

Minoration de la hauteur normalisée des hypersurfaces

par

FRANCESCO AMOROSO (Torino) et SINNOU DAVID (Paris)

1. Introduction. Dans un article célèbre, D. H. Lehmer posait la question suivante (voir [Le], §13, page 476) : « The following problem arises immediately. If ε is a positive quantity, to find a polynomial of the form: $f(x) = x^r + a_1x^{r-1} + \dots + a_r$, where the a 's are integers, such that the absolute value of the product of those roots of f which lie outside the unit circle, lies between 1 and $1 + \varepsilon$ (...). Whether or not the problem has a solution for $\varepsilon < 0.176$ we do not know. » ⁽¹⁾

Cette question, toujours ouverte, est la source de nombreuses conjectures : généralisation aux minimums successifs de la hauteur (ou hauteur d'un point dans \mathbb{G}_m^n), hauteur normalisée d'une sous-variété de \mathbb{G}_m^n , ou encore analogues des ces questions sur les variétés abéliennes. Après une brève description de ces questions, nous nous intéresserons plus particulièrement aux hypersurfaces de \mathbb{G}_m^n , pour lesquelles nous donnerons des minoration du type de celles déjà obtenues par Dobrowolski pour les points de \mathbb{G}_m .

1.1. Conjectures. Notons, pour $f(x) \in \mathbb{C}[x]$, $f \neq 0$,

$$\log M(f) = \frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\theta})| d\theta;$$

si $f = 0$, on conviendra que $M(0) = 0$. On appellera $M(f)$ la *mesure de Mahler du polynôme f* .

On déduit aisément de la formule de Jensen la relation

$$M(f) = |a| \prod_{j=1}^{\delta} \max\{|\alpha_j|, 1\},$$

2000 *Mathematics Subject Classification*: 11G10, 11J81, 14G40.

⁽¹⁾ La valeur 0.176 correspond au polynôme $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$ pour lequel le produit en question vaut ≈ 1.17628 .

où l'on a noté $f(x) = a(x - \alpha_1) \cdots (x - \alpha_\delta)$ la factorisation de f . La mesure de Mahler est donc liée à la hauteur de Weil logarithmique et absolue ⁽²⁾ d'un nombre algébrique non nul α par la formule

$$h(\alpha) = \frac{\log M(f)}{\deg(f)},$$

où f est le polynôme minimal de α sur \mathbb{Z} (*i. e.* le polynôme irréductible $\in \mathbb{Z}[x]$ de coefficient directeur ≥ 1 et de contenu 1 qui s'annule en α). Remarquons que $M(f) \geq 1$ pour tout polynôme non nul $f \in \mathbb{Z}[x]$ et que, par un théorème classique de Kronecker, la mesure de Mahler d'un polynôme irréductible $f \in \mathbb{Z}[x]$, $f \neq \pm x$, est égale à 1 si et seulement si f est un polynôme cyclotomique.

La question posée par Lehmer peut donc se traduire par les deux conjectures suivantes, équivalentes entre elles :

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

$$h(\alpha) \geq c/D.$$

CONJECTURE 1.2. *Il existe un nombre réel $c > 0$ tel que pour tout polynôme irréductible $f \in \mathbb{Z}[x]$, $f \neq \pm x$, qui n'est pas un polynôme cyclotomique, on a*

$$\log M(f) \geq c.$$

On notera que Lehmer dans son texte était moins catégorique, et formulait plutôt la question en sens inverse.

On peut chercher à savoir quelle est la bonne généralisation des conjectures 1.1 et 1.2 en dimension supérieure. Pour ceci, introduisons d'abord quelques notations. Dans toute la suite du texte, nous plongerons \mathbb{G}_m^n de façon naturelle dans $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$. 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. Soit W une sous-variété de \mathbb{G}_m^n ; par « degré » de W , noté $\deg(W)$, on entendra le degré de l'adhérence de Zariski de W dans \mathbb{P}^n .

Dans [Am-Da] nous avons énoncé la généralisation suivante de la conjecture 1.1 :

CONJECTURE 1.3. *Pour tout entier $n \geq 1$ il existe une constante $c(n) > 0$ telle que pour tout point $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{G}_m^n(\overline{\mathbb{Q}})$, dont les coordonnées $\alpha_1, \dots, \alpha_n$ sont multiplicativement indépendantes, on ait*

$$h(\alpha) \geq c(n)/\delta(\alpha),$$

⁽²⁾ Avec la métrique du sup aux places archimédiennes.

où $h(\alpha)$ est la hauteur de Weil du point projectif défini par $(1, \alpha_1, \dots, \alpha_n)$ et où $\delta(\alpha)$ est le degré minimal d'une hypersurface de \mathbb{G}_m^n définie sur \mathbb{Q} et passant par α .

Soit maintenant V une sous-variété algébrique propre et réduite de \mathbb{G}_m^n . On peut alors définir sa « hauteur normalisée », notée $\widehat{h}(V)$, avec des méthodes de géométrie d'Arakelov (voir la série [Zh1], [Zh2], [Zh3]), ou à l'aide d'une construction « à la Néron–Tate » (voir [Da-Ph2] ou [Ph2], pour une construction analogue sur les variétés abéliennes).

On peut également généraliser la conjecture 1.3 pour les sous-variétés quelconques de \mathbb{G}_m^n ; on obtient ainsi la conjecture générale suivante :

CONJECTURE 1.4. *Pour tout entier $n \geq 1$ il existe une constante $c(n) > 0$ telle que pour toute sous-variété algébrique V de \mathbb{G}_m^n définie sur \mathbb{Q} et \mathbb{Q} -irréductible qui n'est pas une réunion de translatés de sous-groupes algébriques par des points de torsion, on ait*

$$\widehat{h}(V) \geq c(n) \deg(V)^{(s-\dim(V)-1)/(s-\dim(V))},$$

où s désigne la dimension du plus petit sous-groupe algébrique de \mathbb{G}_m^n contenant V .

On remarquera les liens entre cette conjecture et la conjecture qui ont été précédemment énoncés dans l'article [Da-Ph2] :

CONJECTURE 1.5. *Soit W une sous-variété définie sur un corps de nombres \mathbb{K} et géométriquement irréductible de \mathbb{G}_m^n . Alors, si W n'est pas un translaté d'un sous-groupe algébrique, on a*

$$\widehat{h}(W) \geq c(n) \deg(W)^{(s-\dim(V)-1)/(s-\dim(V))},$$

où s désigne la dimension du plus petit sous-groupe algébrique de \mathbb{G}_m^n contenant W .

Cette dernière conjecture implique en effet, pour les variétés qui ne sont pas réunion de translatés de sous-groupes algébriques par des points de torsion, la conjecture 1.4. D'autre part, elle est plus forte que la conjecture 1.4, car elle ne dépend pas du corps de définition de V . En effet, si W est une sous-variété de \mathbb{G}_m^n définie sur $\overline{\mathbb{Q}}$, on peut considérer le cycle V formé des conjugués de W sous l'action de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. La variété V est ainsi définie sur \mathbb{Q} et \mathbb{Q} -irréductible ; de plus, on a clairement $\widehat{h}(V) = [\mathbb{Q}(W) : \mathbb{Q}] \widehat{h}(W)$, et $\deg(V) = [\mathbb{Q}(W) : \mathbb{Q}] \deg(W)$, rapportée à W , la conjecture 1.4 donne alors

$$\widehat{h}(W) \geq c(n) \frac{\deg(W)^{(s-\dim(V)-1)/(s-\dim(V))}}{[\mathbb{Q}(W) : \mathbb{Q}]^{1/(s-\dim(W))}},$$

ce qui montre bien qu'elle est plus faible que la conjecture 1.5. En contrepartie, la nature arithmétique de la conjecture 1.4 (elle dépend du degré

d'un corps de définition de V) permet d'englober en un seul énoncé le cas de toutes les sous-variétés dont la hauteur normalisée est non nulle : le cas des translatés de sous-groupes algébriques par des points d'ordre infini se ramène en effet essentiellement au problème de Lehmer classique (*i. e.* aux conjectures 1.1 ou 1.2).

Le cas des hypersurfaces est particulièrement intéressant. On montre alors que la notion de hauteur normalisée est liée à la mesure de Mahler de l'une de ses équations. Plus précisément, soit $F \in \mathbb{C}[x_1, \dots, x_n]$; on définit sa mesure de Mahler en posant $M(0) = 0$ et

$$(1) \quad \log M(F) = \frac{1}{(2\pi)^n} \int_0^{2\pi} \dots \int_0^{2\pi} \log |F(e^{i\theta_1}, \dots, e^{i\theta_n})| d\theta_1 \wedge \dots \wedge d\theta_n$$

si $F \neq 0$. Soit maintenant V une hypersurface de \mathbb{G}_m^n définie sur \mathbb{Q} et soit $F = 0$ une de ses équations à coefficients entiers de contenu 1; la « hauteur normalisée » de V pour le plongement projectif que nous avons fixé, $\mathbb{G}_m^n \hookrightarrow \mathbb{P}^n$, n'est alors rien d'autre que le logarithme de la mesure de Mahler du polynôme F (voir [Da-Ph2], proposition 2.1(vii)) :

$$\widehat{h}(V) = \log M(F).$$

La mesure de Mahler des polynômes de plusieurs variables a été étudiée par plusieurs auteurs. En particulier, Boyd, Lawton et Smyth ont montré indépendamment (voir [Boy], [La] et [Sm]) que la mesure de Mahler d'un polynôme irréductible

$$F \in \mathbb{Z}[x_1, \dots, x_n],$$

$F \neq \pm x_j$, est égale à 1 si et seulement si F est un « polynôme cyclotomique généralisé », *i. e.* un polynôme irréductible F appartenant à $\mathbb{Z}[x_1, \dots, x_n]$ pour lequel il existe deux multi-indices $\lambda \in \mathbb{Z}^n$, $\mu \in \mathbb{Z}^n$ et un polynôme cyclotomique $\varphi \in \mathbb{Z}[y]$, tels que

$$F(\mathbf{x}) = \mathbf{x}^\lambda \varphi(\mathbf{x}^\mu)$$

(voir [Do-La-Sc]).

Cette généralisation d'un théorème classique de Kronecker a également été retrouvée dans le contexte de la théorie des hauteurs, car on sait que $\widehat{h}(V) = 0$ si et seulement si V est une réunion de translatés de sous-groupes algébriques par des points de torsion de \mathbb{G}_m^n (voir [Zh1], [Zh2]), ce qui est équivalent à dire que F est un polynôme cyclotomique généralisé. Elle a de plus été reliée aux questions de densité de petits points (voir [Zh3]) et aux problèmes d'équidistributions de petits points (voir [Sz-UI-Zh]).

Dans le cas particulier des hypersurfaces, la conjecture 1.4 se traduit donc par la conjecture « bien connue » suivante qui généralise à la dimension supérieure la conjecture 1.2 :

CONJECTURE 1.6. *Pour tout entier $n \geq 1$ il existe une constante $c(n) > 0$ telle que pour tout polynôme irréductible $F \in \mathbb{Z}[x_1, \dots, x_n]$, $F \neq \pm x_j$, qui n'est pas un polynôme cyclotomique généralisé, on ait*

$$\log M(F) \geq c(n).$$

1.2. Résultats. Dans le cadre des conjectures 1.1 et 1.2, le meilleur résultat connu à ce jour (aux constantes numériques près) est la minoration de Dobrowolski (voir [Do], et [Vo] pour la constante numérique la plus récente, à savoir $c = 1/4$) :

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

si $\alpha \in \overline{\mathbb{Q}}^*$ est un nombre algébrique de degré D et n'est pas une racine de l'unité. On peut bien évidemment reformuler cette inégalité dans un langage polynomial :

$$\log M(f) \geq c \left(\frac{\log(\log(3D))}{\log(3D)} \right)^3$$

pour tout polynôme irréductible $f \in \mathbb{Z}[x]$, $f \neq \pm x$, de degré D , qui n'est pas un polynôme cyclotomique.

Récemment nous avons adapté dans [Am-Da] la méthode de Dobrowolski pour aborder la conjecture 1.3.

Nous donnerons ici un résultat beaucoup plus précis dans la direction de la conjecture 1.6 : l'exposant du logarithme du degré est absolu au lieu de se comporter en n^{n^2} comme dans [Am-Da].

Soit V une sous-variété de \mathbb{G}_m^n ; on notera G_V le stabilisateur de V , *i. e.* l'ensemble

$$G_V = \{ \mathbf{x} \in \mathbb{G}_m^n : \mathbf{x} \cdot V = V \},$$

où

$$\xi \cdot V = \{ \xi \cdot \mathbf{x} = (x_1 \xi_1, \dots, x_n \xi_n) : \mathbf{x} \in V \}.$$

Notre résultat principal est le suivant :

THÉORÈME 1.7. *Soit V une hypersurface \mathbb{Q} -irréductible de \mathbb{G}_m^n de degré D et notons $s = \dim G_V$. Alors, si V n'est pas une réunion de translatés de sous-groupes algébriques par des points de torsion de \mathbb{G}_m^n , on a*

$$\widehat{h}(V) \geq \frac{1}{C(n+1)^{1+4/(n-s)}(n-s)^2} \times \frac{(\log((n+1)\log((n+1)D)))^{2+1/(n-s)}}{(\log((n+1)D))^{1+2/(n-s)}},$$

où $C > 0$ est une constante absolue.

On en déduit :

COROLLAIRE 1.8. *Soit n un entier ≥ 2 et $F \in \mathbb{Z}[x_1, \dots, x_n]$ un polynôme irréductible. Supposons qu'il n'existe pas un polynôme $P \in \mathbb{Z}[y_1, \dots, y_{n-1}]$ et des multi-indices $\lambda_0, \dots, \lambda_{n-1} \in \mathbb{Z}^n$ tels que*

$$F(\mathbf{x}) = \mathbf{x}^{\lambda_0} P(\mathbf{x}^{\lambda_1}, \dots, \mathbf{x}^{\lambda_{n-1}}).$$

On a alors

$$\log M(F) \geq \frac{1}{C(n+1)^{1+4/n} n^2} \cdot \frac{(\log((n+1) \log((n+1)D)))^{2+1/n}}{(\log((n+1)D))^{1+2/n}}.$$

On notera que le théorème 1.7 permet d'obtenir une minoration beaucoup plus forte (dans le cas particulier des hypersurfaces) que celle de [Da-Ph2], théorème 1.2, *i. e.* la minoration

$$\widehat{h}(V) \geq 2^{-41} \deg(V)^{-2} \log(\deg(V) + 1)^{-2}$$

(valable pour toute sous-variété V de \mathbb{G}_m^n , géométriquement irréductible définie sur un corps de nombres et telle que V n'est pas translatée d'un sous-groupe algébrique). Toutefois, elle est plus faible que l'estimation citée ci-dessus, puisqu'elle dépend du corps de définition de V et n'est donc pas de nature géométrique comme on est en droit de s'y attendre.

On trouvera au paragraphe 2 un énoncé de réduction (voir proposition 2.4) permettant de supposer, moyennant une perte modérée sur le degré, que l'hypersurface étudiée a un stabilisateur connexe, et une preuve totalement élémentaire du théorème de densité des petits points (voir proposition 2.7). Au paragraphe 3, on utilisera des techniques inspirées de la théorie de Kummer pour étudier les extensions du type $\mathbb{Q}(V)/\mathbb{Q}([p]V)$, où p est un nombre premier. Cela nous permettra de nous ramener aux cas où le degré de cette extension est « petit » (voir proposition 3.7). Au paragraphe 4, on trouvera essentiellement un lemme à la Thue–Siegel, permettant de construire directement une fonction auxiliaire s'annulant sur V avec multiplicités (voir théorème 4.1); on y trouvera également l'étape classique d'extrapolation. Enfin, le paragraphe 5 est consacré à la preuve du théorème 1.7.

2. Hauteur normalisée des hypersurfaces. Après quelques rappels sur la variation de la hauteur normalisée par isogénie, nous montrons que pour minorer la hauteur d'une hypersurface, on peut se ramener au cas où son stabilisateur est connexe. Dans une deuxième partie, nous montrons qu'il est possible de retrouver un énoncé maintenant classique de densité des petits points dans une hypersurface par simple spécialisation de certaines coordonnées en des racines de l'unité.

Dans tout ce texte, le mot « hypersurface » désignera une sous-variété algébrique (donc réduite) de $\mathbb{G}_m^n \hookrightarrow \mathbb{P}^n$ de codimension 1, irréductible sur son corps de définition.

Soit $F \in \overline{\mathbb{Q}}[x_1, \dots, x_n]$ et soit \mathbb{K} un corps de nombres qui contient les coefficients de F . Soit encore ν une place de \mathbb{K} ; si $\nu \nmid \infty$, on note $M_\nu(F)$ sa norme de Gauss en ν , c'est-à-dire le maximum des valeurs absolues ν -adiques des coefficients de F . Si $\nu \mid \infty$ est associée à un plongement σ de \mathbb{K} dans $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, on pose, comme le fait P. Philippon dans [Ph1], $M_\nu(F) = M(\sigma F)$, où $M(P)$ est la mesure de Mahler du polynôme $P \in \mathbb{C}[x_1, \dots, x_n]$ (se reporter à la relation (1) pour la définition de mesure de Mahler). On définit alors la hauteur normalisée de F comme

$$\widehat{h}(F) = \sum_\nu \frac{[\mathbb{K}_\nu : \mathbb{Q}_\nu]}{[\mathbb{K} : \mathbb{Q}]} \log M_\nu(F),$$

où la somme est faite sur toutes les places de \mathbb{K} . On vérifie que cette définition ne dépend pas du choix du corps \mathbb{K} , et, par la formule du produit, que $\widehat{h}(\lambda F) = \widehat{h}(F)$ pour tout nombre algébrique non nul $\lambda \in \overline{\mathbb{Q}}^*$. Remarquons que, si $F \in \mathbb{Z}[x_1, \dots, x_n]$ est de contenu 1, alors $\widehat{h}(F) = \log M(F)$.

Soit maintenant V une hypersurface de \mathbb{G}_m^n , définie par un polynôme F appartenant à l'anneau $\overline{\mathbb{Q}}[x_1, \dots, x_n]$. On pose

$$\widehat{h}(V) = \widehat{h}(F).$$

2.1. Isogénies. On appellera « transformation monomiale » une isogénie de \mathbb{G}_m^n , i. e. une application φ de \mathbb{G}_m^n dans \mathbb{G}_m^n donnée par

$$\varphi(\mathbf{x}) = (\mathbf{x}^{\lambda_1}, \dots, \mathbf{x}^{\lambda_n}),$$

où les $\lambda_j \in \mathbb{Z}^n$ sont des multi-indices tels que $\det(\lambda_1, \dots, \lambda_n) \neq 0$. Le lemme 2.2 ci-dessous montre les relations entre la hauteur normalisée d'une hypersurface et la hauteur normalisée de son image directe et réciproque par une transformation monomiale. Vérifions tout d'abord le lemme suivant qui montre l'invariance des mesures de Mahler et de Gauss par une telle transformation.

LEMME 2.1. *Pour tout $P \in \mathbb{C}[x_1, \dots, x_n]$ et pour tous multi-indices $\lambda_1, \dots, \lambda_n \in \mathbb{Z}^n$ tels que $\det(\lambda_1, \dots, \lambda_n) \neq 0$, on a*

$$M(P(\mathbf{x}^{\lambda_1}, \dots, \mathbf{x}^{\lambda_n})) = M(P).$$

De même, pour toute place finie d'un corps de nombres \mathbb{K} , et tout polynôme $P \in \mathbb{K}[x_1, \dots, x_n]$,

$$M_\nu(P(\mathbf{x}^{\lambda_1}, \dots, \mathbf{x}^{\lambda_n})) = M_\nu(P).$$

Enfin, pour tout point de torsion $\xi \in \mathbb{G}_m^n$, on a $\widehat{h}(\xi \cdot V) = \widehat{h}(V)$.

Démonstration. La première partie du lemme 2.1 se démontre à l'aide d'un changement de variables; supposons tout d'abord que la matrice $(\lambda_1, \dots, \lambda_n)$ est diagonale. Alors

$$\begin{aligned}
 & \log M(P(x_1^{\lambda_1}, \dots, x_n^{\lambda_n})) \\
 &= \frac{1}{(2\pi)^n} \int_0^{2\pi} \cdots \int_0^{2\pi} \log |F(e^{i\lambda_1\theta_1}, \dots, e^{i\lambda_n\theta_n})| d\theta_1 \wedge \cdots \wedge d\theta_n \\
 &= \frac{1}{(2\pi)^n \lambda_1 \cdots \lambda_n} \int_0^{2\lambda_1\pi} \cdots \int_0^{2\lambda_n\pi} \log |F(e^{iu_1}, \dots, e^{iu_n})| du_1 \wedge \cdots \wedge du_n \\
 &= \log M(P).
 \end{aligned}$$

Si par contre la matrice $A = (\lambda_1, \dots, \lambda_n) \in \text{Gl}_n(\mathbb{Z})$, la propriété est claire puisque A induit une bijection de $(S^1)^n$ dans lui même. Le cas général en découle par la théorie des diviseurs élémentaires.

La deuxième partie du lemme est immédiate puisque les coefficients des deux polynômes sont les mêmes (il n’y a pas de simplifications puisque la matrice $(\lambda_1, \dots, \lambda_n)$ est inversible).

Enfin, l’assertion sur l’invariance de la hauteur découle des deux premières en remarquant que la translation par une racine de l’unité se traduit par une multiplication des variables par des racines de l’unité, ce qui ne change ni la mesure de Mahler ni celle de Gauss d’une forme définissant V (voir [Da-Ph2], proposition 2.1(iii) pour des détails et le cas général). ■

On en déduit :

LEMME 2.2. *Soient V une hypersurface de \mathbb{G}_m^n et φ une transformation monomiale. On a alors*

$$\widehat{h}(\varphi^{-1}(V)) = \widehat{h}(V) \quad \text{et} \quad \widehat{h}(\varphi(V)) \leq \left| \frac{\ker(\varphi)}{\ker(\varphi) \cap G_V} \right| \widehat{h}(V).$$

Démonstration. La première assertion découle de la définition de \widehat{h} et du lemme 2.1. Pour montrer la deuxième, on pose $Y = \varphi(V)$ et on remarque que

$$\varphi^{-1}(Y) = \bigcup_{\xi \in \ker(\varphi)} (\xi \cdot V).$$

Si $\xi \cdot \tilde{\xi}^{-1} \in G_V$ on a $\xi \cdot V = \tilde{\xi} \cdot V$. De plus, \widehat{h} est invariante par translation par des points de torsion (toujours par le lemme 2.1) ; donc

$$\widehat{h}(Y) = \widehat{h}(\varphi^{-1}(Y)) \leq \left| \frac{\ker(\varphi)}{\ker(\varphi) \cap G_V} \right| \widehat{h}(V). \quad \blacksquare$$

Soit maintenant V une hypersurface ; la proposition 2.4 montrera qu’il est possible de supposer que son stabilisateur est connexe, quitte à la remplacer par une autre hypersurface de degré légèrement plus grand. On commence par démontrer le lemme suivant, qui permet de « présenter » la « partie

discrète » d'un sous-groupe de \mathbb{G}_m^n . Si H est un sous-groupe de \mathbb{G}_m^n , on notera π_H la projection ⁽³⁾ $H \rightarrow H/H^0$. On a :

LEMME 2.3. *Soit H un sous-groupe de \mathbb{G}_m^n tel que H/H^0 soit de rang k . Alors, quitte à renuméroter les coordonnées, on peut trouver des éléments $\xi_1, \dots, \xi_k \in H$ tels que $\pi_H(\xi_i)$, $1 \leq i \leq k$, engendrent H/H^0 et tels que $\xi_{l,1} = \dots = \xi_{l,l-1} = 1$ pour $l = 1, \dots, k$. De plus, on peut supposer que $\xi_{l,l}$ est une racine d_l -ième primitive de l'unité, que $\xi_l^{d_l} = (1, \dots, 1)$ et que $d_k \mid \dots \mid d_1$.*

Démonstration. Par la théorie des diviseurs élémentaires, H/H^0 est isomorphe à

$$\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z},$$

avec $d_k \mid \dots \mid d_1$ et $k \leq n$. Soient $\xi'_1, \dots, \xi'_k \in H$ d'ordre ⁽⁴⁾ respectivement d_1, \dots, d_k et tels que les $\pi_H(\xi'_i)$ engendrent H/H^0 . Nous allons construire $\xi_1, \dots, \xi_k \in H$ par récurrence. Commençons par ξ_1 : quitte à renuméroter les coordonnées, on peut supposer que la première coordonnée $\xi'_{1,1}$ est une racine primitive d_1 -ième de l'unité ; on pose donc $\xi_1 = \xi'_{1,1}$. Supposons maintenant que ξ_1, \dots, ξ_l sont construits pour un certain l , $1 \leq l < k$. Choisissons des entiers e_1, \dots, e_l tels que $\xi'_{l+1,j} = \xi_{j,j}^{e_j}$ pour $j = 1, \dots, l$ (cela est possible car d_{l+1} divise d_1, \dots, d_l et donc $(\xi'_{l+1,j})^{d_j} = 1$, et car $\xi_{j,j}$ est une racine d_j -ième primitive de l'unité). Posons dans ces conditions

$$\xi_{l+1} := \xi_1^{-e_1} \dots \xi_l^{-e_l} \xi'_{l+1} = (1, \dots, 1, \xi_{l+1,l+1}, \dots, \xi_{l+1,n}),$$

et ξ_{l+1} est d'ordre d_{l+1} . Quitte à renuméroter les $n - l$ dernières coordonnées de \mathbb{G}_m^n , on peut de plus supposer que $\xi_{l+1,l+1}$ est une racine primitive d_{l+1} -ième de l'unité. Le lemme 2.3 est donc entièrement établi. ■

Nous pouvons maintenant passer à la réduction aux hypersurfaces de stabilisateur connexe :

PROPOSITION 2.4. *Soit V une hypersurface \mathbb{Q} -irréductible de degré D . Il existe alors une hypersurface V_1 de degré $\leq n^2 D$ dont le stabilisateur est connexe et telle que $\widehat{h}(V_1) \leq \widehat{h}(V)$ et $\dim G_{V_1} = \dim G_V$.*

Démonstration. Appliquons le lemme 2.3 à G_V ; soient donc ξ_1, \dots, ξ_k des éléments de G_V vérifiant les propriétés de ce lemme. On peut donc écrire

$$\xi_l = (1, \dots, 1, \omega_l^{\lambda_{l,l}}, \omega_l^{\lambda_{l,l+1}}, \dots, \omega_l^{\lambda_{l,n}}),$$

avec $\lambda_{l,l} = 1$, et ω_l une racine primitive d_l -ième de l'unité, pour $1 \leq l \leq k$, et l'on peut imposer $0 \leq \lambda_{l,j} < d_l$, pour j compris entre l et n .

⁽³⁾ Rappelons que H^0 dénote la composante neutre de H , i. e. son plus grand sous-groupe connexe.

⁽⁴⁾ Un tel choix est possible car H^0 est divisible.

Posons

$$\begin{aligned} x_1 &= t_1, \\ x_2 &= t_1^{\lambda_{1,2}} t_2, \\ x_3 &= t_1^{\lambda_{1,3}} t_2^{\lambda_{2,3}} t_3, \\ &\vdots \\ x_n &= t_1^{\lambda_{1,n}} t_2^{\lambda_{2,n}} t_3^{\lambda_{3,n}} \dots t_k^{\lambda_{k,n}} t_n. \end{aligned}$$

Ce changement de variable définit un isomorphisme φ de \mathbb{G}_m^n dans lui-même. Soit $F(x) = 0$ une équation de V et considérons l'hypersurface $\tilde{V} = \varphi^{-1}(V)$ qui est donc définie par l'équation

$$G(t_1, \dots, t_n) = F(t_1, t_1^{\lambda_{1,2}} t_2, \dots, t_1^{\lambda_{1,n}} \dots t_k^{\lambda_{k,n}} t_n) = 0.$$

Dans ces conditions, on a ⁽⁵⁾

$$(2) \quad \mu_{d_1} \times \dots \times \mu_{d_k} \times \{1\} \times \dots \times \{1\} \subset G_{\tilde{V}} \setminus G_{\tilde{V}}^0.$$

Cette inclusion montre qu'il existe un polynôme $H \in \mathbb{Q}[t_1, \dots, t_n]$ tel que

$$G(t_1, \dots, t_n) = H(t_1^{d_1}, \dots, t_k^{d_k}, t_{k+1}, \dots, t_n).$$

Considérons la transformation monomiale

$$\psi(t_1, \dots, t_n) = (t_1^{d_1}, \dots, t_k^{d_k}, t_{k+1}, \dots, t_n),$$

et soit $V_1 = \psi(\tilde{V})$. Cette hypersurface a donc pour équation H . Nous allons montrer que V_1 vérifie la conclusion de la proposition 2.4. Tout d'abord,

$$G_{V_1} = G_{\psi \circ \varphi^{-1}(V)} = \psi \circ \varphi^{-1}(G_V),$$

et ce dernier est connexe par construction de ψ ; donc G_{V_1} est connexe et $\dim G_{V_1} = \dim G_V$. Calculons ensuite la hauteur normalisée de V_1 . Le lemme 2.2 nous assure que $\hat{h}(\tilde{V}) = \hat{h}(V)$. De plus, le même lemme et la nature du stabilisateur (voir la relation (2)) de \tilde{V} nous assure que $\hat{h}(V_1) \leq \hat{h}(\tilde{V})$.

Passons maintenant à l'étude du degré de V_1 . Tout d'abord, par définition de φ , on a ⁽⁶⁾

$$\deg_{t_l}(G) \leq \sum_{j=l}^n \lambda_{l,j} \deg_{x_j}(F)$$

pour $1 \leq l \leq k$ et $\deg_{x_l}(G) = \deg_{x_l}(F)$ pour $k+1 \leq l \leq n$. Par ailleurs, par construction de H ,

$$\deg_{t_l}(H) = \frac{1}{d_l} \deg_{t_l}(G),$$

⁽⁵⁾ On désigne par μ_n le sous-groupe de \mathbb{G}_m formé des racines n -ièmes de l'unité.

⁽⁶⁾ On conviendra que $\lambda_{l,j} = 0$ si $j < l$.

pour $1 \leq l \leq k$ et $\deg_{t_l}(H) = \deg_{t_l}(G)$ si $k + 1 \leq l \leq n$. Au total, on obtient donc

$$\begin{aligned} \deg(V_1) &\leq \frac{1}{d_1} \deg_{x_1}(F) + \left(1 + \frac{1}{d_2}\right) \deg_{x_2}(F) \\ &\quad + \dots + \left(k - 1 + \frac{1}{d_k}\right) \deg_{x_k}(F) \\ &\quad + (k + 1) \deg_{x_{k+1}}(F) + \dots + (k + 1) \deg_{x_n}(F) \\ &\leq (1 + 2 + \dots + k + (n - k)(k + 1)) \deg(V) \\ &\leq \frac{n(n + 1)}{2} \deg(V) \leq n^2 \deg(V). \end{aligned}$$

La proposition 2.4 est donc entièrement établie. ■

2.2. Résultats de densité. Soient V une sous-variété algébrique propre et réduite de \mathbb{G}_m^n et θ un nombre réel; on désigne par $V(\theta)$ l'ensemble des $\alpha \in V(\overline{\mathbb{Q}})$ de hauteur de Weil $h(\alpha) \leq \theta$. Introduisons maintenant le *minimum essentiel* de V :

$$\widehat{\mu}_{\text{ess}}(V) := \inf\{\theta > 0 : \overline{V(\theta)} = V\}.$$

Rappelons que minimum essentiel et hauteur sont très liés. Plus précisément, on dispose de la relation suivante, montrée dans [Zh2], théorème 5.2, et [Zh3], théorème 1.10, qui est valable pour toute sous-variété algébrique propre, géométriquement irréductible V de \mathbb{G}_m^n :

$$(3) \quad \frac{\widehat{h}(V)}{(\dim(V) + 1) \deg(V)} \leq \widehat{\mu}_{\text{ess}}(V) \leq \frac{\widehat{h}(V)}{\deg(V)},$$

(plus précisément, l'inégalité de gauche est une version faible du théorème de Zhang qui permet en fait d'inclure tous les minimums successifs algébriques). On pourra également se reporter à [Da-Ph1], §3, corollaire 3.2, pour une preuve plus élémentaire de ces inégalités, écrite dans le cadre des variétés abéliennes mais qui s'adapte immédiatement au cas multiplicatif.

Dans ce paragraphe on montrera, avec des méthodes élémentaires (*i. e.* plus élémentaires encore que celle de [Da-Ph1]) un résultat de densité qui implique la majoration du minimum essentiel contenue dans la relation (3).

Commençons par la remarque élémentaire suivante :

LEMME 2.5. *Soit $P \in \mathbb{C}[y]$ de degré $\leq d$ et soit p un nombre premier; alors ⁽⁷⁾*

$$\prod_{\omega \in \mu_p^*} |P(\omega)| \leq p^d M(P)^{p-1}.$$

⁽⁷⁾ On désigne par μ_n^* l'ensemble des racines primitive n -ièmes de l'unité.

Démonstration. Si $P = 0$ l'énoncé est clair (en vertu de la convention choisie pour $M(0)$); soit donc

$$P(y) = a(y - \alpha_1) \cdots (y - \alpha_\delta),$$

avec $a \in \mathbb{C}^*$ et $\delta \leq d$. On a alors

$$\begin{aligned} \prod_{\omega \in \mu_p^*} |P(\omega)| &= |a|^{p-1} \prod_{j=1}^{\delta} |1 + \cdots + \alpha_j^{p-1}| \leq p^\delta |a|^{p-1} \prod_{j=1}^{\delta} \max\{|\alpha_j|, 1\}^{p-1} \\ &= p^\delta M(P)^{p-1}, \end{aligned}$$

ce qui montre le lemme 2.5. ■

Nous allons maintenant montrer le lemme suivant qui nous permettra de ramener, au moins dans certaines situations, le problème de la minoration des hauteurs normalisées des hypersurfaces au problème de la minoration de la hauteur de Weil d'un point dans \mathbb{G}_m^n .

LEMME 2.6. Soient n un entier ≥ 2 et $F(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ un polynôme non nul de degré $\leq d_j$ par rapport à la variable x_j ($j = 1, \dots, n - 1$). Alors, pour tous premiers p_1, \dots, p_{n-1} on a ⁽⁸⁾

$$\begin{aligned} \prod_{j=1}^{n-1} (p_j - 1)^{-1} \sum_{\substack{\omega_j \in \mu_{p_j}^* \\ j=1, \dots, n-1}} \log M(F(\omega_1, \dots, \omega_{n-1}, z)) \\ \leq \log M(F) + \sum_{j=1}^{n-1} \frac{d_j \log p_j}{p_j - 1}, \end{aligned}$$

où $M(F(\omega_1, \dots, \omega_{n-1}, z))$ désigne la mesure de Mahler du polynôme $P(\omega_1, \dots, \omega_{n-1}, z)$ de $\mathbb{C}[z]$.

Démonstration. Supposons tout d'abord que $n = 2$, et soit θ un nombre réel, $\theta \in [0, 1]$. D'après le lemme 2.5

$$\frac{1}{p_1 - 1} \sum_{\omega \in \mu_{p_1}^*} \log |F(\omega, e^{2i\pi\theta})| \leq \log M(F(x_1, e^{2\pi i\theta})) + \frac{d_1 \log p_1}{p_1 - 1}.$$

En intégrant par rapport à θ , on en déduit

$$\begin{aligned} \frac{1}{p_1 - 1} \sum_{\omega \in \mu_{p_1}^*} \log M(F(\omega, z)) &= \frac{1}{2\pi} \int_0^1 \frac{1}{p_1 - 1} \sum_{\omega \in \mu_{p_1}^*} \log |(F(\omega, e^{i\theta}))| d\theta \\ &\leq \frac{1}{2\pi} \int_0^1 \left(\log M(F(x_1, e^{2\pi i\theta})) + \frac{d_1 \log p_1}{p_1 - 1} \right) d\theta \\ &\leq \log M(F) + \frac{d_1 \log p_1}{p_1 - 1}, \end{aligned}$$

⁽⁸⁾ Avec les conventions usuelles : $\log 0 = -\infty$ et $-\infty + c = -\infty$, $-\infty \leq c$ pour $c \in \mathbb{R} \cup \{-\infty\}$.

ce qui montre le lemme pour $n = 2$. Supposons maintenant, par hypothèse de récurrence, que ce dernier est vrai pour un certain $n \geq 2$, et soient $F \in \mathbb{C}[x_1, \dots, x_{n+1}]$ un polynôme, et p_1, \dots, p_n des nombres premiers.

Soit comme précédemment $\theta \in [0, 1]$; on peut donc écrire, par hypothèse de récurrence,

$$\begin{aligned} \prod_{j=1}^{n-1} \frac{1}{p_j - 1} \sum_{\substack{\omega_j \in \mu_{p_j}^* \\ j=1, \dots, n-1}} \log M(F(\omega_1, \dots, \omega_{n-1}, x_n, e^{2i\pi\theta})) \\ \leq \log M(F(x_1, \dots, x_n, e^{2i\pi\theta})) + \sum_{j=1}^{n-1} \frac{d_j \log p_j}{p_j - 1}. \end{aligned}$$

Soit maintenant $\omega = (\omega_1, \dots, \omega_{n-1})$ un élément de $\prod_{j=1}^{n-1} \mu_{p_j}^*$. Le lemme 2.5, appliqué à la fonction $y \mapsto F(\omega_1, \dots, \omega_{n-1}, y, e^{2i\pi\theta})$ avec $p = p_n$, donne pour sa part

$$\begin{aligned} \frac{1}{p_n - 1} \sum_{\omega_n \in \mu_{p_n}^*} \log |F(\omega_1, \dots, \omega_{n-1}, \omega_n, e^{2i\pi\theta})| \\ \leq \log M(F(\omega_1, \dots, \omega_{n-1}, y, e^{2i\pi\theta})) + \frac{d_n \log p_n}{p_n - 1}. \end{aligned}$$

On déduit des deux formules précédentes l'inégalité

$$\begin{aligned} \prod_{j=1}^n (p_j - 1)^{-1} \sum_{\substack{\omega_j \in \mu_{p_j}^* \\ j=1, \dots, n}} \log |F(\omega_1, \dots, \omega_n, e^{2i\pi\theta})| \\ \leq \prod_{j=1}^{n-1} (p_j - 1)^{-1} \sum_{\substack{\omega_j \in \mu_{p_j}^* \\ j=1, \dots, n-1}} \log M(F(\omega_1, \dots, \omega_{n-1}, x_n, e^{2i\pi\theta})) + \frac{d_n \log p_n}{p_n - 1} \\ \leq \log M(F(x_1, \dots, x_n, e^{2i\pi\theta})) + \sum_{j=1}^n \frac{d_j \log p_j}{p_j - 1}. \end{aligned}$$

En intégrant cette inégalité sur $[0, 1]$ par rapport à θ , on obtient la relation voulue, ce qui montre le lemme 2.6. ■

On déduit de ce lemme la proposition principale de ce paragraphe :

PROPOSITION 2.7. *Soit V une hypersurface définie sur un corps de nombres \mathbb{K} et \mathbb{K} -irréductible de \mathbb{G}_m^n et soit ε un nombre réel > 0 . Soit de plus F une équation de V ; quitte à renuméroter les variables, on peut supposer que le degré partiel $d_n = \deg_{x_n}(F)$ est ≥ 1 . On a alors :*

(i) Soit Γ l'ensemble des points $(\omega_1, \dots, \omega_{n-1}, \alpha) \in V$ où les $\omega_1, \dots, \omega_{n-1}$ sont des racines de l'unité et où $\alpha \in \overline{\mathbb{Q}}^*$ est de hauteur

$$h(\alpha) \leq \widehat{h}(V)/d_n + \varepsilon.$$

Le sous-ensemble Γ de $V(\overline{\mathbb{Q}})$ est alors Zariski-dense dans V .

(ii) De même, soit $\widetilde{\Gamma}$ l'ensemble des points $(\omega_1\alpha, \dots, \omega_n\alpha) \in V$ où $\omega_1, \dots, \omega_n$ sont des racines de l'unité et où $\alpha \in \overline{\mathbb{Q}}^*$ est de hauteur

$$h(\alpha) \leq \widehat{h}(V)/\deg(V) + \varepsilon.$$

Le sous-ensemble $\widetilde{\Gamma}$ de $V(\overline{\mathbb{Q}})$ est alors également Zariski-dense dans V .

En particulier

$$\widehat{\mu}_{\text{ess}}(V) \leq \frac{\widehat{h}(V)}{\max_{1 \leq j \leq n} \deg_j(V)} \quad \text{et} \quad \widehat{\mu}_{\text{ess}}(V) \leq \frac{\widehat{h}(V)}{\deg(V)},$$

où l'on note $\deg_j(V) = \deg_{x_j}(F)$.

Démonstration. La proposition est triviale pour $n = 1$; en effet, dans ce cas $V = \{\alpha\}$ où $\alpha \in \overline{\mathbb{Q}}$, et $\widehat{h}(V) = h(\alpha)$, $\deg(V) = \deg_1(V) = 1$, et $V(h(\alpha) + \varepsilon) = \{\alpha\} = V$; nous supposons donc pour la suite de la preuve que $n \geq 2$.

Notons N_0 le maximum des nombres premiers divisant le discriminant de \mathbb{K} . Soit encore N un entier $\geq \max\{N_0, d_1 + 1, \dots, d_{n-1} + 1, 3\}$, tel que de plus,

$$\left(\sum_{j=1}^{n-1} d_j \right) \frac{\log(N+1)}{Nd_n} < \varepsilon.$$

Pour toutes racines p_j -ièmes primitives de l'unité ω_j ($1 \leq j \leq n-1$), avec p_1, \dots, p_{n-1} premiers tels que $N < p_1 < \dots < p_{n-1}$, on a donc

$$[\mathbb{K}(\omega_1, \dots, \omega_{n-1}) : \mathbb{K}] = (p_1 - 1) \cdots (p_{n-1} - 1)$$

(en effet, grâce à l'hypothèse $N \geq N_0$ les discriminants de \mathbb{K} et de $\mathbb{Q}(\omega_1, \dots, \omega_{n-1})$ sont premiers entre eux et donc ces deux corps sont linéairement disjoints). De plus,

$$\deg F(\omega_1, \dots, \omega_{n-1}, z) = d_n$$

(en effet, notons $G(x_1, \dots, x_{n-1})$ le coefficient de $x_n^{d_n}$ dans F ; si $G(\omega_1, \dots, \omega_{n-1}) = 0$, alors G est identiquement nul sur $\mu_{p_1}^* \times \dots \times \mu_{p_n}^*$, contrairement au fait que les degrés partiels de G sont strictement inférieurs à $p_1 - 1$).

Fixons donc p_1, \dots, p_{n-1} et $\omega_1, \dots, \omega_{n-1}$ comme ci-dessus et notons

$$P_\omega(x) := F(\omega_1, \dots, \omega_{n-1}, x).$$

Soit ensuite ν une place de \mathbb{K} et notons ν_1, \dots, ν_r ses extensions à $\mathbb{L} = \mathbb{K}(\omega_1, \dots, \omega_{n-1})$. Si $\nu \mid \infty$, on a, par le lemme 2.6,

$$\begin{aligned} \sum_{j=1}^r \frac{[\mathbb{L}_{\nu_j} : \mathbb{K}_{\nu_j}]}{[\mathbb{L} : \mathbb{K}]} \log M_{\nu_j}(P_\omega) \\ \leq \log M_\nu(F) + \sum_{j=1}^{n-1} \frac{d_j \log p_j}{p_j - 1} \leq \log M_\nu(F) + d_n \varepsilon \end{aligned}$$

(notons que tous les P_ω sont conjugués sous l'action de Galois ; le membre de gauche n'est donc qu'une reformulation de la moyenne intervenant dans le lemme 2.6).

D'autre part, si $\nu \nmid \infty$, l'inégalité ultramétrique assure que

$$\sum_{j=1}^r \frac{[\mathbb{L}_{\nu_j} : \mathbb{K}_{\nu_j}]}{[\mathbb{L} : \mathbb{K}]} \log M_{\nu_j}(P_\omega) \leq \log M_\nu(F).$$

On a donc

$$\min_{P_\omega(\alpha)=0} \{h(\alpha)\} \leq \frac{\widehat{h}(P_\omega)}{d_n} \leq \frac{\widehat{h}(V)}{d_n} + \varepsilon.$$

Considérons la réunion Ω_N des ensembles $\mu_{p_1}^* \times \dots \times \mu_{p_n}^*$ avec p_1, \dots, p_n premiers tels que $N < p_1 < \dots < p_{n-1}$. On remarque alors que

$$\Gamma' := \{(\omega, \alpha) \in V : \omega \in \Omega_N \text{ et } h(\alpha) \leq \min_{P_\omega(\beta)=0} \{h(\beta)\}\}$$

est Zariski-dense dans V (car Ω_N est Zariski-dense dans \mathbb{G}_m^{n-1}) ; le point (i) de la proposition 2.7 est donc démontré.

Pour montrer que (i) entraîne (ii), on considère l'hypersurface \widetilde{V} définie par le polynôme

$$\widetilde{F}(x_1, \dots, x_n) = F(x_1 x_n, \dots, x_{n-1} x_n, x_n),$$

et on remarque que $\deg_{x_n}(\widetilde{V}) = \deg(V)$ (où le degré partiel d'une hypersurface est par exemple défini comme étant celui d'une de ses équations), que $\widehat{h}(\widetilde{V}) = \widehat{h}(V)$ (cf. le lemme 2.1) et enfin que $\varphi^{-1}(\Gamma) = \widetilde{\Gamma}$, où φ est la transformation monômiale induite par le changement de variables ci-dessus. Les dernières assertions sont des conséquences directes des points (i) et (ii). La proposition 2.7 est maintenant entièrement établie. ■

3. Propriétés galoisiennes. L'objet de ce paragraphe est de contrôler la variation du degré d'une sous-variété V de \mathbb{G}_m^n définie sur \mathbb{Q} et \mathbb{Q} -irréductible sous l'action d'une multiplication par un entier p . Si pour une variété géométriquement irréductible, ce type d'énoncé est maintenant classique, le cas général est un peu plus délicat. Il convient en effet de tenir

compte du degré de $\mathbb{Q}(V)$ sur $\mathbb{Q}([p]V)$. Nous utilisons donc un argument de type « kummérien ».

LEMME 3.1. *Soit W une sous-variété propre et géométriquement irréductible de \mathbb{G}_m^n , et soit p un nombre premier ne divisant pas $|G_W/G_W^0|$. On a alors*

$$\deg([p]W) = |p|^{\dim(W) - \dim(G_W)} \deg(W),$$

où l'on a noté

$$[p]W = \{\mathbf{x}^p = (x_1^p, \dots, x_n^p) : \mathbf{x} \in W\}.$$

Démonstration. Voir [Hi], lemme 6. ■

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 supposer que les multiples des composantes géométriquement irréductibles de V sont distincts. Pour ce faire, on utilise le lemme suivant qui est l'analogie pour les sous-variétés de \mathbb{G}_m^n du lemme 2(i) de Dobrowolski.

LEMME 3.2. *Soit V une sous-variété propre de \mathbb{G}_m^n , définie sur \mathbb{Q} et \mathbb{Q} -irréductible; soit ensuite W une de ses composantes géométriquement irréductibles et σ un élément de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ tel que $\sigma(W) \neq W$. Supposons que V ne soit pas une réunion de translatés de sous-groupes algébriques par des points de torsion de \mathbb{G}_m^n . Alors, pour tous les entiers l, l' avec $|l| \neq |l'|$, les sous-variétés $[l](W)$ et $[l'](\sigma(W))$ sont distinctes.*

Démonstration. Voir [Am-Da], lemme 2.3(i). ■

On déduit immédiatement des lemmes 3.1 et 3.2 :

SCOLIE 3.3. *Soit V une sous-variété propre de \mathbb{G}_m^n , définie sur \mathbb{Q} et \mathbb{Q} -irréductible, et soit W une de ses composantes géométriquement irréductible. Soit ensuite Λ un ensemble de premiers ne divisant pas $|G_W/G_W^0|$. Alors, si V n'est pas un sous-groupe algébrique de \mathbb{G}_m^n , on a*

$$\deg\left(\bigcup_{p \in \Lambda} [p]V\right) = \left(\sum_{p \in \Lambda} p^{\dim(V) - \dim(G_W)} [\mathbb{Q}(W) : \mathbb{Q}([p]W)]^{-1}\right) \deg(V).$$

Démonstration. Par les lemmes précédents on a

$$\begin{aligned} \deg\left(\bigcup_{p \in \Lambda} [p]V\right) &= \deg\left(\bigcup_{p \in \Lambda, \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} [p](\sigma(W))\right) \\ &= \sum_{p \in \Lambda} \deg\left(\bigcup_{\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} [p](\sigma(W))\right) \\ &= \sum_{p \in \Lambda} \deg([p]W)[\mathbb{Q}([p]W) : \mathbb{Q}] \end{aligned}$$

$$\begin{aligned}
 &= \deg(W) \sum_{p \in \Lambda} p^{\dim(V) - \dim(G_W)} [\mathbb{Q}([p]W) : \mathbb{Q}] \\
 &= \left(\sum_{p \in \Lambda} p^{\dim(V) - \dim(G_W)} \frac{[\mathbb{Q}([p]W) : \mathbb{Q}]}{[\mathbb{Q}(W) : \mathbb{Q}]} \right) \deg(V). \blacksquare
 \end{aligned}$$

Pour pouvoir utiliser efficacement la scolie 3.3, nous aurons besoin que le degré du corps de définition $\mathbb{Q}(W)$ d'une composante géométriquement irréductible W de V ne baisse pas « trop » si l'on remplace V par $[p]V$ pour p premier. Pour ce faire, on considère l'extension « kummerienne » $\mathbb{Q}(W, \omega_p) \subset \mathbb{Q}([p]W, \omega_p)$ de $\mathbb{Q}(W)$ (où l'on a noté ω_p une racine primitive p -ième de l'unité et $\mathbb{Q}(W, \omega_p) = \mathbb{Q}(W)(\omega_p)$); cette extension est abélienne de degré une puissance de p . Le lemme suivant, qui généralise un lemme de Rausch (voir [Ra], lemme 3), montre que si ce degré vaut 1, alors, quitte à translater W par un élément de

$$\ker([p]) = \{ \mathbf{x} \in \mathbb{G}_m^n : [p]\mathbf{x} = (1, \dots, 1) \},$$

on peut supposer $\mathbb{Q}([p]W) = \mathbb{Q}(W)$. Rappelons que dans son texte Rausch suppose que le nombre algébrique α est de degré $< p$ sur $\mathbb{Q}(\alpha^p)$, ce qui revient à supposer dans notre situation que p ne divise pas $[\mathbb{Q}(W) : \mathbb{Q}([p]W)]$. Avec un argument galoisien, on peut montrer que cette dernière hypothèse est en fait équivalente à la suivante : $\mathbb{Q}(W, \omega_p) = \mathbb{Q}([p]W, \omega_p)$ (de plus, si celle-ci n'est pas satisfaite, alors $[\mathbb{Q}(W) : \mathbb{Q}([p]W)] \mid (p-1)$). Toutefois, dans la suite de ce texte, nous n'utiliserons pas cette remarque.

LEMME 3.4. *Soit V une sous-variété propre de \mathbb{G}_m^n , définie sur \mathbb{Q} et \mathbb{Q} -irréductible, et soit W une de ses composantes géométriquement irréductible. Soit ensuite p un nombre premier tel que*

$$\mathbb{Q}(W, \omega_p) = \mathbb{Q}([p]W, \omega_p).$$

Alors, il existe $\zeta \in \ker([p])$ tel que $\mathbb{Q}(\zeta \cdot W) = \mathbb{Q}([p]W)$.

Démonstration. Remarquons d'abord que, par hypothèse,

$$\mathbb{Q}([p]W) \subset \mathbb{Q}(W) \subset \mathbb{Q}(W, \omega_p) = \mathbb{Q}([p]W, \omega_p).$$

Si $\mathbb{Q}(W) = \mathbb{Q}([p]W)$, le résultat est banal (choisir $\zeta = (1, \dots, 1)$); nous supposons donc que $\mathbb{Q}(W) \neq \mathbb{Q}([p]W)$. Soit σ un générateur du groupe cyclique

$$G = \text{Gal}(\mathbb{Q}([p]W, \omega_p) / \mathbb{Q}([p]W))$$

et notons $\tilde{\sigma}$ une de ses extensions à $\overline{\mathbb{Q}}$ ⁽⁹⁾. On a $[p]\tilde{\sigma}(W) = \tilde{\sigma}([p]W) = [p]W$, et donc il existe $\xi \in \ker([p])$ tel que $\tilde{\sigma}(W) = \xi \cdot W$.

⁽⁹⁾ Remarquons que si Z est une sous-variété géométriquement irréductible de \mathbb{G}_m^n , et si $\tau \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, alors $\tau(Z) = Z$ si et seulement si τ laisse le corps $\mathbb{Q}(Z)$ fixe.

On remarque alors :

FAIT 3.5. Avec les notations ci-dessus, $\sigma(\xi) \neq \xi$.

Démonstration. Si $\xi = (1, \dots, 1)$, alors $\tilde{\sigma}(W) = W$ et donc $\mathbb{Q}(W)$ est stable sous l'action de G ; on en déduit que $\mathbb{Q}(W) = \mathbb{Q}([p]W)$. Par ailleurs, si $\xi \neq (1, \dots, 1)$ et $\sigma(\xi) = \xi$, alors $\mathbb{Q}(\xi) = \mathbb{Q}(\omega_p)$ est stable sous l'action de G ; donc G est réduit à l'identité et $\mathbb{Q}([p]W)$ est égal à $\mathbb{Q}([p]W, \omega_p)$; a fortiori on a encore $\mathbb{Q}(W) = \mathbb{Q}([p]W)$. Dans les deux cas, on obtient donc une contradiction avec l'hypothèse $\mathbb{Q}(W) \neq \mathbb{Q}([p]W)$. ■

Revenons maintenant à la démonstration du lemme 3.4 : par le fait 3.5, $\sigma(\xi) = \xi^\lambda$ avec $\lambda \in \mathbb{Z}$ et $\lambda \not\equiv 1 \pmod{p}$. Soit donc u une solution de la congruence

$$(\lambda - 1)u + 1 \equiv 0 \pmod{p}$$

et notons $\zeta = \xi^u$. On a

$$(4) \quad \tilde{\sigma}(\zeta \cdot W) = \sigma(\zeta) \cdot \tilde{\sigma}(W) = \xi^{\lambda u + 1} \cdot W = \zeta \cdot W,$$

ce qui montre que $\mathbb{Q}(\zeta \cdot W)$ est stable sous l'action de G , et donc $\mathbb{Q}(\zeta \cdot W) \subset \mathbb{Q}([p]W)$. D'autre part, $[p](\zeta \cdot W) = [p]W$, et donc ces deux corps sont égaux. Cela achève de démontrer le lemme 3.4. ■

Soit comme auparavant V une sous-variété propre de \mathbb{G}_m^n , définie sur \mathbb{Q} et \mathbb{Q} -irréductible, et soit W une de ses composantes géométriquement irréductible. Soit Λ un ensemble de premiers ne divisant pas $|G_W/G_W^0|$ et tels que $\mathbb{Q}(W, \omega_p) = \mathbb{Q}([p]W, \omega_p)$ pour tout $p \in \Lambda$.

Soit ensuite $c > 1$. La scolie 3.3 montre alors que *ou bien*

$$\deg \left(\bigcup_{p \in \Lambda} [p]V \right) \geq c^{-1} \left(\sum_{p \in \Lambda} p^{\dim(V) - \dim(G_W)} \right) \deg(V),$$

ou bien il existe un premier $p \in \Lambda$ tel que $[\mathbb{Q}(W) : \mathbb{Q}([p]W)] > c$. Dans ce dernier cas, le lemme 3.4 montre qu'il existe $\zeta \in \ker([p])$ tel que $\mathbb{Q}(\zeta \cdot W) = \mathbb{Q}([p]W)$, et donc que la variété

$$\tilde{V} = \bigcup_{\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} \sigma(\zeta \cdot W)$$

est de degré $< c^{-1} \deg(V)$ et sa hauteur normalisée vérifie $\widehat{h}(\tilde{V})/\deg(\tilde{V}) = \widehat{h}(V)/\deg(V)$.

Le lemme suivant montre que le stabilisateur d'une variété \mathbb{Q} -irréductibles et celui d'une de ses composantes géométriquement irréductibles sont très liés.

LEMME 3.6. $G_W \subset G_V$ et $G_W^0 = G_V^0$.

Démonstration. Par un lemme de Kolchin (voir par exemple [Bor], corollaire 8.3 ⁽¹⁰⁾), tout sous-groupe de \mathbb{G}_m^n est défini sur \mathbb{Q} ; c'est en particulier le cas pour G_W . Soit donc \mathbf{x} un élément de G_W et $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. On a $\mathbf{x} \cdot \sigma(W) = \sigma(\sigma^{-1}(\mathbf{x}) \cdot W) \subset \sigma(W)$. On en déduit bien $G_W \subset G_V$. Pour montrer la deuxième affirmation, il suffit de remarquer que l'image de l'application $f : G_V^0 \times W \rightarrow V$ définie par $f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$ est connexe et contient W . Elle est donc égale à W puisque W est une composante connexe de V et par suite, on a la suite d'inclusions $G_W^0 \subset G_V^0 \subset G_W \subset G_V$. On en déduit bien que $G_V^0 = G_W^0$. Le lemme 3.6 est donc établi. ■

L'autre point à contrôler pour une application de la scolie 3.3 est la liste des premiers divisant la « partie discrète » du stabilisateur de W , sans perdre les propriétés galoisiennes décrites au lemme 3.4. C'est ce que nous faisons dans la proposition ci-dessous :

PROPOSITION 3.7. *Soit V une sous-variété propre de \mathbb{G}_m^n , définie sur \mathbb{Q} et \mathbb{Q} -irréductible, et soit W une de ses composantes géométriquement irréductible. Soit ensuite p un premier tel que $p \nmid |G_V/G_V^0|$; alors p satisfait*

$$(5) \quad p \nmid |G_W/G_W^0| \quad \text{et} \quad \mathbb{Q}(W, \omega_p) = \mathbb{Q}([p]W, \omega_p).$$

Démonstration. Comme G_W/G_W^0 est un sous-groupe de G_V/G_V^0 , si p est un premier ne divisant pas $|G_V/G_V^0|$, p ne divise pas non plus $|G_W/G_W^0|$. Montrons que $\mathbb{Q}(W, \omega_p) = \mathbb{Q}([p]W, \omega_p)$. Supposons qu'il existe un élément

$$\sigma \in \text{Gal}(\mathbb{Q}(W, \omega_p)/\mathbb{Q}([p]W, \omega_p))$$

d'ordre p et notons $\tilde{\sigma}$ une de ses extensions à $\overline{\mathbb{Q}}$. On a

$$[p]\tilde{\sigma}(W) = \tilde{\sigma}([p]W) = [p]W,$$

et donc il existe $\xi \in \ker([p])$ tel que $\tilde{\sigma}(W) = \xi \cdot W$. Soit $\tau \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ et soit $l \in \mathbb{Z}$ tel que $\tau^{-1}(\xi) = \xi^l$. On a alors

$$\xi \cdot \tau(W) = \tau(\xi^l \cdot W) = (\tau \circ \tilde{\sigma}^l)(W)$$

(car $\sigma(\xi) = \xi$); donc $\xi \in G_V$. Par le lemme 3.6, $G_V^0 = G_W^0$ et donc $\xi \notin G_V^0$ (sinon $\sigma = \text{Id}$). On en déduit que $p \mid |G_V/G_V^0|$, ce qui est absurde. Cela complète la preuve de la proposition 3.7. ■

4. Approximation diophantienne. Nous rassemblons dans ce paragraphe les énoncés nécessaires à l'étape de transcendance. On y trouvera en particulier une généralisation d'un lemme classique de Thue–Siegel, qui

⁽¹⁰⁾ On notera que sur les variétés abéliennes, ceci est encore vrai (quitte à faire une extension de degré relatif borné du corps de définition) pour les sous-groupes connexes. Le cas des tores est un peu particulier : l'action du groupe de Galois est diagonale sur les racines de l'unité, ce qui permet de traiter le cas général.

nous permettra de construire des polynômes nuls (avec multiplicité) sur une sous-variété V de $\mathbb{G}_m^n \subset \mathbb{P}^n$ et ayant une hauteur de Weil « proche » de la hauteur normalisée de V . Ce type d'énoncé nécessite usuellement une majoration de la fonction de Hilbert arithmétique, suivi d'un passage à la limite dans un « plongement enroulé » dans le formalisme de [Ph2], III, ou, dans le formalisme de la géométrie d'Arakelov, une majoration de la fonction de Hilbert arithmétique pour des « métriques adéliques ». Notre approche permet d'éviter le recours à de tels outils, et de se contenter de la géométrie des nombres classique, dont le résultat de Bombieri–Vaaler.

4.1. Construction de la fonction auxiliaire. Soit donc V une sous-variété propre de $\mathbb{G}_m^n \subset \mathbb{P}^n$, définie sur \mathbb{Q} et \mathbb{Q} -irréductible, et notons \mathfrak{P} son idéal de définition dans l'anneau $\mathbb{Q}[x_0, \dots, x_n]$. Soient ensuite L et T deux entiers strictement positifs ; on note $\mathfrak{P}^{(T)}$ la T -ième puissance symbolique de \mathfrak{P} (i. e. l'idéal homogène engendré par les polynômes nuls à l'ordre T sur V) et l'on note aussi $N = \binom{L+n}{n}$ la dimension du \mathbb{Q} -espace vectoriel $\mathbb{Q}[x_0, \dots, x_n]_L$ engendré par les polynômes homogènes de degré L . Enfin, si $F \in \overline{\mathbb{Q}}[x_0, \dots, x_n]$, on note $h(F)$ la hauteur de Weil du point projectif défini par les coefficients de F .

THÉOREME 4.1. *Soit $r := H(\mathfrak{P}^{(T)}; L)$ la valeur en L de la fonction de Hilbert géométrique de $\mathfrak{P}^{(T)}$ et supposons $r < N$. Il existe alors une base $\{F_1, \dots, F_{N-r}\}$ du \mathbb{Q} -espace vectoriel $[\mathfrak{P}^{(T)}]_L \cup \{0\}$ telle que*

$$\sum_{j=1}^{N-r} h(F_j) \leq r((T+n) \log(L+1) + L\widehat{\mu}_{\text{ess}}(V)).$$

De plus, on peut supposer que les polynômes F_j sont de contenu 1.

Démonstration. Fixons un nombre réel $\theta > \widehat{\mu}_{\text{ess}}(V)$ et considérons, pour $d \in \mathbb{N}^*$, l'ensemble fini

$$S_d = \{\alpha \in V(\overline{\mathbb{Q}}) : h(\alpha) \leq \theta \text{ et } [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d\},$$

qui est stable sous l'action de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (car V est définie sur \mathbb{Q}). On a $S_i \subset S_j$ pour $1 \leq i \leq j$; de plus, par définition du minimum essentiel, la réunion S des S_d est Zariski-dense dans V .

Considérons maintenant le \mathbb{Q} -espace vectoriel de dimension finie \mathcal{A}_d engendré par les polynômes F appartenant à $\mathbb{Q}[x_0, \dots, x_n]_L$ nuls sur S_d à un ordre $\geq T$. On a

$$\mathcal{A}_1 \supset \dots \supset \mathcal{A}_d \supset \dots \supset [\mathfrak{P}^{(T)}]_L \cup \{0\}$$

et donc il existe $d_0 \in \mathbb{N}$ tel que $\mathcal{A}_d = \mathcal{A}_{d_0}$ pour $d \geq d_0$. Les polynômes de \mathcal{A}_{d_0} (que nous noterons désormais \mathcal{A}) sont alors nuls à un ordre $\geq T$ sur S et donc sur V , car S est Zariski-dense dans V . On en déduit que

$$\mathcal{A} = [\mathfrak{P}^{(T)}]_L \cup \{0\}.$$

Pour terminer la preuve du théorème 4.1, il suffit d'utiliser des arguments désormais classiques; on considère la matrice $|S_{d_0}| \cdot \binom{T+n}{n} \times \binom{L+n}{n}$ définie par

$$(6) \quad A = \left(\binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}} \boldsymbol{\alpha}^{\boldsymbol{\mu}-\boldsymbol{\lambda}} \right)$$

où les lignes (respectivement les colonnes) sont indexées par les couples $(\boldsymbol{\alpha}, \boldsymbol{\lambda})$, où $\boldsymbol{\alpha} \in S_{d_0}$ ⁽¹¹⁾ et $\boldsymbol{\lambda} \in \mathbb{N}^{n+1}$ est un multi-indice tel que $|\boldsymbol{\lambda}| \leq T$ (respectivement par le multi-indice $\boldsymbol{\mu} \in \mathbb{N}^{n+1}$ tel que $|\boldsymbol{\mu}| = L$), et où

$$\binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}} = \prod_{j=0}^n \binom{\mu_j}{\lambda_j}.$$

Si l'on identifie $\mathbb{Q}[x_0, \dots, x_n]_L$ à \mathbb{Q}^N de façon standard, on a donc

$$\mathcal{A} = \{\boldsymbol{x} \in \mathbb{Q}^N : A\boldsymbol{x} = 0\}.$$

Le théorème 8 de [Bo-Va] montre alors qu'il existe une base $\{F_1, \dots, F_{N-r}\}$ de \mathcal{A} telle que

$$\sum_{j=1}^{N-r} h(F_j) \leq r \log H_{L_2}(\mathcal{A}),$$

où $H_{L_2}(\mathcal{A})$ est la hauteur ⁽¹²⁾ (non logarithmique) du sous-espace \mathcal{A} , *i. e.* la hauteur du point de la Grassmannienne qui correspond au sous-espace \mathcal{A} (voir [St-Va], p. 498). Par le principe de dualité (voir [St-Va], (2.2)), la hauteur de \mathcal{A} est égale à la hauteur d'une sous-matrice B de A de rang maximal, *i. e.* à la hauteur du sous-espace engendré par les lignes de B . En majorant $H_{L_2}(B)$ par le produit des hauteurs de ces lignes (inégalité d'Hadamard, voir [Bo-Va], équation (2.6)), et en utilisant l'inégalité (obtenue à partir de la formule du multinôme)

$$\sum_{|\boldsymbol{\mu}| \leq L} \binom{\boldsymbol{\mu}}{\boldsymbol{\lambda}} \leq (L+1)^{T+n},$$

on obtient (voir la preuve de la proposition 4.2 dans [Am-Da] pour les détails)

$$H_{L_2}(\mathcal{A}) \leq (T+n) \log(L+1) + L\theta.$$

Donc, pour tout $\theta > \widehat{\mu}_{\text{ess}}(V)$, il existe une base $\{F_1, \dots, F_{N-r}\}$ (formée

⁽¹¹⁾ L'ordre choisit dans S_{d_0} est sans importance.

⁽¹²⁾ Dans *loc. cit.*, les auteurs normalisent la hauteur des sous-espaces avec la norme L_2 à l'infini; nous faisons donc de même et nous le signalons avec un L_2 en indice; toutes les autres hauteurs restent bien entendu normalisées avec la métrique du sup à l'infini.

de polynômes que l'on peut supposer de contenu 1) du \mathbb{Q} -espace vectoriel $[\mathfrak{P}^{(T)}]_L \cup \{0\}$ telle que

$$\sum_{j=1}^{N-r} h(F_j) \leq r((T+n)\log(L+1) + L\theta).$$

On remarque pour finir que l'ensemble des polynômes de $\mathbb{Q}[x_0, \dots, x_n]_L$ de hauteur bornée et de contenu 1 est fini; on peut donc faire tendre θ vers $\widehat{\mu}_{\text{ess}}(V)$. La preuve du théorème 4.1 est maintenant complète, puisque le supplément est trivial. ■

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

LEMME 4.2. *Soit V une sous-variété propre de $\mathbb{G}_m^n \subset \mathbb{P}^n$, définie sur \mathbb{Q} et \mathbb{Q} -irréductible, et soit F un élément de $\mathbb{Z}[x_1, \dots, x_n]$, de degré $\leq L$, de contenu 1, nul sur V à un ordre $\geq T$. Soit aussi p un nombre premier tel que*

$$-T \log p + h(F) + n \log(L+1) + pL\widehat{\mu}_{\text{ess}}(V) < 0.$$

Alors, F est identiquement nul sur $[p]V$.

Démonstration. Soit h_0 un nombre réel $> \widehat{\mu}_{\text{ess}}(V)$ et tel que

$$-T \log p + h(F) + n \log(L+1) + pLh_0 < 0.$$

Il suffit de montrer que pour tout $\alpha \in V(\overline{\mathbb{Q}})$ de hauteur $\leq h_0$ on a $F(\alpha^p) \neq 0$. Soit donc $\alpha \in V(\overline{\mathbb{Q}})$ de hauteur $\leq h_0$ et supposons que $F(\alpha) = 0$. Soit ν une place de $\mathbb{Q}(\alpha)$; si ν est archimédienne on a

$$|F(\alpha^p)|_\nu \leq (L+1)^n |F|_\nu \max\{1, |\alpha_1|_\nu, \dots, |\alpha_n|_\nu\}^{pL}$$

(rappelons que $|F|_\nu$ désigne le maximum des coefficients de F pour la valeur absolue ν). D'autre part, si $\nu \in \mathcal{M}_{\mathbb{F}}$ est non-archimédienne,

$$|F(\alpha^p)|_\nu \leq \max\{1, |\alpha_1|_\nu, \dots, |\alpha_n|_\nu\}^{pL}.$$

De plus, si $\nu | p$, la généralisation du lemme-clé de Dobrowolski, démontrée dans [Am-Da] (voir *op. cit.*, théorème 3.1), montre que

$$|F(\alpha^p)|_\nu \leq p^{-T} \max\{1, |\alpha_1|_\nu, \dots, |\alpha_n|_\nu\}^{pL}.$$

Si $F(\alpha^p) \neq 0$, on déduit alors de la formule du produit,

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

où encore, en passant au log, en utilisant les trois majorations obtenues ci-dessus et en tenant compte du fait que F est de contenu 1,

$$0 \leq -T \log p + h(F) + n \log(L+1) + pLh(\alpha),$$

ce qui contredit l'hypothèse $F(\alpha^p) \neq 0$. Le lemme 4.2 est donc établi. ■

5. Preuve du théorème principal. Après avoir choisi les paramètres de telle sorte que l'on puisse appliquer les énoncés du paragraphe 4 précédent, nous démontrerons une version faible du théorème principal, c'est-à-dire sous des hypothèses restrictives sur son stabilisateur et son corps de définition. Une application des réductions obtenues aux paragraphes 2 et 3 permettra de conclure dans le cas général.

5.1. Le choix des paramètres. Soit V une hypersurface \mathbb{Q} -irréductible de \mathbb{G}_m^n de degré D et notons $s = \dim G_V$. Posons

$$L = \left[C_0^{1/2} D \left(\frac{(n+1)(n-s) \log((n+1)D)}{\log((n+1) \log((n+1)D))} \right)^2 \right]$$

et

$$T = \left[C_0^{1/4} \frac{(n+1)(n-s) \log((n+1)D)}{\log((n+1) \log((n+1)D))} \right].$$

Posons aussi

$$N = C_0 \left(\frac{(n+1)^4 (\log((n+1)D))^2}{\log((n+1) \log((n+1)D))} \right)^{1/(n-s)}.$$

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, \dots des constantes absolues > 0 (effectivement calculables).

Notons que l'on a les inégalités suivantes que l'on utilisera plusieurs fois dans la suite :

FAIT 5.1. (i) $(n+1)DT \leq L$ et $DT^2/L \leq c_1$;

(ii) $\log(L+1) \leq c_2 \log(C_0) \log((n+1)D)$;

(iii) $c_3 \frac{\log((n+1) \log((n+1)D))}{n-s} \leq \log(N) \leq c_4 \log(C_0) \frac{\log((n+1) \log((n+1)D))}{n-s}$;

(iv) $T \log(N/2) \geq c_5 C_0^{1/4} (n+1) \log((n+1)D)$.

Démonstration. C'est un calcul direct. ■

La proposition suivante montre que le théorème 1.7 est vrai sous des hypothèses « techniques » supplémentaires :

PROPOSITION 5.2. *Il existe une constante absolue $C_1 > 0$ ayant les propriétés suivantes. Soit V une hypersurface \mathbb{Q} -irréductible de \mathbb{G}_m^n de degré D et notons $s = \dim G_V$. Soit ensuite W une des composantes géométriquement irréductible; supposons que le stabilisateur de W soit connexe et que pour tout premier p on ait*

$$[\mathbb{Q}(W) : \mathbb{Q}([p]W)] \leq n^2.$$

Alors, si V n'est pas une réunion de translatés de sous-groupes algébriques par des points de torsion de \mathbb{G}_m^n , on a

$$\widehat{h}(V) \geq \frac{1}{C_1(n+1)^{1+4/(n-s)}(n-s)^2} \cdot \frac{(\log((n+1)\log((n+1)D)))^{2+1/(n-s)}}{(\log((n+1)D))^{1+2/(n-s)}}.$$

Démonstration. Supposons que la conclusion de la proposition soit fautive avec $C_1 = C_0^{3/2}$; en utilisant la relation entre hauteur normalisée et minimum essentiel (cf. la relation (3)), on en déduit que

$$(7) \quad D\widehat{\mu}_{\text{ess}}(V) < c(n)^{-1} \frac{(\log((n+1)\log((n+1)D)))^{2+1/(n-s)}}{(\log((n+1)D))^{1+2/(n-s)}},$$

où l'on a noté

$$c(n) = C_0^{3/2}(n+1)^{1+4/(n-s)}(n-s)^2.$$

Montrons maintenant le lemme suivant qui résume l'étape de la transcendance :

LEMME 5.3. *Il existe un polynôme non nul $F \in \mathbb{Z}[x_1, \dots, x_n]$ de degré $\leq L$ qui s'annule sur $[p]V$ pour tout premier p avec $N/2 \leq p \leq N$.*

Démonstration. Appliquons le théorème 4.1 à V ; ce dernier montre qu'il existe un polynôme non nul $F \in \mathbb{Z}[x_1, \dots, x_n]$, de contenu 1 et de degré $\leq L$, qui est nul sur V à un ordre $\geq T$ et tel que

$$h(F) \leq k(T+n)\log(L+1) + kL\widehat{\mu}_{\text{ess}}(V),$$

où

$$k = \frac{H(\mathfrak{P}^{(T)}; L)}{\binom{L+n}{n} - H(\mathfrak{P}^{(T)}; L)} = \frac{\binom{L+n}{n} - \binom{L-DT+n}{n}}{\binom{L+n}{n} - \binom{L-DT+n}{n}}.$$

Soit p un nombre premier vérifiant $N/2 \leq p \leq N$ et notons

$$\begin{aligned} \varepsilon &:= -T \log p + h(F) + n \log(L+1) + pL\widehat{\mu}_{\text{ess}}(V) \\ &\leq -T \log(N/2) + (k(T+n) + n) \log(L+1) + (N+k)L\widehat{\mu}_{\text{ess}}(V). \end{aligned}$$

Le lemme 4.2 nous assure que le lemme 5.3 est vrai si $\varepsilon < 0$; il suffit donc de vérifier que notre choix de paramètres assure cette condition.

Remarquons d'abord que grâce au théorème des accroissements finis, puis au fait 5.1(i) (majoration de DT), on a

$$k \leq \left(1 + \frac{DT}{L-DT}\right)^n - 1 \leq n \left(1 + \frac{DT}{L-DT}\right)^{n-1} \frac{DT}{L-DT} \leq 3n \frac{DT}{L}.$$

Donc, en tenant compte du fait 5.1(i) (majoration de DT^2/L),

$$k(T+n) + n \leq 3n \frac{DT(T+n)}{L} + n \leq c_6 n,$$

et, en tenant compte du fait 5.1(ii) (pour majorer $\log(L + 1)$),

$$(8) \quad (k(T + n) + n) \log(L + 1) \leq c_7(\log C_0)n \log((n + 1)D).$$

Enfin, grâce à l'hypothèse (7) (et à l'inégalité $k \leq 3$),

$$\begin{aligned} (N + k)\widehat{\mu}_{\text{ess}}(V) &< c_8c(n)^{-1}C_0(n + 1)^{4/(n-s)} \frac{(\log((n + 1) \log((n + 1)D)))^2}{D(\log((n + 1)D))} \\ &= c_8C_0^{-1/2}(n + 1)^{-1}(n - s)^{-2} \frac{(\log((n + 1) \log((n + 1)D)))^2}{D(\log((n + 1)D))}. \end{aligned}$$

Donc, en tenant compte de la valeur de L ,

$$(9) \quad (N + k)L\widehat{\mu}_{\text{ess}}(V) \leq c_8(n + 1) \log((n + 1)D).$$

En utilisant les inégalités (8), (9), et en tenant compte du fait 5.1(iv) (pour minorer $T \log(N/2)$), on obtient

$$\varepsilon \leq (-c_5C_0^{1/4} + c_7 \log C_0 + c_8)(n + 1) \log((n + 1)D).$$

Pour C_0 assez grand, on peut assurer $c_5C_0^{1/4} \geq 2c_7 \log C_0 + 2c_8$, c'est-à-dire $\varepsilon < 0$, ce qui montre le lemme 5.3. ■

Revenons maintenant à la preuve de la proposition 5.2. Le lemme 5.3 nous assure, par comparaison des degrés, que

$$(10) \quad \deg \left(\bigcup_{N/2 \leq p \leq N} [p]V \right) \leq L.$$

D'autre part, on a supposé que le stabilisateur des composantes géométriquement irréductibles W de V est connexe et que pour tout premier p on a $[\mathbb{Q}(W) : \mathbb{Q}([p]W)] \leq n^2$; donc, par la scolie 3.3, par le théorème de Tchebychev, et en tenant compte du fait 5.1(iii) (pour majorer $\log N$), on a

$$\begin{aligned} \deg \left(\bigcup_{N/2 \leq p \leq N} [p]V \right) &\geq \frac{1}{n^2} \left(\sum_{N/2 \leq p \leq N} p^{n-1-s} \right) D \geq \frac{D}{n^2} \cdot \frac{c_9 N^{n-s}}{\log N} \\ &\geq \frac{(n - s)c_{10}C_0^{n-s}}{\log C_0} \cdot D \left(\frac{(n + 1) \log((n + 1)D)}{\log((n + 1) \log((n + 1)D))} \right)^2 \\ &> L \end{aligned}$$

pour C_0 assez grand, puisque l'on a toujours $s \leq n - 1$. Ceci contredit l'inégalité (10). La proposition 5.2 est donc établie. ■

5.2. Preuve du théorème principal. On suppose que le théorème 1.7 est faux pour $C = C_0^2$; soit donc V une hypersurface \mathbb{Q} -irréductible de \mathbb{G}_m^n de

degré minimal D qui contredit la conclusion de ce théorème, *i. e.* telle que

$$(11) \quad \widehat{h}(V) < \frac{1}{C_0^2(n+1)^{1+4/(n-s)}(n-s)^2} \times \frac{(\log((n+1)\log((n+1)D)))^{2+1/(n-s)}}{(\log((n+1)D))^{1+2/(n-s)}},$$

où l'on a noté s la dimension de G_V . La proposition 2.4 montre qu'il existe une hypersurface \mathbb{Q} -irréductible V_1 de \mathbb{G}_m^n de degré $\leq n^2D$ dont le stabilisateur est connexe et telle que $\widehat{h}(V_1) \leq \widehat{h}(V)$ et $\dim G_{V_1} = \dim G_V$. Soit W une composante géométriquement irréductible de cette dernière; on déduit alors de la proposition 3.7 que G_W est connexe et que

$$\mathbb{Q}(W, \omega_p) = \mathbb{Q}([p]W, \omega_p)$$

pour tout premier p . Nous distinguons maintenant deux cas :

(a) PREMIER CAS : $[\mathbb{Q}(W) : \mathbb{Q}([p]W)] \leq n^2$ pour tout premier p . La proposition 5.2 (dans laquelle on peut prendre $C_1 = C_0^{3/2}$, comme on l'a vu au paragraphe 5.1) montre alors que

$$\widehat{h}(V_1) \geq \frac{(\log((n+1)\log(n^2(n+1)D)))^{2+1/(n-s)}}{C_0^{3/2}(n+1)^{1+4/(n-s)}(n-s)^2(\log(n^2(n+1)D))^{1+2/(n-s)}}.$$

Donc

$$\widehat{h}(V) \geq \frac{c_{11}}{C_0^{3/2}(n+1)^{1+4/(n-s)}(n-s)^2} \times \frac{(\log((n+1)\log((n+1)D)))^{2+1/(n-s)}}{(\log((n+1)D))^{1+2/(n-s)}},$$

qui contredit (11) pour C_0 assez grand.

(b) DEUXIÈME CAS : *il existe un premier p tel que $[\mathbb{Q}(W) : \mathbb{Q}([p]W)] > n^2$.* Dans ce cas, le lemme 3.4 montre qu'il existe $\zeta \in \ker([p])$ tel que $\mathbb{Q}(\zeta \cdot W) = \mathbb{Q}([p]W)$, et donc que la variété

$$V_2 = \bigcup_{\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} \sigma(\zeta \cdot W)$$

est de degré

$$D' = [\mathbb{Q}(W) : \mathbb{Q}([p]W)]^{-1} \deg(V_1) < n^{-2} \deg(V_1) \leq D$$

et sa hauteur normalisée vérifie

$$\frac{\widehat{h}(V_2)}{\deg(V_2)} = \frac{\widehat{h}(V_1)}{\deg(V_1)}.$$

Par hypothèse de minimalité, on en déduit que

$$\widehat{h}(V_2) \geq \frac{1}{C_0^2(n+1)^{1+4/(n-s)}(n-s)^2} \frac{(\log((n+1)\log((n+1)D')))^{2+1/(n-s)}}{(\log((n+1)D'))^{1+2/(n-s)}}.$$

On vérifie que la fonction

$$x \mapsto \frac{(\log((n+1)\log((n+1)x)))^{2+1/(n-s)}}{(\log((n+1)x))^{1+2/(n-s)}}$$

est décroissante (pour $n \geq 3$, ou, dans tous les cas pour $x \geq c_{12}$); donc

$$\begin{aligned} \widehat{h}(V) &\geq \widehat{h}(V_1) = \frac{\deg(V_1)\widehat{h}(V_2)}{\deg(V_2)} \geq n^2\widehat{h}(V_2) \\ &\geq \frac{c_{13}n^2}{C_0^2(n+1)^{1+4/(n-s)}(n-s)^2} \frac{(\log((n+1)\log((n+1)D)))^{2+1/(n-s)}}{(\log((n+1)D))^{1+2/(n-s)}}, \end{aligned}$$

qui contredit à nouveau (11).

Le théorème 1.7 est donc entièrement établi. ■

Références

- [Am-Da] F. Amoroso et S. David, *Le problème de Lehmer en dimension supérieure*, J. Reine Angew. Math. 513 (1999), 145–179.
- [Bo-Va] E. Bombieri and J. Vaaler, *On Siegel's lemma*, Invent. Math. 73 (1983), 11–32.
- [Bor] A. Borel, *Linear Algebraic Groups*, Benjamin, Reading, MA, 1969.
- [Boy] D. Boyd, *Kronecker's theorem and Lehmer's problem for polynomials in several variables*, J. Number Theory 13 (1980), 116–121.
- [Da-Ph1] S. David et P. Philippon, *Minors des hauteurs normalisées des sous-variétés de variétés abéliennes*, dans : Contemp. Math. 210, K. Murty et M. Waldschmidt (éds.), Amer. Math. Soc., 1988, 333–364.
- [Da-Ph2] —, —, *Minors des hauteurs normalisées des sous-variétés des tores*, Ann. Scuola Norm. Sup. Pisa (4) 28 (1999), 489–543.
- [Do] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401.
- [Do-La-Sc] E. Dobrowolski, W. Lawton and A. Schinzel, *On a problem of Lehmer*, in: Studies in Pure Mathematics, To the memory of Paul Turán, P. Erdős (éd.), Birkhäuser, Basel, 1983, 135–144.
- [Hi] M. Hindry, *Autour d'une conjecture de S. Lang*, Invent. Math. 94 (1988), 575–603.
- [La] W. Lawton, *A generalization of a theorem of Kronecker*, J. Sci. Fac. Chiang-mai Univ. (Thaïlande) 4 (1977), 15–23.
- [Le] D. H. Lehmer, *Factorisation of some cyclotomic functions*, Ann. of Math. 34 (1933), 461–479.
- [Ph1] P. Philippon, *Critères pour l'indépendance algébrique*, Publ. Math. Inst. Hautes Etud. Sci. 64 (1986), 5–52.

- [Ph2] P. Philippon, *Sur des hauteurs alternatives I, II et III*, Math. Ann. 289 (1991), 255–283; Ann. Inst. Fourier (Grenoble) 44 (1994), 1043–1065; J. Math. Pures Appl. 74 (1995), 345–365.
- [Ra] U. Rausch, *On a theorem of Dobrowolski about the product of conjugate numbers*, Colloq. Math. 50 (1985), 137–142.
- [Sc] 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), 329–331.
- [Sm] C. J. Smyth, *A Kronecker-type theorem for complex polynomials in several variables*, Canad. Math. Bull. 24 (1981), 447–452; *Errata*, ibid. 25 (1982), 504.
- [St-Va] T. Struppeck and J. Vaaler, *Inequalities for heights of algebraic subspaces and the Thue–Siegel principle*, in: Analytic Number Theory, Proc. Conf. in Honor of Paul T. Bateman, Progr. Math. 85, Birkhäuser, Boston, 1990, 494–527.
- [Sz-Ul-Zh] L. Szpiro, E. Ullmo et S. Zhang, *Équidistribution des petits points*, Invent. Math. 127 (1997), 337–347.
- [Vo] P. Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith. 74 (1996), 81–95.
- [Zh1] S. Zhang, *Positive line bundles on arithmetic surfaces*, Ann. of Math. 136 (1992), 569–587.
- [Zh2] —, *Positive line bundles on arithmetic varieties*, J. Amer. Math. Soc. 8 (1995), 187–221.
- [Zh3] —, *Small points and adelic metrics*, J. Algebraic Geom. 4 (1995), 281–300.

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

U.M.R. 9994 (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, France
 E-mail: david@math.jussieu.fr

*Reçu le 28.7.1998
 et révisé le 12.3.1999*

(3455)