.2.1) pour lesquelles V soit un translaté de sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^n$ en utilisant la variété $V^{-1}V$ que l'on va définir. La Proposition 5.2.2 donne une majoration du degré de $V^{-1}V$ dans le cas où $V^{-1}V$ est un sous-tore.

On considère le morphisme φ défini par :

$$\begin{aligned}\varphi : \mathbb{G}_{\mathrm{m}}^n \times \mathbb{G}_{\mathrm{m}}^n &\longrightarrow \mathbb{G}_{\mathrm{m}}^n \\ (\mathbf{x}, \mathbf{y}) &\mapsto \mathbf{x}^{-1} \cdot \mathbf{y}\end{aligned}$$

On note $V^{-1}V$ l'image de $V \times V$ via ce morphisme.

Proposition 5.2.1. *Soient V une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ et $\boldsymbol{\alpha} \in V$. Alors V est un translaté de sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^n$ si et seulement si $\boldsymbol{\alpha}^{-1}V = V^{-1}V$.*

Démonstration. Supposons que V est un translaté de sous-groupe algébrique. On a alors $V = \boldsymbol{\beta}H$ où $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$ et H est un sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^n$. Comme $\boldsymbol{\alpha} \in V$, on peut prendre $\boldsymbol{\beta} = \boldsymbol{\alpha}$. Par suite, on a :

$$V^{-1}V = (\boldsymbol{\alpha}H)^{-1}(\boldsymbol{\alpha}H) = H^{-1}H = H = \boldsymbol{\alpha}^{-1}V.$$

Supposons que $\boldsymbol{\alpha}^{-1}V = V^{-1}V$ et posons $H = \boldsymbol{\alpha}^{-1}V$. Soient $\boldsymbol{\gamma}_1, \boldsymbol{\gamma}_2 \in H$. Il existe $\mathbf{y}_1, \mathbf{y}_2 \in V$ tels que $\boldsymbol{\gamma}_1 = \boldsymbol{\alpha}^{-1}\mathbf{y}_1$ et $\boldsymbol{\gamma}_2 = \boldsymbol{\alpha}^{-1}\mathbf{y}_2$. Ainsi, on a :

$$\boldsymbol{\gamma}_1^{-1}\boldsymbol{\gamma}_2 = (\boldsymbol{\alpha}^{-1}\mathbf{y}_1)^{-1}(\boldsymbol{\alpha}^{-1}\mathbf{y}_2) = \mathbf{y}_1^{-1}\mathbf{y}_2 \in V^{-1}V = \boldsymbol{\alpha}^{-1}V = H.$$

Donc H est un sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^n$. Ainsi $V = \boldsymbol{\alpha}H$ est un translaté de sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^n$. □

Proposition 5.2.2. *Soit V une sous-variété de $\mathbb{G}_{\mathrm{m}}^n$. Notons $d = \dim(V^{-1}V)$. Si $V^{-1}V$ est un sous-tore de $\mathbb{G}_{\mathrm{m}}^n$ alors on a :*

$$\deg(V^{-1}V) \leqslant n^d \deg(V)^2.$$

Démonstration. On considère le plongement $\iota_n : \mathbb{G}_{\mathrm{m}}^n \hookrightarrow \mathbb{P}^n$ défini par $\iota_n(x_1, \cdots, x_n) = (1 : x_1 : \cdots : x_n)$ et le plongement $\iota_{2n} : \mathbb{G}_{\mathrm{m}}^n \times \mathbb{G}_{\mathrm{m}}^n \hookrightarrow \mathbb{P}^{2n}$ défini par $\iota_{2n}\left((x_1, \cdots, x_n), (y_1, \cdots, y_n)\right) = (1 : x_1 : \cdots : x_n : y_1 : \cdots : y_n)$. Ainsi, le degré de $V^{-1}V = \varphi(V \times V)$ est le degré de l'adhérence de Zariski de $\iota_n(\varphi(V \times V))$ dans $\mathbb{P}^n$ et le degré de $V \times V$ est le degré de l'adhérence de Zariski de $\iota_{2n}(V \times V)$ dans $\mathbb{P}^{2n}$. En multipliant l'expression $\mathbf{x}^{-1} \cdot \mathbf{y}$ par $x_1 \cdots x_n$, on obtient l'application :

$$\begin{aligned}\iota_n \circ \varphi : \mathbb{G}_{\mathrm{m}}^n \times \mathbb{G}_{\mathrm{m}}^n &\longrightarrow \mathbb{P}^n \\ (\mathbf{x}, \mathbf{y}) &\mapsto (x_1 \cdots x_n : y_1 x_2 x_3 \cdots x_n : \cdots : x_1 x_2 \cdots x_{n-1} y_n).\end{aligned}$$

On définit également le morphisme $\widetilde{\varphi}$:

$$\begin{aligned}\widetilde{\varphi} : \mathbb{P}^{2n} &\longrightarrow \mathbb{P}^n \\ (z_0 : z_1 : \cdots : z_{2n}) &\mapsto (z_1 \cdots z_n : z_{n+1} z_2 z_3 \cdots z_n : \cdots : z_1 z_2 \cdots z_{n-1} z_{2n})\end{aligned}$$

de telle sorte que $\iota_n \circ \varphi = \widetilde{\varphi} \circ \iota_{2n}$. De plus, $\widetilde{\varphi}$ est de degré n. Comme $\dim(V^{-1}V) = d$, le degré de $V^{-1}V \subseteq \mathbb{P}^n$ est son degré d'intersection avec d hyperplans génériques $H_1, \cdots, H_d$ dans $\mathbb{P}^n$. Chaque H_i est défini par une équation linéaire homogène non triviale. Remarquons que $\widetilde{\varphi}^{-1}(H_i)$ est une hypersurface car elle est le lieu des zéros d'une équation linéaire homogène composée avec l'application $\widetilde{\varphi}$ homogène de degré n. Par suite, on a $\deg(\widetilde{\varphi}^{-1}(H_i)) = n$. On a alors :

$$\begin{aligned}\deg(V^{-1}V) &= \#\left((i_n \circ \varphi)(V \times V) \cap H_1 \cap \cdots \cap H_d\right) \\ &\leqslant \#\left(\iota_{2n}(V \times V) \cap \widetilde{\varphi}^{-1}(H_1) \cap \cdots \cap \widetilde{\varphi}^{-1}(H_d)\right) \\ &\leqslant n^d \deg\left(V \times V\right),\end{aligned}$$

où on utilise le Théorème de Bézout dans la dernière inégalité. En considérant le plongement ι_{2n}, on a $\deg(V \times V) \leqslant \deg(V)^2$. Par suite, on obtient :

$$\deg(V^{-1}V) \leqslant n^d \deg(V)^2.$$

□

5.3 Bounded Height Conjecture

On fixe un entier $n \geqslant 1$. Si V est une variété de $\mathbb{G}_{\mathrm{m}}^n$ alors la *Bounded Height Conjecture* stipule que la hauteur de l'ensemble des points appartenant à un certain ouvert de Zariski de V et à la réunion de tous les sous-groupes algébriques de $\mathbb{G}_{\mathrm{m}}^n$ de codimension au moins $\dim(V)$ est majorée par une constante ne dépendant que de V. Dans [25, Theorem 1], P. Habegger a donné une démonstration de telle conjecture avec des bornes explicites. On va l'énoncer dans le cas correspondant à notre situation mais son résultat est plus général.

Théorème 5.3.1. *Soient V une variété irréductible de $\mathbb{G}_{\mathrm{m}}^3$. Soit T_1 un sous-tore de $\mathbb{G}_{\mathrm{m}}^3$ de dimension 1. Si $\boldsymbol{\alpha} \in V^o \cap T_1$ alors on a :*

$$h(\boldsymbol{\alpha}) \leqslant c_3 \deg(V)^2 \left(h(V) + \deg(V)\right),$$

où $c_3 = 6^{270}$.

Démonstration. Dans le Theorem 1 de [25], on prend $n = 3$, $s = 2$ et $m = 1$ et d'après [25, Equation (3)], on obtient $V^{\mathrm{oa},1} = V^{\mathrm{o}}$. □

La constante c_3 ici est trop grande pour des applications algorithmiques. Pour obtenir une version explicite plus fine, on va expliciter le Theorem 1 de U. Zannier [40, p. 524, Appendix], suffisant dans notre cas, et dont le Theorem 1 de P. Habegger [25] est une généralisation. On va commencer par un lemme d'évitement pour les sous-espaces vectoriels sur $\mathbb{Q}$ (Lemme 5.3.3).

Si $F \in \mathbb{Z}[x_1, \cdots, x_n]$ alors le lemme suivant donne un vecteur $\mathbf{c} \in \mathbb{Z}^n$ tel que $F(\mathbf{c}) \neq 0$ et dont la norme est contrôlé par le degré de F.

Lemme 5.3.2. *Soit $F \in \mathbb{Z}[x_1, \cdots, x_n]$ un polynôme non nul de degré total d. Soient $d_i = \deg_{x_i}(F)$ pour tout $i \in \{1, \cdots, n\}$. Alors il existe $\mathbf{c} = (c_1, \cdots, c_n) \in \mathbb{Z}^n$ tel que $F(\mathbf{c}) \neq 0$ et $|c_i| \leqslant (d_i + 1)/2$ et $\|\mathbf{c}\|_1 \leqslant (d + n)/2$.*

Démonstration. Montrons le résultat par récurrence sur n. Si $n = 1$, $F \in \mathbb{Z}[x]$ est de degré d_1. Notons d_1' la partie entière de $(d_1 + 1)/2$. En particulier, on a $d_1' \leqslant (d_1 + 1)/2 < d_1' + 1$ et donc $d_1 < 2d_1' + 1$. Par suite, il existe $c_1 \in \{-d_1', -d_1' - 1, \cdots, 0, 1, \cdots, d_1'\}$ tel que $F(c_1) \neq 0$. Par suite, on a le résultat pour $n = 1$. Supposons qu'on ait le résultat pour tout polynôme homogène non nul à $n - 1$ variables. On écrit F comme suit :

$$F(x_1, \cdots, x_n) = \sum_{i=0}^{d_n} F_i(x_1, \cdots, x_{n-1}) x_n^i.$$

Le polynôme F_{d_n} est non nul de degré au plus $d - d_n$. D'après l'hypothèse de récurrence, il existe $(c_1, \cdots, c_{n-1}) \in \mathbb{Z}^{n-1}$ tel que $F_{d_n}(c_1, \cdots, c_{n-1}) \neq 0$ et $|c_i| \leqslant (d_i + 1)/2$ (car $\deg_{x_i}(F_{d_n}) \leqslant d_i$) et $\|(c_1, \cdots, c_{n-1})\|_1 \leqslant (d - d_n + n - 1)/2$. Posons

$$\widetilde{F}(x_n) = F(c_1, \cdots, c_{n-1}, x_n) = \sum_{i=0}^{d_n} F_i(c_1, \cdots, c_{n-1}) x_n^i.$$

Donc $\widetilde{F} \in \mathbb{Z}[x_n]$ est non nul de degré d_n. En appliquant le même argument que pour le cas $n = 1$, il existe $c_n \in \mathbb{Z}$ tel que $|c_n| \leqslant (d_n + 1)/2$ et $\widetilde{F}(c_n) \neq 0$. Par suite, on peut prendre $\mathbf{c} = (c_1, \cdots, c_{n-1}, c_n)$ car on a $F(\mathbf{c}) = \widetilde{F}(c_n) \neq 0$ et $|c_i| \leqslant (d_i + 1)/2$ pour tout $i = 1, \cdots, n$. De plus, on a $\|\mathbf{c}\|_1 \leqslant (d - d_n + n - 1)/2 + (d_n + 1)/2 = (d + n)/2$. Cela prouve la récurrence et ainsi on a la conclusion du lemme. □

Lemme 5.3.3. *(Lemme d'évitement) Soient $r, s \geqslant 1$ deux entiers et $X_1, \cdots, X_s$ des sous-espaces vectoriels de $\mathbb{Q}^r$ de dimension $< r$. Alors il existe un vecteur non nul $\mathbf{c} \in \mathbb{Z}^r$ tel que $\mathbf{c} \notin \bigcup_{i=1}^s X_i$ et $\|\mathbf{c}\|_\infty \leqslant (s+1)/2$.*

Démonstration. Remarquons tout d'abord que pour tout $i = 1, \cdots, s$, il existe une application linéaire non nulle $f_i : \mathbb{Q}^r \to \mathbb{Q}$ tel que $f_{i|X_i} = 0$ (puisque $\dim(X_i) < r$, on peut considérer la projection sur $\mathbb{Q}\mathbf{e}$ où $\mathbf{e}$ est un vecteur de la base canonique de $\mathbb{Z}^r$ et $\mathbf{e} \notin X_i$). En multipliant par un certain entier, on peut supposer que chaque f_i est de la forme $\sum_{j=1}^r a_{i,j} x_j$ avec $a_{i,j} \in \mathbb{Z}$. Ensuite, on définit $F = \prod_{i=1}^s f_i \in \mathbb{Z}[x_1, \cdots, x_r]$. Ainsi F est homogène de degré s. On a donc $\deg_{x_i}(F) \leqslant s$ et $F(\mathbf{0}) = 0$. D'après le Lemme 5.3.2, il existe $\mathbf{c} = (c_1, \cdots, c_r) \in \mathbb{Z}^r$ tel que $F(\mathbf{c}) \neq 0$ et $\|\mathbf{c}\|_\infty \leqslant (s+1)/2$. Comme F est homogène et $F(\mathbf{c}) \neq 0$, on a $\mathbf{c} \neq \mathbf{0}$ et $\mathbf{c} \notin \bigcup_{i=1}^s X_i$. □

On va maintenant donner une version explicite du Theorem 1 de U. Zannier [40, p. 524]. Si $F \in \mathbb{C}[\mathbf{x}^{\pm 1}]$ alors on rappelle que $n_F = \#\mathrm{Supp}(F)$, $\deg(F)$ est son degré total, $\deg_\infty(F)$ la maximum de ses degrés partiels et $\|F\|_i$ est la norme L_i du vecteur formé par ses coefficients non nuls. On note :

$$\begin{aligned} D &= \max\left(\deg_\infty(F), \deg_\infty(G)\right) \\ h &= \max(\log \|F\|_1, \log \|G\|_1) \\ N &= \max(\#\mathrm{Supp}(F), \#\mathrm{Supp}(G)). \end{aligned}$$

Proposition 5.3.4. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\mathrm{pgcd}(F, G) = 1$. Notons V la variété de $\mathbb{G}_{\mathrm{m}}^3$ définie par $F = G = 0$. Soit $\mathbf{a} \in \mathbb{Z}^3$ un vecteur primitif et $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^3$. On note T_1 le sous-tore de $\mathbb{G}_{\mathrm{m}}^3$ défini par $T_1 = \{\xi^{\mathbf{a}},\ \xi \in \mathbb{G}_{\mathrm{m}}\}$. Si $\boldsymbol{\alpha} \in V^o \cap \boldsymbol{\zeta} T_1$ alors soit il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ tel que $\|\mathbf{b}\|_\infty \leqslant 2D$ soit on a :*

$$h(\boldsymbol{\alpha}) \leqslant 459 N^3 D^3 h^2.$$

Démonstration. Soit Z une composante irréductible de V contenant $\boldsymbol{\alpha}$. On a $0 \leqslant \dim(Z) \leqslant \dim(V) = 1$. Soit σ une décomposition de F et G suivant Z de la forme :

$$\sigma : \ F = \sum_{i=1}^p F_i \quad \text{et} \quad G = \sum_{j=1}^q G_i,$$

tels que

— les F_i et les G_j sont non nuls

— $\mathrm{Supp}(F_i) \cap \mathrm{Supp}(F_j) = \mathrm{Supp}(G_i) \cap \mathrm{Supp}(G_j) = \emptyset$ pour $i \neq j$
— $F_i = G_j = 0$ sur Z pour tout i, j

On considère une telle décomposition σ de F et G tels que p et q soient maximaux. Pour alléger l'écriture, on pose :

$$r = p + q \quad \text{et} \quad f_i = \begin{cases} F_i & \text{si } 1 \leqslant i \leqslant p, \\ G_{i-p} & \text{si } p+1 \leqslant i \leqslant r. \end{cases}$$

Soit $\widetilde{V}$ la variété de $\mathbb{G}_{\mathrm{m}}^3$ définie par les $f_i = 0$. Alors on a $Z \subseteq \widetilde{V} \subseteq V$. On note $n_i = \#\mathrm{Supp}(f_i)$. On a donc $\sum_{i=1}^{p} n_i = n_F$ et $\sum_{i=p+1}^{r} n_i = n_G$. Comme chaque f_i a au moins deux monômes, on a $n_i \geqslant 2$. On en déduit que $p \leqslant n_F/2$ et $q \leqslant n_G/2$.

Pour $i \in 1, \cdots, r$, on choisit $\boldsymbol{\lambda}_i \in \mathrm{Supp}(f_i)$ et on pose $g_i = \mathbf{x}^{-\boldsymbol{\lambda}_i} f_i$. Dans ce cas on a $\mathbf{0} \in \bigcap_i \mathrm{Supp}(g_i)$. Remarquons que les g_i définissent encore $\widetilde{V}$. On pose :

$$S = \bigcup_i \mathrm{Supp}(g_i).$$

Comme $\mathbf{0} \in \bigcap_i \mathrm{Supp}(g_i)$, on a :

$$\#E \leqslant 1 + \sum_{i=1}^{r} (\#\mathrm{Supp}(g_i) - 1) = 1 + \sum_{i=1}^{r} (n_i - 1) = n_F + n_G - (r-1). \tag{5.3.1}$$

Si $\boldsymbol{\lambda} \in S$ alors on note $\Lambda_{\boldsymbol{\lambda}}$ le sous-groupe de $\mathbb{Z}^3$ engendré par les vecteurs de la forme $\boldsymbol{\mu} - \boldsymbol{\lambda}$ où $\boldsymbol{\mu} \in S$ et $r_{\boldsymbol{\lambda}}$ son rang. Ainsi on a la propriété suivante :

$$\forall \boldsymbol{\lambda} \in S,\ r_{\boldsymbol{\lambda}} = 3. \tag{5.3.2}$$

Supposons d'abord qu'il existe $\boldsymbol{\lambda} \in S$ tel que $\Lambda_{\boldsymbol{\lambda}}$ est de rang $r_{\boldsymbol{\lambda}} < 3$. En multipliant les g_i par le monôme $\mathbf{x}^{-\boldsymbol{\lambda}}$ et en effectuant un changement de variables (par un automorphisme de $\mathbb{G}_{\mathrm{m}}^3$), on se ramène au cas où les g_i dépendent seulement de $r_{\boldsymbol{\lambda}}$ variables. Soit $W \subset \mathbb{G}_{\mathrm{m}}^{r_{\boldsymbol{\lambda}}}$ la variété définie par ces équations. Donc on a $\widetilde{V} \simeq W \times \mathbb{G}_{\mathrm{m}}^{3-r_{\boldsymbol{\lambda}}}$. Ceci contredit le fait que $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ i.e. $\boldsymbol{\alpha}$ n'est pas contenu dans un translaté de sous-tore de $\mathbb{G}_{\mathrm{m}}^3$ contenu dans V. Ainsi $\Lambda_{\boldsymbol{\lambda}}$ est de rang 3 pour tout $\boldsymbol{\lambda} \in S$.

On écrit les g_i sous la forme :

$$g_i = \sum_{\boldsymbol{\lambda} \in \mathrm{Supp}(g_i)} \beta_{i,\boldsymbol{\lambda}} \mathbf{x}^{\boldsymbol{\lambda}} = \sum_{\boldsymbol{\lambda} \in S} \beta_{i,\boldsymbol{\lambda}} \mathbf{x}^{\boldsymbol{\lambda}},$$

où $\beta_{i,\boldsymbol{\lambda}} \coloneqq 0$ si $\boldsymbol{\lambda} \in S \setminus \mathrm{Supp}(g_i)$. Si $\emptyset \neq \Gamma \subsetneq S$, on définit :

$$X_\Gamma = \left\{ (c_1, \cdots, c_r) \in \mathbb{Q}^r \mid \sum_{\boldsymbol{\lambda} \in \Gamma} \left(\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}} \right) \mathbf{x}^{\boldsymbol{\lambda}} = 0 \text{ sur } Z \right\}.$$

Ainsi, X_Γ est un sous-espace vectoriel de $\mathbb{Q}^r$. On va montrer que, pour tout $\emptyset \neq \Gamma \subsetneq S$, $\dim(X_\Gamma) \neq r$. Supposons que pour un certain $\emptyset \neq \Gamma \subsetneq S$, X_Γ soit de dimension r. On a $X_\Gamma = X_{S \setminus \Gamma}$. En effet, si $\mathbf{c} \in \mathbb{Q}^r$ alors on a :

$$\sum_{\boldsymbol{\lambda} \in \Gamma} \left(\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}} \right) \mathbf{x}^{\boldsymbol{\lambda}} + \sum_{\boldsymbol{\lambda} \in S \setminus \Gamma} \left(\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}} \right) \mathbf{x}^{\boldsymbol{\lambda}} = \sum_{i=1}^{r} c_i g_i = 0 \text{ sur } Z.$$

Par suite, quitte à remplacer Γ par $S \setminus \Gamma$, on peut supposer que $\mathbf{0} \in \Gamma$. Pour $i = 1, \cdots, r$, on a :

$$\sum_{\boldsymbol{\lambda} \in \Gamma} \beta_{i,\boldsymbol{\lambda}} \mathbf{x}^{\boldsymbol{\lambda}} = 0 \text{ sur } Z$$

et donc

$$\sum_{\boldsymbol{\lambda} \in \Gamma \cap \mathrm{Supp}(g_i)} \beta_{i,\boldsymbol{\lambda}} \mathbf{x}^{\boldsymbol{\lambda}} = 0 \text{ sur } Z.$$

Or aucune sous-somme de g_i ne s'annule sur Z, alors on a soit $\mathrm{Supp}(g_i) \cap \Gamma = \mathrm{Supp}(g_i)$ (i.e. $\mathrm{Supp}(g_i) \subseteq \Gamma$) ou $\mathrm{Supp}(g_i) \cap \Gamma = \emptyset$. Le deuxième cas ne peut pas être vrai car $\mathbf{0} \in \Gamma \cap (\bigcap_i \mathrm{Supp}(g_i))$. Donc on a $\mathrm{Supp}(g_i) \subseteq \Gamma$ pour tout i et donc $S = \Gamma$. Ceci est une contradiction car $\Gamma \neq S$. On en conclut que, pour tout $\emptyset \neq \Gamma \subsetneq S$, X_Γ n'est pas de dimension r.

On va ensuite définir un polynôme P, ne dépendant que de F et G, tel que P s'annule sur $\widetilde{V}$. Comme S est fini, le nombre de $\emptyset \neq \Gamma \subsetneq S$ est égal à $2^{\#S} - 2$. En remarquant que $X_\Gamma = X_{S \setminus \Gamma}$, le nombre de X_Γ est donc majoré par $t := (2^{\#S} - 2)/2$. Par suite, d'après Le lemme 5.3.3, il existe $\mathbf{c} = (c_1, \cdots, c_r) \in \mathbb{Z}^r$ tel que $\mathbf{c} \notin \bigcup_\Gamma X_\Gamma$, où Γ parcourt l'ensemble $\{\Gamma \mid \emptyset \neq \Gamma \subsetneq S\}$, et tel $\mathbf{c}$ vérifie :

$$0 < \|\mathbf{c}\|_\infty \leqslant (t+1)/2.$$

D'après (5.3.1), on obtient :

$$\|\mathbf{c}\|_\infty \leqslant 2^{n_F + n_G - 1 - r} = 2^{2-r} 2^{N-3}. \tag{5.3.3}$$

On définit maintenant le polynôme P :

$$P = \sum_{i=1}^{r} c_i g_i = \sum_{\boldsymbol{\lambda} \in S} \left(\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}} \right) \mathbf{x}^{\boldsymbol{\lambda}}.$$

Ce polynôme s'annule sur $\widetilde{V}$ car les g_i s'annulent sur $\widetilde{V}$. Pour $\emptyset \neq \Gamma \subsetneq S$, on définit également :

$$P_\Gamma(\mathbf{x}) = \sum_{\boldsymbol{\lambda} \in \Gamma} \left(\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}} \right) \mathbf{x}^{\boldsymbol{\lambda}}.$$

On définit aussi les deux sous-variétés de $\mathbb{G}_{\mathrm{m}}^3$:

$$V_\Gamma = \{\mathbf{x} \in \mathbb{G}_{\mathrm{m}}^3 \mid P_\Gamma(\mathbf{x}) = 0\} \quad \text{et} \quad Z_\Gamma = Z \cap V_\Gamma.$$

On va considérer les deux cas suivants : $\boldsymbol{\alpha} \in \bigcup_\Gamma Z_\Gamma$ ou $\boldsymbol{\alpha} \notin \bigcup_\Gamma Z_\Gamma$. On note :

$$C_1 = \big(\log M(F) \deg(G) + \log M(G) \deg(F) + (4 + \log 2) \deg(F) \deg(G)\big) \max\big(\deg(F), \deg(G)\big) + \deg(F) \deg(G) \log\left(2^{N-3} \left(\|F\|_2 + \|G\|_2\right)\right)$$

et

$$C_2 = 48(N-2) \max(\deg_\infty(F), \deg_\infty(G))^2 \left(\log(N-2) + (N-1) \log\left(2^{N-3}(\|F\|_\infty + \|G\|_\infty)\right)\right).$$

Cas I : Supposons que $\boldsymbol{\alpha} \in \bigcup_\Gamma Z_\Gamma$. On va montrer que $h_2(\boldsymbol{\alpha}) \leqslant C_1$.

Il existe donc un sous-ensemble non vide $\Gamma \subsetneq S$ tel que $\boldsymbol{\alpha} \in Z_\Gamma$. Remarquons que Z_Γ est une sous-variété de Z et $Z_\Gamma \subsetneq Z$ car $\mathbf{c} \notin X_\Gamma$. Alors on a $\dim(Z_\Gamma) = 0$ car $\dim(Z) \leqslant 1$ et Z est irréductible. Ainsi $\boldsymbol{\alpha}$ est un point isolé de $Z \cap V_\Gamma$. D'après le Théorème de Bézout Arithmétique (Théorème 1.6.2.3), on a :

$$h_2(\boldsymbol{\alpha}) \leqslant h(Z)\deg(P_\Gamma) + \log M(P_\Gamma)\deg(Z) + \frac{1}{2}\left(2\log 2 + \frac{11}{6}\right)\deg(Z)\deg(P_\Gamma).$$

D'après le Théorème de Bézout Géométrique (Théorème 1.6.2.1), on a :

$$\deg(Z) \leqslant \deg(V) \leqslant \deg(F)\deg(G).$$

Comme Z est une composante irréductible de $V = V(F, G)$, d'après le Corollaire 1.6.2.4 (qui est une conséquence du Théorème de Bézout Arithmétique), on a :

$$h(Z) \leqslant \log M(F)\deg(G) + \log M(G)\deg(F) + \frac{1}{2}\left(\frac{13}{3} + 2\log 2 + \frac{11}{6}\right)\deg(F)\deg(G).$$

En combinant ces inégalités, on a :

$$h_2(\boldsymbol{\alpha}) \leqslant C_0\deg(P_\Gamma) + \deg(F)\deg(G)\log M(P_\Gamma), \tag{5.3.4}$$

où

$$C_0 = \log M(F)\deg(G) + \log M(G)\deg(F) + (4 + \log 2)\deg(F)\deg(G).$$

On va donner une majoration de $\deg(P_\Gamma)$ et $M(P_\Gamma)$ en fonction de F et G. Par construction de P_Γ, on a $\deg(P_\Gamma) \leqslant \deg(P) \leqslant \max(\deg(F), \deg(G))$ et $M(P_\Gamma) \leqslant \|P_\Gamma\|_2 \leqslant P_\Gamma \leqslant \|P\|_2$. Or, on a :

$$\|P\|_2 \leqslant \|\mathbf{c}\|_\infty \left(\sum_{i=1}^{r} \|g_i\|_2\right) = \|\mathbf{c}\|_\infty \left(\sum_{i=1}^{p} \|F_i\|_2 + \sum_{j=1}^{q} \|G_j\|_2\right).$$

Par l'inégalité de Cauchy-Schwarz, on a :

$$\sum_{i=1}^{p} \|F_i\|_2 = \sum_{i=1}^{p} \sqrt{\|F_i\|_2^2} \leqslant \sqrt{p}\sqrt{\sum_{i=1}^{p} \|F_i\|_2^2} = \sqrt{p}\|F\|_2.$$

On a une inégalité similaire pour la majoration de $\sum_{j=1}^{q} \|G_j\|_2$. Par suite :

$$\|P\|_2 \leqslant \|\mathbf{c}\|_\infty \left(\sqrt{p}\|F\|_2 + \sqrt{q}\|G\|_2\right).$$

D'après (5.3.3), on déduit que :

$$\begin{aligned}\|P\|_2 &\leqslant 2^{N-3}2^{(1-p)+(1-q)}\left(\sqrt{p}\|F\|_2 + \sqrt{q}\|G\|_2\right)\\ &\leqslant 2^{N-3}\left(2^{1-q}\|F\|_2 + 2^{1-p}\|G\|_2\right)\\ &\leqslant 2^{N-3}\left(\|F\|_2 + \|G\|_2\right)\end{aligned}$$

où, au deuxième inégalité, on a utilisé l'inégalité $\sqrt{x} \leqslant x \leqslant 2^{x-1}$ pour $x \geqslant 1$ entier. D'après l'inégalité (5.3.4), on a :

$$h_2(\boldsymbol{\alpha}) \leqslant C_0\max(\deg(F), \deg(G)) + \deg(F)\deg(G)\log\left(2^{N-3}\left(\|F\|_2 + \|G\|_2\right)\right) = C_1.$$

Cas II : $\boldsymbol{\alpha} \notin \bigcup_\Gamma Z_\Gamma$. On va montrer que $h_2(\boldsymbol{\alpha}) \leqslant C_2$.

Comme $\boldsymbol{\alpha} \in \boldsymbol{\zeta} T_1$, il existe $\xi \in \mathbb{G}_{\mathrm{m}}$ tel que $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$ où $\mathbf{a}$ est vu comme un vecteur ligne. Comme P s'annule sur $\widetilde{V}$, P s'annule en $\boldsymbol{\alpha}$. Ainsi, on a :

$$\sum_{\boldsymbol{\lambda} \in S} \left(\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}} \right) \boldsymbol{\zeta}^{\boldsymbol{\lambda}} \xi^{\mathbf{a}\boldsymbol{\lambda}} = 0. \tag{5.3.5}$$

Notons $s = \#S$ et posons $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_s$ les éléments de S. Pour tout $\boldsymbol{\lambda}_j \in E$, on pose $l_j = \mathbf{a}\boldsymbol{\lambda}_j$.

S'il existe $\boldsymbol{\lambda}_i \neq \boldsymbol{\lambda}_j \in S$ tels que $l_i = l_j$ alors le vecteur $\mathbf{b} = \boldsymbol{\lambda}_i - \boldsymbol{\lambda}_j$ est orthogonal à $\mathbf{a}$. Comme $\boldsymbol{\lambda}_i \in \mathrm{Supp}(g_i) \subseteq \mathcal{D}(f_i)$, on a :

$$\|\mathbf{b}\|_\infty \leqslant 2 \max\left(\deg_\infty(F), \deg_\infty(G)\right).$$

On peut maintenant supposer que tous les l_j sont distincts. Quitte à renuméroter les l_j, on peut supposer que $l_1 > l_2 > \cdots > l_s$. Pour $j \in \{1, \cdots, s\}$, on note :

$$\mu_j = \boldsymbol{\zeta}^{\boldsymbol{\lambda}_j} \sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}_j}.$$

On peut récrire (5.3.5) sous la forme :

$$\sum_{j=1}^{s} \mu_j \xi^{l_j} = 0. \tag{5.3.6}$$

Puisque $\boldsymbol{\alpha}$ n'appartient à aucun des Z_Γ, donc aucune sous-somme de (5.3.6) ne s'annule sur un sous-ensemble non vide $\Gamma \neq S$. En particulier, cela implique que les μ_j sont tous non nuls. Pour $j \in \{1, \cdots, s\}$, on pose $m_j = l_j - l_s = \mathbf{a}(\boldsymbol{\lambda}_j - \boldsymbol{\lambda}_s)$. On a alors $m_1 > m_2 > \cdots > m_s = 0$. Or, d'après la propriété (5.3.2), tout sous-groupe $\Lambda_{\boldsymbol{\lambda}}$ est de rang 3. En particulier, $\Lambda_{\boldsymbol{\lambda}_s}$ est de rang 3 et donc il existe trois vecteurs (colonnes) $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in S - \boldsymbol{\lambda}_s$ qui sont linéairement indépendants. En écrivant

$$\begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix} \begin{pmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{pmatrix} = \begin{pmatrix} \mathbf{a}\mathbf{v}_1 \\ \mathbf{a}\mathbf{v}_2 \\ \mathbf{a}\mathbf{v}_3 \end{pmatrix},$$

et utilisant les formules de Cramer, on a :

$$\|\mathbf{a}\|_\infty \leqslant 2\|\mathbf{v}_2\|_\infty \|\mathbf{v}_3\|_\infty |\mathbf{a}\mathbf{v}_1| + 2\|\mathbf{v}_1\|_\infty \|\mathbf{v}_3\|_\infty |\mathbf{a}\mathbf{v}_2| + 2\|\mathbf{v}_1\|_\infty \|\mathbf{v}_2\|_\infty |\mathbf{a}\mathbf{v}_3|. \tag{5.3.7}$$

Puisque $\mathbf{v}_i \in S - \boldsymbol{\lambda}_s$, on a :

$$\|\mathbf{v}_i\|_\infty \leqslant 2 \max\left(\deg_\infty(F), \deg_\infty(G)\right).$$

D'après la définition de m_1, on a :

$$|\mathbf{a}\mathbf{v}_i| \leqslant m_1 \text{ pour tout } i = 1, 2, 3.$$

En combinant ces inégalités, (5.3.7) devient :

$$\|\mathbf{a}\|_\infty \leqslant 24 m_1 \max\left(\deg_\infty(F), \deg_\infty(G)\right)^2. \tag{5.3.8}$$

Par ailleurs, en appliquant le Lemme 4.3.2 à (5.3.6), on a :

$$h(\xi) \leqslant \frac{(s-1)\left(\log(s-1)+h_1(\boldsymbol{\mu})\right)}{m_1}, \tag{5.3.9}$$

où $h_1(\boldsymbol{\mu}) = \sum_{j=1}^{s} h(\mu_j)$. Soit $j \in \{1, \cdots, s\}$. Puisque $\boldsymbol{\zeta}^{\boldsymbol{\lambda}_j} \in \boldsymbol{\mu}_\infty$, on a :

$$h(\mu_j) = h(\boldsymbol{\zeta}^{\boldsymbol{\lambda}_j} \sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}_j}) = h(\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}_j}).$$

Comme $\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}_j} \in \mathbb{Z}$, on en déduit que $h(\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}_j}) = \log|\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}_j}|$. Or on a :

$$|\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}_j}| \leqslant \sum_{i=1}^{r} |c_i \beta_{i,\boldsymbol{\lambda}_j}| \leqslant \|\mathbf{c}\|_\infty \left(p\|F\|_\infty + q\|G\|_\infty\right).$$

D'après (5.3.3), on obtient :

$$|\sum_{i=1}^{r} c_i \beta_{i,\boldsymbol{\lambda}_j}| \leqslant 2^{N-3} 2^{(1-p)+(1-q)} \left(p\|F\|_\infty + q\|G\|_\infty\right) \leqslant 2^{N-3} \ \left(\|F\|_\infty + \|G\|_\infty\right),$$

où on a utilisé à nouveau l'inégalité $x \leqslant 2^{x-1}$ pour $x \geqslant 1$ pour la deuxième inégalité. Ainsi, on a :

$$\begin{aligned} h_1(\boldsymbol{\mu}) &\leqslant \sum_{j=1}^{s} \log(2^{N-3}(\|F\|_\infty + \|G\|_\infty)) \\ &\leqslant s \log\left(2^{N-3}(\|F\|_\infty + \|G\|_\infty)\right). \end{aligned}$$

D'après (5.3.1), on a $s = \#E \leqslant n_F + n_G - (r-1) \leqslant n_F + n_G - 1 = N - 1$. En combinant ces inégalités, (5.3.9) devient :

$$h(\xi) \leqslant \frac{(N-2)\left(\log(N-2) + (N-1)\log\left(2^{N-3}(\|F\|_\infty + \|G\|_\infty)\right)\right)}{m_1}. \tag{5.3.10}$$

D'après le Lemme 1.6.1.3, on a :

$$h(\boldsymbol{\alpha}) \leqslant 2\|\mathbf{a}\|_\infty h(\xi).$$

En combinant (5.3.8) et (5.3.10), on a

$$h(\boldsymbol{\alpha}) \leqslant 48D^2(N-2)\ \left(\log(N-2) + (N-1)\log\left(2^{N-3}(\|F\|_\infty + \|G\|_\infty)\right)\right) = C_2.$$

Enfin, en majorant $\deg(F), \deg(G)$ par $3D$ et $\log M(F), \log M(G)$ par h, on a :

$$\max(C_1, C_2) \leqslant 459N^3D^3h^2.$$

□

5.4 Bornes explicites dans les trois cas : Cas 1, Cas 2 et Cas 3

Dans cette section, on va donner les propositions mentionnées suivant les trois cas et leurs démonstrations. Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$. On note :

$$\begin{aligned} D &= \max\left(\deg_\infty(F), \deg_\infty(G)\right) \\ h &= \max(\log \|F\|_1, \log \|G\|_1) \\ N &= \max(\#\mathrm{Supp}(F), \#\mathrm{Supp}(G)). \end{aligned}$$

Cas 1 : $\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$.

Proposition 5.4.1. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$. Soient $\mathbf{a} \in \mathbb{Z}^3$ un vecteur primitif et $\xi \in \mathbb{G}_{\mathrm{m}} \setminus \boldsymbol{\mu}_\infty$. On note $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$. Soit T_2 le sous-tore de $\mathbb{G}_{\mathrm{m}}^n$ défini par (5.1.2). Si $\boldsymbol{\alpha}$ est un point isolé de $V(F,G) \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^o$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :*

$$\|\mathbf{b}\|_\infty \leqslant 107406 N^3 D^5 h^2 2^c \frac{\log(150552 N^3 D^7 h^2 2^c)^4}{\log\log(376380 N^3 D^7 h^2 2^c)^3}.$$

Si, de plus, $\boldsymbol{\zeta} \in \{\pm 1\}^3$ alors on a :

$$\|\mathbf{b}\|_\infty \leqslant 99144 N^3 D^5 h^2 \left(\frac{\log(74358 N^3 D^7 h^2)}{\log\log(74358 N^3 D^7 h^2)}\right)^3.$$

Démonstration. On note $V = V(F,G)$ et $T_1 = \{\gamma^{\mathbf{a}} \in \mathbb{G}_{\mathrm{m}}^3,\ \gamma \in \overline{\mathbb{Q}}^*\}$. On pose $P = \xi^{\mathbf{u}} - 1$ où $\mathbf{u}$ est défini comme dans (5.1.1). On a donc $T_2 = V(P)$. Par hypothèse, on a $\boldsymbol{\alpha} \in V^{\mathrm{o}} \cap \boldsymbol{\zeta} T_1$. D'après la Proposition 5.3.4, soit il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ tel que $\|\mathbf{b}\| \leqslant 2D$ soit on a :

$$h(\boldsymbol{\alpha}) \leqslant 459 N^3 D^3 h^2. \tag{5.4.1}$$

Comme la borne dans la majoration est plus petit que celle annoncée dans la proposition, on suppose que l'on est dans le second cas. On note $C = 459 N^3 D^3 h^2$. D'après le Lemme 1.6.1.3, on a :

$$\|\mathbf{a}\|_\infty h(\xi) \leqslant h(\boldsymbol{\alpha}) \leqslant C. \tag{5.4.2}$$

Par définition de P, on a $\deg(P) \leqslant \|\mathbf{u}\|_1$. D'après (5.1.1), on a :

$$\deg(P) \leqslant \sqrt{3}\|\mathbf{u}\|_2 \leqslant \sqrt{3\gamma_2}\|\mathbf{a}\|_2^{1/2} \leqslant \sqrt{2}\|\mathbf{a}\|_\infty^{1/2}.$$

On pose $\mathbb{K} = \mathbb{Q}(\boldsymbol{\zeta})$ et $d = [\mathbb{K}(\xi) : \mathbb{K}]$. Puisque $\mathbf{a}$ est primitif, on a $\mathbb{K}(\boldsymbol{\alpha}) = \mathbb{K}(\xi)$ et donc $d = [\mathbb{K}(\boldsymbol{\alpha}) : \mathbb{K}]$. Comme $\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$, d'après le Théorème 1.6.2.1, on a :

$$d = [\mathbb{K}(\boldsymbol{\alpha}) : \mathbb{K}] \leqslant \deg(F)\deg(G)\deg(P) \leqslant \sqrt{2}\deg(F)\deg(G)\|\mathbf{a}\|_\infty^{1/2}.$$

En majorant $\deg(F)$ et $\deg(G)$ par $3D$, on a :

$$d \leqslant 9\sqrt{2} D^2 \|\mathbf{a}\|_\infty^{1/2}. \tag{5.4.3}$$

Supposons $\boldsymbol{\zeta} \in \{\pm 1\}^3$:

Dans ce cas $\mathbb{K} = \mathbb{Q}$. Par définition de la fonction ℓ (voir la Sous-section 1.2.2 pour la défination), on a $1/\log M(\xi) \leqslant \ell(d)$. D'après (5.4.2), on en déduit que :

$$\|\mathbf{a}\|_\infty \leqslant C\frac{[\mathbb{Q}(\xi):\mathbb{Q}]}{\log M(\xi)} \leqslant Cd\ell(d).$$

D'après (5.4.3), on en déduit que :

$$\|\mathbf{a}\|_\infty^{1/2} \leqslant 9\sqrt{2}CD^2\ell(d). \tag{5.4.4}$$

Cela montre que la norme de $\mathbf{a}$ est majorée par une constante ne dépendant que de F et G. Déterminons explicitement une majoration pour la norme de $\mathbf{a}$. En utilisant le fait que ℓ est croissante et en multipliant (5.4.4) par $9\sqrt{2}D^2$, celle-ci peut s'écrire sous la forme :

$$X \leqslant C_1\ell(X)$$

où

$$X = 9\sqrt{2}D^2\|\mathbf{a}\|_\infty^{1/2} \quad \text{et} \quad C_1 = (9\sqrt{2}D^2)^2C = 74358N^3D^7h^2.$$

Soit τ la fonction définie par $\tau(x) = 4(\log(x)/\log\log(x))^3$ pour tout $x \geqslant 3$. D'après le Théorème 1.2.2.3, on en déduit que $\ell(X) \leqslant \tau(X)$ car $X \geqslant 3$. Comme $C_1 \geqslant 2$ et $3 \leqslant X \leqslant C_1\tau(X)$, d'après le Lemme A.2.2, on a :

$$X \leqslant 3C_1\tau(4C_1).$$

En remplaçant X et C_1 par leur expression respective, on en déduit que :

$$\|\mathbf{a}\|_\infty^{1/2} \leqslant 12393\sqrt{2}N^3D^5h^2\tau(4C_1).$$

En utilisant la défition de τ, on en déduit que :

$$\|\mathbf{a}\|_\infty^{1/2} \leqslant 49572\sqrt{2}N^3D^5h^2\left(\frac{\log(74358N^3D^7h^2)}{\log\log(74358N^3D^7h^2)}\right)^3.$$

D'après le Théorème 1.4.1, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_2 \leqslant (2/\sqrt{3})^{1/2}\|\mathbf{a}\|_2^{1/2}.$$

En simplifiant les expressions dans les $\log$, on en déduit que :

$$\|\mathbf{b}\|_2 \leqslant 99144N^3D^5h^2\left(\frac{\log(74358N^3D^7h^2)}{\log\log(74358N^3D^7h^2)}\right)^3.$$

Supposons $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^3$:

En appliquant le Théorème 1.2.3.2 (avec $\mathbb{K} = \mathbb{Q}$ et $\mathbb{L} = \mathbb{Q}(\boldsymbol{\zeta})$), on en déduit :

$$\frac{1}{h(\xi)} \leqslant d\frac{2^c\log(2d)^4}{\log\log(5d)^3} = d\lambda(d).$$

où c est une constante absolue strictement positive. En remplaçant $\ell(d)$ par $\lambda(d)$ dans le cas précédent et refaisant le même calcul, on a :

$$\|\mathbf{a}\|_\infty^{1/2} \leqslant 9\sqrt{2}CD^2\lambda(d).$$

D'après le Lemme A.2.3, λ est croissante. En utilisant ce fait et la majoration (5.4.3) de d, on obtient :

$$X \leqslant 2^c C\frac{\log(2X)^4}{\log\log(5X)^3}$$

où

$$X = 9\sqrt{2}D^2\|\mathbf{a}\|_\infty^{1/2} \quad \text{et} \quad C_2 = (9\sqrt{2}D^2)^2C2^c = 162C2^c.$$

Puisque $C_2 \geqslant 44$, d'après le Lemme A.2.4, on a :

$$X \leqslant 13C_2\frac{\log(2C_2)^4}{\log\log(5C_2)^3}.$$

En remplaçant X, C_2 et C par leur expression respective, on en déduit que :

$$\|\mathbf{a}\|_2^{1/2} \leqslant 53703\sqrt{2}N^3D^5h^22^c\frac{\log(150552N^3D^7h^22^c)^4}{\log\log(376380N^3D^7h^22^c)^3}.$$

D'après le Théorème 1.4.1, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_2 \leqslant (2/\sqrt{3})^{1/2}\|\mathbf{a}\|_2^{1/2}.$$

Par suite, on a :

$$\|\mathbf{b}\|_2 \leqslant 107406N^3D^5h^22^c\frac{\log(150552N^3D^7h^22^c)^4}{\log\log(376380N^3D^7h^22^c)^3}.$$

□

Cas 2 : $\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta}T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$.

Proposition 5.4.2. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\mathrm{pgcd}(F, G) = 1$. Soient $\mathbf{a} \in \mathbb{Z}^3$ un vecteur non nul, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^3$ et $\xi \in \mathbb{G}_{\mathrm{m}} \setminus \boldsymbol{\mu}_\infty$ tels que $\boldsymbol{\zeta}\xi^{\mathbf{a}} \in V(F, G)$. On note $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$ et $V = V(F, G)$. Soit T_2 un sous-tore de $\mathbb{G}_{\mathrm{m}}^3$ de dimension 2. Si $\boldsymbol{\alpha} \in V^o \cap \boldsymbol{\zeta}T_2$ et $\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta}T_2$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :*

$$\|\mathbf{b}\|_\infty \leqslant 1458D^4.$$

Démonstration. Puisque $\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta}T_2$, il existe une composante irréductible $Y \subseteq V \cap \boldsymbol{\zeta}T_2$ de dimension 1 et contenant $\boldsymbol{\alpha}$. En particulier, Y est une composante irréductible de V car $\dim(Y) = 1 = \dim(V)$. Comme $\boldsymbol{\alpha} \in V^{\mathrm{o}}$, Y n'est pas un translaté de sous-tore de $\mathbb{G}_{\mathrm{m}}^3$. On note φ le morphisme défini par :

$$\begin{aligned}\varphi : \mathbb{G}_{\mathrm{m}}^3 \times \mathbb{G}_{\mathrm{m}}^3 &\longrightarrow \mathbb{G}_{\mathrm{m}}^3\\ (\mathbf{x}, \mathbf{y}) &\mapsto \mathbf{x}^{-1}\mathbf{y}\end{aligned}$$

On note $Y^{-1}Y$ l'image de Y par φ. Puisque $Y \subseteq \boldsymbol{\zeta} T_2$, on a $Y^{-1}Y \subseteq T_2$. De plus, $Y^{-1}Y$ est irréductible car $Y \times Y$ est irréductible et l'application φ est continue. Comme $\boldsymbol{\alpha} \in Y$, on a $\boldsymbol{\alpha}^{-1}Y \subseteq Y^{-1}Y$. Ainsi, on a :

$$1 = \dim(\boldsymbol{\alpha}^{-1}Y) \leqslant \dim(Y^{-1}Y) \leqslant \dim(T_2) = 2.$$

Supposons $\dim(Y^{-1}Y) = 1$. Puisque $Y^{-1}Y$ est irréductible, on a l'égalité $\boldsymbol{\alpha}^{-1}Y = Y^{-1}Y$. D'après la Proposition 5.2.1, Y est un translaté de sous-groupe algébrique de $\mathbb{G}_{\mathrm{m}}^3$. Comme Y est irréductible, Y est un translaté de sous-tore de $\mathbb{G}_{\mathrm{m}}^3$. Ceci contredit l'hypothèse $\boldsymbol{\alpha} \in V^{\mathrm{o}}$. On en déduit que $\dim(Y^{-1}Y) = 2$.

Vu que $Y^{-1}Y \subseteq T_2$ et T_2 est aussi un sous-tore de dimension 2, on a $T_2 = Y^{-1}Y$. D'après le Proposition 5.2.2, on a :

$$\deg(T_2) \leqslant 3^2 \deg(Y)^2.$$

Puisque Y est une composante irréductible de V, on a $\deg(Y) \leqslant \deg(V)$. D'après le Théorème de Bézout Géométrique, on a $\deg(V) \leqslant \deg(F)\deg(G)$. Ainsi, on obtient :

$$\deg(T_2) \leqslant 9(\deg(F)\deg(G))^2.$$

Puisque T_2 est un sous-tore de $\mathbb{G}_{\mathrm{m}}^3$ de dimension 2, T_2 est défini par un vecteur primitif $\mathbf{b} \in \mathbb{Z}^3$. Comme $\xi^{\mathbf{a}} \in T_2$ et $\xi \notin \boldsymbol{\mu}_\infty$, on a $\mathbf{a} \cdot \mathbf{b} = 0$. Enfin, on a :

$$\max(\|\mathbf{b}_-\|_1, \|\mathbf{b}_+\|_1) = \deg(T_2) \leqslant 9(\deg(F)\deg(G))^2,$$

où $\mathbf{b}_+$ (respectivement $\mathbf{b}_-$) est le vecteur obtenu à partir de $\mathbf{b}$ en ne gardant que les coordonnées dont le signe est positif (respectivement négatif). Enfin, on en déduit que :

$$\|\mathbf{b}_1\|_1 \leqslant 2\max(\|\mathbf{b}_{1,+}\|_1, \|\mathbf{b}_{1,-}\|_1) \leqslant 18(\deg(F)\deg(G))^2.$$

En majorant $\deg(F)$ et $\deg(G)$ par $3D$, on a la majoration voulue. □

Cas 3 : $\boldsymbol{\alpha} \notin V^{\mathrm{o}}$.

Proposition 5.4.3. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\mathrm{pgcd}(F, G) = 1$. On note $V = V(F, G)$. Soient $\mathbf{a} \in \mathbb{Z}^3$ un vecteur non nul, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^3$ et $\xi \in \mathbb{G}_{\mathrm{m}} \setminus \boldsymbol{\mu}_\infty$. On note $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$. Si $\boldsymbol{\alpha} \in V^a$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :*

$$\|\mathbf{b}\|_\infty \leqslant \frac{225}{4} D^4 h\ell(254D^6).$$

Démonstration. Comme $\boldsymbol{\alpha} \in V^{\mathrm{a}}$, $\boldsymbol{\alpha}$ appartient à un translaté de sous-tore $\boldsymbol{\alpha}T \subseteq V$ de dimension non nulle. Comme $\mathrm{pgcd}(F, G) = 1$, V est de dimension 1 et donc il en est de même pour T. Ainsi, l'inclusion $\boldsymbol{\alpha}T \subseteq V$ est maximal. On va construire un automorphisme φ de $\mathbb{G}_{\mathrm{m}}^3$ tel que $\varphi(T) = \{\mathbf{y} \in \mathbb{G}_{\mathrm{m}}^3 \mid y_1 = y_2 = 1\}$. D'après la Proposition 1.3.2.3, il existe trois vecteurs $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \boldsymbol{\mu}_3$ formant une base de $\mathbb{Z}^3$ tels que :

— T est défini par les équations $\mathbf{x}^{\boldsymbol{\mu}_1} - 1 = \mathbf{x}^{\boldsymbol{\mu}_2} - 1 = 0$,
— ces trois vecteurs sont définis comme suit :

$$\begin{cases} \boldsymbol{\mu}_1 = & c_1\boldsymbol{\lambda}_1, \\ \boldsymbol{\mu}_2 = & c_{2,1}\boldsymbol{\lambda}_1 + c_2\boldsymbol{\lambda}_2, \\ \boldsymbol{\mu}_3 = & c_{3,1}\boldsymbol{\lambda}_1 + c_{3,2}\boldsymbol{\lambda}_2 + c_3\boldsymbol{\lambda}_3, \end{cases} \tag{5.4.5}$$

où $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \mathcal{D}(F) \cup \mathcal{D}(G)$, $\boldsymbol{\lambda}_3$ est un vecteur de la base standard de $\mathbb{Z}^3$, les $c_{i,j}$ (pour $i = 2, 3$ et $j = 1, i-1$) et c_k (pour $k = 1, 2, 3$) sont des nombres rationnels tels que $|c_{i,j}| \leqslant 1/2$ et $0 < c_k \leqslant 1$. Notons M la matrice dont les colonnes sont les vecteurs $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \boldsymbol{\mu}_3$. On considère l'automorphisme φ_M de $\mathbb{G}_{\mathrm{m}}^3$ défini par :

$$\begin{aligned} \varphi_M : \mathbb{G}_{\mathrm{m}}^3 &\longrightarrow \mathbb{G}_{\mathrm{m}}^3 \\ \mathbf{x} &\mapsto \mathbf{x}^M = (\mathbf{x}^{\boldsymbol{\mu}_1}, \mathbf{x}^{\boldsymbol{\mu}_2}, \mathbf{x}^{\boldsymbol{\mu}_3}). \end{aligned}$$

On a alors :

$$\varphi_M(T) = \{\mathbf{y} \in \mathbb{G}_{\mathrm{m}}^3 \mid y_1 = y_2 = 1\}.$$

En effet, en notant $T' \coloneqq \{\mathbf{y} \in \mathbb{G}_{\mathrm{m}}^3 \mid y_1 = y_2 = 1\}$, on a $\varphi_M(T) \subseteq T'$ car T est défini par les équations $\mathbf{x}^{\boldsymbol{\mu}_1} = \mathbf{x}^{\boldsymbol{\mu}_2} = 1$. Comme $\dim(\varphi_M(T)) = \dim(T')$ et T' est irréductible, on a l'égalité.

Puisque $\{\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \boldsymbol{\mu}_3\}$ forme une base de $\mathbb{Z}^3$, $M \in \mathrm{GL}_n(\mathbb{Z})$. On considère le changement de variable $\mathbf{x} = \varphi_M^{-1}(\mathbf{y}) = \mathbf{y}^{M^{-1}}$. On écrit :

$$F(\mathbf{y}^{M^{-1}}) = \sum_{i \in I} F_i(y_1, y_2)\, y_3^i \quad \text{et} \quad G(\mathbf{y}^{M^{-1}}) = \sum_{j \in J} G_j(y_1, y_2)\, y_3^j. \tag{5.4.6}$$

On considère la sous-variété W de $\mathbb{G}_{\mathrm{m}}^2$ définie par :

$$W = \{(y_1, y_2) \in \mathbb{G}_{\mathrm{m}}^2 \mid F_i(y_1, y_2) = G_j(y_1, y_2) = 0, \forall i \in I, j \in J\}.$$

On a alors :

$$\begin{aligned} (y_1, y_2) \in W &\iff F_i(y_1, y_2) = G_j(y_1, y_2) = 0,\ \forall i \in I, j \in J, \\ &\iff F(\varphi_M^{-1}(\mathbf{y})) = G(\varphi_M^{-1}(\mathbf{y})) = 0,\ \forall y_3 \in \mathbb{G}_{\mathrm{m}}, \\ &\iff \varphi_{M^{-1}}(\mathbf{y}) \in V,\ \forall y_3 \in \mathbb{G}_{\mathrm{m}}, \\ &\iff \mathbf{y} \in \varphi_M(V),\ \forall y_3 \in \mathbb{G}_{\mathrm{m}}. \end{aligned}$$

Ainsi, on obtient :

$$W = \{(y_1, y_2) \in \mathbb{G}_{\mathrm{m}}^2 \mid \forall y_3 \in \mathbb{G}_{\mathrm{m}},\ (y_1, y_2, y_3) \in \varphi_M(V)\}. \tag{5.4.7}$$

Par conséquent, on a $W \times \mathbb{G}_{\mathrm{m}} \subseteq \varphi_M(V)$ et donc :

$$\dim(W) + 1 = \dim(W \times \mathbb{G}_{\mathrm{m}}) \leqslant \dim(\varphi_M(V)) = \dim(V) = 1.$$

On en déduit que W est de dimension nulle dans $\mathbb{G}_{\mathrm{m}}^2$. Ensuite, on note $\boldsymbol{\beta}$ l'image de $\boldsymbol{\alpha}$ par φ_M i.e.

$$\boldsymbol{\beta} = (\boldsymbol{\zeta}^{\boldsymbol{\mu}_1} \xi^{\mathbf{a}\boldsymbol{\mu}_1}, \boldsymbol{\zeta}^{\boldsymbol{\mu}_2} \xi^{\mathbf{a}\boldsymbol{\mu}_2}, \boldsymbol{\zeta}^{\boldsymbol{\mu}_3} \xi^{\mathbf{a}\boldsymbol{\mu}_3}).$$

On pose $\boldsymbol{\beta}' = (\beta_1, \beta_2)$. On a :

$$\begin{aligned} \boldsymbol{\beta}' \times \mathbb{G}_{\mathrm{m}} &= \{(\beta_1, \beta_2, \beta_3 y_3) \in \mathbb{G}_{\mathrm{m}}^3,\ y_3 \in \mathbb{G}_{\mathrm{m}}\} \\ &= \boldsymbol{\beta}\varphi(T) \quad \text{car} \quad \varphi(T) = \{\mathbf{y} \in \mathbb{G}_{\mathrm{m}}^n \mid y_1 = y_2 = 1\} \\ &= \varphi_M(\boldsymbol{\alpha} T) \\ &\subseteq \varphi(V). \end{aligned}$$

D'après (5.4.7), on en déduit que $\boldsymbol{\beta}' \in W$. Comme $\dim(W) = 0$, $(\boldsymbol{\zeta}^{\boldsymbol{\mu}_1}\xi^{\mathbf{a}\boldsymbol{\mu}_1}, \boldsymbol{\zeta}^{\boldsymbol{\mu}_2}\xi^{\mathbf{a}\boldsymbol{\mu}_2})$ est un point isolé de W. D'après le Corollaire 3.2.2, il existe un vecteur non nul $(\eta_1, \eta_2) \in \mathbb{Z}^2$ orthogonal au vecteur $(\mathbf{a}\boldsymbol{\mu}_1, \mathbf{a}\boldsymbol{\mu}_2) \in \mathbb{Z}^2$ tel que pour $i = 1, 2$:

$$|\eta_i| \leqslant 2D_W h_W \ell(2D_W^2), \tag{5.4.8}$$

où

$$D_W = \max_{i\in I, j\in J}(\max(\deg_\infty(F_i), \deg_\infty(G_j))) \quad \text{et} \quad h_W = \max_{i\in I, j\in J}(\max(\log\|F_i\|_1, \log\|G_j\|_1)).$$

On considère le vecteur $\mathbf{b}$ défini par $\mathbf{b} = \eta_1\boldsymbol{\mu}_1 + \eta_2\boldsymbol{\mu}_2$. On a $\mathbf{b} \neq 0$ car (η_1, η_2) est non nul et $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2$ sont linéairement indépendants. Comme (η_1, η_2) est orthogonal à $(\mathbf{a}\boldsymbol{\mu}_1, \mathbf{a}\boldsymbol{\mu}_2)$, on a $\mathbf{ab} = 0$. En utilisant (5.4.5), on a :

$$\begin{aligned}\|\mathbf{b}\|_\infty &\leqslant |\eta_1|\|\boldsymbol{\mu}_1\|_\infty + |\eta_2|\|\boldsymbol{\mu}_2\|_\infty\\ &\leqslant |\eta_1|\|c_1\boldsymbol{\lambda}_1\|_\infty + |\eta_2|\|c_{21}\boldsymbol{\lambda}_1 + c_2\boldsymbol{\lambda}_2\|_\infty\\ &\leqslant (|\eta_1| + (3/2)|\eta_2|)\, D.\end{aligned}$$

D'après (5.4.8), on en déduit que :

$$\|\mathbf{b}\|_\infty \leqslant 5DD_W h_W \ell(2D_W^2). \tag{5.4.9}$$

Il reste à déterminer une majoration de h_W et D_W en fonction de h et D. Par construction des F_i et G_j, on a $\|F_i\|_1 \leqslant \|F\|_1$ et $\|G_j\|_1 \leqslant \|G\|_1$. On a donc $h_W \leqslant \max(\log\|F\|_1, \log\|G\|_1) = h$. Par ailleurs, les exposants des F_i sont donnés par les vecteurs $M^{-1}\boldsymbol{\lambda}$ où $\boldsymbol{\lambda}$ parcourt $\mathrm{Supp}(F)$. D'après les formules de Cramer, on a :

$$M^{-1}\boldsymbol{\lambda} = \pm\left((\boldsymbol{\mu}_2 \wedge \boldsymbol{\mu}_3)\boldsymbol{\lambda}, (\boldsymbol{\mu}_3 \wedge \boldsymbol{\mu}_1)\boldsymbol{\lambda}, (\boldsymbol{\mu}_1 \wedge \boldsymbol{\mu}_2)\boldsymbol{\lambda}\right).$$

Ainsi, on a :

$$\begin{aligned}\deg_{y_1}(F_i) &\leqslant \sup_{\boldsymbol{\lambda},\boldsymbol{\lambda}'\in\mathrm{Supp}(F)} |(\boldsymbol{\mu}_2 \wedge \boldsymbol{\mu}_3)(\boldsymbol{\lambda} - \boldsymbol{\lambda}')|\\ &\leqslant \|(\boldsymbol{\mu}_2 \wedge \boldsymbol{\mu}_3)\|_1 \sup_{\boldsymbol{\lambda},\boldsymbol{\lambda}'\in\mathrm{Supp}(F)} \|\boldsymbol{\lambda} - \boldsymbol{\lambda}'\|_\infty\\ &\leqslant \|(\boldsymbol{\mu}_2 \wedge \boldsymbol{\mu}_3)\|_1 \deg_\infty(F)\\ &\leqslant \|(\boldsymbol{\mu}_2 \wedge \boldsymbol{\mu}_3)\|_1 D,\end{aligned}$$

où on a utilisé le fait que $|\mathbf{u}\cdot\mathbf{v}| \leqslant \|\mathbf{u}\|_1\|\mathbf{v}\|_\infty$ dans la deuxième ligne. Notons $D_1 = \max(\deg_1(F), \deg_1(G))$. En utilisant (5.4.5) et les majorations sur les $c_{i,j}$ et c_k, on en déduit que :

$$\begin{aligned}\|\boldsymbol{\mu}_2 \wedge \boldsymbol{\mu}_3\|_1 &\leqslant \frac{3}{4}\|\boldsymbol{\lambda}_1 \wedge \boldsymbol{\lambda}_2\|_1 + \frac{1}{2}\|\boldsymbol{\lambda}_1 \wedge \boldsymbol{\lambda}_3\|_1 + \|\boldsymbol{\lambda}_2 \wedge \boldsymbol{\lambda}_3\|_1,\\ &\leqslant \frac{3}{4}\|\boldsymbol{\lambda}_1\|_1\|\boldsymbol{\lambda}_2\|_1 + \frac{1}{2}\|\boldsymbol{\lambda}_1\|_1\|\boldsymbol{\lambda}_3\|_1 + \|\boldsymbol{\lambda}_2\|_1\|\boldsymbol{\lambda}_3\|_1,\\ &\leqslant \frac{3}{4}D_1\left(D_1 + 2\right),\end{aligned}$$

où on utilise le fait que $\|\mathbf{u} \wedge \mathbf{v}\|_1 \leqslant \|\mathbf{u}\|_1\|\mathbf{v}\|_1$ dans la deuxième ligne. On en déduit que :

$$\deg_{y_1}(F_i) \leqslant (3/4)DD_1(D_1 + 2).$$

On a une même majoration pour $\deg_{y_1}(G_j)$. En appliquant le même procédé, on trouve :

$$\deg_{y_2}(F_i) \leqslant \|(\boldsymbol{\mu}_3 \wedge \boldsymbol{\mu}_1)\|_1 D \leqslant (1/2)DD_1(D_1+2).$$

On a aussi une même majoration pour $\deg_{y_2}(G_j)$. On obtient :

$$D_W \leqslant (3/4)DD_1(D_1+2).$$

Comme $D_1 \leqslant 3D$, on en déduit que :

$$D_W \leqslant (3^2 5/4)D^3.$$

Enfin, comme la fonction ℓ est croissante, (5.4.9) devient :

$$\begin{aligned}\|\mathbf{b}\|_\infty &\leqslant 5D(3^2 5/4)D^3 h\ell(2(3^2 5/4)^2 D^6)\\ &= (3^2 5^2/4)D^4 h\ell(3^4 5^2 D^6/2^3)\\ &\leqslant (225/4)D^4 h\ell(254D^6).\end{aligned}$$

Cela complète la preuve de la proposition. □

5.5 Version explicite de la Conjecture de Schinzel

Suivant l'approche BMZ, on a une version explicite du Théorème 2 dans le cas $n = 3$. On note :

$$\begin{aligned}D &= \max\left(\deg_\infty(F), \deg_\infty(G)\right)\\ h &= \max(\log\|F\|_1, \log\|G\|_1)\\ N &= \max(\#\mathrm{Supp}(F), \#\mathrm{Supp}(G)).\end{aligned}$$

Théorème 5.5.1. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\mathrm{pgcd}(F,G) = 1$. Soient $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$ et $\mathbf{a} \in \mathbb{Z}^3$. On pose $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$. Si $\boldsymbol{\alpha} \in V(F,G)$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ et tel que :*

$$\|\mathbf{b}\|_\infty \leqslant 107406N^3D^5h^2 2^c \frac{\log(150552N^3D^7h^2 2^c)^4}{\log\log(376380N^3D^7h^2 2^c)^3}.$$

où c est une constante absolue strictement positif. Si, de plus, $\boldsymbol{\zeta} \in \{\pm 1\}^3$ alors on a :

$$\|\mathbf{b}\|_\infty \leqslant 99144N^3D^5h^2\left(\frac{\log(74358N^3D^7h^2)}{\log\log(74358N^3D^7h^2)}\right)^3.$$

Démonstration. Quitte à remplacer ξ par $\xi^{\mathrm{pgcd}(a_1,a_2,a_3)}$, on peut supposer que $\mathbf{a}$ est primitif. On note :

$$V = V(F,G) \quad \text{et} \quad T_1 = \left\{\xi^{\mathbf{a}} \in \mathbb{G}_{\mathrm{m}}^3,\ \xi \in \overline{\mathbb{Q}}^*\right\}.$$

D'après le Théorème 1.4.1, il existe un vecteur non nul $\mathbf{u} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{u}\|_2 \leqslant \sqrt{\gamma_2}\|\mathbf{a}\|_2^{1/2},$$

où $\gamma_2 = 2/\sqrt{3}$ est la constante d'Hermite en dimension 2. Quitte à diviser $\mathbf{u}$ par son pgcd, on peut supposer que $\mathbf{u}$ est primitif. On note T_2 le sous-tore de $\mathbb{G}_{\mathrm{m}}^3$ défini par le vecteur $\mathbf{u}$ i.e.

$$T_2 = \{\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^3 \mid \boldsymbol{\alpha}^{\mathbf{u}} = 1\}.$$

Si $\boldsymbol{\alpha} \in V^{\mathrm{a}}$ alors d'après la Proposition 5.4.3, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_\infty \leqslant 225 D^4 h \left(\frac{\log(254D^6)}{\log\log(254D^6)}\right)^3.$$

Si $\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ alors d'après la Proposition 5.4.2, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_\infty \leqslant 1458 D^4.$$

Si $\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ alors d'après la Proposition 5.4.1, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_\infty \leqslant 99144 N^3 D^5 h^2 \left(\frac{\log(74358 N^3 D^7 h^2)}{\log\log(74358 N^3 D^7 h^2)}\right)^3 \quad \text{si } \boldsymbol{\zeta} \in \{\pm 1\}^3,$$

et

$$\|\mathbf{b}\|_\infty \leqslant 107406 N^3 D^5 h^2 2^c \frac{\log(150552 N^3 D^7 h^2 2^c)^4}{\log\log(376380 N^3 D^7 h^2 2^c)^3} \quad \text{sinon.}$$

En prenant le maximum entre ces trois bornes, on a le résultat voulu. □

6. Cas $n = 3$: approche R

Dans ce chapitre, on présente une nouvelle approche, encore dans le cas $n = 3$, que l'on développera ensuite dans le Chapitre 8 pour n quelconque. Cette approche, que l'on appelle *approche R* (comme résultant), est similaire à l'approche BMZ décrite dans le Chapitre 5. La nouveauté de la preuve consiste à utiliser une majoration de type Bézout Arithmétique (Proposition 3.1.7) pour les points isolés, que l'on obtient à l'aide du résultant.

On va aussi décrire un algorithme qui permet de calculer les sous-tores de $\mathbb{G}_{\mathrm{m}}^n$ dont un translaté est contenu dans V et y est maximal (Algorithme 11) pour n quelconque. Dans le cas particulier $n = 3$, on va déduire, à l'aide de cet algorithme, une procédure permettant de calculer explicitement les vecteurs $\mathbf{b} \in \mathbb{Z}^3$ du Théorème 2 dans le cas où $\boldsymbol{\zeta}\xi^{\mathbf{a}} \in V^{\mathrm{a}}$ (Algorithme 12).

6.1 Présentation de l'approche

Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\mathrm{pgcd}(F, G) = 1$. Soient $\mathbf{a} \in \mathbb{Z}^3$ un vecteur primitif et $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^3$. On note :

$$V = V(F, G) \quad \text{et} \quad T_1 = \left\{ \xi^{\mathbf{a}} \in \mathbb{G}_{\mathrm{m}}^3,\ \xi \in \overline{\mathbb{Q}}^* \right\}.$$

On s'intéresse aux points $\boldsymbol{\alpha} \in V \cap \boldsymbol{\zeta} T_1$ qui ne sont pas de torsion. On cherche à déterminer un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ et dont la norme est majorée par une constante ne dépendant que de F et G. À l'aide du Lemme 1.4.2, on construit un sous-tore auxiliaire T_2 de $\mathbb{G}_{\mathrm{m}}^3$ de dimension 2 contenant T_1 et tel que $\deg(T_2) \ll \deg(T_1)^{1/2}$. On rappelle que V^{a} est la réunion des translatés de sous-tores de dimension non nulle contenus dans V et $V^{\mathrm{o}} = V \setminus V^{\mathrm{a}}$. On est alors dans l'un des trois cas suivants :

Cas 1 : $\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$ (Proposition 6.2.2). Dans ce cas, on montre que la norme de $\mathbf{a}$ est majorée uniquement en fonction de F et G. En écrivant $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$, l'idée consiste d'une part à minorer la hauteur de $h(\xi)$ soit en utilisant la minoration de Dobrowolski soit la minoration relative de F. Amoroso et U. Zannier et d'autre part à majorer la hauteur de $\boldsymbol{\alpha}$ en utilisant la majoration de type Bézout arithmétique. La Proposition 6.2.2 est valable pour n quelconque mais n'est explicite que pour $\boldsymbol{\zeta} \in \{\pm 1\}^n$. Pour déduire un vecteur $\mathbf{b}$ ayant les propriétés requises, on peut utiliser le Théorème 1.4.1.

Cas 2 : $\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ (Proposition 5.4.2).

Cas 3 : $\boldsymbol{\alpha} \notin V^{\mathrm{o}}$ (Proposition 5.4.3).

Contrairement à l'approche BMZ, on note que l'hypothèse $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ n'est plus nécessaire dans le cas **Cas 1**. Le Tableau 6.1 récapitule le schéma de la preuve.

Hypothèses	$\boldsymbol{\alpha} \in V^{\mathrm{o}}$	$\boldsymbol{\alpha} \in V^{\mathrm{a}}$
$\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$	Proposition 6.2.2	Proposition 6.2.2 ou Proposition 5.4.3
$\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$	Proposition 5.4.2	Proposition 5.4.3

Tableau 6.1 – Schéma de démonstration de l'approche R

On note :

$$D = \max\left(\deg_\infty(F), \deg_\infty(G)\right) \quad \text{et} \quad h = \max\left(\log\|F\|_1, \log\|G\|_1\right)$$

Sous l'hypothèse $\mathrm{pgcd}(F,G) = 1$, le Tableau 6.2 donne asymptotiquement l'ordre de grandeur des différentes bornes associées aux différents cas.

Hypothèses	$\boldsymbol{\alpha} \in V^{\mathrm{o}}$	$\boldsymbol{\alpha} \in V^{\mathrm{a}}$
$\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$	Dh	Dh ou D^4h
$\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$	D^4	D^4h

Tableau 6.2 – Ordre de grandeur des bornes suivant l'approche R

Dans la Section 6.2, on donne une nouvelle borne explicite du nouveau Cas 1. Dans la Section 6.3, on donne une nouvelle borne explicite de la Conjecture de Schinzel dans le cas $n = 3$ (Théorème 6.3.1). La dernière Section 6.4 contient un algorithme sur le calcul des translatés de sous-tores maximaux contenus dans V.

6.2 Borne explicite du nouveau Cas - 1

Dans cette section, on va construire le sous-tore T_2 de $\mathbb{G}_{\mathrm{m}}^n$ annoncé précédemment pour n quelconque.

Lemme 6.2.1. *Soient $n \geqslant 2$ un entier et $\mathbf{a} \in \mathbb{Z}^n$ un vecteur non nul. Alors il existe deux vecteurs linéairement indépendants $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}^n$ tels que $\langle \mathbf{u}_1, \mathbf{u}_2 \rangle$ est saturé, $\mathbf{a} \in \langle \mathbf{u}_1, \mathbf{u}_2 \rangle$ et*

$$\gamma_2^{-1}\|\mathbf{u}_1\|_2\|\mathbf{u}_2\|_2 \leqslant \det(\mathbf{u}_1, \mathbf{u}_2) \leqslant \gamma_{n-1}^{1/2}\|\mathbf{a}\|_2^{(n-2)/(n-1)}.$$

Le sous-ensemble T_2 de $\mathbb{G}_{\mathrm{m}}^n$ défini par :

$$T_2 = \left\{\gamma_1^{\mathbf{u}_1}\gamma_2^{\mathbf{u}_2} \in \mathbb{G}_{\mathrm{m}}^n, (\gamma_1, \gamma_2) \in \mathbb{G}_{\mathrm{m}}^2\right\},$$

est un sous-tore et contient tous les points de la forme $\xi^{\mathbf{a}}$ où $\xi \in \mathbb{G}_{\mathrm{m}}$.

Démonstration. Les deux vecteurs $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}^n$ sont donnés par le Lemme 1.4.2 et T_2 est un tore d'après la Proposition 1.3.2.2. □

Remarque. Par définition de T_2, on peut observer que le degré de T_2 est inférieur au degré de T_1 à la puissance $(n-2)/(n-1)$ à une constante près. Le fait que cette puissance du degré dans T_1 est strictement inférieure à 1 est crucial pour démontrer le résultat suivant.

La proposition suivante donne une majoration de la norme de $\mathbf{a}$ dans le cas où $\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$. On rappelle que γ_d est la constante d'Hermite de dimension d.

Proposition 6.2.2. *Soit $n \geqslant 2$ un entier. Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$. Soient $\mathbf{a} \in \mathbb{Z}^n$ un vecteur primitif, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ et $\xi \in \mathbb{G}_{\mathrm{m}} \setminus \boldsymbol{\mu}_\infty$. On note $\mathbb{K} = \mathbb{Q}(\boldsymbol{\zeta})$, $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$ et T_2 le sous-tore de $\mathbb{G}_{\mathrm{m}}^n$ défini dans le Lemme 6.2.1. Si $\boldsymbol{\alpha}$ est un point isolé de $V(F,G) \cap \boldsymbol{\zeta} T_2$ alors on a :*

$$\|\mathbf{a}\|_2^{1/(n-1)} \leqslant 2\sqrt{n}\gamma_2\gamma_{n-1}^{1/2}\left(\deg_\infty(G)\log\|F\|_1 + \deg_\infty(F)\log\|G\|_1\right)\lambda(d),$$

où

$$d = [\mathbb{K}(\boldsymbol{\alpha}) : \mathbb{K}] \quad \textit{et} \quad \lambda(d) = \frac{2^c \log(2d)^4}{\log\log(5d)^3}$$

où c est une constante absolue strictement positive. On a aussi :

$$[\mathbb{K}(\boldsymbol{\alpha}) : \mathbb{K}] \leqslant 2n\gamma_2\gamma_{n-1}^{1/2} \deg_\infty(F) \deg_\infty(G) \|\mathbf{a}\|_2^{(n-2)/(n-1)}.$$

Si, de plus $\boldsymbol{\zeta} \in \boldsymbol{\mu}_{\mathbb{Q}}^n$ alors on peut remplacer $\lambda(d)$ par $\ell(d)$.

En particulier, pour $n = 3$, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_2 \leqslant 2^{c+4} 3^{1/2} 13 Dh \frac{\log(2^{c+7} D^3 h)^4}{\log\log(2^{c+7} 5 D^3 h)^3}.$$

Si de plus, $\boldsymbol{\zeta} \in \{\pm 1\}^3$ alors on a la majoration (sans la constante c) :

$$\|\mathbf{b}\|_2 \leqslant \sqrt{12288} Dh \left(\frac{\log(256 D^3 h)}{\log\log(256 D^3 h)} \right)^3.$$

Démonstration. Soient $\mathbf{u}_1, \mathbf{u}_2$ les deux vecteurs définis dans le Lemme 6.2.1. Comme $\mathbf{a} \in \langle \mathbf{u}_1, \mathbf{u}_2 \rangle$, il existe $\boldsymbol{\eta} = (\eta_1, \eta_2) \in \mathbb{Z}^2$ tel que $\mathbf{a} = \eta_1 \mathbf{u}_1 + \eta_2 \mathbf{u}_2$. Comme $\mathbf{a}$ est primitif, alors il en est de même pour $\boldsymbol{\eta}$. Puisque $\langle \mathbf{u}_1, \mathbf{u}_2 \rangle$ est saturé, il existe $n-2$ vecteurs $\mathbf{u}_3, \cdots, \mathbf{u}_n \in \mathbb{Z}^n$ tels que $\{\mathbf{u}_1, \cdots, \mathbf{u}_n\}$ est une base de $\mathbb{Z}^n$. Soit U la matrice dont les lignes sont $\mathbf{u}_i$. On considère l'automorphisme φ_U qui est défini par :

$$\begin{aligned} \varphi_U : \mathbb{G}_{\mathrm{m}}^n &\longrightarrow \mathbb{G}_{\mathrm{m}}^n \\ \mathbf{x} &\mapsto \mathbf{x}^U \end{aligned}$$

On remarque que si $(y_1, y_2) \in \mathbb{G}_{\mathrm{m}}^2$ alors on a :

$$\varphi_U(y_1, y_2, 1, \cdots, 1) = y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2}.$$

On en déduit que :

$$\varphi_U^{-1}(T_2) = \left\{ (y_1, y_2, 1, \cdots, 1) \in \mathbb{G}_{\mathrm{m}}^n, (y_1, y_2) \in \mathbb{G}_{\mathrm{m}}^2 \right\}.$$

Notons $\boldsymbol{\vartheta} = \varphi^{-1}(\boldsymbol{\zeta}) \in \boldsymbol{\mu}_\infty^n$. Puisque

$$\varphi_U(\xi^{\eta_1}, \xi^{\eta_2}, 1, \cdots, 1) = \xi^{\eta_1 \mathbf{u}_1} \xi^{\eta_2 \mathbf{u}_2} = \xi^{\mathbf{a}},$$

on a :

$$\varphi_U^{-1}(\boldsymbol{\zeta} \xi^{\mathbf{a}}) = \boldsymbol{\vartheta} \varphi_U^{-1}(\xi^{\mathbf{a}}) = (\vartheta_1 \xi^{\eta_1}, \vartheta_2 \xi^{\eta_2}, \vartheta_3, \cdots, \vartheta_n).$$

Posons maintenant $P(y_1, y_2) = F(\boldsymbol{\zeta} y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})$ et $Q(y_1, y_2) = G(\boldsymbol{\zeta} y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2})$. On a :

$$\varphi_U^{-1}(V \cap \boldsymbol{\zeta} T_2) = \{ (\vartheta_1 y_1, \vartheta_2 y_2, \vartheta_3, \cdots, \vartheta_n) \in \mathbb{G}_{\mathrm{m}}^n, (y_1, y_2) \in V(P, Q) \}.$$

En effet, soit $\mathbf{z} \in \mathbb{G}_{\mathrm{m}}^n$. On a $\mathbf{z} = (\vartheta_1 y_1, \vartheta_2 y_2, \vartheta_3, \cdots, \vartheta_n)$ avec $P(y_1, y_2) = Q(y_1, y_2) = 0$ si et seulement si $\varphi(\mathbf{z}) = \boldsymbol{\zeta} y_1^{\mathbf{u}_1} y_2^{\mathbf{u}_2} \in \boldsymbol{\zeta} T_2$ avec $F(\varphi(\mathbf{z})) = G(\varphi(\mathbf{z})) = 0$.

Notons $\boldsymbol{\beta} = (\xi^{\eta_1}, \xi^{\eta_2})$. Puisque $\boldsymbol{\zeta}\boldsymbol{\xi}^{\mathbf{a}}$ est un point isolé de $V \cap \boldsymbol{\zeta}T_2$, $\varphi_U^{-1}(\boldsymbol{\zeta}\boldsymbol{\xi}^{\mathbf{a}})$ est un point isolé de $\varphi_U^{-1}(V \cap \boldsymbol{\zeta}T_2)$. Donc $\boldsymbol{\beta}$ est un point isolé de $V(F(\boldsymbol{\zeta}y_1^{\mathbf{u}_1}y_2^{\mathbf{u}_2}), G(\boldsymbol{\zeta}y_1^{\mathbf{u}_1}y_2^{\mathbf{u}_2}))$. D'après la Proposition 3.1.7, et en utilisant la majoration de la norme L_2 par la norme L_1 d'un vecteur, on en déduit que :

$$[\mathbb{K}(\boldsymbol{\beta}) : \mathbb{Q}(\beta_1)] \log M(\beta_i) \leqslant \sqrt{n}\|\mathbf{u}_2\|_2 \left(\deg_\infty(G) \log \|F\|_1 + \deg_\infty(F) \log \|G\|_1\right) [\mathbb{K} : \mathbb{Q}],$$

$$[\mathbb{K}(\boldsymbol{\beta}) : \mathbb{Q}(\beta_2)] \log M(\beta_i) \leqslant \sqrt{n}\|\mathbf{u}_1\|_2 \left(\deg_\infty(G) \log \|F\|_1 + \deg_\infty(F) \log \|G\|_1\right) [\mathbb{K} : \mathbb{Q}]$$

et

$$[\mathbb{K}(\boldsymbol{\beta}) : \mathbb{K}] \leqslant 2n \deg_\infty(F) \deg_\infty(G) \|\mathbf{u}_1\|_2 \|\mathbf{u}_2\|_2.$$

Par construction des vecteurs $\mathbf{u}_1$ et $\mathbf{u}_2$, on a :

$$\gamma_2^{-1}\|\mathbf{u}_1\|_2\|\mathbf{u}_2\|_2 \leqslant \det(\mathbf{u}_1, \mathbf{u}_2) \leqslant \gamma_{n-1}^{1/2}\|\mathbf{a}\|_2^{(n-2)/(n-1)}. \tag{6.2.1}$$

On en déduit que :

$$[\mathbb{K}(\boldsymbol{\beta}) : \mathbb{K}] \leqslant 2n\gamma_2\gamma_{n-1}^{1/2} \deg_\infty(F) \deg_\infty(G) \|\mathbf{a}\|_2^{(n-2)/(n-1)}.$$

De plus, comme $\boldsymbol{\eta}$ est primitif, on a $[\mathbb{K}(\xi) : \mathbb{K}] = [\mathbb{K}(\boldsymbol{\beta}) : \mathbb{K}]$. D'autre part, puisque $0 \neq \xi \notin \boldsymbol{\mu}_\infty$, on a $h(\xi) \neq 0$. Par suite, on a :

$$\begin{aligned}
|\eta_1| = \frac{h(\beta_1)}{h(\xi)} &= \frac{\log M(\beta_1)}{[\mathbb{Q}(\beta_1) : \mathbb{Q}]} \times \frac{1}{h(\xi)} \\
&\leqslant \frac{\sqrt{n}\|\mathbf{u}_2\|_2[\mathbb{K} : \mathbb{Q}]}{[\mathbb{K}(\boldsymbol{\beta}) : \mathbb{Q}(\beta_1)][\mathbb{Q}(\beta_1) : \mathbb{Q}]} \times \frac{(\deg_\infty(G) \log \|F\|_1 + \deg_\infty(F) \log \|G\|_1)}{h(\xi)} \\
&= \frac{\sqrt{n}\|\mathbf{u}_2\|_2}{[\mathbb{K}(\boldsymbol{\beta}) : \mathbb{K}]} \times \frac{(\deg_\infty(G) \log \|F\|_1 + \deg_\infty(F) \log \|G\|_1)}{h(\xi)}.
\end{aligned}$$

On obtient :

$$|\eta_1| \leqslant \sqrt{n}\|\mathbf{u}_2\|_2 \left(\deg_\infty(G) \log \|F\|_1 + \deg_\infty(F) \log \|G\|_1\right) \frac{1}{[\mathbb{K}(\boldsymbol{\beta}) : \mathbb{K}]h(\xi)}. \tag{6.2.2}$$

En appliquant le Théorème 1.2.3.2 (avec $\mathbb{K} = \mathbb{Q}$ et $\mathbb{L} = \mathbb{Q}(\boldsymbol{\zeta})$), on en déduit :

$$\frac{1}{h(\xi)} \leqslant \frac{2^c d \log(2d)^4}{\log\log(5d)^3} = d\lambda(d). \tag{6.2.3}$$

où c est une constante absolue strictement positive. Comme $d = [\mathbb{K}(\boldsymbol{\beta}) : \mathbb{K}] = [\mathbb{K}(\xi) : \mathbb{K}]$, l'inégalité (6.2.2) devient :

$$|\eta_1| \leqslant \sqrt{n}\|\mathbf{u}_2\|_2 \left(\deg_\infty(G) \log \|F\|_1 + \deg_\infty(F) \log \|G\|_1\right) \lambda(d).$$

Similairement, on a :

$$|\eta_2| \leqslant \sqrt{n}\|\mathbf{u}_1\|_2 \left(\deg_{x_1}(G) \log \|F\|_1 + \deg_{x_1}(F) \log \|G\|_1\right) \lambda(d).$$

Comme $\mathbf{a} = \eta_1\mathbf{u}_1 + \eta_2\mathbf{u}_2$, on a :

$$\|\mathbf{a}\|_2 \leqslant 2\sqrt{n} \left(\deg_\infty(G) \log \|F\|_1 + \deg_\infty(F) \log \|G\|_1\right) \|\mathbf{u}_1\|_2\|\mathbf{u}_2\|_2\lambda(d).$$

D'après (6.2.1), on a :

$$\|\mathbf{a}\|_2 \leqslant 2\sqrt{n}\gamma_2\gamma_{n-1}^{1/2}\left(\deg_\infty(G)\log\|F\|_1 + \deg_\infty(F)\log\|G\|_1\right)\|\mathbf{a}\|_2^{(n-2)/(n-1)}\lambda(d).$$

En simplifiant par $\|\mathbf{a}\|_2$, on a :

$$\|\mathbf{a}\|_2^{1/(n-1)} \leqslant 2\sqrt{n}\gamma_2\gamma_{n-1}^{1/2}\left(\deg_\infty(G)\log\|F\|_1 + \deg_\infty(F)\log\|G\|_1\right)\lambda(d). \tag{6.2.4}$$

Si $\boldsymbol{\zeta} \in \boldsymbol{\mu}_{\mathbb{Q}}^n$ alors $\mathbb{K} = \mathbb{Q}$. Ainsi au lieu d'utiliser l'inégalité (6.2.3), on utilise l'inégalité suivante :

$$\frac{1}{h(\xi)} = \frac{d}{\log M(\xi)} \leqslant d\ell(d).$$

Comme $[\mathbb{Q}(\boldsymbol{\beta}) : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}]$, l'inégalité (6.2.2) devient :

$$|\eta_1| \leqslant \sqrt{n}\|\mathbf{u}_2\|_2\left(\deg_\infty(G)\log\|F\|_1 + \deg_\infty(F)\log\|G\|_1\right)\ell(d).$$

Ainsi, il suffit de remplacer $\lambda(d)$ par $\ell(d)$ dans (6.2.4).

On suppose maintenant que $n = 3$ et $\boldsymbol{\zeta} = \mathbf{1}$.

Déterminons explicitement une borne pour la norme de $\mathbf{a}$. On a $\gamma_2 = 2/\sqrt{3}$. En majorant $\deg_\infty(F), \deg_\infty(G)$ par D et $\log\|F\|_1, \log\|G\|_1$ par h, on obtient :

$$\|\mathbf{a}\|_2^{1/2} \leqslant 2^{7/2}3^{-1/4}Dh\ell(d) \quad \text{et} \quad d \leqslant 2^{5/2}3^{1/4}D^2\|\mathbf{a}\|_2^{1/2}.$$

En utilisant le fait que ℓ est croissante et en multipliant la première inégalité par $2^{5/2}3^{1/4}D^2$, celle-ci peut s'écrire sous la forme :

$$X \leqslant C\ell(X)$$

où

$$X = 2^{5/2}3^{1/4}D^2\|\mathbf{a}\|_2^{1/2} \quad \text{et} \quad C = 2^6D^3h.$$

Soit τ la fonction définie par $\tau(x) = 4(\log(x)/\log\log(x))^3$ pour tout $x \geqslant 3$. D'après le Théorème 1.2.2.3, on en déduit que $\ell(X) \leqslant \tau(X)$ car $X \geqslant 3$. Comme $C \geqslant 2$ et $C\tau(X) \geqslant X \geqslant 3$, d'après le Lemme A.2.2, on a :

$$X \leqslant 3C\tau(4C).$$

En remplaçant X et C par leur expression respective, on en déduit que :

$$\|\mathbf{a}\|_2^{1/2} \leqslant 2^{7/2}3^{3/4}Dh\tau(2^8D^3h).$$

D'après le Théorème 1.4.1, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_2 \leqslant (2/\sqrt{3})^{1/2}\|\mathbf{a}\|_2^{1/2}.$$

Par suite, on a :

$$\|\mathbf{b}\|_2 \leqslant 2^4 3^{1/2}Dh\tau(2^8D^3h) = \sqrt{12288}Dh\left(\frac{\log(256D^3h)}{\log\log(256D^3h)}\right)^3.$$

On suppose enfin que $n = 3$ et $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^3$.

Déterminons explicitement une borne pour la norme de $\mathbf{a}$. En refaisant le même calcul dans le cas précédent, on a :

$$\|\mathbf{a}\|_2^{1/2} \leqslant 2^{7/2}3^{-1/4}Dh\lambda(d) \quad \text{et} \quad d \leqslant 2^{5/2}3^{1/4}D^2\|\mathbf{a}\|_2^{1/2}.$$

D'après le Lemme A.2.3, λ est croissante. En utilisant ce fait et en multipliant la première inégalité par $2^{5/2}3^{1/4}D^2$, celle-ci peut s'écrire sous la forme :

$$X \leqslant 2^c C\frac{\log(2X)^4}{\log\log(5X)^3}$$

où

$$X = 2^{5/2}3^{1/4}D^2\|\mathbf{a}\|_2^{1/2} \quad \text{et} \quad C = 2^6D^3h.$$

Puisque $C \geqslant 44$, d'après le Lemme A.2.4, on a :

$$X \leqslant 2^c 13C\frac{\log(2^{c+1}C)^4}{\log\log(2^c 5C)^3}.$$

En remplaçant X et C par leur expression respective, on en déduit que :

$$\|\mathbf{a}\|_2^{1/2} \leqslant 2^{c+7/2}3^{-1/4}13Dh\frac{\log(2^{c+7}D^3h)^4}{\log\log(2^{c+7}5D^3h)^3}.$$

D'après le Théorème 1.4.1, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_2 \leqslant (2/\sqrt{3})^{1/2}\|\mathbf{a}\|_2^{1/2}.$$

Par suite, on a :

$$\|\mathbf{b}\|_2 \leqslant 2^{c+4}3^{1/2}13Dh\frac{\log(2^{c+7}D^3h)^4}{\log\log(2^{c+7}5D^3h)^3}.$$

□

Remarque. En appliquant cette proposition avec $n = 3$ et $\boldsymbol{\zeta} = \mathbf{1}$, on peut obtenir la même majoration pour le degré de ξ que dans la Proposition 4.3.1, bien que les conditions imposées sur les vecteurs $\mathbf{u}_1$ et $\mathbf{u}_2$ puissent différer légèrement.

6.3 Version explicite la Conjecture de Schinzel

Une version explicite du Théorème 2 pour $n = 3$ se déduit directement du théorème suivant. Pour $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$, on note :

$$D = \max\left(\deg_\infty(F), \deg_\infty(G)\right) \quad \text{et} \quad h = \max(\log\|F\|_1, \log\|G\|_1).$$

Théorème 6.3.1. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$. Soient $\mathbf{a} \in \mathbb{Z}^3$ un vecteur non nul, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^3$ et $\xi \in \mathbb{G}_{\mathrm{m}} \setminus \boldsymbol{\mu}_\infty$ tels que $\boldsymbol{\zeta}\xi^{\mathbf{a}} \in V(F,G)$. Si $\boldsymbol{\zeta}\xi^{\mathbf{a}}$ appartient à une composante irréductible de $V(F,G)$ de codimension 2 alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :*

$$\|\mathbf{b}\|_2 \leqslant 2^c 208\sqrt{3} D^4 (3D\log 2 + h) \frac{\log(2^c 128 D^5 (3D\log 2 + h))^4}{\log\log(254D^3)^3},$$

où c est une constante absolue strictement positive.

Si, de plus, $\boldsymbol{\zeta} = \mathbf{1}$ alors on a :

$$\|\mathbf{b}\|_\infty \leqslant 225 D^4 (3D\log 2 + h) \left(\frac{\log(256 D^5 (3D\log 2 + h))}{\log\log(256 D^3 \log 2)} \right)^3.$$

Si, de plus, $\mathrm{pgcd}(F,G) = 1$ et $\boldsymbol{\zeta} = \mathbf{1}$ alors on a :

$$\|\mathbf{b}\|_\infty \leqslant 225 D^4 h \left(\frac{\log(256 D^6 h)}{\log\log(256 D^3 \log 2)} \right)^3.$$

Démonstration. Quitte à remplacer ξ par $\xi^{\mathrm{pgcd}(a_1,a_2,a_3)}$, on peut supposer que $\mathbf{a}$ est primitif. Dans toute la suite, on note $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$ et T_2 le sous-tore de $\mathbb{G}_{\mathrm{m}}^3$ défini dans le Lemme 6.2.1.

I. Supposons $\mathrm{pgcd}(F,G) = 1$ et $\boldsymbol{\zeta} = \mathbf{1}$

Dans ce cas, toutes les composantes irréductibles de $V = V(F,G)$ sont de codimension 2. Si $\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$ alors, d'après la Proposition 6.2.2, on a :

$$\|\mathbf{b}\|_2 \leqslant \sqrt{12288} D h \left(\frac{\log(256 D^3 h)}{\log\log(256 D^3 h)} \right)^3. \tag{6.3.1}$$

Si $\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ alors, d'après la Proposition 5.4.2, on a :

$$\|\mathbf{b}\|_\infty \leqslant 1458 D^4. \tag{6.3.2}$$

Si $\boldsymbol{\alpha} \in V^{\mathrm{a}}$ alors, d'après la Proposition 5.4.3, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_\infty \leqslant (225/4) D^4 h \ell(254 D^6) \leqslant 225 D^4 h \left(\frac{\log(254 D^6)}{\log\log(254 D^6)} \right)^3. \tag{6.3.3}$$

En prenant le maximum entre les bornes (6.3.1), (6.3.2) et (6.3.3) et en minorant h par $\log 2$, on a :

$$\|\mathbf{b}\|_\infty \leqslant 225 D^4 h \left(\frac{\log(256 D^6 h)}{\log\log(256 D^3 \log 2)} \right)^3.$$

Cela donne la borne voulue dans le cas où $\mathrm{pgcd}(F,G) = 1$ et $\boldsymbol{\zeta} = \mathbf{1}$.

On revient maintenant dans les hypothèses initiales. On pose $H = \mathrm{pgcd}(F,G)$, $P = F/H$ et $Q = G/H$. On note aussi :

$$D_H = \max\left(\deg_\infty(P), \deg_\infty(Q)\right) \quad \text{et} \quad h_H = \max(\log\|P\|_1, \log\|Q\|_1).$$

On va déterminer tout d'abord une majoration de D_H et h_H en fonction de D et h. Par définition de P et Q, on a $\deg_\infty(P) \leqslant \deg_\infty(F)$ et $\deg_\infty(Q) \leqslant \deg_\infty(G)$. D'après la relation (1.2.1) entre la mesure de Mahler et la norme L_1 d'un polynôme, on a :

$$\|P\|_1 \leqslant 2^{\deg_1(P)} M(P) \leqslant 2^{3\deg_\infty(F)} M(F).$$

On a une inégalité similaire pour $\|Q\|_1$. Ainsi, on obtient :

$$D_H \leqslant D \quad \text{et} \quad h_H \leqslant 3D\log 2 + h. \tag{6.3.4}$$

Par hypothèse, $\boldsymbol{\alpha}$ appartient à une composante irréductible de codimension au moins 2 de $V(F,G)$. On a donc $\boldsymbol{\alpha} \in V(P,Q)$. Dans toute la suite, on note $V = V(P,Q)$.

II. Supposons $\mathrm{pgcd}(F,G) \neq 1$ et $\boldsymbol{\zeta} = \mathbf{1}$:

Si $\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$ alors, d'après la Proposition 6.2.2, on en déduit :

$$\|\mathbf{b}\|_2 \leqslant \sqrt{12288} D_H h_H \left(\frac{\log(256 D_H^3 h_H)}{\log\log(256 D_H^3 h_H)}\right)^3. \tag{6.3.5}$$

Si $\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ alors, d'après la Proposition 5.4.2, on a :

$$\|\mathbf{b}\|_\infty \leqslant 1458 D_H^4. \tag{6.3.6}$$

Si $\boldsymbol{\alpha} \in V^{\mathrm{a}}$ alors, d'après la Proposition 5.4.3, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_\infty \leqslant (225/4) D_H^4 h_H \ell(254 D_H^6). \tag{6.3.7}$$

La fonction ℓ est croissante par définition et la fonction $x \mapsto (\log(x)/\log\log(x))^3$ est croissante pour $x \geqslant e^e$. En utilisant les majorations de (6.3.4), en minorant h_H par $\log 2$ et en prenant le maximum entre les bornes (6.3.5), (6.3.6) et (6.3.7), on a :

$$\|\mathbf{b}\|_\infty \leqslant 225 D^4 (3D\log 2 + h) \left(\frac{\log(256 D^5 (3D\log 2 + h))}{\log\log(256 D^3 \log 2)}\right)^3.$$

Cela donne la borne voulue dans le cas où $\mathrm{pgcd}(F,G) \neq 1$ et $\boldsymbol{\zeta} = \mathbf{1}$.

III. Supposons $\mathrm{pgcd}(F,G) \neq 1$ et $\boldsymbol{\zeta} \neq 1$:

On considère enfin le cas sans condition supplémentaire sur $\mathrm{pgcd}(F,G)$ ni sur $\boldsymbol{\zeta}$. Si $\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$ alors, d'après la Proposition 6.2.2, on a :

$$\|\mathbf{b}\|_2 \leqslant 2^{c+4} 3^{1/2} 13 D_H h_H \frac{\log(2^c 128 D_H^3 h_H)^4}{\log\log(2^c 640 D_H^3 h_H)^3}. \tag{6.3.8}$$

Si $\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ alors, d'après la Proposition 5.4.2, on a :

$$\|\mathbf{b}\|_\infty \leqslant 1458 D_H^4. \tag{6.3.9}$$

Si $\boldsymbol{\alpha} \in V^{\mathrm{a}}$ alors, d'après la Proposition 5.4.3, il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^3$ orthogonal à $\mathbf{a}$ tel que :

$$\|\mathbf{b}\|_\infty \leqslant (225/4) D_H^4 h_H \ell(254 D_H^6). \tag{6.3.10}$$

En utilisant les majorations de (6.3.4) et en prenant le maximum entre les les bornes (6.3.8), (6.3.9) et (6.3.10), on en déduit que :

$$\|\mathbf{b}\|_2 \leqslant 2^c 208\sqrt{3} D^4 (3D\log 2 + h) \frac{\log(2^c 128 D^5 (3D\log 2 + h))^4}{\log\log(254 D^3)^3}.$$

□

6.4 Algorithmes pour les translatés de sous-tores maximaux

On remarque que, dans la preuve du Théorème 2 dans le cas où $n = 3$, on se ramène à considérer deux cas suivant si $\boldsymbol{\alpha}$ appartient à un translaté de sous-tore contenu dans V ou non. Ainsi, ces translatés de sous-tore jouent un rôle important. On va donner ici un algorithme qui calcule les sous-tores H_Λ de $\mathbb{G}_{\mathrm{m}}^n$ dont un translaté est contenu dans V et y est maximal. L'ensemble des tels Λ est fini et est calculé par l'Algorithme 11. On va donner ensuite, dans le cas particulier $n = 3$, une procédure permettant de résoudre la Conjecture de Schinzel dans le cas où le point $\boldsymbol{\alpha}$ considéré appartient à un translaté de sous-tore contenu dans V (Algorithme 12).

On fixe $n \geqslant 2$ un entier. Soit $s \geqslant 1$ un entier. Soient $F_1, \cdots, F_s \in \mathbb{Z}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$. On note $V = V(F_1, \cdots, F_s)$. Pour $i \in \{1, \cdots, s\}$, on écrit :

$$F_i(\mathbf{x}) = \sum_{\boldsymbol{\lambda} \in \mathrm{Supp}(F_i)} f_{\boldsymbol{\lambda},i} \mathbf{x}^{\boldsymbol{\lambda}}.$$

Soit Λ un sous-groupe de $\mathbb{Z}^n$. On fixe un système $\mathcal{R}$ de représentants pour $\mathbb{Z}^n/\Lambda$. Pour $\chi \in \mathcal{R}$ et $i \in \{1, \cdots, s\}$, on définit :

$$S_{\chi,i} = \{\boldsymbol{\lambda} \in \mathrm{Supp}(F_i) \mid \boldsymbol{\lambda} - \chi \in \Lambda\}.$$

En d'autres termes, les ensembles $S_{\chi,i}$ forment une partition de $\mathrm{Supp}(F_i)$ suivant les classes modulo Λ. Soit $F_{\chi,i} \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$ le polynôme défini par par :

$$F_{\chi,i}(\mathbf{x}) = \sum_{\boldsymbol{\lambda} \in S_{\chi,i}} f_{\boldsymbol{\lambda},i} \mathbf{x}^{\boldsymbol{\lambda}}.$$

On note M le sous-groupe de $\mathbb{Z}^n$ engendré par $\bigcup_{\chi,i}(S_{\chi,i} - S_{\chi,i})$ où la différence est prise au sens de la somme de Minkwoski :

$$M = \langle \bigcup_{\chi,i} (S_{\chi,i} - S_{\chi,i}) \rangle. \tag{6.4.1}$$

Par construction, $S_{\chi,i} - S_{\chi,i} \subseteq \Lambda$ et donc $M \subseteq \Lambda$. D'après la définition (1.3.1), $H_\Lambda \subseteq H_M$. La proposition suivante, basée sur [42, Lemma 4], donne une relation entre les translatés de sous-tores $\boldsymbol{\beta} H_\Lambda$ contenus dans V et les polynômes $F_{\chi,i}$.

Proposition 6.4.1. *Soient $F_1, \cdots, F_s \in \mathbb{C}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$. On note $V = V(F_1, \cdots, F_s)$. Soit Λ un sous-groupe de $\mathbb{Z}^n$ et soit $\mathcal{R}$ un système de représentants pour $\mathbb{Z}^n/\Lambda$. Soit $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$. Avec les notations ci-dessus, on a les assertions suivantes.*

(**1**) *$\boldsymbol{\beta} H_\Lambda \subseteq V$ si et seulement si $F_{\chi,i}(\boldsymbol{\beta}) = 0$ pour tout $i \in \{1, \cdots, s\}$ et pour tout $\chi \in \mathcal{R}$.*
(**2**) *Si $\boldsymbol{\beta} H_\Lambda \subseteq V$ alors on a $\boldsymbol{\beta} H_\Lambda \subseteq \boldsymbol{\beta} H_M \subseteq V$.*
(**3**) *Si $\boldsymbol{\beta} H_\Lambda \subseteq V$ est un translaté de sous-groupe algébrique maximal dans V alors on a $\Lambda = M$.*
(**4**) *Si $\boldsymbol{\beta} H_\Lambda \subseteq V$ est un translaté de sous-tore maximal dans V alors on a $\Lambda = M^{\mathrm{sat}}$.*

Démonstration. Si $\chi \in \mathcal{R}$ alors on note φ_χ le caractère de H_Λ défini par $\varphi_\chi(\boldsymbol{\alpha}) = \boldsymbol{\alpha}^\chi$.

(**1**) Supposons que $\boldsymbol{\beta} H_\Lambda \subseteq V$. Soit $i \in \{1, \cdots, s\}$. Soit $\boldsymbol{\alpha} \in H_\Lambda$. On a :

$$0 = F_i(\boldsymbol{\beta}\boldsymbol{\alpha}) = \sum_{\chi \in \mathcal{R}} \sum_{\boldsymbol{\lambda} \in S_{\chi,i}} f_{\boldsymbol{\lambda},i} \boldsymbol{\beta}^{\boldsymbol{\lambda}} \boldsymbol{\alpha}^{\boldsymbol{\lambda}} = \sum_{\chi \in \mathcal{R}} \left(\sum_{\boldsymbol{\lambda} \in S_{\chi,i}} f_{\boldsymbol{\lambda},i} \boldsymbol{\beta}^{\boldsymbol{\lambda}} \right) \boldsymbol{\alpha}^\chi = \sum_{\chi \in \mathcal{R}} F_{\chi,i}(\boldsymbol{\beta}) \boldsymbol{\alpha}^\chi.$$

On en déduit que :

$$\sum_{\chi\in\mathcal{R}} F_{\chi,i}(\boldsymbol{\beta})\varphi_\chi = 0.$$

Comme $\mathcal{R}$ forme un système de représentants, les $(\varphi_\chi)_{\chi\in\mathcal{R}}$ sont deux à deux distincts. D'après le Théorème d'Artin [46, Theorem 4.3], les φ_χ sont linéairement indépendants. Donc $F_{\chi,i}(\boldsymbol{\beta}) = 0$ pour tout χ.

Réciproquement, supposons que $F_{\chi,i}(\boldsymbol{\beta}) = 0$ pour tout $i \in \{1,\cdots,s\}$ et pour tout $\chi \in \mathcal{R}$. Soient $\boldsymbol{\alpha} \in H_\Lambda$ et $i \in \{1,\cdots,s\}$. On a :

$$F_i(\boldsymbol{\beta}\boldsymbol{\alpha}) = \sum_{\chi\in\mathcal{R}}\sum_{\boldsymbol{\lambda}\in S_{\chi,i}} f_{\boldsymbol{\lambda},i}\boldsymbol{\beta}^{\boldsymbol{\lambda}}\boldsymbol{\alpha}^{\boldsymbol{\lambda}} = \sum_{\chi\in\mathcal{R}}\Big(\sum_{\boldsymbol{\lambda}\in S_{\chi,i}} f_{\boldsymbol{\lambda},i}\boldsymbol{\beta}^{\boldsymbol{\lambda}}\Big)\boldsymbol{\alpha}^{\chi} = \sum_{\chi\in\mathcal{R}} F_{\chi,i}(\boldsymbol{\beta})\boldsymbol{\alpha}^{\chi} = 0.$$

Cela montre que $\boldsymbol{\beta}H_\Lambda \subseteq V$.

$(\mathbf{2})$ Supposons que $\boldsymbol{\beta}H_\Lambda \subseteq V$. Montrons que $\boldsymbol{\beta}H_M \subseteq V$. Soit $\boldsymbol{\alpha} \in H_M$. On a :

$$F_i(\boldsymbol{\beta}\boldsymbol{\alpha}) = \sum_{\chi\in\mathcal{R}}\sum_{\boldsymbol{\lambda}\in S_{\chi,i}} f_{\boldsymbol{\lambda},i}\boldsymbol{\beta}^{\boldsymbol{\lambda}}\boldsymbol{\alpha}^{\boldsymbol{\lambda}}.$$

Comme $\boldsymbol{\alpha} \in H_M$, l'application

$$\begin{aligned}\mathbb{Z}^n &\longrightarrow \overline{\mathbb{Q}}^\times\\ \boldsymbol{\lambda} &\mapsto \boldsymbol{\alpha}^{\boldsymbol{\lambda}}\end{aligned}$$

est constante sur $S_{\chi,i}$ et on note $\boldsymbol{\alpha}^{\chi,i}$ sa valeur. Par suite, on a :

$$F_i(\boldsymbol{\beta}\boldsymbol{\alpha}) = \sum_{\chi\in\mathcal{R}}\left(\sum_{\boldsymbol{\lambda}\in S_{\chi,i}} a_{i,\boldsymbol{\lambda}}\boldsymbol{\beta}^{\boldsymbol{\lambda}}\right)\boldsymbol{\alpha}^{\chi,i} = \sum_{\chi\in\mathcal{R}} F_{\chi,i}(\boldsymbol{\beta})\boldsymbol{\alpha}^{\chi,i}.$$

D'après $(\mathbf{1})$, $F_{\chi,i}(\boldsymbol{\beta}) = 0$ pour tout χ et donc $F_i(\boldsymbol{\beta}\boldsymbol{\alpha}) = 0$. Cela montre que $\boldsymbol{\beta}H_M \subseteq V$. Par construction, on a $H_\Lambda \subseteq H_M$ et donc $\boldsymbol{\beta}H_\Lambda \subseteq \boldsymbol{\beta}H_M \subseteq V$.

$(\mathbf{3})$ Si $\boldsymbol{\beta}H_\Lambda \subseteq V$ est maximal alors, d'après $(\mathbf{2})$ et par maximalité, on a $H_\Lambda = H_M$ et donc $\Lambda = M$.

$(\mathbf{4})$ Supposons que $\boldsymbol{\beta}H_\Lambda$ est un translaté de sous-tore. Donc Λ est saturé. Comme $M \subseteq \Lambda$, on a $M \subseteq M^{\mathrm{sat}} \subseteq \Lambda^{\mathrm{sat}} = \Lambda$ et donc $\boldsymbol{\beta}H_\Lambda \subseteq \boldsymbol{\beta}H_{M^{\mathrm{sat}}} \subseteq \boldsymbol{\beta}H_M \subseteq V$, où la dernière inclusion suit de $(\mathbf{2})$. Par maximalité, on en déduit que $\Lambda = M^{\mathrm{sat}}$. □

Proposition 6.4.2. *Soient $F_1,\cdots,F_s \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$. On note $V = V(F_1,\cdots,F_s)$. La liste $\mathcal{M}$ renvoyée par l'Algorithme 11 vérifie la propriété suivante. Soit Λ un sous-groupe saturé de $\mathbb{Z}^n$. On a $\Lambda \in \mathcal{M}$ si et seulement si $\boldsymbol{\beta}H_\Lambda \subset V$ est maximal pour un certain $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$.*

Démonstration. Supposons $\boldsymbol{\beta}H_\Lambda \subset V$ est maximal pour un certain $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$. D'après $(\mathbf{4})$, $\Lambda = M^{\mathrm{sat}}$ où M est définie comme dans (6.4.1). En particulier, les générateurs de Λ appartiennent à $\mathcal{D}$ définie à l'étape 3. Enfin, le système S possède $\boldsymbol{\beta}$ comme solution et donc Λ a été mis dans $\mathcal{M}$ à un moment donné. Par maximalité, il n'a pas été retiré. Ainsi Λ est renvoyé par l'Algorithme 11.

Réciproquement, supposons que Λ est renvoyé par l'Algorithme 11. Par construction, Λ est saturé et le système (S) possède une solution $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$ sinon Λ aurait été retiré à l'étape 11. Pour tout $i \in \{1,\cdots,s\}$ et $j \in \{1,\cdots,p_i\}$, on a donc :

$$(S) : \sum_{\boldsymbol{\lambda}\in S_{i,j}} f_{\boldsymbol{\lambda},i}\boldsymbol{\beta}^{\boldsymbol{\lambda}} = 0.$$

D'après l'assertion $(\mathbf{1})$ de la Proposition 6.4.1, on a $\boldsymbol{\beta} H_\Lambda \subseteq V$. De plus, cette dernière inclusion est maximale sinon Λ aurait été retiré à l'étape 7. □

Algorithme 11 : Translatés de sous-tores contenus dans V maximaux

Entrée : $F_1, \cdots, F_s \in \mathbb{Z}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$.

Sortie : Une liste finie $\mathcal{M}$ de sous-groupes de $\mathbb{Z}^n$.

1 Écrire les F_i sous la forme :

$$F_i(\mathbf{x}) = \sum_{\boldsymbol{\lambda} \in \mathrm{Supp}(F_i)} f_{\boldsymbol{\lambda},i} \mathbf{x}^{\boldsymbol{\lambda}}.$$

2 Initialiser $\mathcal{M} = \{\}$.
3 Calculer $\mathcal{D} = \bigcup_i \mathcal{D}(\mathrm{Supp}(F_i))$.
4 Pour $(\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_n) \in \mathcal{D}^n$, faire :
5 définir $\Lambda = \langle \boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_n \rangle$;
6 calculer le rang et le saturé de Λ en appliquant l'Algorithme 15 à Λ ;
7 s'il existe $\Lambda' \in \mathcal{M}$ tel que $\Lambda' \subseteq \Lambda^{\mathrm{sat}}$ alors revenir à l'étape 4 ;
8 définir la relation d'équivalence $\sim$ telle que $\boldsymbol{\eta} \sim \boldsymbol{\mu}$ si $\boldsymbol{\eta} - \boldsymbol{\mu} \in \Lambda^{\mathrm{sat}}$;
9 pour tout $i \in \{1, \cdots, s\}$, calculer la partition de $\mathrm{Supp}(F_i)$ en classes d'équivalence :

$$\mathrm{Supp}(F_i) = S_{i,1} \cup \cdots \cup S_{i,p_i};$$

10 résoudre le système (S) dans $\mathbb{G}_{\mathrm{m}}^n$ et noter $\mathcal{Z}$ l'ensemble de ses solutions :

$$(S) : \sum_{\boldsymbol{\lambda} \in S_{i,j}} f_{\boldsymbol{\lambda},i} \mathbf{x}^{\boldsymbol{\lambda}} = 0, \text{ pour } i \in \{1, \cdots, s\} \text{ et } j \in \{1, \cdots, p_i\};$$

11 si $\#\mathcal{Z} = 0$ alors revenir à l'étape 4 ;
12 enlever tous les $\Lambda' \in \mathcal{M}$ vérifiant $\Lambda' \supseteq \Lambda^{\mathrm{sat}}$;
13 mettre Λ^{sat} dans $\mathcal{M}$.
14 Renvoyer $\mathcal{M}$.

Proposition 6.4.3. *Soit $s \geqslant 1$ un entier et soient $F_1, \cdots, F_s \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$. On note $V = V(F_1, \cdots, F_s)$. La liste $\mathcal{M}$ renvoyée par l'Algorithme 11 vérifie la propriété suivante. Soit Λ un sous-groupe saturé de $\mathbb{Z}^n$. On a $\Lambda \in \mathcal{M}$ si et seulement si $\boldsymbol{\beta} H_\Lambda \subset V$ est maximal pour un certain $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$.*

Démonstration. Supposons $\boldsymbol{\beta} H_\Lambda \subset V$ est maximal pour un certain $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$. D'après $(\mathbf{4})$, $\Lambda = M^{\mathrm{sat}}$ où M est définie comme dans (6.4.1). En particulier, les générateurs de Λ appartiennent à $\mathcal{D}$ définie à l'étape 3. Enfin, le système S possède $\boldsymbol{\beta}$ comme solution et donc Λ a été mis dans $\mathcal{M}$ à un moment donné. Par maximalité, il n'a pas été retiré. Ainsi Λ est renvoyé par l'Algorithme 11.

Réciproquement, supposons que Λ est renvoyé par l'Algorithme 11. Par construction, Λ est saturé et le système (S) possède une solution $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^n$ sinon Λ aurait été retiré à l'étape 11. Pour tout $i \in \{1, \cdots, s\}$ et $j \in \{1, \cdots, p_i\}$, on a donc :

$$(S) : \sum_{\boldsymbol{\lambda} \in S_{i,j}} f_{\boldsymbol{\lambda},i} \boldsymbol{\beta}^{\boldsymbol{\lambda}} = 0.$$

D'après l'assertion $(\mathbf{1})$ de la Proposition 6.4.1, on a $\boldsymbol{\beta} H_\Lambda \subseteq V$. De plus, cette dernière inclusion est maximale sinon Λ aurait été retiré à l'étape 7. □

Remarques. $(\mathbf{1})$ Dans [42, Lemma 4], l'auteur a considéré l'ensemble $\mathcal{D}(\bigcup_i \mathrm{Supp}(F_i))$ qui est largement plus grand par rapport à $\bigcup_i \mathcal{D}(\mathrm{Supp}(F_i))$. Pour réduire la taille de $\mathcal{D}$ défini à l'étape 3, on peut aussi se demander s'il est possible de remplacer $\mathrm{Supp}(F_i)$ par la différence de ses points extrémaux.

$(\mathbf{2})$ Pour calculer les solutions du système (S) défini à l'étape 10, on peut utiliser l'algorithme de B. Buchberger sur les bases de Gröbner [17].

$(\mathbf{3})$ L'Algorithme 11 n'est pas très efficace en pratique car, pour chaque n-uplet de $\mathcal{D}^n$, il faut calculer une racine du système S, ce qui peut être coûteux. De plus, l'ensemble $\mathcal{D}^n$ est de taille exponentielle par rapport à n. Une des améliorations possibles consiste à trier $\mathcal{D}$. On peut aussi faire un test sur le cardinal de $S_{i,j}$: si $\#S_{i,j} = 1$ alors on retire Λ. En effet, si c'était le cas alors $\boldsymbol{\beta}$ ne serait pas un point de $\mathbb{G}_{\mathrm{m}}^n$.

$(\mathbf{4})$ Une implémentation de l'Algorithme 11 a été faite dans le cas particulier où $n = 3$ et $s = 2$ et $\mathrm{pgcd}(F_1, F_2) = 1$. Sous ces conditions, tout sous-groupe dans $\mathcal{M}$ est de rang 2.

Algorithme 12 : Conjecture de Schinzel dans le cas où $V = V(F, G)$ et $\boldsymbol{\alpha} \in V^{\mathrm{a}}$

Entrée : $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\mathrm{pgcd}(F, G) = 1$.

Sortie : une liste de vecteurs de $\mathbb{Z}^3$.

1 Appliquer l'Algorithme 11 et noter $\mathcal{M}$ la liste renvoyée.
2 Pour tout $\Lambda \in \mathcal{M}$:
3 noter $\{\boldsymbol{\mu}_1, \boldsymbol{\mu}_2\}$ une base de Λ ;
4 trouver $\boldsymbol{\mu}_3 \in \mathbb{Z}^3$ tel que $\{\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \boldsymbol{\mu}_3\}$ soit une base de $\mathbb{Z}^3$ en appliquant l'Algorithme 15 à Λ et noter $M \in \mathrm{GL}_3(\mathbb{Z})$ la matrice dont les colonnes sont les $\boldsymbol{\mu}_i$;
5 définir les $(F_i)_i$ et $(G_j)_j$ tels que :

$$F(\mathbf{y}^{M^{-1}}) = \sum_{i \in I} F_i(y_1, y_2)\, y_3^i \quad \text{et} \quad G(\mathbf{y}^{M^{-1}}) = \sum_{j \in J} G_j(y_1, y_2)\, y_3^j.$$

6 résoudre le système (S) suivant dans $\mathbb{G}_{\mathrm{m}}^2$ et noter W l'ensemble de ses solutions :

$$(S) : \Big\{ F_i(y_1, y_2) = G_j(y_1, y_2) = 0, \forall i \in I, j \in J$$

7 pour tout $\boldsymbol{\gamma} \in W$:
8 calculer une base de l'ensemble $R_f(\boldsymbol{\gamma})$ en appliquant l'Algorithme 6 ;
9 si $\dim(R_f(\boldsymbol{\gamma})) = 1$ alors :
10 noter $\boldsymbol{\eta} \in \mathbb{Z}^2$ un générateur de $R_f(\boldsymbol{\gamma})$ et poser $\mathbf{b} = \eta_1 \boldsymbol{\mu}_1 + \eta_2 \boldsymbol{\mu}_2$;
11 mettre $\mathbf{b}$ dans $\mathcal{B}$.
12 Renvoyer $\mathcal{B}$.

Proposition 6.4.4. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ tels que $\mathrm{pgcd}(F, G) = 1$. On note $V = V(F, G)$. L'Algorithme 12 termine et renvoie une liste $\mathcal{B}$ de vecteurs non nuls dans $\mathbb{Z}^3$ vérifiant la propriété suivante. Soient $\mathbf{a} \in \mathbb{Z}^n$, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^3$ et $\boldsymbol{\xi} \in \mathbb{G}_{\mathrm{m}} \setminus \boldsymbol{\mu}_\infty$. Si $\boldsymbol{\zeta}\boldsymbol{\xi}^{\mathbf{a}} \in V^a$ alors il existe $\mathbf{b} \in \mathcal{B}$ tel que $\mathbf{ab} = 0$.*

Démonstration. On reprend essentiellement la preuve de la Proposition 5.4.3. On note $\boldsymbol{\alpha} = \boldsymbol{\zeta}\boldsymbol{\xi}^{\mathbf{a}}$. Comme

$\boldsymbol{\alpha} \in V^{\mathrm{a}}$, $\boldsymbol{\alpha}$ appartient à un translaté de sous-tore $\boldsymbol{\alpha}T \subseteq V$ de dimension non nulle. Comme $\mathrm{pgcd}(F, G) = 1$, V est de dimension 1 et donc il en est de même pour T. Ainsi $\boldsymbol{\alpha}T \subset V$ est maximal. D'aprés la Proposition 6.4.2, il existe $\Lambda \in \mathcal{M}$ telle que $T = H_\Lambda$. Soient $\boldsymbol{\mu}_1$ et $\boldsymbol{\mu}_2$ définis comme à l'étape 3, M comme à l'étape 4 et W comme à l'étape 6. On note φ_M l'automorphisme de $\mathbb{G}_{\mathrm{m}}^3$ défini par $\varphi_M(\mathbf{x}) = \mathbf{x}^M$. On a alors :

$$\begin{aligned}(y_1, y_2) \in W &\iff F_i(y_1, y_2) = G_j(y_1, y_2) = 0,\ \forall i \in I, j \in J,\\ &\iff F(\mathbf{y}^{M^{-1}}) = G(\mathbf{y}^{M^{-1}}) = 0,\ \forall y_3 \in \mathbb{G}_{\mathrm{m}},\\ &\iff \mathbf{y}^{M^{-1}} \in V,\ \forall y_3 \in \mathbb{G}_{\mathrm{m}},\\ &\iff \mathbf{y} \in \varphi_M(V),\ \forall y_3 \in \mathbb{G}_{\mathrm{m}}.\end{aligned}$$

Ainsi, on obtient :

$$W = \{(y_1, y_2) \in \mathbb{G}_{\mathrm{m}}^2 \mid \forall y_3 \in \mathbb{G}_{\mathrm{m}},\ (y_1, y_2, y_3) \in \varphi_M(V)\}. \tag{6.4.2}$$

Par conséquent, on a $W \times \mathbb{G}_{\mathrm{m}} \subseteq \varphi_M(V)$ et donc :

$$\dim(W) + 1 = \dim(W \times \mathbb{G}_{\mathrm{m}}) \leqslant \dim(\varphi_M(V)) = \dim(V) = 1.$$

On en déduit que W est de dimension nulle dans $\mathbb{G}_{\mathrm{m}}^2$ et donc W est un ensemble fini. Ensuite, on note $\boldsymbol{\beta}$ l'image de $\boldsymbol{\alpha}$ par φ_M i.e.

$$\boldsymbol{\beta} = (\boldsymbol{\zeta}^{\boldsymbol{\mu}_1}\boldsymbol{\xi}^{\mathbf{a}\boldsymbol{\mu}_1}, \boldsymbol{\zeta}^{\boldsymbol{\mu}_2}\boldsymbol{\xi}^{\mathbf{a}\boldsymbol{\mu}_2}, \boldsymbol{\zeta}^{\boldsymbol{\mu}_3}\boldsymbol{\xi}^{\mathbf{a}\boldsymbol{\mu}_3}).$$

On pose $\boldsymbol{\beta}' = (\beta_1, \beta_2)$. On a :

$$\begin{aligned}\boldsymbol{\beta}' \times \mathbb{G}_{\mathrm{m}} &= \{(\beta_1, \beta_2, \beta_3 y_3) \in \mathbb{G}_{\mathrm{m}}^3,\ y_3 \in \mathbb{G}_{\mathrm{m}}\}\\ &= \boldsymbol{\beta}\varphi(T) \quad \text{car} \quad \varphi(T) = \{\mathbf{y} \in \mathbb{G}_{\mathrm{m}}^n \mid y_1 = y_2 = 1\}\\ &= \varphi_M(\boldsymbol{\alpha}T)\\ &\subseteq \varphi(V).\end{aligned}$$

D'après (6.4.2), on en déduit que $\boldsymbol{\beta}' \in W$. En particulier, $\boldsymbol{\beta}'$ est l'un des $\boldsymbol{\gamma}$ défini à l'étape 7. De plus, par construction de $\boldsymbol{\beta}'$ et tenant compte du fait $\xi \notin \boldsymbol{\mu}_\infty$, on a $\dim R_f(\boldsymbol{\beta}') = 1$. Enfin, soient $\boldsymbol{\eta}$ et $\mathbf{b}$ définis comme à l'étape 10. Puisque On a $\boldsymbol{\beta}'^{\boldsymbol{\eta}} = \boldsymbol{\zeta}^{\eta_1\boldsymbol{\mu}_1 + \eta_2\boldsymbol{\mu}_2}\boldsymbol{\xi}^{\eta_1\mathbf{a}\boldsymbol{\mu}_1 + \eta_2\mathbf{a}\boldsymbol{\mu}_2} \in \boldsymbol{\mu}_\infty$. Comme $\xi \notin \boldsymbol{\mu}_\infty$, on en déduit que $\eta_1\mathbf{a}\boldsymbol{\mu}_1 + \eta_2\mathbf{a}\boldsymbol{\mu}_2 = 0$ i.e. $\mathbf{ab} = 0$. □

Remarque. L'Algorithme 12 peut être généralisé pour le cas n quelconque à condition que la sous-variété W définie à l'étape 6 est de dimension nulle.

7. Cas $n = 3$: Comparaisons et Algorithmes

Dans la Section 7.1 du présent chapitre, on va comparer asymptotiquement les bornes des différentes approches par rapport à leur ordre de grandeur. Ensuite, dans la Section 7.2, comme application de la borne explicite, on va rendre effectif l'algorithme correspondant au Théorème 1 pour le calcul de la partie non-cyclotomique du pgcd de deux polynômes $f, g \in \mathbb{Z}[x]$ qui sont des spécialisations de deux polynômes F et G à (seulement) trois variables (Algorithme 14). En plus de l'algorithme, on fera également l'analyse de sa complexité (Théorème 7.2.2). Dans la Section 7.3, on donne un exemple sur cet algorithme.

7.1 Comparaisons des bornes

Dans cette section, on va comparer les différentes bornes que l'on a obtenues suivant les quatre approches : S (Chapitre 4), BMZ (Chapitre 5) et R (Chapitre 6).

7.1.1 Comparaisons au niveau de l'ordre de grandeur

On note :

$$\begin{aligned} D &= \max\left(\deg_\infty(F), \deg_\infty(G)\right) \\ h &= \max(\log \|F\|_1, \log \|G\|_1) \\ N &= \max(\#\mathrm{Supp}(F), \#\mathrm{Supp}(G)). \end{aligned}$$

Le Tableau 7.1 ci-après donne asymptotiquement l'ordre de grandeur des différentes bornes associées aux différentes approches.

Hypothèses	S	BMZ	R
$\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$	ND^4	$N^3D^5h^2$	Dh
$\boldsymbol{\alpha}$ est un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{a}}$	D^5h	D^4h	Dh
$\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$	D^6	D^4	D^4
$\boldsymbol{\alpha}$ n'est pas un point isolé de $V \cap \boldsymbol{\zeta} T_2$ et $\boldsymbol{\alpha} \in V^{\mathrm{a}}$	D^5h	D^4h	D^4h
Maximum	D^6h	$N^3D^5h^2$	D^4h

Tableau 7.1 – Ordre de grandeur des bornes suivant les différentes approches

On observe que l'approche R donne asymptotiquement le meilleur ordre de grandeur D^4h. Au niveau de chaque cas individuel, l'approche R est plus fine et notamment dans le cas où $\boldsymbol{\alpha}$ est un point isolé. Cela est dû fait qu'on a utilisé une majoration de type Bézout Arithmétique qui est plus fine dans notre situation. Comparées à l'approche R, les deux approches S et BMZ sont moins précises.

7.1.2 Comparaisons numériques

Afin de mieux comparer les différentes bornes dans le cas pratique, on va considérer des polynômes générés aléatoirement.

Exemple 7.1.2.1. On commence par générer aléatoirement deux polynômes lacunaires F et G à 3 variables de degrés partiels majorés par 8 et de nombre de coefficients non nuls majoré par 5 et de taille majoré par 20.

$$F(x_1, x_2, x_3) = -8x_3^2x_1^4 + 11x_2^3x_1^2 + -8x_2^3 + 14x_2$$
$$G(x_1, x_2, x_3) = 16x_2^5x_1^6 + 4x_3^7x_2^4x_1^5 - 3x_3^5x_2^4x_1^3 + 5x_3^7.$$

On vérifie que $\mathrm{pgcd}(F, G) = 1$. On a alors les bornes suivantes :

Approches	S	BMZ	R
Bornes	3×10^{12}	2×10^{15}	10^9

On va augmenter la taille des coefficients de deux polynômes F et G dans les deux exemples suivants.

Exemple 7.1.2.2. On ajoute 200 à la taille des coefficients.

$$F(x_1, x_2, x_3) = -208x_3^2x_1^4 + 11x_2^3x_1^2 + -8x_2^3 + 14x_2 + 200$$
$$G(x_1, x_2, x_3) = 16x_2^5x_1^6 + 204x_3^7x_2^4x_1^5 - 203x_3^5x_2^4x_1^3 + 5x_3^7.$$

On vérifie que $\mathrm{pgcd}(F, G) = 1$. On a les bornes suivantes :

Approches	S	BMZ	R
Bornes	9×10^{12}	7×10^{15}	2×10^9

En comparant avec l'Exemple 7.1.2.2, on remarque que les trois bornes ne changent pas drastiquement si la taille des coefficients augmente. Cela est dû au fait que les bornes dépendent des coefficients de P et Q en leur logarithme.

Maintenant, on va augmenter la taille des degrés partiels de deux polynômes F et G.

Exemple 7.1.2.3. On ajoute 50 au degré partiel.

$$F(x_1, x_2, x_3) = -8x_3^2x_1^{54} + 11x_2^3x_1^2 - 8x_2^3 + 14x_2^{50}$$
$$G(x_1, x_2, x_3) = 16x_2^{55}x_1^6 + 4x_3^7x_2^4x_1^5 - 3x_3^{55}x_2^4x_1^3 + 5x_3^{57}.$$

On vérifie que $\mathrm{pgcd}(F, G) = 1$. On a alors les bornes suivantes :

Approches	S	BMZ	R
Bornes	2×10^{18}	10^{20}	2×10^{13}

Par rapport à l'Exemple 7.1.2.1, on remarque déjà une différence non négligeable au niveau des bornes. On observe également que la borne de l'approche de S est le plus sensible par rapport au degré.

On va ajouter des monômes aux deux polynômes F et G dans l'exemple suivant.

Exemple 7.1.2.4. On augmente à 10 le nombre de monômes non nuls.

$$\begin{aligned} F(x_1,x_2,x_3) &= 4x_2^6x_1^5x_3^7 + 5x_2^2x_3^7 - 3x_2^6x_1^3x_3^5 + x_3^3 - 8x_1^5x_3^2 - 8x_2x_1^4x_3^2 + 16x_2^7x_1^6 + \\ &\quad 11x_2^3x_1^3 + 11x_2^4x_1^2 - 8x_2^3x_1 + 14x_2x_1 - 8x_2^4 + 14x_2^2 \\ G(x_1,x_2,x_3) &= 4x_2^4x_1^5x_3^{10} + 5x_3^{10} - 3x_2^4x_1^3x_3^8 + 16x_2^5x_1^6x_3^3 - 8x_2^2x_1^4x_3^2 + 11x_2^5x_1^2 + x_1 + \\ &\quad - 8x_2^5 + 14x_2^3 + x_2. \end{aligned}$$

On vérifie que $\mathrm{pgcd}(F,G) = 1$. On a alors les bornes suivantes :

Approches	S	BMZ	R
Bornes	6×10^{14}	6×10^{17}	7×10^{9}

Par rapport à l'exemple 7.1.2.1, on remarque une différence non négligeable au niveau des bornes.

Enfin, dans l'exemple suivant, on augmente les trois paramètres.

Exemple 7.1.2.5. On ajoute 100 à la taille des coefficients, 25 au degré partiel et 10 au nombre de monômes.

$$\begin{aligned} F(x_1,x_2,x_3) &= x_3^{25} + 40x_2^5x_1^5x_3^7 + 50x_2x_3^7 - 30x_2^5x_1^3x_3^5 - 8x_1^5x_3^2 - 8x_2x_1^4x_3^2 + 160x_2^6x_1^6 + 11x_2^3x_1^3 + \\ &\quad 11x_2^4x_1^2 - 8x_2^3x_1 + 14x_2x_1 - 8x_2^4 + 14x_2^2 \\ G(x_1,x_2,x_3) &= 40x_2^4x_1^5x_3^8 + 50x_3^8 - 30x_2^4x_1^3x_3^6 - 8x_2x_1^4x_3^2 + 160x_2^5x_1^6x_3 + 11x_2^4x_1^2 + x_1 + x_2^{25} + \\ &\quad - 8x_2^4 + 14x_2^2. \end{aligned}$$

On vérifie que $\mathrm{pgcd}(F,G) = 1$.On a alors les bornes suivantes :

Approches	S	BMZ	R
Bornes	3×10^{17}	2×10^{20}	5×10^{11}

D'après ces différents exemples, on peut en déduire que l'approche par le résultant est plus précise que les autres approches. L'approche S et BMZ donnent parfois des bornes similaires.

7.2 Recherche des facteurs communs non-cyclotomiques : algorithme et complexité

Pour rendre effectif l'algorithme dans [29], on a besoin d'une procédure préliminaire (Algorithme 13) qui est nécessaire à l'exécution de l'algorithme principal (Algorithme 14). Soit n un entier. On s'intéressera au deux cas : $n = 2$ ou $n = 3$.

Algorithme 13 : Changement de n variables à $n-1$ variables

Entrée : $F, G \in \mathbb{Z}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$ et $\mathbf{a} \in \mathbb{Z}^n$, tous non nuls.

Sortie : $\emptyset$ ou $P, Q \in \mathbb{Z}[y_1^{\pm 1}, \cdots, y_{n-1}^{\pm 1}]$ et $\mathbf{c} \in \mathbb{Z}^{n-1}$ tels que $F(t^{\mathbf{a}}) = P(t^{\mathbf{c}})$ et $G(t^{\mathbf{a}}) = Q(t^{\mathbf{c}})$.

1 Déterminer une base $\{\mathbf{v}_1, \cdots, \mathbf{v}_{n-1}\}$ de $\mathbf{a}^{\perp}$.
2 Calculer le plus petit vecteur non nul $\mathbf{b}$ par rapport à la norme L_2 dans $\mathbf{a}^{\perp}$ à partir de cette base.
3 Si $n = 2$ alors calculer la borne du Corollaire 3.2.2 en l'appliquant à F et G et la noter B ;
4 Si $n = 3$ alors calculer la borne du Théorème 6.3.1 en l'appliquant à F et G et la noter B ;
5 Si $\|\mathbf{b}\|_2 > \sqrt{n}B$ alors renvoyer $\emptyset$.
6 Déterminer une base réduite $\{\mathbf{u}_1, \cdots, \mathbf{u}_{n-1}\}$ de $\mathbf{b}^{\perp}$.
7 Déterminer les coordonnés $\mathbf{c}$ de $\mathbf{a}$ dans cette base.
8 Poser $P(\mathbf{y}) = F(\mathbf{y}^U)$ et $Q(\mathbf{y}) = G(\mathbf{y}^U)$ où U est la matrice dont les lignes sont $\mathbf{u}_1, \cdots, \mathbf{u}_{n-1}$.
9 Renvoyer P, Q et $\mathbf{c}$.

Proposition 7.2.1. *Soit n un entier tel que $2 \leqslant n \leqslant 3$. Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$ et $\mathbf{a} \in \mathbb{Z}^n$. On note :*

$$\begin{aligned} D &= \max\left(\deg_\infty(F), \deg_\infty(G)\right), \\ N &= \max\left(\#\mathrm{Supp}(F), \#\mathrm{Supp}(G)\right), \\ h &= \max(\log\|F\|_1, \log\|G\|_1). \end{aligned}$$

S'il existe $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$ tel que $\xi^{\mathbf{a}}$ appartient à une composante irréductible de $V(F, G)$ de codimension 2 alors l'Algorithme 13 renvoie deux polynômes $P, Q \in \mathbb{Z}[y_1^{\pm 1}, \cdots, y_{n-1}^{\pm 1}]$ et un vecteur non nul $\mathbf{c} \in \mathbb{Z}^{n-1}$ satisfaisant $F(t^{\mathbf{a}}) = P(t^{\mathbf{c}})$ et $G(t^{\mathbf{a}}) = Q(t^{\mathbf{c}})$. Il nécessite au plus :

$$\mathcal{O}(hN\log N) + nN\widetilde{\mathcal{O}}(\log D) + N\widetilde{\mathcal{O}}(\log\|\mathbf{a}\|)$$

opérations binaires. De plus, on a :

$$\begin{cases} \|\mathbf{c}\|_\infty \leqslant (n-1)\|\mathbf{a}\|_2, \\ \max(\log\|P\|_1, \log\|Q\|_1) \leqslant h, \\ \max\left(\#\mathrm{Supp}(P), \#\mathrm{Supp}(Q)\right) \leqslant N, \\ \max\left(\deg_\infty(P), \deg_\infty(Q)\right) \leqslant 2^n BD, \end{cases} \tag{7.2.1}$$

où B est la borne du Corollaire 3.2.2 si $n = 2$ ou du Théorème 6.3.1 si $n = 3$ appliqué à F et G.

Démonstration. Supposons qu'il existe $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$ tel que $\xi^{\mathbf{a}}$ appartient à une composante irréductible de $V(F, G)$ de codimension 2. Si $n = 2$ (resp. si $n = 3$) alors d'après le Corollaire 3.2.2 (resp. d'après le Théorème 6.3.1), il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^n$ orthogonal à $\mathbf{a}$ vérifiant :

$$\|\mathbf{b}\|_\infty \leqslant B$$

où

$$B = \begin{cases} 8hD \left(\dfrac{\log(2D^2)}{\log\log(2D^2)} \right)^3 & \text{si } n = 2 \\ 225D^4(3D\log 2 + h) \left(\dfrac{\log(256D^5(3D\log 2 + h))}{\log\log(256D^3\log 2)} \right)^3 & \text{si } n = 3. \end{cases}$$

Ainsi, on a également $\|\mathbf{b}\|_2 \leqslant \sqrt{n}B$. En particulier, le vecteur $\mathbf{b}$ défini à l'étape 2 satisfait ces conditions. On choisit donc ce vecteur $\mathbf{b}$ à l'étape 6. Remarquons que $\mathbf{b}$ est primitif. Comme $\mathbf{a}$ et $\mathbf{b}$ sont orthogonaux, le vecteur $\mathbf{a}$ est bien une combinaison linéaire des vecteurs $\mathbf{u}_1, \cdots, \mathbf{u}_{n-1}$. Ainsi, on a bien $\mathbf{a} = c_1\mathbf{u}_1 + \cdots + c_{n-1}\mathbf{u}_{n-1}$ à étape 7. Pour voir que les polynômes P et Q définis à l'étape 8 satisfont les propriétés requises, il suffit de faire la substitution $\mathbf{y} = t^{\mathbf{u}}$.

Évaluons maintenant le nombre d'opérations binaires effectuées par l'algorithme ainsi que la taille de la sortie.

L'étape 1 consiste à déterminer une base de $\mathbf{a}^\perp$. Si $n = 2$ alors il suffit de prendre comme base le vecteur $\mathbf{v}_1 = (-a_2, a_1)/\operatorname{pgcd}(a_1, a_2)$. Si $n = 3$ alors on construit une base de $\mathbf{a}^\perp$ comme suit. On calcule d_1 le pgcd de a_1 et a_2, d_2 celui de d_1 et a_3 et quatre entiers relatifs u_1, u_2, v_1, v_2 tels que $u_1a_1 + u_2a_2 = d_1$ et $v_1d_1 + v_2a_3 = d_2$. On considère la matrice :

$$V = \begin{pmatrix} -a_2/d_1 & u_1 & 0 \\ a_1/d_1 & u_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & -a_3/d_2 & v_1 \\ 0 & d_1/d_2 & v_2 \end{pmatrix} = \begin{pmatrix} -a_2/d_1 & -u_1a_3/d_2 & u_1v_1 \\ a_1/d_1 & -u_2a_3/d_2 & u_2v_1 \\ 0 & d_1/d_2 & v_2 \end{pmatrix}.$$

Par construction, V est de déterminant ± 1 et $\mathbf{a} \cdot V = (0, 0, d_2)$. En notant $\mathbf{v}_1$ et $\mathbf{v}_2$ les deux premières colonnes de V, on a $\mathbf{a} \cdot \mathbf{v}_1 = \mathbf{a} \cdot \mathbf{v}_2 = 0$ et donc $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{a}^\perp$. Comme $\det(V) = \pm 1$, donc $\{\mathbf{v}_1, \mathbf{v}_2\}$ est une base de $\mathbf{a}^\perp$. En utilisant l'algorithme d'Euclide étendu, on peut calculer d_1, u_1, u_2 en $\widetilde{\mathcal{O}}(\log \|\mathbf{a}\|)$ opérations binaires en faisant appel à l'algorithme de A. Schönhage [33]. Puisque $d_1 \leqslant \|\mathbf{a}\|_\infty$, le calcul de d_2, v_1, v_2 nécessite le même nombre d'opérations binaires. Ainsi, cette étape nécessite $\widetilde{\mathcal{O}}(\log \|\mathbf{a}\|)$ opérations binaires.

L'étape 2 consiste à calculer le plus petit vecteur non nul $\mathbf{b}$ par rapport à la norme L_2 dans $\mathbf{a}^\perp$. Si $n = 2$ alors $\mathbf{b} = \mathbf{v}_1$ où $\mathbf{v}_1$ est défini à l'étape 1. Il n'y a donc rien à faire. Si $n = 3$ alors il faut trouver $\lambda_1, \lambda_2 \in \mathbb{Z}$ tel que $\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2$ soit le plus petit vecteur par rapport à la norme L_2 où $\mathbf{v}_1, \mathbf{v}_2$ sont définis à l'étape 1. Comme $\mathbf{v}_1$ et $\mathbf{v}_2$ sont de taille plus petite que $\mathcal{O}(\log \|\mathbf{a}\|)$, en utilisant l'algorithme de A. Schönhage [43], on peut trouver $\mathbf{b}$ en $\widetilde{\mathcal{O}}(\log \|\mathbf{a}\|)$ opérations binaires. Ainsi, l'étape 2 nécessite $\widetilde{\mathcal{O}}(\log \|\mathbf{a}\|)$ opérations binaires.

La calcul de la norme L_1 de F nécessite de parcourir tous ses coefficients qui peut être au nombre de $\mathcal{O}(N)$ et chaque somme coûte $\mathcal{O}(h)$. Le calcul de h se fait donc en $\mathcal{O}(Nh)$ opérations binaires. Le calcul de D nécessite une comparaison de $N \times n$ entiers de taille $\mathcal{O}(\log D)$. Ainsi, les étapes 3 et 4 nécessitent $\mathcal{O}(hN) + \mathcal{O}(nN \log D)$ opérations binaires.

Comme $\|\mathbf{b}\|_2 \leqslant \|\mathbf{v}_1\|_2 \leqslant \|\mathbf{a}\|_2$, ainsi le calcul l'étape 5 se fait au plus en $\widetilde{\mathcal{O}}(\log \|\mathbf{a}\|)$ opérations binaires.

L'étape 6 consiste à déterminer une base de $\mathbf{b}^\perp$ que l'on construit comme à l'étape 1 ; d'où on a une complexité de $\widetilde{\mathcal{O}}(\log \|\mathbf{b}\|) = \widetilde{\mathcal{O}}(\log \|\mathbf{a}\|)$. Si $n = 2$ alors cette base est déjà réduite. Si $n = 3$ alors, pour trouver une base réduite, on fait appel à l'algorithme de A. Schönhage comme à l'étape 2 ; d'où on a une complexité $\widetilde{\mathcal{O}}(\log \|\mathbf{a}\|)$. Comme $\det(\mathbf{b}^\perp) = \|\mathbf{b}\|_2$, d'après [35, Theorem 5 et Theorem 7], on

en déduit que :

$$\|\mathbf{u}_1\|_2^2 \leqslant \|\mathbf{u}_1\|_2\|\mathbf{u}_2\|_2 \leqslant \frac{2}{\sqrt{3}}\|\mathbf{b}\|_2. \tag{7.2.2}$$

De plus, on a :

$$\|\mathbf{u}_1\|_2^2\|\mathbf{u}_2\|_2^2 - (\mathbf{u}_1 \cdot \mathbf{u}_2)^2 = \|\mathbf{b}\|_2^2. \tag{7.2.3}$$

L'étape 7 consiste à calculer $\mathbf{c}$. Si $n = 2$ alors $\mathbf{a} = c_1\mathbf{u}_1$ et donc c'est trivial. En particulier, on a $\|\mathbf{c}\| \leqslant \|\mathbf{a}\|$. Si $n = 3$ alors $\mathbf{a} = c_1\mathbf{u}_1 + c_2\mathbf{u}_2$ et donc :

$$\begin{pmatrix} \mathbf{a} \cdot \mathbf{u}_1 \\ \mathbf{a} \cdot \mathbf{u}_2 \end{pmatrix} = \begin{pmatrix} \mathbf{u}_1 \cdot \mathbf{u}_1 & \mathbf{u}_1 \cdot \mathbf{u}_2 \\ \mathbf{u}_1 \cdot \mathbf{u}_2 & \mathbf{u}_2 \cdot \mathbf{u}_2 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

D'après les formules de Cramer, on a :

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \frac{1}{\|\mathbf{b}\|_2^2} \begin{pmatrix} \mathbf{u}_2 \cdot \mathbf{u}_2 & -\mathbf{u}_1 \cdot \mathbf{u}_2 \\ -\mathbf{u}_1 \cdot \mathbf{u}_2 & \mathbf{u}_1 \cdot \mathbf{u}_1 \end{pmatrix} \begin{pmatrix} \mathbf{a} \cdot \mathbf{u}_1 \\ \mathbf{a} \cdot \mathbf{u}_2 \end{pmatrix}$$

En utilisant l'égalité (7.2.3) et les inégalités (7.2.2), on en déduit que :

$$|c_1| \leqslant 2\|\mathbf{a}\|_2 \quad \text{et} \quad |c_2| \leqslant (12)^{1/4}\frac{\|\mathbf{a}\|_2}{\|\mathbf{b}\|_2^{1/2}} \leqslant (12)^{1/4}\|\mathbf{a}\|_2.$$

D'après les majorations (7.2.2), $\mathbf{u}_1$ et $\mathbf{u}_2$ sont de taille plus petite que $\mathcal{O}(\log \|\mathbf{b}\|) = \mathcal{O}(\log \|\mathbf{a}\|)$. L'étape 7 nécessite donc $\widetilde{\mathcal{O}}(\log \|\mathbf{a}\|)$ opérations binaires.

L'étape 8 consiste à évaluer F et G en $\mathbf{y}^U$. Cela consiste à faire N fois la multiplication $U \cdot \boldsymbol{\lambda}$ où $\boldsymbol{\lambda} \in \mathrm{Supp}(F)$. Puis, il faut faire la somme de N monômes. Comme U est de taille $\mathcal{O}(\log \|\mathbf{a}\|)$, l'étape 8 nécessite $\mathcal{O}(hN \log N) + N\widetilde{\mathcal{O}}(\log D) + N\widetilde{\mathcal{O}}(\log \|\mathbf{a}\|)$ opérations binaires.

En combinant ces différentes opérations, l'algorithme nécessite au total :

$$\mathcal{O}(hN \log N) + nN\widetilde{\mathcal{O}}(\log D) + N\widetilde{\mathcal{O}}(\log \|\mathbf{a}\|)$$

opérations binaires.

Enfin, il reste à montrer les inégalités dans (7.2.1). D'après les calculs faits précédemment, on a $\|\mathbf{c}\|_\infty \leqslant (n-1)\|\mathbf{a}\|_2$. Par construction de P, on a $\#\mathrm{Supp}(P) \leqslant \#\mathrm{Supp}(F)$ et $\|P\|_1 \leqslant \|F\|_1$. Déterminons une majoration du degré de P. Si $n = 2$ alors $P(y_1) = F(y_1^{\mathbf{u}_1})$ et donc :

$$\deg_\infty(P) \leqslant 2\|\mathbf{u}_1\|_\infty \deg_\infty(F) \leqslant 2\|\mathbf{b}\|_\infty \deg_\infty(F) \leqslant 2BD.$$

Si $n = 3$ alors $P(\mathbf{y}) = F(\mathbf{y}^U)$ et donc pour $i \in \{1, 2\}$, on a :

$$\deg_{y_i}(P) \leqslant \sqrt{3}\|\mathbf{u}_i\|_2 \deg_\infty(F) \leqslant 2\sqrt{3}BD.$$

en utilisant les inégalités (7.2.2). On a des inégalités similaires pour Q en fonction de G. □

On est maintenant en mesure de décrire l'algorithme principal qui permet de calculer la partie non-cyclotomique du $\gcd$ de deux polynômes lacunaires de la forme $f(t) = F(t^{\mathbf{a}})$ et $g(t) = G(t^{\mathbf{a}})$ où F et G sont deux polynômes à trois variables.

Algorithme 14 : Partie non-cyclotomique du $\gcd$ de deux polynômes lacunaires

Entrée : $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ non nuls et $\mathbf{a} \in \mathbb{Z}^3$.

Sortie : $h \in \mathbb{Z}[t^{\pm 1}]$ tel que $h \mid \gcd(f, g)$ et $\gcd(f, g)/h$ est un produit de polynômes cyclotomiques où $f(t) = F(t^{\mathbf{a}})$ et $g(t) = G(t^{\mathbf{a}})$.

1 Appliquer l'Algorithme 13 à $F_3 = F, G_3 = G$ et $\mathbf{a}_3 = \mathbf{a}$.
2 Si le résultat de l'étape 1 est $\emptyset$, calculer $H_3 = \gcd(F_3, G_3)$ et renvoyer $h(t) = H_3(t^{\mathbf{a}_3})$.
3 Sinon, noter F_2, G_2 et $\mathbf{a}_2$ le résultat de l'étape 1.
4 Appliquer l'Algorithme 13 à F_2, G_2 et $\mathbf{a}_2$.
5 Si le résultat de l'étape 4 est $\emptyset$, calculer $H_2 = \gcd(F_2, G_2)$ et renvoyer $h(t) = H_2(t^{\mathbf{a}_2})$.
6 Sinon, noter F_1, G_1 et $\mathbf{a}_1$ le résultat de l'étape 4.
7 Calculer $H_1 = \gcd(F_1, G_1)$ et renvoyer $h(t) = H_1(t^{\mathbf{a}_1})$.

Théorème 7.2.2. *Soient $F, G \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$. On pose :*

$$\begin{aligned} D &= \max\left(\deg_\infty(F), \deg_\infty(G)\right) \\ h &= \max(\log \|F\|_1, \log \|G\|_1) \\ N &= \max(\#\mathrm{Supp}(F), \#\mathrm{Supp}(G)). \end{aligned}$$

Soit $\mathbf{a} \in \mathbb{Z}^3$. On définit $f, g \in \mathbb{Z}[x^{\pm 1}]$ par :

$$f(t) = F(t^{\mathbf{a}}) \quad \text{et} \quad g(t) = G(t^{\mathbf{a}}).$$

L'Algorithme 14 appliqué aux polynômes F et G ainsi qu'au vecteur $\mathbf{a}$ permet de calculer un polynôme $p_1 \in \mathbb{Z}[t^{\pm 1}]$ tel que $p_1 \mid \gcd(f, g)$ et $\gcd(f, g)/p_1$ est un produit de polynômes cyclotomiques. Il nécessite au plus :

$$\widetilde{\mathcal{O}}(D^{24}h^7) + ND^{12}h^3\widetilde{\mathcal{O}}(\log \|\mathbf{a}\|)$$

opérations binaires.

Remarque. Les deux termes D^{12} et D^{24} dans la complexité de cet algorithme sont dûs essentiellement au calcul de $\gcd$ de deux polynômes denses à 2 et à 3 trois variables. Par rapport au degré de f et g, la complexité de cet algorithme est linéaire en $\|\mathbf{a}\|$.

Démonstration. On commence par montrer que le polynôme h renvoyé par l'Algorithme 14 divise le $\gcd$ de f et g et que $\gcd(f, g)/h$ est un produit de polynômes cyclotomiques. Pour tout $i \in \{1, 2, 3\}$, on note :

$$V_i = \{\mathbf{x} \in \mathbb{G}_{\mathrm{m}}^i \mid F_i = G_i = 0\} \quad \text{et} \quad T_i = \{\xi^{\mathbf{a}_i} \in \mathbb{G}_{\mathrm{m}}^i, \xi \in \overline{\mathbb{Q}}^*\}.$$

Initialement, on a :

$$\begin{cases} f(t) = F_3(t^{\mathbf{a}_3}) \\ g(t) = G_3(t^{\mathbf{a}_3}). \end{cases}$$

Supposons que l'Algorithme 13 renvoie $\emptyset$ à l'étape 1. On calcule donc $H_3 = \mathrm{pgcd}(F_3, G_3)$. Comme H_3 est un diviseur de F_3 et G_3, donc $h(t) = H_3(t^{\mathbf{a}_3})$ est un diviseur du pgcd de $F_3(t^{\mathbf{a}_3})$ et $G_3(t^{\mathbf{a}_3})$. D'après la Proposition 7.2.1, tous les points de $V_3 \cap T_3$ qui sont de la forme $\xi^{\mathbf{a}_3}$ où $\xi \notin \boldsymbol{\mu}_\infty$ appartiennent à une composante irréductible de V_3 de codimension 1. Donc, ces points annulent H_3. Montrons que $\mathrm{pgcd}(f, g)/h$ ne peut s'annuler qu'en des racines de l'unité. Soit $\xi \notin \boldsymbol{\mu}_\infty$ tel que $h(\xi) \neq 0$ et $f(\xi)/h(\xi) = g(\xi)/h(\xi) = 0$. On a alors $F_3(\xi^{\mathbf{a}_3})/H_3(\xi^{\mathbf{a}_3}) = G_3(\xi^{\mathbf{a}_3})/H_3(\xi^{\mathbf{a}_3}) = 0$. Cela montre que $\xi^{\mathbf{a}_3}$ appartient à une composante irréductible de V_3 de codimension 2. Ainsi, on a une contradiction et donc $\mathrm{pgcd}(f, g)/h$ ne peut s'annuler qu'en des racines de l'unité.

On suppose maintenant que l'Algorithme 13 ne renvoie pas $\emptyset$ à l'étape 1. À l'étape 3, on a donc :

$$\begin{cases} f(t) = F_2(t^{\mathbf{a}_2}) \\ g(t) = G_2(t^{\mathbf{a}_2}). \end{cases}$$

Supposons que l'Algorithme 13 renvoie $\emptyset$ à l'étape 4. À l'étape 5, on calcule donc $H_2 = \mathrm{pgcd}(F_2, G_2)$. Comme H_2 est un diviseur de F_2 et G_2, donc $h(t) = H_2(t^{\mathbf{a}_2})$ est un diviseur du pgcd de $F_2(t^{\mathbf{a}_2})$ et $G_2(t^{\mathbf{a}_2})$. D'après la Proposition 7.2.1, tous les points de $V_2 \cap T_2$ qui sont de la forme $\xi^{\mathbf{a}_2}$ où $\xi \notin \boldsymbol{\mu}_\infty$ appartiennent à une composante irréductible de V_2 de codimension 1. Donc ces points annulent H_2. Comme précédemment, le polynôme $\mathrm{pgcd}(f, g)/h$ ne peut s'annuler qu'en des racines de l'unité.

On suppose maintenant que l'Algorithme 13 ne renvoie pas $\emptyset$ à l'étape 4. À l'étape 6, on a alors :

$$\begin{cases} f(t) = F_1(t^{\mathbf{a}_1}) \\ g(t) = G_1(t^{\mathbf{a}_1}). \end{cases}$$

Comme H_1 est un diviseur de F_1 et G_1, donc $h(t) = H_1(t^{\mathbf{a}_1})$ est un diviseur du pgcd de $F_1(t^{\mathbf{a}_1})$ et $G_1(t^{\mathbf{a}_1})$. Comme F_1 et G_1 sont des polynômes univariés, donc tous les de points de $V_1 \cap T_1$ qui sont de la forme $\xi^{\mathbf{a}_1}$ où $\xi \in \mathbb{G}_{\mathrm{m}}^1$ appartiennent à une composante irréductible de V_1 de codimension 1. Ainsi, ces points annulent $\mathrm{pgcd}(F_3, G_3) = H_3$. Par suite, $\mathrm{pgcd}(f, g)/h$ ne peut s'annuler qu'en des racines de l'unité. D'où l'algorithme est correct.

Il nous reste à évaluer le nombre d'opérations binaires de l'algorithme. L'exécution de l'étape 1 nécessite un appel à l'Algorithme 13 appliqué à F_3, G_3 et $\mathbf{a}_3$. D'après la Proposition 7.2.1, cela nécessite :

$$\mathcal{O}(h_3 N_3 \log N_3) + N_3 \widetilde{\mathcal{O}}(\log D_3) + N_3 \widetilde{\mathcal{O}}(\log \|\mathbf{a}_3\|),$$

opérations binaires où :

$$\begin{aligned} D_3 &= \max\left(\deg_\infty(F_3), \deg_\infty(G_3)\right), \\ N_3 &= \max\left(\#\mathrm{Supp}(F_3), \#\mathrm{Supp}(G_3)\right), \\ h_3 &= \max(\log \|F_3\|_1, \log \|G_3\|_1). \end{aligned}$$

A l'étape 2, on calcule H_3 qui est le pgcd de F_3 et G_3. Cela nécessite $\mathcal{O}(h_3^2 D_3^3 + h_3 D_3^4)$ opérations binaires d'après [14, Equation (95), p.502]. L'évaluation pour obtenir $H_3(t^{\mathbf{a}_3})$ nécessite $(D_3^3 \log D_3)\widetilde{\mathcal{O}}(\log(\|\mathbf{a}_3\|))$ opérations binaires. Donc l'étape 2 nécessite :

$$\mathcal{O}(h_3^2 D_3^3) + \mathcal{O}(h_3 D_3^4) + (D_3^3 \log D_3)\widetilde{\mathcal{O}}(\log \|\mathbf{a}_3\|)$$

opérations binaires.

Ensuite, l'exécution de l'étape 4 nécessite à nouveau un appel à l'Algorithme 13 appliqué à F_2, G_2 et $\mathbf{a}_2$. D'après la Proposition 7.2.1, cela requiert :

$$\mathcal{O}(h_2 N_2 \log N_2) + N_2 \widetilde{\mathcal{O}}(\log D_2) + N_2 \widetilde{\mathcal{O}}(\log \|\mathbf{a}_2\|)$$

opérations binaires où :

$$\begin{aligned} D_2 &= \max\left(\deg_\infty(F_2), \deg_\infty(G_2)\right), \\ N_2 &= \max\left(\#\mathrm{Supp}(F_2), \#\mathrm{Supp}(G_2)\right), \\ h_2 &= \max(\log \|F_2\|_1, \log \|G_2\|_1). \end{aligned}$$

De plus, d'après les inégalités (7.2.1), on a :

$$\begin{cases} \|\mathbf{a}_2\|_\infty \leqslant 2\|\mathbf{a}_3\|_2, \\ h_2 \leqslant h_3, \\ N_2 \leqslant N_3, \\ D_2 \leqslant 4B_3 D_3, \end{cases} \tag{7.2.4}$$

où B_3 est la borne du Théorème 6.3.1 appliqué à F_3 et G_3. Ainsi, l'étape 4 nécessite :

$$\mathcal{O}(h_3 N_3 \log N_3) + N_3 \widetilde{\mathcal{O}}(\log(B_3 D_3)) + N_3 \widetilde{\mathcal{O}}(\log \|\mathbf{a}_3\|)$$

opérations binaires .

A l'étape 5, on calcule H_2 qui est le $\gcd$ de F_2 et G_2. D'après [14, Equation (95), p.502], cela nécessite $\mathcal{O}(h_2^2 D_2^2 + h_2 D_2^3)$ opérations binaires. L'évaluation pour obtenir $H_2(t^{\mathbf{a}_2})$ nécessite $(D_2^2 \log D_2)\widetilde{\mathcal{O}}(\log(\|\mathbf{a}_2\|))$ opérations binaires (ici on peut remplacer D_2^2 par $\#\mathrm{Supp}(H_2)$). Donc l'étape 5 nécessite :

$$\mathcal{O}(h_2^2 D_2^2) + \mathcal{O}(h_2 D_2^3) + (D_2^2 \log D_2)\widetilde{\mathcal{O}}(\log \|\mathbf{a}_2\|)$$

opérations binaires. D'après les inégalités (7.2.4), on en déduit que l'étape 5 nécessite :

$$\mathcal{O}(h_3^2 B_3^2 D_3^2) + \mathcal{O}(h_3 B_3^3 D_3^3) + (B_3^2 D_3^2 \log(B_3 D_3))\widetilde{\mathcal{O}}(\log \|\mathbf{a}_3\|)$$

opérations binaires.

Enfin, à l'étape 7, on calcule H_1 qui est le $\gcd$ de F_1 et G_1. D'après [14, Equation (95), p.502], cela nécessite $\mathcal{O}(h_1^2 D_1 + h_1 D_1^2)$ opérations binaires où :

$$\begin{aligned} D_1 &= \max\left(\deg_\infty(F_1), \deg_\infty(G_1)\right), \\ N_1 &= \max\left(\#\mathrm{Supp}(F_1), \#\mathrm{Supp}(G_1)\right), \\ h_1 &= \max(\log \|F_1\|_1, \log \|G_1\|_1). \end{aligned}$$

L'évalue $H_1(t^{\mathbf{a}_1})$ nécessite $(D_1 \log D_1)\widetilde{\mathcal{O}}(\log(\|\mathbf{a}_1\|))$ opérations binaires. Ainsi, l'étape 7 nécessite :

$$\mathcal{O}(h_1^2 D_1) + \mathcal{O}(h_1 D_1^2) + (D_1 \log D_1)\widetilde{\mathcal{O}}(\log \|\mathbf{a}_1\|)$$

opérations binaires. D'après les inégalités (7.2.1), on a :

$$\begin{cases} \|\mathbf{a}_1\|_\infty \leqslant \|\mathbf{a}_2\|_2 \\ h_1 \leqslant h_2 \\ N_1 \leqslant N_2 \\ D_1 \leqslant 2B_2 D_2, \end{cases}$$

où B_2 est la borne du Théorème 3.2.1 appliqué à F_2 et G_2. L'étape 7 nécessite donc :

$$\mathcal{O}(h_2^2 B_2 D_2) + \mathcal{O}(h_2 B_2^2 D_2^2) + (B_2 D_2 \log(B_2 D_2))\widetilde{\mathcal{O}}(\log \|\mathbf{a}_2\|)$$

opérations binaires. D'après les inégalités (7.2.4), on a $h_2 \leqslant h_3$ et $D_2 \leqslant 4B_3 D_3$. Ainsi, l'étape 7 nécessite :

$$\mathcal{O}(h_3^2 B_2 B_3 D_3) + \mathcal{O}(h_3 B_2^2 B_3^2 D_3^2) + (B_2 B_3 D_3 \log(B_2 B_3 D_3))\widetilde{\mathcal{O}}(\log \|\mathbf{a}_3\|)$$

opérations binaires. Or B_2 est de taille $\mathcal{O}(h_2 D_2 \log(D_2)) = \mathcal{O}(h_3 B_3 D_3 \log(B_3 D_3))$ et B_3 de taille $\mathcal{O}(D_3^5 h_3 \log^3(h_3 D_3))$. Au total, l'exécution de l'algorithme nécessite au plus :

$$\begin{aligned}
&\mathcal{O}(h_3 N_3 \log N_3) + N_3\widetilde{\mathcal{O}}(\log D_3) + N_3\widetilde{\mathcal{O}}(\log \|\mathbf{a}_3\|) \quad \text{(Etape 1)}\\
+\ &\mathcal{O}(h_3^2 D_3^3) + \mathcal{O}(h_3 D_3^4) + (D_3^3 \log D_3)\widetilde{\mathcal{O}}(\log \|\mathbf{a}_3\|) \quad \text{(Etape 2)}\\
+\ &\mathcal{O}(h_3 N_3 \log N_3) + N_3\widetilde{\mathcal{O}}(\log(B_3 D_3)) + N_3\widetilde{\mathcal{O}}(\log \|\mathbf{a}_3\|) \quad \text{(Etape 4)}\\
+\ &\mathcal{O}(h_3^2 B_3^2 D_3^2) + \mathcal{O}(h_3 B_3^3 D_3^3) + (B_3^2 D_3^2 \log(B_3 D_3))\widetilde{\mathcal{O}}(\log \|\mathbf{a}_3\|) \quad \text{(Etape 5)}\\
+\ &\mathcal{O}(h_3^2 B_2 B_3 D_3) + \mathcal{O}(h_3 B_2^2 B_3^2 D_3^2) + (B_2 B_3 D_3 \log(B_2 B_3 D_3))\widetilde{\mathcal{O}}(\log \|\mathbf{a}_3\|) \quad \text{(Etape 7)}\\
=\ &\widetilde{\mathcal{O}}(h_3^7 D_3^{24}) + (N_3 h_3^3 D_3^{12})\widetilde{\mathcal{O}}(\log \|\mathbf{a}_3\|)
\end{aligned}$$

opérations binaires. Cela complète la preuve. □

Remarques. (**1**) Notons que le polynôme h renvoyé par l'Algorithme 14 peut avoir des facteurs cyclotomiques.

(**2**) Si f et g sont des quadrinômes lacunaires et si $\mathrm{Supp}(f) = \mathrm{Supp}(g)$ alors on peut prendre F et G comme les linéarisations de f et g. Dans ce cas, $D = 1$ et $\|\mathbf{a}_1\|_\infty = \deg(f) = \deg(g)$.

7.3 Exemple sur la recherche des facteurs communs non-cyclotomiques

Pour illustrer l'Algorithme 14, considérons les deux polynômes $F_3, G_3 \in \mathbb{Z}[x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$ et le vecteur $\mathbf{a}_3 \in \mathbb{Z}^3$ définis par :

$$\begin{aligned}
F_3(x_1, x_2, x_3) &= 1 + 2x_2 + 4x_3,\\
G_3(x_1, x_2, x_3) &= 1 + 16x_2x_3 + 16x_1 + 16x_3^2,\\
\mathbf{a}_3 &= (629249751, 168899897, 141923589).
\end{aligned}$$

Étape 1

On applique l'Algorithme 13 à F_3, G_3 et $\mathbf{a}_3$:

- on calcule le plus petit vecteur $\mathbf{b}$ orthogonal à $\mathbf{a}_3$: $\mathbf{b} = (-2009, 7704, -261)$. On a, par ailleurs, $B_3 = 5085406$ et donc $\|\mathbf{b}\|_\infty \leqslant B_3$;
- on calcule une base réduite de $\mathbf{b}^\perp$: $\mathbf{u}_1 = (-18, -3, 50)$ et $\mathbf{u}_2 = (-135, -37, -53)$;
- on détermine les coordonnées $\mathbf{a}_2$ de $\mathbf{a}_3$ dans cette base : $\mathbf{a}_2 = (-1841972, -4415513)$;
- on pose $F_2(\mathbf{y}) = F_1(\mathbf{y}^U)$ et $G_2(\mathbf{y}) = G_1(\mathbf{y}^U)$ où la i-ème ligne de U est le vecteur $\mathbf{u}_i$.

Étape 3

On a :

$$\begin{aligned} F_2(y_1, y_2) &= 4y_1^{53} + y_1^3 y_2^{53} + 2y_2^{16}, \\ G_2(y_1, y_2) &= 16y_1^{118} y_2^{29} + 16y_1^{65} y_2^{45} + y_1^{18} y_2^{135} + 16, \\ \mathbf{a}_2 &= (-1841972, -4415513). \end{aligned}$$

Étape 4

On applique l'Algorithme 13 à F_2, G_2 et $\mathbf{a}_2$:

- on calcule le plus petit vecteur $\mathbf{b}$ orthogonal à $\mathbf{a}_2$: $\mathbf{b} = (-4415513, 1841972)$; cependant on a $\|\mathbf{b}\|_\infty > B_2$ avec $B_2 = 93623$;
- on renvoie alors $\emptyset$.

Étape 5

On calcule $H_2 = \mathrm{pgcd}(F_2, G_2)$. On trouve $H_2(y_1, y_2) = 1$. Enfin, on conclut que $F_3(t^{\mathbf{a}_3})$ et $G_3(t^{\mathbf{a}_3})$ n'ont aucun facteur non-cyclotomique.

8. Cas général : vers une version explicite de la Conjecture de Schinzel

Dans ce chapitre, on présente une nouvelle méthode pour démontrer le Théorème 2 pour n quelconque en explicitant la dépendance de la constante par rapport à la taille des coefficients et au degré des polynômes. La dépendance de la constante n'est cependant pas explicite en n. Notre méthode s'inspire de l'approche de S. Checcoli, F. Veneziano et E. Viada dans [15], où ils ont démontré un théorème analogue au Théorème 2 pour le cas des courbes elliptiques. L'idée principale consiste à utiliser le Théorème de Bézout Arithmétique (Théorème 1.6.2.3) et une version fonctorielle du Théorème de Dobrowolski généralisé (Théorème 8.2.4). Pour expliciter la dépendance en n, il faudra expliciter la méthode de transfert de G. Rémond [39] qui permet de déduire une version fonctorielle du Théorème de Dobrowolski généralisé à partir de la version relative de E. Delsinne [20].

8.1 Présentation de l'approche

On fixe un entier $n \geqslant 2$. Soient $s \geqslant 2$ un entier et $F_1, \cdots, F_s \in \mathbb{Z}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$. On note V la sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie par $F_1 = \cdots = F_s = 0$. Soient $\mathbf{a} \in \mathbb{Z}^n$ un vecteur primitif et $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$. On note :

$$T = \{\xi^{\mathbf{a}} = (\xi^{a_1}, \cdots, \xi^{a_n}) \in \mathbb{G}_{\mathrm{m}}^n,\ \xi \in \mathbb{G}_{\mathrm{m}}\}.$$

On s'intéresse aux points $\boldsymbol{\alpha} \in V \cap \boldsymbol{\zeta} T$ qui ne sont pas de torsion et tels que V est de dimension au plus $n-2$ en $\boldsymbol{\alpha}$. On chercher à montrer que pour tout tel point $\boldsymbol{\alpha}$, 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 montre le théorème suivant.

Théorème 8.1.1. *Soient $n \geqslant 2$ et $s \geqslant 2$ deux entiers positifs. Soient $F_1, \cdots, F_s \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$. On note V la sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie par $F_1 = \cdots = F_s = 0$. Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon, n)$ ne dépendant que de ε et n et vérifiant la propriété suivante. Soient $\mathbf{0} \neq \mathbf{a} \in \mathbb{Z}^n$, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ et $\xi \in \overline{\mathbb{Q}} \setminus \boldsymbol{\mu}_\infty$. On note $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$. Si V est de codimension au moins 2 en $\boldsymbol{\alpha}$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^n$ orthogonal à $\mathbf{a}$ tel que :*

$$\|\mathbf{b}\|_2 \leqslant c(\varepsilon, n) \left(hD^{(n-1)^2} + D^{(n-1)^2+n}\right)^{1+\varepsilon},$$

où

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

On rappelle que V^{a} est la réunion des translatés de sous-tores de $\mathbb{G}_{\mathrm{m}}^n$ contenus dans V et $V^{\mathrm{o}} = V \setminus V^{\mathrm{a}}$. On rappelle également que $\dim_{\boldsymbol{\alpha}}(V)$ est la dimension maximale des composantes irréductibles de V contenant $\boldsymbol{\alpha}$. Pour démontrer Théorème 8.1.1, on sépare les deux cas : $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ et $\boldsymbol{\alpha} \in V^{\mathrm{a}}$.

Cas 1 : $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ (Proposition 8.3.1).

Puisque $\boldsymbol{\alpha}$ n'est pas un point de torsion et $\boldsymbol{\alpha} \in \boldsymbol{\zeta} T$, il existe $\xi \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}_\infty$ tel que $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$. Soit $\{\mathbf{b}_1, \cdots, \mathbf{b}_{n-1}\}$ une base réduite de $\mathbf{a}^\perp$ telle que $\|\mathbf{b}_1\|_2 \leqslant \|\mathbf{b}_2\|_2 \leqslant \cdots \leqslant \|\mathbf{b}_{n-1}\|_2$. Pour $i \in \{1, \cdots, n-$

$1\}$, le sous-groupe de $\mathbb{Z}^n$ engendré par les vecteurs $\mathbf{b}_1, \cdots, \mathbf{b}_i$ est primitif. On note T_i le sous-tore de $\mathbb{G}_{\mathrm{m}}^n$ de dimension $n-i$ défini par :

$$T_i = \{\mathbf{x} \in \mathbb{G}_{\mathrm{m}}^n \mid \mathbf{x}^{\mathbf{b}_1} = \cdots = \mathbf{x}^{\mathbf{b}_i} = 1\}.$$

On pose aussi $T_0 = \mathbb{G}_{\mathrm{m}}^n$. On a donc la suite de sous-tores suivante :

$$T_{n-1} \subset T_{n-2} \subset \cdots \subset T_1 \subset T_0 = \mathbb{G}_{\mathrm{m}}^n.$$

Pour $i \in \{0, 1, \cdots, n-2\}$, on a $\dim_{\boldsymbol{\alpha}}(V \cap \boldsymbol{\zeta} T_{i+1}) \leqslant \dim(\boldsymbol{\zeta} T_{i+1}) = n-i-1$. Si $\dim_{\boldsymbol{\alpha}}(V \cap \boldsymbol{\zeta} T_{i+1}) = n-i-1$ alors $\boldsymbol{\zeta} T_{i+1} \subseteq V$ et ceci contredit le fait que $\boldsymbol{\alpha} \in V^{\mathrm{o}}$. Ainsi, pour $i \in \{0, 1, \cdots, n-2\}$, on a :

$$\dim_{\boldsymbol{\alpha}}(V \cap \boldsymbol{\zeta} T_{i+1}) \leqslant n-i-2.$$

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

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

Par minimalité de m, on a $\dim_{\boldsymbol{\alpha}}(V \cap \boldsymbol{\zeta} T_i) \leqslant n-i-2$ pour $i \in \{1, \cdots, m\}$ et cela est aussi vrai pour $i = 0$ car $\dim_{\boldsymbol{\alpha}}(V) \leqslant n-2$. En particulier, on a :

$$\dim_{\boldsymbol{\alpha}}(V \cap \boldsymbol{\zeta} T_{m+1}) = \dim_{\boldsymbol{\alpha}}(V \cap \boldsymbol{\zeta} T_m) = n-m-2. \tag{8.1.1}$$

Soit Y une composante irréductible de $V \cap \boldsymbol{\zeta} T_{m+1}$ de dimension $n-m-2$ contenant $\boldsymbol{\alpha}$. D'après (8.1.1), Y est aussi une composante irréductible de $V \cap \boldsymbol{\zeta} T_m$.

En utilisant le Théorème de Bézout Arithmétique de P. Philippon, on majore la hauteur de Y en fonction de V et $\boldsymbol{\zeta} T_m$. En appliquant à Y une version effective et fonctorielle du Théorème de Dobrowolski généralisé (Théorème 8.2.4) qui provient des travaux de F. Amoroso, S. David, E. Delsinne, G. Rémond et U. Zannier, on minore la hauteur de Y en fonction de $\boldsymbol{\zeta} T_{m+1}$. Ensuite, on montre que la norme du vecteur $\mathbf{b}_{m+1}$ est majorée par une constante ne dépendant que de n et F_i (Proposition 8.3.1) et on choisit $\mathbf{b} = \mathbf{b}_{m+1}$. On note que la borne obtenue n'est pas complètement explicite en la dépendance en n. Pour expliciter cette dépendance en n, il faudrait expliciter davantage le résultat de G. Rémond qu'on utilise pour déduire la version fonctorielle à partir du théorème de E. Delsinne.

Cas 2 : $\boldsymbol{\alpha} \in V^{\mathrm{a}}$ (Proposition 8.3.2).

Dans ce cas, on construit à partir de V une sous-variété $W \subseteq \mathbb{G}_{\mathrm{m}}^r$ avec $r < n$ et un point $\boldsymbol{\beta} \in \mathbb{G}_{\mathrm{m}}^r$ qui n'est pas de torsion tels que $\boldsymbol{\beta} \in W^{\mathrm{o}} \cap B$ avec B un translaté de sous-tore par un point de torsion de dimension 1. On applique ensuite ce qu'on a obtenu dans le **Cas 1**.

Comme mentionné ci-dessus, l'approche repose sur une version effective et fonctorielle du Théorème de Dobrowolski généralisé. Pour énoncer ce théorème, on rappelle dans la Section 8.2 la définition de la hauteur normalisée et de l'indice d'obstruction. Dans la Section 8.3, on donne les propositions qui permettent de traiter les deux cas $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ et $\boldsymbol{\alpha} \in V^{\mathrm{a}}$ et on en déduit la démonstration du Théorème 8.1.1.

8.2 Théorème de Dobrowolski généralisé

Le problème de Lehmer et le Théorème de Dobrowolski se généralisent en dimension supérieure. Avant d'énoncer ces généralisations, on rappelle la définition de la hauteur normalisée et de l'indice d'obstruction d'une variété qui interviennent dans les énoncés.

Hauteur normalisée :

Soit $n \geqslant 1$ un entier et soit V une sous-variété algébrique de $\mathbb{G}_{\mathrm{m}}^n$ défini sur un corps $\mathbb{K} \subseteq \overline{\mathbb{Q}}$ et $\mathbb{K}$-irréductible. On considère le plongement naturel $\iota_n : \mathbb{G}_{\mathrm{m}}^n \hookrightarrow \mathbb{P}^n$ défini par $\iota_n(\alpha_1, \cdots, \alpha_n) = (1 : \alpha_1 : \cdots : \alpha_n)$. D'après [37], la *hauteur normalisée de V (par rapport au plongement ι_n)* est définie par :

$$\widehat{h}(V) = \lim_{m \to +\infty} \frac{h([m]V)\deg(V)}{m \deg([m]V)} \tag{8.2.1}$$

où $[m]$ est le morphisme *multiplication par m* (i.e. $[m](x_1, \cdots, x_n) = (x_1^m, \cdots, x_n^m)$).

D'après [19, Proposition 2.1, p.497], on a la relation suivante entre $\widehat{h}(V)$ et $h(V)$:

$$\left|\widehat{h}(V) - h(V)\right| \leqslant \frac{7}{2}(\dim V + 1)\deg(V)\log(n+1). \tag{8.2.2}$$

Minimum essentiel :

Pour $\theta > 0$, on note :

$$V(\theta) = \{\boldsymbol{\alpha} \in V(\overline{\mathbb{Q}}^*) \mid \widehat{h}(\boldsymbol{\alpha}) \leqslant \theta\}.$$

Le *minimum essentiel de V*, noté $\hat{\mu}^{\mathrm{ess}}(V)$, est défini par :

$$\hat{\mu}^{\mathrm{ess}}(V) = \inf\left\{\theta \in \mathbb{R} \mid \overline{V(\theta)} = V\right\}.$$

Le minimum essentiel de V est donc le seuil de la hauteur à partir duquel les points de V deviennent denses dans V. Si $\boldsymbol{\alpha} \in \mathbb{G}_{\mathrm{m}}^n$ alors on a $\hat{\mu}^{\mathrm{ess}}(\{\boldsymbol{\alpha}\}) = \hat{h}(\boldsymbol{\alpha})$. D'après [48, Théorème 5.2], on dispose également des inégalités suivantes appelées *inégalités de Zhang* :

$$\frac{\widehat{h}(V)}{(\dim(V)+1)\deg(V)} \leqslant \hat{\mu}^{\mathrm{ess}}(V) \leqslant \frac{\widehat{h}(V)}{\deg(V)}. \tag{8.2.3}$$

On dit que V est une *variété de torsion* si V est une réunion finie de translatés de sous-tores de $\mathbb{G}_{\mathrm{m}}^n$ par des points de torsion. D'après [47], $\hat{\mu}^{\mathrm{ess}}(V) = 0$ si et seulement si V est une variété de torsion.

Trouver une minoration du minimum essentiel (ou de la hauteur normalisée) d'une variété qui n'est pas de torsion est une des généralisations du Problème de Lehmer. D'après F. Amoroso et S. David [1], le bon invariant pour la minoration du minimum essentiel n'est pas le degré géométrique de V mais son *indice d'obstruction* qui est plus fin.

Indice d'obstruction :

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

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

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

Variété faiblement transverse :

Soit V une sous-variété algébrique irréductible de $\mathbb{G}_{\mathrm{m}}^n$. On dit que V est *faiblement transverse* si elle n'est contenue dans aucune sous-variété de torsion stricte de $\mathbb{G}_{\mathrm{m}}^n$.

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

Conjecture 8.2.1. *Soit V une sous-variété irréductible sur $\mathbb{Q}$ de $\mathbb{G}_{\mathrm{m}}^n$. On suppose que V est faiblement transverse. Alors, on a :*

$$\hat{\mu}^{\mathsf{ess}}(V) \geqslant \frac{c(n)}{\omega_{\mathbb{Q}}(V)}.$$

Cette conjecture a été énoncée et démontrée à un ε près par F. Amoroso et S. David dans [2]. Une version de ce résultat avec une dépendance explicite en n a été fait également dans [2].

On rappelle que $\mathbb{Q}^{\mathrm{ab}}$ désigne l'extension abélienne maximale de $\mathbb{Q}$ et, d'après le Théorème de Kronecker-Weber, $\mathbb{Q}^{\mathrm{ab}}$ est la réunion de toutes les extensions cyclotomiques de $\mathbb{Q}$. La version relative de la Conjecture 8.2.1 consiste à remplacer $\omega_{\mathbb{Q}}(V)$ par $\omega_{\mathbb{Q}^{\mathrm{ab}}}(V)$.

Conjecture 8.2.2. *Soit V une sous-variété irréductible de $\mathbb{G}_{\mathrm{m}}^n$. On suppose que V est faiblement transverse. Alors, on a :*

$$\hat{\mu}^{\mathsf{ess}}(V) \geqslant \frac{c(n)}{\omega_{\mathbb{Q}^{ab}}(V)}.$$

Cette conjecture a été aussi démontrée à un ε près par E. Delsinne dans [20] et son résultat est également explicite en n. On va énoncer la version faible de son résultat principal, sans expliciter la dépendance de la constante en n.

Théorème 8.2.3. *[20, Corollaire 1.7] Soit V une sous-variété irréductible de $\mathbb{G}_{\mathrm{m}}^n$. On suppose que V est faiblement transverse. Alors, pour tout $\varepsilon > 0$, on a :*

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

On s'intéresse maintenant à la version fonctorielle du Théorème 8.2.3 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. La version suivante se déduit du théorème qui précède à l'aide d'un résultat de transfert de G. Rémond [39].

Théorème 8.2.4. *Soit V une sous-variété irréductible de $\mathbb{G}_{\mathrm{m}}^n$. Soit $W \subseteq \mathbb{G}_{\mathrm{m}}^n$ la plus petite sous-variété de torsion contenant V. Alors, pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon, n) > 0$ tel que :*

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

Démonstration. On applique la version torique du Théorème 3.7 de [39, p.261] avec $\Gamma = \boldsymbol{\mu}_{\infty}^n$. En effet, d'après le Théorème 8.2.3, $\boldsymbol{\mu}_{\infty}^n$ est de Dobrowolski. D'après le Théorème de Kronecker-Weber, le corps K_{Γ} de rationalité de $\boldsymbol{\mu}_{\infty}^n$ est la réunion de toutes les extensions cyclotomiques de $\mathbb{Q}$. Donc on a $K_{\Gamma} = \mathbb{Q}^{\mathrm{ab}}$. □

8.3 Propositions clés et Démonstration du Théorème 8.1.1

On donne ici les deux propositions clés et leurs démonstrations.

Cas 1 : α n'appartient à aucun translaté de sous-tore contenu dans V

On suppose d'abord que $\boldsymbol{\alpha} \in V^{\mathrm{o}}$.

Proposition 8.3.1. *Soient $n \geqslant 2$ et $s \geqslant 2$ deux entiers positifs. Soient $F_1, \cdots, F_s \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$. On note V la sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie par $F_1 = \cdots = F_s = 0$. Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon, n)$ ne dépendant que de ε et n et vérifiant la propriété suivante. Soient $\mathbf{0} \neq \mathbf{a} \in \mathbb{Z}^n$, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ et $\xi \in \overline{\mathbb{Q}} \setminus \boldsymbol{\mu}_\infty$. On note $\boldsymbol{\alpha} = \boldsymbol{\zeta}\xi^{\mathbf{a}}$. Si V est de codimension $k \geqslant 2$ en $\boldsymbol{\alpha}$ et $\boldsymbol{\alpha} \in V^o$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^n$ orthogonal à $\mathbf{a}$ tel que :*

$$\|\mathbf{b}\|_2 \leqslant c(\varepsilon, n) \left(hD^{k-1} + D^k\right)^{1+\varepsilon},$$

où l'on a noté :

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

Démonstration. Soit $\varepsilon > 0$. Dans la preuve, $c_0, c_1, \cdots, c_7$ désigneront des constantes strictement positives qui ne dépendent que de ε et n.

Soit $\{\mathbf{b}_1, \cdots, \mathbf{b}_{n-1}\}$ une base réduite de $\mathbf{a}^\perp$ telle que $\|\mathbf{b}_1\|_2 \leqslant \|\mathbf{b}_2\|_2 \leqslant \cdots \leqslant \|\mathbf{b}_{n-1}\|_2$. Pour $i \in \{1, \cdots, n-1\}$, on note T_i le sous-tore de $\mathbb{G}_{\mathrm{m}}^n$ défini par le sous-groupe primitif engendré par les vecteurs $\mathbf{b}_1, \cdots, \mathbf{b}_i$. On note $m \in \{0, \cdots, n-2\}$ le plus petit entier vérifiant :

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

Soit Y une composante irréductible de $V \cap \boldsymbol{\zeta} T_{m+1}$ de dimension $n-2-m$ et contenant $\boldsymbol{\alpha}$. D'après l'égalité (8.1.1), Y est également une composante irréductible de $V \cap \boldsymbol{\zeta} T_m$. Pour $i \in \{1, \cdots, n-1\}$, on note $G_i(\mathbf{x}) = \mathbf{x}^{\mathbf{b}_i} - \boldsymbol{\zeta}^{\mathbf{b}_i}$. On note $\mathbb{Q}^{\mathrm{ab}}(Y)$ le corps de définition de Y sur $\mathbb{Q}^{\mathrm{ab}}$ et $[\mathbb{Q}^{\mathrm{ab}}(Y) : \mathbb{Q}^{\mathrm{ab}}]$ son degré sur $\mathbb{Q}^{\mathrm{ab}}$. Pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})$, $\sigma(Y) \subseteq \sigma(V \cap \boldsymbol{\zeta} T_m) \subseteq V \cap \boldsymbol{\zeta} T_m$ car V et T_m sont définis sur $\mathbb{Q}$ et $\boldsymbol{\zeta} \in \mathbb{Q}^{\mathrm{ab}}$. On obtient alors :

$$\hat{Y} := \bigcup_{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})} \sigma(Y) \subseteq V \cap \boldsymbol{\zeta} T_m. \tag{8.3.1}$$

D'après (8.3.1) et le Corollaire 1.6.2.5 (qui est une conséquence du Théorème de Bézout Arithmétique), on a :

$$[\mathbb{Q}^{\mathrm{ab}}(Y) : \mathbb{Q}^{\mathrm{ab}}] h(Y) \leqslant \left(h(V) + \frac{m}{2}\left(\log(n+1) + \sum_{i=1}^{n} \frac{1}{i}\right) \deg(V)\right) \prod_{i=1}^{m} \deg(G_i).$$

D'après le Corollaire 1.6.2.6 (qui est aussi une conséquence des théorèmes de Bézout Géométrique et Arithmétique), on a :

$$\deg(V) \leqslant D^k \quad \text{et} \quad h(V) \leqslant c_0(n)\left(hD^{k-1} + D^k\right). \tag{8.3.2}$$

Par suite :

$$[\mathbb{Q}^{\mathrm{ab}}(Y) : \mathbb{Q}^{\mathrm{ab}}] h(Y) \leqslant c_1(n)\left(hD^{k-1} + D^k\right) \prod_{i=1}^{m} \deg(G_i). \tag{8.3.3}$$

On va minorer $\hat{\mu}^{\mathrm{ess}}(Y)$ en utilisant le Théorème 8.2.4 et ensuite appliquer les inégalités de Zhang pour majorer $\hat{\mu}^{\mathrm{ess}}(Y)$ en fonction de $h(Y)$.

Soit $W \subseteq \mathbb{G}_{\mathrm{m}}^n$ la plus petite sous-variété de torsion contenant Y. On a alors $Y \subseteq W \subseteq \boldsymbol{\zeta} T_{m+1}$. De plus, $\dim(Y) = n-m-2$ par choix de Y et $\dim(\boldsymbol{\zeta} T_{m+1}) = n-m-1$ par définition de T_{m+1}. Par ailleurs, Y n'est pas de torsion car $\boldsymbol{\alpha} \in Y$ et $\boldsymbol{\alpha} \in V^{\mathrm{o}}$. On en déduit que $W = \boldsymbol{\zeta} T_{m+1}$.

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

$$\omega_{\mathbb{Q}^{\mathrm{ab}}}(Y, \boldsymbol{\zeta} T_{m+1}) = \min_{Z} \left(\frac{\deg(Z)}{\deg(\boldsymbol{\zeta} T_{m+1})} \right)^{1/\mathrm{codim}_{\boldsymbol{\zeta} T_{m+1}}(Z)}$$

où Z parcourt les sous-variétés strictes de $\boldsymbol{\zeta} T_{m+1}$, définies sur $\mathbb{Q}^{\mathrm{ab}}$ et contenant Y. La variété $\hat{Y}$ définie dans (8.3.1) est une sous-variété de $\boldsymbol{\zeta} T_{m+1}$ définie sur $\mathbb{Q}^{\mathrm{ab}}$ et de dimension $= n-m-2$. Comme $\dim(\boldsymbol{\zeta} T_{m+1}) = n-m-1$, l'inclusion $\hat{Y} \subset \boldsymbol{\zeta} T_{m+1}$ est stricte. On a donc :

$$\omega_{\mathbb{Q}^{\mathrm{ab}}}(Y, \boldsymbol{\zeta} T_{m+1}) \leqslant \frac{\deg(\hat{Y})}{\deg(\boldsymbol{\zeta} T_{m+1})}.$$

On pose :

$$\varepsilon' = \frac{\varepsilon}{1 + (n-2)(1+\varepsilon)}. \tag{8.3.4}$$

D'après le Théorème 8.2.4, il existe une constante $c(\varepsilon', n) =: c_2(\varepsilon, n)$ strictement positive telle que :

$$\hat{\mu}^{\mathrm{ess}}(Y) \geqslant \frac{c_2(\varepsilon, n)}{\omega_{\mathbb{Q}^{\mathrm{ab}}}(Y, \boldsymbol{\zeta} T_{m+1})^{1+\varepsilon'} \deg(\boldsymbol{\zeta} T_{m+1})^{\varepsilon'}} \geqslant c_2(\varepsilon, n) \frac{\deg(\boldsymbol{\zeta} T_{m+1})}{\deg(\hat{Y})^{1+\varepsilon'}}.$$

En utilisant les inégalités de Zhang (8.2.3), on majore le minimum essentiel de Y en fonction de la hauteur normalisée :

$$c_2(\varepsilon, n) \frac{\deg(\boldsymbol{\zeta} T_{m+1})}{\deg(\hat{Y})^{1+\varepsilon'}} \leqslant \hat{\mu}^{\mathrm{ess}}(Y) \leqslant \frac{\hat{h}(Y)}{\deg(Y)}.$$

À l'aide de la relation (8.2.2), on majore $\hat{h}(Y)$ en fonction de $h(Y)$:

$$c_2(\varepsilon, n) \frac{\deg(\boldsymbol{\zeta} T_{m+1})}{\deg(\hat{Y})^{1+\varepsilon'}} \leqslant \frac{h(Y)}{\deg(Y)} + \frac{7}{2} (\dim Y + 1) \log(n+1).$$

On majore $h(Y)$ à l'aide de l'inégalité (8.3.3) et $\dim(Y)$ par $n-3$:

$$c_2(\varepsilon, n) \frac{\deg(\boldsymbol{\zeta} T_{m+1})}{\deg(\hat{Y})^{1+\varepsilon'}} \leqslant \frac{c_1(n) \left(h D^{k-1} + D^k \right)}{[\mathbb{Q}^{\mathrm{ab}}(Y) : \mathbb{Q}^{\mathrm{ab}}] \deg(Y)} \prod_{i=1}^{m} \deg(G_i) + \frac{7}{2}(n-2) \log(n+1).$$

En multipliant les deux membres par $\deg(\hat{Y})^{1+\varepsilon'}$, on a :

$$c_2(\varepsilon, n) \deg(\boldsymbol{\zeta} T_{m+1}) \leqslant \frac{c_1(n) \left(h D^{k-1} + D^k \right) \deg(\hat{Y})^{1+\varepsilon'}}{[\mathbb{Q}^{\mathrm{ab}}(Y) : \mathbb{Q}^{\mathrm{ab}}] \deg(Y)} \prod_{i=1}^{m} \deg(G_i) + \frac{7}{2}(n-2) \log(n+1) \deg(\hat{Y})^{1+\varepsilon'}.$$

Par définition, on a $\deg(\hat{Y}) = [\mathbb{Q}^{\mathrm{ab}}(Y) : \mathbb{Q}^{\mathrm{ab}}] \deg(Y)$. En simplifiant le dénominateur, on obtient :

$$c_2(\varepsilon, n) \deg(\boldsymbol{\zeta} T_{m+1}) \leqslant c_1(n) \left(hD^{k-1} + D^k\right) \deg(\hat{Y})^{\varepsilon'} \prod_{i=1}^{m} \deg(G_i) + \frac{7}{2}(n-2)\log(n+1)\deg(\hat{Y})^{1+\varepsilon'}. \quad (8.3.5)$$

Il faut maintenant majorer $\deg(\hat{Y})$. On applique le Théorème de Bézout Géométrique (Théorème 1.6.2.1) en tenant compte de (8.3.1) :

$$\deg(\hat{Y}) \leqslant \deg(V) \prod_{i=1}^{m} \deg(G_i) \leqslant D^k \prod_{i=1}^{m} \deg(G_i),$$

où la majoration de $\deg(V)$ suit de (8.3.2). En remplaçant $\deg(\hat{Y})$ par cette majoration dans (8.3.5), on obtient :

$$\begin{aligned} c_2(\varepsilon, n) \deg(\boldsymbol{\zeta} T_{m+1}) &\leqslant c_1(n) \left(hD^{k-1} + D^k\right) D^{k\varepsilon'} \left(\prod_{i=1}^{m} \deg(G_i)\right)^{1+\varepsilon'} + \\ &\quad \frac{7}{2}(n-2)\log(n+1) D^{k(1+\varepsilon')} \left(\prod_{i=1}^{m} \deg(G_i)\right)^{1+\varepsilon'} \\ &\leqslant c_3(n) \left(hD^{k(1+\varepsilon')-1} + D^{k(1+\varepsilon')}\right) \left(\prod_{i=1}^{m} \deg(G_i)\right)^{1+\varepsilon'}. \end{aligned}$$

D'après [9], le degré de T_{m+1} est égal au maximum des valeurs absolues des déterminants des mineurs $(m+1) \times (m+1)$ de la matrice formée par les vecteurs $\mathbf{b}_1, \cdots, \mathbf{b}_{m+1}$. Comme $\{\mathbf{b}_1, \cdots, \mathbf{b}_{n-1}\}$ est une base réduite, on peut minorer $\deg(T_{m+1})$ par $c_4(n) \prod_{i=1}^{m+1} \|\mathbf{b}_i\|_2$.

En majorant $\deg(G_i)$ par $\|\mathbf{b}_i\|_1 \leqslant \sqrt{n}\|\mathbf{b}_i\|_2$, on obtient :

$$\prod_{i=1}^{m+1} \|\mathbf{b}_i\|_2 \leqslant c_6(\varepsilon, n) \left(hD^{k(1+\varepsilon')-1} + D^{k(1+\varepsilon')}\right) \left(\prod_{i=1}^{m} \|\mathbf{b}_i\|_2\right)^{1+\varepsilon'}.$$

En simplifiant par $\prod_{i=1}^{m} \|\mathbf{b}_i\|_2$, on a :

$$\|\mathbf{b}_{m+1}\|_2 \leqslant c_6(\varepsilon, n) \left(hD^{k(1+\varepsilon')-1} + D^{k(1+\varepsilon')}\right) \left(\prod_{i=1}^{m} \|\mathbf{b}_i\|_2\right)^{\varepsilon'}.$$

En majorant $\prod_{i=1}^{m} \|\mathbf{b}_i\|_2$ par $\|\mathbf{b}_{m+1}\|_2^m$, on a :

$$\|\mathbf{b}_{m+1}\|_2^{1-m\varepsilon'} \leqslant c_6(\varepsilon, n) \left(hD^{k(1+\varepsilon')-1} + D^{k(1+\varepsilon')}\right).$$

Comme $m \leqslant n-2$, on a $1-(n-2)\varepsilon' \leqslant 1-m\varepsilon'$ et donc :

$$\|\mathbf{b}_{m+1}\|_2^{1-(n-2)\varepsilon'} \leqslant c_6(\varepsilon, n) \left(hD^{k(1+\varepsilon')-1} + D^{k(1+\varepsilon')}\right). \quad (8.3.6)$$

Par définition (8.3.4) de ε', on a :

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

Ainsi, l'inégalité (8.3.6) montre que la norme de $\mathbf{b}_{m+1}$ est majorée par une constante ne dépendant que de ε, n, D et h. On va déterminer la dépendance de telle constante en D et en h. On a :

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

Par définition (8.3.4) de ε', on a :

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

Par suite, on a :

$$\|\mathbf{b}_{m+1}\|_2 \leqslant c_7(\varepsilon,n)\left(\frac{h}{D}+1\right)^{1+\varepsilon} D^{k(1+\varepsilon)}.$$

Enfin, puisque $\boldsymbol{\zeta}\boldsymbol{\xi}^{\mathbf{a}} \in \boldsymbol{\zeta}T_{m+1}$, on a $\boldsymbol{\xi}^{\mathbf{a}} \in T_{m+1}$ et donc $\boldsymbol{\xi}^{\mathbf{a}\mathbf{b}_{m+1}} = 0$. Comme $\boldsymbol{\xi}$ n'est pas une racine de l'unité, $\mathbf{a}\mathbf{b}_{m+1} = 0$. On choisit donc $\mathbf{b} = \mathbf{b}_{m+1}$. □

Cas 2 : α appartient à un translaté de sous-tore contenu dans V

On suppose maintenant $\boldsymbol{\alpha} \in V^{\mathrm{a}}$.

Proposition 8.3.2. *Soient $n \geqslant 2$ et $s \geqslant 2$ deux entiers positifs. Soient $F_1, \cdots, F_s \in \mathbb{Z}[\mathbf{x}^{\pm 1}]$. On note V la sous-variété de $\mathbb{G}_{\mathrm{m}}^n$ définie par $F_1 = \cdots = F_s = 0$. Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon, n)$ ne dépendant que de ε et n et vérifiant la propriété suivante. Soient $\mathbf{0} \neq \mathbf{a} \in \mathbb{Z}^n$, $\boldsymbol{\zeta} \in \boldsymbol{\mu}_\infty^n$ et $\xi \in \overline{\mathbb{Q}} \setminus \boldsymbol{\mu}_\infty$. On note $\boldsymbol{\alpha} = \boldsymbol{\zeta}\boldsymbol{\xi}^{\mathbf{a}}$. Si V est de codimension au moins 2 en $\boldsymbol{\alpha}$ et $\boldsymbol{\alpha} \in V^a$ alors il existe un vecteur non nul $\mathbf{b} \in \mathbb{Z}^n$ orthogonal à $\mathbf{a}$ tel que :*

$$\|\mathbf{b}\|_2 \leqslant c(\varepsilon,n)\left(hD^{(n-1)^2}+D^{(n-1)^2+n}\right)^{1+\varepsilon},$$

où l'on a noté :

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

Démonstration. Soit $\varepsilon > 0$. Dans la preuve, $\kappa_1, \kappa_2, \kappa_3$ désigneront des constantes strictement positives qui ne dépendent que de n et ε.

D'après l'hypothèse, il existe un sous-tore T de $\mathbb{G}_{\mathrm{m}}^n$ de dimension non nulle tel que $\boldsymbol{\alpha}T \subseteq V$. On choisit T tel que $\boldsymbol{\alpha}T$ soit maximal dans V. Notons $r = n - \dim(T)$. On va construire un automorphisme φ de $\mathbb{G}_{\mathrm{m}}^n$ tel que $\varphi(T) = \{\mathbf{y} \in \mathbb{G}_{\mathrm{m}}^n \mid y_1 = \cdots = y_r = 1\}$.

D'après la Proposition 1.3.2.3 qui suit le Lemme 4 de W. Schmidt [42], il existe n vecteurs $\boldsymbol{\mu}_1, \cdots, \boldsymbol{\mu}_n$ formant une base de $\mathbb{Z}^n$ tels que :

— T est défini par les équations $\mathbf{x}^{\boldsymbol{\mu}_1} - 1 = \cdots = \mathbf{x}^{\boldsymbol{\mu}_r} - 1 = 0$,
— les $\boldsymbol{\mu}_i$ sont définis comme suit :

$$\begin{cases}\boldsymbol{\mu}_1 = & c_1\boldsymbol{\lambda}_1,\\ \boldsymbol{\mu}_2 = & c_{2,1}\boldsymbol{\lambda}_1 + c_2\boldsymbol{\lambda}_2,\\ \boldsymbol{\mu}_3 = & c_{3,1}\boldsymbol{\lambda}_1 + c_{3,2}\boldsymbol{\lambda}_2 + c_3\boldsymbol{\lambda}_3,\\ \vdots & \\ \boldsymbol{\mu}_n = & c_{n,1}\boldsymbol{\lambda}_1 + c_{n,2}\boldsymbol{\lambda}_2 + \cdots + c_n\boldsymbol{\lambda}_n,\end{cases} \tag{8.3.7}$$

où $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_r \in \bigcup_i \mathcal{D}(F_i)$, les vecteurs $\boldsymbol{\lambda}_{r+1}, \cdots, \boldsymbol{\lambda}_n$ sont des vecteurs de la base canonique de $\mathbb{Z}^n$, les constantes $c_{i,j}$ (pour $1 \leqslant j < i \leqslant n$) et c_k (pour $1 \leqslant k \leqslant n$) sont des nombres rationnels vérifiant $|c_{i,j}| \leqslant 1/2$ et $0 < c_k \leqslant 1$. Par définition des $\boldsymbol{\mu}_i$, on a :

$$\|\boldsymbol{\mu}_i\|_\infty \leqslant n \max_{1 \leqslant j \leqslant s} \deg(F_j) \leqslant nD. \tag{8.3.8}$$

On note M la matrice dont les colonnes sont formées par les vecteurs $\boldsymbol{\mu}_1, \cdots, \boldsymbol{\mu}_n$. Par construction, $M \in \mathrm{GL}_n(\mathbb{Z})$. On considère l'automorphisme φ de $\mathbb{G}_{\mathrm{m}}^n$ défini par :

$$\begin{aligned} \varphi : \mathbb{G}_{\mathrm{m}}^n &\longrightarrow \mathbb{G}_{\mathrm{m}}^n \\ \mathbf{x} &\mapsto \mathbf{x}^M = (\mathbf{x}^{\boldsymbol{\mu}_1}, \cdots, \mathbf{x}^{\boldsymbol{\mu}_n}). \end{aligned}$$

On a alors :

$$\varphi(T) = \{\mathbf{y} \in \mathbb{G}_{\mathrm{m}}^n \mid y_1 = \cdots = y_r = 1\}.$$

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

$$F_i(\varphi^{-1}(\mathbf{y})) = \sum_{j=1}^{t} F_{i,j}(y_1, \cdots, y_r) y_{r+1}^{\theta_{j,r+1}} \cdots y_n^{\theta_{j,n}} \tag{8.3.9}$$

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

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

On considère la sous-variété W de $\mathbb{G}_{\mathrm{m}}^r$ définie par :

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

On a alors :

$$W = \{(y_1, \cdots, y_r) \in \mathbb{G}_{\mathrm{m}}^r \mid \forall (y_{r+1}, \cdots, y_n) \in \mathbb{G}_{\mathrm{m}}^{n-r},\ (y_1, \cdots, y_n) \in \varphi(V)\}. \tag{8.3.10}$$

En effet, on note $W' \coloneqq \{(y_1, \cdots, y_r) \in \mathbb{G}_{\mathrm{m}}^r \mid \forall (y_{r+1}, \cdots, y_n) \in \mathbb{G}_{\mathrm{m}}^{n-r},\ (y_1, \cdots, y_n) \in \varphi(V)\}$. Soit $(y_1, \cdots, y_r) \in W$. Pour tout $j \in \{1, \cdots, s'\}$, on a $G_j(y_1, \cdots, y_r) = 0$. Donc pour tout $i \in \{1, \cdots, s\}$, on a $F_i(\varphi^{-1}(\mathbf{y})) = 0$ pour $(y_{r+1}, \cdots, y_n) \in \mathbb{G}_{\mathrm{m}}^{n-r}$. Ainsi, $\varphi^{-1}(\mathbf{y}) \in V$ et donc $\mathbf{y} \in \varphi(V)$. Ceci prouve l'inclusion $W \subseteq W'$. Pour l'autre inclusion, soit $(y_1, \cdots, y_r) \in W'$. Pour tout $(y_{r+1}, \cdots, y_n) \in \mathbb{G}_{\mathrm{m}}^{n-r}$, $\mathbf{y} \in \varphi(V)$. Par suite, on a $\varphi^{-1}(\mathbf{y}) \in V$ et donc $F_i(\varphi^{-1}(\mathbf{y})) = 0$ pour tout $i \in \{1, \cdots, s\}$. Puisque cela est vrai pour tout $(y_{r+1}, \cdots, y_n) \in \mathbb{G}_{\mathrm{m}}^{n-r}$ et en utilisant (8.3.9), on en déduit que $G_j(y_1, \cdots, y_r) = 0$ pour tout $j \in \{1, \cdots, s'\}$.

On note ensuite $\boldsymbol{\beta}$ l'image de $\boldsymbol{\alpha}$ par φ i.e. $\boldsymbol{\beta} = \varphi(\boldsymbol{\alpha}) = (\boldsymbol{\zeta}^{\boldsymbol{\mu}_1}\boldsymbol{\xi}^{\mathbf{a}\boldsymbol{\mu}_1}, \cdots, \boldsymbol{\zeta}^{\boldsymbol{\mu}_n}\boldsymbol{\xi}^{\mathbf{a}\boldsymbol{\mu}_n})$ et on pose $\boldsymbol{\beta}' = (\boldsymbol{\zeta}^{\boldsymbol{\mu}_1}\boldsymbol{\xi}^{\mathbf{a}\boldsymbol{\mu}_1}, \cdots, \boldsymbol{\zeta}^{\boldsymbol{\mu}_r}\boldsymbol{\xi}^{\mathbf{a}\boldsymbol{\mu}_r})$. On a :

$$\begin{aligned} \{\boldsymbol{\beta}'\} \times \mathbb{G}_{\mathrm{m}}^{n-r} &= \{(\beta_1, \cdots, \beta_r, \beta_{r+1} y_{r+1}, \cdots, \beta_n y_n) \in \mathbb{G}_{\mathrm{m}}^n,\ (y_{r+1}, \cdots, y_n) \in \mathbb{G}_{\mathrm{m}}^{n-r}\} \\ &= \boldsymbol{\beta}\varphi(T) \quad \text{car} \quad \varphi(T) = \{\mathbf{y} \in \mathbb{G}_{\mathrm{m}}^n \mid y_1 = \cdots = y_r = 1\} \\ &= \varphi(\boldsymbol{\alpha} T) \\ &\subseteq \varphi(V). \end{aligned}$$

D'après (8.3.10), on déduit que $\boldsymbol{\beta}' \in W$.

Supposons qu'il existe un sous-tore $T' \subseteq \mathbb{G}_{\mathrm{m}}^r$ de dimension non nulle tel que $\boldsymbol{\beta}'T' \subseteq W$. On a alors $\boldsymbol{\beta}(T' \times \mathbb{G}_{\mathrm{m}}^{n-r}) \subseteq W \times \mathbb{G}_{\mathrm{m}}^{n-r} \subseteq \varphi(V)$. Cela implique que $\boldsymbol{\alpha}$ est contenu dans un translaté de sous-tore de dimension $\geqslant n-r+1$ contenu dans V. Cela contredit le fait que $\boldsymbol{\alpha}T \subseteq V$ est maximal dans V. On déduit donc $\boldsymbol{\beta}' \in W^{\mathrm{o}}$.

De nouveau par (8.3.10), on a $W \times \mathbb{G}_{\mathrm{m}}^{n-r} \subseteq \varphi(V)$ et donc :

$$\dim_{\boldsymbol{\beta}'}(W) + n - r = \dim_{\boldsymbol{\beta}}(W \times \mathbb{G}_{\mathrm{m}}^{n-r}) \leqslant \dim_{\boldsymbol{\beta}}(\varphi(V)) = \dim_{\boldsymbol{\alpha}}(V) \leqslant n-2.$$

Cela implique que $W \subseteq \mathbb{G}_{\mathrm{m}}^r$ est de codimension $k' \geqslant 2$ en $\boldsymbol{\beta}'$.

On remarque également que si $\mathbf{a}\boldsymbol{\mu}_1 = 0$ alors on a la conclusion de la proposition avec $\mathbf{b} = \boldsymbol{\mu}_1$ car $\|\boldsymbol{\mu}_1\|_\infty \leqslant nD$ d'après (8.3.8). On suppose dorénavant que $\mathbf{a}\boldsymbol{\mu}_1 \neq 0$. Ainsi le vecteur $(\mathbf{a}\boldsymbol{\mu}_1, \cdots, \mathbf{a}\boldsymbol{\mu}_r)$ est non nul. Puisque $\boldsymbol{\beta} = (\boldsymbol{\zeta}^{\boldsymbol{\mu}_1}\xi^{\mathbf{a}\boldsymbol{\mu}_1}, \cdots, \boldsymbol{\zeta}^{\boldsymbol{\mu}_r}\xi^{\mathbf{a}\boldsymbol{\mu}_r})$ et ξ n'est pas une racine de l'unité, d'après la Proposition 8.3.1, il existe une constante $\kappa_1(\varepsilon, n)$, qui ne dépend que de ε et n, et un vecteur non nul $\boldsymbol{\eta} \in \mathbb{Z}^r$ orthogonal à $(\mathbf{a}\boldsymbol{\mu}_1, \cdots, \mathbf{a}\boldsymbol{\mu}_r)$ tels que :

$$\|\boldsymbol{\eta}\|_2 \leqslant \kappa_1(\varepsilon, n)\left(h'D'^{k'-1} + D'^{k'}\right)^{1+\varepsilon} \tag{8.3.11}$$

où

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

On considère ensuite le vecteur $\mathbf{b}$ défini par $\mathbf{b} = \eta_1\boldsymbol{\mu}_1 + \cdots + \eta_r\boldsymbol{\mu}_r$. Puisque $(\eta_1, \cdots, \eta_r)$ est non nul et $\boldsymbol{\mu}_1, \cdots, \boldsymbol{\mu}_r$ sont linéairement indépendants, $\mathbf{b}$ est aussi non nul. Comme $(\eta_1, \cdots, \eta_r) \in \mathbb{Z}^r$ est orthogonal à $(\mathbf{a}\boldsymbol{\mu}_1, \cdots, \mathbf{a}\boldsymbol{\mu}_r)$, on a $\mathbf{ab} = 0$. On va déterminer une majoration de la norme de $\mathbf{b}$ en fonction de D et h.

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

$$(n-1)^{(n-1)/2} \max_{1 \leqslant i \leqslant n} \|\boldsymbol{\mu}_i\|_\infty^{n-1} \leqslant n^{3(n-1)/2} D^{n-1}.$$

Par suite, on a :

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

Par ailleurs, on a :

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

En remplaçant D' et h' par ces majorations dans (8.3.11), on obtient :

$$\|\boldsymbol{\eta}\|_2 \leqslant \kappa_2(\varepsilon, n)\left(hD^{n(k'-1)} + D^{nk'}\right)^{1+\varepsilon}$$

En majorant k' par $r \leqslant n-1$, on obtient :

$$\|\boldsymbol{\eta}\|_2 \leqslant \kappa_2(\varepsilon, n)\left(hD^{n(n-2)} + D^{n(n-1)}\right)^{1+\varepsilon}.$$

Enfin, par définition de $\mathbf{b}$, on a :

$$\|\mathbf{b}\|_2 \leqslant \kappa_3(\varepsilon, n)\left(hD^{n(n-2)+1} + D^{n(n-1)+1}\right)^{1+\varepsilon}.$$

□

Démonstration du Théorème 8.1.1

Démonstration. Soit $\varepsilon > 0$. Dans la preuve, c_1 et c_2 désigneront des constantes strictement positives qui ne dépendent que de ε et n. On note k la codimension de V dans $\mathbb{G}_{\mathrm{m}}^n$.

Si $\boldsymbol{\alpha} \in V^{\mathrm{o}}$ alors d'après la Proposition 8.3.1, il existe une constante $c_1(\varepsilon, n)$ qui ne dépend que de ε et n, et un vecteur $\mathbf{b} \in \mathbb{Z}^n$ orthogonal à $\mathbf{a}$ tels que :

$$\|\mathbf{b}\|_2 \leqslant c_1(\varepsilon, n) \left(hD^{k-1} + D^k\right)^{1+\varepsilon}.$$

Si $\boldsymbol{\alpha} \in V^{\mathrm{a}}$ alors d'après la Proposition 8.3.2, il existe une constante $c_2(\varepsilon, n)$, qui ne dépend que de ε et n, et un vecteur $\mathbf{b} \in \mathbb{Z}^n$ orthogonal à $\mathbf{a}$ tels que :

$$\|\mathbf{b}\|_2 \leqslant c_2(\varepsilon, n) \left(hD^{(n-1)^2} + D^{(n-1)^2+n}\right)^{1+\varepsilon}.$$

En majorant k par n et en prenant le maximum entre les deux bornes, on a le résultat voulu. □

Annexe A. Algorithme et résultats annexes

A.1 Algorithme pour les sous-groupes de $\mathbb{Z}^n$

Soit $M \in M_{n,m}(\mathbb{Z})$. On dit que M est sous la forme normale d'Hermite (abrégé HNF) s'il existe un entier $r \leqslant m$ et une application strictement croissante $f : [r+1, m] \to [1, n]$ vérifiant :

(i) les r premières colonnes de M sont égales à $\mathbf{0}$,

(ii) pour $j \in \{r+1, \cdots, m\}$, on a :

$$m_{f(i),j} \geqslant 1 \text{ et } m_{i,j} = 0 \text{ si } i > f(j) \quad \text{et} \quad 0 \leqslant m_{f(k),j} < m_{f(k),k} \text{ si } k < j.$$

Remarque. Si $m = n$ et $f(k) = k$ alors M est sous-HNF si elle satisfait les conditions suivantes :

(i) M est triangulaire supérieure i.e. $m_{ij} = 0$ si $i > j$,

(ii) pour tout i, $m_{i,i} > 0$,

(ii) pour tout $j > i$, $0 \leqslant m_{i,j} < m_{i,i}$.

Théorème A.1.1. *[16, Theorem 2.4.3] Soit M une matrice de taille $n \times m$ à coefficients dans $\mathbb{Z}$. Alors il existe une unique matrice H de taille $n \times m$ sous la forme HNF telle que $H = MU$ où $U \in GL_m(\mathbb{Z})$.*

L'algorithme correspondant à ce théorème est [16, Algorithm 2.4.4]. Soit Λ un sous-groupe de $\mathbb{Z}^n$ engendré par $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_m$. L'algorithme suivant permet de calculer le rang de Λ, son saturé, son orthogonal et un complété de Λ^{sat} en une base de $\mathbb{Z}^n$ à partir de la HNF de la matrice M dont les lignes sont les coordonnés de $\boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_m$ par rapport à la base canonique de $\mathbb{Z}^n$.

Algorithme 15 : Caractéristiques d'un sous-groupe de $\mathbb{Z}^n$

Entrée : $\Lambda = \langle \boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_m \rangle$ sous-groupe de $\mathbb{Z}^n$

Sortie : $\text{rang}(\Lambda)$, Λ^{sat}, $\Lambda^{\perp}$ et le completé de Λ^{sat} en une base de $\mathbb{Z}^n$

1 Poser M la matrice de taille $m \times n$ dont la i-ème ligne est le vecteur $\boldsymbol{\lambda}_i$.

2 Calculer H et U tels $MU = H$ en utilisant la HNF ou l'algorithme LLL, où H est la forme normale de Hermite de M et $U \in \text{GL}_n(\mathbb{Z})$.

3 Poser $r =$ le nombre de colonnes non nuls de H, $\mathbf{u}_j$ la j-ième colonne de U et $\boldsymbol{\mu}_i$ la i-ème ligne de U^{-1}.

4 Renvoyer r, $\Lambda^{\text{sat}} = \langle \boldsymbol{\mu}_{n-r+1}, \cdots, \boldsymbol{\mu}_n \rangle$, $\Lambda^{\perp} = \langle \mathbf{u}_1, \cdots, \mathbf{u}_{n-r} \rangle$ et U^{-1}.

Proposition A.1.2. *Soit $\Lambda = \langle \boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_m \rangle$ un sous-groupe de $\mathbb{Z}^n$. Alors l'algorithme 15 renvoie respectivement le rang de Λ, une base de son saturé, une base de son orthogonal et un complété de Λ^{sat} en une base de $\mathbb{Z}^n$.*

Démonstration. D'après l'étape 2, on a $MU = H$ où H est la forme normale d'Hermite de M. Par définition la forme normale d'Hermite, le rang de M est égale au nombre des colonnes non nuls de H. Donc r est bien le rang de Λ. Dans toute la suite, on peut supposer que $m = r$.

On note $\Lambda' = \langle \boldsymbol{\mu}_{n-r+1}, \cdots, \boldsymbol{\mu}_n \rangle$ où $\boldsymbol{\mu}_i$ la i-ème ligne de U^{-1}. Puisque U est unimodulaire, Λ' est saturé de rang r. On note $h_{i,j}$ la i-ème ligne et la j-ème colonne de H. Comme H est triangulaire supérieure

et $M = HU^{-1}$, on a :

$$\begin{cases} \boldsymbol{\lambda}_1 & = h_{1,1}\boldsymbol{\mu}_{n-r+1} + h_{1,2}\boldsymbol{\mu}_{n-r+2} + \cdots + h_{1,n}\boldsymbol{\mu}_n, \\ \boldsymbol{\lambda}_2 & = 0\boldsymbol{\mu}_{n-r+1} + h_{2,2}\boldsymbol{\mu}_{n-r+2} + \cdots + h_{2,n}\boldsymbol{\mu}_n, \\ & \vdots \\ \boldsymbol{\lambda}_{r-1} & = 0\boldsymbol{\mu}_{n-r+1} + \cdots + 0\boldsymbol{\mu}_{n-2} + h_{r-1,n-1}\boldsymbol{\mu}_{n-1} + h_{r-1,n}\boldsymbol{\mu}_n, \\ \boldsymbol{\lambda}_r & = 0\boldsymbol{\mu}_{n-r+1} + \cdots + 0\boldsymbol{\mu}_{n-1} + h_{r,n}\boldsymbol{\mu}_n. \end{cases} \tag{A.1.1}$$

Ainsi, on a $\Lambda \subseteq \Lambda'$. Comme ils ont le même rang et Λ' est saturé, on déduit que $\Lambda' = \Lambda^{\mathrm{sat}}$. Puisque $U \in \mathrm{GL}_n(\mathbb{Z})$, U^{-1} est une base de $\mathbb{Z}^n$.

Par ailleurs, on peut écrire $MU = [\mathbf{0} \mid H']$ où $H' \in M_{n,n-r}(\mathbb{Z})$ telle que $H = [\mathbf{0} \mid H']$. On a donc $\mathbf{u}_1, \cdots, \mathbf{u}_{n-r} \in \Lambda^{\perp}$. D'après la dernière équation de (A.1.1), on a $0 = \boldsymbol{\lambda}_r \mathbf{u}_j = h_{rn}\boldsymbol{\mu}_n \mathbf{u}_j$ pour tout $1 \leqslant j \leqslant n-r$. Comme $h_{r,n} \neq 0$, $\boldsymbol{\mu}_n \mathbf{u}_j = 0$. En remontant dans les équations de (A.1.1), on a $\boldsymbol{\mu}_i \mathbf{u}_j = 0$ pour tout $n-r+1 \leqslant i \leqslant n$ et pour tout $1 \leqslant j \leqslant n-r$. Cela implique $\langle \mathbf{u}_1, \cdots, \mathbf{u}_{n-r} \rangle \subseteq (\Lambda^{\mathrm{sat}})^{\perp} \subseteq \Lambda^{\perp}$. Comme $\langle \mathbf{u}_1, \cdots, \mathbf{u}_{n-r} \rangle$, $(\Lambda^{\mathrm{sat}})^{\perp}$ et $\Lambda^{\perp}$ sont saturés de même rang, on a $\langle \mathbf{u}_1, \cdots, \mathbf{u}_{n-r} \rangle = (\Lambda^{\mathrm{sat}})^{\perp} = \Lambda^{\perp}$. □

A.2 Résultats auxiliaires

On donne ici les preuves de certains résultats mentionnés dans cette thèse.

Lemme A.2.1. *Notons $e = \exp(1)$. Soit f la fonction définie par :*

$$\forall\ x > e,\ f(x) = x\left(\frac{\log\log x}{\log x}\right)^3.$$

Alors :

(i) f est strictement croissante sur $]e, +\infty[$,

(ii) pour tout $x > e$, on a $f(x) < x$,

(iii) pour tout $x > 6$, on a :

$$x \leqslant f\left(3x\left(\frac{\log x}{\log\log x}\right)^3\right). \tag{A.2.1}$$

Si C est une constante positive telle que $C > 6$ et si on note

$$X_{\max}(C) = \sup\{x \in \mathbb{R}_+ \mid e < x, f(x) \leqslant C\}$$

alors on a :

$$C < C\left(\frac{\log C}{\log\log C}\right)^3 \leqslant X_{\max}(C) \leqslant 3C\left(\frac{\log C}{\log\log C}\right)^3.$$

Démonstration. (i) On a $f(x) > 0$ pour tout réel $x > e$. On peut alors définir la fonction $\log(f)$:

$$\forall\ x > e,\ \log(f)(x) = \log(x) - 3\log\log x + 3\log\log\log x.$$

Pour montrer que f est strictement croissante sur $]e,+\infty[$, il suffit alors de montrer que $\log(f)$ est strictement croissante sur $]e,\infty[$. Pour tout $x>e$, on a :

$$\begin{aligned}(\log(f))'(x) &= \frac{1}{x}-\frac{3}{x\log x}+\frac{3}{x\log x\log\log x}\\ &= \frac{\log x\log\log x-3\log\log x+3}{x\log x\log\log x}.\end{aligned}$$

D'une part, on a $x\log x\log\log x>0$ car $x>e$. D'autre part, posons $g(y)=y\log y-3\log y+3$ pour tout $y>1$. Montrons que g est positive sur $]1,+\infty[$. Considérons les trois cas suivants :

1er cas : $1<y\leqslant e$

Cela implique que $0<y\log y$ et $-3\leqslant -3\log y$. Ainsi, on a $g(y)=y\log y-3\log y+3>0$.

2ème cas : $e<y\leqslant 3$

Cela implique que $e<y\log y$ et $-3\log 3\leqslant -3\log y$. Ainsi, on a $g(y)=y\log y-3\log y+3>2$.

3ème cas : $y>3$

Cela implique que $y\log y>3\log y$. Ainsi on a $g(y)=y\log y-3\log y+3>3$.

D'où on a (i) car

$$(\log(f))'(x)=\frac{g(\log x)}{x\log x\log\log x}.$$

En particulier, f^{-1} est aussi strictement croissante sur $]0,+\infty[$.

(ii) Soit $x>e$. On a $\log\log x<\log x$. Par suite, on a $(\log\log x/\log x)^3<1$. Ainsi, il s'ensuit que $f(x)=x(\log\log x/\log x)^3<x$.

(iii) Soit $x>e$. On a :

$$f\left(3x\left(\frac{\log x}{\log\log x}\right)^3\right)=3x\left(\frac{\log x}{\log\log x}\right)^3\frac{\left(\log\log\left(3x(\log x)^3/(\log\log x)^3\right)\right)^3}{\left(\log\left(3x(\log x)^3/(\log\log x)^3\right)\right)^3}.$$

Ainsi pour montrer (A.2.1), il suffit de montrer que :

$$\log\log x\times\log\left(3x(\log x)^3/(\log\log x)^3\right)\leqslant 3^{1/3}\log x\times\log\log\left(3x(\log x)^3/(\log\log x)^3\right).$$

En posant $A(x)=\log x+3\log\log x-3\log\log\log x+\log 3$, cette dernière inégalité est équivalente à :

$$\log\log x\times A(x)\leqslant 3^{1/3}\log x\times\log A(x). \tag{A.2.2}$$

Supposons d'abord $x>e^{e^e}$. Comme $\log\log x\geqslant\log\log\log x$, on a $\log x\leqslant A(x)$. Pour montrer (A.2.2), il suffit de montrer que :

$$\log\log x\times A(x)\leqslant 3^{1/3}\log x\times\log\log x \text{ i.e. } A(x)\leqslant 3^{1/3}\log x.$$

Considérons la fonction g définie par : $\forall\, y>e^e,\ h(y)=(3^{1/3}-1)y-3\log y+3\log\log y-\log 3$. On a $h(\log x)=3^{1/3}\log x-A(x)$. Montrons d'abord que h est positive sur $[e^e,+\infty[$. Pour tout $y>e^e$, on a :

$$h'(y)=3^{1/3}-1-\frac{3}{y}+\frac{3}{y\log y}=\frac{(3^{1/3}-1)y\log y-3\log y+3}{y\log y}.$$

Pour tout $y > e^e$, on a $y > 3/(3^{1/3}-1)$ et donc $(3^{1/3}-1)y\log y - 3\log y + 3 \geqslant 3$. Par suite, $h'(y) \geqslant 0$ pour tout $y \geqslant e^e$. Ainsi h est croissante sur $[e^e, +\infty[$. Comme $g(e^e) > 0$, h est positive sur $[e^e, +\infty[$. Comme $x > e^{e^e}$, on en déduit que $h(\log x) \geqslant 0$ i.e. $A(x) \leqslant 3^{1/3}\log x$. Cela prouve (A.2.1) pour $x > e^{e^e}$.

Pour $e \leqslant x \leqslant e^{e^e} < 3814280$, on vérifie (A.2.2) par une étude de fonction définie.

Pour la dernière assertion, il faut montrer que, pour tout entier $C \geqslant 6$:

$$C < C\left(\frac{\log C}{\log\log C}\right)^3 \leqslant X_{\max}(C) \leqslant 3C\left(\frac{\log C}{\log\log C}\right)^3, \tag{A.2.3}$$

La première inégalité est claire car $\log\log C \leqslant \log C$ pour tout $C \geqslant 6$. Pour la troisième inégalité, il suffit de montrer que :

$$f(M_C) \geqslant C \quad \text{où} \quad M_C = 3C\left(\frac{\log C}{\log\log C}\right)^3.$$

D'après (A.2.1), on a :

$$C \leqslant f\left(3C\left(\frac{\log C}{\log\log C}\right)^3\right) = f(M_C).$$

Pour la deuxième inégalité, il suffit de montrer que :

$$f(m_C) \leqslant C \quad \text{où} \quad m_C = C(\log C/\log\log C)^3.$$

La fonction $y \mapsto s(y) = y/\log y$ est strictement positive sur $[e, +\infty[$. Ainsi, $x \mapsto s(\log x) = \log x/\log\log x$ est aussi strictement croissante sur $[e^e, +\infty[$. Comme $6 \leqslant C \leqslant m_C$, on a $s(\log C) \leqslant s(\log m_C)$. On a ainsi :

$$\frac{\log C}{\log\log C} \leqslant \frac{\log m_C}{\log\log m_C}.$$

Cela implique que :

$$\left(\frac{\log C}{\log\log C}\right)^3 \left(\frac{\log\log m_C}{\log m_C}\right)^3 \leqslant 1,$$

et donc

$$C\left(\frac{\log C}{\log\log C}\right)^3 \left(\frac{\log\log m_C}{\log m_C}\right)^3 \leqslant C.$$

Par suite, on a

$$m_C\left(\frac{\log\log m_C}{\log m_C}\right)^3 \leqslant C \text{ i.e. } f(m_C) \leqslant C.$$

D'où on a la deuxième inégalité de (A.2.3) et cela complète la preuve du lemme. □

Lemme A.2.2. *Soit τ la fonctions définie par $\tau(x) = 4(\log(x)/\log\log(x))^3$ pour tout $x \geqslant 3$. Soit C un réel tel que $C \geqslant 2$. Si $x > e$ et $x \leqslant C\tau(x)$ alors on a $x \leqslant 3C\tau(4C)$.*

Démonstration. Pour $x > e$, on a :

$$x\left(\frac{\log\log x}{\log x}\right)^3 \leqslant 4C.$$

Comme $C \geqslant 2$, on a $3C \geqslant 6$. D'après le Lemme A.2.1, on en déduit que :

$$x \leqslant 12C\left(\frac{\log 4C}{\log\log 4C}\right)^3 \quad \text{i.e.} \quad x \leqslant 3C\tau(4C).$$

□

Lemme A.2.3. *Soit c une constante positive. Soit λ la fonction définie par : $\forall x \geqslant 1$,*

$$\lambda(x) = \frac{2^c \log(2x)^4}{\log\log(5x)^3}$$

Alors λ est croissante.

Démonstration. On a :

$$\lambda'(x) = 2^c \frac{4\log\left(\log\left(5x\right)\right)\ \left(\log\left(2x\right)\right)^3 \log\left(5x\right) - 5\left(\log\left(2x\right)\right)^4}{x\left(\log\left(\log\left(5x\right)\right)\right)^6 \log\left(5x\right)}.$$

Ainsi, si $x \geqslant 1$ alors on a $\lambda'(x) \geqslant 0$. □

Lemme A.2.4. *Soit f la fonction définie par :*

$$\forall\ x > 1,\ \ f(x) = x\frac{\log\log(5x)^3}{\log(2x)^4}.$$

Alors f est strictement croissante sur $\mathbb{R}_{>e^4}$ et pour tout réel $x > 44$, on a :

$$x \leqslant f\left(13x\frac{\log(2x)^4}{\log\log(5x)^3}\right).$$

En particulier, si C est une constante positive telle que $C > 44$ et si on note :

$$X_{\max}(C) = \sup\left\{x \in \mathbb{R}_+\ ,\ x > e^4, f(x) \leqslant C\right\},$$

alors on a :

$$X_{\max}(C) \leqslant 13C\frac{\log(2C)^4}{\log\log(5C)^3}.$$

Démonstration. Comme $f(x) > 0$ pour $x > 1$, on peut définir la fonction $\log(f)$:

$$\forall\ x > 0,\ \log(f)(x) = \log x - 4\log\log x.$$

Pour montrer que f est strictement croissante sur $]e^4, +\infty[$, il suffit alors de montrer que $\log(f)$ est strictement croissante sur $]e^4, \infty[$. Soit g la fonction définie par $\forall y > 0,\ g(y) = y - 4\log y$. Cette fonction g est strictement croissante sur $]4, +\infty[$. Comme la fonction $\log$ est croissante sur $\mathbb{R}_+$ et $\log(f)(x) = g(\log(x))$, alors $\log(f)$ est croissante sur $]e^4, +\infty[$.

En faisant une étude de fonctions, on montre que pour tout $x > e^4$:

$$x \leqslant f\left(13x\frac{\log(2x)^4}{\log\log(5x)^3}\right). \tag{A.2.4}$$

On note :

$$M_C = 13C\frac{\log(2C)^4}{\log\log(5C)^3}.$$

Puisque f est croissante sur $\mathbb{R}_{>e^4}$ et $M_C \geqslant e^4$, pour montrer la dernière assertion, il suffit de montrer que $C \leqslant f(M_C)$. En prenant $x = C$ dans (A.2.4), on a une telle inégalité. □

Bibliographie

[1] Francesco Amoroso and Sinnou David, *Le probleme de Lehmer en dimension supérieure*, (1999).

[2] _____, *Minoration de la hauteur normalisée dans un tore*, Journal of the Institute of Mathematics of Jussieu **2** (2003), no. 3, 335–381.

[3] Francesco Amoroso and Emmanuel Delsinne, *Une minoration relative explicite pour la hauteur dans une extension d'une extension abélienne*, Diophantine geometry **4** (2007), 1–24.

[4] Francesco Amoroso, Louis Leroux, and Martin Sombra, *Overdetermined systems of sparse polynomial equations*, Foundations of Computational Mathematics **15** (2015), no. 1, 53–87.

[5] Francesco Amoroso and Umberto Zannier, *A relative Dobrowolski lower bound over abelian extensions*, Annali della Scuola Normale Superiore di Pisa-Classe di Scienze **29** (2000), no. 3, 711–727.

[6] Eric Bach, James Driscoll, and Jeffrey Shallit, *Factor Refinement*, Journal of Algorithms **15** (1993), no. 2, 199–222.

[7] David N Bernshtein, *The number of roots of a system of equations*, Functional Analysis and its applications **9** (1975), no. 3, 183–185.

[8] Daniel J Bernstein, *Factoring into coprimes in essentially linear time*, Journal of Algorithms **54** (2005), no. 1, 1–30.

[9] Daniel Bertrand and Patrice Philippon, *Sous-groupes algébriques de groupes algébriques commutatifs*, Illinois journal of mathematics **32** (1988), no. 2, 263–280.

[10] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, vol. 4, Cambridge university press, 2007.

[11] Enrico Bombieri, David Masser, and Umberto Zannier, *Anomalous subvarieties-structure theorems and applications*, International Mathematics Research Notices (2007).

[12] David W Boyd, *Reciprocal polynomials having small measure. II*, Mathematics of Computation **53** (1989), no. 187, 355–357.

[13] _____, *Uniform approximation to Mahler's measure in several variables*, Canadian Mathematical Bulletin **41** (1998), no. 1, 125–128.

[14] William S Brown, *On Euclid's algorithm and the computation of polynomial greatest common divisors*, Journal of the ACM (JACM) **18** (1971), no. 4, 478–504.

[15] Sara Checcoli, Francesco Veneziano, and Evelina Viada, *On torsion anomalous intersections*, Accounts Lincei-Mathematics and Applications **25** (2014), no. 1, 1–36.

[16] Henri Cohen, *A course in computational algebraic number theory*, vol. 8, Springer-Verlag Berlin, 1993.

[17] David Cox, John Little, and Donal OShea, *Ideals, varieties, and algorithms : an introduction to computational algebraic geometry and commutative algebra*, Springer Science & Business Media, 2013.

[18] VI Danilov, *Algebraic Varieties and Schemes, Encyclopedia of Mathematical Sciences, vol. 23*, 1994.

[19] Sinnou David and Patrice Philippon, *Minorations des hauteurs normalisées des sous-variétés des tores*, Annali della Scuola Normale Superiore di Pisa-Classe di Scienze **28** (1999), no. 3, 489–543.

[20] Emmanuel Delsinne, *Le probleme de Lehmer relatif en dimension supérieure*, Annales scientifiques de l'École normale supérieure, vol. 42, 2009, pp. 981–1028.

[21] Edward Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arithmetica **34** (1979), no. 4, 391–401.

[22] Harold Gordon Eggleston, *Convexity*, 1966.

[23] Michael Filaseta, Andrew Granville, and Andrzej Schinzel, *Irreducibility and greatest common divisor algorithms for sparse polynomials*, London Mathematical Society Lecture Note Series **352** (2008), 155.

[24] William Fulton, *Intersection theory*, vol. 2, Springer Science & Business Media, 2013.

[25] Philipp Habegger, *Intersecting subvarieties of $\mathbf{G}_m^n$ with algebraic subgroups*, Mathematische Annalen **342** (2008), no. 2, 449–466.

[26] Leopold Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, (1857).

[27] Serge Lang, *Algebra*, vol. 211, Springer Science & Business Media, 2012.

[28] Pierre Lelong, *Mesure de Mahler des polynômes et majoration par convexité*, Comptes rendus de l'Académie des sciences. Série 1, Mathématique **315** (1992), no. 2, 139–142.

[29] Louis Leroux, *Algorithmes pour les polynômes lacunaires*, Theses, Université de Caen, March 2011.

[30] ———, *Computing the torsion points of a variety defined by lacunary polynomials*, Mathematics of Computation **81** (2012), no. 279, 1587–1607.

[31] Kurt Mahler, *On some inequalities for polynomials in several variables*, J. London Math. Soc **37** (1962), no. 1, 341–344.

[32] César Martinez Metzmeier, *Two problems in arithmetic geometry. Explicit Manin-Mumford, and arithmetic Bernstein-Kusnirenko*, Ph.D. thesis, Normandie, 2017.

[33] Niels Möller, *On Schönhage's algorithm and subquadratic integer gcd computation*, Mathematics of Computation **77** (2008), no. 261, 589–607.

[34] Michael J Mossinghoff, Georges Rhin, and Qiang Wu, *Minimal Mahler measures*, Experimental Mathematics **17** (2008), no. 4, 451–458.

[35] Phong Q Nguyen, *Hermite's constant and lattice algorithms*, The LLL Algorithm, Springer, 2009, pp. 19–69.

[36] Alexander M Ostrowski, *On multiplication and factorization of polynomials, I. Lexicographic orderings and extreme aggregates of terms*, aequationes mathematicae **13** (1975), no. 3, 201–228.

[37] Patrice Philippon, *Sur des hauteurs alternatives III*, Journal de mathématiques pures et appliquées **74** (1995), no. 4, 345–365.

[38] Robert Alexander Rankin, *On positive definite quadratic forms*, Journal of the London Mathematical Society **1** (1953), no. 3, 309–314.

[39] Gaël 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** (2017), 243–284.

[40] Andrzej Schinzel, *Polynomials with special regard to reducibility. With an appendix by Umberto Zannier.*, vol. 77, Cambridge University Press, 2000.

[41] ———, *On the greatest common divisor of two univariate polynomials, I*, A Panorama of number theory or the view from Baker's garden (2003), 337–352.

[42] Wolfgang M Schmidt, *Heights of points on subvarieties of $\mathbf{G}_m^n$*, Number Theory (Paris, 1993–1994). London Mathematical Society Lecture Notes Series **235** (1996), 157–187.

[43] Arnold Schönhage, *Fast reduction and composition of binary quadratic forms*, Proceedings of the 1991 international symposium on Symbolic and algebraic computation, 1991, pp. 128–133.

[44] Carl Ludwig Siegel, *Lectures on the geometry of numbers*, Springer Science & Business Media, 2013.

[45] Paul Voutier, *An effective lower bound for the height of algebraic numbers*, arXiv preprint arXiv :1211.3110 (2012).

[46] Umberto Zannier, *Lecture notes on Diophantine analysis*, vol. 8, Springer, 2015.

[47] Shouwu Zhang, *Positive line bundles on arithmetic surfaces*, Columbia University, 1991.

[48] ———, *Positive line bundles on arithmetic varieties*, Journal of the American Mathematical Society **8** (1995), no. 1, 187–221.

[49] Boris Zilber, *Exponential sums equations and the Schanuel conjecture*, Journal of the London Mathematical Society **65** (2002), no. 1, 27–44.

Titre : Conjecture de Schinzel et algorithmique des polynômes lacunaires

Résumé : En géométrie diophantienne, la théorie des intersections improbables est un domaine en constante évolution. Dans ce contexte, des progrès significatifs ont été réalisés par plusieurs auteurs, dont E. Bombieri, P. Habegger, D. Masser, G. Rémond et U. Zannier, en ce qui concerne l'intersection des variétés dans une puissance $\mathbb{G}_{\mathrm{m}}^n$ du tore multiplicatif. Plus particulièrement, ils ont résolu la conjecture de Schinzel qui concerne l'intersection d'une variété de codimension $\geqslant 2$ dans $\mathbb{G}_{\mathrm{m}}^n$ avec un translaté d'un tore de dimension 1 par un point de torsion. Cette conjecture est désormais prouvée avec plusieurs méthodes mais les bornes obtenues dans les preuves ne sont pas explicites, bien qu'elles soient effectives. L'objectif de cette thèse est d'expliciter ces bornes et d'appliquer le résultat obtenu pour rendre effectif un algorithme pour le calcul du plus grand commun diviseur (PGCD) de deux polynômes lacunaires. Premièrement, pour le cas $n = 2$, nous obtenons une version explicite de cette conjecture. Deuxièmement, pour le cas $n = 3$, nous décrivons trois différentes approches dont l'une est inspirée de la preuve de A. Schinzel, une autre inspirée de la preuve E. Bombieri, D. Masser et U. Zannier et la dernière basée sur une nouvelle approche. Les résultats obtenus sont également explicites. Troisièmement, pour n quelconque, nous avons généralisé la nouvelle approche du cas $n = 3$ et nous obtenons une borne explicite en fonction du degré et de la hauteur de la variété, mais sans la dépendance explicite en n. Ces différentes approches reposent sur l'utilisation d'une majoration de type Bézout arithmétique et d'un théorème de Dobrowolski sur la conjecture de Lehmer. Les résultats obtenus ont permis d'obtenir un algorithme qui permet de calculer la partie non-cyclotomique du PGCD de deux polynômes à une variable, qui sont des spécialisations de deux polynômes à deux ou trois variables. Nous donnons une analyse de la complexité de cet algorithme et nous avons également réalisé des implémentations relatives aux polynômes multivariés et aux sous-variétés de $\mathbb{G}_{\mathrm{m}}^n$ dans le langage de calcul formel Pari/GP.

Mots-clés : géométrie diophantienne · borne explicite · polynôme lacunaire · PGCD · algorithmes.

Title : Schinzel's Conjecture and algorithms for sparse polynomials

Abstract : In diophantine geometry, the theory of unlikely intersections is a constantly evolving field. In this context, significant progress has been made by several authors, including E. Bombieri, P. Habegger, D. Masser, G. Rémond, and U. Zannier, on the intersection of varieties in the torus $\mathbb{G}_{\mathrm{m}}^n$. More specifically, they have solved Schinzel's conjecture on the intersection of a variety of codimension $\geqslant 2$ in $\mathbb{G}_{\mathrm{m}}^n$ with a translate a torus of dimension 1 by a torsion point. This conjecture has now been proven using various methods, but the bounds obtained in the proofs are not explicit, although they are effective. This thesis aims to make these bounds explicit and to apply the obtained result to develop an algorithm for computing the greatest common divisor (GCD) of two sparse polynomials. Firstly, we obtain an explicit version of this conjecture for the case $n = 2$. Secondly, for the case $n = 3$, we describe three different approaches, one inspired by A. Schinzel's proof, another inspired by the proof of E. Bombieri, D. Masser, and U. Zannier, and the last one based on a new approach. The obtained results are all explicit. Thirdly, for arbitrary n, we generalize the new approach from the case $n = 3$ and obtain an explicit bound in terms of the degree and height of the variety, but without explicit dependence on n. These different approaches rely on an arithmetic Bézout type bound and on Dobrowolski's theorem. The obtained results lead to an algorithm for computing the non-cyclotomic part of the GCD of two univariate polynomials, which are specializations of two polynomials in two or three variables. We give the complexity of this algorithm and implement some algorithms related to multivariate polynomials and subvarieties of $\mathbb{G}_{\mathrm{m}}^n$ in the computer algebra system Pari/GP.

Keywords : diophantine geometry · explicit bound · sparse polynomials · GCD · algorithms.