APPROXIMATION DIOPHANTIENNE ET INDÉPENDANCE ALGÉBRIQUE DE LOGARITHMES

par Damien ROY * et Michel WALDSCHMIDT

0. Introduction

Ce travail propose une nouvelle approche à l'indépendance algébrique pour les petits degrés de transcendance. Au lieu du critère de Gel'fond usuel, on emploie un nouveau résultat d'approximation diophantienne qui complète des résultats antérieurs de E. Wirsing [34] et de A. Durand [7]. Ce résultat assure l'existence de bonnes approximations algébriques à des familles de nombres dans un sous-corps de $\mathbf{C}$ de degré de transcendance 1 sur $\mathbf{Q}$. A l'aide de cet outil, nous donnons ici, à la suite de notre note [22], des démonstrations d'indépendance algébrique basées, en dernière analyse, sur la technique des déterminants d'interpolation de M. Laurent [13]. Ce sujet connaît une certaine effervescence présentement et des points de vue complémentaires à celui que nous présentons ici viennent d'être proposés par M. Laurent et D. Roy dans [14] et par P. Philippon dans [17]. Le résultat principal que nous démontrons par notre méthode est lui-aussi nouveau et nous examinons ses conséquences. Nous poursuivons cette étude dans [23].

Soit $\theta \in \mathbf{C}$ un nombre transcendant sur $\mathbf{Q}$. Il découle d'un résultat de E. Wirsing que, pour tout entier $D \geq 2$, il existe une infinité de nombres algébriques α de degré $\leq D$ qui vérifient

$$|\theta - \alpha| \leq M(\alpha)^{-D/4}$$

où $M(\alpha)$ désigne la mesure de Mahler de α (voir l'inégalité (4') de [34]). Dans [22], nous avons montré comment cet énoncé permet d'utiliser les déterminants d'interpolation pour retrouver un résultat connu d'indépendance algébrique. Dans la situation plus générale que nous considérons ici, cet énoncé ne suffit plus. Au lieu de borner le degré des approximations de θ, on a plutôt besoin de borner leur hauteur logarithmique absolue $h_1(\alpha) = \deg(\alpha)^{-1} \log M(\alpha)$. Ainsi, pour tout nombre réel $\kappa \geq 10^7$, nous montrons qu'il existe une infinité de nombres algébriques α de hauteur $h_1(\alpha) \leq \kappa$ qui vérifient

$$|\theta - \alpha| \leq \exp(-10^{-7}\kappa \deg(\alpha)^2).$$

Le théorème d'approximation établi au §3 généralise cet énoncé à l'approximation simultanée de plusieurs nombres dans un corps K algébrique sur $\mathbf{Q}(\theta)$.

On applique ce résultat de la manière suivante. On suppose un groupe algébrique commutatif linéaire $G \subseteq \mathbf{A}^d$ défini sur K. On note T_G l'espace tangent en son élément neutre. On se donne aussi un sous-espace

* Travail partiellement supporté par le CRSNG.

W de $T_G(K)$ et un sous-groupe de type fini Y de $T_G(\mathbf{C})$ dont l'image Γ sous l'exponentielle de $G(\mathbf{C})$ est contenue dans $G(K)$. Enfin, on désigne par n la dimension sur $\mathbf{C}$ du sous-espace de $T_G(\mathbf{C})$ engendré par W et Y. On suppose que n est petit et on cherche quelles contraintes cela impose à W et Γ. Pour cela, on choisit des générateurs de W et de Γ, et on construit, grâce au théorème d'approximation du §3, un corps de nombres $\tilde{K}$, un sous-espace $\tilde{W}$ de $T_G(\tilde{K})$ engendré par de bonnes approximations des générateurs de W, et un sous-groupe $\tilde{\Gamma}$ de $G(\tilde{K})$ engendré par de bonnes approximations des générateurs de Γ. Cela nous place tout juste dans les conditions d'application d'un résultat général d'approximation diophantienne dans les groupes algébriques commutatifs dû à M. Waldschmidt [33]. Le cas particulier que nous utilisons est énoncé au §2. On en déduit au §5 des contraintes sur $\tilde{W}$ et $\tilde{\Gamma}$ qu'on relève ensuite à W et Γ. Les principes généraux qui permettent ce relèvement sont exposés au §4. Au §6, on transforme ce résultat en termes de W et de Y grâce à un résultat général de D. Roy [19] formulé en termes de catégories. On obtient ainsi un énoncé plus maniable du point de vue des applications. Cet énoncé est présenté au §1 et quelques applications en sont données au §1 et au §7.

On convient des notations suivantes. Pour tout corps $K \subseteq \mathbf{C}$, on désigne par $\mathcal{L}_K$ le groupe additif des logarithmes des éléments non nuls de K

$$\mathcal{L}_K = \{z \in \mathbf{C}\,;\, e^z \in K\}.$$

On écrit aussi $\mathcal{L}$ pour désigner le $\mathbf{Q}$-espace vectoriel $\mathcal{L}_{\overline{\mathbf{Q}}}$ des logarithmes de nombres algébriques. Pour toute paire d'entiers positifs d et ℓ, on note $\mathrm{Mat}_{d\times\ell}(\mathbf{C})$ l'espace vectoriel des matrices $d \times \ell$ à coefficients dans $\mathbf{C}$. La première application que nous donnons de notre résultat du §1 est la suivante:

Théorème 0.1. *Soit K un sous-corps de $\mathbf{C}$ de degré de transcendance 1 sur $\mathbf{Q}$, soit M une matrice $d \times \ell$ à coefficients dans $\mathcal{L}_K \cap K$ et soit n le rang de M. Alors il existe un sous-espace vectoriel T de $\mathrm{Mat}_{d\times\ell}(\mathbf{C})$, défini sur $\mathbf{Q}$, qui contient M, et qui consiste de matrices de rang $\leq 2n$. De plus, si M possède au moins une colonne non nulle dont tous les coefficients appartiennent à $\mathcal{L}$, alors on peut préciser que T consiste de matrices de rang $< 2n$.*

Pour $d = \ell = 2$, ce résultat est démontré sous une forme équivalente par W. D. Brownawell dans [4] et par M. Waldschmidt dans [28], et conduit ces deux auteurs à la solution d'une conjecture de Schneider. Au §7, nous déduisons du théorème 0.1 l'énoncé suivant.

Théorème 0.2. *Soit $V \subseteq \mathbf{C}^n$ le lieu des zéros dans $\mathbf{C}^n$ d'un polynôme $P \in \mathbf{Q}[X_1, \dots, X_n]$ homogène de degré ≤ 2 et soit $(\lambda_1, \dots, \lambda_n)$ un point de V à coordonnées dans $\mathcal{L}$. Alors, ou bien $(\lambda_1, \dots, \lambda_n)$ est contenu dans un sous-espace vectoriel de $\mathbf{C}^n$ défini sur $\mathbf{Q}$ et contenu dans V, ou bien le corps $\mathbf{Q}(\lambda_1, \dots, \lambda_n)$ est de degré de transcendance ≥ 2 sur $\mathbf{Q}$.*

L'intérêt de ce dernier résultat est lié au fait que la conjecture d'indépendance des logarithmes est équivalente à l'énoncé suivant (voir [21]):

Conjecture 0.3. *Soit V un sous-ensemble algébrique fermé de $\mathbf{C}^n$, défini sur $\overline{\mathbf{Q}}$. Alors l'ensemble $V \cap \mathcal{L}^n$ des points de V à coordonnées dans $\mathcal{L}$ est contenu dans la réunion de tous les sous-espaces vectoriels de $\mathbf{C}^n$, rationnels sur $\mathbf{Q}$, contenus dans V.*

Le théorème 0.2 signifie donc qu'au moins un des deux énoncés suivants est vrai:

(i) le corps $\mathbf{Q}(\mathcal{L})$ est de degré de transcendance > 1 sur $\mathbf{Q}$;

(ii) la conjecture 0.3 est vérifiée pour toutes les hypersurfaces de $\mathbf{C}^n$ définies par un polynôme homogène de degré 2 à coefficients dans $\mathbf{Q}$.

On s'attend en fait à ce que ces deux assertions soient vraies.

Le théorème 0.2 implique aussi que la conjecture 0.3 est vraie pour toute courbe algébrique irréductible $V \subset \mathbf{C}^n$ définie sur $\mathbf{Q}$ de degré d, pourvu qu'on ait $n(n+1) > 4d+2$ et que la courbe V ne soit pas contenue dans un sous-espace de $\mathbf{C}^n$ distinct de $\mathbf{C}^n$ et défini sur $\mathbf{Q}$.

1. Le résultat principal

Notre résultat principal est le suivant:

Théorème 1.1. *Soient d_0 et d_1 des entiers ≥ 0 de somme $d > 0$, soit $K \subset \mathbf{C}$ un corps de degré de transcendance ≤ 1 sur $\mathbf{Q}$, soit W un sous-K-espace vectoriel de K^d, soit Y un sous-groupe de $K^{d_0} \times (\mathcal{L}_K)^{d_1}$ de type fini, et soit Y_a un sous-groupe de Y contenu dans $K^{d_0} \times \mathcal{L}^{d_1}$. On désigne par n la dimension du sous-espace de $\mathbf{C}^d$ engendré par W et Y, et on suppose $d > 2n$. On suppose aussi que $\mathbf{C}^d$ est le seul sous-espace de $\mathbf{C}^d$ qui contienne à la fois W et Y et qui soit de la forme $T_0 \times T_1$ où T_0 est un sous-espace de $\mathbf{C}^{d_0}$ défini sur K et T_1 un sous-espace de $\mathbf{C}^{d_1}$ défini sur $\mathbf{Q}$. Alors, il existe des entiers d_0' et d_1', tous deux ≥ 0 mais non tous deux nuls, et une application linéaire surjective*

$$g\colon \mathbf{C}^{d_0} \times \mathbf{C}^{d_1} \longrightarrow \mathbf{C}^{d_0'} \times \mathbf{C}^{d_1'}$$

qui vérifie

$$g(K^{d_0} \times 0) = K^{d_0'} \times 0 \quad \textit{et} \quad g(0 \times \mathbf{Q}^{d_1}) = 0 \times \mathbf{Q}^{d_1'},$$

tels qu'en posant

$$W' = g(W), \quad Y' = g(Y), \quad Y_a' = g(Y_a),$$

$$d' = d_0' + d_1', \quad \ell_0' = \dim_K(W'), \quad \ell_1' = \mathrm{rang}_{\mathbf{Z}}(Y'), \quad \ell_a' = \mathrm{rang}_{\mathbf{Z}}(Y_a')$$

et en désignant par n' la dimension du sous-espace de $\mathbf{C}^{d'}$ engendré par W' et Y', on ait $d' > 2n' > \ell_0'$ et

$$\frac{d_1}{d-2n} \geq \frac{d_1'}{d'-2n'} \geq \frac{\ell_1'}{2n'-\ell_0'}$$

avec en plus l'inégalité stricte

$$\frac{d_1'}{d'-2n'} > \frac{\ell_1'}{2n'-\ell_0'}$$

si $d_0' < n'$, ou $\ell_0' < n'$, ou $\ell_a' > 0$.

Ce résultat généralise plusieurs résultats antérieurs concernant l'indépendance algébrique des valeurs de la fonction exponentielle usuelle. Ainsi, le corollaire 8.2 de [30] correspond au cas particulier où l'on prend $d_0 = 0$ et $W = 0$. De même, le cas où $n = 1$ contient la plupart des énoncés d'indépendance algébrique que donne la méthode de Gel'fond en une variable (à l'exception cependant du théorème de Lindemann-Weierstrass et des résultats de G. V. Chudnovsky démontrés au chapitre 2 de [6]). Nous le ferons voir par le corollaire 1.2 ci-dessous.

Dans l'énoncé du théorème 1.1, nous avons admis que le corps K puisse être algébrique sur $\mathbf{Q}$. Signalons que, dans ce cas particulier, *le théorème du sous-groupe algébrique* (théorème 4.1 de [31]) et ses avatars (théorèmes 6.1 à 6.8 de [19]) fournissent un résultat plus précis.

La démonstration du théorème 1.1 fait intervenir plusieurs outils que nous décrirons dans les paragraphes ultérieurs. Dans le reste de ce paragraphe, nous en tirons simplement quelques corollaires et montrons comment le théorème 1 de l'introduction s'en déduit. On a déjà fait allusion au premier corollaire:

Corollaire 1.2. *Soient d_1 et ℓ_1 des entiers positifs, et soient $\{x_1, \ldots, x_{d_1}\}$ et $\{y_1, \ldots, y_{\ell_1}\}$ des familles de nombres complexes linéairement indépendants sur $\mathbf{Q}$. On désigne par K_1 le corps obtenu en adjoignant à $\mathbf{Q}$ les $d_1\ell_1$ nombres $\exp(x_i y_j)$ $(1 \leq i \leq d_1,\ 1 \leq j \leq \ell_1)$, et on pose*

$$K_2 = K_1(x_1, \ldots, x_{d_1}), \qquad K_3 = K_2(y_1, \ldots, y_{\ell_1}).$$

On définit ensuite

$$\kappa_1 = d_1\ell_1, \quad \kappa_2 = \kappa_1 + d_1, \quad \kappa_3 = \kappa_2 + \ell_1.$$

Ainsi, pour $t = 1, 2, 3$, le corps K_t est obtenu en adjoignant κ_t éléments à $\mathbf{Q}$. Alors on peut affirmer que le degré de transcendance de K_t sur $\mathbf{Q}$ est ≥ 2 dans les cas suivants:
(a) $t = 1, 2$ et $\kappa_t \geq 2(d_1 + \ell_1)$;
(b) $t = 3$ et $\kappa_3 > 2(d_1 + \ell_1)$;
(c) $t = 3$, $\kappa_3 = 2(d_1 + \ell_1)$ et $x_i y_1 \in \mathcal{L}$ pour $i = 1, \dots, d_1$.

Remarque. Ce résultat est démontré sous cette forme au chapitre 7 de [29], et sous forme partielle au chapitre 12 de [2]. Comme il est expliqué dans ces deux volumes, le cas particulier où $t = 2$ implique le théorème de Gel'fond concernant l'indépendance algébrique de α^β et α^{β^2} lorsque $\alpha, \beta \in \overline{\mathbf{Q}}$ vérifient $\alpha \neq 0, 1$ et $[\mathbf{Q}(\beta) : \mathbf{Q}] = 3$ (voir §4 du chapitre 3 de [9]). Les cas (a), $t = 2$ et (b) sont dus à R. Tijdeman [27], qui parvint à éliminer des hypothèses superflues dans les énoncés antérieurs de A.O. Gel'fond et A.A. Smelev, tandis que les cas (a), $t = 1$ et (c) sont dus à W. D. Brownawell et à M. Waldschmidt. Le cas (c) (voir [4] et [28]) fournit une réponse positive au huitième problème posé par Th. Schneider dans [25]: au moins un des deux nombres e^e, e^{e^2} est transcendant. Notons enfin que, sous les hypothèses du corollaire, on peut aussi affirmer que K est de degré de transcendance ≥ 1 sur $\mathbf{Q}$ si $\kappa_t > d_1 + \ell_1$, et cela regroupe plusieurs résultats de transcendance bien connus concernant la fonction exponentielle usuelle (théorèmes de Hermite-Lindemann, Gel'fond-Schneider et des six exponentielles).

Démonstration. Explicitons d'abord la conclusion du théorème 1.1 lorsque, dans les hypothèses de ce théorème, on suppose $n = 1$. On trouve $n' = n = 1$ car $0 < n' \leq n$. Cela signifie que g est injective sur W et sur Y. Donc, si on pose $\ell_0 = \dim_K(W)$, $\ell_1 = \mathrm{rang}_{\mathbf{Z}}(Y)$ et $\ell_a = \mathrm{rang}_{\mathbf{Z}}(Y_a)$, alors on obtient $\ell_0' = \ell_0$, $\ell_1' = \ell_1$ et $\ell_a' = \ell_a$, et le théorème livre

$$\frac{d_1}{d-2} \geq \frac{\ell_1}{2-\ell_0},$$

avec l'inégalité stricte si $d_0 = 0$ ou $\ell_0 = 0$ ou $\ell_a > 0$.

Plaçons-nous maintenant dans les hypothèses du corollaire et supposons qu'un des corps K_t soit de degré de transcendance ≤ 1 sur $\mathbf{Q}$.

Si $t = 1, 2$, on pose $d_0 = 0$, $K = K_t$ et $w = (x_1, \dots, x_{d_1})$. On définit Y comme le sous-groupe de $(\mathcal{L}_K)^{d_1}$ de rang ℓ_1 engendré par $y_1 w, \dots, y_{\ell_1} w$, et on pose $Y_a = 0$. On pose aussi $W = 0$ si $t = 1$ et $W = Kw$ si $t = 2$. Alors, pourvu que d_1 soit > 2, les hypothèses du théorème 1.1 sont satisfaites; on a $n = 1$, et la conclusion du théorème s'écrit

$$\frac{d_1}{d_1-2} > \frac{\ell_1}{2-\ell_0}.$$

On en tire $\kappa_t = d_1\ell_1 + d_1\ell_0 < 2(d_1 + \ell_1)$. Cette inégalité demeure vérifiée si $d_1 \leq 2$. Le cas (a) est donc exclu.

Si $t = 3$, on pose $d_0 = 1$, $K = K_3$, $w = (1, x_1, \dots, x_{d_1})$, $W = Kw$, et on définit Y comme le sous-groupe de $K \times (\mathcal{L}_K)^{d_1}$ de rang ℓ_1 engendré par $y_1 w, \dots, y_{\ell_1} w$. Alors, si $d_1 > 1$, les hypothèses du théorème 1.1 sont satisfaites; on a $n = 1$, et la conclusion se lit

$$\frac{d_1}{d_1-1} \geq \ell_1,$$

avec l'inégalité stricte si $y_1 w \in K \times \mathcal{L}^{d_1}$. On en tire $\kappa_3 = d_1\ell_1 + d_1 + \ell_1 \leq 2(d_1 + \ell_1)$ avec l'inégalité stricte si $x_i y_1 \in \mathcal{L}$ pour $i = 1, \dots, d_1$. On a encore l'inégalité stricte si $d_1 = 1$. Donc, les cas (b) et (c) sont exclus. Le corollaire est démontré.

Corollaire 1.3. *Soient d_1 un entier positif, $K \subset \mathbf{C}$ un corps de degré de transcendance 1 sur $\mathbf{Q}$ et X un sous-groupe de type fini de $(\mathcal{L}_K \cap K)^{d_1}$. On pose $n = \dim_{\mathbf{C}}(\mathbf{C}X)$, et on suppose $d_1 > n$. On suppose aussi que $\mathbf{C}^{d_1}$ est le seul sous-espace de $\mathbf{C}^{d_1}$ défini sur $\mathbf{Q}$ qui contienne X. Alors, il existe un entier positif d_1' et une application linéaire surjective*

$$g_1 \colon \mathbf{C}^{d_1} \longrightarrow \mathbf{C}^{d_1'}$$

définie sur $\mathbf{Q}$ tels qu'en posant $X' = g_1(X)$, $n' = \dim_{\mathbf{C}}(\mathbf{C}X')$ et $\ell_1' = \mathrm{rang}_{\mathbf{Z}}(X')$ on ait $d_1' > n' > 0$ et

$$\frac{d_1}{d_1 - n} \geq \frac{d_1'}{d_1' - n'} \geq \frac{\ell_1'}{n'}$$

avec en plus l'inégalité stricte $d_1'/(d_1' - n') > \ell_1'/n'$ si $X' \cap \mathcal{L}^{d_1'} \neq 0$.

Démonstration. (a) Supposons d'abord qu'il existe un entier positif d_1' avec $d_1' < d_1$ et une application linéaire surjective $g_1 \colon \mathbf{C}^{d_1} \to \mathbf{C}^{d_1'}$ définie sur $\mathbf{Q}$ tels qu'en posant $X' = g_1(X)$ et $n' = \dim_{\mathbf{C}}(\mathbf{C}X')$, on ait $d_1' > n'$ et

$$\frac{d_1}{d_1 - n} \geq \frac{d_1'}{d_1' - n'}.$$

Alors, X' est un sous-groupe de type fini de $(\mathcal{L}_K \cap K)^{d_1'}$ et $\mathbf{C}^{d_1'}$ est le seul sous-espace de $\mathbf{C}^{d_1'}$ défini sur $\mathbf{Q}$ qui contienne X'. Par récurrence sur d_1, cela permet de supposer que le corollaire s'applique au sous-groupe X'. Il existe donc un entier positif d_1'' et une application linéaire surjective $g_1' \colon \mathbf{C}^{d_1'} \to \mathbf{C}^{d_1''}$ définie sur $\mathbf{Q}$ tels qu'en posant $X'' = g_1'(X')$, $n'' = \dim_{\mathbf{C}}(\mathbf{C}X'')$ et $\ell_1'' = \mathrm{rang}_{\mathbf{Z}}(X'')$ on ait $d_1'' > n'' > 0$ et

$$\frac{d_1'}{d_1' - n'} \geq \frac{d_1''}{d_1'' - n''} \geq \frac{\ell_1''}{n''}$$

avec en plus l'inégalité stricte $d_1''/(d_1'' - n'') > \ell_1''/n''$ si $X'' \cap \mathcal{L}^{d_1''} \neq 0$. On voit alors que le corollaire est vérifié pour X en considérant la composée $g_1' \circ g_1$.

(b) Supposons au contraire qu'il n'existe pas d'entier d_1' et d'application linéaire g_1 comme ci-dessus. On choisit une application linéaire injective $\varphi \colon \mathbf{C}^n \to \mathbf{C}^{d_1}$ définie sur K, d'image $\mathbf{C}X$, et on pose $d_0 = n$, $d = d_0 + d_1$,

$$W = \{(x, \varphi(x))\,;\, x \in K^n\}, \quad Y = \{(x, \varphi(x))\,;\, x \in K^n,\ \varphi(x) \in X\} \quad \text{et} \quad Y_a = 0.$$

Pour ce choix de W, Y et Y_a, les hypothèses du théorème 1.1 sont vérifiées car on a $Y \subset W$, $\dim_{\mathbf{C}}(\mathbf{C}W) = n$ et $d > 2n$. Soient d_0', d_1' et g comme dans la conclusion de ce théorème. Avec les mêmes notations, on a donc $d' > 2n' > 0$ et

$$\frac{d_1}{d - 2n} \geq \frac{d_1'}{d' - 2n'}. \tag{1.2}$$

On va voir que g est bijective. Pour le montrer, on observe d'abord que g est le produit d'une application linéaire $g_0 \colon \mathbf{C}^{d_0} \to \mathbf{C}^{d_0'}$ définie sur K et d'une application linéaire $g_1 \colon \mathbf{C}^{d_1} \to \mathbf{C}^{d_1'}$ définie sur $\mathbf{Q}$. Puisque g_0 est surjective, on a $\ell_0' \geq d_0'$, d'où $n' \geq d_0'$. L'hypothèse $d' > 2n' > 0$ entraîne donc $d_1' > n' > 0$ et on obtient à la fois

$$\frac{d_1}{d - 2n} = \frac{d_1}{d_1 - n} \quad \text{et} \quad \frac{d_1'}{d' - 2n'} \geq \frac{d_1'}{d_1' - n'}. \tag{1.3}$$

Les inégalités (1.2) et (1.3) livrent $d_1/(d_1 - n) \geq d_1'/(d_1' - n')$. En vertu de l'hypothèse sur X, cela implique $d_1' = d_1$ et aussi que l'égalité prévaut dans l'inégalité de droite de (1.3), donc $d_0' = n'$. L'égalité $d_1' = d_1$

signifie que g_1 est bijective. On en déduit $\dim_{\mathbf{C}}(\mathbf{C}Y') \geq \dim_{\mathbf{C}}(\mathbf{C}X)$, donc $n' \geq n$. Comme $n = d_0$ et $n' = d_0'$, cela implique $d_0' = d_0$. Ainsi, g est bien bijective.

Désignons par ℓ_1 le rang commun de X et de Y. Puisque g est bijective, on a $\ell_0' = n' = n$, $\ell_1' = \ell_1$ et la conclusion du théorème se résume à $d_1 > n > 0$ et

$$\frac{d_1}{d_1 - n} \geq \frac{\ell_1}{n}$$

avec l'inégalité stricte si $Y \cap (K^{d_0} \times \mathcal{L}^{d_1}) \neq 0$, c'est-à-dire si $X \cap \mathcal{L}^{d_1} \neq 0$. Ainsi, le corollaire est vérifié dans ce cas en prenant pour g_1 l'application identité de $\mathbf{C}^{d_1}$.

Corollaire 1.4. *Soient d un entier positif, K un sous-corps de $\mathbf{C}$ de degré de transcendance 1 sur $\mathbf{Q}$, et X un sous-groupe de type fini de $(\mathcal{L}_K \cap K)^d$. On pose $n = \dim_{\mathbf{C}}(\mathbf{C}X)$. Alors, il existe un sous-espace U de $\mathbf{C}^d$ défini sur $\mathbf{Q}$ tel que*

$$\mathrm{rang}_{\mathbf{Z}}(X/(X \cap U)) + \dim_{\mathbf{C}}(U) \leq 2n$$

avec l'inégalité stricte si $X \cap \mathcal{L}^d \neq 0$.

Démonstration. On procède par récurrence sur d. Soit $\ell = \mathrm{rang}_{\mathbf{Z}}(X)$. Si $d < 2n$, on prend $U = \mathbf{C}^d$. Si $n = 0$, on prend $U = 0$. Cela permet de supposer $d \geq 2n$ et $n > 0$. Par récurrence sur d, on peut aussi supposer que $\mathbf{C}^d$ est le seul sous-espace de $\mathbf{C}^d$ défini sur $\mathbf{Q}$ qui contienne X. Dans ce cas, comme on a $d > n > 0$, le corollaire 1.3 montre l'existence d'une application linéaire surjective $g\colon \mathbf{C}^d \to \mathbf{C}^{d'}$ définie sur $\mathbf{Q}$ telle qu'en posant

$$X' = g(X), \quad \ell' = \mathrm{rang}_{\mathbf{Z}}(X') \quad \text{et} \quad n' = \dim_{\mathbf{C}}(\mathbf{C}X'),$$

on ait $n' > 0$ et

$$\frac{d}{d-n} \geq \frac{\ell'}{n'}$$

avec l'inégalité stricte si $X' \cap \mathcal{L}^{d'} \neq 0$. Puisque $d \geq 2n$, on en déduit

$$\ell' \leq 2n'$$

avec l'inégalité stricte si $X' \cap \mathcal{L}^{d'} \neq 0$. Si g est injective, on obtient $\ell \leq 2n$ avec l'inégalité stricte si $X \cap \mathcal{L}^d \neq 0$, et le corollaire est vérifié en prenant $U = 0$. Sinon, on pose

$$X^* = X \cap \ker(g), \quad d^* = \dim_{\mathbf{C}}(\ker(g)) \quad \text{et} \quad n^* = \dim_{\mathbf{C}}(\mathbf{C}X^*),$$

et on identifie $\ker(g)$ à $\mathbf{C}^{d^*}$ via un isomorphisme défini sur $\mathbf{Q}$. Puisque g n'est ni nulle ni injective, on a $d > d^* > 0$. De l'hypothèse de récurrence on déduit qu'il existe un sous-espace U de $\ker(g)$ défini sur $\mathbf{Q}$ tel que

$$\mathrm{rang}_{\mathbf{Z}}(X^*/(X^* \cap U)) + \dim_{\mathbf{C}}(U) \leq 2n^*$$

avec l'inégalité stricte si $X^* \cap \mathcal{L}^d \neq 0$. On en déduit

$$\begin{aligned}
\mathrm{rang}_{\mathbf{Z}}(X/(X \cap U)) &= \mathrm{rang}_{\mathbf{Z}}(X') + \mathrm{rang}_{\mathbf{Z}}(X^*/(X^* \cap U)) \\
&\leq 2n' + 2n^* - \dim_{\mathbf{C}}(U) \\
&\leq 2n - \dim_{\mathbf{C}}(U).
\end{aligned}$$

De plus, si $X \cap \mathcal{L}^d \neq 0$, on a $X' \cap \mathcal{L}^{d'} \neq 0$ ou $X^* \cap \mathcal{L}^d \neq 0$, et alors cette inégalité est stricte.

Démonstration du théorème 0.1

Soit X le sous-groupe de $(\mathcal{L}_K \cap K)^d$ engendré par les ℓ colonnes de M, et soit U un sous-espace de $\mathbf{C}^d$ défini sur $\mathbf{Q}$ qui vérifie la conclusion du corollaire 1.4 pour ce choix de X. On note S le sous-espace de $\mathbf{C}^\ell$ engendré par les points $x \in \mathbf{Z}^\ell$ avec $Mx \in U$, et on note T le sous-espace de $\mathrm{Mat}_{d\times\ell}(\mathbf{C})$ constitué des matrices N telles que $Nx \in U$ pour tout $x \in S$. Par construction, on a $M \in T$ et

$$\mathrm{rang}(N) \le \dim_{\mathbf{C}}(\mathbf{C}^\ell/S) + \dim_{\mathbf{C}}(U)$$

pour tout $N \in T$. Comme $\dim_{\mathbf{C}}(\mathbf{C}^\ell/S) = \mathrm{rang}_{\mathbf{Z}}(X/(X \cap U))$, T possède la propriété requise.

2. Une version effective du théorème du sous-groupe linéaire

Comme on l'a dit dans l'introduction, la démonstration du théorème 1.1 se fonde sur un résultat d'approximation diophantienne dans les groupes algébriques commutatifs (théorème 2.1 de [33]). Nous allons rappeler ici l'énoncé de ce dernier dans le cas des groupes commutatifs linéaires. Auparavant, il convient de fixer quelques notations et de préciser certains concepts.

On fixe tout d'abord un choix d'entiers $d_0, d_1 \ge 0$ de somme $d > 0$, et on désigne par G le groupe $\mathbf{G}_{\mathrm{a}}^{d_0} \times \mathbf{G}_{\mathrm{m}}^{d_1}$ plongé dans l'espace affine $\mathbf{A}^d$ en tant que l'ouvert $\mathbf{A}^{d_0} \times (\mathbf{A} \setminus \{0\})^{d_1}$ avec la loi de groupe donnée par l'addition sur les d_0 premières composantes et par la multiplication sur les d_1 dernières composantes. On identifie à $\mathbf{C}^d$ l'espace tangent de $G(\mathbf{C})$ en son élément neutre, de sorte que l'application exponentielle de $G(\mathbf{C})$, notée $\exp_G\colon \mathbf{C}^d \to G(\mathbf{C})$, soit donnée par

$$\exp_G(x_1, \dots, x_{d_0}, y_1, \dots, y_{d_1}) = (x_1, \dots, x_{d_0}, e^{y_1}, \dots, e^{y_{d_1}}).$$

Pour $1 \le i \le d$, la notation $z^{(i)}$ désignera la i-ème coordonnée d'un élément z de $\mathbf{C}^d$ ou encore de $G(\mathbf{C})$, de sorte que $z = \big(z^{(1)}, \dots, z^{(d)}\big)$. Quand z appartient à $\mathbf{C}^d$, on pose $\|z\| = \max\{|z^{(1)}|, \dots, |z^{(d)}|\}$. On note aussi $\pi_0\colon \mathbf{A}^d \to \mathbf{A}^{d_0}$ la projection sur les d_0 premières composantes et $\pi_1\colon \mathbf{A}^d \to \mathbf{A}^{d_1}$ celle sur les d_1 dernières. On pose enfin $G_i = \pi_i(G)$ pour $i = 0, 1$; ainsi $G_0 = \mathbf{G}_{\mathrm{a}}^{d_0}$ et $G_1 = \mathbf{G}_{\mathrm{a}}^{d_1}$.

On désigne par T_H l'espace tangent à l'élément neutre d'un sous-groupe algébrique H de G. De plus, on dit qu'un sous-ensemble algébrique V de G est *incomplètement défini* dans G par une famille de polynômes $\mathcal{F}$ si V est une réunion de composantes irréductibles de l'ensemble des zéros de $\mathcal{F}$ dans G.

On plonge aussi l'espace affine $\mathbf{A}^d$ dans l'espace multi-projectif $\mathbf{P}^{d_0} \times (\mathbf{P}^1)^{d_1}$ via l'application

$$\mathbf{A}^d \longrightarrow \mathbf{P}^{d_0} \times (\mathbf{P}^1)^{d_1}$$
$$(x_1, \dots, x_d) \mapsto ((1 : x_1 : \cdots : x_{d_0}), (1 : x_{d_0+1}), \dots, (1 : x_d))$$

Étant donné un sous-ensemble algébrique V de G de dimension n, on désigne par $H(V\,; T_0, T_1, \dots, T_{d_1})$ sa fonction d'Hilbert-Samuel associée à ce plongement et par $\mathcal{H}(V\,; T_0, T_1, \dots, T_{d_1})$ le produit par $n!$ de la partie homogène de degré n du polynôme en $T_0, T_1, \dots, T_{d_1}$ qui coïncide avec $H(V\,; T_0, T_1, \dots, T_{d_1})$ pour toutes valeurs entières suffisamment grandes de $T_0, T_1, \dots, T_{d_1}$.

On utilise aussi la notion de hauteur logarithmique absolue de Weil sur $\mathbf{P}^n(\overline{\mathbf{Q}})$ définie, pour un point $(x_0 : x_1 : \cdots : x_n)$ à coordonnées $x_0, \dots, x_n$ dans un corps de nombres $\tilde{K}$, par

$$h(x_0 : x_1 : \cdots : x_n) = [\tilde{K} : \mathbf{Q}]^{-1} \sum_v [\tilde{K}_v : \mathbf{Q}_v] \log \max\{|x_0|_v, |x_1|_v, \dots, |x_n|_v\}$$

où la somme est étendue aux places v du corps $\tilde{K}$ et où chaque valeur absolue $|\ |_v$ est normalisée de telle sorte qu'elle étende la valeur absolue usuelle de $\mathbf{Q}$ si v est archimédienne et qu'elle vérifie $|p|_v = 1/p$ si v est ultramétrique et si p est le nombre premier qui appartient à son idéal de valuation. En fait, on n'aura besoin que de la version affine de cette hauteur sur $\overline{\mathbf{Q}}^n$ qu'on notera h_1 et qui est donnée par

$$h_1(x_1, \dots, x_n) = h(1 : x_1 : \cdots : x_n)$$

pour tout $(x_1, \dots, x_n) \in \overline{\mathbf{Q}}^n$.

Cela dit, le théorème 2.1 de [33] admet pour cas particulier:

Théorème 2.1. *Soient ℓ_0 et N des entiers ≥ 0. On se donne d'abord des éléments $w_1, \ldots, w_{\ell_0}$, $\eta_1, \ldots, \eta_N$ de $T_G(\mathbf{C})$, un corps de nombres $\tilde{K} \subset \mathbf{C}$, et des éléments $\tilde{w}_1, \ldots, \tilde{w}_{\ell_0}$ de $T_G(\tilde{K})$ et $\tilde{\eta}_1, \ldots, \tilde{\eta}_N$ de $T_G(\mathbf{C})$ tels que les images $\tilde{\gamma}_1, \ldots, \tilde{\gamma}_N$ de $\tilde{\eta}_1, \ldots, \tilde{\eta}_N$ sous $\exp_G$ appartiennent toutes à $G(\tilde{K})$. On note n la dimension du sous-espace de $T_G(\mathbf{C})$ engendré par $w_1, \ldots, w_{\ell_0}$ et $\eta_1, \ldots, \eta_N$, D le degré de $\tilde{K}$ sur $\mathbf{Q}$, et $\tilde{W}$ le sous-espace de $T_G(\tilde{K})$ engendré par $\tilde{w}_1, \ldots, \tilde{w}_{\ell_0}$. On écrit $\tilde{\Sigma} = \{\tilde{\gamma}_1, \ldots, \tilde{\gamma}_N\}$ et on suppose que $\tilde{\Sigma}$ contient l'élément neutre de $G(\tilde{K})$. On suppose aussi que les points $\eta_1, \ldots, \eta_N$ n'appartiennent pas tous à $T_{G_0 \times 1}(\mathbf{C})$. On se donne aussi des nombres réels $A_1, \ldots, A_{d_1}$, B_1, B_2, E tous $\geq e$, des nombres réels positifs U, V, et des entiers positifs S_0, $T_0, T_1, \ldots, T_{d_1}$ qui satisfont $B_1 \geq 2d$, $B_2 \geq d$,*

$$
\begin{aligned}
&h_1(\tilde{\gamma}_1^{(i)}, \ldots, \tilde{\gamma}_N^{(i)}) \leq \log B_1 \quad (1 \leq i \leq d_0),\\
&h_1(\tilde{w}_j^{(1)}, \ldots, \tilde{w}_j^{(d)}) \leq \log B_2 \quad (1 \leq j \leq \ell_0),\\
&\max\Big\{h_1(\tilde{\gamma}_j^{(d_0+i)}),\ \frac{2}{D},\ \frac{E}{D}|\tilde{\eta}_j^{(d_0+i)}|\Big\} \leq \log A_i \quad (1 \leq i \leq d_1,\ 1 \leq j \leq N).
\end{aligned}
$$

On suppose en outre

$$\|w_j - \tilde{w}_j\| \leq e^{-V} \quad (1 \leq j \leq \ell_0) \quad \text{et} \quad \|\eta_j - \tilde{\eta}_j\| \leq e^{-V} \quad (1 \leq j \leq N),$$

où $\|\ \|$ désigne la norme du maximum, et aussi que les différents paramètres remplissent les conditions

$$
\begin{aligned}
&U \geq D \max\{T_0 \log B_1, S_0 \log B_2, \sum_{i=1}^{d_1} T_i \log A_i\}, \qquad V \geq (12d+13)U,\\
&D \log B_1 \geq \log E, \quad D \log B_2 \geq \log E, \quad B_2 \geq dS_0 + T_0 + T_1 + \cdots + T_{d_1},\\
&\text{et} \quad \frac{1}{8}\exp\big(U/(2D)\big) \geq \binom{T_0+d_0}{d_0}(T_1+1)\cdots(T_{d_1}+1) \geq 4\Big(\frac{V}{\log E}\Big)^n.
\end{aligned}
$$

Alors, il existe un sous-groupe algébrique connexe H de G, distinct de G, incomplètement défini dans G par des polynômes de $\tilde{K}[X_1, \ldots, X_{d_0}, Y_1, \ldots, Y_{d_1}]$ de degré $\leq T_i$ en Y_i pour $i = 1, \ldots, d_1$, tel que, si on pose

$$\tilde{\ell}_0 = \dim_{\tilde{K}}\big((\tilde{W} + T_H(\tilde{K}))/T_H(\tilde{K})\big),$$

on ait

$$S_0^{\tilde{\ell}_0}\,\mathrm{Card}\big((\tilde{\Sigma} + H(\tilde{K}))/H(\tilde{K})\big) \cdot \mathcal{H}(H; T_0, T_1, \ldots, T_{d_1}) \leq \frac{d!}{d_0!} T_0^{d_0} T_1 \cdots T_{d_1}.$$

Remarques. Pour déduire cet énoncé du théorème 2.1 de [33], on a utilisé le fait que

$$H(G; T_0, T_1, \ldots, T_{d_1}) = \binom{T_0+d_0}{d_0}(T_1+1)\cdots(T_{d_1}+1),$$

le fait que, dans les notations de [33], l'hypothèse $\{\eta_1, \ldots, \eta_N\} \not\subset T_{G_0 \times 1}(\mathbf{C})$ se traduit par $r_3 \geq 1$, et enfin le fait que, si r_1, r_2 et r_3 sont trois entiers ≥ 0 de somme égale à n, alors on a, en vertu des hypothèses sur les paramètres,

$$
\begin{aligned}
\binom{T_0+r_1}{r_1}\binom{dS_0+r_2}{r_2}\Big(\frac{V}{\log E}\Big)^{r_3} &\leq (2T_0)^{r_1}((d+1)S_0)^{r_2}\Big(\frac{V}{\log E}\Big)^{r_3}\\
&\leq \Big(\frac{2U}{D\log B_1}\Big)^{r_1}\Big(\frac{(d+1)U}{D\log B_2}\Big)^{r_2}\Big(\frac{V}{\log E}\Big)^{r_3}\\
&\leq \Big(\frac{2U}{\log E}\Big)^{r_1}\Big(\frac{(d+1)U}{\log E}\Big)^{r_2}\Big(\frac{V}{\log E}\Big)^{r_3}\\
&\leq \Big(\frac{V}{\log E}\Big)^{n}.
\end{aligned}
$$

Nous avons aussi modifié quelques notations pour les harmoniser au travail présent.

3. Approximations algébriques de nombres transcendants

Pour appliquer le théorème 2.1 aux données du théorème 1.1, on a besoin de bonnes approximations algébriques d'éléments d'un sous-corps de $\mathbf{C}$ de degré de transcendance 1 sur $\mathbf{Q}$. A cet effet, on emploiera le résultat suivant.

Théorème 3.1. *Soit K un sous-corps de $\mathbf{C}$ de type fini et de degré de transcendance 1 sur $\mathbf{Q}$ et soient $a_1, \ldots, a_n$ des éléments de K. Alors, il existe une constante $c > 0$ qui ne dépend que de K et des nombres $a_1, \ldots, a_n$, et qui possède la propriété suivante. Soit κ un nombre réel $\geq c$. Pour une infinité d'entiers D, il existe une place $\mathbf{p}$ de K de degré D et un plongement de son corps résiduel $\tilde{K}$ dans $\mathbf{C}$ tels que les nombres $a_1, \ldots, a_n$ appartiennent à l'anneau de valuation $\mathcal{O}$ de $\mathbf{p}$ et que leurs images $\tilde{a}_1, \ldots, \tilde{a}_n$ sous l'homomorphisme de réduction $\tau\colon \mathcal{O} \to \tilde{K}$ associé à $\mathbf{p}$ vérifient*

$$h_1(\tilde{a}_1, \ldots, \tilde{a}_n) \leq \kappa, \qquad \max_{1 \leq i \leq n} \{|a_i - \tilde{a}_i|\} \leq \exp(-c^{-1}\kappa D^2),$$

et aussi $\tilde{a}_i = a_i$ pour chaque indice i avec $a_i \in \overline{\mathbf{Q}}$.

Le reste du paragraphe est consacré à la démonstration du théorème 3.1.

(i) Réduction au cas d'un seul nombre

On montre d'abord comment le théorème 3.1 se déduit du résultat suivant:

Théorème 3.2. *Il existe une constante absolue $c_0 > 0$ qu'on peut prendre égale à 10^7 et qui possède la propriété suivante. Soit κ un nombre réel $\geq c_0$ et soit $\theta \in \mathbf{C}$ un nombre complexe transcendant sur $\mathbf{Q}$. Alors, pour une infinité d'entiers $d \geq 1$, il existe un nombre algébrique α de degré d et de hauteur $h_1(\alpha) \leq \kappa$ qui vérifie*

$$|\theta - \alpha| \leq \exp(-c_0^{-1}\kappa d^2). \tag{3.1}$$

Dans ce but, on rappelle d'abord le fait suivant:

Lemme 3.3. *Soient n un entier positif et X une sous-variété algébrique fermée de $\mathbf{A}^n$ définie sur $\overline{\mathbf{Q}}$ de dimension 1. Alors, il existe une application linéaire $\pi\colon \mathbf{A}^n \to \mathbf{A}$ définie sur $\mathbf{Q}$ et une constante $c_1 > 0$ telle que*

$$h_1(x) \leq h_1(\pi(x)) + c_1 \quad \textit{pour tout } x \in X(\overline{\mathbf{Q}}). \tag{3.2}$$

Démonstration. Il n'y a pas de restriction à supposer $n \geq 2$. On plonge $\mathbf{A}^n$ dans $\mathbf{P}^n$ sous l'application usuelle qui envoie un point $(x_1, \ldots, x_n)$ de $\mathbf{A}^n$ sur le point $(1 : x_1 : \cdots : x_n)$ de $\mathbf{P}^n$. Soit $\overline{X}$ la fermeture de Zariski de X dans $\mathbf{P}^n$ et soit H l'hyperplan de $\mathbf{P}^n$ d'équation $x_0 = 0$. Puisque $\overline{X}$ est de dimension 1 et que $\overline{X}$ n'est pas contenu dans H, leur intersection $\overline{X} \cap H$ est une réunion finie de points. Il existe donc une sous-variété linéaire Λ de H définie sur $\mathbf{Q}$ et de dimension $n-2$ qui ne rencontre pas $\overline{X}$. Cette variété Λ est déterminée dans H par une équation linéaire de la forme $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$ avec $\lambda_1, \ldots, \lambda_n \in \mathbf{Q}$ non tous nuls. Soit $\pi\colon \mathbf{P}^n - \Lambda \to \mathbf{P}^1$ la projection de centre Λ donnée par

$$\pi(x_0 : x_1 : \cdots : x_n) = (x_0 : \lambda_1 x_1 + \cdots + \lambda_n x_n).$$

D'après la seconde proposition du paragraphe 2.3 de [26], on a $h(x) = h(\pi(x)) + \mathcal{O}(1)$ pour tout $x \in \overline{X}(\overline{\mathbf{Q}})$, où $\mathcal{O}(1)$ désigne une fonction bornée de x. En particulier, il existe une constante $c_1 > 0$ telle que $h(x) \leq$

$h(\pi(x)) + c_1$ pour tout $x \in \overline{X}(\overline{\mathbf{Q}})$. Par restriction, π détermine une application linéaire de $\mathbf{A}^n$ dans $\mathbf{A}$ qui vérifie (3.2).

Démonstration du théorème 3.1.

On peut supposer que les a_i ne sont pas tous algébriques sinon le résultat est immédiat. Soit X la plus petite sous-variété algébrique fermée de $\mathbf{A}^n$ définie sur $\overline{\mathbf{Q}}$ qui contient le point $a = (a_1, \ldots, a_n)$, et soient $\pi\colon \mathbf{A}^n \to \mathbf{A}$ et $c_1 > 0$ comme dans l'énoncé du lemme 3.3. On pose $\theta = \pi(a)$. La relation (3.2) implique que la restriction de π à X est non constante, donc θ est transcendant sur $\mathbf{Q}$. De plus, comme a est un point générique de X sur $\overline{\mathbf{Q}}$, la variété X est non singulière en ce point. Donc, $X(\mathbf{C})$ est, au voisinage de ce point, une sous-variété analytique de $\mathbf{C}^n$ (voir §1B de [16]). Comme θ est transcendant sur $\mathbf{Q}$, la différentielle de π au point a est non nulle. Alors $\pi\colon X(\mathbf{C}) \to \mathbf{C}$ est un isomorphisme local au point a. Il existe donc un voisinage ouvert U de θ dans $\mathbf{C}$ et une fonction holomorphe $\varphi\colon U \to \mathbf{C}^n$ qui applique θ sur a et qui vérifie $\varphi(z) \in X(\mathbf{C})$ et $\pi(\varphi(z)) = z$ pour tout $z \in U$. On en déduit $\varphi(\alpha) \in X(\overline{\mathbf{Q}})$ pour tout $\alpha \in \overline{\mathbf{Q}} \cap U$. Enfin, quitte à remplacer U par un voisinage ouvert de θ plus petit, on peut supposer qu'il existe une constante $c_2 > 0$ telle que

$$\|a - \varphi(z)\| \le c_2|\theta - z| \quad \text{pour tout } z \in U,$$

où la norme dans le membre de gauche est celle du maximum.

On pose $c = \max\{2c_1,\ 1 + 2c_0[K\colon \mathbf{Q}(\theta)]^2\}$ et on choisit un nombre réel $\kappa \ge c$. Le théorème 3.2 montre que, pour une infinité d'entiers $d \ge 1$, il existe un nombre algébrique α de degré d et de hauteur $h_1(\alpha) \le \kappa/2$ qui vérifie

$$|\theta - \alpha| \le \exp(-(2c_0)^{-1}\kappa d^2).$$

Fixons le choix d'un tel entier d et d'un tel nombre α, en prenant d assez grand pour que la condition ci-dessus implique $\alpha \in U$. On pose $A = \mathbf{Q}[a_1, \ldots, a_n]$ et $\tilde{a} = \varphi(\alpha)$. Puisque $\tilde{a} \in X(\overline{\mathbf{Q}})$, il existe un homomorphisme d'anneaux $\tau\colon A \to \overline{\mathbf{Q}}$ qui applique a_i sur la i-ième composante $\tilde{a}_i$ de $\tilde{a}$ pour $i = 1, \ldots, n$. Puisque $\theta = \pi(a)$, on a $\theta \in A$ et $\tau(\theta) = \pi(\tilde{a}) = \alpha$. En vertu du théorème 1 du chapitre 1 de [5], l'homomorphisme τ s'étend en un homomorphisme d'anneaux $\tau\colon \mathcal{O} \to \overline{\mathbf{Q}}$ où $\mathcal{O}$ est un anneau de valuation de K qui contient A. Soit $\mathbf{p}$ l'idéal maximal de cet anneau. Alors, $\mathbf{p}$ est une place non triviale de K sur $\mathbf{Q}$ et τ définit un plongement dans $\mathbf{C}$ de son corps résiduel $\tilde{K}$. De plus, si on désigne par D le degré de $\mathbf{p}$ sur $\mathbf{Q}$, on a

$$d \le D \le [K\colon \mathbf{Q}(\theta)]d$$

car $\mathbf{p}$ étend une place de $\mathbf{Q}(\theta)$ de degré d. Cette place $\mathbf{p}$ remplit les conditions du théorème 3.1. En effet, puisque $\pi(\tilde{a}) = \alpha$ et $h_1(\alpha) \le \kappa/2$, le lemme 3.3 livre $h_1(\tilde{a}) \le \kappa/2 + c_1 \le \kappa$. De plus, on trouve

$$\|a - \tilde{a}\| \le c_2|\theta - \alpha| \le \exp(-c^{-1}\kappa D^2)$$

pour d assez grand. Enfin, comme $D \ge d$, l'entier D peut être supposé arbitrairement grand et l'inégalité de Liouville donne alors $\tilde{a}_i = a_i$ pour chaque i avec $a_i \in \overline{\mathbf{Q}}$.

(ii) Majoration du résultant

Pour démontrer le théorème 3.2 on emploie une majoration du résultant $R(F, G)$ de deux polynômes F et G qui tient compte de la distance d'un nombre $\theta \in \mathbf{C}$ à la réunion de l'ensemble $Z(F)$ des zéros de F et de l'ensemble $Z(G)$ des zéros de G. La démonstration présentée ici utilise les idées de Wirsing dans [34]. On montre d'abord:

Lemme 3.4. *Soient $\theta \in \mathbf{C}$ et $t \in \mathbf{R}$. Soient $F, G \in \mathbf{C}[X]$ des polynômes non constants et m, n leurs degrés respectifs. On désigne par f le nombre de zéros α de F avec $|\theta - \alpha| \le t$ et par g le nombre de zéros β de G avec $|\theta - \beta| \le t$, compte tenu de leurs multiplicités. Enfin, on note ρ la distance de θ à la réunion des zéros de F et de G. Alors, on a*

$$\rho^{fg}|R(F,G)| \le 2^{mn} M(F)^{n-g} M(G)^{m-f} |F(\theta)|^g |G(\theta)|^f \tag{3.3}$$

Démonstration. Écrivons

$$F(X) = a_0 \prod_{i=1}^{m} (X - \alpha_i) \quad \text{et} \quad G(X) = b_0 \prod_{j=1}^{n} (X - \beta_j)$$

et posons $p_i = |\theta - \alpha_i|$ pour $i = 1, \ldots, m$ et $q_j = |\theta - \beta_j|$ pour $j = 1, \ldots, n$. Pour tout choix d'indices i et j, on a

$$|\alpha_i - \beta_j| \le p_i + q_j \le 2 \max\{p_i, q_j\}.$$

On en déduit

$$\prod_{\substack{p_i \le t \\ q_j > t}} |\alpha_i - \beta_j| \le \Big(\prod_{q_j > t} 2q_j \Big)^f \quad \text{et} \quad \prod_{\substack{p_i > t \\ q_j \le t}} |\alpha_i - \beta_j| \le \Big(\prod_{p_i > t} 2p_i \Big)^g . \tag{3.4}$$

D'autre part, on a aussi

$$(2\rho)|\alpha_i - \beta_j| \le \big(2\min\{p_i, q_j\}\big)\big(2\max\{p_i, q_j\}\big) = (2p_i)(2q_j),$$

donc

$$(2\rho)^{fg} \prod_{\substack{p_i \le t \\ q_j \le t}} |\alpha_i - \beta_j| \le \Big(\prod_{p_i \le t} 2p_i \Big)^g \Big(\prod_{q_j \le t} 2q_j \Big)^f . \tag{3.5}$$

Enfin, puisque

$$|\alpha_i - \beta_j| \le |\alpha_i| + |\beta_j| \le 2 \max\{1, |\alpha_i|\} \max\{1, |\beta_j|\},$$

on trouve

$$\begin{aligned} \prod_{\substack{p_i > t \\ q_j > t}} |\alpha_i - \beta_j| &\le 2^{(m-f)(n-g)} \Big(\prod_{p_i > t} \max\{1, |\alpha_i|\} \Big)^{n-g} \Big(\prod_{q_j > t} \max\{1, |\beta_j|\} \Big)^{m-f} \\ &\le 2^{(m-f)(n-g)} \Big(\frac{M(F)}{|a_0|} \Big)^{n-g} \Big(\frac{M(G)}{|b_0|} \Big)^{m-f} . \end{aligned} \tag{3.6}$$

En multipliant termes à termes les inégalités (3.4) à (3.6) et en tenant compte des relations

$$|F(\theta)| = |a_0| \prod_{i=1}^{m} p_i \quad \text{et} \quad |G(\theta)| = |b_0| \prod_{j=1}^{n} q_j ,$$

on obtient bien

$$\rho^{fg}|R(F,G)| = \rho^{fg} |a_0|^n |b_0|^m \prod_{i,j} |\alpha_i - \beta_j| \le 2^{mn} M(F)^{n-g} M(G)^{m-f} |F(\theta)|^g |G(\theta)|^f .$$

Nous tirons d'abord une première conséquence du lemme 3.4.

Proposition 3.5. *Soit θ un nombre complexe, F et G des polynômes de $\mathbf{C}[X]$ non constants, m et n des entiers positifs qui majorent respectivement les degrés de F et de G, et ρ la distance de θ à la réunion des zéros de F et de G. Supposons que les valeurs absolues des coefficients dominants de F et de G soient toutes deux ≥ 1. Alors, pour tout entier $s \geq 0$, on a*

$$\min\{1,\rho\}^{s^2/4}|R(F,G)| \leq 2^{mn} M(F)^n M(G)^m \max\big\{|F(\theta)|, |G(\theta)|\big\}^s \tag{3.7}$$

Démonstration. L'hypothèse sur les coefficients dominants de F et G livre $M(F) \geq 1$ et $M(G) \geq 1$. Il n'y a donc pas de restriction à supposer $m = \deg(F)$ et $n = \deg(G)$.

Considérons d'abord le cas $s \leq m+n$. Si les $m+n$ nombres réels

$$|\theta - \alpha|,\ (\alpha \in Z(F)) \quad \text{et} \quad |\theta - \beta|,\ (\beta \in \mathbf{Z}(G))$$

sont deux-à-deux distincts, il existe un nombre réel t tel que s soit la somme du nombre f de zéros α de F avec $|\theta - \alpha| \leq t$ et du nombre g de zéros β de G avec $|\theta - \beta| \leq t$. Dans ce cas, l'inégalité (3.7) découle du lemme 3.4 car, puisque $f + g = s$, on a $fg \leq s^2/4$. En général, on peut approcher F et G d'aussi près qu'on le souhaite par des paires de polynômes $\tilde{F}$ et $\tilde{G}$ de degrés respectifs m et n tels que

$$\mathrm{Card}\big\{|\theta - \gamma|\,;\, \gamma \in Z(\tilde{F}\tilde{G})\big\} = m+n.$$

Comme (3.7) est vérifiée pour chacune de ces paires de polynômes, elle l'est aussi, par continuité, pour F et G.

Supposons maintenant $s = m+n+k$ avec $k > 0$. L'hypothèse sur les coefficients dominants de F et G implique aussi $\rho^m \leq |F(\theta)|$ et $\rho^n \leq |G(\theta)|$. On obtient ainsi

$$\begin{aligned}\min\{1,\rho\}^{s^2/4} &\leq \min\{1,\rho\}^{(m+n)^2/4}\rho^{(m+n)k/2}\\ &\leq \min\{1,\rho\}^{(m+n)^2/4}\max\big\{|F(\theta)|,|G(\theta)|\big\}^k.\end{aligned}$$

L'inégalité (3.7) étant vérifiée pour $s = m+n$, elle l'est donc aussi pour $s = m+n+k$.

La proposition 3.5 s'applique par exemple à toute paire de polynômes F et G non constants, premiers entre eux, à coefficients entiers. Le nombre $R(F,G)$ est alors un entier non nul et on peut minorer sa valeur absolue par 1. Dans cet ordre d'idées, nous montrons encore:

Proposition 3.6. *Soit $\theta \in \mathbf{C}$ et soient F, $G \in \mathbf{Z}[X]$ des polynômes non constants et premiers entre eux. On suppose*

$$\mathrm{dist}(\theta, Z(F)) \leq \mathrm{dist}(\theta, Z(G))$$

et on désigne par s le nombre de zéros α de F avec $|\theta - \alpha| \leq \mathrm{dist}(\theta, Z(G))$, compte tenu de leurs multiplicités. Alors, on a

$$0 \leq (\log 2)\deg(F)\deg(G) + \deg(F)\log M(G) + \deg(G)\log M(F) + s\log|G(\theta)|.$$

Démonstration. Soit $t = \mathrm{dist}(\theta, Z(G))$ et soit $(G_k)_{k\geq 1}$ une suite de polynômes de même degré que G qui converge vers G et qui vérifie $\mathrm{dist}(\theta, Z(G_k)) > t$ pour tout $k \geq 1$. Pour tout $k \geq 1$, le lemme 3.4 appliqué à F et G_k donne

$$|R(F,G_k)| \leq 2^{\deg(F)\deg(G)} M(F)^{\deg(G)} M(G_k)^{\deg(F)-s}|G_k(\theta)|^s.$$

On obtient le résultat annoncé en prenant le logarithme des deux membres de cette inégalité, en passant à la limite lorsque $k \to \infty$ et en minorant $M(G)$ par 1.

En particulier, on retrouve un résultat bien connu en minorant s par 1 dans la proposition 3.6 (voir lemme 1 de [3], pp. 145–146 de [9], et lemme 4 de [27]):

Corollaire 3.7. *Soit $\theta \in \mathbf{C}$ et soient F, $G \in \mathbf{Z}[X]$ des polynômes non nuls premiers entre eux. Alors, on a*

$$1 \leq 2^{\deg(F)\deg(G)} M(F)^{\deg(G)} M(G)^{\deg(F)} \max\{|F(\theta)|, |G(\theta)|\}.$$

(iii) Résultats auxiliaires

Lemme 3.8. *Soit $\theta \in \mathbf{C}$ et soit $a \in \mathbf{R}$ avec $0 < a < 1/2$. Alors, pour tout entier δ suffisamment grand et tout nombre réel $\mu \geq \delta$, il existe un polynôme non nul $P \in \mathbf{Z}[X]$ qui vérifie*

$$\deg(P) \leq \delta, \quad \log M(P) \leq \mu \quad \text{et} \quad |P(\theta)| \leq \exp(-a\delta\mu). \tag{3.8}$$

Démonstration. Soit H la partie entière de $e^\mu/(\delta+1)$. Pour un polynôme $P \in \mathbf{R}[X]$ de degré $\leq \delta$, les parties réelles et imaginaires de $P(\theta)$ sont des formes linéaires en les coefficients de P, dont la somme des valeurs absolues des coefficients est $\leq (1 + |\theta| + \cdots + |\theta|^\delta)$. En vertu du lemme de Thue-Siegel (cf. Lemme 1.3.2 de [29]), il existe donc un polynôme non nul $P \in \mathbf{Z}[X]$, de degré $\leq \delta$, de hauteur $\leq H$, tel que les parties réelles et imaginaires de $P(\theta)$ soient majorées en valeur absolue par

$$(1 + |\theta| + \cdots + |\theta|^\delta) H^{-(\delta-1)/2}.$$

Ce polynôme vérifie $\log M(P) \leq \mu$ et, pour δ assez grand, il remplit aussi la troisième des conditions (3.8).

Proposition 3.9. *Soit $\theta \in \mathbf{C}$ et soit $b \in \mathbf{R}$ avec $0 < b < 1/16$. Alors, pour tout entier δ assez grand et tout nombre réel $\mu \geq \delta$, il existe un polynôme non nul $Q \in \mathbf{Z}[X]$ qui est une puissance d'un polynôme irréductible de $\mathbf{Z}[X]$ et qui vérifie*

$$\deg(Q) \leq \delta, \quad \log M(Q) \leq \mu \quad \text{et} \quad |Q(\theta)| \leq \exp(-b\delta\mu).$$

Démonstration. On pose $a = 4b + 1/4$. Si δ est assez grand, le lemme 3.8 montre qu'il existe un polynôme non nul $P \in \mathbf{Z}[X]$ qui vérifie (3.8). On écrit $P = mP_1P_2\cdots P_r$ où m est un entier et où $P_1, P_2, \ldots, P_r$ sont des puissances de polynômes irréductibles de $\mathbf{Z}[X]$ ordonnées de telle sorte qu'on ait

$$\mathrm{dist}(\theta, Z(P_1)) \leq \mathrm{dist}(\theta, Z(P_2)) \leq \ldots \leq \mathrm{dist}(\theta, Z(P_r)).$$

On pose $F = m\prod_{i\leq 4} P_i$ et $G = \prod_{i>4} P_i$. Alors, on a $\mathrm{dist}(\theta, Z(F)) \leq \mathrm{dist}(\theta, Z(G))$ et, si r est > 4, le nombre de zéros de F dont la distance à θ est $\leq \mathrm{dist}(\theta, Z(G))$ est au moins 4. Dans ce cas, la proposition 3.6 livre

$$-4\log|G(\theta)| \leq (\log 2)\deg(F)\deg(G) + \deg(F)\log M(G) + \deg(G)\log M(F).$$

Comme $\deg(F) + \deg(G) \leq \delta$ et $\log M(F) + \log M(G) \leq \mu$, le membre de droite de cette inégalité est $\leq \delta\mu$. On en déduit

$$\log|F(\theta)| = \log|P(\theta)| - \log|G(\theta)| \leq -a\delta\mu + (1/4)\delta\mu = -4b\delta\mu.$$

Cette dernière inégalité est encore vérifiée si $r \leq 4$ car alors $F = P$. On en déduit que, dans tous les cas, il existe un entier positif $i \leq 4$ avec $\log|P_i(\theta)| \leq -b\delta\mu$. Ce polynôme possède les propriétés requises.

Lemme 3.10. *Soient $\theta \in \mathbf{C}$, $\delta \in \mathbf{Z}$ et $\mu, b \in \mathbf{R}$ avec*

$$0 < b \leq 1/4 \quad \text{et} \quad 0 < \delta \leq \mu.$$

Supposons qu'il existe des polynômes $F, G \in \mathbf{Z}[X]$ premiers entre eux, de degré $\leq \delta$ et de mesure de Mahler $\leq e^\mu$, qui vérifient

$$\mathrm{dist}(\theta, Z(F)) \leq \mathrm{dist}(\theta, Z(G)) \quad \text{et} \quad \max\{|F(\theta)|, |G(\theta)|\} \leq \exp(-b\delta\mu).$$

Alors, on a

$$\mathrm{dist}(\theta, Z(F)) \leq \exp(-(1/3)b^2\delta\mu) \quad \text{et} \quad \max\{\deg(F), \deg(G)\} > (1/3)b\delta.$$

Si en plus on suppose $\deg(F) \le (1/3)b\delta$, *alors on a:*

$$\log|G(\theta)| > -3\deg(G)\log M(F).$$

Démonstration. Soit $\rho = \mathrm{dist}(\theta, Z(F))$. Puisque $|F(\theta)| \le 1$, on a $\rho \le 1$. Alors, la proposition 3.5 donne

$$\rho^{s^2/4} \le \exp\{(\log 2)\delta^2 + 2\delta\mu - sb\delta\mu\} \le \exp\{-(sb - 2.7)\delta\mu\}$$

pour tout entier $s \ge 0$. En posant $s = [5.4/b] + 1$, on a $5.4/b \le s \le 5.65/b$, donc

$$\rho \le \exp(-10.8 s^{-2}\delta\mu) \le \exp(-(1/3)b^2\delta\mu).$$

Si on applique plutôt la proposition 3.6 tout en supposant $\deg(F) \le (1/3)b\delta$, on trouve

$$\begin{aligned} 0 &< \deg(F)\deg(G) + \deg(F)\log M(G) + \deg(G)\log M(F) + \log|G(\theta)| \\ &< \deg(G)\log M(F) + (2/3)b\delta\mu + \log|G(\theta)| \\ &< \deg(G)\log M(F) + (1/3)\log|G(\theta)| \end{aligned}$$

d'où la dernière inégalité du lemme. Enfin, puisque $\log M(F) \le \mu$, cette inégalité entraîne $\deg(G) > (1/3)b\delta$. Ainsi au moins un des polynômes F ou G est de degré $> (1/3)b\delta$.

(iv) Démonstration du théorème 3.2

Soit κ un nombre réel $\ge 10^7$ et soit $\theta \in \mathbf{C}$ un nombre transcendant sur $\mathbf{Q}$. On pose $a = (3600)^{-1}$. La proposition 3.9 montre que, pour tout entier n assez grand, il existe un polynôme non nul $Q_n \in \mathbf{Z}[X]$ qui est une puissance d'un polynôme irréductible et qui vérifie

$$\deg(Q_n) \le n, \quad \log M(Q_n) \le a\kappa n \quad \text{et} \quad \log|Q_n(\theta)| \le -18^{-1}a\kappa n^2. \tag{3.9}$$

On va montrer que, pour une infinité d'entiers n, on a en plus

$$\deg(Q_n) \ge an \quad \text{et} \quad \mathrm{dist}(\theta, Z(Q_n)) \le \exp(-10^{-7}\kappa n^2). \tag{3.10}$$

Le théorème 3.2 en découle. En effet, soit α_n une racine de Q_n dont la distance à θ est minimale. Pour chaque entier n qui vérifie (3.10), on a

$$\deg(\alpha_n) \le n, \quad h_1(\alpha_n) = \deg(Q_n)^{-1}\log M(Q_n) \le \kappa$$

et aussi

$$0 < |\theta - \alpha_n| \le \exp(-10^{-7}\kappa n^2).$$

S'il existe une infinité de tels entiers n, l'encadrement de $|\theta - \alpha_n|$ montre que, parmi les nombres α_n qui leur correspondent, il y a une infinité de nombres algébriques distincts. Leur hauteur étant bornée, il faut que leur degré tende vers l'infini. La conclusion suit.

Pour démontrer l'existence d'une infinité d'entiers n qui vérifient (3.10), on suppose au contraire qu'il existe un entier $n_0 \ge 20$ tel que, pour tout $n \ge n_0$, on ait

$$\deg(Q_n) < an \quad \text{ou} \quad \mathrm{dist}(\theta, Z(Q_n)) > \exp(-10^{-7}\kappa n^2). \tag{3.11}$$

On va montrer que cela mène à une contradiction. Pour cela, on procède en plusieurs étapes:

1) Pour tout entier $k \ge n_0$, il existe un nombre fini d'entiers $m \ge k$ tels que $R(Q_k, Q_m) = 0$.

En effet, soit P le facteur irréductible de Q_k. Si $R(Q_k, Q_m) = 0$, alors $Q_m = P^t$ où t est un entier $\leq m$ et, en vertu de (3.9), on obtient $\log|P(\theta)| \leq -18^{-1}a\kappa m$. Comme θ est transcendant sur $\mathbf{Q}$, cette inégalité n'est vérifiée que pour un nombre fini d'entiers m.

En vertu de ce résultat, il existe une infinité d'entiers $m \geq n_0$ avec $R(Q_m, Q_{m+1}) \neq 0$.

2) Soit m un entier $\geq n_0$ pour lequel $R(Q_m, Q_{m+1}) \neq 0$ et soit (F, G) une permutation de (Q_m, Q_{m+1}) pour laquelle

$$\operatorname{dist}(\theta, Z(F)) \leq \operatorname{dist}(\theta, Z(G)).$$

Alors, F et G vérifient les conditions du lemme 3.10 avec $b = 1/20$, $\delta = m + 1$ et $\mu = a\kappa(m + 1)$. En tenant compte de (3.11), on en déduit successivement

$$\begin{aligned}
&\operatorname{dist}(\theta, Z(F)) \leq \exp(-1200^{-1}a\kappa(m+1)^2),\\
&\deg(F) < a(m+1),\\
&\deg(G) \geq 60^{-1}(m+1),\\
&\operatorname{dist}(\theta, Z(G)) > \exp(-10^{-7}\kappa(m+1)^2)
\end{aligned} \tag{3.12}$$

et aussi

$$\log|G(\theta)| > -3\deg(G)\log M(F). \tag{3.13}$$

3) Soit k un entier $\geq n_0$ et soit m le plus grand entier pour lequel $R(Q_k, Q_m) = 0$. Alors, on a:

$$\operatorname{dist}(\theta, Z(Q_m)) > \operatorname{dist}(\theta, Z(Q_{m+1})).$$

Supposons le contraire. Puisque $R(Q_m, Q_{m+1}) \neq 0$, les inégalités (3.12) et (3.13) sont vérifiées avec $F = Q_m$ et $G = Q_{m+1}$, donc on trouve:

$$\begin{aligned}
&\deg(Q_m) < a(m+1),\\
&\operatorname{dist}(\theta, Z(Q_{m+1})) > \exp(-10^{-7}\kappa(m+1)^2),\\
&\log|Q_{m+1}(\theta)| > -3a\kappa m\deg(Q_{m+1}).
\end{aligned} \tag{3.14}$$

Soit n le plus grand entier pour lequel $R(Q_{m+1}, Q_n) = 0$. Puisque Q_{m+1} et Q_n sont des puissances d'un même polynôme irréductible de $\mathbf{Z}[X]$, la distance de θ à l'ensemble des zéros de l'un et de l'autre est la même. On a donc

$$\operatorname{dist}(\theta, Z(Q_n)) > \exp(-10^{-7}\kappa n^2).$$

Comme $R(Q_n, Q_{n+1}) \neq 0$, on en déduit que les inégalités (3.12) sont vérifiées avec n au lieu de m, en posant $F = Q_{n+1}$ et $G = Q_n$. En particulier, on obtient

$$\deg(Q_{n+1}) < a(n+1). \tag{3.15}$$

Comme Q_{m+1} et Q_n sont des puissances d'un même polynôme, on a aussi

$$\frac{\log|Q_{m+1}(\theta)|}{\deg(Q_{m+1})} = \frac{\log|Q_n(\theta)|}{\deg(Q_n)} \leq -18^{-1}a\kappa n.$$

Si on compare cette inégalité avec la minoration de $\log|Q_{m+1}(\theta)|$ donnée par (3.14), on en déduit

$$n \leq 54m.$$

Or, en vertu du choix de l'entier m, on a $R(Q_m, Q_{n+1}) \neq 0$. Si on applique le corollaire 3.7 à cette paire de polynômes en tenant compte des majorations de leurs degrés données par (3.14) et (3.15), on obtient

$$\begin{aligned} 0 &\leq (\log 2)a^2(m+1)(n+1) + 2a^2\kappa(m+1)(n+1) - 18^{-1}a\kappa m^2, \\ &\leq \big(54(\log 2)\kappa^{-1} + 108 - 20^{-1}a^{-1}\big)a^2\kappa(m+1)^2, \end{aligned}$$

ce qui est impossible puisque $\kappa \geq 10^7$ et $a^{-1} = 3600$.

4) Soit m le plus grand entier $\geq n_0$ tel que $R(Q_{n_0}, Q_m) = 0$ et soit n le plus grand entier $\geq m+1$ tel que $R(Q_{m+1}, Q_n) = 0$. En vertu du résultat précédent appliqué à $k = n_0$ puis à $k = m+1$, on a

$$\mathrm{dist}(\theta, Z(Q_m)) > \mathrm{dist}(\theta, Z(Q_{m+1})) \quad \text{et} \quad \mathrm{dist}(\theta, Z(Q_n)) > \mathrm{dist}(\theta, Z(Q_{n+1})).$$

Alors, les inégalités (3.12) livrent

$$\begin{aligned} &\deg(Q_{m+1}) < a(m+1), \\ &\log|Q_m(\theta)| > -3m \log M(Q_{m+1}), \\ &\deg(Q_n) \geq 60^{-1}n. \end{aligned}$$

On en déduit

$$\frac{\log M(Q_{m+1})}{\deg(Q_{m+1})} \geq \frac{54^{-1}a\kappa m}{a(m+1)} > 60^{-1}\kappa$$

et

$$\frac{\log M(Q_n)}{\deg(Q_n)} \leq \frac{a\kappa n}{60^{-1}n} = 60a\kappa.$$

Or, comme Q_{m+1} et Q_n sont des puissances d'un même polynôme, ces deux quotients sont égaux. Puisque $a = 3600^{-1}$, c'est la contradiction cherchée.

4. Relèvement du sous-groupe obstructeur

Soit $K \subset \mathbf{C}$ un sous-corps de $\mathbf{C}$ de type fini et de degré de transcendance 1 sur $\mathbf{Q}$. Le corps K est donc un corps de fonctions en une variable sur $\mathbf{Q}$.

Étant donné un entier positif n, un point non nul $x = (x_0, x_1, \ldots, x_n)$ de K^{n+1} et une place non triviale $\mathbf{q}$ de K sur $\mathbf{Q}$, on définit l'ordre de x en $\mathbf{q}$ par

$$\mathrm{ord}_{\mathbf{q}}(x) = \min\{\mathrm{ord}_{\mathbf{q}}(x_0), \ldots, \mathrm{ord}_{\mathbf{q}}(x_n)\}.$$

On définit aussi la *hauteur* du point projectif $(x_0 : x_1 : \cdots : x_n) \in \mathbf{P}^n(K)$ déterminé par x en posant

$$\mathbf{h}(x_0 : x_1 : \cdots : x_n) = -\sum_{\mathbf{q}} \mathrm{ord}_{\mathbf{q}}(x) \deg(\mathbf{q})$$

où la somme est étendue à toutes les places non triviales $\mathbf{q}$ de K sur $\mathbf{Q}$. Enfin, on définit sur K^n une version affine de cette hauteur en posant

$$\mathbf{h}_1(x_1, \ldots, x_n) = \mathbf{h}(1 : x_1 : \ldots : x_n)$$

pour tout $(x_1, \ldots, x_n) \in K^n$. C'est simplement le degré du ppcm des diviseurs des pôles de $x_1, \ldots, x_n$.

Soient d, d_0, d_1 et G comme au §2. Le but de ce paragraphe est de démontrer le résultat suivant:

Théorème 4.1. *Soit K un sous-corps de $\mathbf{C}$ de type fini et de degré de transcendance 1 sur $\mathbf{Q}$, et soit $\mathbf{p}$ une place non triviale de K en tant que corps de fonctions d'une variable sur $\mathbf{Q}$. On note $\mathcal{O}$ l'anneau de valuation de $\mathbf{p}$, D son degré, et on choisit un plongement de son corps résiduel $\tilde{K}$ dans $\mathbf{C}$. On se donne des entiers ℓ_0, N et $T_1, \dots, T_{d_1}$ tous ≥ 0, un sous-espace W de $T_G(K)$ de dimension ℓ_0 engendré par des éléments $w_1, \dots, w_{\ell_0}$ de $T_G(K)$, un sous-ensemble fini $\Sigma = \{\gamma_1, \dots, \gamma_N\}$ de $G(K)$ et un sous-groupe algébrique H de G incomplètement défini dans G par des polynômes de $\tilde{K}[X_1, \dots, X_{d_0}, Y_1, \dots, Y_{d_1}]$ de degré $\leq T_i$ en Y_i pour $i = 1, \dots, d_1$. On suppose que les coordonnées des w_j, des γ_j et des γ_j^{-1} appartiennent à l'anneau $\mathcal{O}$. Pour $j = 1, \dots, \ell_0$ (resp. $j = 1, \dots, N$), on note $\tilde{w}_j$ (resp. $\tilde{\gamma}_j$) l'élément de $T_G(\tilde{K})$ (resp. de $G(\tilde{K})$) dont les coordonnées sont les images des coordonnées de w_j (resp. de γ_j) sous l'homomorphisme de réduction $\tau\colon \mathcal{O} \to \tilde{K}$ associé à $\mathbf{p}$. On désigne par $\tilde{W}$ le sous-espace de $T_G(\tilde{K})$ engendré par $\tilde{w}_1, \dots, \tilde{w}_{\ell_0}$ et on pose $\tilde{\Sigma} = \{\tilde{\gamma}_1, \dots, \tilde{\gamma}_N\}$. On se donne aussi des nombres réels $A'_1, \dots, A'_{d_1}, B_1, B_2$ tous $\geq e$ qui vérifient*

$$\begin{aligned}
&\mathbf{h}_1(\gamma_1^{(i)}, \dots, \gamma_N^{(i)}) \leq \log B_1 \quad (1 \leq i \leq d_0),\\
&\mathbf{h}_1(w_j^{(1)}, \dots, w_j^{(d)}) \leq \log B_2 \quad (1 \leq j \leq \ell_0),\\
&\mathbf{h}_1(\gamma_j^{(d_0+i)}) \leq \log A'_i \quad (1 \leq i \leq d_1,\ 1 \leq j \leq N).
\end{aligned}$$

On suppose enfin

$$D > \max\Big\{ 2d_1 \sum_{i=1}^{d_1} T_i \log A'_i,\ 2d_0 \log B_1 + \ell_0 \log B_2 \Big\}.$$

Alors, il existe un sous-groupe algébrique L de G défini sur K, connexe si H est connexe, qui vérifie les trois conditions suivantes:

(i) *L et H possèdent la même fonction d'Hilbert-Samuel;*

(ii) $\mathrm{Card}\big((\Sigma + L(K))/L(K)\big) \leq \mathrm{Card}\big((\tilde{\Sigma} + H(\tilde{K}))/H(\tilde{K})\big)$;

(iii) $\dim_K \big((W + T_L(K))/T_L(K)\big) \leq \dim_{\tilde{K}} \big((\tilde{W} + T_H(\tilde{K}))/T_H(\tilde{K})\big)$.

La démonstration de ce résultat utilise plusieurs lemmes. Dans la suite, on fixe le choix d'un corps K et d'une place $\mathbf{p}$ de K comme dans l'énoncé du théorème 4.1. On note $\mathcal{O}$ l'anneau de valuation de $\mathbf{p}$, D son degré, et on fixe aussi un plongement de son corps résiduel $\tilde{K}$ dans $\mathbf{C}$. On note $\tau\colon \mathcal{O} \to \tilde{K}$ l'homomorphisme de réduction associé à $\mathbf{p}$ et, pour tout $x \in \mathcal{O}$, on désigne par $\tilde{x}$ l'image de x sous τ. Pour tout entier $n > 0$, on étend cette définition aux points $x = (x_1, \dots, x_n)$ de $\mathcal{O}^n$ en posant $\tilde{x} = (\tilde{x}_1, \dots, \tilde{x}_n)$. Enfin, si V est un sous-espace de K^n, on désigne par $\tilde{V}$ le sous-espace de $\tilde{K}^n$ constitué des points $\tilde{x}$ avec $x \in V \cap \mathcal{O}^n$. On verra plus loin que cette définition est compatible avec celle de $\tilde{W}$ dans l'énoncé du théorème 4.1, en vertu des hypothèses de ce théorème.

Si x est un élément non nul de K, alors $\mathbf{h}_1(x)$ est le degré commun des diviseurs des pôles et des zéros de x. Dans ce contexte, on utilisera la version suivante du lemme de Liouville:

Lemme 4.2. *Soit x un élément non nul de K. Si $\mathbf{h}_1(x) < D$, alors on a $x \in \mathcal{O}$ et $\tilde{x} \neq 0$.*

Démonstration. En effet si $x \notin \mathcal{O}$ (resp. $x \in \mathcal{O}$ et $\tilde{x} = 0$), alors $\mathbf{p}$ divise le diviseur des pôles (resp. des zéros) de x et par suite on a $\mathbf{h}_1(x) \geq \deg(\mathbf{p}) = D$.

Pour chaque entier $n > 0$, on étend la notion de hauteur aux sous-espaces V de K^n. Si $V \neq 0$ et si $\{x_1, \dots, x_m\}$ désigne une base quelconque de V, on définit la *hauteur* de V par

$$\mathbf{h}(V) = \mathbf{h}(x_1 \wedge \ldots \wedge x_m)$$

c'est-à-dire comme étant la hauteur du point projectif déterminé par le $\binom{n}{m}$-uplet dont les coordonnées sont les mineurs d'ordre m de la matrice $m \times n$ ayant pour lignes $x_1, \dots, x_m$. Si $V = 0$, on pose simplement $\mathbf{h}(V) = 0$. Ainsi, pour tout sous-espace V de K^n défini sur $\mathbf{Q}$, on a $\mathbf{h}(V) = 0$.

Lemme 4.3. *Soit V un sous-espace de K^n et soient $x_1, \ldots, x_m$ des éléments de $V \cap \mathcal{O}^n$. Alors, on a $\dim_{\tilde{K}}(\tilde{V}) = \dim_K(V)$ et les trois conditions suivantes sont équivalentes:*

(i) $\{x_1, \ldots, x_m\}$ est à la fois une base de $V \cap \mathcal{O}^n$ en tant que module sur $\mathcal{O}$ et une base de V en tant qu'espace vectoriel sur K;

(ii) $\{\tilde{x}_1, \ldots, \tilde{x}_m\}$ est une base de $\tilde{V}$ en tant qu'espace vectoriel sur $\tilde{K}$;

(iii) $m = \dim_K(V)$ et $\mathrm{ord}_{\mathbf{p}}(x_1 \wedge \ldots \wedge x_m) = 0$.

Démonstration. Puisque $\mathcal{O}$ est un anneau principal dont le corps des fractions est K et que $V \cap \mathcal{O}^n$ est un $\mathcal{O}$-module sans torsion, $V \cap \mathcal{O}^n$ est un $\mathcal{O}$-module libre de rang égal à $\dim_K(V)$. En particulier, toute base de $V \cap \mathcal{O}^n$ en tant que $\mathcal{O}$-module est aussi une base de V en tant qu'espace vectoriel sur K. Par ailleurs, puisque $\mathcal{O}$ est un anneau local, le lemme de Nakayama (cf. prop. 2.8 de [1]) montre que $x_1, \ldots, x_m$ constituent un système de générateurs de $V \cap \mathcal{O}^n$ en tant que $\mathcal{O}$-module si et seulement si $\tilde{x}_1, \ldots, \tilde{x}_m$ engendrent $\tilde{V}$ en tant qu'espace vectoriel sur $\tilde{K}$. On en déduit $\dim_{\tilde{K}}(\tilde{V}) = \dim_K(V)$ et l'équivalence entre (i) et (ii). L'équivalence entre (ii) et (iii) découle simplement du fait que $\{\tilde{x}_1, \ldots, \tilde{x}_m\}$ est une base de $\tilde{V}$ si et seulement si on a $m = \dim_{\tilde{K}}(\tilde{V})$ et que le produit extérieur $\tilde{x}_1 \wedge \ldots \wedge \tilde{x}_m$ est $\neq 0$.

Une base $\{x_1, \ldots, x_m\}$ de V qui est contenue dans $\mathcal{O}^n$ et qui remplit les conditions équivalentes du lemme 4.3 est dite *régulière* (en $\mathbf{p}$).

Lemme 4.4. *Soit V un sous-espace de K^n. Si $x_1, \ldots, x_k$ sont des éléments de $V \cap \mathcal{O}^n$ dont les images $\tilde{x}_1, \ldots, \tilde{x}_k$ dans $\tilde{V}$ sont linéairement indépendantes sur $\tilde{K}$, alors on peut compléter $\{x_1, \ldots, x_k\}$ en une base régulière de V.*

Démonstration. Si $\tilde{x}_1, \ldots, \tilde{x}_k$ sont linéairement indépendants sur $\tilde{K}$, on peut compléter $\{\tilde{x}_1, \ldots, \tilde{x}_k\}$ en une base $\{\tilde{x}_1, \ldots, \tilde{x}_k, y_{k+1}, \ldots, y_m\}$ de $\tilde{V}$. Pour chacun des y_j avec $j = k+1, \ldots, m$, il existe $x_j \in V \cap \mathcal{O}^n$ tel que $\tilde{x}_j = y_j$. Alors $\{x_1, \ldots, x_m\}$ est une base régulière de V en vertu du lemme 4.3.

Lemme 4.5. *Soient V_1, V_2 des sous-espaces de K^n. On pose $U = V_1 \cap V_2$ et $W = V_1 + V_2$. Alors, on a*

$$\mathbf{h}(U) + \mathbf{h}(W) \le \mathbf{h}(V_1) + \mathbf{h}(V_2). \tag{4.1}$$

De plus, si $\mathbf{h}(V_1) + \mathbf{h}(V_2) < D$, alors $\tilde{U} = \tilde{V}_1 \cap \tilde{V}_2$ et $\tilde{W} = \tilde{V}_1 + \tilde{V}_2$.

Démonstration. La première partie du lemme est un analogue pour les corps de fonctions du lemme 8A du chapitre I de [24]. La démonstration du présent lemme s'inspire des mêmes idées. On choisit d'abord une base $\{u_1, \ldots, u_\ell\}$ de U qu'on complète d'une part en une base $\{u_1, \ldots, u_\ell, x_1, \ldots, x_r\}$ de V_1 et d'autre part en une base $\{u_1, \ldots, u_\ell, y_1, \ldots, y_s\}$ de V_2. Alors,

$$\{u_1, \ldots, u_\ell, x_1, \ldots, x_r, y_1, \ldots, y_s\} \tag{4.2}$$

est une base de W et, pour montrer l'inégalité (4.1), il suffit d'établir que, pour toute place $\mathbf{q}$ de K sur $\mathbf{Q}$, on a:

$$\begin{aligned} &\mathrm{ord}_{\mathbf{q}}(u_1 \wedge \ldots \wedge u_\ell) + \mathrm{ord}_{\mathbf{q}}(u_1 \wedge \ldots \wedge u_\ell \wedge x_1 \wedge \ldots \wedge x_r \wedge y_1 \wedge \ldots \wedge y_s) \\ &\qquad \ge \mathrm{ord}_{\mathbf{q}}(u_1 \wedge \ldots \wedge u_\ell \wedge x_1 \wedge \ldots \wedge x_r) + \mathrm{ord}_{\mathbf{q}}(u_1 \wedge \ldots \wedge u_\ell \wedge y_1 \wedge \ldots \wedge y_s). \end{aligned} \tag{4.3}$$

En fait, il suffit de le montrer pour $\mathbf{q} = \mathbf{p}$. On observe d'abord que la différence entre le membre de gauche et le membre de droite de (4.3) est une constante indépendante du choix des u_i, x_i et y_i. Pour évaluer cette différence, on peut donc choisir pour $\{u_1, \ldots, u_\ell\}$ une base régulière de U et la compléter, selon le lemme

4.4, d'une part en une base régulière $\{u_1, \ldots, u_\ell, x_1, \ldots, x_r\}$ de V_1 et d'autre part en une base régulière $\{u_1, \ldots, u_\ell, y_1, \ldots, y_s\}$ de V_2. Alors, le membre de droite de (4.3) est nul et celui de gauche est réduit à

$$\operatorname{ord}_{\mathbf{p}}(u_1 \wedge \ldots \wedge u_\ell \wedge x_1 \wedge \ldots \wedge x_r \wedge y_1 \wedge \ldots \wedge y_s). \tag{4.4}$$

Comme ce dernier est un entier ≥ 0, cela démontre (4.3).

De plus, si pour le choix particulier des u_i, x_i et y_i indiqué ci-dessus, (4.2) n'est pas une base régulière de W, alors (4.4) est un entier positif et on a l'inégalité stricte dans (4.3) pour $\mathbf{q} = \mathbf{p}$. En sommant les contributions de toutes les places $\mathbf{q}$ de K sur $\mathbf{Q}$, on en déduit

$$\mathbf{h}(U) + \mathbf{h}(W) + D \leq \mathbf{h}(V_1) + \mathbf{h}(V_2),$$

donc $\mathbf{h}(V_1) + \mathbf{h}(V_2) \geq D$. Si on suppose au contraire $\mathbf{h}(V_1) + \mathbf{h}(V_2) < D$, alors

$$\{\tilde{u}_1, \ldots, \tilde{u}_\ell, \tilde{x}_1, \ldots, \tilde{x}_r, \tilde{y}_1, \ldots, \tilde{y}_s\}$$

est une base de $\tilde{W}$. On en déduit $\tilde{W} = \tilde{V}_1 + \tilde{V}_2$ et aussi que $\{\tilde{u}_1, \ldots, \tilde{u}_\ell\}$ est une base de $\tilde{V}_1 \cap \tilde{V}_2$, donc $\tilde{V}_1 \cap \tilde{V}_2 = \tilde{U}$.

Lemme 4.6. *Soit k un entier positif $\leq n$, soit $\pi: \mathbf{C}^n \to \mathbf{C}^k$ l'application linéaire de projection sur les k premières coordonnées donnée par $\pi(a_1, \ldots, a_n) = (a_1, \ldots, a_k)$, et soit V un sous-espace de K^n. On pose $V_1 = \pi(V)$. Alors, on a $\mathbf{h}(V_1) \leq \mathbf{h}(V)$. De plus, si $\mathbf{h}(V) < D$, alors $\tilde{V}_1 = \pi(\tilde{V})$.*

Démonstration. Soit $\{e_1, \ldots, e_n\}$ la base canonique de K^n. Le noyau de π est donc le sous-espace V_0 de K^n engendré par $e_{k+1}, \ldots, e_n$. On pose $W = V_0 + V$ et on complète $\{e_{k+1}, \ldots, e_n\}$ en une base $\{e_{k+1}, \ldots, e_n, x_1, \ldots, x_r\}$ de W avec $x_1, \ldots, x_r \in V$. Alors, $\{\pi(x_1), \ldots, \pi(x_r)\}$ est une base de $\pi(V) = V_1$ et, pour toute place non triviale $\mathbf{q}$ de K sur $\mathbf{Q}$, on trouve

$$\operatorname{ord}_{\mathbf{q}}(e_{k+1} \wedge \ldots \wedge e_n \wedge x_1 \wedge \ldots \wedge x_r) = \operatorname{ord}_{\mathbf{q}}(\pi(x_1) \wedge \ldots \wedge \pi(x_r)).$$

Cela implique $\mathbf{h}(W) = \mathbf{h}(V_1)$. En vertu du lemme 4.5, on en déduit

$$\mathbf{h}(V_1) \leq \mathbf{h}(V_0) + \mathbf{h}(V) = \mathbf{h}(V)$$

car V_0 étant défini sur $\mathbf{Q}$ sa hauteur est nulle. Si on suppose en outre $\mathbf{h}(V) < D$, le même lemme donne $\tilde{W} = \tilde{V}_0 + \tilde{V}$, donc $\dim_{\tilde{K}}(\tilde{V}_0 + \tilde{V}) = \dim_K(V_0 + V)$. Comme $\tilde{V}_0$ est le noyau de la restriction de π à $\tilde{K}^n$, on trouve dans ce cas

$$\dim_{\tilde{K}}(\pi(\tilde{V})) = \dim_K(\pi(V)).$$

Or, on a $\pi(V) = V_1$ et $\dim_K(V_1) = \dim_{\tilde{K}}(\tilde{V}_1)$. On en déduit $\dim_{\tilde{K}}(\pi(\tilde{V})) = \dim_{\tilde{K}}(\tilde{V}_1)$ et l'inclusion $\pi(\tilde{V}) \subset \tilde{V}_1$ entraîne $\pi(\tilde{V}) = \tilde{V}_1$.

Lemme 4.7. *Soient V_1, V_2 des sous-espaces de K^n et S un sous-espace de $\tilde{K}^n$. On suppose que $U = V_1 \cap V_2$ vérifie $\tilde{U} = \tilde{V}_1 \cap \tilde{V}_2$. Alors, il existe un sous-espace R de K^n avec $\tilde{R} = S$ qui remplit les conditions*

$$\dim_K(V_i \cap R) = \dim_{\tilde{K}}(\tilde{V}_i \cap S)$$

pour $i = 1, 2$.

Démonstration. Désignons par $\tau^n: \mathcal{O}^n \to \tilde{K}^n$ l'application qui à $x \in \mathcal{O}^n$ associe $\tilde{x} \in \tilde{K}^n$. On choisit d'abord une famille ordonnée $\mathcal{C}$ d'éléments de $U \cap \mathcal{O}^n$ dont l'image $\tilde{\mathcal{C}}$ sous τ^n constitue une base de $\tilde{U} \cap S$. Puis, pour

$i = 1, 2$, on choisit une famille ordonnée $\mathcal{B}_i$ d'éléments de $V_i \cap \mathcal{O}^n$ dont l'image $\tilde{\mathcal{B}}_i$ sous τ^n, une fois jointe à $\mathcal{C}$, constitue une base de $\tilde{V}_i \cap S$. Comme

$$\tilde{U} \cap S = (\tilde{V}_1 \cap S) \cap (\tilde{V}_2 \cap S),$$

la famille ordonnée d'éléments de S qu'on obtient en joignant $\tilde{\mathcal{C}}$, $\tilde{\mathcal{B}}_1$ et $\tilde{\mathcal{B}}_2$ est linéairement indépendante sur $\tilde{K}$. Par suite, il existe une famille ordonnée $\mathcal{B}$ d'éléments de $\mathcal{O}^n$ dont l'image $\tilde{\mathcal{B}}$ sous τ^n, jointe à cette dernière, constitue une base de S. On définit simplement R comme le sous-espace de K^n engendré par $\mathcal{C}$, $\mathcal{B}_1$, $\mathcal{B}_2$ et $\mathcal{B}$. Alors, on a $S \subseteq \tilde{R}$ mais aussi

$$\dim_{\tilde{K}}(\tilde{R}) = \dim_K(R) \leq \dim_{\tilde{K}}(S),$$

d'où l'égalité $S = \tilde{R}$. De plus, pour $i = 1, 2$, si on pose $W_i = V_i \cap R$, on a $\tilde{W}_i \supseteq \tilde{V}_i \cap S$ car W_i contient $\mathcal{B}_i$ et $\mathcal{C}$, mais on a aussi $\tilde{W}_i \subseteq \tilde{V}_i \cap S$ car $\tilde{R} = S$. On en déduit $\tilde{W}_i = \tilde{V}_i \cap S$. Donc R possède toutes les propriétés annoncées.

Lemme 4.8. *Soit d_1 un entier positif, soient $T_1, \ldots, T_{d_1}$ des entiers ≥ 0, soit G_1 le groupe $\mathbf{G}_{\mathrm{m}}^{d_1}$ plongé dans $\mathbf{A}^{d_1}$ de la manière usuelle, soit H_1 un sous-groupe algébrique de G_1 incomplètement défini dans G_1 par des polynômes de $\mathbf{C}[Y_1, \ldots, Y_{d_1}]$ de degré $\leq T_i$ en Y_i pour $i = 1, \ldots, d_1$ et soit Φ_1 le sous-groupe de $\mathbf{Z}^{d_1}$ constitué des éléments φ de $\mathbf{Z}^{d_1}$ pour lesquels le monôme Y^φ induit le caractère trivial sur H_1. Alors, Φ_1 possède une base constituée d'éléments $(a_1, \ldots, a_{d_1})$ avec $|a_i| \leq d_1 T_i$ pour $i = 1, \ldots, d_1$.*

Démonstration. Soit E l'ensemble des éléments $(a_1, \ldots, a_{d_1})$ de $\mathbf{Z}^{d_1}$ qui vérifient $0 \leq a_i \leq T_i$ pour $i = 1, \ldots, d_1$ et soit J l'idéal de $K[Y_1, \ldots, Y_{d_1}]$ engendré par les polynômes $Y^\alpha - Y^\beta$ avec $\alpha, \beta \in E$ et $\alpha - \beta \in \Phi_1$. On observe d'abord que J contient tout polynôme de $K[Y_1, \ldots, Y_{d_1}]$ qui s'annule sur H_1 et dont le degré en Y_i est $\leq T_i$ pour $i = 1, \ldots, d_1$.

En effet, soit P un tel polynôme et soit R un sous-ensemble maximal d'éléments de E incongrus modulo Φ_1. Modulo J, on peut écrire $P \equiv \sum_{\alpha \in R} p_\alpha Y^\alpha$. Or, les monômes Y^α avec $\alpha \in R$ définissent des caractères distincts de H_1. En vertu d'un théorème d'Artin, ces caractères sont linéairement indépendants sur K. Comme P et les éléments de J s'annulent sur H_1, on en déduit que tous les p_α sont nuls, c'est-à-dire que $P \in J$.

Soit H l'ensemble des zéros de J dans G_1. Comme $H_1 \subseteq H$, le résultat ci-dessus implique que les groupes H_1 et H ont la même dimension. Donc Φ_1 est de même rang que son sous-groupe Φ engendré par les points $\alpha - \beta$ avec $\alpha, \beta \in E$ et $\alpha - \beta \in \Phi_1$. Soit r le rang commun de ces deux groupes et soit

$$C = \{(x_1, \ldots, x_{d_1}) \in \mathbf{R}^{d_1}\ ;\ |x_1| \leq T_1, \ldots, |x_{d_1}| \leq T_{d_1}\}.$$

Comme Φ est engendré par des éléments de C, ses minima successifs par rapport à ce convexe sont tous ≤ 1. Alors, les minima successifs de Φ_1 par rapport à C sont aussi ≤ 1 et, d'après un argument de K. Mahler (voir thm. 1 de [15] ou §10.2 de [10]), on en déduit que rC contient une base de Φ_1 en tant que $\mathbf{Z}$-module.

Démonstration du théorème 4.1.

On note comme d'habitude $\pi_0\colon \mathbf{A}^{d_0+d_1} \to \mathbf{A}^{d_0}$ la projection sur les d_0 premières composantes et $\pi_1\colon \mathbf{A}^{d_0+d_1} \to \mathbf{A}^{d_1}$ celle sur les d_1 dernières composantes. Alors, le groupe H s'écrit $H_0 \times H_1$ où $H_0 = \pi_0(H)$ et $H_1 = \pi_1(H)$ sont respectivement des sous-groupes algébriques de $G_0 = \mathbf{G}_{\mathrm{a}}^{d_0}$ et $G_1 = \mathbf{G}_{\mathrm{m}}^{d_1}$ définis sur $\tilde{K}$. De plus, H_1 est incomplètement défini dans G_1 par des polynômes de $\tilde{K}[Y_1, \ldots, Y_{d_1}]$ de degré $\leq T_i$ en Y_i pour $i = 1, \ldots, d_1$. On démontre l'existence du groupe L par des réductions successives.

1) On choisira le groupe algébrique L de la forme $L_0 \times H_1$ où L_0 est un sous-groupe algébrique de $\mathbf{G}_{\mathrm{a}}^{d_0}$ défini sur K de même dimension que H_0 et qu'il reste à déterminer. La condition (i) sera alors vérifiée.

2) On désigne par Σ' l'ensemble des produits $\gamma\delta^{-1}$ avec $\gamma, \delta \in \Sigma$. Alors, pour tout $\gamma \in \Sigma'$, on a

$$\pi_1(\gamma) \in H_1 \Longleftrightarrow \pi_1(\tilde{\gamma}) \in H_1.$$

En effet, soit Φ_1 le sous-groupe de $\mathbf{Z}^{d_1}$ constitué des éléments $\varphi \in \mathbf{Z}^{d_1}$ pour lesquels le monôme $Y^\varphi \in \mathbf{Z}[Y_1^{\pm 1}, \ldots, Y_{d_1}^{\pm 1}]$ induit le caractère trivial sur H_1. Le lemme 4.8 montre que Φ_1 possède une base $\{\varphi_1, \ldots, \varphi_r\}$ constituée d'éléments de la forme $(a_1, \ldots, a_{d_1})$ avec $|a_i| \le d_1 T_i$ pour $i = 1, \ldots, d_1$. Alors, le groupe H_1 est l'ensemble des zéros dans G_1 des fonctions $Y^{\varphi_i} - 1$ avec $i = 1, \ldots, r$. Or, pour tout $\gamma \in \Sigma'$ et tout $i = 1, \ldots, r$, le nombre $\pi_1(\gamma)^{\varphi_i} - 1$ est un élément de $\mathcal{O}$ de hauteur $\le 2d_1 \sum_{i=1}^{d_1} T_i \log A_i' < D$. Donc, grâce au lemme 4.2, on trouve

$$\begin{aligned} \pi_1(\gamma) \in H_1(K) &\Longleftrightarrow \pi_1(\gamma)^{\varphi_i} - 1 = 0 \quad (i = 1, \ldots, r) \\ &\Longleftrightarrow \pi_1(\tilde{\gamma})^{\varphi_i} - 1 = 0 \quad (i = 1, \ldots, r) \\ &\Longleftrightarrow \pi_1(\tilde{\gamma}) \in H_1(\tilde{K}). \end{aligned}$$

3) On choisira aussi le groupe L_0 de telle sorte que $L_0(K)$ contienne l'ensemble

$$E = \{\pi_0(\gamma)\,;\, \gamma \in \Sigma',\ \pi_0(\tilde{\gamma}) \in H_0(\tilde{K})\}.$$

Alors, la condition (ii) sera elle-aussi satisfaite.

En effet, pour tout $\gamma \in \Sigma'$ tel que $\tilde{\gamma} \in H(\tilde{K})$, on a d'une part $\pi_1(\tilde{\gamma}) \in H_1(\tilde{K})$, donc $\pi_1(\gamma) \in H_1(K)$ en vertu de 2), et d'autre part $\pi_0(\tilde{\gamma}) \in H_0(\tilde{K})$, donc $\pi_0(\gamma) \in E \subset L_0(K)$; en conclusion $\gamma \in L(K)$. On en déduit que, pour tout couple d'éléments γ, δ de Σ, on a

$$\tilde{\gamma} \equiv \tilde{\delta} \bmod H(\tilde{K}) \Longrightarrow \gamma \equiv \delta \bmod L(K)$$

en appliquant cette dernière observation à l'élément $\gamma\delta^{-1}$ de Σ'. Cela démontre (ii).

4) Avant de poursuivre, on observe que $\{w_1, \ldots, w_{\ell_0}\}$ est une base de $W \cap \mathcal{O}^d$ et que, par suite, la définition de $\tilde{W}$ donnée dans l'énoncé du théorème 4.1 coïncide la définition de $\tilde{W}$ pour un sous-espace quelconque W de $T_G(K) = K^d$.

En effet, soit M la matrice $d \times \ell_0$ dont les colonnes sont $w_1, \ldots, w_{\ell_0}$. Alors, M est de rang ℓ_0 et, si Δ désigne un mineur non nul d'ordre ℓ_0 de cette matrice, on a

$$\mathbf{h}_1(\Delta) \le \sum_{j=1}^{\ell_0} \mathbf{h}_1(w_j) \le \ell_0 \log B_2 < D,$$

donc $\mathrm{ord}_{\mathbf{p}}(\Delta) = 0$ en vertu du lemme 4.2. Cela montre $\mathrm{ord}_{\mathbf{p}}(w_1 \wedge \ldots \wedge w_{\ell_0}) = 0$, et l'affirmation à vérifier découle du lemme 4.3.

5) En vertu du lemme 4.3, on a $\dim_K(W) = \dim_{\tilde{K}}(\tilde{W})$. La condition (iii) sera donc remplie si on choisit L_0 de telle sorte que

$$\dim_K(W \cap T_L(K)) \ge \dim_{\tilde{K}}(\tilde{W} \cap T_H(\tilde{K})). \tag{4.5}$$

6) On pose $V = W \cap (K^{d_0} \times T_{H_1}(K))$. Alors, la condition (4.5) sera remplie si on choisit L_0 de telle sorte que

$$\dim_K(V \cap (L_0(K) \times K^{d_1})) \ge \dim_{\tilde{K}}(\tilde{V} \cap (H_0(\tilde{K}) \times \tilde{K}^{d_1})). \tag{4.6}$$

En effet, on a

$$\mathbf{h}(W) \le \ell_0 \log B_2 \quad \text{et} \quad \mathbf{h}(K^{d_0} \times T_{H_1}(K)) = 0$$

car $K^{d_0} \times T_{H_1}(K)$ est un sous-espace de K^d défini sur $\mathbf{Q}$. Comme la somme de ces deux hauteurs est $< D$, le lemme 4.5 donne

$$\mathbf{h}(V) \le \ell_0 \log B_2 \quad \text{et} \quad \tilde{V} = \tilde{W} \cap (\tilde{K}^{d_0} \times T_{H_1}(\tilde{K})).$$

On obtient donc les égalités

$$\begin{aligned} W \cap T_L(K) &= W \cap \big(L_0(K) \times T_{H_1}(K)\big) = V \cap \big(L_0(K) \times K^{d_1}\big) \\ \tilde{W} \cap T_H(\tilde{K}) &= \tilde{W} \cap \big(H_0(\tilde{K}) \times T_{H_1}(\tilde{K})\big) = \tilde{V} \cap \big(H_0(\tilde{K}) \times \tilde{K}^{d_1}\big), \end{aligned}$$

indépendamment du choix de L_0. On en déduit que les conditions (4.5) et (4.6) sont équivalentes.

7) Soit $V_1 = \pi_0(V)$. L'inégalité (4.6) est vérifiée si on choisit L_0 tel que

$$\dim_K(V_1 \cap L_0(K)) \ge \dim_{\tilde{K}}(\tilde{V}_1 \cap H_0(\tilde{K})). \tag{4.7}$$

En effet, soit $V_0 = V \cap (0 \times K^{d_1})$ le noyau de la restriction de π_0 à V. On obtient la suite exacte

$$0 \longrightarrow V_0 \xrightarrow{i} V \cap (L_0(K) \times K^{d_1}) \xrightarrow{\pi_0} V_1 \cap L_0(K) \longrightarrow 0$$

qui montre que, quel que soit L_0, le membre de gauche de (4.6) est la somme des dimensions de V_0 et de $V_1 \cap L_0(K)$. Comme $\mathbf{h}(V) < D$ et $\mathbf{h}(0 \times K^{d_1}) = 0$, le lemme 4.5 donne $\tilde{V}_0 = \tilde{V} \cap (0 \times \tilde{K}^{d_1})$, c'est-à-dire que $\tilde{V}_0$ est le noyau de la restriction de π_0 à $\tilde{V}$. Le lemme 4.6 donne aussi $\mathbf{h}(V_1) \le \mathbf{h}(V)$ et, comme $\mathbf{h}(V) < D$, il donne en plus $\tilde{V}_1 = \pi_0(\tilde{V})$. Donc, on a aussi une suite exacte

$$0 \longrightarrow \tilde{V}_0 \xrightarrow{i} \tilde{V} \cap (H_0(\tilde{K}) \times \tilde{K}^{d_1}) \xrightarrow{\pi_0} \tilde{V}_1 \cap H_0(\tilde{K}) \longrightarrow 0$$

qui nous apprend que le membre de droite de (4.6) est la somme des dimensions de $\tilde{V}_0$ et de $\tilde{V}_1 \cap H_0(\tilde{K})$. Comme $\dim_K(V_0) = \dim_{\tilde{K}}(\tilde{V}_0)$, les conditions (4.6) et (4.7) sont équivalentes.

8) En vertu de 7), il suffit, pour conclure, de montrer l'existence d'un sous-espace R de K^{d_0}, de même dimension sur K que $H_0(\tilde{K})$ sur $\tilde{K}$, qui contient E et qui vérifie

$$\dim_K(V_1 \cap R) \ge \dim_{\tilde{K}}(\tilde{V}_1 \cap H_0(\tilde{K})).$$

On définira alors L_0 comme étant le sous-groupe algébrique de $\mathbf{G}_{\mathrm{a}}^{d_0}$ défini sur K pour lequel $L_0(K) = R$.

Pour montrer l'existence de R, on désigne par V_2 le sous-espace de K^{d_0} engendré par E et on pose $U = V_1 \cap V_2$. Comme $\mathbf{h}(V_1) \le \mathbf{h}(V) \le \ell_0 \log B_2$ et $\mathbf{h}(V_2) \le 2d_0 \log B_1$, on trouve $\mathbf{h}(V_1) + \mathbf{h}(V_2) < D$ ce qui, suivant le lemme 4.5, entraîne $\tilde{U} = \tilde{V}_1 \cap \tilde{V}_2$. En vertu du lemme 4.7, il existe donc un sous-espace R de K^{d_0} avec $\tilde{R} = H_0(\tilde{K})$ et

$$\dim_K(V_i \cap R) \ge \dim_{\tilde{K}}(\tilde{V}_i \cap H_0(\tilde{K})) \tag{4.8}$$

pour $i = 1, 2$. On en déduit $\dim_K(R) = \dim_{\tilde{K}}(H_0(\tilde{K}))$. Pour conclure, il reste seulement à montrer $E \subset R$, c'est-à-dire $V_2 \subseteq R$. Pour le voir, on choisit dans E une base $\{x_1, \ldots, x_m\}$ de V_2. Puisque cette base est contenue dans $\mathcal{O}^{d_0}$ et vérifie

$$\mathbf{h}_1(x_1 \wedge \ldots \wedge x_m) \le 2d_0 \log B_1,$$

les lemmes 4.2 et 4.3 montrent qu'il s'agit d'une base régulière de V_2. Ainsi, $\{\tilde{x}_1, \ldots, \tilde{x}_m\}$ est une base de $\tilde{V}_2$. Comme $\tilde{x} \in H_0(\tilde{K})$ pour tout $x \in E$, cela implique $\tilde{V}_2 \subseteq H_0(\tilde{K})$. Donc, pour $i = 2$, l'inégalité (4.8) devient $\dim_K(V_2 \cap R) = \dim_{\tilde{K}}(\tilde{V}_2)$. On en tire $V_2 \subseteq R$ comme requis.

5. Construction d'un sous-groupe algébrique

Reprenons les notations du paragraphe 2. Nous allons combiner les résultats des paragraphes 2, 3 et 4 pour montrer:

Théorème 5.1. *Soit $K \subset \mathbf{C}$ un corps de type fini et de degré de transcendance 1 sur $\mathbf{Q}$, soit W un sous-espace de $T_G(K)$, soit Y un sous-groupe de $T_G(\mathbf{C})$ de type fini dont l'image Γ sous $\exp_G$ est contenue dans $G(K)$, et soit Y_a un sous-groupe de Y dont l'image Γ_a sous $\exp_G$ est contenue dans $G_0(K) \times G_1(K \cap \overline{\mathbf{Q}})$. On désigne par λ le rang de Γ et par n la dimension du sous-espace de $T_G(\mathbf{C})$ engendré par W et Y. Alors, il existe un sous-groupe algébrique connexe L de G, distinct de G et défini sur K, tel que, si on pose*

$$d' = \dim(G/L), \quad d'_0 = \dim(G_0/\pi_0(L)), \quad d'_1 = \dim(G_1/\pi_1(L)),$$

$$\ell'_0 = \dim_K((W + T_L(K))/T_L(K)),$$

$$\lambda' = \mathrm{rang}_{\mathbf{Z}}((\Gamma + L(K))/L(K)) \quad et \quad \lambda'_a = \mathrm{rang}_{\mathbf{Z}}((\Gamma_a + L(K))/L(K)),$$

on ait

$$\big((d-2n) + \epsilon(n-d_0)\big)(d'_1 + \lambda') \le d_1\big((d' - \ell'_0) + \epsilon(\ell'_0 - d'_0) - \epsilon^2 \lambda'_a\big), \tag{5.1}$$

pour tout nombre réel positif $\epsilon \le (2d(d+\lambda)+1)^{-1}$.

Au paragraphe suivant, on montrera comment, par des manipulations algébriques, on en déduit le théorème 1.1.

Rappelons que nous utilisons ici deux notions de hauteur. L'une est la version affine de la hauteur logarithmique absolue de Weil sur $\overline{\mathbf{Q}}$, qu'on note h_1, et l'autre est son analogue pour le corps K vu comme corps de fonctions en une variable sur $\mathbf{Q}$, qu'on note $\mathbf{h}_1$ (voir §2 et §4).

Démonstration du théorème 5.1.

Soient ℓ_0 la dimension de W, ℓ_1 le rang de Y et ℓ_a le rang de Y_a. Quitte, par exemple, à remplacer Y_a par l'ensemble de tous les points $\eta \in Y$ tels que $\exp_G(\eta) \in G_0(K) \times G_1(K \cap \overline{\mathbf{Q}})$, on peut supposer que le quotient Y/Y_a est sans torsion. Cela permet de compléter une base $\{\eta_1, \dots, \eta_{\ell_a}\}$ de Y_a en une base $\{\eta_1, \dots, \eta_{\ell_1}\}$ de Y. Fixons un tel choix de bases de Y et Y_a et choisissons aussi une base $\{w_1, \dots, w_{\ell_0}\}$ de W en tant qu'espace vectoriel sur K. On pose $\gamma_j = \exp_G(\eta_j)$ pour $j = 1, \dots, \ell_1$. Alors, $\{\gamma_1, \dots, \gamma_{\ell_1}\}$ constitue un système de générateurs du groupe Γ, et $\{\gamma_1, \dots, \gamma_{\ell_a}\}$ un système de générateurs de son sous-groupe Γ_a. Notons qu'en vertu du choix de Y_a, on a

$$\pi_1(\gamma_1), \dots, \pi_1(\gamma_{\ell_a}) \in G_1(\overline{\mathbf{Q}}).$$

On peut aussi supposer

$$d > 2n > 0, \quad n \ge d_0 \quad \text{et} \quad d_1 > 0.$$

En effet, si $n < d_0$, alors W et Y sont contenus dans $T_L(\mathbf{C})$ où L est un sous-groupe algébrique de G défini sur K de la forme $L_0 \times G_1$ avec $L_0 \ne G_0$. Pour ce choix de L, le théorème 5.1 est vérifié car les entiers d'_1, ℓ'_0, λ' et λ'_a sont nuls et l'inégalité (5.1) se résume à $0 \le (1-\epsilon)d_1 d'_0$. Cela permet de supposer $n \ge d_0$. Si $n = 0$ ou si $d \le 2n$, le théorème 5.1 est vérifié avec L réduit à l'élément neutre. Pour le montrer on distingue trois cas. Si $d < 2n$, le membre de gauche de (5.1) est ≤ 0 tandis que celui de droite est $\ge \epsilon d_1(d_1 - 1/2) \ge 0$. Si $d = 2n$, on a $n > 0$ et $d_1 > 0$; le membre de gauche de (5.1) est $\le 1/2$ et celui de droite est $\ge d_1 n/2 \ge 1/2$. Enfin, si $n = 0$, on a $d_0 = 0$ et les deux membres de (5.1) se réduisent à d_1^2. Cela permet de supposer $n > 0$ et $d > 2n$. Alors, on a aussi $d_1 > 0$.

On observe encore que si $Y \subset T_{G_0\times 1}(\mathbf{C})$, alors le théorème 5.1 est vérifié avec $L = G_0 \times \{1\}$. En effet, pour ce choix de L, on a bien $L \neq G$ car $d_1 > 0$, et on obtient $\lambda'_a = \lambda' = d'_0 = 0$ et $d'_1 = d_1$. De plus, comme $\ell'_0 \leq n$ et $d_0 \leq n$, on trouve que le membre de gauche de (5.1) est $\leq d_1(d_1 - n)$ et que celui de droite est $\geq d_1(d_1 - n)$. Cette remarque permet de supposer que $\eta_1, \dots, \eta_{\ell_1}$ ne sont pas tous contenus dans $T_{G_0\times 1}(\mathbf{C})$.

Le théorème 3.1 montre qu'il existe une constante $c > 1$ qui ne dépend que de K, des w_j et des γ_j, et qui possède la propriété suivante:

Soit κ un nombre réel $\geq c$. Pour une infinité d'entiers D, il existe une place $\mathbf{p}$ de K de degré D et un plongement de son corps résiduel $\tilde{K}$ dans $\mathbf{C}$ tels que si $\mathcal{O}$ désigne l'anneau de valuation de $\mathbf{p}$, alors, pour $i = 1, \dots, d$, les nombres $w_1^{(i)}, \dots, w_{\ell_0}^{(i)}$ et $\gamma_1^{(i)}, \dots, \gamma_{\ell_1}^{(i)}$ appartiennent à $\mathcal{O}$ et, si $\tilde{w}_1^{(i)}, \dots, \tilde{w}_{\ell_0}^{(i)}$ et $\tilde{\gamma}_1^{(i)}, \dots, \tilde{\gamma}_{\ell_1}^{(i)}$ désignent leurs images respectives sous l'homomorphisme de réduction $\tau\colon \mathcal{O} \to \tilde{K}$ associé à τ, alors on a:

$$
\begin{aligned}
& h_1(\tilde{w}_j^{(1)}, \dots, \tilde{w}_j^{(d)}) \leq \kappa \quad (1 \leq j \leq \ell_0), \\
& h_1(\tilde{\gamma}_1^{(i)}, \dots, \tilde{\gamma}_{\ell_1}^{(i)}) \leq \kappa \quad (1 \leq i \leq d), \\
& |w_j^{(i)} - \tilde{w}_j^{(i)}| \leq \exp(-c^{-1}\kappa D^2) \quad (1 \leq i \leq d,\ 1 \leq j \leq \ell_0), \\
\text{et}\quad & |\gamma_j^{(i)} - \tilde{\gamma}_j^{(i)}| \leq \exp(-c^{-1}\kappa D^2) \quad (1 \leq i \leq d,\ 1 \leq j \leq \ell_1),
\end{aligned}
\tag{5.2}
$$

avec en plus $\tilde{\gamma}_j^{(i)} = \gamma_j^{(i)}$ pour $i = d_0 + 1, \dots, d$ et $j = 1, \dots, \ell_a$.

Fixons donc le choix d'un nombre réel $\kappa \geq c$ très grand, et choisissons une place $\mathbf{p}$, comme ci-dessus, de degré $D \geq \exp(\exp(\kappa))$. En vertu du lemme 4.2, non seulement les points $\gamma_1, \dots, \gamma_{\ell_1}$ mais aussi leurs inverses dans $G(K)$ ont leurs coordonnées dans $\mathcal{O}$, et aucune des d_1 dernières coordonnées de ces $2\ell_1$ points ne s'annule sous τ. Il en va donc de même de tout point de Γ. Pour tout $\gamma \in \Gamma$, on désigne par $\tilde{\gamma}$ le point de $\tilde{K}^d$ dont les coordonnées sont les images sous τ de celles de γ. Alors, chacun de ces points $\tilde{\gamma}$ appartient à $G(\tilde{K})$ et leur ensemble forme un sous-groupe $\tilde{\Gamma}$ de $G(\tilde{K})$. De plus, en vertu du choix de $\mathbf{p}$, on a

$$\pi_1(\tilde{\gamma}_j) = \pi_1(\gamma_j) \qquad (1 \leq j \leq \ell_a).$$

On pose aussi $\tilde{w}_j = (\tilde{w}_j^{(1)}, \dots, \tilde{w}_j^{(d)})$ pour $j = 1, \dots, \ell_0$ et on note $\tilde{W}$ le sous-espace de $T_G(\tilde{K})$ engendré par ces ℓ_0 points. En vertu des inégalités (5.2), on a

$$\|w_j - \tilde{w}_j\| \leq \exp(-c^{-1}\kappa D^2) \quad (1 \leq j \leq \ell_0)$$

et on observe que, si κ est assez grand, alors, pour $j = 1, \dots, \ell_1$, il existe un point $\tilde{\eta}_j$ de $T_G(\mathbf{C})$ tel que

$$\exp_G(\tilde{\eta}_j) = \tilde{\gamma}_j \quad \text{et} \quad \|\eta_j - \tilde{\eta}_j\| \leq \exp(-(2c)^{-1}\kappa D^2).$$

On définit des entiers $S_0, S_1, \dots, S_{\ell_1}$ et $T_0, T_1, \dots, T_{d_1}$ en posant

$$
\begin{aligned}
& S_0 = T_0 = \left[\frac{\kappa D}{(\log \kappa)(\log D)}\right], \\
& T_1 = \cdots = T_{d_1} = \left[\left((\log \kappa)^d \kappa^{n-d_0} (\log D)^{d_0-n} D^{2n-d_0}\right)^{1/d_1}\right], \\
& S_1 = \cdots = S_{\ell_a} = \left[\frac{\kappa D}{(\log \kappa)^2 T_1}\right] \\
\text{et}\qquad & S_{\ell_a+1} = \cdots = S_{\ell_1} = \left[\frac{D}{(\log \kappa)^2 T_1}\right].
\end{aligned}
$$

Comme $d > 2n > 0$ et $n \geq d_0$, on trouve que, pour κ assez grand, on a

$$D^{1/(2d_1)} < T_1 < D^{1-1/(2d_1)}.$$

On pose $N = (S_1+1)\cdots(S_{\ell_1}+1)$ et

$$\Sigma = \{\gamma_1^{s_1}\cdots\gamma_{\ell_1}^{s_{\ell_1}}\,;\,0\le s_1\le S_1,\ldots,0\le s_{\ell_1}\le S_{\ell_1}\}.$$

Comme Σ est un ensemble de cardinalité $\le N$ qui contient $\gamma_1,\ldots,\gamma_{\ell_1}$, on peut numéroter ses éléments en écrivant, avec des répétitions possibles, $\Sigma = \{\gamma_1,\ldots,\gamma_N\}$. Soit $\tilde\Sigma = \{\tilde\gamma_1,\ldots,\tilde\gamma_N\}$. Pour chaque $j = \ell_1+1,\ldots,N$, on choisit une écriture de γ_j sous la forme $\gamma_j = \gamma_1^{s_1}\cdots\gamma_{\ell_1}^{s_{\ell_1}}$ avec des entiers $s_1,\ldots,s_{\ell_1}$ qui vérifient $0\le s_m\le S_m$ pour $m=1,\ldots,\ell_1$, et on pose

$$\eta_j = s_1\eta_1+\cdots+s_{\ell_1}\eta_{\ell_1} \quad \text{et} \quad \tilde\eta_j = s_1\tilde\eta_1+\cdots+s_{\ell_1}\tilde\eta_{\ell_1}.$$

Alors, pour $j=1,\ldots,N$, on a $\gamma_j = \exp_G(\eta_j)$, $\tilde\gamma_j = \exp_G(\tilde\eta_j)$ et, si κ est assez grand, on trouve

$$\|\eta_j-\tilde\eta_j\| \le \exp\big(-(4c)^{-1}\kappa D^2\big).$$

On définit aussi des nombres réels positifs $A_1,\ldots,A_{d_1}$, $A'_1,\ldots,A'_{d_1}$, B_1, B_2, E, U et V en posant

$$A_1=\cdots=A_{d_1}=\exp\Big(\frac{\kappa D}{T_1\log\kappa}\Big), \qquad A'_1=\cdots=A'_{d_1}=\exp\Big(\frac{D}{T_1\log\kappa}\Big),$$

$$B_1=B_2=E=D, \qquad V=(4c)^{-1}\kappa D^2 \quad\text{et}\quad U=(12d+13)^{-1}V.$$

On peut vérifier que, pour κ assez grand et pour le choix de paramètres établi ci-dessus, toutes les hypothèses du théorème 2.1 sont remplies. Par exemple, le sous-espace de $T_G(\mathbf{C})$ engendré par $w_1,\ldots,w_{\ell_0}$ et $\eta_1,\ldots,\eta_N$ est de dimension n car il coïncide avec celui engendré par W et Y. Nous allons encore vérifier les trois inégalités concernant la hauteur, les autres contraintes étant plus ou moins immédiates.

Pour κ assez grand, on trouve en effet, pour $i=1,\ldots,d_0$,

$$\begin{aligned} h_1(\tilde\gamma_1^{(i)},\ldots,\tilde\gamma_N^{(i)}) &\le \log(S_1+\cdots+S_{\ell_1}) + h_1(\tilde\gamma_1^{(i)},\ldots,\tilde\gamma_{\ell_1}^{(i)})\\ &\le \log(\ell_1\kappa D^{1-1/(2d_1)})+\kappa\\ &\le \log D\ , \end{aligned}$$

pour $j=1,\ldots,\ell_0$,

$$h_1(\tilde w_j^{(1)},\ldots,\tilde w_j^{(d)}) \le \kappa \le \log D\ ,$$

et, pour $i=1,\ldots,d_1$ et $j=1,\ldots,N$,

$$\begin{aligned} h_1(\tilde\gamma_j^{(d_0+i)}) &\le \sum_{m=1}^{\ell_1} S_m h_1(\tilde\gamma_m^{(d_0+i)})\\ &\le \sum_{m=1}^{\ell_a} S_m h_1(\gamma_m^{(d_0+i)}) + \sum_{m=\ell_a+1}^{\ell_1} S_m\kappa\\ &\le \frac{\kappa D}{(\log\kappa)^2 T_1}\Big(\sum_{m=1}^{\ell_a} h_1(\gamma_m^{(d_0+i)})+\ell_1\Big)\\ &\le \log A_i \end{aligned}$$

et

$$\begin{aligned} \frac{E}{D}|\tilde\eta_j^{(d_0+i)}| &\le \sum_{m=1}^{\ell_1} S_m\|\tilde\eta_m\|\\ &\le \frac{\kappa D}{(\log\kappa)^2 T_1}\sum_{m=1}^{\ell_1}(\|\eta_m\|+1)\\ &\le \log A_i. \end{aligned}$$

De même, les conditions du théorème 4.1 sont remplies pour ce choix de paramètres, en prenant pour groupe H le sous-groupe algébrique de G que fournit la conclusion du théorème 2.1. En effet, pour $i = 1, \dots, d_0$ et $j = 1, \dots, \ell_0$, les quantités $\mathbf{h}_1(\gamma_1^{(i)}, \dots, \gamma_N^{(i)})$ et $\mathbf{h}_1(w_j^{(1)}, \dots, w_j^{(d)})$ sont bornées par des constantes qui ne dépendent que de $w_1, \dots, w_{\ell_0}$ et $\gamma_1, \dots, \gamma_{\ell_1}$. Ces quantités sont donc respectivement majorées par $\log B_1$ et $\log B_2$ pour κ assez grand. De même, pour $i = 1, \dots, d_1$ et $j = 1, \dots, N$ et κ assez grand, on a:

$$\mathbf{h}_1\big(\gamma_j^{(d_0+i)}\big) \le \sum_{m=\ell_a+1}^{\ell_1} S_m \mathbf{h}_1\big(\gamma_m^{(d_0+i)}\big) \le \frac{D}{(\log\kappa)^2 T_1} \sum_{m=\ell_a+1}^{\ell_1} \mathbf{h}_1\big(\gamma_m^{(d_0+i)}\big) \le \log A_i'$$

car $\gamma_1^{(d_0+i)}, \dots, \gamma_{\ell_a}^{(d_0+i)} \in \overline{\mathbf{Q}}$. Ici aussi, les autres contraintes n'impliquent qu'un peu de calcul.

Soit L le sous-groupe algébrique de G que livre le théorème 4.1. Il est connexe car H l'est, et distinct de G car sa fonction d'Hilbert-Samuel est égale à celle de H et que H est distinct de G. Il est aussi défini sur K et, en employant les notations du théorème 5.1, on trouve, grâce aux théorèmes 2.1 et 4.1:

$$\begin{aligned} S_0^{\ell_0'} &\operatorname{Card}\big((\Sigma + L(K))/L(K)\big) \cdot \mathcal{H}(L; T_0, T_1, \dots, T_{d_1}) \\ &\le S_0^{\tilde\ell_0} \operatorname{Card}\big((\tilde\Sigma + H(\tilde K))/H(\tilde K)\big) \cdot \mathcal{H}(H; T_0, T_1, \dots, T_{d_1}) \\ &\le \frac{d!}{d_0!} T_0^{d_0} T_1 \cdots T_{d_1}. \end{aligned}$$

On a d'une part

$$\mathcal{H}(L; T_0, T_1, \dots, T_{d_1}) \ge T_0^{d_0 - d_0'} T_1^{d_1 - d_1'},$$

et d'autre part

$$\operatorname{Card}\Big(\big(\Sigma + L(K)\big)/L(K)\Big) \ge S_1^{\lambda_a'} S_{\ell_1}^{\lambda' - \lambda_a'}.$$

On en déduit

$$S_0^{\ell_0'} S_1^{\lambda_a'} S_{\ell_1}^{\lambda' - \lambda_a'} \le \frac{d!}{d_0!} T_0^{d_0'} T_1^{d_1'}.$$

En tenant compte du choix des paramètres, on peut réécrire cette dernière inégalité sous la forme

$$\Big(\frac{D}{T_1(\log\kappa)^2}\Big)^{\lambda' + d_1'} \le (\log\kappa)\kappa^{-\lambda_a'} T_0^{d_0' - \ell_0'} \Big(\frac{D}{(\log\kappa)^2}\Big)^{d_1'},$$

avec l'introduction d'un facteur $\log\kappa$ pour s'affranchir des constantes. Si on prend les logarithmes des deux membres de cette inégalité et qu'on les multiplie par $d_1/\log D$, on trouve

$$\begin{aligned} &\big((d-2n) + \epsilon_1(n - d_0) + \epsilon_2(d_0 - n) - \epsilon_3(d + 2d_1)\big)(d_1' + \lambda') \\ &\qquad \le d_1\big((d' - \ell_0') + \epsilon_1(\ell_0' - d_0') + \epsilon_2(d_0' - \ell_0' - \lambda_a') + \epsilon_3(1 + \ell_0')\big), \end{aligned} \tag{5.3}$$

où

$$\epsilon_1 = \frac{\log\log D}{\log D}, \quad \epsilon_2 = \frac{\log\kappa}{\log D} \quad \text{et} \quad \epsilon_3 = \frac{\log\log\kappa}{\log D}.$$

Or, les coefficients des ϵ_i dans les deux membres de (5.3) sont des entiers de valeur absolue $\le 3d(d+\lambda)$. Donc, si on choisit κ suffisamment grand pour que les nombres ϵ_1, ϵ_2/ϵ_1 et ϵ_3/ϵ_2 soient tous $< (6d(d+\lambda)+1)^{-1}$, alors (5.3) implique

$$(d - 2n)(d_1' + \lambda') \le d_1(d' - \ell_0') \tag{5.4}$$

et, en cas d'égalité dans (5.4),

$$(n - d_0)(d_1' + \lambda') \le d_1(\ell_0' - d_0') \tag{5.5}$$

et, en cas d'égalité dans (5.4) et (5.5),

$$(d_0 - n)(d_1' + \lambda') \le d_1(d_0' - \ell_0' - \lambda_a')$$

c'est-à-dire $\lambda_a' = 0$, par comparaison avec (5.5). Comme λ_a' et chacun des nombres apparaissant dans les deux membres de (5.4) et (5.5) sont des entiers de valeur absolue $\le d(d+\lambda)$, ce résultat est équivalent à l'inégalité (5.1) du théorème quelque soit ϵ avec $0 < \epsilon \le (2d(d+\lambda)+1)^{-1}$. Le théorème est démontré.

6. Démonstration du résultat principal

Le but de ce paragraphe est de montrer comment le théorème 1.1 se déduit du théorème 5.1. Pour cela, on utilise un résultat général qui s'énonce en termes de catégories (proposition 2.1 de [19]). On rappelle d'abord le contexte dans lequel il s'inscrit.

Soit $\mathcal{C}$ une catégorie qui possède un objet nul. Dans cette catégorie, on dit qu'un morphisme est un *noyau* (resp. un *conoyau*) s'il est noyau (resp. conoyau) d'un morphisme de $\mathcal{C}$. On dit que la catégorie $\mathcal{C}$ est *admissible* si elle vérifie les deux conditions suivantes:
(i) tout morphisme de $\mathcal{C}$ admet à la fois un noyau et un conoyau;
(ii) la composée de deux noyaux de $\mathcal{C}$ (resp. de deux conoyaux de $\mathcal{C}$), lorsqu'elle est définie, est encore un noyau de $\mathcal{C}$ (resp. un conoyau de $\mathcal{C}$).
On note $\mathrm{Ob}(\mathcal{C})$ la collection des objets de $\mathcal{C}$, et $\mathbf{N}$ l'ensemble des entiers rationnels ≥ 0. Enfin, on dit qu'une fonction $a\colon \mathrm{Ob}(\mathcal{C}) \to \mathbf{N}$ est *additive* (resp. *sur-additive*, *resp. sous-additive*) si elle vérifie

$$a(X) = a(X^*) + a(X'), \quad \big(\text{resp. } a(X) \geq a(X^*) + a(X'), \ \text{resp. } a(X) \leq a(X^*) + a(X')\ \big),$$

pour toute paire de morphismes $i\colon X^* \to X$ et $s\colon X \to X'$ de $\mathcal{C}$ qui vérifient les conditions équivalentes suivantes:
(i) i est un noyau et s est un conoyau de i,
(ii) s est un conoyau et i est un noyau de s.

La proposition 2.1 de [19] assure l'équivalence de six énoncés dans une catégorie admissible. Si on ne retient que les premier et sixième de ces énoncés, ce résultat s'énonce ainsi:

Proposition 6.1. *Soient $\mathcal{C}$ une catégorie admissible, et a, b, c, d, r des fonctions définies sur $\mathrm{Ob}(\mathcal{C})$ à valeurs dans $\mathbf{N}$. Supposons que r soit additive, que a et d soient sur-additives, que b et c soient sous-additives et majorées par des fonctions sur-additives, et que a, b, c, d s'annulent en tout objet en lequel r s'annule. Alors, les énoncés suivants sont équivalents:*

Énoncé 1. *Pour tout objet X de $\mathcal{C}$ tel que $b(X) \neq 0$, il existe un conoyau $s\colon X \to X'$ vérifiant*

$$b(X') + d(X') \neq 0 \quad \text{et} \quad \frac{a(X') + c(X')}{b(X') + d(X')} \leq \frac{a(X)}{b(X)} \ .$$

Énoncé 2. *Soit X un objet de $\mathcal{C}$. Supposons $b(X) \neq 0$. Alors, la famille des conoyaux $s\colon X \to X'$ qui vérifient $b(X') \neq 0$ et qui minimisent le rapport $a(X')/b(X')$ est non vide. Soit $s\colon X \to X'$ un membre de cette famille pour lequel $r(X')$ est minimal. Si $c(X') \neq 0$, alors on a*

$$d(X') \neq 0 \quad \text{et} \quad \frac{a(X)}{b(X)} \geq \frac{a(X')}{b(X')} \geq \frac{c(X')}{d(X')} \ .$$

Remarque. Le lecteur qui n'a pas accès à [19] pourra consulter le théorème 3 de [20]. Ce résultat suppose que les fonctions b et c sont additives mais le lecteur vérifiera qu'il suffit de les prendre sous-additives et majorées par des fonctions sur-additives. De plus le résultat en question établit l'équivalence de quatre énoncés au lieu de six. Le premier d'entre eux est l'énoncé 1 de la proposition 6.1. Un peu de travail montre que le quatrième est équivalent à l'énoncé 2 de la proposition 6.1.

On va maintenant construire des catégories admissibles munies de fonctions qui satisfont les hypothèses de la proposition 6.1. Pour celles-ci, on montrera que l'énoncé 1 de la proposition 6.1 est vérifié, en s'appuyant sur le théorème 5.1. On déduira alors le théorème 1.1 du fait que l'énoncé 2 est vérifié pour les mêmes catégories et les mêmes fonctions.

(i) Construction de la catégorie $\mathcal{C}$

Soit K un sous-corps de $\mathbf{C}$ de type fini et de degré de transcendance 1 sur $\mathbf{Q}$. On forme une catégorie $\mathcal{C}$ de la manière suivante:

Un *objet* de $\mathcal{C}$ est une famille

$$X = (d_0, d_1, W, Y, Y_a) \tag{6.1}$$

où d_0, d_1 sont des entiers ≥ 0, W un sous-K-espace vectoriel de $K^{d_0} \times K^{d_1}$, Y un sous-groupe de $\mathbf{C}^{d_0} \times \mathbf{C}^{d_1}$ de type fini contenu dans $K^{d_0} \times (\mathcal{L}_K)^{d_1}$, et Y_a un sous-groupe de Y contenu dans $K^{d_0} \times \mathcal{L}^{d_1}$.

Un *morphisme* de X dans un objet $X' = (d_0', d_1', W', Y', Y_a')$ est la donnée d'une application linéaire

$$g: \mathbf{C}^{d_0} \times \mathbf{C}^{d_1} \longrightarrow \mathbf{C}^{d_0'} \times \mathbf{C}^{d_1'}$$

qui vérifie

$$g(K^{d_0} \times 0) \subseteq K^{d_0'} \times 0, \qquad g(0 \times \mathbf{Q}^{d_1}) \subseteq 0 \times \mathbf{Q}^{d_1'}.$$

$$g(W) \subseteq W', \quad g(Y) \subseteq Y' \quad \text{et} \quad g(Y_a) \subseteq Y_a'.$$

On note $m(g, X, X'): X \to X'$ le morphisme correspondant de X dans X' et on dit que g est l'application linéaire sous-jacente à ce morphisme. On définit enfin la composition des morphismes par la composition des applications linéaires sous-jacentes.

Cette catégorie admet un objet nul, à savoir la famille dont toutes les composantes sont nulles. De plus, étant donné un objet $X^* = (d_0^*, d_1^*, W^*, Y^*, Y_a^*)$ de $\mathcal{C}$ et des morphismes $m(f, X^*, X)$ de X^* dans X et $m(g, X, X')$ de X dans X', on peut montrer que $m(f, X^*, X)$ est un noyau de $m(g, X, X')$ si et seulement si l'application linéaire f est injective, d'image égale au noyau de g et vérifie

$$W^* = f^{-1}(W), \quad Y^* = f^{-1}(Y) \quad \text{et} \quad Y_a^* = f^{-1}(Y_a). \tag{6.2}$$

On peut aussi montrer que $m(g, X, X')$ est un conoyau de $m(f, X^*, X)$ si et seulement si g est surjective de noyau égal à l'image de f et vérifie

$$g(W) = W', \quad g(Y) = Y' \quad \text{et} \quad g(Y_a) = Y_a'. \tag{6.3}$$

On en déduit d'une part que tout morphisme de $\mathcal{C}$ admet à la fois un noyau et un conoyau et d'autre part que les noyaux de $\mathcal{C}$ sont les morphismes de la forme $m(f, X^*, X)$ pour lesquels f est injectif et vérifie 6.2 et que les conoyaux de $\mathcal{C}$ sont les morphismes de la forme $m(g, X, X')$ pour lesquels g est surjectif et vérifie (6.3). Par suite, la catégorie $\mathcal{C}$ est admissible.

(ii) Fonctions sur $\mathrm{Ob}(\mathcal{C})$

On définit des fonctions de $\mathrm{Ob}(\mathcal{C})$ dans $\mathbf{N}$ en posant, pour tout objet X de $\mathcal{C}$ de la forme (6.1),

$$d_0(X) = d_0, \quad d_1(X) = d_1, \quad d(X) = d_0 + d_1,$$

$$\ell_0(X) = \dim_K(W), \quad \ell_1(X) = \mathrm{rang}_{\mathbf{Z}}(Y), \quad \ell_a(X) = \mathrm{rang}_{\mathbf{Z}}(Y_a)$$

$$n(X) = \dim_{\mathbf{C}}(\mathbf{C}W + \mathbf{C}Y),$$

$$\kappa(X) = \mathrm{rang}_{\mathbf{Z}}(Y \cap (0 \times \omega \mathbf{Z}^{d_1})) \quad \text{et} \quad \kappa_a(X) = \mathrm{rang}_{\mathbf{Z}}(Y_a \cap (0 \times \omega \mathbf{Z}^{d_1})),$$

où $\omega = 2\pi \mathrm{i}$. Les fonctions d_0, d_1, d, ℓ_0, ℓ_1 et ℓ_a sont additives car, si $m(f, X^*, X)$ est un noyau de $m(g, X, X')$ et si $m(g, X, X')$ est un conoyau de $m(f, X^*, X)$, alors f et g induisent des suites exactes d'applications linéaires

$$0 \longrightarrow K^{d_0^*} \times 0 \longrightarrow K^{d_0} \times 0 \longrightarrow K^{d_0'} \times 0 \longrightarrow 0,$$
$$0 \longrightarrow 0 \times \mathbf{Q}^{d_1^*} \longrightarrow 0 \times \mathbf{Q}^{d_1} \longrightarrow 0 \times \mathbf{Q}^{d_1'} \longrightarrow 0,$$
$$0 \longrightarrow W^* \longrightarrow W \longrightarrow W' \longrightarrow 0.$$

et des suites exactes d'homomorphismes de groupes

$$0 \longrightarrow Y^* \longrightarrow Y \longrightarrow Y' \longrightarrow 0 \quad \text{et} \quad 0 \longrightarrow Y_a^* \longrightarrow Y_a \longrightarrow Y_a' \longrightarrow 0.$$

De son côté, la fonction n est sur-additive car, dans la situation ci-dessus, g applique surjectivement $\mathbf{C}W + \mathbf{C}Y$ sur $\mathbf{C}W' + \mathbf{C}Y'$ et le noyau de la restriction de g à $\mathbf{C}W + \mathbf{C}Y$ contient l'image de $\mathbf{C}W^* + \mathbf{C}Y^*$ par f. Par ailleurs, la fonction κ est sous-additive car, pour tout objet X de $\mathcal{C}$ de la forme (6.1), on a

$$\kappa(X) = \dim_{\mathbf{Q}}(\mathbf{Q}Y \cap (0 \times \omega \mathbf{Q}^{d_1}))$$

et, dans la situation présente, g applique $\mathbf{Q}Y \cap (0 \times \omega \mathbf{Q}^{d_1})$ dans $\mathbf{Q}Y' \cap (0 \times \omega \mathbf{Q}^{d_1'})$ et le noyau de la restriction de g à $\mathbf{Q}Y \cap (0 \times \omega \mathbf{Q}^{d_1})$ coïncide avec l'image de $\mathbf{Q}Y^* \cap (0 \times \omega \mathbf{Q}^{d_1^*})$ sous f. De même, la fonction κ_a est elle-aussi sous-additive.

Lemme 6.2. *Pour tout objet X de $\mathcal{C}$, il existe un objet X' de $\mathcal{C}$ et un conoyau $s: X \to X'$ tels que*

$$d_0(X') = d_0(X), \quad d_1(X') = d_1(X) - \kappa(X) \quad \textit{et} \quad n(X') = n(X) - \kappa(X).$$

Démonstration. Écrivons $X = (d_0, d_1, W, Y, Y_a)$ et posons $\kappa = \kappa(X)$ et $n = n(X)$. Le sous-espace de $\mathbf{C}^{d_0} \times \mathbf{C}^{d_1}$ engendré par $Y \cap (0 \times \omega \mathbf{Z}^{d_1})$ est de la forme $0 \times T_1$ où T_1 est un sous-espace de $\mathbf{C}^{d_1}$ défini sur $\mathbf{Q}$ de dimension κ. Il existe donc une application linéaire

$$g: \mathbf{C}^{d_0} \times \mathbf{C}^{d_1} \longrightarrow \mathbf{C}^{d_0} \times \mathbf{C}^{d_1 - \kappa}$$

de noyau $0 \times T_1$ qui applique $K^{d_0} \times 0$ sur $K^{d_0} \times 0$ et $0 \times \mathbf{Q}^{d_1}$ sur $0 \times \mathbf{Q}^{d_1 - \kappa}$. On pose

$$W' = g(W), \quad Y' = g(Y) \quad \text{et} \quad Y_a' = g(Y_a).$$

Alors, $X' = (d_0, d_1 - \kappa, W', Y', Y_a')$ est un objet de $\mathcal{C}$ et le morphisme $s = m(g, X, X')$ de X dans X' est un conoyau. Comme $\mathbf{C}W + \mathbf{C}Y$ contient $0 \times T_1$, on a bien $n(X') = n - \kappa$.

(iii) Les catégories $\mathcal{C}_\epsilon$

Pour tout $\epsilon > 0$ avec ϵ^{-1} entier, on désigne par $\mathcal{C}_\epsilon$ la sous-catégorie de $\mathcal{C}$ dont les objets sont les objets X de $\mathcal{C}$ avec

$$2d(X)(d(X) + \ell_1(X)) + 1 \leq \epsilon^{-1}$$

et dont les morphismes sont les morphismes de $\mathcal{C}$ entre ces objets. C'est aussi une catégorie admissible car tout morphisme de $\mathcal{C}$ qui est un noyau ou un conoyau d'un morphisme de $\mathcal{C}_\epsilon$ est aussi un morphisme de $\mathcal{C}_\epsilon$.

On définit des fonctions a_ϵ, b_ϵ, c_ϵ, d_ϵ et r_ϵ de $\mathrm{Ob}(\mathcal{C}_\epsilon)$ dans $\mathbf{N}$ en posant, pour tout objet X de $\mathcal{C}_\epsilon$,

$$\begin{aligned}
a_\epsilon(X) &= \epsilon^{-2}\big(d_1(X) - \kappa(X)\big),\\
b_\epsilon(X) &= \epsilon^{-2} \max\big\{0, (1-\epsilon)d_0(X) + d_1(X) - (2-\epsilon)n(X) + \epsilon^2 \kappa_a(X)\big\},\\
c_\epsilon(X) &= \epsilon^{-2} \ell_1(X),\\
d_\epsilon(X) &= \epsilon^{-2}\big((2-\epsilon)n(X) - (1-\epsilon)\ell_0(X) - \epsilon^2 \ell_a(X)\big),\\
r_\epsilon(X) &= \epsilon^{-2} d(X).
\end{aligned}$$

Alors, on obtient:

Lemme 6.3. *Les fonctions r_ϵ et c_ϵ sont additives, tandis que a_ϵ et d_ϵ sont sur-additives et que b_ϵ est sous-additive et majorée par r_ϵ. Toutes ces fonctions s'annulent en chaque objet en lequel r_ϵ s'annule. De plus, on a $r_\epsilon(X) = 0$ pour tout objet X de $\mathcal{C}_\epsilon$ tel que $b_\epsilon(X) + d_\epsilon(X) = 0$.*

Démonstration. La première affirmation découle des observations faites en (ii). La seconde est claire. Pour vérifier la dernière, supposons que X soit un objet de $\mathcal{C}_\epsilon$ pour lequel $b_\epsilon(X) + d_\epsilon(X) = 0$. On a d'une part $b_\epsilon(X) = 0$, donc $d(X) \le 2n(X)$, et d'autre part $d_\epsilon(X) = 0$, donc $2n(X) \le \ell_0(X)$. Comme $\ell_0(X) \le n(X)$, cela implique $n(X) = 0$ et par suite $d(X) = 0$, donc $r_\epsilon(X) = 0$.

Lemme 6.4. *Soit X un objet de $\mathcal{C}_\epsilon$ avec $b_\epsilon(X) \neq 0$. Alors, la famille des conoyaux $s\colon X \to X'$ qui vérifient $b_\epsilon(X') \neq 0$ et qui minimisent le rapport $a_\epsilon(X')/b_\epsilon(X')$ est non vide. De plus, si $s\colon X \to X'$ est un membre de cette famille pour lequel $r_\epsilon(X')$ est minimal, alors on a $\kappa(X') = 0$.*

Démonstration. La famille F des conoyaux $s\colon X \to X'$ avec $b_\epsilon(X') \neq 0$ est non vide car elle contient le morphisme identité de X dans lui-même. De plus, pour tout conoyau $s\colon X \to X'$ de F, on a $b_\epsilon(X') \le r_\epsilon(X') \le r_\epsilon(X)$. Les quotients $a_\epsilon(X')/b_\epsilon(X')$ associés à ces morphismes appartiennent donc à un sous-ensemble discret de $\mathbf{R}$. Par suite, il existe dans F un conoyau $s\colon X \to X'$ pour lequel le rapport $a_\epsilon(X')/b_\epsilon(X')$ soit minimal. Fixons un tel choix de s avec $r_\epsilon(X')$ minimal. Le lemme 6.2 montre qu'il existe un conoyau $s'\colon X' \to X''$ tel que $d_0(X'') = d_0(X')$, $d_1(X'') = d_1(X') - \kappa(X')$ et $n(X'') = n(X') - \kappa(X')$. Si $\kappa(X')$ était positif, on aurait

$$r_\epsilon(X'') < r_\epsilon(X'), \quad a_\epsilon(X'') \le a_\epsilon(X') \quad \text{et} \quad b_\epsilon(X'') \ge b_\epsilon(X'),$$

et la composée $s' \circ s\colon X \to X''$ serait un membre de F avec $a_\epsilon(X'')/b_\epsilon(X'') \le a_\epsilon(X')/b_\epsilon(X')$ et $r_\epsilon(X'') < r_\epsilon(X')$, en contradiction avec le choix de s.

(iv) Démonstration du théorème 1.1

Soit ϵ un nombre réel positif dont l'inverse ϵ^{-1} est un entier. Le lemme 6.3 montre que la catégorie $\mathcal{C}_\epsilon$ munie des fonctions a_ϵ, b_ϵ, c_ϵ, d_ϵ et r_ϵ vérifie les hypothèses de la proposition 6.1.

(a) Soit $X = (d_0, d_1, W, Y, Y_a)$ un objet de $\mathcal{C}_\epsilon$ avec $b_\epsilon(X) \neq 0$. On va montrer que X vérifie l'énoncé 1 de la proposition 6.1.

Supposons d'abord $\kappa(X) = 0$ et appliquons le théorème 5.1 à W, Y et Y_a. Dans les notations de ce théorème, on a $n = n(X)$. De plus, la condition sur ϵ est remplie. Soit L le sous-groupe algébrique de $G = \mathbf{G}_{\mathrm{a}}^{d_0} \times \mathbf{G}_{\mathrm{m}}^{d_1}$ que fournit le théorème 5.1. On pose $G' = \mathbf{G}_{\mathrm{a}}^{d'_0} \times \mathbf{G}_{\mathrm{m}}^{d'_1}$. Puisque L est connexe et défini sur K, il existe un morphisme de groupes algébriques $h\colon G \to G'$ qui est surjectif, défini sur K et dont le noyau est L. On identifie $T_{G'}(\mathbf{C})$ avec $\mathbf{C}^{d'_0} \times \mathbf{C}^{d'_1}$ de la manière habituelle et on note $\exp_{G'}$ l'application exponentielle correspondante de $\mathbf{C}^{d'_0} \times \mathbf{C}^{d'_1}$ dans $G'(\mathbf{C})$. Soit g l'application linéaire de $\mathbf{C}^{d_0} \times \mathbf{C}^{d_1}$ dans $\mathbf{C}^{d'_0} \times \mathbf{C}^{d'_1}$ pour laquelle $h \circ \exp_G = \exp_{G'} \circ g$. On pose $W' = g(W)$, $Y' = g(Y)$ et $Y'_a = g(Y_a)$. Alors $X' = (d'_0, d'_1, W', Y', Y'_a)$ est un objet de $\mathcal{C}_\epsilon$ et g détermine un morphisme $s = m(g, X, X')$ de X dans X'. Par construction, ce morphisme est un conoyau de $\mathcal{C}_\epsilon$. Avec les notations du théorème 5.1, on a $\lambda' = \ell_1(X') - \kappa(X')$ et $\lambda'_a = \ell_a(X') - \kappa_a(X')$. Comme on suppose $\kappa(X) = 0$, on a $\kappa_a(X) = 0$. Comme on suppose aussi $b_\epsilon(X) > 0$, l'inégalité (5.1) fournit

$$b_\epsilon(X)\big(a_\epsilon(X') + c_\epsilon(X')\big) \le a_\epsilon(X)\big(b_\epsilon(X') + d_\epsilon(X')\big). \tag{6.4}$$

Enfin, puisque $L \neq G$, on a $r_\epsilon(X') \neq 0$. Donc, en vertu du lemme 6.3, on a aussi $b_\epsilon(X') + d_\epsilon(X') > 0$ et l'inégalité (6.4) se réécrit

$$\frac{a_\epsilon(X') + c_\epsilon(X')}{b_\epsilon(X') + d_\epsilon(X')} \le \frac{a_\epsilon(X)}{b_\epsilon(X)}.$$

Ainsi, l'énoncé 1 de la proposition 6.1 est vérifié pour X lorsque $\kappa(X) = 0$.

En général, le lemme 6.4 montre qu'il existe dans $\mathcal{C}_\epsilon$ un conoyau $s'\colon X \to X'$ qui vérifie $b_\epsilon(X') > 0$, $\kappa(X') = 0$ et

$$\frac{a_\epsilon(X')}{b_\epsilon(X')} \le \frac{a_\epsilon(X)}{b_\epsilon(X)} .$$

Pour l'objet X', les considérations précédentes montrent qu'il existe un conoyau $s''\colon X' \to X''$ qui vérifie

$$b_\epsilon(X'') + d_\epsilon(X'') > 0 \quad \text{et} \quad \frac{a_\epsilon(X'') + c_\epsilon(X'')}{b_\epsilon(X'') + d_\epsilon(X'')} \le \frac{a_\epsilon(X')}{b_\epsilon(X')}.$$

L'énoncé 1 de la proposition 6.1 est donc vérifié pour X en prenant pour morphisme s la composée $s'' \circ s'\colon X \to X''$.

(b) Puisque l'énoncé 1 de la proposition 6.1 est vérifié dans la catégorie $\mathcal{C}_\epsilon$ pour les fonctions a_ϵ, b_ϵ, c_ϵ, d_ϵ et r_ϵ, l'énoncé 2 de cette proposition est lui-aussi vérifié dans cette catégorie pour les mêmes fonctions.

Plaçons-nous maintenant dans les hypothèses du théorème 1.1. Le cas général où K est un corps quelconque de degré de transcendance ≤ 1 sur $\mathbf{Q}$ se ramène sans trop de peine au cas où il est de type fini et de degré de transcendance 1 sur $\mathbf{Q}$. Dans ce cas, la famille $X = (d_0, d_1, W, Y, Y_a)$ constitue un objet de $\mathcal{C}$. Pour $1/\epsilon$ entier suffisamment grand, c'est donc un objet de $\mathcal{C}_\epsilon$. Fixons un tel choix de ϵ. Dans les notations de ce théorème, on a $d(X) = d$ et $n(X) = n$. Donc l'hypothèse $d > 2n$ implique $b_\epsilon(X) > 0$. L'énoncé 2 de la proposition 6.1 s'applique donc à X. Il montre d'abord que la famille des conoyaux $s\colon X \to X'$ qui vérifient $b_\epsilon(X') \neq 0$ et qui minimisent le rapport $a_\epsilon(X')/b_\epsilon(X')$ est non vide. Soit $s\colon X \to X'$ un membre de cette famille pour lequel $r_\epsilon(X')$ est minimal. L'énoncé 2 montre aussi que, si $c_\epsilon(X') \neq 0$, alors on a

$$d_\epsilon(X') \neq 0 \quad \text{et} \quad \frac{a_\epsilon(X)}{b_\epsilon(X)} \ge \frac{a_\epsilon(X')}{b_\epsilon(X')} \ge \frac{c_\epsilon(X')}{d_\epsilon(X')} . \tag{6.5}$$

Le lemme 6.4 fournit quant à lui $\kappa(X') = 0$, et par suite $\kappa_a(X') = 0$.

Écrivons $X' = (d_0', d_1', W', Y', Y_a')$. Désignons par g l'application linéaire de $\mathbf{C}^{d_0} \times \mathbf{C}^{d_1}$ dans $\mathbf{C}^{d_0'} \times \mathbf{C}^{d_1'}$ qui est sous-jacente à s, et définissons d', ℓ_0', ℓ_1', ℓ_a' et n' comme dans l'énoncé du théorème 1.1.

Puisque $d' > 0$, on doit avoir $n' \ge d_0'$ et $n' > 0$. En effet, si une de ces conditions n'était pas vérifiée, W' et Y' seraient tous deux contenus dans un même sous-espace de $\mathbf{C}^{d'}$, distinct de $\mathbf{C}^{d'}$, de la forme $T_0' \times T_1'$ où T_0' est un sous-espace de $\mathbf{C}^{d_0'}$ défini sur K et T_1' un sous-espace de $\mathbf{C}^{d_1'}$ défini sur $\mathbf{Q}$. Alors, W et Y seraient contenus tous deux dans $g^{-1}(T_0' \times T_1')$. Or, ce dernier serait lui-même un sous-espace de $\mathbf{C}^d$, distinct de $\mathbf{C}^d$, de la forme $T_0 \times T_1$ où T_0 est un sous-espace de $\mathbf{C}^{d_0}$ défini sur K et T_1 un sous-espace de $\mathbf{C}^{d_1}$ défini sur $\mathbf{Q}$. C'est impossible en vertu des hypothèses du théorème 1.1.

Puisque $\kappa(X') = \kappa_a(X') = 0$, la condition $b_\epsilon \neq 0$ signifie $(d' - 2n') + \epsilon(n' - d_0') > 0$, donc $d' \ge 2n'$. Comme $n' \ge d_0'$, on en déduit $d_1' \ge n' > 0$. D'autre part, comme $n' \ge \ell_0'$, on a aussi $2n' > \ell_0'$, donc $d_\epsilon(X') > 0$. Cela nous apprend que (6.5) est vérifiée sans restriction sur $c_\epsilon(X')$. On obtient donc

$$\frac{d_1}{(d - 2n) + \epsilon(n - d_0)} \ge \frac{d_1'}{(d' - 2n') + \epsilon(n' - d_0')} \ge \frac{\ell_1'}{(2n' - \ell_0') + \epsilon(\ell_0' - n') - \epsilon^2 \ell_a'}$$

où les dénominateurs sont tous positifs. En vertu du choix de ϵ, puisque $d_1' > 0$, l'inégalité de gauche entraîne $d' > 2n'$ et

$$\frac{d_1}{d - 2n} \ge \frac{d_1'}{d' - 2n'}.$$

D'autre part, comme $\epsilon(n' - d_0') \ge 0$ et $\epsilon(\ell_0' - n') - \epsilon^2 \ell_a' \le 0$, celle de droite livre

$$\frac{d_1'}{d' - 2n'} \ge \frac{\ell_1'}{2n' - \ell_0'},$$

avec l'inégalité stricte si $n' > d_0'$ ou $n' > \ell_0'$ ou $\ell_a' > 0$. Le théorème 1.1 est démontré.

7. Applications

Dans ce paragraphe, nous montrons comment le théorème 0.2 se déduit du théorème 7.1 ci-dessous. Nous donnons quelques applications de ces deux résultats et concluons par la démonstration du théorème 7.1.

Théorème 7.1. *Soit n un entier positif, soit*

$$W = \{(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbf{C}^{2n}\,;\, x_1y_1 + \cdots + x_ny_n = 0\},$$

et soit w un point de W. Supposons que le corps K engendré par les coordonnées de w et leurs exponentielles soit de degré de transcendance ≤ 1 sur $\mathbf{Q}$. Supposons aussi que les n premières coordonnées de w appartiennent à $\mathcal{L}$. Alors, w appartient à un sous-espace vectoriel de $\mathbf{C}^{2n}$ défini sur $\mathbf{Q}$ et contenu dans W.

Démonstration du théorème 0.2.

Soit $b\colon \mathbf{C}^{2n} \to \mathbf{C}$ la forme quadratique donnée par

$$b(x_1, \ldots, x_n, y_1, \ldots, y_n) = x_1y_1 + \cdots + x_ny_n, \tag{7.1}$$

et soit $\theta\colon \mathbf{C}^n \to \mathbf{C}^{2n}$ une application linéaire définie sur $\mathbf{Q}$ telle que $P(x) = b(\theta(x))$ pour tout $x \in \mathbf{C}^n$. On pose $v = (\lambda_1, \ldots, \lambda_n)$, $w = \theta(v)$, et on désigne par K le sous-corps de $\mathbf{C}$ engendré par les coordonnées de w et leurs exponentielles. Alors, w est un point de W à coordonnées dans $\mathcal{L}$ et K est contenu dans une extension algébrique du corps $K_0 = \mathbf{Q}(\lambda_1, \ldots, \lambda_n)$. Donc, si K_0 est de degré de transcendance ≤ 1 sur $\mathbf{Q}$, il en va de même de K, et le théorème 7.1 montre qu'il existe un sous-espace vectoriel U de $\mathbf{C}^{2n}$ qui est défini sur $\mathbf{Q}$ et qui vérifie $w \in U \subset W$. Alors, $\theta^{-1}(U)$ est un sous-espace vectoriel de $\mathbf{C}^n$ défini sur $\mathbf{Q}$ avec $v \in \theta^{-1}(U) \subset V$, comme requis.

Remarque. Il serait très intéressant de supprimer l'hypothèse d'homogénéité pour le polynôme P dans l'énoncé du théorème 0.2. Cela donnerait la transcendance de nombres tels que e^{ℓ^2} pour $\ell \in \mathcal{L}$, $\ell \neq 0$. On ne sait pas actuellement démontrer la transcendance du nombre e^{π^2}.

(i) Autres conséquences

Plus généralement, la conclusion du théorème 0.2 s'étend à tout sous-ensemble algébrique fermé V de $\mathbf{C}^n$ défini par des polynômes homogènes de $\mathbf{Q}[X_1, \ldots, X_n]$ de degré ≤ 2. Par exemple, on sait que la grassmannienne des sous-espaces de $\mathbf{C}^m$ de dimension k est une intersection de quadriques définies sur $\mathbf{Q}$, donc le théorème 0.2 s'étend au cône affine sur ces variétés (comparer avec [21]).

Pour les courbes, on a le résultat suivant:

Corollaire 7.2. *Soient n un entier positif et $V \subset \mathbf{C}^n$ une courbe algébrique irréductible définie sur $\mathbf{Q}$. Supposons que le degré d de V vérifie $4d + 2 < n(n+1)$ et que V ne soit contenu dans aucun sous-espace de $\mathbf{C}^n$ défini sur $\mathbf{Q}$ autre que $\mathbf{C}^n$. Alors, on a $V \cap \mathcal{L}^n \subset \{0\}$.*

Démonstration. Soit E le sous-espace de $\mathbf{C}[X_1, \ldots, X_n]$ constitué des polynômes homogènes de degré 2. On pose $N = 2d+1$ et on choisit N points distincts $v_1, \ldots, v_N$ de V. Puisque E est de dimension $n(n+1)/2$ et que ce nombre est $> N$, il existe un élément non nul P de E qui s'annule en chacun de ces points. On a $V \subset Z(P)$ sinon $V \cap Z(P)$ serait une réunion finie d'au plus $2d$ points, en contradiction avec le choix de P. Comme V est défini sur $\mathbf{Q}$, l'idéal de définition de V contient donc un polynôme non nul $P_0 \in E \cap \mathbf{Q}[X_1, \ldots, X_n]$.

Soit $v \in V \cap \mathcal{L}^n$. Puisque $P_0(v) = 0$, le théorème 0.2 montre qu'il existe un sous-espace U de $\mathbf{C}^n$ défini sur $\mathbf{Q}$ tel que $v \in U \subset Z(P_0)$. En vertu de l'hypothèse, on a $V \not\subset U$. Donc, $V \cap U$ est une réunion finie de points à coordonnées dans $\overline{\mathbf{Q}}$. Comme v est l'un de ces points, le théorème d'Hermite-Lindemann donne $v = 0$.

Corollaire 7.3. *Soit $q \in \mathbf{Q}[X,Y]$ une forme quadratique de discriminant non nul, et soit λ un élément de $\mathcal{L}$ qui n'est ni réel ni imaginaire pur. Supposons que λ et son conjugué complexe $\overline{\lambda}$ soient algébriquement dépendants sur $\mathbf{Q}$. Alors le nombre*

$$\exp\left(\sqrt{q(\lambda,\overline{\lambda})}\right)$$

est transcendant.

Démonstration. En effet, supposons au contraire qu'il existe $\lambda' \in \mathcal{L}$ tel que $q(\lambda,\overline{\lambda}) = (\lambda')^2$. Soit V le lieu des zéros dans $\mathbf{C}^3$ du polynôme $P = q(X,Y) - Z^2$. Alors, $v = (\lambda,\overline{\lambda},\lambda')$ est un point de V dont les coordonnées appartiennent à $\mathcal{L}$ et engendrent un corps de degré de transcendance ≤ 1 sur $\mathbf{Q}$. Selon le théorème 0.2, il existe donc un sous-espace vectoriel U de $\mathbf{C}^3$ défini sur $\mathbf{Q}$, avec $v \in U \subset V$. Comme q n'est pas un carré, le polynôme P est irréductible, donc U est de dimension ≤ 1. C'est une contradiction car, selon l'hypothèse, λ et $\overline{\lambda}$ sont linéairement indépendants sur $\mathbf{Q}$.

Ce dernier énoncé a quelques applications intéressantes; en voici une qui ne semble pas figurer explicitement dans la littérature, quoiqu'on puisse aussi la déduire de la partie (c) du corollaire 1.2, avec

$$d_1 = \ell_1 = 2, \quad x_1 = |\lambda|, \quad x_2 = \lambda, \quad y_1 = 1, \quad y_2 = |\lambda|/\lambda.$$

Corollaire 7.4. *Soit λ un élément de $\mathcal{L}$ qui n'est pas réel. Alors l'une au moins des deux propriétés suivantes est vraie:*
(i) Les nombres λ et $\overline{\lambda}$ sont algébriquement indépendants sur $\mathbf{Q}$.
(ii) Le nombre $e^{|\lambda|}$ est transcendant.

Par exemple, on peut affirmer que si $\log 2$ et π sont algébriquement dépendants sur $\mathbf{Q}$, le nombre $\exp(\sqrt{(\log 2)^2 + \pi^2})$ est transcendant.

Étant donné un hyperplan H de $\mathbf{C}^n$, on sait que la dimension sur $\mathbf{Q}$ de $H \cap \mathcal{L}^n$ est finie si et seulement si $H \cap \mathbf{Q}^n = 0$. De plus, lorsque cette dimension est finie, on sait qu'elle est $\leq n(n-1)$ (thm. 2 de [8], thm. 1.1 de [32]). On conjecture toutefois qu'elle est $\leq n(n-1)/2$ (voir [18]). Le théorème 7.1 permet d'établir cette borne dans un cas particulier:

Corollaire 7.5. *Soient $a_1,\dots,a_n$ des nombres complexes linéairement indépendants sur $\mathbf{Q}$, soit H l'hyperplan de $\mathbf{C}^n$ donné par*

$$H = \{(z_1,\dots,z_n) \in \mathbf{C}^n \,;\, a_1z_1 + \cdots + a_nz_n = 0\},$$

et soit K un sous-corps de $\mathbf{C}$ de degré de transcendance ≤ 1 sur $\mathbf{Q}$. On considère $\mathcal{E} = \mathcal{L}_K \cap K$ et $\mathcal{E}_0 = \mathcal{L} \cap \mathcal{E}$ comme espaces vectoriels sur $\mathbf{Q}$. Alors,
(i) si $a_1,\dots,a_n \in \mathcal{E}$, on a $\dim_{\mathbf{Q}}(H \cap (\mathcal{E}_0)^n) \leq n(n-1)/2$;
(ii) si $a_1,\dots,a_n \in \mathcal{E}_0$, on a $\dim_{\mathbf{Q}}(H \cap \mathcal{E}^n) \leq n(n-1)/2$.

Démonstration. On se borne au cas où $a_1,\dots,a_n \in \mathcal{E}$ car l'autre cas est similaire. On pose $a = (a_1,\dots,a_n)$ et on choisit $z \in H \cap (\mathcal{E}_0)^n$. Alors, le point $w = (z,a)$ remplit les conditions du théorème 7.1. Dans les notations de ce théorème, il existe donc un sous-espace U de $\mathbf{C}^{2n}$ défini sur $\mathbf{Q}$ tel que $w \in U \subset W$. Comme la forme quadratique b donnée par (7.1) est non dégénérée et qu'elle s'annule identiquement sur U, on doit avoir $\dim U \leq n$. Comme les n coordonnées de a sont linéairement indépendantes sur $\mathbf{Q}$, on en déduit que U est de dimension n et qu'il existe une application linéaire $\varphi\colon \mathbf{C}^n \to \mathbf{C}^n$ définie sur $\mathbf{Q}$ telle que U consiste des points $(\varphi(y),y)$ avec $y \in \mathbf{C}^n$. On a $z = \varphi(a)$ et le fait que b s'annule identiquement sur U signifie que φ est antisymétrique par rapport à la forme bilinéaire standard de $\mathbf{C}^n$. Comme les endomorphismes antisymétriques de $\mathbf{C}^n$ définis sur $\mathbf{Q}$ constituent un espace vectoriel sur $\mathbf{Q}$ de dimension $n(n-1)/2$, on obtient bien $\dim_{\mathbf{Q}}(H \cap (\mathcal{E}_0)^n) \leq n(n-1)/2$.

(ii) Algèbres de Clifford

La démonstration du théorème 7.1 utilise l'algèbre de Clifford A attachée à une forme quadratique $q: \mathbf{C}^m \to \mathbf{C}$ (voir §8, chap. XIV de [12] et chap. 5 de [11]). C'est une algèbre simple, de dimension 2^m sur $\mathbf{C}$, qui contient $\mathbf{C}^m$ comme sous-espace vectoriel, qui est engendrée par $\mathbf{C}^m$ en tant que $\mathbf{C}$-algèbre, et qui vérifie

$$v^2 = q(v) \cdot 1 \quad \text{pour tout } v \in \mathbf{C}^m.$$

De plus, si $\{v_1, \ldots, v_m\}$ est une base de $\mathbf{C}^m$ sur $\mathbf{C}$, alors les produits $v_{i_1} \ldots v_{i_r}$ avec $i_1 < \cdots < i_r$ constituent une base de A sur $\mathbf{C}$, en interprétant le produit vide comme étant égal à 1. Cette algèbre permet la construction suivante:

Lemme 7.6. *Soient m un entier positif, $q \in \mathbf{Q}[X_1, \ldots, X_m]$ un polynôme homogène de degré 2, et $V = Z(q)$ l'ensemble des zéros de q dans $\mathbf{C}^m$. Alors, il existe une application linéaire injective définie sur $\mathbf{Q}$*

$$\theta: \mathbf{C}^m \longrightarrow \mathrm{Mat}_{2^m \times 2^m}(\mathbf{C})$$

telle que, pour tout $v \in \mathbf{C}^m$, le rang de $\theta(v)$ soit un multiple de 2^{m-1} et telle qu'on ait

$$V = \{v \in \mathbf{C}^m \,;\, \det \theta(v) = 0\}. \tag{7.2}$$

De plus, si m est un entier pair et si $q = \sum_{i=1}^{n} X_i X_{n+i}$ avec $n = m/2$, alors on peut choisir θ de telle sorte que, pour tout $v = (x_1, \ldots, x_m) \in \mathbf{C}^m$, les coefficients de la première colonne de $\theta(v)$ appartiennent à $\{0, x_1, \ldots, x_n\}$.

Démonstration. Soit A l'algèbre de Clifford de q considéré comme forme quadratique sur $\mathbf{C}^m$, et soit A_0 la sous-$\mathbf{Q}$-algèbre de A engendrée par $\mathbf{Q}^m$. Comme q définit par restriction une forme quadratique $q_0: \mathbf{Q}^m \to \mathbf{Q}$, cette sous-algèbre A_0 est isomorphe à l'algèbre de Clifford de q_0. En particulier, elle est de dimension 2^m sur $\mathbf{Q}$ et toute base de A_0 sur $\mathbf{Q}$ est une base de A sur $\mathbf{C}$. On fixe le choix d'une base de A dans A_0 et, pour tout $v \in \mathbf{C}^m$, on désigne par M_v la matrice de l'application linéaire $L_v: A \to A$ donnée par la multiplication à gauche par v, relative à ce choix de base. Si $v \in \mathbf{Q}^m$, alors L_v applique A_0 dans lui-même, donc M_v est à coefficients dans $\mathbf{Q}$. Cela signifie que l'application linéaire $\theta: \mathbf{C}^m \to \mathrm{Mat}_{2^m \times 2^m}(\mathbf{C})$ qui à $v \in \mathbf{C}^m$ associe M_v est définie sur $\mathbf{Q}$.

Soit $v \in \mathbf{C}^m$. Puisque M_v^2 est la matrice de la multiplication à gauche par $v^2 = q(v) \cdot 1$, on a

$$M_v^2 = q(v) \cdot I$$

où I est la matrice identité d'ordre 2^m. En prenant le déterminant des deux membres de cette égalité, puis en extrayant la racine carrée, on trouve

$$\det M_v = \pm q(v)^{2^{m-1}}, \tag{7.3}$$

donc (7.2) est vérifié. Si $q(v) \neq 0$, la formule (7.3) montre que M_v est inversible, donc de rang 2^m. Si $v = 0$, alors M_v est nul, donc de rang 0. Enfin, si $v \neq 0$ et si $q(v) = 0$, la relation $L_v^2 = 0$ signifie que l'image de L_v est contenue dans son noyau. Donc le rang de M_v est $\leq 2^{m-1}$. D'autre part, si on complète $\{v\}$ en une base $\{v, v_2, \ldots, v_m\}$ de $\mathbf{C}^m$, on trouve que L_v est injectif sur le sous-espace de A engendré par les produits $v_{i_1} \cdots v_{i_r}$ avec $2 \leq i_1 < \cdots < i_r$. Donc le rang de M_v est aussi $\geq 2^{m-1}$ et par suite il est égal à 2^{m-1}. Ainsi, dans tous les cas, le rang de M_v est un multiple de 2^{m-1}.

Enfin, supposons que m soit pair et qu'on ait $q = \sum_{i=1}^{n} X_i X_{n+i}$ avec $n = m/2$. Dans ce cas, on désigne par $\{e_1, \ldots, e_m\}$ la base canonique de $\mathbf{C}^m$ et on choisit pour base de A l'ensemble formé des produits

$e_{i_1}\cdots e_{i_r}$ avec $i_1 < \cdots < i_r$ en faisant en sorte que le produit $\alpha = e_{n+1}e_{n+2}\cdots e_{2n}$ soit le premier élément de cette base. Soit U le sous-espace de $\mathbf{C}^m$ engendré par $e_{n+1},\ldots,e_{2n}$. Comme q est identiquement nul sur U, la sous-algèbre de A engendrée par U est isomorphe à l'algèbre extérieure de U et on a $e_i\cdot\alpha = 0$ pour $i = n+1,\ldots,2n$. Donc, pour tout $v = (x_1,\ldots,x_m)\in\mathbf{C}^m$, on trouve

$$L_v(\alpha) = \sum_{i=1}^{n} x_i e_i e_{n+1}e_{n+2}\cdots e_{2n}.$$

Cela démontre la dernière assertion du lemme.

Remarque. Dans le cas de la forme quadratique $b\colon \mathbf{C}^{2n}\to\mathbf{C}$ donnée par (7.1), on peut raffiner le lemme 7.6 et montrer l'existence d'applications linéaires injectives

$$\varphi_n\colon \mathbf{C}^{2n}\longrightarrow \mathrm{Mat}_{2^{n-1}\times 2^{n-1}}(\mathbf{C}) \quad\text{et}\quad \psi_n\colon \mathbf{C}^{2n}\longrightarrow \mathrm{Mat}_{2^{n-1}\times 2^{n-1}}(\mathbf{C})$$

qui sont définies sur $\mathbf{Q}$ et possèdent les propriétés suivantes.
Pour tout $n\geq 2$ et tout $v = (x_1,\ldots,x_n,y_1,\ldots,y_n)\in\mathbf{C}^{2n}$, on a
(i) $\varphi_n(v)\psi_n(v) = \psi_n(v)\varphi_n(v) = (x_1y_1+\cdots+x_ny_n)I_{2^{n-1}}$;
(ii) $\det\varphi_n(v) = \det\psi_n(v) = (x_1y_1+\cdots+x_ny_n)^{2^{n-2}}$;
(iii) les rangs de $\varphi_n(v)$ et de $\psi_n(v)$ sont égaux et ce sont des multiples de 2^{n-2};
(iv) tous les éléments de la première colonne de $\varphi_n(v)$ appartiennent à $\{0,\pm x_1,\ldots,\pm x_n\}$.
On construit ces applications par récurrence sur n. Pour $n = 1$, on définit

$$\varphi_1(x_1,y_1) = (\,x_1\,) \quad\text{et}\quad \psi_1(x_1,y_1) = (\,y_1\,)\,.$$

En général, pour $n\geq 1$ et pour tout $v' = (x_1,\ldots,x_{n+1},y_1,\ldots,y_{n+1})\in\mathbf{C}^{2n+2}$, on pose

$$\varphi_{n+1}(v') = \begin{pmatrix} x_{n+1}I_{2^{n-1}} & \psi_n(v)\\ -\varphi_n(v) & y_{n+1}I_{2^{n-1}}\end{pmatrix} \quad\text{et}\quad \psi_{n+1}(v') = \begin{pmatrix} y_{n+1}I_{2^{n-1}} & -\psi_n(v)\\ \varphi_n(v) & x_{n+1}I_{2^{n-1}}\end{pmatrix}$$

où $v = (x_1,\ldots,x_n,y_1,\ldots,y_n)$. On laisse au lecteur le soin de vérifier que les applications ainsi définies vérifient les propriétés (i) à (iv), pour $n\geq 2$.

Le rapport de cette construction avec les algèbres de Clifford est le suivant. Soit n un entier ≥ 2 et soit θ_n l'application linéaire de $\mathbf{C}^{2n}$ dans $\mathrm{Mat}_{2^n\times 2^n}(\mathbf{C})$ donnée par

$$\theta_n(v) = \begin{pmatrix} 0 & \psi_n(v)\\ \varphi_n(v) & 0\end{pmatrix}$$

pour tout $v\in\mathbf{C}^{2n}$. Alors, θ_n est injective, définie sur $\mathbf{Q}$ et vérifie

$$\theta_n(v)^2 = (x_1y_1+\cdots+x_ny_n)I_{2^n}$$

pour tout $v = (x_1,\ldots,x_n,y_1,\ldots,y_n)\in\mathbf{C}^{2n}$. Donc, si A désigne l'algèbre de Clifford de la forme quadratique $x_1y_1+\cdots+x_ny_n$, il existe un homomorphisme d'algèbres de A dans $\mathrm{Mat}_{2^n\times 2^n}(\mathbf{C})$ qui coïncide avec θ_n sur $\mathbf{C}^{2n}$. Comme $\theta_n\neq 0$ et que A est une algèbre simple de dimension 2^{2n}, cet homomorphisme est en fait un isomorphisme.

(iii) Démonstration du théorème 7.1.

Soit $b\colon \mathbf{C}^{2n} \to \mathbf{C}$ la forme quadratique donnée par (7.1). On pose $N = 2^{2n-1}$ et on considère l'application linéaire $\theta\colon \mathbf{C}^{2n} \to \mathrm{Mat}_{2N\times 2N}(\mathbf{C})$ associée par le lemme 7.6 à cette forme quadratique. On considère aussi la matrice $M = \theta(w)$. Comme $\det(M) = 0$, son rang est $\leq N$. Comme θ est définie sur $\mathbf{Q}$, ses coefficients appartiennent à $\mathcal{L}_K \cap K$. De plus, les coefficients de sa première colonne appartiennent à $\mathcal{L}$. Si cette colonne n'est pas nulle, alors K n'est pas algébrique sur $\mathbf{Q}$ et le théorème 0.1 montre que M appartient à un sous-espace T de $\mathrm{Mat}_{2N\times 2N}(\mathbf{C})$ qui est défini sur $\mathbf{Q}$ et qui consiste de matrices de rang $< 2N$. C'est bien sûr encore le cas si cette colonne est nulle. On pose $U = \theta^{-1}(T)$. Alors, U est un sous-espace de $\mathbf{C}^{2n}$ qui contient w, qui est défini sur $\mathbf{Q}$ car θ est défini sur $\mathbf{Q}$, et qui est contenu dans W car la fonction déterminant s'annule identiquement sur T.

Références

[1] M. F. Atiyah et I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Pub. Co., 1969.

[2] A. Baker, *Transcendental Number Theory*, Cambridge Univ. Press, 2-ième éd., 1979.

[3] W. D. Brownawell, Sequences of diophantine approximations, *J. Number Theory* **6** (1974), 11–21.

[4] W. D. Brownawell, The algebraic independence of certain numbers related to the exponential function, *J. Number Theory* **6** (1974), 22–31.

[5] C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, Math. Surveys N° 6, Amer. Math. Soc., 1951.

[6] G. V. Chudnovsky, *Contributions to the Theory of Transcendental Numbers*, Math. Surveys and Monographs N° 19, Amer. Math. Soc., 1984.

[7] A. Durand, Approximations algébriques d'un nombre transcendant, *C. R. Acad. Sci. Paris, Série A*, **287** (1978), 595–597.

[8] M. Emsalem, Sur les idéaux dont l'image par l'application d'Artin dans une $\mathbf{Z}_p$-extension est triviale, *J. reine angew. Math.* **382** (1987), 181–198.

[9] A. O. Gel'fond, *Transcendental and Algebraic Numbers*, Moscow, 1952; trad. anglaise: Dover Publ., 1960.

[10] P. M. Gruber et C. G. Lekkerkerker, *Geometry of Numbers*, North Holland, 1987.

[11] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Inc., 1973.

[12] S. Lang, *Algebra*, 3-ième éd., Addison-Wesley, 1993.

[13] M. Laurent, Sur quelques résultats récents de transcendance, Journées Arithmétiques de Luminy 1989, *Astérisque* **198-200**, 209–230.

[14] M. Laurent et D. Roy, Critères d'indépendance algébrique avec multiplicités et déterminants d'interpolation, manuscrit.

[15] K. Mahler, A theorem on inhomogeneous diophantine inequalities, *Proc. Kon. Ned. Akad. Wet.* **41** (1938), 634–637.

[16] D. Mumford, *Algebraic Geometry I: Complex Projective Varieties*, 2-ième éd., Springer Verlag, 1995.

[17] P. Philippon, Une approche méthodique pour la transcendance et l'indépendance algébrique de valeurs de fonctions analytiques, *J. Number Theory*, **64** (1997), 291–338.

[18] D. Roy, Matrices dont les coefficients sont des formes linéaires; *Sém. Th. Nombres, Paris* (1987-88), Prog. in Math. **81**, Birkhäuser Verlag (1990), 273–281.

[19] D. Roy, Transcendance et questions de répartition dans les groupes algébriques, *Approximations Diophantiennes et Nombres Transcendants, Luminy 1990*, éd. P. Philippon, W. de Gruyter (1992), 249–274.

[20] D. Roy, Matrices whose coefficients are linear forms in logarithms, *J. Number Theory* **41** (1992), 22–47.

[21] D. Roy, Points whose coordinates are logarithms of algebraic numbers on algebraic varieties, *Acta Math.* **175** (1995), 49–73.

[22] D. Roy et M. Waldschmidt, Quadratic relations between logarithms of algebraic numbers, *Proc. Japan Acad. Ser. A* **71** (1995), 151–153.

[23] D. Roy et M. Waldschmidt, Simultaneous approximation and algebraic independence, Ramanujan Math. J., **1** (1997).

[24] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Math. vol. 1467, Springer Verlag, 1991.

[25] Th. Schneider, *Einführung in die transzendenten Zahlen*, Springer Verlag, 1957; trad. française, *Introduction aux Nombres Transcendants*, Paris, Gauthier-Villars, 1959.

[26] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics **E15**, Vieweg, 1990.

[27] R. Tijdeman, On the algebraic independence of certain numbers, *Proc. Nederl. Akad. Wetensch., Ser. A* **74** (= Indag. Math. **33**) (1971), 146–162.

[28] M. Waldschmidt, Solution du huitième problème de Schneider, *J. Number Theory* **5** (1973), 191–202.

[29] M. Waldschmidt, *Nombres Transcendants*, Lecture Notes in Math., **402**, Springer Verlag, 1974.

[30] M. Waldschmidt, Transcendance et exponentielles en plusieurs variables; *Invent. Math.*, **63** (1981), 97–127.

[31] M. Waldschmidt, On the transcendence methods of Gel'fond and Schneider in several variables, dans: *New Advances in transcendence theory*, éd. A. Baker, Cambridge Univ. Press (1988), 375–398.

[32] M. Waldschmidt, Dependence of logarithms of algebraic points, *Coll. Math. Soc. János Bolyai* **51** (1987), 1013-1035.

[33] M. Waldschmidt, Approximation diophantienne dans les groupes algébriques commutatifs, *J. reine angew. Math.* , à paraître.

[34] E. Wirsing, Approximation mit algebraischen Zahlen beschränkten Grades, *J. reine angew. Math.* , **206** (1961), 67-77.

Damien ROY
Département de Mathématiques
Université d'Ottawa
585 King Edward
Ottawa, Ontario K1N 6N5
CANADA

Michel WALDSCHMIDT
Institut de Mathématiques de Jussieu
Case 247 Problèmes Diophantiens
4, Place Jussieu
75252 PARIS Cedex 05
FRANCE