J. reine angew. Math. **513** (1999), 145–179

Journal für die reine und angewandte Mathematik

Le problème de Lehmer en dimension supérieure

Par *Francesco Amoroso* à Torino et *Sinnou David* à Paris

Abstract. We study a higher dimensional Lehmer problem, or alternatively the Lehmer problem for a power of the multiplicative group. More precisely, if $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent algebraic numbers, we provide a lower bound for the product of the heights of the α_i's in terms of the degree D of the number field generated by the α_i's. This enables us to study the successive minima for the height function in a given number field. Our bound is a generalisation of an earlier result of Dobrowolski and is best possible up to a power of $\log(D)$. This, in particular, shows that the Lehmer problem is true for number fields having a «small» Galois group.

1. Introduction

Soit α un nombre algébrique; notons $h(\alpha)$ sa hauteur de Weil logarithmique et absolue. On sait alors que $h(\alpha)$ est nul si et seulement si α est une racine de l'unité. Le problème de Lehmer (voir [Le], §13, page 476) consiste à déterminer quelle est la minoration optimale (en fonction du degré $[\mathbb{Q}(\alpha) : \mathbb{Q}]$) de la hauteur $h(\alpha)$ si α n'est pas une racine de l'unité. Plus précisément:

Conjecture 1.1. *Il existe un nombre réel $c > 0$ tel que pour tout $\alpha \in \mathbb{G}_m(\bar{\mathbb{Q}})$, de degré D sur $\mathbb{Q}$, qui n'est pas une racine de l'unité, on ait*

$$h(\alpha) \geqq \frac{c}{D}.$$

On notera que Lehmer dans son texte était moins catégorique, et formulait plutôt la question en sens inverse. Alternativement, on peut également formuler la conjecture comme ceci: l'ensemble des mesures de Mahler des nombres algébriques n'est pas dense dans $[1, +\infty[$.

Rappelons que dans le cadre du problème de Lehmer, le meilleur résultat connu à ce jour (aux constantes numériques près) est la minoration de Dobrowolski ([Do]) qui obtient

$$h(\alpha) \geqq \frac{c}{D}\left(\frac{\log(\log(3D))}{\log(3D)}\right)^3,$$

si α n'est pas une racine de l'unité. Pour des raffinements des constantes numériques, on pourra se reporter aux travaux de Louboutin (voir [Lou]), ou plus récemment, de Voutier (voir [Vou]). Dans la direction de problème de Lehmer, d'autres résultats partiels existent toutefois. On sait en particulier que le problème de Lehmer est vrai si $\mathbb{Q}(\alpha)$ est totalement réel ou est un «corps C.M.» (voir [Schi]); que si $Dh(\alpha)$ est assez petit, alors α est un nombre réciproque (voir [Sm]). On sait également que si un nombre premier assez petit devant D est totalement décomposé dans $\mathbb{Q}(\alpha)$, alors $Dh(\alpha) \geqq c$ (voir [Mi]). On sait également conclure sous des hypothèses galoisiennes assez fortes (voir par exemple le manuscrit de M. Laurent, [La]).

On notera qu'à l'exception du résultat de Smyth (et de celui de Mignotte sur la décomposition des premiers dans $\mathbb{Q}(\alpha)$), toutes ces minorations ont en commun de traiter des cas où l'on attend (ou où l'on sait obtenir) des minorations bien plus fortes que celle de la conjecture 1.1.

On peut chercher à savoir quelle est la bonne généralisation de la conjecture 1.1 en dimension supérieure; pour ceci, il convient tout d'abord de normaliser convenablement la hauteur. Parmi les divers choix raisonnables qui sont possibles, nous effectuerons le suivant: soit $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$; nous désignerons par $h(\boldsymbol{\alpha})$ la hauteur de Weil du point projectif défini par $(1, \alpha_1, \ldots, \alpha_n)$. Remarquons que cette normalisation de la hauteur permet de conserver la propriété $h(\boldsymbol{\alpha}) = 0$ si et seulement si $\boldsymbol{\alpha}$ est de torsion. Géométriquement, ce choix revient à plonger $\mathbb{G}_m^n$ dans $\mathbb{P}^n$ naturellement, et à considérer la hauteur projective associée. Remarquons aussi que l'on a la majoration suivante:

$$h(\boldsymbol{\alpha}) \leqq h(\alpha_1) + \cdots + h(\alpha_n).$$

Notons par ailleurs, que le choix $h'(\boldsymbol{\alpha}) = h(\alpha_1) + \cdots + h(\alpha_n)$ correspond pour sa part au plongement

$$\mathbb{G}_m^n \hookrightarrow (\mathbb{P}^1)^n \xrightarrow{\text{Segre}} \mathbb{P}^{2^n - 1}.$$

De même, chaque compactification équivariante d'un tore conduit à une normalisation différente de la hauteur. Mais le choix des métriques à l'infini est imposé si l'on veut une hauteur «normalisée» $\hat{h}(\cdot)$, au sens de Philippon (voir [Ph3]), (voir aussi les constructions de Zhang, [Zha1]).

Dans tout le texte, nous noterons D le degré de l'extension $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$. Pour énoncer les conjectures les plus précises en dimension supérieure, il est utile de remplacer $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ par une notion plus géométrique que le nombre D; nous introduisons donc la notion suivante:

Définition 1.2. Soit $F_0 \in \mathbb{Q}[x_1, \ldots, x_n]$ un polynôme non nul s'annulant en $\boldsymbol{\alpha}$ de degré minimal. On appelera *indice d'obstruction* du point $\boldsymbol{\alpha}$ la quantité $\deg F_0$, que l'on notera $\delta(\boldsymbol{\alpha})$.

On dispose de l'encadrement

$$1 \leqq \delta(\boldsymbol{\alpha}) \leqq nD^{1/n}. \tag{1}$$

L'indice d'obstruction coïncide clairement avec le degré du corps de définition en dimension 1, mais il se trouve que c'est cette notion, plus géométrique, qui intervient naturellement dans notre construction.

Vérifions enfin l'assertion (1): si $\binom{\delta+n}{n} > D$, l'algèbre linéaire assure l'existence d'un polynôme non nul $F \in \mathbb{Q}[x_1, \ldots, x_n]$ s'annulant en $\boldsymbol{\alpha}$ et de degré au plus δ. Il suffit donc de remarquer que $\binom{\delta+n}{n} > n^{-n}\delta^n$ pour obtenir l'encadrement souhaité.

Avec ces notations on peut poser:

Conjecture 1.3. *Soit n un entier $\geqq 1$. Il existe alors un nombre réel $c(n) > 0$ tel que pour tout $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$, tel que $\alpha_1, \ldots, \alpha_n$ soient multiplicativement indépendants, on ait*

$$h(\boldsymbol{\alpha}) \geqq \frac{c(n)}{\delta(\boldsymbol{\alpha})}.$$

On notera que cette conjecture est clairement la meilleure possible, car si $m \geqq 1$, et si $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ est tel que $\boldsymbol{\beta}^m = (\beta_1^m, \ldots, \beta_n^m) = \boldsymbol{\alpha}$, on a

$$h(\boldsymbol{\beta}) = \frac{1}{m} h(\boldsymbol{\alpha}), \quad \delta(\boldsymbol{\beta}) \leqq m\delta(\boldsymbol{\alpha}).$$

On notera également que l'on ne peut faire l'économie de l'hypothèse d'indépendance multiplicative des coordonnées de $\boldsymbol{\alpha}$ (prendre $\boldsymbol{\alpha} = (\sqrt[m]{2}, \sqrt[m]{4}, \ldots, \sqrt[m]{2^n})$ ou plus simplement encore $\boldsymbol{\alpha} = (\sqrt[m]{2}, \ldots, \sqrt[m]{2})$).

Comme nous le fait remarquer l'arbitre, il est interessant de noter que ces résultats ne seraient plus vrais dans le cadre par exemple d'un corps de fonctions sur une courbe algébrique: il suffit de prendre par exemple $\alpha_i = f + i$ (pour $1 \leqq i \leqq n$), où f est une fonction algébrique de hauteur suffisamment petite (alors que le problème de Lehmer est lui, trivialement vrai dans ce cadre puisqu'il n'y a pas de places archimédiennes).

On peut également songer à des questions de volumes, en fait de nature «multi-homogène», a priori plus fortes que la conjecture 1.3:

Conjecture 1.4. *Soit n un entier $\geqq 1$. Il existe alors un nombre réel $c(n) > 0$ tel que pour tout $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$, tel que $\alpha_1, \ldots, \alpha_n$ soient multiplicativement indépendants, on ait*

$$\prod_{i=1}^{n} h(\alpha_i) \geqq \frac{c(n)}{D},$$

où $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$.

Toutefois, on peut aisément vérifier que la conjecture 1.3 implique la conjecture 1.4. Montrons cette implication. Soit k un entier positif assez grand et notons $A_i = [k.h(\alpha_i)]$. Soient ensuite $\beta_1, \ldots, \beta_n \in \bar{\mathbb{Q}}$ tels que $\beta_i^{A_i} = \alpha_i$ pour $i = 1, \ldots, n$. On a alors, pour $k \to +\infty$,

$$h(\boldsymbol{\beta}) \leqq A_1^{-1} h(\alpha_1) + \cdots + A_n^{-1} h(\alpha_n) \sim \frac{n}{k}.$$

L'inégalité (1) donne donc

$$\delta(\boldsymbol{\beta}) \leqq n[\mathbb{Q}(\beta_1, \ldots, \beta_n) : \mathbb{Q}]^{1/n} \leqq n(A_1 \cdots A_n D)^{1/n} \sim n\big(h(\alpha_1) \cdots h(\alpha_n) D\big)^{1/n} k.$$

La conjecture 1.3 implique maintenant

$$n \geqq \frac{c(n)}{n\big(h(\alpha_1) \cdots h(\alpha_n) D\big)^{1/n}},$$

d'où l'on déduit facilement la minoration pour le produit des hauteurs annoncée dans la conjecture 1.4.

Dans la direction de la conjecture 1.3, nous obtenons la minoration suivante:

Théorème 1.5. *Pour tout entier $n \geqq 1$, il existe un nombre réel $c(n) > 0$, tel que pour tout élément $\boldsymbol{\alpha}$ de $\mathbb{G}_m^n(\bar{\mathbb{Q}})$, dont les coordonnées sont multiplicativement indépendantes, on ait*

$$h(\boldsymbol{\alpha}) \geqq \frac{c(n)}{\delta(\boldsymbol{\alpha})} \log\big(3\delta(\boldsymbol{\alpha})\big)^{-\kappa(n)},$$

où $\kappa(n) = (n+1)(n+1)!^n - n$.

En utilisant l'inégalité (1) et une astuce «à la Landau» tout à faite similaire à celle qui nous a permis de montrer la conjecture 1.4 à partir de la conjecture 1.3, on en déduit:

Théorème 1.6. *Pour tout entier $n \geqq 1$, il existe un nombre réel $c(n) > 0$, tel que pour tout élément $\boldsymbol{\alpha}$ de $\mathbb{G}_m^n(\bar{\mathbb{Q}})$, dont les coordonnées sont multiplicativement indépendantes, on ait*

$$\prod_{i=1}^{n} h(\alpha_i) \geqq \frac{c(n)}{D} \log(3D)^{-n\kappa(n)},$$

où $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$.

Comme nous n'avons pas réellement cherché à optimiser les estimations, ce résultat ne coïncide pas tout à fait avec celui de Dobrowolski pour $n = 1$, puisque nous n'avons pas le terme correctif en $\log\log(3D)$ au numérateur. Toutefois, même si des raffinements ne sont pas à exclure, il semble que la croissance très rapide de κ en n soit inhérente à la méthode.

En dimension supérieure, aucun résultat donnant mieux que la minoration de Dobrowolski n'était connue.

Citons toutefois le résultat récent de Matveev (voir [Ma]) qui a étudié les minima successifs pour une fonction hauteur modifiée. Plus précisément, Matveev obtient des minorations pour la fonction: $h_*(\alpha) = \max\{Dh(\alpha), |\log(\alpha)|_v\}$, où v est une place divisant l'infini.

Nos résultats permettent également d'obtenir quelques informations partielles sur la structure du corps de nombres engendré par un contre-exemple éventuel au problème de Lehmer:

Corollaire 1.7. *Il existe une constante $c > 0$, telle que pour tout $\alpha \in \mathbb{G}_m(\bar{\mathbb{Q}})$ de degré D sur $\mathbb{Q}$, qui n'est pas une racine de l'unité, on ait*:

Si l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne, alors: $h(\alpha) \geqq c/D$.

Plus généralement, on a le corollaire suivant, qui montre qu'un contre-exemple éventuel au problème de Lehmer possède un «gros» groupe de Galois:

Corollaire 1.8. *Pour tout entier $m \geqq 1$, il existe une constante $c(m) > 0$, telle que la propriété suivante soit vraie. Soit α un nombre algébrique, de degré D sur $\mathbb{Q}$, notons D_G le degré sur $\mathbb{Q}$ de la clôture galoisienne de $\mathbb{Q}(\alpha)/\mathbb{Q}$. Alors, si α n'est pas une racine de l'unité, et si $D_G \leqq D^m$, on a*

$$h(\alpha) \geqq \frac{c(m)}{D}.$$

L'intérêt de ces corollaires est le suivant. La manière la plus naturelle de construire des nombres de petite hauteur est de procéder par extraction de racine. Heuristiquement, l'énoncé de la conjecture 1.1 affirme que l'on ne peut construire autrement des nombres de hauteur plus petite encore. Le corollaire 1.8 permet de dire qu'au moins dans les extensions algébriques de ce type, c'est effectivement le cas. En particulier, ce corollaire n'est pas une conséquence des résultats de Schinzel (ou Laurent), puisque ce dernier traite de cas où l'on peut obtenir bien mieux que Lehmer, ce qui n'est pas (et pour cause!) le cas ici. Par contre, il n'est pas exclu que le corollaire 1.7 ne soit pas nouveau.

En étudiant les groupes de relations multiplicatives, D. Bertrand (voir [Be], §2) a posé des questions liées au problème de Lehmer. Fixons tout d'abord quelques notations. Soient $\mathbb{K}$ un corps de nombres, $\Sigma_{\mathbb{K}}$ l'ensemble des places à l'infini de $\mathbb{K}$ et $\sigma_{\mathbb{K}}$ le cardinal de $\Sigma_{\mathbb{K}}$. Donc $\sigma_{\mathbb{K}} = r_{\mathbb{K}} + s_{\mathbb{K}}$, où $r_{\mathbb{K}}$ est le nombre des plongements de $\mathbb{K}$ dans $\mathbb{R}$ et $s_{\mathbb{K}}$ est la moitié du nombre des plongements non-réels de $\mathbb{K}$ dans $\mathbb{C}$. Notons également $\mathbb{U}_{\mathbb{K}}$ le groupe des unités de $\mathbb{K}$ (il est alors de rang $\sigma_{\mathbb{K}} - 1$), et $\mu(\mathbb{K})$ le sous-groupe des racines de l'unité. Considérons le plongement logarithmique:

$$\mathscr{L}: \quad \mathbb{U}_{\mathbb{K}} \to \mathbb{R}^{\sigma_{\mathbb{K}}},$$

$$\alpha \quad \mapsto (d_v \log|\alpha|_v)_{v \in \Sigma_{\mathbb{K}}},$$

où d_v vaut 1 si v est réelle et 2 sinon. L'image de $\mathscr{L}$ est un réseau dans un hyperplan de $\mathbb{R}^{\sigma_{\mathbb{K}}}$ (isomorphe à $\mathbb{U}_{\mathbb{K}}/\mu(\mathbb{K})$). Munissons $\mathbb{R}^{\sigma_{\mathbb{K}}}$ de la norme L_2 naturelle. Si G est un sous-groupe discret de $\mathbb{R}^{\sigma}$, on notera $\mathrm{Vol}(G)$ son covolume (dans le $\mathbb{R}$-sous-espace vectoriel $G \otimes_{\mathbb{Z}} \mathbb{R}$ de $\mathbb{R}^{\sigma}$). Pour tout entier $n \in [1, \sigma_{\mathbb{K}}[$, on pose alors

$$V_n(\mathbb{K}) = \min\{\mathrm{Vol}(\mathscr{L}(\Delta)),\ \Delta \text{ sous-groupe de } \mathbb{U}_{\mathbb{K}} \text{ de rang } n\}.$$

Donc $V_1(\mathbb{K})$ est le minimum de $\|\mathscr{L}(\alpha)\|_{L_2}$ pour $\alpha \in \mathbb{U}_{\mathbb{K}} \setminus \mu(\mathbb{K})$ (où $\mu(\mathbb{K})$ est l'ensemble des racines de l'unité de $\mathbb{K}$), et $V_{\sigma_{\mathbb{K}}-1}(\mathbb{K}) = 2^{r_{\mathbb{K}}} \pi^{s_{\mathbb{K}}} \mathrm{Reg}(\mathbb{K})$, où $\mathrm{Reg}(\mathbb{K})$ est le régulateur de $\mathbb{K}$.

La question posée par D. Bertrand peut alors se formuler ainsi:

Problème 1.9 (Bertrand). (i) *Existe-t-il une constante $c > 0$ et une fonction $f : [2, +\infty[\cap \mathbb{N} \to \mathbb{N}$, vérifiant $1 \leqq f(\sigma) < \sigma$ et $\limsup_{\sigma \to \infty} f(\sigma)/\sigma < 1$, telles que*

$$V_{f(\sigma_{\mathbb{K}})}(\mathbb{K}) \geqq c$$

pour tout corps de nombres $\mathbb{K}$?

(ii) *Existe-t-il une constante $c > 0$ et un nombre $n \geqq 2$ tel que pour tout corps de nombres $\mathbb{K}$ tel que $\sigma_{\mathbb{K}} \geqq n+1$, on ait*

$$V_n(\mathbb{K}) \geqq c?$$

(iii) *Existe-t-il une constante $c > 0$ telle que pour tout corps de nombres $\mathbb{K}$, tel que $\sigma_{\mathbb{K}} \geqq 2$, on ait*

$$V_1(\mathbb{K}) \geqq \frac{c}{\sqrt{\sigma_{\mathbb{K}}}}?$$

On notera que le point (iii) est une conséquence du problème de Lehmer, et que le point (ii) entraîne le point (i) (choisir $f(\sigma) = 1$ si $\sigma \leqq n$ et $f(\sigma) = n$ sinon). On notera aussi que la conjecture 1.4 entraîne une propriété plus forte que le point (ii), à savoir

$$V_n(\mathbb{K}) \geqq c(n) D^{\frac{n-2}{2}}$$

(confer la démonstration du corollaire 1.10, dans le paragraphe 6). On pourra noter (suivant D. Bertrand) que les questions posées dans le problème 1.9 sont de nature intermédiaire entre les problèmes de type Lehmer (conjectures 1.1 et 1.3) et des questions de type Schinzel-Zassenhaus (puisque la norme L_2 s'intercale entre les normes L_1 et L_∞); on pourrait également formuler des analogues de ces derniers en dimension supérieure.

Dans cette direction, nous obtenons le

Corollaire 1.10. *Pour tout entier $n \geqq 1$, il existe une constante $c(n) > 0$, telle que pour tout corps de nombres $\mathbb{K}$ tel que $\sigma_{\mathbb{K}} \geqq n+1$, on ait*

$$V_n(\mathbb{K}) \geqq c(n) D^{\frac{n-2}{2}} \log(3D)^{-n\kappa(n)},$$

où $D = [\mathbb{K} : \mathbb{Q}]$.

En particulier, si $n = 3$, on en déduit la minoration

$$V_3(\mathbb{K}) \geqq c(3) D^{\frac{1}{2}} \log(3D)^{-55293} \geqq c > 0 .$$

Ce résultat répond donc affirmativement à la question (ii) (et donc aussi à la question (i)) du problème ci-dessus.

Signalons enfin qu'une généralisation de notre résultat dans le cadre des variétés abéliennes à multiplications complexes se trouve dans [Da-Hi].

Le plan de cet article est le suivant. On a rassemblé au paragraphe 2 différentes estimations sur les sous-variétés algébriques de $\mathbb{G}_m^n$ et en particulier sur leur stabilisateur. On y trouvera également un analogue des lemmes 2 et 3 de [Do] en dimension supérieure (lemme 2.3). Dans le paragraphe 3, on trouvera deux résultats qui sont importants pour la preuve du théorème principal. Le premier (théorème 3.1) est un analogue du lemme-clef de Dobrowolski (voir [Do], lemme 1), qui permet d'extrapoler, nécessitant un argument plus sophistiqué qu'une simple application du petit théorème de Fermat sur les polynômes. Le deuxième (théorème 3.3) est une version du lemme de zéros de Philippon (voir [Ph1], théorème 2. 1, et [Ph2], théorèmes 1 ou 2) avec multiplications. Au paragraphe 4, nous avons développé la machinerie de transcendance (lemme de Siegel, estimation du rang, extrapolation). La preuve du théorème 1.5 est donnée au paragraphe 5 (choix des paramètres au § 5.1, argument de descente au § 5.2, et enfin preuve au § 5.3). Le théorème 1.6 et les différents corollaires sont enfin démontrés au paragraphe 6.

Notations. Dans tout ce texte, on note $\alpha_1, \ldots, \alpha_n$ des nombres algébriques non nuls et $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$. On note aussi $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, D son degré, $\mathbb{F}$ sa clôture galoisienne, $\sigma_1, \ldots, \sigma_D$ les $\mathbb{Q}$-homomorphismes $\mathbb{K} \to \mathbb{F}$ et $\mathscr{M}_{\mathbb{F}}$ l'ensemble des valeurs absolues de $\mathbb{F}$, normalisées de la façon usuelle (i.e. $|p|_v = p^{-1}$ si v divise le nombre premier p). Enfin, on note $h(\boldsymbol{\alpha})$ la hauteur de Weil du point projectif défini par $(1, \alpha_1, \ldots, \alpha_n)$.

Au cours de diverses discussions, R. Dvornicich et P. Philippon ont bien voulu nous donner leurs point de vue sur bien des questions. C'est un plaisir pour nous de pouvoir les remercier chaleureusement ici. C'est également un plaisir de remercier M. Mignotte qui a bien voulu nous faire part de ses commentaires sur une version initiale de ce travail.

2. Géométrie

Soit n un entier $\geqq 1$; dans toute la suite du texte, nous plongerons $\mathbb{G}_m^n$ naturellement dans $\mathbb{P}^n$. Soient $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{G}_m^n$ et soit $l \in \mathbb{Z}$; on notera:

$$\boldsymbol{x}.\boldsymbol{y} = (x_1 y_1, \ldots, x_n y_n), \quad [l]\boldsymbol{x} = (x_1^l, \ldots, x_n^l),$$

et $\ker([l]) = \{\boldsymbol{x} \in \mathbb{G}_m^n, [l]\boldsymbol{x} = (1, \ldots, 1)\}$. Si W est une sous-variété de $\mathbb{G}_m^n$, on notera G_W le stabilisateur de W, i.e. l'ensemble

$$G_W = \{\boldsymbol{x} \in \mathbb{G}_m^n,\ \boldsymbol{x}.W = W\} = \bigcap_{\boldsymbol{y} \in W} \boldsymbol{y}^{-1}.W;$$

on notera également G_W^0 la composante neutre de G_W, i.e. le plus grand sous-groupe connexe de G_W. Par «degré» de la variété W, noté $\deg(W)$, on entendra le degré de l'adhérence de Zariski de W dans $\mathbb{P}^n$. Remarquons que $\dim(G_W) \leqq \dim(W)$ (par définition du stabilisateur). De plus, on a $\deg(G_W) \leqq \deg(W)^{\dim(W)+1}$; en effet, notons s la dimension de G_W et d celle de W. Il existe des hypersurfaces $(Z_i)_{1 \leqq i \leqq n-d}$ de degré au plus $\deg(W)$ telles que W soit une composante isolée de l'intersection des Z_i et de $\mathbb{G}_m^n$. Par définition de G_W, il existe des éléments $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{d-s}$ de W tels que les composantes connexes de G_W soient des composantes isolées de

$$\boldsymbol{x}_0^{-1}.W \cap \Big(\bigcap_{1 \leqq i \leqq d-s} \boldsymbol{x}_i^{-1}.Z_{j_i}\Big),$$

où $1 \leqq j_i \leqq n-d$. Le théorème de Bézout donne donc bien (puisque le degré d'une sous-variété de $\mathbb{G}_m^n$ est invariant par translation)

$$\deg(G_W) \leqq \deg(W)^{d-s+1} \leqq \deg(W)^{d+1}.$$

On pourra également se reporter à [Hi], lemme 8 pour ce point.

Dans l'énoncé suivant on trouvera des résultats plus ou moins «bien connus» sur le degré de l'image d'une variété géométriquement irréductible par des morphismes de multiplication.

Lemme 2.1. *Soit W une sous-variété propre et géométriquement irréductible de $\mathbb{G}_m^n$, et soit $l \in \mathbb{Z}$. On a alors les propriétés suivantes*:

(i)
$$\deg([l]\,W) = \frac{|l|^{\dim(W)} \deg(W)}{|\ker([l]) \cap G_W|}.$$

(ii)
$$|\ker([l]) \cap G_W| = |l|^{\dim(G_W)}.|\ker([l]) \cap (G_W/G_W^0)|,$$

où l'on note indifféremment $[l]$ la multiplication par l dans $\mathbb{G}_m^n$ ou dans le tore quotient $\mathbb{G}_m^n/G_W^0$. Plus particulièrement, on a l'encadrement

$$|l|^{\dim(G_W)} \leqq |\ker([l]) \cap G_W| \leqq |G_W/G_W^0|.|l|^{\dim(G_W)}.$$

Démonstration. Pour les points (i) voir par exemple [Hi], lemme 6. Pour le point (ii), il suffit de remarquer que

$$|\ker([l]) \cap G_W| = |\ker([l]) \cap G_W^0|.|\ker([l]) \cap (G_W/G_W^0)|$$

et que $|\ker([l]) \cap G_W^0| = |l|^{\dim(G_W)}$. Le lemme 2.1 est donc entièrement établi.

Soit V une sous-variété propre de $\mathbb{G}_m^n$, définie sur $\mathbb{Q}$ et $\mathbb{Q}$-irréductible. Nous aurons besoin dans la suite de travailler avec des «bons» entiers, pour lesquels les conjugués (sous l'action du groupe de Galois absolu) des multiples des composantes géométriquement irréductibles de V sont distincts *et* tels que les degrés de ces multiples ne soient pas trop petits. Cela nous conduit à poser la définition suivante:

Définition 2.2. Soit V une sous-variété algébrique propre de $\mathbb{G}_m^n$, définie sur $\mathbb{Q}$ et $\mathbb{Q}$-irréductible, et notons $W_1, \ldots, W_k$ ses composantes $\bar{\mathbb{Q}}$-irréductibles. On pose

$$E(V) = \{l \in \mathbb{Z},\ \exists i, j,\ 1 \leqq i < j \leqq k,\ [l](W_i) = [l](W_j)\}$$
$$\cup \{l \in \mathbb{Z},\ \exists i,\ 1 \leqq i \leqq k,\ \deg([l]W_i) < \deg(W_i)\}\,.$$

Nous nous proposons maintenant de montrer quelques propriétés de l'ensemble $E(V)$ qui nous seront utile dans la suite. Pour ce faire, on commence par montrer le lemme suivant qui est l'analogue pour les sous-variétés de $\mathbb{G}_m^n$ des lemmes de Dobrowolski qui affirment que les conjugués des multiples d'un point sont essentiellement distincts (voir [Do], lemme 2, point (ii) et lemme 3).

Lemme 2.3. *Soit V une sous-variété propre de $\mathbb{G}_m^n$, définie sur $\mathbb{Q}$ et $\mathbb{Q}$-irréductible, de dimension d; nous noterons $W_1, \ldots, W_k$ ses composantes géométriquement irréductibles.*

(i) *Supposons que V ne soit pas une réunion de translatés des sous-tores*[1]*) de $\mathbb{G}_m^n$ par des points de torsion. Alors, pour tous les entiers l, l' avec $|l| \neq |l'|$ et pour tout les entiers i, j tels que $1 \leqq i, j \leqq k$, les sous-variétés $[l](W_i)$ et $[l'](W_j)$ sont distinctes.*

(ii) *Soit $\mathscr{P}$ un sous-ensemble de $\mathbb{Z}$ formé de nombres deux à deux premiers entre eux. Alors, le sous-ensemble de $\mathscr{P}$*

$$\mathscr{Q} = \{l \in \mathscr{P},\ \exists i, j,\ 1 \leqq i < j \leqq k,\ [l](W_i) = [l](W_j)\}$$

est de cardinal au plus $(\log k)/(\log 2)$.

Démonstration. Démontrons (i). Soit $W = W_1$, et supposons donné un élément σ de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que $[l](W) = [l']\big(\sigma(W)\big)$. Puisque les multiplications par des entiers commutent entre elles et avec σ, on déduit, par itération de l'hypothèse,

$$[l^n](W) = [l'^n]\big(\sigma^n(W)\big) \tag{2}$$

pour tout entier $n \geqq 1$. Soit n_0 le plus petit entier n pour lequel $\sigma^n(W) = W$. On tire de la relation précédente que $[l^m](W) = [l'^m](W)$, pour tout multiple m de n_0. L'égalité des deux variétés assure celle de leur degré; le lemme 2.1, point (i) nous assure alors que

$$\frac{|l|^{dm}}{|\ker([l^m]) \cap G_W|} = \frac{|l'|^{dm}}{|\ker([l'^m]) \cap G_W|}\,,$$

[1]) Nous utiliserons le vocable «sous-tore» pour désigner les sous-groupes algébriques *connexes* de $\mathbb{G}_m^n$, et le terme «sous-groupe algébrique» lorsqu'il n'y a pas d'hypothèse de connexité spécifique.

pour tout multiple $m \geqq 1$ de n_0. Si les nombres $|l|$ et $|l'|$ sont distincts, quitte à échanger les rôles de l et l', nous pouvons supposer que $|l| < |l'|$. Notons d_0 la dimension de G_W; le lemme 2.1, point (ii) donne maintenant

$$\left(\frac{|l|}{|l'|}\right)^{dm} \leqq |G_W/G_W^0| \left(\frac{|l|}{|l'|}\right)^{d_0 m},$$

ce qui est impossible (faire tendre m vers l'infini et remarquer que $d_0 \leqq d$), sauf si $d = d_0$, i.e. sauf si W est un translaté d'un sous-tore H de $\mathbb{G}_m^n$. Posons donc $W = \boldsymbol{x}.H$; on tire de la relation $[l^{n_0}](W) = [l'^{n_0}](W)$, que $[l^{n_0}.l'^{-n_0}]\boldsymbol{x} \in H$, c'est-à-dire que $\boldsymbol{x}$ est de torsion modulo H.

Soit maintenant K un supplémentaire de H dans $\mathbb{G}_m^n$ et écrivons $\boldsymbol{x} = \boldsymbol{k}.\boldsymbol{h}$ avec $\boldsymbol{k} \in K$ et $\boldsymbol{h} \in H$: on en déduit facilement que $W = \boldsymbol{k}.H$ et que $\boldsymbol{k}$ est un point de torsion de $\mathbb{G}_m^n$. On a alors

$$V = \{\sigma(\boldsymbol{k})H,\ \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\}$$

(rappelons que H est défini sur $\mathbb{Q}$). Mais, $\{\sigma(\boldsymbol{k}),\ \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\}$ est un ensemble fini de points de torsion, et par suite V est une réunion de translatés de sous-tores de $\mathbb{G}_m^n$ par des points de torsion; c'est ce que l'on voulait. Le point (i) est donc établi.

Passons maintenant au point (ii). Ce point ne diffère pas de l'argument de Dobrowolski (voir [Do], lemme 3) dans le cas de la dimension 0; seules des modifications de nature purement formelles sont nécessaires au cours de la rédaction. Nous donnons toutefois une preuve complète afin de rassurer le lecteur. Pour tout élément l de $\mathbb{Z}$ et pour tout indice i, $1 \leqq i \leqq k$, notons:

$$\mathscr{I}(l, i) = \{j,\ [l](W_i) = [l](W_j)\}.$$

On remarque que, pour tout $l \in \mathbb{Z}$, les ensembles $\mathscr{I}(l, i)$ $(1 \leqq i \leqq k)$ ont même cardinal (en effet le groupe de Galois $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ permute transitivement les W_i), et deux d'entres eux sont soit disjoints soit égaux. Nous allons montrer que pour tout $l, l' \in \mathbb{Z}$ premiers entre eux et pour tout indice i, on a

$$|\mathscr{I}(ll', i)| \geqq |\mathscr{I}(l, i)|.|\mathscr{I}(l', i)|. \tag{3}$$

On commence par noter que

$$\mathscr{I}(ll', i) \supset \bigcup_{j \in \mathscr{I}(l,i)} \mathscr{I}(l', j). \tag{4}$$

En effet, si $m \in \mathscr{I}(l', j)$ et si $j \in \mathscr{I}(l, i)$, on a $[l'](W_m) = [l'](W_j)$ et $[l](W_j) = [l](W_i)$, ce qui donne $[ll'](W_i) = [ll'](W_m)$, c'est-à-dire $m \in \mathscr{I}(ll', i)$. Pour montrer l'inégalité (3), il suffit donc de montrer que la réunion dans l'inclusion (4) est disjointe. Démontrons cela.

Soient donc $j_1, j_2 \in \mathscr{I}(l, i)$ et supposons $\mathscr{I}(l', j_1) \cap \mathscr{I}(l', j_2) \neq \emptyset$: on a alors $[l]W_{j_1} = [l]W_{j_2}$ et $[l']W_{j_1} = [l']W_{j_2}$, ce que revient à dire qu'il existe $\boldsymbol{x} \in \ker([l])$ et $\boldsymbol{x}' \in \ker([l'])$ tels que $W_{j_2} = \boldsymbol{x}.W_{j_1} = \boldsymbol{x}'.W_{j_1}$. On en tire que $(\boldsymbol{x}')^{-1}\boldsymbol{x}$ est un élément du

stabilisateur $G_{W_{j_1}}$ de W_{j_1}. Comme l et l' sont premiers entre eux, il existe (Bézout) des entiers u et v tels que $ul + vl' = 1$. Comme $\boldsymbol{x}$ est dans $\ker[l]$ et $\boldsymbol{x}'$ est dans $\ker[l']$, on en déduit que

$$\boldsymbol{x} = \boldsymbol{x}^{1-ul} = \boldsymbol{x}^{vl'} = \big((\boldsymbol{x}')^{-1}\boldsymbol{x}\big)^{vl'} \in G_{W_{j_1}}$$

et donc $W_{j_2} = \boldsymbol{x}.W_{j_1} = W_{j_1}$, c'est-à-dire $j_1 = j_2$. On a bien montré que la réunion dans (4) est disjointe, et donc la relation (3) est aussi démontrée.

Dire que l appartient à l'ensemble $\mathscr{Q}$ introduit dans le lemme 2.3, revient à dire que $|\mathscr{I}(l, i)| \geqq 2$ (pour au moins un i, c'est-à-dire pour tout i). On en tire, grâce à (3),

$$2^{|\mathscr{Q}|} \leqq \prod_{l \in \mathscr{P}} |\mathscr{I}(l,1)| \leqq \left| \mathscr{I}\Big(\prod_{l \in \mathscr{P}} l, 1\Big) \right| \leqq k\,.$$

Le point (ii) et donc le lemme 2.3 est entièrement établi.

Nous pouvons maintenant énoncer la proposition suivante qui résume les propriétés principales de l'ensemble $E(V)$ dont nous aurons besoin; pour l'essentiel, ces dernières seront utilisées au paragraphe 5.2:

Proposition 2.4. *Soit V une sous-variété propre de $\mathbb{G}_m^n$, définie sur $\mathbb{Q}$ et $\mathbb{Q}$-irréductible, de dimension d et notons $W_1, \ldots, W_k$ ses composantes $\bar{\mathbb{Q}}$-irréductibles. On a alors*:

(i) $$|E(V) \cap \{p \text{ premier}\}| \leqq \frac{d+1}{\log(2)} \log \deg(V).$$

(ii) *Si $l, l' \in \mathbb{Z}$, $l \notin E(V)$ et $l' \notin E([l]V)$, alors $l'l \notin E(V)$.*

(iii) *Si Λ est un ensemble fini d'entiers positifs ne rencontrant pas $E(V)$ et si V n'est pas une réunion de translatés de sous-tores de $\mathbb{G}_m^n$ par des points de torsion, on a*

$$\deg\Big(\bigcup_{l \in \Lambda} [l]V\Big) \geqq |\Lambda| \deg(V)\,.$$

(iv) *Soit $l \notin E(V)$ un entier et $\tilde{V}$ une sous-variété de $\mathbb{G}_m$, définie sur $\mathbb{Q}$ et ayant la même dimension que V, et telle que $V \subset [l]^{-1}\tilde{V}$. On a alors*

$$\deg(V) \leqq \deg(\tilde{V})\,.$$

Démonstration. Montrons (i). Tout d'abord, si $l \in \mathbb{Z}$ tel que $\deg([l]W_i) < \deg(W_i)$ pour un certain indice i, alors cette inégalité est vraie pour tout i (car, comme l'on a déjà remarqué avant, le groupe de Galois $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ permute transitivement les W_i). Posons $W = W_1$; en utilisant le lemme 2.1, points (i) et (ii), et l'inégalité $\dim(G_W) \leqq \dim(W)$, on en déduit que $\deg([l]W) \geqq \deg(W)$ pour tout entier l premier à $|G_W/G_W^0|$. Il y a au plus $\log(|G_W/G_W^0|)/\log(2)$ premiers qui divisent $|G_W/G_W^0|$ et l'on a

$$|G_W/G_W^0| \leqq \deg(G_W) \leqq \deg(W)^{d+1}\,.$$

Donc l'ensemble des nombres premiers p pour lesquels $\deg([p]W_i) < \deg(W_i)$ (pour au moins un i, c'est-à-dire pour tout i) est de cardinal au plus:

$$\frac{d+1}{\log 2}\log\big(\deg(W)\big) = \frac{d+1}{\log 2}\log\left(\frac{\deg(V)}{k}\right)$$

(puisque $\deg(V) = k\deg(W)$).

D'autre part, le lemme 2.3, point (ii), donne

$$|\{p \text{ premier}, \exists i,j,\ 1 \leqq i < j \leqq k,\ [p](W_i) = [p](W_j)\}| \leqq \frac{\log k}{\log(2)}.$$

On en déduit que $E(V) \cap \{p \text{ premier}\}$ est de cardinal au plus:

$$\frac{\log k}{\log 2} + \frac{d+1}{\log 2}\log\left(\frac{\deg(V)}{k}\right) \leqq \frac{d+1}{\log 2}\log\deg(V),$$

ce qui montre le point (i).

Montrons (ii). Tout d'abord, pour $i = 1, \ldots, k$, on a $\deg(W_i) \leqq \deg([l]W_i)$ (car $l \notin E(V)$) et $\deg([l]W_i) \leqq \deg([l'l]W_i)$ (car $[l]W_i$ est une composante géométriquement irréductible de $[l]V$ et car $l' \notin E([l]V)$); donc,

$$\deg(W_i) \leqq \deg([l'l]W_i).$$

Ensuite, $[l]V = [l]W_1 \cup \cdots \cup [l]W_k$, et les variétés géométriquement irréductibles:

$$[l]W_1, \ldots, [l]W_k$$

sont distinctes, car $l \notin E(V)$. On a donc

$$[l'l]W_i \neq [l'l]W_j, \quad 1 \leqq i < j \leqq k,$$

car $l' \notin E([l]V)$.

Montrons maintenant (iii). Le lemme 2.3, points (i) et (ii), assure que $[l]W_i \neq [l']W_j$ pour $l, l' \in \Lambda$ et $1 \leqq i, j \leqq k$ avec $(l,i) \neq (l',j)$; d'autre part, par hypothèse sur Λ, on a $\deg([l]W_i) \geqq \deg(W_i)$ pour $i = 1, \ldots, k$ et pour tout $l \in \Lambda$. Donc

$$\deg\Big(\bigcup_{l\in\Lambda}[l]V\Big) = \sum_{l\in\Lambda}\sum_{i=1}^{k}\deg([l]W_i) \geqq |\Lambda|\deg(V).$$

Montrons enfin, le point (iv). Par le lemme 2.3, point (ii), on a $[l]W_i \neq [l]W_j$ pour $1 \leqq i < j \leqq k$, et, comme auparavant, $\deg([l]W_i) \geqq \deg(W_i)$ pour $i = 1, \ldots, k$. Donc, $\deg([l]V) \geqq \deg(V)$. D'autre part, $[l]V \subset \tilde{V}$ et ces variétés ont la même dimension; on en déduit:

$$\deg(V) \leqq \deg([l]V) \leqq \deg(\tilde{V}).$$

La proposition 2.4 est donc entièrement établie.

Nous terminons ce paragraphe avec un résultat de M. Chardin (voir [Ch], corollaire 2, chapitre 1, page 8 et exemple 1, page 9) qui nous sera utile dans la suite du texte. Soit $\wp \subset \mathbb{Q}[x_0, \ldots, x_n]$ un idéal homogène, premier, de codimension r; le résultat cité de loc. cit. nous assure de l'existence d'un polynôme homogène et non nul $F \in \wp$ dont le degré est majoré par

$$\left(\frac{n! \deg(\wp)}{(n-r)!}\right)^{1/r}.$$

En utilisant l'inégalité $\dfrac{n!}{(n-r)!} \leqq n^r$, et la définition 1.2, on en déduit:

Proposition 2.5. *Soit V une sous-variété algébrique propre de $\mathbb{G}_m^n$, définie sur $\mathbb{Q}$ et $\mathbb{Q}$-irréductible, passant par un certain $\boldsymbol{\alpha} \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$. On a alors*

$$\delta(\boldsymbol{\alpha}) \leqq n\big(\deg(V)\big)^{1/\operatorname{codim}(V)}.$$

3. Deux résultats auxiliaires

Comme on l'a déjà rappelé dans l'introduction, nous avons rassemblé dans ce paragraphe deux résultats qui seront utiles pour la preuve du théorème principal: la généralisation en plusieurs variables du lemme-clef de Dobrowolski et une version du lemme de zéros de Philippon avec multiplications.

3.1. Une généralisation du lemme-clef de Dobrowolski. Le théorème suivant généralise le lemme 1 de Dobrowolski (voir [Do], lemme 1); la difficulté essentielle étant que les anneaux de polynômes en plusieurs variables ne sont plus principaux:

Théorème 3.1. *Soit $F \in \mathbb{Z}[x_1, \ldots, x_n]$ de degré $\leqq L$ et nul à un ordre $\geqq T$ en $\boldsymbol{\alpha} \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$. Pour tout nombre premier $p \in \mathbb{Z}$ et pour tout $v \in \mathscr{M}_{\mathbb{F}}$ divisant p, on a la majoration*

$$|F(\boldsymbol{\alpha}^p)|_v \leqq p^{-T} \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{pL},$$

où l'on a noté $\boldsymbol{\alpha}^p = (\alpha_1^p, \ldots, \alpha_n^p)$.

Démonstration. Notons $\mathcal{O}_{\mathbb{K}}$ l'anneau des entiers du corps de nombres $\mathbb{K}$ et supposons pour le moment que $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_{\mathbb{K}}$. Il existe alors des éléments $\alpha_{n+1}, \ldots, \alpha_s$ de $\mathcal{O}_{\mathbb{K}}$ tels que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha_1, \ldots, \alpha_s]$. Notons $\mathfrak{q}$ l'idéal de définition de $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s)$(pour alléger, nous noterons encore par la même lettre ce nouveau point) dans $\mathbb{Z}[\boldsymbol{x}] = \mathbb{Z}[x_1, \ldots, x_s]$.

Nous allons vérifier que $\mathfrak{q}^T$ est primaire. Soit $\mathfrak{m}$ un idéal maximal de $\mathbb{Z}[\boldsymbol{x}]$ contenant $\mathfrak{q}$ et soit $\mathscr{A} = \mathbb{Z}[\boldsymbol{x}]_{\mathfrak{m}}$. Par abus de notation, on notera encore $\mathfrak{q}$ (respectivement $\mathfrak{m}$) l'extension de $\mathfrak{q}$ (respectivement de $\mathfrak{m}$) à l'anneau $\mathscr{A}$. L'anneau $\mathscr{A}$ est local régulier de dimension $s+1$ et $\mathscr{A}/\mathfrak{q}$ est un anneau de valuations discrètes (grâce à l'hypothèse $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\boldsymbol{\alpha}]$); il est donc a fortiori régulier. On déduit alors d'un théorème de Chevalley (voir [Za-Sa], chapitre 8, §11, theorem 26, page 303) que $\mathfrak{q}$ est engendré par un sous-

ensemble d'un système de paramètres de l'anneau $\mathscr{A}$. Ce système est une suite régulière et donc $\mathfrak{q}^T$ est primaire dans $\mathscr{A} = \mathbb{Z}[\boldsymbol{x}]_{\mathfrak{m}}$ (confer [Za-Sa], appendix 6, corollary 2, page 399 et lemma 5, page 401). Cette propriété étant vraie pour tout idéal maximal $\mathfrak{m}$ de $\mathbb{Z}[\boldsymbol{x}]$ contenant $\mathfrak{q}$, on en déduit bien que $\mathfrak{q}^T$ est primaire dans $\mathbb{Z}[\boldsymbol{x}]$.

Montrons maintenant que $F \in \mathfrak{q}^T$. Pour cela, notons

$$\mathfrak{M}_j = \big(x_1 - \sigma_j(\alpha_1), \ldots, x_s - \sigma_j(\alpha_s)\big), \quad j = 1, \ldots, D,$$

l'idéal de définition de $\sigma_j(\boldsymbol{\alpha})$ dans $\bar{\mathbb{Q}}[\boldsymbol{x}]$. On a alors

$$\mathfrak{q}\bar{\mathbb{Q}}[\boldsymbol{x}] = \bigcap_{j=1}^{D} \mathfrak{M}_j = \prod_{j=1}^{D} \mathfrak{M}_j.$$

Puisque par hypothèse, F est nulle en $\boldsymbol{\alpha}$ à un ordre $\geqq T$, la relation ci-dessus montre que $F \in (\mathfrak{q}\bar{\mathbb{Q}}[\boldsymbol{x}])^T \cap \mathbb{Q}[\boldsymbol{x}]$, et donc

$$F \in (\mathfrak{q}\bar{\mathbb{Q}}[\boldsymbol{x}])^T \cap \mathbb{Q}[\boldsymbol{x}] = (\mathfrak{q}^T\bar{\mathbb{Q}}[\boldsymbol{x}]) \cap \mathbb{Q}[\boldsymbol{x}] = \mathfrak{q}^T\mathbb{Q}[\boldsymbol{x}]$$

(la dernière égalité découle des relations entre extension et contraction des idéaux dans les anneaux de polynômes sur un corps: confer [Za-Sa], chapitre 7, §11, page 221, relation (1)). Il existe donc un entier rationnel $a \neq 0$ tel que $aF \in \mathfrak{q}^T$; par ailleurs, nous avons déjà montré que $\mathfrak{q}^T$ est primaire, d'où: $F \in \mathfrak{q}^T$, comme annoncé.

On peut alors écrire

$$F = \sum_{i \in \mathbb{N}^T} f_{i_1} \cdots f_{i_T},$$

où les f_{i_l} sont des éléments de $\mathfrak{q}$. Soit $p \in \mathbb{Z}$ un premier; le petit théorème de Fermat appliqué aux f_{i_l} donne:

$$f_{i_l}(x_1^p, \ldots, x_s^p) = f_{i_l}(\boldsymbol{x})^p + p g_{i_l}(\boldsymbol{x}), \quad g_{i_l}(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}].$$

On en tire

$$F(\boldsymbol{\alpha}^p) = p^T \sum_{i \in \mathbb{N}^T} g_{i_1}(\boldsymbol{\alpha}) \cdots g_{i_T}(\boldsymbol{\alpha}) = p^T \beta$$

avec $\beta \in \mathscr{O}_{\mathbb{K}}$. Donc: $|F(\boldsymbol{\alpha}^p)|_v \leqq p^{-T}$, ce qui établit a fortiori le théorème 3.1 sous l'hypothèse supplémentaire $\alpha_1, \ldots, \alpha_n \in \mathscr{O}_{\mathbb{K}}$.

Dans le cas général, nous allons nous ramener au cas précédent; pour ceci, utilisons la remarque suivante («théorème d'approximation forte»):

Lemme 3.2. *Soit $\mathbb{K}$ un corps de nombres, $\alpha_1, \ldots, \alpha_n$ des éléments de $\mathbb{K}$ et soit v une place finie de $\mathbb{K}$. Il existe alors un élément $\beta \in \mathscr{O}_{\mathbb{K}}$ tel que*

$$\begin{cases} \beta\alpha_1, \ldots, \beta\alpha_n \in \mathcal{O}_{\mathbb{K}} \\ \text{et} \\ |\beta|_v = \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{-1}. \end{cases}$$

Démonstration. Fixons une place archimédienne quelconque v_0, et notons Σ l'ensemble fini:

$$\Sigma = \{v \in \mathcal{M}_{\mathbb{K}},\ v \nmid \infty,\ \text{et } \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\} > 1\} \cup \{v\}.$$

Pour toute place $v \in \Sigma$, notons aussi θ_v^{-1} celui des éléments $\alpha_1, \ldots, \alpha_n$ (vus comme des éléments du complété $\mathbb{K}_v$ de $\mathbb{K}$ en v) de valeur absolue maximale en v (si $v = v$ et si $\max_{1 \leqq i \leqq n} \{|\alpha_i|_v\} < 1$, on posera $\theta_v = 1$). D'après le théorème de [Ca-Fr], chapitre II, §15, page 67, il existe un élément $\beta \in \mathbb{K}$ tel que

$$\begin{cases} |\beta - \theta_v|_v < \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{-1}, & \text{pour tout } v \in \Sigma, \\ |\beta|_v \leqq 1, & \text{si } v \notin \Sigma \cup \{v_0\}. \end{cases}$$

En utilisant l'inégalité ultramétrique, l'on en déduit:

$$\begin{cases} |\beta|_v = \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{-1}, & \text{pour tout } v \in \Sigma, \\ |\beta|_v \leqq 1, & \text{si } v \notin \Sigma \cup \{v_0\}. \end{cases}$$

En particulier, pour toute place finie v de $\mathbb{K}$ on a $|\beta|_v \leqq 1$ (et donc $\beta \in \mathcal{O}_{\mathbb{K}}$); de même, pour tout i, $1 \leqq i \leqq n$, et $|\beta\alpha_i|_v \leqq 1$ (et donc $\beta\alpha_i \in \mathcal{O}_{\mathbb{K}}$). Enfin, on a bien $|\beta|_v = \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{-1}$ (car $v \in \Sigma$). Le lemme 3.2 est donc établi.

Fixons un tel β; le polynôme

$$G(x_0, \ldots, x_n) = x_0^L F\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \in \mathbb{Z}[x_0, \ldots, x_n]$$

est nul à un ordre $\geqq T$ en $(\beta, \beta\alpha_1, \ldots, \beta\alpha_n) \in \mathcal{O}_{\mathbb{K}}^{n+1}$, et donc

$$|G(\beta^p, \beta^p\alpha_1^p, \ldots, \beta^p\alpha_n^p)|_v \leqq p^{-T}$$

par la première partie de la preuve. D'autre part,

$$\begin{aligned} |G(\beta^p, \beta^p\alpha_1^p, \ldots, \beta^p\alpha_n^p)|_v &= |\beta|_v^{pL} |F(\boldsymbol{\alpha}^p)|_v \\ &= |F(\boldsymbol{\alpha}^p)|_v \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{-pL}. \end{aligned}$$

Le théorème 3.1 est donc maintenant établi.

3.2. Une généralisation du lemme de zéros de Philippon. L'objet de ce paragraphe est d'etablir une version «avec multiplications» du lemme de zéros de P. Philippon (voir [Ph1], théorème 2. 1, et [Ph2], théorèmes 1 ou 2).

Soient $\mathbb{K}$ un corps de nombres, et $\boldsymbol{\alpha} \in \mathbb{G}_m^n(\mathbb{K})$; soient de plus $N_1, \ldots, N_n$ des nombres réels $\geqq 1$ et notons $\mathscr{P}_j$ $(j = 1, \ldots, n)$ des ensembles d'entiers tels que $\mathscr{P}_j \subset [1, N_j]$ et $1 \in \mathscr{P}_j$ $(j = 1, \ldots, n)$. Notons aussi, pour $j = 1, \ldots, n$,

$$\Sigma_j = \{\boldsymbol{\alpha}^{p_j \cdots p_n},\ (p_j, \ldots, p_n) \in \mathscr{P}_j \times \cdots \times \mathscr{P}_n\}$$

et $\Sigma_{n+1} = \{\boldsymbol{\alpha}\}$. On a donc $[p]\Sigma_{r+1} \subset \Sigma_r$ pour tout élément p de $\mathscr{P}_r$ et pour tout entier $r = 1, \ldots, n$.

Théorème 3.3. *Soit $F \in \mathbb{Q}[x_1, \ldots, x_n]$ un polynôme non identiquement nul de degré $\leqq L$, s'annulant sur Σ_1. Il existe alors un entier r $(1 \leqq r \leqq n)$ et une sous-variété algébrique V propre et $\mathbb{Q}$-irréductible de $\mathbb{G}_m^n$ rencontrant Σ_{r+1}, telle que*

$$\deg\Big(\bigcup_{p \in \mathscr{P}_r} [p]V\Big) \leqq (N_1 \cdots N_{r-1} L)^{\operatorname{codim}(V)}. \tag{5}$$

De plus, on a $\operatorname{codim}(V) \leqq r$.

Démonstration. Pour alléger, nous notons encore par la même lettre l'homogénéité du polynôme F:

$$x_0^{\deg F} F\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right).$$

Par abus de notation nous noterons encore $\boldsymbol{\alpha}$ le point projectif défini par $(1, \alpha_1, \ldots, \alpha_n)$. On définit une suite d'idéaux homogènes:

$$\mathfrak{I}_1, \ldots, \mathfrak{I}_{n+1} \subset \mathbb{Q}[x_0, x_1, \ldots, x_n],$$

en posant $\mathfrak{I}_1 = (F)$ et, pour $2 \leqq r \leqq n+1$,

$$\mathfrak{I}_r = \big(G(\boldsymbol{x}^p);\ G \in \mathfrak{I}_{r-1},\ p \in \mathscr{P}_{r-1}\big).$$

Soit X_r la variété définie par $\mathfrak{I}_r$. On a alors $[p]X_{r+1} \subset X_r$ pour tout $p \in \mathscr{P}_r$ et pour $r = 1, \ldots, n$. Notons Y_r la réunion des composantes de X_r rencontrant Σ_r. Par hypothèse sur F, on a $\Sigma_r \subset X_r$ et donc $Y_r \neq \emptyset$. De plus,

$$[p]Y_{r+1} \subset Y_r, \quad \forall p \in \mathscr{P}_r, \tag{6}$$

pour $r = 1, 2, \ldots, n$. En effet, si V est une composante isolée de X_{r+1} rencontrant Σ_{r+1}, pour tous $p \in \mathscr{P}_r$, on a $[p]V \subset X_r$ (car $[p]X_{r+1} \subset X_r$) et $[p]V \cap \Sigma_r \neq \emptyset$ (car $[p]\Sigma_{r+1} \subset \Sigma_r$); donc $[p]V$ est contenue dans une composante de X_r rencontrant Σ_r, ce qui montre (6).

La propriété (6) donne en particulier les inclusions $Y_{n+1} \subset Y_n \subset \cdots \subset Y_1$ (rappelons que $1 \in \mathscr{P}_r$): par le principe des tiroirs, il existe alors un indice $r \leqq n$ pour lequel Y_r et Y_{r+1} ont la même dimension, disons d. Si l'on prend pour r le plus grand indice pour lequel cette propriété est vérifiée, on a bien $n - d \leqq r$. Soit donc V une composante irréductible de dimension d de Y_{r+1}. Par la propriété (6),

$$W = \bigcup_{p \in \mathscr{P}_r} [p] V \subset Y_r$$

et donc $\deg(W) \leqq \deg(Y_r)$ (car toutes les variétés $[p]V$ ont dimension $d = \dim(Y_r)$). Par ailleurs, la variété Y_r est incomplètement définie par des polynômes de degré au plus $N_1 \cdots N_{r-1} L$ et donc:

$$\deg(W) \leqq (N_1 \cdots N_{r-1} L)^{\operatorname{codim}(V)}$$

(voir [Ph1], proposition 3.3). Le théorème 3.3 est donc établi.

4. La transcendance

4.1. La construction de la fonction auxiliaire. Soient L, T deux entiers strictement positifs; notre fonction auxiliaire sera un polynôme non nul $F \in \mathbb{Q}[x_1, \ldots, x_n]$ de degré total $\leqq L$, s'annulant en $\boldsymbol{\alpha}$ à un ordre $\geqq T$. Il s'agit donc de résoudre le système linéaire homogène dont la matrice des coefficients est la matrice $\binom{T+n}{n} \times \binom{L+n}{n}$ définie par

$$A = \left(\binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}} \boldsymbol{\alpha}^{\mu - \lambda} \right) \tag{7}$$

où les lignes (respectivement les colonnes) sont indexées par les multi-indices $\boldsymbol{\lambda} \in \mathbb{N}^n$, $|\boldsymbol{\lambda}| \leqq T$ (respectivement $\boldsymbol{\mu} \in \mathbb{N}^n$, $|\boldsymbol{\mu}| \leqq L$), et où $\binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}} = \binom{\mu_1}{\lambda_1} \cdots \binom{\mu_n}{\lambda_n}$.

Notons r le rang sur $\mathbb{Q}$ du système linéaire associé à la matrice (7), i.e.

$$\binom{L+n}{n} - \dim_{\mathbb{Q}} \{ \boldsymbol{x} \in \mathbb{Q}^{\binom{L+n}{n}},\ A\boldsymbol{x} = 0 \},$$

et considérons l'exposant de Dirichlet:

$$\frac{r}{\binom{L+n}{n} - r}$$

du système linéaire. Nous nous proposons de majorer cet exposant à l'aide de l'indice d'obstruction («astuce de Philippon-Waldschmidt», [Ph-Wa], § 6):

Lemme 4.1. *Supposons $2\delta(\boldsymbol{\alpha}) T \leqq L$. Alors, le système considéré admet une solution non triviale et, de plus, l'exposant de Dirichlet du système est majoré par $2^{n+1} \delta(\boldsymbol{\alpha}) T / L$.*

Démonstration. Soit $F_0 \in \mathbb{Q}[x_1, \ldots, x_n]$ un polynôme non nul s'annulant en $\boldsymbol{\alpha}$ de degré minimal $= \delta(\boldsymbol{\alpha})$. Alors, pour tout $G \in \mathbb{Q}[x_1, \ldots, x_n]$ de degré $\leqq L - \delta(\boldsymbol{\alpha}) T$, le polynôme $G.F_0^T$ est une solution de notre système. Donc l'exposant de Dirichlet est majoré par

$$\frac{\binom{L+n}{n}-\binom{L-\delta(\boldsymbol{\alpha})T+n}{n}}{\binom{L-\delta(\boldsymbol{\alpha})T+n}{n}}=\prod_{j=1}^{n}\left(1+\frac{\delta(\boldsymbol{\alpha})T}{L-\delta(\boldsymbol{\alpha})T+j}\right)-1$$

$$\leqq\left(1+\frac{2\delta(\boldsymbol{\alpha})T}{L}\right)^{n}-1$$

$$=\sum_{j=1}^{n}\binom{n}{j}\left(\frac{2\delta(\boldsymbol{\alpha})T}{L}\right)^{j}\leqq\frac{2^{n+1}\delta(\boldsymbol{\alpha})T}{L}.$$

Le lemme 4.1 est donc établi.

On peut maintenant construire la fonction auxiliaire. Si F est un polynôme à coefficients dans $\bar{\mathbb{Q}}$, on définit sa hauteur comme étant la hauteur de Weil du point projectif défini par les coefficients de F. Si ces coefficients sont des entiers premiers entre eux on a donc $h(F)=\log|\text{maximum des coefficients}|$.

Proposition 4.2. *Soit $\boldsymbol{\alpha}\in\mathbb{G}_m^n(\bar{\mathbb{Q}})$ et soient L et T deux entiers $\geqq 1$ vérifiant les inégalités*

$$2\delta(\boldsymbol{\alpha})T\leqq L,\quad et\quad h(\boldsymbol{\alpha})\leqq\frac{T\log(L+1)}{L}.$$

Il existe alors un polynôme non nul $F\in\mathbb{Z}[x_1,\ldots,x_n]$ de degré $\leqq L$, s'annulant en $\boldsymbol{\alpha}$ à un ordre $\geqq T$ tel que

$$h(F)\leqq\frac{4^{n+1}\delta(\boldsymbol{\alpha})T^2\log(L+1)}{L}. \tag{8}$$

Démonstration. Posons $N=\binom{L+n}{n}$. Le lemme 4.1, montre que le $\mathbb{Q}$-espace vectoriel

$$\mathscr{A}=\{\boldsymbol{x}\in\mathbb{Q}^N,\ A\boldsymbol{x}=0\}$$

est de dimension $N-r>0$; de plus, il assure également que

$$\frac{r}{N-r}\leqq\frac{2^{n+1}\delta(\boldsymbol{\alpha})T}{L}. \tag{9}$$

On déduit alors du théorème 8 de [Bo-Va] l'existence d'un polynôme non identiquement nul $F\in\mathbb{Z}[x_1,\ldots,x_n]$ de degré total $\leqq L$ et nul à un ordre $\geqq T$ en $\boldsymbol{\alpha}$, tel que:

$$h(F)\leqq\frac{1}{N-r}\log H(\mathscr{A})$$

où $H(\mathscr{A})$ est la hauteur[2]) (non logarithmique) du sous-espace $\mathscr{A}$, i.e. la hauteur du point de la Grassmannienne qui correspond au sous-espace $\mathscr{A}$ (voir [St-Va], p. 498).

Considérons maintenant la matrice

$$B = \begin{pmatrix} \sigma_1 A \\ \vdots \\ \sigma_D A \end{pmatrix}$$

(où les σ_i sont les différents plongements de $\mathbb{K} = \mathbb{Q}(\boldsymbol{\alpha})$ dans sa clôture galoisienne $\mathbb{F}$), et soit:

$$\mathscr{B} = \{ y \in \mathbb{F}^N,\ By = 0 \}.$$

On a alors $\dim_{\mathbb{F}} \mathscr{B} = \dim_{\mathbb{Q}} \mathscr{A} = N - r$ et $H(\mathscr{A}) = H(\mathscr{B})$ (voir [St-Va], page 506). Soit $\tilde{B}$ une sous-matrice $r \times N$ de B de rang maximal. Par le principe de dualité (voir [St-Va], (2.2)) on a: $H(\mathscr{B}) = H(\tilde{B})$, où la hauteur d'une matrice est la hauteur du sous-espace vectoriel engendré par ses lignes. En majorant $H(\tilde{B})$ par le produit des hauteurs de ses lignes (inégalité d'Hadamard, voir [Bo-Va], équation (2.6)), on obtient

$$\log H(\tilde{B}) \leqq r \log \max_{j,\lambda} H(\boldsymbol{b}^{(j,\lambda)}) \tag{10}$$

où l'on a noté

$$\boldsymbol{b}^{(j,\lambda)} = (\boldsymbol{b}_{\mu}^{(j,\lambda)})_{|\mu| \leqq L} = \left(\binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}} \sigma_j(\boldsymbol{\alpha})^{\mu - \lambda} \right)_{|\mu| \leqq L} \in \mathbb{F}^N$$

les lignes de la matrice B.

Soient $\boldsymbol{\lambda} \in \mathbb{N}^n$ tel que $|\boldsymbol{\lambda}| \leqq T$ et j un entier tel que $1 \leqq j \leqq D$. En utilisant l'inégalité

$$\left(\sum_{|\mu| \leqq L} \binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}}^2 \right)^{\frac{1}{2}} \leqq \sum_{|\mu| \leqq L} \binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}} = \sum_{\mu_1 = 1}^{L} \cdots \sum_{\mu_n = 1}^{L} \binom{\mu_1}{\lambda_1} \cdots \binom{\mu_n}{\lambda_n}$$

$$= \binom{L+1}{\lambda_1 + 1} \cdots \binom{L+1}{\lambda_n + 1} \leqq (L+1)^{T+n},$$

on trouve, pour toute place archimédienne $v \in \mathscr{M}_{\mathbb{F}}$,

$$|\boldsymbol{b}^{(j,\lambda)}|_v = \left(\sum_{|\mu| \leqq L} |\boldsymbol{b}_{\mu}^{(j,\lambda)}|_v^2 \right)^{\frac{1}{2}} \leqq (L+1)^{T+n} \max\{1, |\sigma_j(\alpha_1)|_v, \ldots, |\sigma_j(\alpha_n)|_v\}^L.$$

Pour v ultramétrique, on obtient:

$$|\boldsymbol{b}^{(j,\lambda)}|_v = \max_{|\mu| \leqq L} |\boldsymbol{b}_{\mu}^{(j,\lambda)}|_v \leqq \max\{1, |\sigma_j(\alpha_1)|_v, \ldots, |\sigma_j(\alpha_n)|_v\}^L.$$

[2]) On notera que ces auteurs utilisent la norme L_2 à l'infini pour les hauteurs de sous-espaces (et *uniquement* pour ces derniers, la métrique du sup étant utilisée pour les autres hauteurs). Nous suivons cette normalisation.

Donc, en mettant ces inégalités ensemble:

$$H(\boldsymbol{b}^{(j,\lambda)}) = \prod_{v \in \mathscr{M}_{\mathbb{F}}} |\boldsymbol{b}^{(j,\lambda)}|_v^{[\mathbb{F}_v:\mathbb{Q}_v]/[\mathbb{F}:\mathbb{Q}]} \leqq (L+1)^{T+n} \exp\{Lh(\boldsymbol{\alpha})\}.$$

En reportant cette estimation dans (10) on obtient

$$\log H(\tilde{B}) \leqq r\big((T+n)\log(L+1) + Lh(\boldsymbol{\alpha})\big).$$

On a donc

$$h(F) \leqq \frac{r}{N-r}\big((T+n)\log(L+1) + Lh(\boldsymbol{\alpha})\big).$$

En utilisant la relation (9) et l'hypothèse sur $h(\boldsymbol{\alpha})$, on en déduit la majoration voulue, ce qui établit la proposition 4.2.

4.2. Extrapolation. Passons maintenant à l'extrapolation proprement dite:

Lemme 4.3. *Soient $F \in \mathbb{Z}[x_1, \ldots, x_n]$ un polynôme de degré $\leqq L$, nul en $\boldsymbol{\alpha}$ à un ordre $\geqq T$, et p un nombre premier tel que*

$$h(F) \leqq \frac{1}{4} T \log p \quad \textit{et tel que} \quad h(\boldsymbol{\alpha}) < \frac{T \log p}{4pL}.$$

Alors, F est nul en $\boldsymbol{\alpha}^p$ à un ordre

$$\geqq \frac{T \log p}{2\big(\log p + (n+1)\log(L+1)\big)}.$$

Démonstration. Il n'y a aucune restriction à supposer que les coefficients de F sont premiers entre eux; c'est ce que nous ferons donc; soit maintenant $\boldsymbol{\lambda} \in \mathbb{N}^n$ avec $|\boldsymbol{\lambda}| = T_0 < T$ et notons

$$\partial_\lambda = \frac{1}{\boldsymbol{\lambda}!}\left(\frac{\partial}{\partial x_1}\right)^{\lambda_1} \circ \cdots \circ \left(\frac{\partial}{\partial x_n}\right)^{\lambda_n}.$$

Soit $v \in \mathscr{M}_{\mathbb{F}}$; on déduit de l'inégalité $\sum_{|\boldsymbol{\mu}| \leqq L} \binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}} \leqq (L+1)^{T_0+n}$ (respectivement de l'inégalité ultramétrique):

$$|\partial_\lambda\big(F(\boldsymbol{\alpha}^p)\big)|_v \leqq \begin{cases} \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{pL}, & \text{si } v \nmid p \text{ et } v \nmid \infty; \\ (L+1)^{T_0+n}|F|_v \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{pL}, & \text{si } v \mid \infty \end{cases}$$

(rappelons que $|F|_v$ désigne le maximum des coefficients de F pour la valeur absolue v).

De plus, si $v \mid p$, le théorème 3.1 nous assure que

$$|\partial_\lambda\big(F(\boldsymbol{\alpha}^p)\big)|_v \leqq p^{-(T-T_0)} \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{pL}.$$

Supposons que $\partial_\lambda F(\alpha^p) \neq 0$; on déduit alors de la formule du produit,

$$\prod_{v \in \mathcal{M}_\mathbb{F}} |\partial_\lambda(F(\alpha^p))|_v^{[\mathbb{F}_v:\mathbb{Q}_v]/[\mathbb{F}:\mathbb{Q}]} = 1,$$

que

$$\begin{aligned} 0 &\leqq -(T-T_0)\log p + h(F) + (T_0+n)\log(L+1) + pLh(\alpha) + \log(L+1) \\ &< -(T-T_0)\log p + (T_0+n)\log(L+1) + \frac{T\log p}{2}. \end{aligned}$$

Donc

$$T_0 > \frac{T\log p}{2\big(\log p + (n+1)\log(L+1)\big)}$$

ce qui établit le lemme 4.3.

En utilisant r fois le lemme 4.3, on en déduit:

Lemme 4.4. *Soit $F \in \mathbb{Z}[x_1, \ldots, x_n]$ de degré $\leqq L$, nul à un ordre $\geqq T$ en α. Soient $p_1, \ldots, p_r (r \geqq 1)$ des nombres premiers et supposons*

$$h(F) \leqq \frac{1}{4} T \min_j \log p_j \tag{11}$$

et

$$h(\alpha) < \frac{T \min_j \log p_j}{4Lp_1 \cdots p_r}. \tag{12}$$

Alors, F est nul en $\alpha^{p_1 \cdots p_r}$ à un ordre

$$\geqq 2^{-r} T \prod_{j=1}^{r} \left(1 + \frac{(n+1)\log(L+1)}{\log p_j}\right)^{-1}.$$

Démonstration. Pour $r = 1$ c'est le lemme 4.3. Supposons l'énoncé vrai pour un certain s, avec $1 \leqq s < r$. Donc le polynôme F est nul en $\alpha^{p_1 \cdots p_s}$ à un ordre

$$T^* \geqq 2^{-s} T \prod_{j=1}^{s} \left(1 + \frac{(n+1)\log(L+1)}{\log p_j}\right)^{-1}.$$

L'hypothèse (12) et l'égalité $h(\alpha^{p_1 \cdots p_s}) = p_1 \cdots p_s h(\alpha)$ impliquent

$$h(\alpha^{p_1 \cdots p_s}) < \frac{T \log p_s}{4p_{s+1}L};$$

on déduit alors du lemme 4.3 (avec α remplacé par $\alpha^{p_1 \cdots p_s}$) que F est nul en $\alpha^{p_1 \cdots p_{s+1}}$ à un ordre

$$\geqq \frac{T^*(\log p_{s+1})}{2(\log p_{s+1} + (n+1)\log(L+1))} \geqq 2^{-(s+1)} T \prod_{j=1}^{s+1} \left(1 + \frac{(n+1)\log(L+1)}{\log p_j}\right)^{-1}.$$

Le lemme 4.4 est donc entièrement établi.

5. Conclusion

5.1. Le choix des paramètres. Soit $\alpha \in \mathbb{G}_m(\bar{\mathbb{Q}})$ et ϱ un nombre réel tel que $0 \leqq \varrho < (n+1)!^{n-1}$. Posons

$$L = \left[C_0^{1/2} \delta(\alpha) \left(\frac{\log(3\delta(\alpha))}{\log\log(3\delta(\alpha))} \right)^{n+1} \right], \quad T = \left[C_0^{1/4} \left(\frac{\log(3\delta(\alpha))}{\log\log(3\delta(\alpha))} \right)^{n} \right],$$

et

$$N_j = \left(C_0 \log(3\delta(\alpha))\right)^{(\varrho+1)(n+1)j.j!}, \quad j = 1, \ldots, n.$$

Définissons ensuite n ensembles d'entiers, en posant

$$\mathscr{P}_j = \{1\} \cup \{p \text{ premier}, \log(3\delta(\alpha)) \leqq p \leqq N_j\}, \quad j = 1, \ldots, n.$$

Ci-dessus, C_0 désigne un nombre réel > 0, ne dépendant que de n, «suffisamment grand» (en d'autres termes, les inégalités que nous serons amenés à écrire seront vraies asymptotiquement en C_0). On notera aussi $c_1, c_2, \ldots$ des nombres réels > 0 (effectivement calculables) ne dépendant que de n.

Notons que l'on a $\sum_{k=1}^{j} k.k! = (j+1)! - 1$; on en déduit la relation suivante que nous utiliserons plusieurs fois par la suite

$$N_1 \cdots N_j = \left(C_0 \log(3\delta(\alpha))\right)^{(\varrho+1)(n+1)((j+1)!-1)}, \tag{13}$$

$(j = 1, \ldots, n)$. Notons que l'on a aussi

$$\log(3\delta(\alpha)) \leqq \log(L+1) \leqq c_1 (\log C_0) \log(3\delta(\alpha)), \tag{14}$$

et

$$\log(N_i) \leqq c_2 \log(C_0) \log\log(3\delta(\alpha)). \tag{15}$$

La proposition suivante, résume l'étape de transcendance:

Proposition 5.1. *Supposons*

$$h(\alpha) < \frac{1}{\delta(\alpha)\left(C_0 \log(3\delta(\alpha))\right)^{(\varrho+1)(n+1)((n+1)!-1)+1}}. \tag{16}$$

Il existe alors un polynôme non nul $F \in \mathbb{Z}[x_1, \ldots, x_n]$ de degré $\leqq L$, s'annulant en $\alpha^{p_1 \cdots p_n}$ pour tout $(p_1, \ldots, p_n) \in \mathscr{P}_1 \times \cdots \times \mathscr{P}_n$.

Démonstration. Notons pour simplifier $\delta = \delta(\alpha)$ et

$$\theta = \frac{\log(3\delta(\alpha))}{\log\log(3\delta(\alpha))}.$$

On a alors

$$\frac{2\delta T}{L} \leqq \frac{2\delta \cdot C_0^{1/4}\theta^n}{(C_0^{1/2}/2)\delta\theta^{n+1}} = \frac{4}{C_0^{1/4}\theta} < 1$$

et, grâce à (16),

$$\frac{L}{T\log(L+1)}\,h(\alpha) < \frac{C_0^{1/2}\delta\theta^{n+1}}{(C_0^{1/4}/2)\theta^n\log(L+1)}\,h(\alpha) \leqq \frac{2C_0^{1/4}\delta\theta}{\log(3\delta)}\,h(\alpha) < 1\,.$$

On déduit donc de la proposition 4.2 l'existence d'un polynôme $F \in \mathbb{Z}[x_1, \ldots, x_n]$ de degré $\leqq L$, s'annulant en α à un ordre $\geqq T$ dont la hauteur satisfait l'inégalité (8). Soit $(p_1, \ldots, p_n) \in \mathscr{P}_1 \times \cdots \times \mathscr{P}_n$ et supposons $p_{j_1}, \ldots, p_{j_r}$ premiers et $p_j = 1$ pour $j \notin \{j_1, \ldots, j_r\}$. Un calcul facile permet de vérifier que les hypothèses du lemme 4.4 sont satisfaites. En effet, l'inégalité (11) se déduit de (8):

$$\frac{4h(F)}{T\min_i \log p_{j_i}} \leqq \frac{4^{n+2}\delta T\log(L+1)}{L\log\log(3\delta)} \leqq \frac{4^{n+2}\delta.C_0^{1/4}\theta^n\log(L+1)}{(C_0^{1/2}/2)\delta\theta^{n+1}.\log\log(3\delta)}$$

$$\leqq \frac{2.4^{n+2}c_1(\log C_0)\log(3\delta)}{C_0^{1/4}\theta.\log\log(3\delta)} = \frac{2.4^{n+2}c_1(\log C_0)}{C_0^{1/4}} < 1\,,$$

tandis que l'on déduit de l'hypothèse (16) (en tenant compte de la relation (13)) l'inégalité (12):

$$\frac{4Lp_{j_1}\cdots p_{j_r}}{T\min_i \log p_{j_i}}\,h(\alpha) < \frac{4C_0^{1/2}\delta\theta^{n+1}}{(C_0^{1/4}/2)\theta^n.\log\log(3\delta)}\,N_{j_1}\cdots N_{j_r}h(\alpha)$$

$$\leqq \frac{8C_0^{1/4}\delta\theta}{\log\log(3\delta)}\,N_1\cdots N_n h(\alpha)$$

$$= \frac{8C_0^{1/4}\delta\theta}{\log\log(3\delta)}\cdot\frac{1}{\delta C_0\log(3\delta)} < 1\,.$$

Le lemme 4.4 nous assure maintenant que F est nul en $\alpha^{p_{j_1}\cdots p_{j_r}}$ à un ordre

$$\geqq 2^{-r}T\prod_{j=1}^{r}\left(1+\frac{(n+1)\log(L+1)}{\log p_j}\right)^{-1} \geqq \frac{C_0^{1/4}\theta^n}{2^{r+1}\big(1+c_1(n+1)(\log C_0)\theta\big)^r} \geqq 1\,.$$

La proposition 5.1 est établie.

Afin de pouvoir tirer parti du lemme de zéros (théorème 3.3), nous montrons dans l'énoncé ci-dessous que l'on peut trouver «beaucoup» de premiers dans les ensembles $\mathscr{P}_i$

qui ne sont pas dans l'ensemble $E(W)$ pour toute sous-variété algébrique W de $\mathbb{G}_m^n$ de degré contrôlé.

Lemme 5.2. *Soit W une variété $\mathbb{Q}$-irréductible dont le degré satisfait l'inégalité*

$$\log \deg(W) \leqq \left(C_0 \log\left(3\delta(\boldsymbol{\alpha})\right)\right)^{(\varrho+1)(n+1)-1}. \tag{17}$$

Il existe alors des sous ensembles $\tilde{\mathscr{P}}_j \subset \mathscr{P}_j$ $(j = 1, \ldots, n)$, dont le cardinal satisfait l'inégalité

$$|\tilde{\mathscr{P}}_j| \geqq c_3 \frac{\left(C_0 \log\left(3\delta(\boldsymbol{\alpha})\right)\right)^{(\varrho+1)(n+1)j.j!}}{(\log C_0) \log\log\left(3\delta(\boldsymbol{\alpha})\right)}$$

et tels que $1 \in \tilde{\mathscr{P}}_j$ et $p_1 \cdots p_n \notin E(W)$ pour tout $(p_1, \ldots, p_n) \in \tilde{\mathscr{P}}_1 \times \cdots \times \tilde{\mathscr{P}}_n$.

Démonstration. Notons comme auparavant δ la quantité $\delta(\boldsymbol{\alpha})$ et définissons une suite d'ensembles $E_1, \ldots, E_n$, en posant $E_1 = E(W)$ et

$$E_j = \bigcup_{p_1 \in \mathscr{P}_1} \cdots \bigcup_{p_{j-1} \in \mathscr{P}_{j-1}} E([p_1 \cdots p_{j-1}]\, W), \quad j = 2, \ldots, n.$$

Posons encore $\tilde{\mathscr{P}}_j = \mathscr{P}_j \setminus E_j$. On a donc $p_1 \cdots p_n \notin E(W)$ pour tout $(p_1, \ldots, p_n) \in \tilde{\mathscr{P}}_1 \times \cdots \times \tilde{\mathscr{P}}_n$ (confer la proposition 2.4, point (ii)).

Nous nous proposons maintenant de minorer le cardinal des ensembles $\tilde{\mathscr{P}}_j$. Tout d'abord, en utilisant le théorème des nombres premiers, on a

$$|\mathscr{P}_j| \geqq \frac{c_4 \left(C_0 \log(3\delta)\right)^{(\varrho+1)(n+1)j.j!}}{\log(C_0) \log\log(3\delta)}. \tag{18}$$

D'autre part, par définition de E_j,

$$|E_j \cap \{p \text{ premier}\}| \leqq N_1 \cdots N_{j-1} \max |E([p_1 \cdots p_{j-1}]\, W) \cap \{p \text{ premier}\}|, \tag{19}$$

où le maximum est pris sur l'ensemble $\mathscr{P}_1 \times \cdots \times \mathscr{P}_{j-1}$.

En utilisant le lemme 2.1, point (i) pour chacune des composantes géométriquement irréductible de W, on obtient

$$\max \deg([p_1 \cdots p_{j-1}]\, W) \leqq (N_1 \cdots N_{j-1})^{\dim(W)} \deg(W);$$

donc, grâce à la proposition 2.4, point (i), et à l'inégalité (17),

$$\begin{aligned} \max |E([p_1 \cdots p_{j-1}]\, W) \cap \{p \text{ premier}\}| &\leqq c_5 \left(\log(N_1 \cdots N_{j-1}) + \log\left(\deg(W)\right)\right) \\ &\leqq c_6 \left(C_0 \log(3\delta)\right)^{(\varrho+1)(n+1)-1}. \end{aligned}$$

L'inégalité (19) (jointe à la formule (13)) donne alors

$$|E_j \cap \{p \text{ premier}\}| \leqq c_7 \big(C_0 \log(3\delta)\big)^{(\varrho+1)(n+1)(j!-1)+(\varrho+1)(n+1)-1}$$
$$= c_7 \big(C_0 \log(3\delta)\big)^{(\varrho+1)(n+1)j!-1}.$$

On déduit de l'inégalité (18) et de la relation ci-dessus la minoration cherchée pour le cardinal des ensembles $\tilde{\mathscr{P}}_j$.

Nous montrons maintenant que si le théorème 1.5 est faux, on peut trouver de petits multiples de $\boldsymbol{\alpha}$ dont l'indice d'obstruction est beaucoup plus faible que celui de $\boldsymbol{\alpha}$:

Proposition 5.3. *Supposons que $\alpha_1, \ldots, \alpha_n$ sont multiplicativement indépendants et que l'inégalité*

$$h(\boldsymbol{\alpha}) < \frac{1}{\delta(\boldsymbol{\alpha})\big(C_0 \log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{(\varrho+1)(n+1)((n+1)!-1)+1}} \tag{20}$$

(*c'est la condition* (16)) *est satisfaite. Alors, pour toute variété $\mathbb{Q}$-irréductible W dont le degré satisfait l'inégalité*

$$\log \deg(W) \leqq \big(C_0 \log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{(\varrho+1)(n+1)-1} \tag{21}$$

(*c'est la condition* (17)), *il existe un entier $l \notin E(W)$,*

$$l \leqq \big(C_0 \log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{(\varrho+1)(n+1)((n+1)!-1)},$$

tel que

$$\delta(\boldsymbol{\alpha}^l) < \frac{\delta(\boldsymbol{\alpha})}{C_0\big(C_0 \log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{\varrho(n+1)}}.$$

Démonstration. Notons comme d'habitude $\delta = \delta(\boldsymbol{\alpha})$. Soit F le polynôme de degré $\leqq L$ fourni par la proposition 5.1. Ce polynôme satisfait en particulier les hypothèses du lemme de zéros (théorème 3.3), appliqué aux nouveaux ensembles d'entiers $\tilde{\mathscr{P}}_j$ donnés par le lemme 5.2. Le lemme de zéros nous fournit donc une indice r et une variété V, $\mathbb{Q}$-irréductible, contenant une certaine puissance $\boldsymbol{\alpha}^l$, avec

$$l \notin E(W) \quad \text{et} \quad l \leqq N_{r+1} \cdots N_n \leqq N_1 \cdots N_n < \big(C_0 \log(3\delta)\big)^{(\varrho+1)(n+1)((n+1)!-1)},$$

pour laquelle l'inégalité (5) est satisfaite. Notons que cette inégalité donne en particulier (car $1 \in \tilde{\mathscr{P}}_j$):

$$\log\big(\deg(V)\big) \leqq n \log(LN_1 \cdots N_n) \leqq c_8 (\log C_0) \log(3\delta).$$

Soit $\mathscr{Q} = \tilde{\mathscr{P}}_r \setminus E(V)$; la proposition 2.4, point (i) et l'inégalité ci-dessus assurent que $|E(V)|$ est négligeable devant la minoration de $|\tilde{\mathscr{P}}_j|$ fournie par le lemme 5.2; on a donc

$$|\mathscr{Q}| \geqq c_9 \frac{\big(C_0 \log(3\delta)\big)^{(\varrho+1)(n+1)r.r!}}{\log(C_0) \log\log(3\delta)}. \tag{22}$$

Comme les cordonnées de $\boldsymbol{\alpha}^l$ sont multiplicativement indépendantes, la composante géométriquement irréductible de V passant par $\boldsymbol{\alpha}^l$ ne peut-être un translaté d'un sous-tore de $\mathbb{G}_m^n$ par un point de torsion. On en tire, en tenant compte encore de l'inégalité (5) et de la proposition 2.4, point (iii):

$$|\mathscr{Q}|\deg(V) \leqq \deg\Big(\bigcup_{p\in\mathscr{P}_r}[p]V\Big) \leqq (LN_1\cdots N_{r-1})^{\operatorname{codim}(V)}.$$

En reportant dans cette inégalité l'estimation (22), et en tenant compte de l'inégalité $\operatorname{codim}(V) \leqq r$ (confer théorème 3.3), on obtient la majoration suivante pour le degré de V:

$$\deg(V)^{1/\operatorname{codim}(V)} \leqq LN_1\cdots N_{r-1}.|\mathscr{Q}|^{-1/r}.$$

En tenant compte de l'inégalité (13), on en déduit:

$$\deg(V)^{1/\operatorname{codim}(V)} \leqq LN_1\cdots N_{r-1}.|\mathscr{Q}|^{-1/r}$$

$$\leqq \frac{c_{10}C_0^{1/2}\delta\big(\log(3\delta)\big)^{n+1}\big(C_0\log(3\delta)\big)^{(\varrho+1)(n+1)(r!-1)}\big(\log(C_0)\log\log(3\delta)\big)^{1/r}}{\big(\log\log(3\delta)\big)^{n+1}\big(C_0\log(3\delta)\big)^{(\varrho+1)(n+1)r!}}$$

$$= \frac{c_{10}\big(\log(C_0)\log\log(3\delta)\big)^{1/r}\delta}{C_0^{n+1/2}\big(\log\log(3\delta)\big)^{n+1}\big(C_0\log(3\delta)\big)^{\varrho(n+1)}} \leqq \frac{\delta}{nC_0\big(C_0\log(3\delta)\big)^{\varrho(n+1)}}.$$

En utilisant la proposition 2.5, on a donc

$$\delta(\boldsymbol{\alpha}^l) \leqq n\big(\deg(V)\big)^{1/\operatorname{codim}(V)} \leqq \frac{\delta}{C_0\big(C_0\log(3\delta)\big)^{\varrho(n+1)}}.$$

La proposition 5.3 est donc entièrement établie.

5.2. La descente finale. La dernière étape de la preuve consiste à construire une suite de variétés passant par des puissances convenables de $\boldsymbol{\alpha}$, vérifiant de bonnes conditions d'inclusion et surtout, de degré «proche» de l'indice d'obstruction du point concerné. Pour ceci, on commence par fixer $2n$ paramètres:

$$\varepsilon_i = \frac{1}{C_0\big(C_0\log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{(n+1)((n+1)!^{n-i}-1)}} < 1, \quad i = 1,\ldots,n,$$

et

$$L_i = \big(C_0(\log C_0)^2\log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{(n+1)(n+1)!^{n-i}((n+1)!-1)}, \quad i = 1,\ldots,n.$$

Les relations contenues dans le lemme suivant, que l'on montre par un calcul facile, nous seront utiles dans la suite:

Lemme 5.4. *Pour $i = 1,\ldots,n$, on a*:

(i) $L_1\cdots L_i = \big(C_0(\log C_0)^2\log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{(n+1)((n+1)!^n-(n+1)!^{n-i})}$.

(ii) $L_{i+1}\cdots L_n = \big(C_0(\log C_0)^2\log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{(n+1)((n+1)!^{n-i}-1)}$.

On définit ensuite un ensemble $\mathscr{W}$ de la façon suivante:

Définition 5.5. On note $\mathscr{W}$ l'ensemble des triplets $(k, \boldsymbol{l}, \boldsymbol{V})$, où $k \in [0, n]$ est un entier, $\boldsymbol{l} = (l_1, \ldots, l_k)$ est un k-uplet d'entiers avec $0 \leqq l_i \leqq L_i$, et $\boldsymbol{V} = (V_0, \ldots, V_k)$ est un $(k+1)$-uplet de sous-variétés propres de $\mathbb{G}_m^n$, définies sur $\mathbb{Q}$ et $\mathbb{Q}$-irréductibles, telles que $\boldsymbol{\alpha} \in V_0$ et telles que:

(i) $l_i \notin E(V_{i-1})$ et $[l_i]^{-1} V_i$ contient V_{i-1} pour $i = 1, \ldots, k$.

(ii) Pour $i = 0, \ldots, k$, l'on a

$$\deg(V_i) \leqq \left(L_{i+1} \cdots L_n \delta(\boldsymbol{\alpha}^{l_1 \cdots l_i})\right)^{\operatorname{codim}(V_i)}.$$

(iii) Pour $i = 1, \ldots, k$, l'on a

$$\delta(\boldsymbol{\alpha}^{l_1 \cdots l_i}) \leqq \varepsilon_i \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}}).$$

Cette définition est motivée par les besoins suivants: tout d'abord, le point (iii) permet de récupérer l'information fournie par les étapes précédentes (confer proposition 5.3); la condition (ii) va assurer que les variétés que l'on va construire sont de «petit» degré. Enfin, le point (i) permet d'assurer que ces variétés sont emboitées et surtout ($l_i \notin E(V_{i-1})$) que leurs degrés se comportent bien par multiplication.

L'inégalité $\varepsilon_i < 1$ donne:

Scolie 5.6. *Si* $(k, \boldsymbol{l}, \boldsymbol{V}) \in \mathscr{W}$, *on a*

$$\delta(\boldsymbol{\alpha}^{l_1 \cdots l_i}) \leqq \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}}), \quad i = 1, \ldots, k.$$

Nous aurons besoin d'assurer qu'il existe un élément $(k, \boldsymbol{l}, \boldsymbol{V})$ de $\mathscr{W}$, pour lequel on a $\dim(V_{i-1}) = \dim(V_i)$ pour au moins un indice i, $1 \leqq i \leqq k-1$. Pour ce faire, nous allons définir:

$$\mathscr{W}_0 = \{(k, \boldsymbol{l}, \boldsymbol{V}) \in \mathscr{W},\ \dim(V_0) < \dim(V_1) < \cdots < \dim(V_k)\}.$$

Nous nous proposons de montrer que $\mathscr{W}_0 \neq \mathscr{W}$. Plus précisément, on montrera la proposition suivante:

Proposition 5.7. *Supposons* $\alpha_1, \ldots, \alpha_n$ *multiplicativement indépendants, et*

$$h(\boldsymbol{\alpha}) < \frac{1}{\delta(\boldsymbol{\alpha})\left(C_0 (\log C_0)^2 \log(3\delta)\right)^{(n+1)(n+1)!^n - n}}. \tag{23}$$

Alors, $\mathscr{W}_0 \neq \mathscr{W}$.

Commençons par mettre une relation d'ordre total sur les suites finies de longueur $\leqq n+1$ d'entiers positifs ou nuls et $< n$. Soient $(v) = (v_i)_{0 \leqq i \leqq k}$, et $(v') = (v'_j)_{0 \leqq j \leqq k'}$ deux telles suites.

Définition 5.8. On dira que $(v) \leqq (v')$ si

$$(v_i)_{0 \leqq i \leqq \min\{k,k'\}} < (v'_i)_{0 \leqq i \leqq \min\{k,k'\}}$$

pour l'ordre lexicographique, ou, si $(v_i)_{0 \leqq i \leqq \min\{k,k'\}} = (v'_i)_{0 \leqq i \leqq \min\{k,k'\}}$ et si la longueur k de la suite (v) est $\geqq$ à la longueur k' de la suite (v').

La démonstration de la proposition 5.7 va se faire par induction sur la suite des dimension de certaines variétés, en utilisant la relation d'ordre definie en 5.8. L'étape inductive est résumée par le lemme suivant:

Lemme 5.9. *Soient $k \geqq 0$ un entier, $l_1, \ldots, l_k$ des entiers $\geqq 1$ et $W_0, \ldots, W_k$ des sous-variétés propres*[3]*) de $\mathbb{G}_m^n$, définies sur $\mathbb{Q}$ et $\mathbb{Q}$-irréductibles, telles que $\boldsymbol{\alpha} \in W_0$ et $[l_i]^{-1} W_i \supset W_{i-1}$ pour $i = 1, \ldots, k$. Alors, pour tout entier $l_{k+1} \geqq 1$ il existe un entier k', $0 \leqq k' \leqq k+1$ et une sous-variété propre $Z_{k'}$ de $\mathbb{G}_m^n$, définie sur $\mathbb{Q}$ et $\mathbb{Q}$-irréductible, de degré*

$$\leqq l_{k'+1} \cdots l_{k+1}\, \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}) \deg(W_{k'}),$$

telle que $[l_{k'}]^{-1} Z_{k'} \supset W_{k'-1}$ et $\operatorname{codim}(Z_{k'}) = \operatorname{codim}(W_{k'}) + 1$. De plus, on a

$$(24) \quad \big(\dim(W_0), \ldots, \dim(W_{k'-1}), \dim(Z_{k'})\big) \prec \big(\dim(W_0), \ldots, \dim(W_k)\big).$$

Démonstration. Soit Z_{k+1} une hypersurface contenant $\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}$ de degré minimal $= \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}})$. Nous allons construire une suite de variétés $Z_0, \ldots, Z_k$ telles que:

(i) $Z_i \subset W_i$, pour $i = 0, \ldots, k$.

(ii) $[l_{i+1} \cdots l_{k+1}]^{-1} Z_{k+1} \supset Z_i$, pour $i = 0, \ldots, k$.

(iii) $[l_i]^{-1} Z_i \supset Z_{i-1}$, pour $i = 1, \ldots, k+1$.

(iv) $\deg(Z_i) \leqq l_{i+1} \cdots l_{k+1}\, \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}) \deg(W_i)$, pour $i = 0, \ldots, k+1$.

Commençons par construire Z_0. Si $W_0 \subset [l_1 \cdots l_{k+1}]^{-1} Z_{k+1}$, on pose $Z_0 = W_0$. Sinon, on coupe la variété W_0 par $[l_1 \cdots l_{k+1}]^{-1} Z_{k+1}$, et on choisit pour Z_0 une des composantes $\mathbb{Q}$-irréductible de dimension maximale passant par $\boldsymbol{\alpha}$ de cette variété. On obtient, par Bézout:

$$\deg(Z_0) \leqq l_1 \cdots l_{k+1}\, \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}) \deg(W_0).$$

Pour $i = 0$, les conditions (i) à (iv) sont donc vérifiées. Soit maintenant i un entier, $0 \leqq i \leqq k-1$ et supposons $Z_0, \ldots, Z_i$ construites. Nous allons construire Z_{i+1}. Comme précédemment, si

$$W_{i+1} \subset [l_{i+2} \cdots l_{k+1}]^{-1} Z_{k+1},$$

on pose $Z_{i+1} = W_{i+1}$. Sinon, on choisit pour Z_{i+1} une composante $\mathbb{Q}$-irréductible de dimension maximale de $[l_{i+2} \cdots l_{k+1}]^{-1} Z_{k+1} \cap W_{i+1}$ parmi les composantes qui contien-

[3]) Avec les conventions: $\operatorname{codim}(W_{k+1}) = 0$, $\deg(W_{k+1}) = 1$, $W_{-1} = \{\sigma\boldsymbol{\alpha},\ \sigma \in \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\}$ et $l_0 = 1$.

nent $[l_{i+1}]Z_i$. Il en existe puisque $[l_{i+1}]W_i \subset W_{i+1}$ (par hypothèse), $Z_i \subset W_i$ (par hypothèse de récurrence (i)), et

$$[l_{i+1}\cdots l_{k+1}]^{-1} Z_{k+1} \supset Z_i$$

(par hypothèse de récurrence (ii)). Comme auparavant, on obtient, par Bézout:

$$\deg(Z_{i+1}) \leqq l_{i+2}\cdots l_{k+1}\,\delta(\boldsymbol{\alpha}^{l_1\cdots l_{k+1}})\deg(W_{i+1}).$$

La variété Z_{i+1} vérifie donc la condition (iv); les conditions (i) à (iii) sont elles vérifiées par construction. Les variétés $Z_0, \ldots, Z_k, Z_{k+1}$ sont donc construites, ce qui achève la récurrence.

Il nous reste à choisir k'. La suite des variétés construites va correspondre à l'un des deux diagrammes suivants:

$$\begin{array}{ccccccccc} W_0 & W_1 & \cdots & W_{k'-1} & W_{k'} & \cdots & W_k & & \\ \| & \| & \vdots & \| & \cup\!\!+ & & & & \\ \boxed{Z_0} & \boxed{Z_1} & \cdots & \boxed{Z_{k'-1}} & \boxed{Z_{k'}} & \cdots & Z_k & Z_{k+1}. \end{array}$$

On peut également obtenir:

$$\begin{array}{ccccccc} W_0 & W_1 & \cdots & \cdots & W_k & & \\ \| & \| & \vdots & \vdots & \| & & \\ \boxed{Z_0} & \boxed{Z_1} & \cdots & \cdots & \boxed{Z_k} & \boxed{Z_{k+1}}. \end{array}$$

On définit alors k' comme le plus petit entier i pour lequel $Z_i \subsetneqq W_i$ si un tel entier existe (ce qui correspond au premier diagramme), et $k' = k+1$ si un tel entier n'existe pas (c'est le deuxième diagramme). La variété $Z_{k'}$ satisfait toutes les propriétés requises: en particulier la propriété de décroissance de la suite des dimensions (24) est assurée par le choix de k' (dans le premier diagramme, la nouvelle suite est strictement plus petite pour l'ordre lexicographique et dans le deuxième, les suites tronquées sont égales, mais la nouvelle suite est strictement plus longue). Le lemme 5.9 est donc entièrement établi.

Nous pouvons maintenant démontrer la proposition 5.7. Remarquons tout d'abord que $\mathscr{W}_0 \neq \emptyset$. En effet, soit V_0 une hypersurface de $\mathbb{G}_m^n$, définie sur $\mathbb{Q}$ et $\mathbb{Q}$-irréductible, passant par $\boldsymbol{\alpha}$, telle que $\deg(V_0) = \delta(\boldsymbol{\alpha})$: le triplet $\big(0, \emptyset, (V_0)\big)$ appartient alors à $\mathscr{W}_0$. Grâce à la définition 5.8, on peut mettre une relation d'ordre (partiel) sur $\mathscr{W}_0$ en posant: $(k, \boldsymbol{l}, \boldsymbol{V}) \leqq (k', \boldsymbol{l}', \boldsymbol{V}')$ si et seulement si

$$(\dim V_i)_{0\leqq i\leqq k} \leqq (\dim V_i')_{0\leqq i\leqq k'}.$$

D'autre part, l'ensemble des suites finies d'entiers compris entre 0 et $n-1$, de longueur au plus n, strictement croissantes (au sens usuel) est fini (en fait de cardinal $\leqq 2^n - 1$). On déduit de ces deux faits qu'il existe un élément $(k, \boldsymbol{l}, \boldsymbol{W})$ de $\mathscr{W}_0$ minimal pour $\leqq$; fixons un tel triplet, et remarquons en particulier que $k \leqq n-1$ (sinon, par le principe des tiroirs, il existerait un indice i, $1 \leqq i \leqq k$ pour lequel $\dim(W_{i-1}) = \dim(W_i)$).

On se propose d'utiliser la proposition 5.3 avec

$$\varrho = (n+1)!^{n-1-k} - 1, \quad W = W_k,$$

et $\boldsymbol{\alpha}$ remplacé par $\boldsymbol{\alpha}^{l_1 \cdots l_k}$. On a $h(\boldsymbol{\alpha}^{l_1 \cdots l_k}) = l_1 \cdots l_k h(\boldsymbol{\alpha})$ et $\delta(\boldsymbol{\alpha}^{l_1 \cdots l_k}) \leqq \delta(\boldsymbol{\alpha})$ (confer scolie 5.6). Donc, en utilisant le lemme 5.4, point (i), et l'hypothèse (23)

$$\begin{aligned} h(\boldsymbol{\alpha}^{l_1 \cdots l_k})\, \delta(\boldsymbol{\alpha}^{l_1 \cdots l_k}) &\leqq \frac{L_1 \cdots L_k \delta(\boldsymbol{\alpha})}{\delta(\boldsymbol{\alpha}) \big(C_0 \log(C_0)^2 \log(3\delta)\big)^{(n+1)(n+1)!^n - n}} \\ &\leqq \big(C_0 (\log C_0)^2 \log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{n-(n+1)(n+1)!^{n-k}} \\ &\leqq \big(C_0 \log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{-e}, \end{aligned}$$

avec

$$\begin{aligned} e &= (n+1)(n+1)!^{n-k} - n \\ &\leqq (n+1)(n+1)!^{n-1-k}\big((n+1)! - 1\big) + 1 \\ &= (\varrho+1)(n+1)\big((n+1)! - 1\big) + 1. \end{aligned}$$

La condition (20) est donc satisfaite. L'inégalité (21) est aussi satisfaite, car, en utilisant le point (ii) (avec $i = k$) de la définition 5.5, la scolie 5.6 et le lemme 5.4 point (i),

$$\log \deg(W_k) \leqq n \sum_{i=1}^{n} \log L_i + n \log \delta(\boldsymbol{\alpha}) \leqq (\log C_0)^2 \log\big(3\delta(\boldsymbol{\alpha})\big).$$

Les hypothèses de la proposition 5.3 sont donc satisfaites. On déduit alors de cette dernière qu'il existe un entier $l_{k+l} \notin E(W_k)$, tel que $l_{k+1} \leqq L_{k+1}$ et $\delta(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}) \leqq \varepsilon_{k+1} \delta(\boldsymbol{\alpha}^{l_1 \cdots l_k})$.

Le triplet $(k, \boldsymbol{l}, \boldsymbol{W}) \in \mathscr{W}_0$, et donc satisfait en particulier les hypothèses du lemme 5.9. Appliquons ce dernier avec l'entier l_{k+1} donné par la proposition 5.3: on en déduit l'existence d'un entier k', $0 \leqq k' \leqq k+1 \leqq n$, et d'une certaine variété $Z_{k'}$ ayant les propriétés décrites dans ce lemme.

Montrons que

$$\big(k', (l_1, \ldots, l_{k'}), (W_0, \ldots, W_{k'-1}, Z_{k'})\big) \in \mathscr{W}. \tag{25}$$

Pour ce faire, il suffit de vérifier les conditions de (i) à (iii) de la définition 5.5 avec $i = k'$. La première partie de la condition (i) est assurée par le choix de l_{k+1} si $k' = k+1$ et par l'hypothèse $(k, \boldsymbol{l}, \boldsymbol{W}) \in \mathscr{W}_0$ sinon; la deuxième partie est assurée par construction de Z_{k+1} (et toujours par hypothèse si $k' < k+1$). Un argument similaire s'applique pour la condition (iii). Montrons donc (ii). Les relations sur la codimension et sur le degré de $Z_{k'}$ (lemme 5.9), la majoration du degré de $W_{k'}$ (définition 5.5) et la scolie 5.6, nous assurent que

$$\begin{aligned} \deg(Z_{k'}) &\leqq l_{k'+1} \cdots l_{k+1} \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{k+1}}) \deg(W_{k'}) \\ &\leqq L_{k'+1} \cdots L_n \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{k'}}) \big(L_{k'+1} \cdots L_n \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{k'}})\big)^{\operatorname{codim}(W_{k'})} \\ &= \big(L_{k'+1} \cdots L_n \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{k'}})\big)^{\operatorname{codim}(Z_{k'})}. \end{aligned}$$

On a donc montré (25). D'autre part, la relation (24) du lemme 5.9 et le choix de $(k, \boldsymbol{l}, \boldsymbol{W})$ montrent que

$$\big(k', (l_1, \ldots, l_{k'}), (W_0, \ldots, W_{k'-1}, Z_{k'})\big) \notin \mathscr{W}_0\,,$$

ce qui établit la proposition 5.7.

5.3. Preuve du théorème principal. Soit $\boldsymbol{\alpha} \in \mathbb{G}_m^n(\bar{\mathbb{Q}})$, dont les coordonnées sont multiplicativement indépendantes, mais dont la hauteur vérifie la relation (23). Appliquons alors la proposition 5.7; on est donc assuré de l'existence de deux sous-variétés propres V_{i-1} et V_i de $\mathbb{G}_m^n$, définies sur $\mathbb{Q}$ et $\mathbb{Q}$-irréductibles, qui vérifient en particulier

$$\dim(V_{i-1}) = \dim(V_i), \quad [l_i]^{-1} V_i \supset V_{i-1}\,,$$

pour un certain entier $l_i \notin E(V_{i-1})$. La proposition 2.4, point (iv) nous assure alors que

$$\deg(V_{i-1}) \leqq \deg(V_i)\,.$$

Mais, comme V_{i-1} passe par $\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}}$, on a

$$\delta(\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}}) \leqq n \deg(V_{i-1})^{1/\operatorname{codim}(V_i)}$$

par la proposition 2.5. En appliquant les relations (ii) et (iii) de la définition 5.5, on en tire

$$\begin{aligned}\delta(\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}}) &\leqq n \deg(V_{i-1})^{1/\operatorname{codim}(V_{i-1})} \leqq n\big(\deg(V_i)\big)^{1/\operatorname{codim}(V_i)} \\ &\leqq n L_{i+1} \cdots L_n \delta(\boldsymbol{\alpha}^{l_1 \cdots l_i}) \leqq n\varepsilon_i L_{i+1} \cdots L_n \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}})\,.\end{aligned}$$

Enfin, le lemme 5.4 point (ii) et la définition de ε_i donnent

$$\begin{aligned}\delta(\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}}) &\leqq \frac{n\big(C_0 \log(C_0)^2 \log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{(n+1)((n+1)!^{n-i}-1)}}{C_0\big(C_0 \log\big(3\delta(\boldsymbol{\alpha})\big)\big)^{(n+1)((n+1)!^{n-i}-1)}}\, \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}}) \\ &= \frac{n(\log C_0)^{2(n+1)((n+1)!^{n-i}-1)}}{C_0}\, \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}}) < \delta(\boldsymbol{\alpha}^{l_1 \cdots l_{i-1}})\,.\end{aligned}$$

Cette inégalité est fausse, une contradiction. L'inégalité (23) est donc aussi fausse et le théorème 1.5 est donc entièrement établi.

6. Preuve des corollaires

Commençons par montrer le théorème 1.6. Tout d'abord, il n'y a pas de restriction à supposer que pour tout i, $1 \leqq i \leqq n$, on ait $h(\alpha_i) \leqq 1$; en effet les points dont la hauteur est plus grande augmentent la valeur du membre de gauche (donc les retirer diminue le membre de gauche), et par ailleurs, le degré du corps engendré par le point dont on a retiré quelques coordonnées est toujours plus petit (et $n\kappa(n)$ est croissante) ce qui a pour effet d'augmenter le membre de droite; les inégalités sont donc bien dans le bon sens.

Soient ensuite $A_1, \ldots, A_n$ des entiers strictement positifs et choisissons $\beta_1, \ldots, \beta_n \in \bar{\mathbb{Q}}$ tels que $\beta_i^{A_i} = \alpha_i$ pour $i = 1, \ldots, n$. On a donc

$$h(\boldsymbol{\beta}) \leqq \sum_{i=1}^{n} h(\beta_i) = A_1^{-1} h(\alpha_1) + \cdots + A_n^{-1} h(\alpha_n),$$

et, grâce à la relation (1),

$$\delta(\boldsymbol{\beta}) \leqq n[\mathbb{Q}(\beta_1, \ldots, \beta_n) : \mathbb{Q}]^{1/n} \leqq n(A_1 \cdots A_n D)^{1/n}.$$

Le théorème 1.5 donne donc la minoration

$$\sum_{i=1}^{n} A_i^{-1} h(\alpha_i) \geqq \frac{c(n)}{n(A_1 \cdots A_n D)^{1/n}} \left(\log\left(3n(A_1 \cdots A_n D)^{1/n}\right)\right)^{-\kappa(n)}. \tag{26}$$

Maintenant, on choisit

$$A_i = \left[\frac{2h(\alpha_i)}{\min_j h(\alpha_j)}\right].$$

On a

$$\sum_{i=1}^{n} A_i^{-1} h(\alpha_i) \leqq n \min_j h(\alpha_j),$$

et

$$A_1 \cdots A_n \leqq \left(\frac{2}{\min_j h(\alpha_j)}\right)^n h(\alpha_1) \cdots h(\alpha_n).$$

En reportant ces deux inégalités dans la formule (26), on obtient

$$\left(h(\alpha_1) \cdots h(\alpha_n)\right)^{1/n} \geqq \frac{c(n)}{2n^2 D^{1/n}} \left(\log\left(\frac{6nD^{1/n}}{\min_j h(\alpha_j)}\right)\right)^{-\kappa(n)}.$$

Pour terminer la preuve du théorème 1.6, il suffit de remarquer que la minoration de Dobrowolski ([Do]) implique:

$$\log\left(\frac{6nD^{1/n}}{\min_j h(\alpha_j)}\right) \leqq c'(n) \log(3D).$$

Le théorème 1.6 est donc établi.

Le corollaire 1.7 correspond au cas $n = 1$ du corollaire 1.8. Il suffit donc de démontrer ce dernier. Pour ce faire, on commence par établir le corollaire suivant (qui a un intérêt en lui même). Nous dirons dans la suite qu'un nombre algébrique α est «kummerien» sur un corps de nombres $\mathbb{L}$, s'il existe un entier $l \geqq 1$ tels que $\alpha^l \in \mathbb{L}$.

Corollaire 6.1. *Soit α un élément de $\mathbb{G}_m(\bar{\mathbb{Q}})$, et notons D_G le degré de la clôture galoisienne $\mathbb{F}$ de $\mathbb{Q}(\alpha)/\mathbb{Q}$. Soit aussi $n \leqq D_G$ un entier strictement positif. Alors, si*

$$h(\alpha) < \left(\frac{c(n)}{D_G}\right)^{1/n} \log(3D_G)^{-\kappa(n)} \tag{27}$$

(*où $c(n)$ est la constante qui intervient dans le théorème* 1.6), *il existe une extension galoisienne $\mathbb{L}$ de $\mathbb{Q}$, de degré majoré par 3^{n^2}, telle que α soit kummerien sur $\mathbb{L}$.*

Démonstration. Notons $\alpha_1, \ldots, \alpha_D$ les conjugués de α sous l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ et soient $i_1, \ldots, i_n$ tels que $1 \leqq i_1 < \cdots < i_n \leqq D$. Si les nombres $\alpha_{i_1}, \ldots, \alpha_{i_n}$ sont multiplicativement indépendants, le théorème 1.6 nous assure que

$$h(\alpha)^n = \prod_{j=1}^{n} h(\alpha_{i_j}) \geqq \frac{c(n)}{D_G} \log(3D_G)^{-n\kappa(n)},$$

contrairement à l'hypothèse.

Soit l le cardinal du groupe des racines de l'unité de $\mathbb{F}$ et notons $\beta = \alpha^l$; notons aussi $\beta_1, \ldots, \beta_{D'}$ les conjugués de β sous l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, et soit $\mathbb{L} = \mathbb{Q}(\beta_1, \ldots, \beta_{D'})$. On peut donc supposer que le $\mathbb{Z}$-module

$$\mathcal{M} = \{\beta_1^{a_1} \cdots \beta_{D'}^{a_{D'}},\ (a_1, \ldots, a_{D'}) \in \mathbb{Z}^{D'}\}$$

est libre (par définition de β) de rang $k \leqq n$ (par la première partie de l'argument). L'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur $\mathcal{M}$ induit alors une représentation

$$\varrho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_k(\mathbb{Z}).$$

Le groupe de Galois $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ s'identifie donc via ϱ à un sous-groupe (fini) de $\mathrm{GL}_k(\mathbb{Z})$. Mais, par un théorème de Serre (voir [Se]; on pourra également se reporter à [Ca], exercice 16, page 51), l'application de réduction mod 3 de $\mathrm{GL}_k(\mathbb{Z})$ vers $\mathrm{GL}_k(\mathbb{Z}/(3\mathbb{Z}))$ est injective sur les sous-groupes finis de $\mathrm{GL}_k(\mathbb{Z})$. On en déduit que $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ est de cardinal au plus 3^{k^2}, d'où le corollaire 6.1.

Nous pouvons maintenant démontrer le corollaire 1.8. Tout d'abord, il n'y a pas de restriction à supposer que α est entier (puisque la minoration de Lehmer est triviale dans le cas contraire), et que D est «suffisamment grand» par rapport à m. Posons $n = m+1$; si la relation (27) n'est pas satisfaite, l'on a

$$h(\alpha) \geqq \left(\frac{c(m+1)}{D^m}\right)^{1/(m+1)} \log(3D^m)^{-\kappa(m+1)},$$

ce qui entraîne bien

$$h(\alpha) \geqq \frac{c'(m)}{D}.$$

On peut donc supposer que (27) est satisfaite; le corollaire 6.1 nous fournit alors un corps de nombres $\mathbb{L}$ de degré $\leqq 3^{(m+1)^2}$ tels que α est kummerien sur $\mathbb{L}$. Par le théorème de Nortchott on a $\boldsymbol{h}(\mathbb{L}) \geqq c''(m)$, où l'on a noté $\boldsymbol{h}(\mathbb{L})$ le minimum de $h(\gamma)$, pour γ parcourant l'ensemble des nombres algébriques de $\mathbb{L}^*$ qui ne sont pas racines de l'unité. Pour terminer la preuve du corollaire 1.8, il suffit d'utiliser le lemme suivant:

Lemme 6.2. *Soit $\alpha \neq 0$ un entier algébrique, kummerien sur $\mathbb{L}$, qui n'est pas une racine de l'unité. On a alors*

$$h(\alpha) \geqq \frac{\boldsymbol{h}(\mathbb{L})}{[\mathbb{L}(\alpha) : \mathbb{L}]}.$$

Démonstration. Soit $P(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ le polynôme minimal de α sur $\mathbb{L}$, et notons $\alpha_1, \ldots, \alpha_d$ les conjugués de α sous l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{L})$. Comme α est kummerien sur $\mathbb{L}$, il existe un entier $l \geqq 1$ tel que pour tout i l'on ait $\alpha_i = \zeta_i \alpha$ pour certaines racines l-ième de l'unité ζ_i.

On en tire que $a_0 = \prod_{i=1}^{d} \alpha_i = \zeta \alpha^d$, où ζ est une racine de l'unité. En particulier, $h(a_0) = dh(\alpha)$. Mais, puisque α n'est pas une racine de l'unité, il en est de même de a_0, et donc, $h(a_0) \geqq \boldsymbol{h}(\mathbb{L})$. Le lemme 6.2, et donc le corollaire 1.8, s'en déduit.

Passons maintenant au corollaire 1.10. Soit $\mathbb{K}$ un corps des nombres et notons (suivant D. Bertrand [Be] § 2 (a)), pour tout entier $n \leqq \sigma_{\mathbb{K}} - 1$,

$$\boldsymbol{h}_{\mathbb{K}}[n] = \min\left\{ \prod_{i=1}^{n} h(\alpha_i),\ (\alpha_i)_{1 \leqq i \leqq n} \in \mathbb{U}_{\mathbb{K}},\ \text{multiplicativement indépendants} \right\}.$$

La relation (3.4)′ de [Be], § 2 (c) (c'est une inégalité de comparaison de normes jointe à inégalité de Minkowski), entraîne

$$V_n(\mathbb{K}) \geqq c(n)\, D^{\frac{n}{2}} \boldsymbol{h}_{\mathbb{K}}[n]$$

(on notera que dans [Be], les hauteurs ne sont pas normalisées, d'où le $D^{n/2}$ au numérateur ici, alors qu'il apparait au dénominateur dans loc. cit). Le corollaire 1.10 suit, en appliquant le théorème 1.6 pour minorer $\boldsymbol{h}_{\mathbb{K}}[n]$.

Références

[Be] *D. Bertrand*, Duality on tori and multiplicative dependence relations, J. Austral. Math. Soc. (A) **62** (1997), 198–216.

[Bo-Va] *E. Bombieri* et *J. Vaaler*, On Siegel's lemma, Invent. Math. **73** (1983), 11–32.

[Ca] *J. W. S. Cassels*, Rational quadratic forms, Academic Press, London–New-York 1971.

[Ca-Fr] *J. W. S. Cassels* et *A. Frölich*, Algebraic number theory, Proceedings of an instructional conference organized by the London Mathematical Society, Academic Press, London–New-York 1967.

[Ch] *M. Chardin*, Une majoration de la fonction de Hilbert et ses conséquences pour l'interpolation algébrique, Bull. Soc. Math. France **117** (1988), 305–318; voir aussi: Contributions à l'algèbre commutative effective et à la théorie de l'élimination, Thèse de doctorat, Université de Paris VI, 1990.

[Da-Hi] *S. David* et *M. Hindry*, Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C. M., manuscrit 1997.

[Do] *E. Dobrowolski*, On a question of Lehmer and the number of irreducible factors of a polynomial, Acta Arith. **34** (1979), 391–401.

[Hi] *M. Hindry*, Autour d'une conjecture de S. Lang, Invent. Math. **94** (1988), 575–603.

[La] *M. Laurent*, Sur la mesure de Mahler de certaines classes d'entiers algébriques, manuscrit inédit 1980.

[Le] *H. Lehmer*, Factorisation of some cyclotomic functions, Ann. Math. **34**, nº 2 (1933), 461–479.

[Lou] *R. Louboutin*, Sur la mesure de Mahler d'un nombre algébrique, C. R. Acad. Sci. Paris (A) **296** (1983), 707–708.

[Ma] *E. Matveev*, On the successive minima of the extended logarithmic height on algebraic numbers, manuscrit 1997.

[Mi] *M. Mignotte*, Estimations élémentaires effectives sur les nombres algébriques, Publ. I. R. M. A., Strasbourg 1979.

[Ph1] *P. Philippon*, Lemmes de zéros dans les groupes algébriques commutatifs, Bull. Soc. Math. France **114** (1986), 355–383.

[Ph2] *P. Philippon*, Nouveaux lemmes de zéros dans les groupes algébriques commutatifs, Rocky Mountain Math. J. **26** (3) (1996), 1069–1088.

[Ph3] *P. Philippon*, Sur des hauteurs alternatives I, II et III, Math. Ann. **289** (1991), 255–283; Ann. Inst. Fourier (Grenoble) **44** (4) (1994), 1043–1065; J. Math. Pures Appl. **74** (4) (1995), 345–365.

[Ph-Wa] *P. Philippon* et *M. Waldschmidt*, Formes linéaires de logarithmes dans les groupes algébriques commutatifs, Ill. J. Math. **32** (2) (1988), 281–314.

[Schi] *A. Schinzel*, On the product of the conjugates outside the unit circle of an algebraic number, Acta Arith. **24** (1973), 385–399; Addendum. ibid. **26** (1973), 329–361.

[Se] *J.-P. Serre*, Rigidité du foncteur de Jacobi d'échelon $n \geqq 3$, appendice à l'exposé 17 du séminaire Cartan, 1960–1961.

[Sm] *C.J. Smyth*, On the product of the conjugates oustide the unit circle, Bull. London Math. Soc. **3** (1971), 169–175.

[St-Va] *T. Struppeck* et *J. Vaaler*, Inequalities for heights of algebraic subspaces and the Thue-Siegel principle, Analytic Number Theory, proceedings of a conference in honor to Paul T. Bateman, Progr. Math. **85** (1990), 494–527.

[Vou] *P. Voutier*, An effective lower bound for the height of algebraic numbers, Acta Arith. **74** (1996), 81–95.

[Za-Sa] *O. Zariski* et *P. Samuel*, Commutative algebra Volumes I et II, Grad. texts Math. **28**, **29**, Springer-Verlag, New-York–Heidelberg–Berlin 1958 et 1960.

[Zha] *S. Zhang*, Positive line bundles on arithmetic surfaces, Ann. Math. **136** (1992), 569–587.

Dipartimento di Matematica, Università di Torino, Via Carlo Alberto 10, I-10123 Torino
e-mail: amoroso@dm.unito.it

U. M. R. 7586 (C. N. R. S.)–U. F. R. 921, Problèmes Diophantiens, Département de mathématiques, Université Pierre et Marie Curie, Tour 46–56, 5-ième étage, case 247, 4, Place Jussieu, F-75005 Paris
e-mail: david@math.jussieu.fr

Eingegangen 8. November 1997, in revidierter Fassung 15. März 1999