

CHEN GONG-LIANG

**Relations de dépendance linéaire entre des
logarithmes de nombres algébriques**

Annales de la faculté des sciences de Toulouse 6^e série, tome 5, n^o 4
(1996), p. 587-597

http://www.numdam.org/item?id=AFST_1996_6_5_4_587_0

© Université Paul Sabatier, 1996, tous droits réservés.

L'accès aux archives de la revue « Annales de la faculté des sciences de Toulouse » (<http://picard.ups-tlse.fr/~annales/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Relations de dépendance linéaire entre des logarithmes de nombres algébriques^(*)

CHEN GONG-LIANG⁽¹⁾

RÉSUMÉ. — Nous étudions le réseau constitué par l'ensemble des relations linéaires à coefficients entiers liant des logarithmes de nombres algébriques. Nous montrons qu'il existe une "petite" famille libre dans ce réseau par une démonstration autonome utilisant les théorèmes classiques de Minkowski.

ABSTRACT. — We study the lattice of linear relations with integral coefficients between the logarithms of algebraic numbers. We prove that there exists a "little" free family in the lattice by an autonomous demonstration using the classical theorems of Minkowski.

0. Introduction et résultats

Étant donnés $\log \alpha_1, \dots, \log \alpha_m$ des logarithmes de nombres algébriques non nuls $\alpha_1, \dots, \alpha_m$, on s'intéresse aux relations linéaires à coefficients rationnels liant ces logarithmes. Si l'on suppose que $\log \alpha_1, \dots, \log \alpha_m$ sont linéairement dépendants sur \mathbb{Q} , l'existence d'une "petite" combinaison linéaire est un résultat classiquement utilisé pour la minoration des combinaisons linéaires de logarithmes de nombres algébriques : il permet de passer du cas où les logarithmes sont \mathbb{Q} -linéairement indépendants au cas général (voir par exemple [W1, sect. 4] ou [W2, chap. VII]). La proposition

(*) Reçu le 1 septembre 1994

(1) Équipe de Théorie des Nombres, Faculté des Sciences, 23 rue du Docteur Paul Michelon, F-42023 ST ÉTIENNE Cedex 2 (France);
Département de Mathématiques, Université de Wuhan, 430072 Wuhan (R.P. de Chine)

Ce travail a été réalisé à l'Université de Saint-Étienne au cours d'un séjour financé par une bourse doctorale du Ministère des Relations Extérieures.

principale de cet article donne une estimation des coefficients d'une telle combinaison linéaire. Mais on doit d'abord définir les notations utilisées dans la suite.

Un réseau \mathcal{L} de \mathbb{R}^n est un sous-groupe discret de rang n (sur \mathbb{Z}) de \mathbb{R}^n . Un tel réseau admet des bases (sur \mathbb{Z}) et elles se déduisent les unes des autres par des transformations unimodulaires. Il en résulte que le volume du parallélépipède construit sur les éléments d'une base est indépendant de la base choisie. C'est le volume d'une maille fondamentale du réseau, appelé aussi volume du réseau et noté $H(\mathcal{L})$. Par abus de langage, nous appellerons encore réseau de \mathbb{R}^m un sous-groupe discret \mathcal{L} de rang $n \leq m$ et nous noterons encore $H(\mathcal{L})$ son volume, c'est-à-dire le volume n -dimensionnel du parallélépipède construit sur une base de \mathcal{L} .

Si (x_1, \dots, x_n) (en notant $x_i = (x_{i1}, \dots, x_{im}) \in \mathbb{R}^m$) est une base de \mathcal{L} , alors

$$H(\mathcal{L}) = \det(X {}^t X)^{1/2} \quad \text{où } X = (x_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \in M_{n,m}(\mathbb{R})$$

est la matrice de la base considérée et ${}^t X$ est sa transposée. En effet $X {}^t X \in M_{n,n}(\mathbb{R})$ est la matrice de Gram $((x_i, x_j))_{1 \leq i, j \leq n}$ relative au produit scalaire euclidien de \mathbb{R}^m noté $\langle \cdot, \cdot \rangle$ (pour ces questions de volume, on peut consulter le paragraphe 8.11 de [Berg] ou le début du chapitre 9 de [G]).

Revenons au cas des logarithmes de nombres algébriques : si le rang sur \mathbb{Z} de la famille des $\log \alpha_i$ ($1 \leq i \leq m$) est r , l'ensemble des relations linéaires

$$\mathcal{L} = \left\{ (t_1, \dots, t_m) \in \mathbb{Z}^m \mid \sum_{1 \leq i \leq m} t_i \log \alpha_i = 0 \right\}$$

est un réseau de rang $m - r$ de \mathbb{R}^m . Le but de cet article est de majorer le volume $H(\mathcal{L})$ de ce réseau. En notant h la hauteur logarithmique absolue et $\overline{\mathbb{Q}}$ la clôture algébrique de \mathbb{Q} dans \mathbb{C} , on a le résultat suivant.

PROPOSITION . — *Soient r et m des nombres entiers vérifiant $1 \leq r \leq m$. Pour $1 \leq j \leq m$, soit $\ell_j \in \mathbb{C}$ tel que $\alpha_j = \exp(\ell_j)$ soit un nombre algébrique. Soit K un corps de nombres contenant $\mathbb{Q}(\alpha_1, \dots, \alpha_m)$ et soit $D = [K : \mathbb{Q}]$.*

Si le rang sur \mathbb{Q} de la famille (ℓ_1, \dots, ℓ_m) est r , alors le réseau \mathcal{L} (de rang $m - r$) des relations linéaires à coefficients dans \mathbb{Z} liant les ℓ_j a un volume majoré par

$$H(\mathcal{L}) \leq (10D)^{3r} r^r \Omega,$$

où

$$\Omega = \min \left\{ \det(A {}^t A)^{1/2} \prod_{1 \leq j \leq r} \max \left(h(\gamma_j), \frac{|\log \gamma_j|}{D} \right) \right\},$$

le minimum étant pris sur les $(\gamma_1, \dots, \gamma_r) \in \overline{\mathbb{Q}}^{\times r}$ et les $A \in M_{r,m}(\mathbb{Q})$ tels que $(\ell_1, \dots, \ell_m) = (\log \gamma_1, \dots, \log \gamma_r)A$. En particulier, on a

$$H(\mathcal{L}) \leq (m - r + 1)^{r/2} r^r (10D)^{3r} \Omega_r,$$

où

$$\Omega_r = \max_{1 \leq j_1 < \dots < j_r \leq m} \prod_{1 \leq i \leq r} V_{j_i} \quad \text{et} \quad V_j = \max \left(h(\alpha_j), \frac{|\ell_j|}{D} \right).$$

La géométrie des nombres permet, connaissant une majoration de $H(\mathcal{L})$, d'extraire de \mathcal{L} une "petite" base. Par exemple, D. W. Masser utilise dans [M] le procédé suivant : si F est une jauge sur \mathbb{R}^n (*symmetric convex distance-function* dans la terminologie de [C]) et si V_F est le volume du convexe $\{x \in \mathbb{R}^n \mid F(x) < 1\}$, le théorème des minima successifs de Minkowski ([C, théorème V, p. 218] ou [S, théorème 16, p. 32]) et un lemme classique ([C, lemme 8, p. 135]) montrent qu'il existe une base (b_1, \dots, b_n) du réseau \mathcal{L} vérifiant

$$\prod_{1 \leq i \leq n} F(b_i) \leq n! \frac{2H(\mathcal{L})}{V_F}.$$

Si F est la norme du maximum ($|x| = \max_{1 \leq i \leq n} |x_i|$), on obtient

$$\prod_{1 \leq i \leq n} |b_i| \leq n! 2^{1-n} H(\mathcal{L});$$

et si F est la norme euclidienne, cela donne

$$\prod_{1 \leq i \leq n} \|b_i\| \leq n! 2\pi^{-n/2} \Gamma\left(1 + \frac{n}{2}\right) H(\mathcal{L}).$$

On dispose aussi de résultats donnant des bases "réduites" vérifiant des inégalités du type

$$\prod_{1 \leq i \leq n} F(b_i) \leq 2^n \left(\frac{3}{2}\right)^{\frac{n(n-1)}{2}} \frac{H(\mathcal{L})}{V_F},$$

l'exposant $n(n-1)/2$ pouvant être éventuellement raffiné (voir [S, p. 99] ou [GrL, pp. 69-72, 124]). On corrigera dans [GrL] une faute d'impression qui se propage à partir du haut de la page 70 en remplaçant $\Gamma((n+1)/2)$ par $\Gamma(1+n/2)$ dès l'énoncé du théorème 3, page 69). Signalons enfin que S. Lang [L1, corollaire 7.8, p. 131] attribue à Ch. Hermite la preuve de l'existence d'une base "presque orthogonalisée" vérifiant

$$\prod_{1 \leq i \leq n} \|b_i\| \leq \left(\frac{2}{\sqrt{3}}\right)^{\frac{n(n-1)}{2}} H(\mathcal{L}).$$

Suivant les valeurs de n , c'est l'une ou l'autre de ces majorations qui est la plus précise!

Le premier résultat donnant une majoration pour les coefficients d'une relation de dépendance linéaire entre logarithmes de nombres algébriques remonte à 1973 et il est dû à A. Baker [B, lemme 2, p. 250]. Il est obtenu par une méthode de transcendance, méthode reprise en 1981 dans [BijCij]. Cependant, l'utilisation de la géométrie des nombres donne des estimations au moins aussi bonnes que les méthodes transcendentes [Lo-vdP2]. La première apparition de la géométrie des nombres dans ce genre de questions remonte aussi à 1973 avec les travaux de H. M. Stark [St, sect. 3, lemme 7] sur la dépendance multiplicative d'unités d'un corps de nombres. Le procédé est généralisé par J. H. Loxton et A. J. van der Poorten [vdPLo1] au cas de nombres algébriques quelconques (plus nécessairement des unités). Dans sa thèse A. Bijlsma [Bij] déduit de [vdPLo1] un énoncé sur les relations de dépendance linéaire entre logarithmes. Cet énoncé est amélioré par M. Waldschmidt [W1] qui ne le déduit pas de [vdPLo1], mais utilise la géométrie des nombres de façon un peu différente [L2, lemme 7.5, p. 241]. Dans un cadre plus général, on peut citer [L1, chap. V, sect. 7] où S. Lang étend les résultats de Stark-Loxton-van der Poorten aux courbes elliptiques. Plus récemment, et dans le cadre très général des groupes algébriques, on doit citer les travaux de D. W. Masser [M] et de D. Bertrand ([Be1], [Be2] et [Be3]).

Les résultats de D. Bertrand concernent les relations de dépendance multiplicative et ne sont pas comparables à la proposition ci-dessus. Cependant, dans le cadre multiplicatif, D. Bertrand décompose $H(\mathcal{L})^2$ en une somme de carrés (correspondant à des multidegrés) qui ont chacun une majoration du type de la majoration globale de $H(\mathcal{L})^2$. Il serait intéressant d'obtenir une décomposition analogue dans le cas traité ici. Par contre, on peut tirer des travaux de D. W. Masser [M] un corollaire proche de notre proposition,

mais qui ne sépare pas les contributions des α_i . Un raffinement (dû à D. Roy, mais non publié) du résultat de D. W. Masser donne, dans le cas particulier étudié ici, essentiellement la même chose que la proposition : la constante $r^r(m-r+1)^{r/2}$ est remplacée par m^r . Notre résultat est donc meilleur pour les petites valeurs de r , plus précisément pour $r < (1 + \sqrt{1 + 4m})/2$. On verra à la section 3 que cette constante peut être améliorée dans certains cas.

Enfin, dans un article récent, E. M. Matveev donne un résultat [M, theorem 6] du même genre que notre proposition. Mais, au lieu d'estimer le volume du réseau \mathcal{L} , il majore le produit des normes des éléments d'une base de \mathcal{L} , en choisissant une norme liée aux données α_i . Son résultat semble donc difficilement comparable au nôtre.

1. Quelques lemmes techniques

Soit

$$a_0X^d + \dots + a_d = a_0 \prod_{1 \leq j \leq d} (X - \alpha_j) \in \mathbb{Z}[X]$$

le polynôme minimal du nombre algébrique α ; on note $h(\alpha)$ la hauteur logarithmique absolue (hauteur de Weil), définie par $h(\alpha) = (1/d) \log M(\alpha)$, où $M(\alpha) = a_0 \prod_{1 \leq j \leq d} \max(1, |\alpha_j|)$ est la mesure de Mahler.

LEMME 1. — Soient $n \in \mathbb{N} \setminus \{0\}$, $m \in \mathbb{Z}$ et $\alpha \neq 0$, β , $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}$ des nombres algébriques. Alors on a :

- (1) $h(\alpha\beta) \leq h(\alpha) + h(\beta)$ et $h(\alpha^{m/n}) = |m/n|h(\alpha)$ pour toute détermination du nombre algébrique $\alpha^{m/n}$;
- (2) $h(\alpha_1 + \dots + \alpha_n) \leq h(\alpha_1) + \dots + h(\alpha_n) + \log n$;
- (3) pour $f \in \mathbb{Z}[X_1, \dots, X_n] \setminus \{0\}$, on a

$$h(f(\alpha_1, \dots, \alpha_n)) \leq \log L(f) + \sum_{1 \leq i \leq n} (\deg_{X_i} f) h(\alpha_i),$$

où $L(f)$ est la longueur (somme des modules des coefficients) de f .

Démonstration. — Voir [W 2, prop. 3.2 et lemme 3.6]. \square

LEMME 2. — Soit $\ell \in \mathbb{C}$ tel que $\alpha = \exp(\ell)$ soit un nombre algébrique de degré au plus égal à d . Alors $\ell = 0$ dès que $\max(h(\alpha), |\ell|/d) \leq (10d)^{-3}$.

Démonstration. — C'est une conséquence d'un résultat du type Blanksby–Montgomery–Dobrowolski (par exemple [W2, théorème 3.16]) et du fait que l'indicatrice d'Euler φ vérifie l'inégalité $N \leq 2\varphi(N)^2$ pour tout entier $N \geq 1$. \square

Remarque. — On peut obtenir des résultats plus fins que le lemme 2 (par exemple remplacer le facteur d^{-3} par un facteur en $d^{-2}(\log d)^{-1}$ en utilisant le théorème de Blanksby–Montgomery, ou par un facteur en $d^{-2}(\log \log d)^{-1}$ en utilisant le théorème de Dobrowolski). Cela améliore la dépendance en D de la constante de la proposition.

LEMME 3. — Soient r et m des nombres entiers vérifiant $1 \leq r < m$. Soit (ℓ_1, \dots, ℓ_m) une famille de nombres complexes de rang r sur \mathbb{Q} . Alors il existe une partie $\{j_1, \dots, j_r\}$ de $\{1, \dots, m\}$ et une matrice $A \in M_{r,m}(\mathbb{Q})$ vérifiant

$$(\ell_1, \dots, \ell_m) = (\ell_{j_1}, \dots, \ell_{j_r})A \quad \text{et} \quad (0 <) \det({}^t A) \leq (m - r + 1)^r.$$

Démonstration. — Soit (t_1, \dots, t_{m-r}) une base du réseau \mathcal{L} des relations linéaires à coefficients dans \mathbb{Z} liant les ℓ_j . On a donc $\sum_{1 \leq j \leq m} t_{ij} \ell_j = 0$ pour $1 \leq i \leq m - r$. Quitte à changer la numérotation des ℓ_j , on peut supposer que

$$\left| \det(t_{ij})_{\substack{1 \leq i \leq m-r \\ r+1 \leq j \leq m}} \right| = \max_{1 \leq j_1 < \dots < j_{m-r} \leq m} \left| \det(t_{ij_k})_{1 \leq i, k \leq m-r} \right| > 0.$$

Notons

$$T = \det(t_{ij})_{\substack{1 \leq i \leq m-r \\ r+1 \leq j \leq m}}$$

et, pour $r + 1 \leq k \leq m$ et $1 \leq j \leq r$, soit T_{kj} le déterminant obtenu en remplaçant la colonne d'indice k de T par la colonne formée des t_{ij} ($1 \leq i \leq m - r$). Alors les formules de Cramer s'écrivent $\ell_k = -\sum_{1 \leq j \leq r} (T_{kj}/T) \ell_j$ pour $r + 1 \leq k \leq m$, c'est-à-dire $(\ell_1, \dots, \ell_m) = (\ell_1, \dots, \ell_r)A$, où A est la matrice

$$A = (I_r A') \quad \text{avec} \quad {}^t A' = -\frac{1}{T} (T_{kj})_{\substack{r+1 \leq k \leq m \\ 1 \leq j \leq r}},$$

et I_r est la matrice identité de dimension r . Par construction les coefficients de $A' \in M_{r,m-r}(\mathbb{Q})$ sont de module au plus 1, donc l'inégalité de Hadamard

$$\det(X {}^tX) \leq \prod_{1 \leq i \leq r} \left(\sum_{1 \leq j \leq m} x_{ij}^2 \right) \quad \text{si } X = (x_{ij}) \in M_{r,m}(\mathbb{R})$$

(voir, par exemple, le paragraphe 9.5 de [G]) donne la majoration annoncée de $\det(A {}^tA)$. \square

2. Le lemme fondamental

LEMME 4. — Soient r et m des nombres entiers vérifiant $1 \leq r < m$. Soit (a_1, \dots, a_r) une famille libre de r vecteurs de \mathbb{R}^m . On suppose que

$$\mathcal{V} = \{u \in \mathbb{Q}^m \mid \langle a_i, u \rangle = 0, 1 \leq i \leq r\}$$

est un sous-espace vectoriel de dimension $m - r$ de \mathbb{Q}^m et que les nombres réels $\varepsilon_i > 0$, $1 \leq i \leq r$, vérifient

$$\mathcal{L} := \mathcal{V} \cap \mathbb{Z}^m = \left\{ u \in \mathbb{Z}^m \mid |\langle a_i, u \rangle| < \varepsilon_i, 1 \leq i \leq r \right\}.$$

Alors le volume $H(\mathcal{L})$ du réseau \mathcal{L} est majoré par

$$H(\mathcal{L}) \leq \det(A {}^tA)^{1/2} \prod_{1 \leq i \leq r} \varepsilon_i^{-1},$$

où $A = (a_{ij}) \in M_{r,m}(\mathbb{R})$ est la matrice des a_i et tA est sa transposée.

Remarque. — Notons $L_i(u) = \langle a_i, u \rangle$. On a supposé que ces r formes linéaires étaient linéairement indépendantes. Si \mathcal{B} est une base du \mathbb{Q} -espace vectoriel engendré par les coefficients a_{ij} des L_i , alors, pour tout i , on peut écrire

$$L_i(u) = \sum_{1 \leq k \leq K_i} \lambda_{ki} L_{ki}(u),$$

où les λ_{ki} sont dans \mathcal{B} et les L_{ki} sont des formes linéaires à coefficients dans \mathbb{Q} . Alors $u \in \mathcal{V}$ si et seulement si $u \in \mathbb{Q}^m$ et $L_{ki}(u) = 0$ pour tout i ($1 \leq i \leq r$) et tout k ($1 \leq k \leq K_i$). L'hypothèse $\dim_{\mathbb{Q}} \mathcal{V} = m - r$ signifie donc

que le système des formes linéaires L_{ki} est de rang r . Il suffit d'en extraire un système libre (L'_1, \dots, L'_r) de rang r pour se ramener au cas où les a_i sont dans \mathbb{Q}^m . D'autre part, on a vu que les L_i sont combinaisons linéaires des L'_i . Comme le rang du système des L_i est r , les L'_i sont combinaisons linéaires des L_i . Il en résulte que l'existence de nombres réels $\varepsilon_i > 0$ tels que $\mathcal{L} = \mathcal{V} \cap \mathbb{Z}^m$ soit l'ensemble des $u \in \mathbb{Z}^m$ vérifiant $|\langle a_i, u \rangle| < \varepsilon_i$ pour $1 \leq i \leq r$ est équivalente à l'existence de nombres réels $\eta_i > 0$ tels que \mathcal{L} soit l'ensemble des $u \in \mathbb{Z}^m$ vérifiant $|L'_i(u)| < \eta_i$ pour $1 \leq i \leq r$. Or l'existence des η_i est claire : on peut choisir $\eta_i = 1/d_i$ où d_i est un dénominateur commun aux coefficients (rationnels) de L'_i .

Démonstration du lemme 4. — Soit (x_1, \dots, x_{m-r}) une base du réseau \mathcal{L} . Comme \mathcal{V} est contenu dans l'orthogonal de l'espace engendré par les a_i ($1 \leq i \leq r$), les vecteurs $a_1, \dots, a_r, x_1, \dots, x_{m-r}$ sont linéairement indépendants et forment donc une base de \mathbb{R}^m .

Soit S l'ensemble des $\sum_{1 \leq i \leq r} t_i a_i + \sum_{r+1 \leq i \leq m} t_i x_{i-r}$, où les $t_i \in \mathbb{R}$ ($1 \leq i \leq m$) vérifient

$$\left| \sum_{1 \leq i \leq r} t_i \langle a_i, a_j \rangle \right| < \varepsilon_j \text{ pour } 1 \leq j \leq r \text{ et } |t_i| < 1 \text{ pour } r+1 \leq j \leq m.$$

L'ensemble S est un ouvert convexe de \mathbb{R}^m , symétrique par rapport à l'origine et dont le volume $\text{vol}(S)$ est, par orthogonalité, le produit de $2^{m-r} H(\mathcal{L})$ et du volume r -dimensionnel de

$$T = \left\{ \sum_{1 \leq i \leq r} t_i a_i \mid \left| \sum_{1 \leq i \leq r} t_i \langle a_i, a_j \rangle \right| < \varepsilon_j, 1 \leq j \leq r \right\}.$$

Or le volume r -dimensionnel du réseau engendré par les a_i est $\det(A {}^t A)^{1/2}$. Le volume de $U = \{ \sum_{1 \leq i \leq r} u_i a_i \mid |u_j| < \varepsilon_j, 1 \leq j \leq r \}$ vaut donc $2^r \det(A {}^t A)^{1/2} \prod_{1 \leq i \leq r} \varepsilon_i$. Enfin U est l'image de T par l'application linéaire dont la matrice est $A {}^t A$ relativement à la base des a_i , et, si f est linéaire, on a $\text{vol}(f(T)) = |\det f| \text{vol}(T)$. Il en résulte que

$$\text{vol}(T) = 2^r \varepsilon_1 \cdots \varepsilon_r \frac{\det(A {}^t A)^{1/2}}{\det(A {}^t A)},$$

donc

$$\text{vol}(S) = 2^m \det(A {}^t A)^{-1/2} H(\mathcal{L}) \prod_{1 \leq i \leq r} \varepsilon_i.$$

Comme les x_j sont orthogonaux aux a_i , si u est dans S , on a $|\langle u, a_j \rangle| < \varepsilon_j$ pour $1 \leq j \leq r$. Si u est dans $S \cap \mathbb{Z}^m$, l'hypothèse montre donc que u est dans $\mathcal{L} \subset \mathcal{V}$, c'est-à-dire que $u = \sum_{r+1 \leq i \leq m} t_i x_{i-r}$. Mais les x_{i-r} sont linéairement indépendants et $u \in \mathcal{L}$, donc les t_i sont dans \mathbb{Z} pour $r+1 \leq i \leq m$, et comme ils sont de module < 1 , ils sont tous nuls, donc $u = 0$. Le premier théorème de Minkowski ([S, théorème 10, p. 12] ou [C, théorème II, p. 71]) montre alors que $\text{vol}(S) \leq 2^m$, d'où le résultat annoncé. \square

3. La preuve de la proposition

On se place dans les hypothèses de la proposition. Pour $1 \leq i \leq r$, soit γ_i un nombre algébrique non nul et $\log \gamma_i$ une détermination de son logarithme. Supposons que la matrice $A \in M_{r,m}(\mathbb{Q})$ vérifie $(\ell_1, \dots, \ell_m) = (\log \gamma_1, \dots, \log \gamma_r)A$. D'après le lemme 3, on peut toujours se mettre dans une telle situation. Comme le système (ℓ_1, \dots, ℓ_m) est de rang r sur \mathbb{Q} , il en est de même du système $(\log \gamma_1, \dots, \log \gamma_r)$ et le rang de la matrice A est r . Les vecteurs lignes $a_1, \dots, a_r \in \mathbb{Q}^m$ de la matrice A sont donc linéairement indépendants.

Pour $u \in \mathbb{Z}^m$, on a

$$(\ell_1, \dots, \ell_m)u = 0 \quad \text{si et seulement si} \quad (\log \gamma_1, \dots, \log \gamma_r)Au = 0,$$

c'est-à-dire $Au = 0$, puisque les nombres $\log \gamma_1, \dots, \log \gamma_r$ sont \mathbb{Q} -linéairement indépendants. Or $Au = 0$ se traduit par $\langle a_i, u \rangle = 0$ pour tout i ($1 \leq i \leq r$). On est donc dans la situation du lemme 4 qui donne la première partie de la proposition si on peut l'appliquer aux ε_i définis par

$$\varepsilon_i^{-1} = (10D)^3 r \max \left(h(\gamma_i), \frac{|\log \gamma_i|}{D} \right).$$

Soit donc $u \in \mathbb{Z}^m$ vérifiant $|\langle a_i, u \rangle| < \varepsilon_i$ pour $1 \leq i \leq r$. Il s'agit de vérifier que u est dans \mathcal{L} . Posons $\ell = u_1 \ell_1 + \dots + u_m \ell_m$ et $\alpha = \exp(\ell)$. Il est clair que le degré de α est au plus D . D'autre part, on a

$$\ell = \sum_{1 \leq j \leq m} u_j \ell_j = \sum_{1 \leq j \leq m} u_j \sum_{1 \leq i \leq r} a_{ij} \log \gamma_i = \sum_{1 \leq i \leq r} \langle a_i, u \rangle \log \gamma_i,$$

donc, après avoir choisi des déterminations quelconques des $\gamma_i^{\langle a_i, u \rangle}$, on voit qu'il existe une racine de l'unité ε telle que $\alpha = \varepsilon \prod_{1 \leq i \leq r} \gamma_i^{\langle a_i, u \rangle}$. Il en résulte (lemme 1) que

$$h(\alpha) \leq \sum_{1 \leq i \leq r} |\langle a_i, u \rangle| h(\gamma_i) \leq \sum_{1 \leq i \leq r} \varepsilon_i h(\gamma_i) \leq (10D)^{-3}$$

et

$$|\ell| \leq \sum_{1 \leq i \leq r} |\langle a_i, u \rangle| |\log \gamma_i| < \sum_{1 \leq i \leq r} \varepsilon_i |\log \gamma_i| \leq 10^{-3} D^{-2}.$$

Le lemme 2 montre alors que $\ell = 0$, c'est-à-dire que $\sum_{1 \leq i \leq r} \langle a_i, u \rangle \log \gamma_i = 0$. Comme les $\log \gamma_i$ sont \mathbb{Q} -linéairement indépendants, on a $\langle a_i, u \rangle = 0$ pour tout i , ce qui est le résultat cherché.

Le lemme 3 donne alors immédiatement la deuxième partie de la proposition. \square

Remarque. — La constante $(m - r + 1)^r$ qui apparaît sous forme de sa racine carrée dans la proposition provient de la majoration de $\det(A^t A)$ faite au lemme 3 par l'inégalité de Hadamard. Si $m - r$ est petit, on obtient une majoration plus fine en appliquant la formule de Lagrange (voir [Bo, p. 103] ou la section 1.2 de [G] où cette formule est appelée formule de Binet–Cauchy $\det(A^t A) = \sum_H A_H^2$ où H parcourt l'ensemble des parties à r éléments de l'ensemble des indices de colonnes et A_H est le déterminant formé des colonnes de A dont les indices sont dans H . On majore ensuite les A_H par l'inégalité de Hadamard. Ce procédé remplace

$$(m - r + 1)^r \quad \text{par} \quad 1 + \sum_{1 \leq k \leq \min(r, m-r)} \binom{m-r}{k} \binom{r}{k} k^k.$$

Cette modification permet d'obtenir une meilleure majoration que celle de D. Roy pour les petites valeurs de m et de $m - r$, par exemple pour $2 \leq m \leq 5$ et pour $m = 6$ et $r \neq 4$.

Bibliographie

- [B] BAKER (A.) . — *A sharpening of the bounds for linear forms in logarithms III*, Acta Arith. 27 (1975), pp. 247-252.
 [Berg] BERGER (M.) . — *Géométrie*, CEDIC/Fernand Nathan, Paris 1979.

Relations de dépendance linéaire entre des logarithmes de nombres algébriques

- [Be1] BERTRAND (D.) .— *Minimal heights and polarizations on Abelian varieties*, Preprint MSRI 06220-87, Berkeley (June 1987).
- [Be2] BERTRAND (D.) .— *Galois representations and transcendental numbers*, in *New Advances in Transcendence Theory* (ed. A. Baker), Cambridge Univ. Press, chap. 3 (1988), pp. 37-55.
- [Be3] BERTRAND (D.) .— *Minimal heights and polarizations on group varieties*, Prep. IHES 1993 et *Duke Math. J.*, **80** (1995), pp. 223-250.
- [Bij] BIJLSMA (A.) .— *Simultaneous approximations in transcendental number theory*, Acad. Proef. Amsterdam, Math. Centrum, 1978.
- [BijCij] BIJLSMA (A.) et CIJSOUW (P. L.) .— *Degree-free bounds for dependence relations*, *J. Australian. Math. Soc.*, série A, **31** (1981), pp. 496-507.
- [Bo] BOURBAKI (N.) .— *Algèbre Chapitre 3*, Hermann, Paris (1958).
- [C] CASSELS (J. W. S.) .— *An introduction to the geometry of numbers*, Springer-Verlag, Berlin - Göttingen - Heidelberg 1959.
- [G] GANTMACHER (F. R.) .— *The theory of matrices*, Chelsea, 1960; *Théorie des matrices*, Dunod, Paris, 1966.
- [GrL] GRUBER (P. M.) et LEKKERKERKER (C. G.) .— *Geometry of numbers*, Second edition, North-Holland, Amsterdam - New-York - Oxford - Tokyo, 1987.
- [L1] LANG (S.) .— *Fundamentals of Diophantine geometry*, Springer-Verlag, New-York - Berlin - Heidelberg - Tokyo, 1983.
- [L2] LANG (S.) .— *Number Theory III*, *Encycl. Math. Sci.*, **60**, Springer-Verlag, Berlin - Heidelberg - New-York, 1991.
- [Lo-vdP2] LOXTON (J. H.) et VAN DER POORTEN (A. J.) .— *Multiplicative dependence in number fields*, *Acta Arith.* **42** (1983), pp. 291-302.
- [M] MASSER (D. W.) .— *Linear relations on algebraic groups*, in *New Advances in Transcendence Theory* (ed. A. Baker), Cambridge Univ. Press, chap. 15 (1988), pp. 248-262.
- [Ma] MATVEEV (E. M.) .— *On linear and multiplicative relations*, *Math. Sbornik* **184**, n° 4 (1993), pp. 23-40; trad. angl. *Russian Acad. Sci. Sb. Math.* **78**, n° 2 (1994), pp. 411-425.
- [S] SIEGEL (C. L.) .— *Lectures on the Geometry of Numbers*, Springer-Verlag, Berlin - Heidelberg - New- York, 1989.
- [St] STARK (H. M.) .— *Further advances in the theory of linear forms in logarithms*, in *Diophantine Approximation and its Applications*, Academic Press, London 1973.
- [vdPLo1] VAN DER POORTEN (A. J.) et LOXTON (J. H.) .— *Multiplicative relations in number fields*, *Bull. Austral. Math. Soc.* **16** (1977), pp. 83-98; addenda and corrigenda, *id.* **17** (1977), pp. 151-155.
- [W1] WALDSCHMIDT (M.) .— *A lower bound for linear forms in logarithms*, *Acta Arith.* **37** (1980), pp. 257-283.
- [W2] WALDSCHMIDT (M.) .— *Linear independence of logarithms of algebraic numbers*, *Madras L. N.*, *IMSc Report* **116**, Madras 1992.