C. R. Acad. Sci. Paris, t. 326, Série I, p. 1163-1166, 1998
Théorie des nombres/*Number Theory*

Le théorème de Dobrowolski en dimension supérieure

Francesco AMOROSO [a], **Sinnou DAVID** [b]

[a] Dipartimento di matematica, Università di Torino, Via Carlo Alberto 10, 10123 Torino, Italie
[b] Problèmes diophantiens, UMR 9994, Université Paris 6, case 247, 4, place Jussieu, 75005 Paris, France

(Reçu le 15 janvier 1998, accepté le 2 février 1998)

Résumé. Nous minorons le produit des hauteurs de Weil de nombres algébriques multiplicativement indépendants en fonction du degré du corps de nombres qu'ils engendrent. Le résultat que nous obtenons généralise à la dimension supérieure le travail de Dobrowolski, et permet en particulier de résoudre le problème de Lehmer pour les corps de nombres ayant un « petit » groupe de Galois. © Académie des Sciences/Elsevier, Paris

Dobrowolski's theorem in higher dimension

Abstract. *We provide a lower bound for the product of the Weil height of multiplicatively independent algebraic numbers, in terms of the degree of the number field they generate. Our bound is a generalization of a result of Dobrowolski and, in particular, shows that the Lehmer problem is true for number fields having a "small" Galois group.* © Académie des Sciences/Elsevier, Paris

1. Introduction

On sait que la hauteur de Weil logarithmique et absolue $\mathrm{h}(\alpha)$ d'un nombre algébrique α est nulle si et seulement si α est une racine de l'unité. Le problème de Lehmer consiste à déterminer quelle est la minoration optimale (en fonction du degré $\deg(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$) de la hauteur $\mathrm{h}(\alpha)$, si α n'est pas une racine de l'unité. Plus précisément, on fait la conjecture suivante :

CONJECTURE 1. – *Il existe un nombre réel $c > 0$ tel que pout tout $\alpha \in \mathbb{G}_m(\overline{\mathbb{Q}})$, qui n'est pas une racine de l'unité, on ait* $\deg(\alpha)\,\mathrm{h}(\alpha) \geq c$.

Dans le cadre du problème de Lehmer, le meilleur résultat connu à ce jour est la minoration de Dobrowolski (*voir* [2]). Dans cette Note, nous généralisons ce résultat en dimension supérieure. Soit $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{G}_m^n(\overline{\mathbb{Q}})$; notons $\mathrm{h}(\boldsymbol{\alpha})$ la hauteur de Weil du point projectif défini par $(1, \boldsymbol{\alpha})$. Cette normalisation de la hauteur permet de conserver la propriété : $\mathrm{h}(\boldsymbol{\alpha}) = 0$, si et seulement si $\boldsymbol{\alpha}$ est de torsion. On appellera aussi *indice d'obstruction* du point $\boldsymbol{\alpha}$, noté $\delta(\boldsymbol{\alpha})$, le degré minimal d'un

Note présentée par Jean-Pierre SERRE.

polynôme non nul à coefficients rationnels, s'annulant en $\boldsymbol{\alpha}$. L'indice d'obstruction coïncide clairement avec le degré $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$ en dimension 1, mais il se trouve que c'est cette notion, plus géométrique, qui intervient naturellement dans notre construction. Ces deux quantités sont liées par la relation $\delta(\boldsymbol{\alpha}) \leq nD^{1/n}$, assurée par l'algèbre linéaire. Notre résultat principal est le suivant :

THÉORÈME 1. – *Pour tout entier $n \geq 1$, il existe $c(n) > 0$, effectivement calculable, tel que pour tout élément $\boldsymbol{\alpha}$ de $\mathbb{G}_m^n(\overline{\mathbb{Q}})$, dont les coordonnées sont multiplicativement indépendantes, on ait :*

$$\delta(\boldsymbol{\alpha})\,\mathrm{h}(\boldsymbol{\alpha}) \geq c(n)\log(3\delta(\boldsymbol{\alpha}))^{-\kappa(n)},$$

où $\kappa(n) = (n+1)(n+1)!^n - n$.

En utilisant la relation entre l'indice d'obstruction et le degré D du corps de définition du point $\boldsymbol{\alpha}$, on en déduit que, dans les hypothèses du théorème 1, $\max_{1\leq i\leq n} \mathrm{h}(\alpha_i) \geq c(n)\, D^{-1/n}\log(3D)^{-\kappa(n)}$. De plus, une astuce « à la Landau », qui consiste à remplacer les α_i par des racines convenables, permet de déduire du théorème 1 le résultat apparemment plus fort suivant :

THÉORÈME 2. – *Pour tout entier $n \geq 1$, il existe un nombre réel $c(n) > 0$, tel que pour tout élément $\boldsymbol{\alpha}$ de $\mathbb{G}_m^n(\overline{\mathbb{Q}})$, dont les coordonnées sont multiplicativement indépendantes, on ait :*

$$\mathrm{h}(\alpha_1)\cdots \mathrm{h}(\alpha_n) \geq c(n)\, D^{-1}\log(3D)^{-n\kappa(n)}.$$

Comme nous n'avons pas réellement cherché à optimiser les estimations, notre 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.

Nos résultats permettent d'obtenir quelques informations partielles sur la structure du corps de nombres engendré par un contre-exemple éventuel au prolème de Lehmer. Plus particulièrement, ils permettent de dire qu'un tel contre-exemple possède un « gros » groupe de Galois :

COROLLAIRE 1. – *Pour tout entier $k \geq 1$, il existe une constante $c(k) > 0$, telle que pour tout $\alpha \in \mathbb{G}_m(\overline{\mathbb{Q}})$, qui n'est pas une racine de l'unité et pour lequel le degré de la clôture galoisienne de $\mathbb{Q}(\alpha)/\mathbb{Q}$ est $\leq \deg(\alpha)^k$, on ait $\deg(\alpha)\,\mathrm{h}(\alpha) \geq c(k)$.*

En particulier; on en déduit que la conjecture de Lehmer est vraie si l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne, ou si l'équation $P(x) = 0$ (où P est le polynôme minimal de α) est résoluble par radicaux.

2. Généralisation des lemmes de Dobrowolski

La preuve du théorème 1 se compose en plusieurs pas intermédiaires. Le premier consiste à généraliser le lemme-clef de Dobrowolski (*voir* [2], lemme 1), qui permet d'extrapoler; cette partie nécessite un argument plus sophistiqué qu'une simple application du petit théorème de Fermat sur les polynômes. Un argument d'algèbre commutative permet d'obtenir :

THÉORÈME 3. – *Soit $F \in \mathbb{Z}[x_1, \ldots, x_n]$ de degré $\leq L$ et nul à un ordre $\geq T$ en $\boldsymbol{\alpha} \in \mathbb{G}_m^n(\overline{\mathbb{Q}})$. Pour tout nombre premier $p \in \mathbb{Z}$ et pour toute valeur absolue ν (normalisée de la façon usuelle) de $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ divisant p, on a la majoration :*

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

Ici, et dans la suite, on note $\boldsymbol{x}^\ell = (x_1^\ell, \ldots, x_n^\ell)$ $(\boldsymbol{x} \in \mathbb{G}_m^n,\ \ell \in \mathbb{Z})$.

Ensuite on passe à l'étude de l'action de la multiplication par ℓ sur les sous-variétés algébriques de $\mathbb{G}_m^n$. Soit V une sous-variété algébrique $\mathbb{Q}$-irréductible de $\mathbb{G}_m^n$ de dimension d, et notons $W_1, \ldots, W_k$ ses composantes $\overline{\mathbb{Q}}$-irréductibles. Nous aurons besoin dans la suite de travailler avec des « bons » entiers ℓ, pour lesquels les conjugués des multiples $[\ell]\, W_j = \{x^\ell,\, x \in W_j\}$ sont distincts *et* tels que les degrés de ces multiples ne sont pas trop petits.

Cela nous conduit à introduire l'ensemble $E(V)$ des entiers $\ell \in \mathbb{Z}$ pour lesquels *ou bien* il existe deux composantes distinctes de V, disons W_i et W_j, telles que $[\ell]\, W_i = [\ell]\, W_j$, *ou bien* $\deg([\ell]\, W_1) < \deg(W_1)$. Remarquons que si $\ell, \ell' \in \mathbb{Z}$ et $\ell \notin E(V)$, $\ell' \notin E([\ell]\, V)$, alors $\ell'\ell \notin E(V)$.

Les propriétés de l'ensemble $E(V)$ dont nous aurons besoin sont résumées dans la proposition suivante, que l'on prouve en étudiant les degrés des images de sous-variétés algébriques de $\mathbb{G}_m^n$ par des multiplications, et à l'aide d'une variante ad hoc 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* [2], lemmes 2 et 3).

PROPOSITION 1. – *On a* $|E(V) \cap \{p \text{ premier}\}| \leq \frac{d+1}{\log(2)} \log\deg(V)$. *De plus, si* Λ *est un ensemble fini d'entiers positifs ne rencontrant pas* $E(V)$, *et si* V *n'est pas un sous-tore de* $\mathbb{G}_m^n$, *on a* $\deg(\bigcup_{\ell\in\Lambda}[\ell]\,(V) \geq |\Lambda| \deg(V)$. *Enfin, si* $\ell \notin E(V)$ *et si* $\widetilde{V}$ *est une sous-variété de* $\mathbb{G}_m^n$, *définie sur* $\mathbb{Q}$, *ayant la même dimension que* V, *et telle que* $V \subset [\ell]^{-1}\, \widetilde{V}$, *on a* $\deg(V) \leq \deg(\widetilde{V})$.

3. Transcendance

L'argument suivant est classique : il s'agit de construire, à l'aide du lemme de Siegel, un polynôme non nul $F \in \mathbb{Q}[x_1, \ldots, x_n]$ de hauteur « petite » et de degré total $\leq L$, s'annulant en $\boldsymbol{\alpha}$ à un ordre $\geq T$, et ensuite d'extrapoler sur des puissances convenables de $\boldsymbol{\alpha}$, à l'aide du théorème 3. Pour ce faire, on majore l'exposant de Dirichlet du système linéaire à résoudre en fonction de l'indice d'obstruction (« astuce de Philippon–Waldschmidt », [5], §. 6). Soit $\rho \in]0, (n+1)!^{n-1}[$ et posons $e = (\rho+1)(n+1)((n+1)!-1)$ et :

$$L = C_0^{1/2}\, \delta(\boldsymbol{\alpha})\, q(\boldsymbol{\alpha})^{n+1}, \quad T = C_0^{1/4}\, q(\boldsymbol{\alpha})^n, \quad N_j = (C_0 \log(3\delta(\boldsymbol{\alpha})))^{(\rho+1)(n+1)j\cdot j!}$$

$(j = 1, \ldots, n)$. Ci-dessus, $q(\boldsymbol{\alpha}) = \log(3\delta(\boldsymbol{\alpha}))/\log\log(3\delta(\boldsymbol{\alpha}))$ et 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). Soit aussi, $\mathcal{P}_j = \{1\} \cup \{p$ premier, $\log(3\delta(\boldsymbol{\alpha})) \leq p \leq N_j\}$ $(j = 1, \ldots, n)$. Les deux étapes de la partie « transcendance », construction de la fonction auxiliaire et extrapolation, sont résumées dans la proposition qui suit :

PROPOSITION 2. – *Supposons* $\delta(\boldsymbol{\alpha})\, \mathrm{h}(\boldsymbol{\alpha}) < (C_0 \log(3\delta(\boldsymbol{\alpha})))^{-e-1}$. *Il existe alors un polynôme non nul* $F \in \mathbb{Z}[x_1, \ldots, x_n]$ *de degré* $\leq L$, *s'annulant en* $\boldsymbol{\alpha}^{p_1\cdots p_n}$ *pour tout* $(p_1, \ldots, p_n) \in \mathcal{P}_1 \times \cdots \times \mathcal{P}_n$.

On démontre ensuite la variante suivante du lemme de zéros de Philippon (*voir* [4], théorème 2.1) :

THÉORÈME 4. – *Soit* $F \in \mathbb{Q}[x_1, \ldots, x_n]$ *comme dans la proposition* 2. *Il existe alors une sous-variété algébrique* $\mathbb{Q}$*-irréductible* V *de* $\mathbb{G}_m^n$ *et un entier* $r \in [\operatorname{codim}(V), n]$ *tels que* $\boldsymbol{\alpha}^{p_j\cdots p_n} \in V$ *pour un certain* $(p_j, \ldots, p_n) \in \mathcal{P}_j \times \cdots \times \mathcal{P}_n$ *et* $\deg\bigcup_{p\in\mathcal{P}_r}[p]\, V \leq (N_1 \cdots N_{r-1} L)^{\operatorname{codim}(V)}$.

Supposons maintenant $\alpha_1, \ldots, \alpha_n$ multiplicativement indépendants, et supposons que l'hypothèse de la proposition 2 est satisfaite. Soit W une variété $\mathbb{Q}$-irréductible telle que $\log\deg(W) \leq (C_0 \log(3\delta(\boldsymbol{\alpha})))^{(\rho+1)(n+1)-1}$. En utilisant la proposition 1, la proposition 2 et le théorème 4, on arrive à la proposition suivante, qui montre que si le théorème 1 est faux, on peut trouver de petits multiples de $\boldsymbol{\alpha}$ dont l'incide d'obstruction est beaucoup plus faible que celui de $\boldsymbol{\alpha}$:

PROPOSITION 3. – *Il existe un entier* $\ell \leq (C_0 \log(3\delta(\boldsymbol{\alpha})))^e$ *tel que* $\ell \notin E(W)$ *et :*

$$\delta(\boldsymbol{\alpha}^\ell) < C_0^{-1}\, (C_0 \log(3\delta(\boldsymbol{\alpha})))^{-\rho(n+1)} \cdot \delta(\boldsymbol{\alpha}).$$

4. 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 :

$$\varepsilon_i = C_0^{-1}\,(C_0 \log(3\delta\,(\boldsymbol{\alpha})))^{-(n+1)\,((n+1)!^{n-i}+1)} < 1,$$
$$L_i = (C_0\,(\log C_0)^2 \log(3\delta\,(\boldsymbol{\alpha})))^{(n+1)\,(n+1)!^{n-i}((n+1)!-1)}$$

$(i = 1, \ldots, n)$. On introduit ensuite un ensemble $\boldsymbol{W}_{\alpha}$ formé des triplets $(k, \boldsymbol{l}, \boldsymbol{V})$, où $k \in [0, n]$ est un entier, $\boldsymbol{l} = (\ell_1, \ldots, \ell_k) \in \mathbb{Z}^k$ avec $0 \le \ell_i \le L_i$, et $\boldsymbol{V} = (V_0, \ldots, V_k)$ est un $(k+1)$-uplet de variétés $\mathbb{Q}$-irréductibles de $\mathbb{G}_m^n$, avec $\boldsymbol{\alpha} \in V_0$. On demande aux éléments $(k, \boldsymbol{l}, \boldsymbol{W}) \in \boldsymbol{W}_{\alpha}$ de satisfaire les propriétés : $\deg(V_i)^{1/\operatorname{codim}(V_i)} \le L_{i+1} \cdots L_n \delta\,(\boldsymbol{\alpha}^{\boldsymbol{l}(i)})$ $(i = 0, \ldots, k)$, et $\delta\,(\boldsymbol{\alpha}^{\boldsymbol{l}(i)}) \le \varepsilon_i \delta\,(\boldsymbol{\alpha}^{\boldsymbol{l}(i-1)})$, $\ell_i \notin E\,(V_{i-1})$, $[\ell_i]^{-1} V_i \supset V_{i-1}\,(i = 1, \ldots, k)$, où l'on a noté $\boldsymbol{\alpha}^{\boldsymbol{l}(i)} = \boldsymbol{\alpha}^{\ell_1 \cdots \ell_i}$.

La proposition suivante, que l'on montre par récurrence, en utilisant plusieurs fois la proposition 3, joue un rôle essentiel dans la dernière partie de la preuve :

PROPOSITION 4. – *Supposons les $\alpha_1, \ldots, \alpha_n$ multiplicativement indépendants, et $\delta\,(\boldsymbol{\alpha})\,\mathrm{h}\,(\boldsymbol{\alpha}) < (C_0\,(\log C_0)^2 \log(3\delta))^{-(n+1)\,(n+1)!^n+n}$. Alors, il existe $(k, \boldsymbol{l}, \boldsymbol{V}) \in \boldsymbol{W}_{\alpha}$ tel que $\dim(V_{i-1}) = \dim(V_i)$ pour au moins un indice $i \in [1, k]$.*

5. Démonstration du théorème 1

Soit $\boldsymbol{\alpha} \in \mathbb{G}_m^n\,(\overline{\mathbb{Q}})$ qui vérifie les hypothèses de la proposition 4. Cette dernière nous assure l'existence de deux variétés $\mathbb{Q}$-irréductibles V_{i-1} et V_i de la même dimension, qui vérifient $[\ell_i]^{-1} V_i \supset V_{i-1}$ pour un certain $\ell_i \notin E\,(V_{i-1})$. La proposition 1 montre alors que $\deg(V_{i-1}) \le \deg(V_i)$. Mais, comme V_{i-1} passe par $\boldsymbol{\alpha}^{\boldsymbol{l}(i-1)}$, on a $\delta\,(\boldsymbol{\alpha}^{\boldsymbol{l}(i-1)}) \le n \deg(V_{i-1})^{1/\operatorname{codim}(V_i)}$ (*voir* [1], chapitre 1, pages 8 et 9). De la définition de $\boldsymbol{W}_{\alpha}$, on déduit alors facilement : $\delta\,(\boldsymbol{\alpha}^{\boldsymbol{l}(i-1)}) < n\varepsilon_i L_{i+1} \cdots L_n\,(\boldsymbol{\alpha}^{\boldsymbol{l}(i-1)}) < \delta\,(\boldsymbol{\alpha}^{\boldsymbol{l}(i-1)})$. Cette contradiction montre que l'hypothèse sur $\mathrm{h}\,(\boldsymbol{\alpha})$ de la proposition 4 est fausse, et le théorème 1 en découle.

Références bibliographiques

[1] Chardin M., Une majoration de la fonction de Hilbert et ses conséquences pour l'interpolation algébrique, Bull. Soc. Math. France 117 (1988) 305–318.

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

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

[4] Philippon P., Waldschmidt M., Formes linéaires de logarithmes dans les groupes algébriques commutatifs, Illinois J. Math. 32 (2) (1988) 281–314.