ANNALES DE L'INSTITUT FOURIER

MICHEL LAURENT
DAMIEN ROY

Sur l'approximation algébrique en degré de transcendance un

Annales de l'institut Fourier, tome 49, nº 1 (1999), p. 27-55
<http://www.numdam.org/item?id=AIF_1999__49_1_27_0>

Ann. Inst. Fourier, Grenoble
49, 1 (1999), 27-55

SUR L'APPROXIMATION ALGÉBRIQUE EN DEGRÉ DE TRANSCENDANCE UN

par M. LAURENT et D. ROY

1. Introduction et résultat principal.

Soit m un entier ≥ 1 et soit $\underline{\theta} = (\theta_1, \ldots, \theta_m)$ un m-uplet de nombres complexes. On suppose que le corps $\mathbb{Q}(\theta_1, \ldots, \theta_m)$ possède un degré de transcendance 1 sur $\mathbb{Q}$ ou, de manière équivalente, que le point $\underline{\theta}$ appartienne à une courbe affine $\mathcal{C}$ dans $\mathbb{C}^m$ définie sur $\mathbb{Q}$. Dans ce contexte, on s'intéresse à l'approximation de $\underline{\theta}$ par des m-uplets de nombres algébriques $\underline{\alpha} = (\alpha_1, \ldots, \alpha_m)$ appartenant à $\mathcal{C}$, de degré et de taille bornés.

On observe d'abord qu'il existe une constante $c > 0$ qui ne dépend que de la courbe $\mathcal{C}$ telle que, pour tout choix de paramètres réels d et t avec $t \gg d \gg 1$, il existe un point algébrique $\underline{\alpha} \in \mathcal{C}(\overline{\mathbb{Q}})$ de degré $d(\underline{\alpha}) \leq d$ et de taille $t(\underline{\alpha}) \leq t$ dont la distance à $\underline{\theta}$ pour la norme du maximum

$$\|\underline{\theta} - \underline{\alpha}\| := \max_{1 \leq \mu \leq m} |\theta_\mu - \alpha_\mu|$$

soit $\leq \exp\bigl(-c\bigl(dt(\underline{\alpha}) + td(\underline{\alpha})\bigr)\bigr)$. Nous l'avons établi dans un travail antérieur pour le cas $m = 1$ avec une constante c absolue (voir prop. 2 de [11]), et G. Diaz a raffiné notre résultat dans [6]. Le cas général s'en déduit par des arguments standards (voir §§5–6 ci-dessous, ou §2 c) de [18]), comme le lecteur pourra le vérifier.

Par contre, l'énoncé ci-dessus est faux si on exige que la distance de $\underline{\alpha}$ à $\underline{\theta}$ soit $\leq \exp(-cdt)$. On s'en convainc facilement dans le cas $m = 1$

Mots-clés : Approximation diophantienne – Indépendance algébrique.
Classification math. : 11J81 – 11J85.

en prenant pour θ un nombre transcendant arbitrairement voisin de 1 et en appliquant l'inégalité de Liouville. Pour contourner cette difficulté, nous nous donnons deux suites de majorants, $(d_n)_{n\geq 0}$ pour le degré et $(t_n)_{n\geq 0}$ pour la taille, avec des conditions de croissance qui seront indiquées plus bas. Sous ces conditions, nous montrons l'existence d'approximations $\underline{\alpha}$ vérifiant $\|\underline{\theta} - \underline{\alpha}\| \leq \exp(-cdt)$, non pas nécessairement pour chacun des couples $(d,t) = (d_n, t_n)$, mais au moins pour une infinité d'entre eux, avec une constante $c > 0$ explicite qui ne dépend que du degré de $\mathcal{C}$. De plus, pour une infinité d'indices n, nous pouvons minorer le degré de l'approximation algébrique $\underline{\alpha}$. Le cas particulier où l'on prend $d_n = n$ et $t_n = \kappa n$ avec une constante $\kappa \gg 1$ a été démontré par D. Roy et M. Waldschmidt avec une constante c non explicite (voir thm. 3.1 de [17]). Notre résultat principal contient ce cas particulier et démontre, tout en les précisant, les conjectures 5-5' de [10] et 1.7 de [18] dans le cas de la dimension 1. On trouvera dans l'article [10] par M. Laurent des motivations heuristiques à ces conjectures en degré de transcendance quelconque.

Des travaux récents (*cf.* [16], [17] et [18]) ont montré l'importance de ce type d'énoncé pour la théorie des nombres transcendants. Sans entrer dans ce sujet, nous tirerons trois corollaires de notre résultat principal. Le premier est essentiellement un résultat de E. Wirsing concernant l'approximation d'un nombre transcendant par des nombres algébriques de degré borné (voir [21]) avec, en information supplémentaire, une minoration du degré des approximants algébriques. Le second précise le théorème 3.2 de [17] en raffinant les constantes. Le dernier généralise au corps des fonctions sur une courbe algébrique le critère d'indépendance avec multiplicités de [11], avec des constantes explicites en fonction de la courbe.

Avant d'énoncer notre résultat principal, il convient de définir précisément les diverses notions de taille utilisées. Nous nous plaçons dans une situation affine. Pour tout m-uplet $\underline{\alpha} = (\alpha_1, \ldots, \alpha_m)$ de nombres algébriques engendrant sur $\mathbb{Q}$ un corps de nombres $\mathbb{K}$ de degré $d(\underline{\alpha})$, nous appellerons *mesure* du m-uplet $\underline{\alpha}$ la somme

$$\mu(\underline{\alpha}) := \sum_v [\mathbb{K}_v : \mathbb{Q}_v] \log \max \Big(1, |\alpha_1|_v, \ldots, |\alpha_m|_v\Big),$$

où v décrit l'ensemble des places de $\mathbb{K}$ et où les valeurs absolues $|.|_v$ désignent les extensions au complété $\mathbb{K}_v$ des normes usuelles sur $\mathbb{R}$ et $\mathbb{Q}_p$. En particulier lorsque $m = 1$, on a $\mu(\alpha) = \log M(\alpha)$ où $M(\alpha)$ désigne la *mesure de Mahler* du nombre α. Nous définissons alors la *taille* du m-uplet $\underline{\alpha}$ par la formule

$$t(\underline{\alpha}) := \max \Big\{\mu(\underline{\alpha}), (\log(m+1))d(\underline{\alpha})\Big\}.$$

L'expression "*courbe affine dans* $\mathbb{C}^m$ *définie sur* $\mathbb{Q}$" désigne pour nous un sous-ensemble algébrique de $\mathbb{C}^m$ de dimension 1 qui s'écrit comme l'ensemble des zéros d'un idéal premier de $\mathbb{Q}[X_1, \dots, X_m]$. Soit $\mathcal{C} \subseteq \mathbb{C}^m$ une telle courbe et soit $\overline{\mathcal{C}}$ son adhérence dans $\mathbb{P}^m$ pour la compactification naturelle $\mathbb{C}^m \subset \mathbb{P}^m(\mathbb{C})$. La *forme de Chow* de $\overline{\mathcal{C}}$, déterminée *a priori* à multiplication près par un scalaire, est un polynôme irréductible $f(\underline{u}, \underline{v}) \in \mathbb{Q}[\underline{u}, \underline{v}]$, séparément homogène de degré $\deg(\mathcal{C})$ en deux familles de variables $\underline{u} = (u_0, \dots, u_m)$ et $\underline{v} = (v_0, \dots, v_m)$, avec la propriété caractéristique que $f(\underline{a}, \underline{b}) = 0$ si et seulement si la sous-variété linéaire projective définie par $a_0X_0 + \cdots + a_mX_m = 0$ et $b_0X_0 + \cdots + b_mX_m = 0$ rencontre $\overline{\mathcal{C}}$. Normalisant f au signe près par les conditions $f \in \mathbb{Z}[\underline{u}, \underline{v}]$ et f primitif, nous définissons la *taille de la courbe* $\mathcal{C}$ par la formule

$$t(\mathcal{C}) := \max\Big\{ \log H(f), (\log(m+1)) \deg(\mathcal{C}) \Big\}$$

où $H(f)$ désigne la hauteur usuelle du polynôme f, c'est-à-dire le maximum des valeurs absolues de ses coefficients.

Le but de cette note est de démontrer le résultat suivant :

THÉORÈME 1. — *Soit $\mathcal{C}$ une courbe algébrique affine dans $\mathbb{C}^m$ définie sur $\mathbb{Q}$ et soit $\underline{\theta}$ un point de $\mathcal{C}$ n'appartenant pas à $\mathcal{C}(\overline{\mathbb{Q}})$. Soient a et b deux nombres réels ≥ 1, $(d_n)_{n\geq 0}$ et $(t_n)_{n\geq 0}$ deux suites croissantes (au sens large) de nombres réels positifs. On suppose que la suite $(t_n)_{n\geq 0}$ est non bornée et que pour tout $n \geq 0$ on a de plus*

$$d_n \geq c_0, \quad t_n \geq 8\frac{t(\mathcal{C})}{\deg(\mathcal{C})} d_n, \quad d_{n+1} \leq a d_n, \quad t_{n+1} \leq b t_n,$$

avec $c_0 = 26 \deg(\mathcal{C})$. Alors il existe une infinité d'indices n ayant la propriété suivante : pour chacun de ces n, il existe $\underline{\alpha} \in \mathcal{C}(\overline{\mathbb{Q}})$ vérifiant

$$c_1^{-1} d_n \leq d(\underline{\alpha}) \leq d_n, \quad t(\underline{\alpha}) \leq t_n, \quad \text{et} \quad \log \|\underline{\theta} - \underline{\alpha}\| \leq -c_2^{-1} d_n t_n,$$

avec

$$c_1 = 1200 \deg(\mathcal{C}) \max\{1, (ab)^2/4\} \quad \text{et} \quad c_2 = 1200 (\deg(\mathcal{C}))^2 \max\{1, (ab)^2/4\}.$$

Le plan de cet article est le suivant. Dans les paragraphes 2 à 4 nous examinons le cas particulier $m = 1$ de l'approximation d'un nombre complexe par des nombres algébriques. Le cas général s'en déduit aisément par projection linéaire sur un des axes de coordonnées (§5 et §6). Nous démontrons dans le §7 le critère d'indépendance algébrique avec multiplicités dont il a été question plus tôt. Le texte est complété par un appendice (§8) dans lequel nous avons regroupé les résultats de calcul différentiel utilisés. On y trouvera notamment une formule explicite donnant les coefficients de Taylor d'une fonction implicite.

2. Approximations algébriques d'un nombre complexe.

Nous examinons dans ce paragraphe le cas particulier où la courbe $\mathcal{C}$ est la droite affine $\mathbf{A}^1$, et nous en tirons deux corollaires. Les constantes numériques contenues dans le théorème 1 peuvent être raffinées dans le cas de la droite affine. L'énoncé obtenu se formule ainsi :

THÉORÈME 2. — *Soient θ un nombre complexe transcendant, a et b deux nombres réels ≥ 1, $(d_n)_{n\geq 0}$ une suite croissante (au sens large) d'entiers positifs, et $(t_n)_{n\geq 0}$ une suite croissante (au sens large) non bornée de nombres réels positifs. On suppose que pour tout $n \geq 0$ on a*

$$d_n \geq \gamma_0, \quad t_n \geq 2d_n, \quad d_{n+1} \leq ad_n, \quad t_{n+1} \leq bt_n,$$

avec $\gamma_0 = 26$. Alors il existe une infinité d'entiers $n \geq 0$ ayant la propriété suivante : pour chacun de ces n, il existe un nombre algébrique α vérifiant

$$\gamma_1^{-1} d_n \leq d(\alpha) \leq d_n \quad \mu(\alpha) \leq t_n \quad \text{et} \quad \log|\theta - \alpha| \leq -\gamma_2^{-1} d_n t_n$$

avec $\gamma_1 = 1000 \max\{1, (ab)^2/4\}$ et $\gamma_2 = 500 \max\{1, (ab)^2/4\}$.

Si nous fixons la suite $(d_n)_{n\geq 0}$ constante égale à d et posons $t_n = n$, $a = 1$, $b = 2$, nous retrouvons aux constantes près un énoncé d'approximation de E. Wirsing [21] avec en plus une minoration du degré des approximants algébriques.

COROLLAIRE 1. — *Soit θ un nombre complexe transcendant. Pour tout entier $d > 25$, il existe une infinité de nombres algébriques α qui vérifient*

$$0.001d \leq d(\alpha) \leq d \quad \text{et} \quad |\theta - \alpha| \leq M(\alpha)^{-0.002d}.$$

On notera que l'assertion du corollaire 1 reste vraie pour un nombre algébrique θ de degré $> d$. En effet, le lecteur vérifiera immédiatement que pour une suite constante égale à d, tous les ingrédients utilisés subsistent pourvu que le nombre complexe θ considéré ne soit pas un nombre algébrique de degré $\leq d$.

Désignons par $h(\alpha) := \mu(\alpha)/d(\alpha)$ la *hauteur logarithmique absolue* du nombre algébrique α. La minoration du degré $d(\alpha)$ permet de majorer immédiatement la hauteur $h(\alpha)$. On retrouve ainsi le théorème 3.2 de [17], avec des constantes meilleures :

COROLLAIRE 2. — *Soient θ un nombre complexe transcendant et κ un nombre réel ≥ 2000. Il existe une infinité de nombres algébriques α qui vérifient*

$$h(\alpha) \leq \kappa \quad et \quad \log|\theta - \alpha| \leq -2 \times 10^{-6}\kappa d(\alpha)^2.$$

Preuve. — On choisit

$$a = b = 4/3, \quad d_n = n, \quad t_n = \gamma_1^{-1}\kappa n.$$

On a $t_n \geq 2d_n$ lorsque $\kappa \geq 2\gamma_1 = 2000$. Le théorème 2 nous fournit alors pour une infinité d'indices n un nombre algébrique α avec

$$h(\alpha) = \frac{\mu(\alpha)}{d(\alpha)} \leq \frac{t_n}{\gamma_1^{-1}d_n} = \kappa$$

$$\log|\theta - \alpha| \leq -\gamma_2^{-1}d_n t_n = -(\gamma_1\gamma_2)^{-1}\kappa n^2 \leq -(\gamma_1\gamma_2)^{-1}\kappa d(\alpha)^2.$$

□

3. Les outils employés dans la preuve du théorème 2.

Commençons par une version du classique principe des tiroirs. Pour tout polynôme $P \in \mathbb{Z}[X]$, on désignera par $M(P) = \exp\int_0^1 \log|P(e^{2\pi i t})|dt$ sa mesure de Mahler et on notera $\mu(P) = \log M(P)$. Rappelons que si P est irréductible et si α est une racine de P, alors $M(P) = M(\alpha)$.

LEMME 1. — *Soit $\theta \in \mathbb{C}$ et soit $\beta \in \mathbb{R}$ avec $0 < \beta < 1/2$. Pour tout entier $d > 1/(1-2\beta)$, pour tout nombre réel $t \geq d$ suffisamment grand en fonction de β et de $|\theta|$, il existe un polynôme non nul $P \in \mathbb{Z}[X]$ qui vérifie*

$$\deg(P) \leq d, \quad \mu(P) \leq t \quad et \quad \log|P(\theta)| \leq -\beta dt.$$

Preuve. — Il s'agit du lemme 3.8 de [17] avec une minoration explicite de l'entier d. Reprenons brièvement l'argumentation. Soit m le plus petit entier $> 1/(1-2\beta)$, soit d un entier $\geq m$, et soit t un réel $\geq d$. On note ϵ le réel positif, fonction de β, tel que $1/m = 1 - 2(1+\epsilon)^2\beta$, et on désigne par H la partie entière de $e^t/\sqrt{d+1}$. En vertu du lemme de Thue-Siegel, il existe un polynôme non nul $P \in \mathbb{Z}[X]$, de degré $\leq d$ et de hauteur $H(P) \leq H$, tel que

$$|P(\theta)| \leq \sqrt{2}(1 + |\theta| + \cdots + |\theta|^d)H^{-(d-1)/2}.$$

Comme $M(P) \le \sqrt{d+1}H(P) \le e^t$, ce polynôme vérifie $\mu(P) \le t$. D'autre part, en choisissant t suffisamment grand en fonction de ϵ, β et $|\theta|$, on peut faire en sorte d'avoir

$$\sqrt{2}(1+|\theta|+\cdots+|\theta|^d) \le \exp(\epsilon\beta dt) \quad \text{et} \quad H \ge \frac{e^t}{\sqrt{t+1}} - 1 \ge \exp\Big(\frac{t}{1+\epsilon}\Big).$$

Comme $(d-1)/d \ge (m-1)/m = 2(1+\epsilon)^2\beta$, on obtient alors

$$\log|P(\theta)| \le \epsilon\beta dt - (d-1)t/(2(1+\epsilon)) \le -\beta dt,$$

comme requis. □

La seconde étape consiste à transformer le polynôme P fourni par le lemme 1. Suivant la terminologie de Choodnovsky (*cf.* [4] et [19]), on “colorie” en rouge ou en bleu le polynôme P selon que les propriétés (i) ou (ii) ci-dessous sont vérifiées, avec une coloration bleue si (i) et (ii) sont vrais.

LEMME 2. — *Soit $\theta \in \mathbb{C}$, soient β, d, t des nombres réels > 0 et soit P un polynôme non nul de $\mathbb{Z}[X]$ tels que*

$$\deg(P) \le d, \quad \mu(P) \le t \quad \text{et} \quad \log|P(\theta)| \le -\beta dt.$$

Alors au moins une des deux conditions suivantes est remplie :

(i) *il existe un facteur Q de P dans $\mathbb{Z}[X]$ qui est une puissance d'un polynôme irréductible de $\mathbb{Z}[X]$ et qui vérifie*

$$\deg(Q) \le d, \quad \mu(Q) \le t \quad \text{et} \quad \log|Q(\theta)| \le -\frac{2\beta}{3}dt\ ;$$

(ii) *il existe deux facteurs F et G de P dans $\mathbb{Z}[X]$ qui sont premiers entre eux et qui vérifient*

$$\deg(F) + \deg(G) \le d, \quad \mu(F) + \mu(G) \le t$$

et

$$\log\max\big\{|F(\theta)|, |G(\theta)|\big\} \le -\frac{\beta}{3}dt.$$

Preuve. — Écrivons $P = mQ_1\cdots Q_s$ où m est un entier, et où $Q_1,\ldots,Q_s$ sont des puissances de polynômes irréductibles de $\mathbb{Z}[X]$ de degré positif ordonnées de telle sorte que l'on ait

$$|Q_1(\theta)| \le \cdots \le |Q_s(\theta)|.$$

Si $|Q_1(\theta)| \le \exp\big(-(2/3)\beta dt\big)$, la condition (i) est remplie avec $Q = Q_1$. Sinon, on désigne par i un entier $\le s$ tel que

$$|Q_i(\theta)\cdots Q_s(\theta)| \le \exp\big(-(1/3)\beta dt\big)$$

et

$$|Q_{i+1}(\theta)\cdots Q_s(\theta)| > \exp\big(-(1/3)\beta dt\big),$$

avec la convention qu'un produit vide est égal à 1. Un tel indice i existe et est nécessairement ≥ 2 car

$$|Q_2(\theta)\cdots Q_s(\theta)| = |(P/mQ_1)(\theta)| \le \exp(-(1/3)\beta dt).$$

On pose $F = Q_1\cdots Q_{i-1}$ et $G = Q_i\cdots Q_s$. Alors, F et G remplissent la condition (ii). C'est clair en ce qui concerne le degré et la mesure de Mahler, ainsi que pour la majoration $|G(\theta)| \le \exp(-(1/3)\beta dt)$. La condition $|F(\theta)| \le \exp(-(1/3)\beta dt)$ est certainement remplie si $|Q_i(\theta)| \le \exp(-(1/3)\beta dt)$ car $|F(\theta)| \le |Q_i(\theta)|^{i-1}$. Si au contraire $|Q_i(\theta)| > \exp(-(1/3)\beta dt)$, il suffit d'écrire $F = P/m(Q_i(Q_{i+1}\cdots Q_s))$. □

Le troisième ingrédient est un résultat d'approximation ayant pour origine les travaux de Wirsing [21]. Nous en utiliserons la version suivante qui reprend une partie du lemme 3.10 de [17].

LEMME 3. — *Soient d un entier et γ, t des nombres réels avec*

$$0 < \gamma < 1/4 \quad \textit{et} \quad t \ge d \ge 1.$$

Soit θ un nombre complexe. Supposons qu'il existe des polynômes $F, G \in \mathbb{Z}[X]$ premiers entre eux, vérifiant

$$\deg(F) \le d, \quad \mu(F) \le t \quad \textit{et} \quad \log|F(\theta)| \le -\gamma dt$$
$$\deg(G) \le d, \quad \mu(G) \le t \quad \textit{et} \quad \log|G(\theta)| \le -\gamma dt.$$

Alors, il existe un nombre algébrique α tel que

$$(FG)(\alpha) = 0 \quad \textit{et} \quad \log|\theta - \alpha| \le -\frac{\gamma^2}{3}dt.$$

Le résultat suivant est le point clé de notre argumentation. Il raffine le lemme 3 en ce sens qu'il fournit une minoration du degré de l'approximation α. L'idée sous-jacente de sa démonstration peut s'exprimer ainsi. Par combinaison linéaire $aF + bG$ à coefficients entiers, le lemme 3 permet de construire de nombreuses approximations algébriques de θ. Une combinaison linéaire générique est irréductible sur $\mathbb{Z}$ et l'on peut espérer qu'il en est de même pour des petits coefficients entiers a et b. En pratique, nous procéderons différemment en utilisant l'inégalité de Liouville.

LEMME 4. — *Soient d un entier et t, ϵ des nombres réels avec*

$$0 < \epsilon < 1/2, \quad t \geq d \geq 7 \quad \text{et} \quad dt \geq 70/\epsilon^2.$$

Soit θ un nombre complexe. Supposons qu'il existe des polynômes $F, G \in \mathbb{Z}[X]$ premiers entre eux, vérifiant

$$\deg(F) \leq d, \quad \mu(F) \leq t \quad \text{et} \quad \log|F(\theta)| \leq -\epsilon dt$$
$$\deg(G) \leq d, \quad \mu(G) \leq t \quad \text{et} \quad \log|G(\theta)| \leq -\epsilon dt.$$

Alors, il existe un nombre algébrique α qui est racine d'un des polynômes F, G ou $F+G$ ayant les propriétés

$$0.04\epsilon^2 d \leq d(\alpha) \leq d, \quad \mu(\alpha) \leq 2t \quad \text{et} \quad \log|\theta - \alpha| \leq -0.16\epsilon^2 dt.$$

Preuve. — Posons $P_1 = F$, $P_2 = G$ et $P_3 = F + G$. Montrons tout d'abord que l'on a

$$\deg(P_i) \leq d, \quad \mu(P_i) \leq 2t \quad \text{et} \quad \log|P_i(\theta)| \leq -2\gamma dt, \quad (i = 1, 2, 3),$$

avec $\gamma = 0.49\epsilon$. C'est bien clair par hypothèse pour $i = 1, 2$. Comme $d \geq 7$, on a

$$\begin{aligned}\mu(F+G) &\leq \log(d+1) + \max\{\log H(F), \log H(G)\}\\ &\leq \log(d+1) + d(\log 2) + t \leq 2t,\end{aligned}$$

et puisque $\epsilon dt \geq 70/\epsilon \geq 140$, on a aussi

$$\log|(F+G)(\theta)| \leq (\log 2) - \epsilon dt \leq -0.98\,\epsilon dt = -2\gamma dt.$$

Nous allons maintenant utiliser deux fois le lemme 3 avec t remplacé par $2t$. Remarquons que les polynômes P_1, P_2, P_3 sont premiers entre eux deux à deux. Une première application au couple de polynômes (P_1, P_2) nous fournit un nombre α_1 racine de P_1P_2 tel que

$$d(\alpha_1) \leq d, \quad \mu(\alpha_1) \leq 2t \quad \text{et} \quad \log|\theta - \alpha_1| \leq -\frac{\gamma^2}{3} d(2t) \leq -0.16\epsilon^2 dt.$$

Supposons par exemple que $P_1(\alpha_1) = 0$. On applique alors le lemme 3 au couple (P_2, P_3) d'où un deuxième nombre algébrique α_2 racine de P_2P_3 ayant les mêmes propriétés d'approximation :

$$d(\alpha_2) \leq d, \quad \mu(\alpha_2) \leq 2t \quad \text{et} \quad \log|\theta - \alpha_2| \leq -0.16\epsilon^2 dt.$$

Les nombres α_1 et α_2 sont nécessairement distincts puisque $P_1(\alpha_1) = P_2P_3(\alpha_2) = 0$ et que les polynômes P_1 et P_2P_3 sont premiers entre eux.

Dans l'autre alternative où $P_2(\alpha_1) = 0$, on choisit plutôt le couple (P_1, P_3). On a donc construit deux approximations distinctes α_1 et α_2 de θ. Nous allons montrer qu'au moins l'un de ces deux nombres algébriques possèdent les propriétés énoncées dans le lemme 4. Il nous reste uniquement à vérifier que $\delta := \max\{d(\alpha_1), d(\alpha_2)\} \geq 0.04\epsilon^2 d$. On observe d'abord que α_1 étant racine de F ou de G, on a $\mu(\alpha_1) \leq t$. Comme $\delta \leq d \leq t$, l'inégalité de Liouville (*cf.* lemme 3.14 de [20]) s'écrit

$$\begin{aligned}\log|\alpha_1 - \alpha_2| &\geq -[\mathbb{Q}(\alpha_1 - \alpha_2) : \mathbb{Q}]h(\alpha_1 - \alpha_2)\\ &\geq -[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]\big((\log 2) + h(\alpha_1) + h(\alpha_2)\big)\\ &\geq -\delta^2(\log 2) - d(\alpha_2)\mu(\alpha_1) - d(\alpha_1)\mu(\alpha_2)\\ &\geq -\delta^2 \log 2 - 3\delta t \geq -3.7\delta t.\end{aligned}$$

D'autre part comme $|\alpha_1 - \alpha_2|$ est majoré par la somme des distances de θ à α_1 et α_2, on a aussi

$$\log|\alpha_1 - \alpha_2| \leq \log 2 - 0.16\epsilon^2 dt \leq -0.15\epsilon^2 dt,$$

puisque $\epsilon^2 dt \geq 70$. Par comparaison de la majoration et de la minoration, il vient

$$\delta \geq \frac{0.15}{3.7}\epsilon^2 d \geq 0.04\epsilon^2 d. \qquad \square$$

4. Preuve du théorème 2.

La démonstration du théorème 2 utilise les mêmes étapes que celle du classique critère de Gel'fond [2], à ceci près que la suite de polynômes de valeur absolue petite en θ n'est pas une donnée initiale mais est construite par le principe des tiroirs.

Posons $\beta = 0.48$. Pourvu que l'indice n soit suffisamment grand, l'entier $d = d_n \geq 26$ et le réel $t = t_n/2$ satisfont les conditions du lemme 1, d'où la construction d'un polynôme P_n. Nous appliquons alors le lemme 2 à ce polynôme P_n pour les valeurs de β, d et t que l'on vient d'indiquer. Supposons d'abord que la condition (ii) du lemme 2 soit remplie. Les hypothèses du lemme 4 étant alors satisfaites avec $\epsilon = \beta/3 = 0.16$, il existe, si n est assez grand, un nombre algébrique α qui vérifie

$$\frac{1}{1000}d_n \leq d(\alpha) \leq d_n, \quad \mu(\alpha) \leq t_n$$

et

$$\log|\theta - \alpha| \leq -0.16\epsilon^2 d_n(t_n/2) \leq -\frac{1}{500}d_n t_n.$$

Le théorème est donc vérifié si cette situation se présente pour une infinité d'entiers n. Supposons au contraire qu'il existe un entier $n_0 \geq 0$ tel que la condition (ii) du lemme 3 ne soit pas remplie quel que soit $n \geq n_0$. Pour chaque $n \geq n_0$, il existe donc un polynôme $Q_n \in \mathbb{Z}[X]$ qui est une puissance d'un polynôme irréductible et qui vérifie

$$\deg(Q_n) \leq d_n, \quad \mu(Q_n) \leq t_n/2$$

et

$$\log|Q_n(\theta)| \leq -(2\beta/3)d_n(t_n/2) = -0.16\, d_n t_n.$$

Choisissons un entier $m \geq n_0$ arbitrairement grand. Si, pour un indice $n \geq m$, le polynôme Q_n n'est pas premier à Q_m, alors Q_n et Q_m sont deux puissances d'un même polynôme irréductible de $\mathbb{Z}[X]$. On a alors

$$\frac{\log|Q_m(\theta)|}{\deg(Q_m)} = \frac{\log|Q_n(\theta)|}{\deg(Q_n)} \leq -0.16\, t_n.$$

Comme t_n tend vers l'infini avec n et que $Q_m(\theta) \neq 0$ car θ est transcendant, cette inégalité ne peut tenir que pour un nombre fini d'indices n. Soit n le plus petit entier $\geq m$ pour lequel Q_m et Q_n sont premiers entre eux. Alors les polynômes $F = Q_{n-1}$ et $G = Q_n$ sont premiers entre eux, et le lemme 4 s'applique avec $d = d_n$, $t = t_n/2$ et $\epsilon = 0.32(ab)^{-1}$. Il assure l'existence d'un nombre algébrique α qui vérifie

$$\frac{d_n}{250(ab)^2} \leq d(\alpha) \leq d_n, \quad \mu(\alpha) \leq t_n$$

et

$$\log|\theta - \alpha| \leq -0.16\epsilon^2 d_n \frac{t_n}{2} \leq -\frac{d_n t_n}{125(ab)^2},$$

comme requis. □

Remarque. — Le lemme 4 permet, dans certains cas, de donner explicitement des équations pour les bonnes approximations que prédit le théorème 2. Considérons par exemple un nombre θ de la forme

$$\theta = \sum_{i=0}^{\infty} 2^{-\varphi(i)}$$

où $\varphi : \mathbb{N} \to \mathbb{N}$ est une fonction qui vérifie $\varphi(0) > 1$ et $\varphi(i+1) \geq \varphi(i)^2$ pour $i \geq 0$. Pour tout entier $k \geq 0$, on pose

$$\theta_k = \sum_{i=0}^{k} 2^{-\varphi(i)} \in \mathbb{Q} \quad \text{et} \quad L_k = 2^{\varphi(k)}(X - \theta_k) \in \mathbb{Z}[X].$$

Le nombre θ_k est, par construction, une bonne approximation rationnelle de θ, et L_k est son polynôme minimal sur $\mathbb{Z}$. On vérifie aisément que

$$\deg(L_k) = 1, \quad \mu(L_k) = \varphi(k)\log 2 \quad \text{et} \quad |\theta - \theta_k| \geq \exp(-\varphi(k+1)).$$

Par ailleurs, si $k \geq 1$, on a $\varphi(k) \geq 4$ et, comme $\varphi(k+1) \geq \varphi(k)^2$, on obtient

$$\log|L_k(\theta)| \leq -(\varphi(k+1) - \varphi(k) - 1)\log 2 \leq -\varphi(k+1)/3.$$

Donnons-nous aussi des nombres réels $a, b \geq 1$ et des suites $(d_n)_{n\geq 0}$ et $(t_n)_{n\geq 0}$ comme dans l'énoncé du théorème, mais avec la contrainte

$$9b \leq d_n \leq \sqrt{t_n}$$

en remplacement de $t_n \geq 2d_n$ et de $d_n \geq \gamma_0$. Pour tout entier k tel que $\varphi(k) \geq t_0$, il existe un entier $n \geq 1$ tel que

$$t_n/b \leq \varphi(k) \leq t_n.$$

Posons $F = (L_{k-1})^{d_n}$ et $G = L_k$. Alors, F et G sont deux polynômes de $\mathbb{Z}[X]$ premiers entre eux avec

$$\begin{aligned}
&\deg(F) = d_n,\\
&\mu(F) = d_n\varphi(k-1)\log 2 \leq d_n\sqrt{t_n} \leq t_n,\\
&\log|F(\theta)| \leq -\frac{1}{3}d_n\varphi(k) \leq -\frac{1}{3b}d_n t_n,\\
&\deg(G) = 1 \leq d_n,\\
&\mu(G) = \varphi(k)\log 2 \leq t_n,\\
&\log|G(\theta)| \leq -\frac{1}{3}\varphi(k+1) \leq -\frac{1}{3}\varphi(k)^2 \leq -\frac{1}{3b^2}t_n^2 \leq -\frac{1}{3b}d_n t_n.
\end{aligned}$$

Le lemme 4 s'applique donc avec $\epsilon = 1/(3b)$, et montre qu'il existe une racine α de F, G ou $F+G$ qui vérifie

$$\frac{1}{225\,b^2}d_n \leq d(\alpha) \leq d_n, \quad \mu(\alpha) \leq 2t_n \quad \text{et} \quad \log|\theta - \alpha| \leq -\frac{1}{60\,b^2}d_n t_n.$$

Si $d_n > 60\,b^2$, ce nombre α n'est pas une racine de F car $|\theta - \theta_k| \geq \exp(-\varphi(k)) \geq \exp(-t_n)$. De plus, si $d_n > 225\,b^2$, on a $\alpha \notin \mathbb{Q}$, donc $G(\alpha) \neq 0$. Dans ce cas, α est nécessairement une racine de $F+G$. En variant l'entier k, on obtient une infinité d'approximations de θ avec les propriétés souhaitées.

5. Préliminaires sur les hauteurs.

Nous aurons besoin de majorer la hauteur des points d'intersection d'une courbe et d'une hypersurface projective. L'estimation obtenue est un cas très particulier de résultats généraux sur la théorie de l'intersection arithmétique qui se retrouvent dans [1] et [15]. Comme nos normalisations sont bien différentes de celles de ces deux références, nous avons trouvé plus simple de nous ramener aux résultats de [14]. Il nous faut tout de même établir d'abord deux lemmes.

On note $L(P)$ la *longueur* d'un polynôme $P \in \mathbb{C}[T_1, \ldots, T_n]$ en n variables, c'est-à-dire la somme des valeurs absolues de ses coefficients, et on désigne par $M(P)$ sa mesure de Mahler

$$M(P) = \exp\left\{\int_0^1 \cdots \int_0^1 \log\left|P(e(t_1), \ldots, e(t_n))\right| \mathrm{d}\underline{t}\right\},$$

où $e(t) = \exp(2\pi i t)$. On montre d'abord :

LEMME 5. — *Soient k et n des entiers avec $1 \leq k \leq n$, soit $F \in \mathbb{C}[T_1, \ldots, T_n]$, et soit $(q_1, \ldots, q_k)$ un point de $\mathbb{C}^k$. Supposons que F soit homogène de degré δ en $(T_1, \ldots, T_k)$, et posons*

$$G = F(q_1, \ldots, q_k, T_{k+1}, \ldots, T_n).$$

Alors, on a

$$M(G) \leq \Big(\sum_{i=1}^{k} |q_i|\Big)^{\delta} M(F).$$

Preuve. — Supposons d'abord $k = n$, et écrivons $F = \sum p_{\underline{a}}\, T_1^{a_1} \cdots T_n^{a_n}$. Pour tout $\underline{a} \in \mathbb{N}^n$ de longueur $|\underline{a}| := a_1 + \cdots + a_n = \delta$, le lemme 1.13 de [14] donne

$$|p_{\underline{a}}| \leq \binom{\delta}{\underline{a}} M(F) \quad \text{où} \quad \binom{\delta}{\underline{a}} = \frac{\delta!}{a_1! \cdots a_n!}.$$

Cela implique

$$|F(\underline{q})| \leq \sum \binom{\delta}{\underline{a}} M(F) |q_1|^{a_1} \cdots |q_n|^{a_n} = \Big(\sum_{i=1}^{n} |q_i|\Big)^{\delta} M(F).$$

Dans le cas général, pour $y_{k+1}, \ldots, y_n \in \mathbb{C}$ fixes, on en déduit

$$|G(y_{k+1}, \ldots, y_n)| \leq \left(\sum_{i=1}^{k} |q_i|\right)^{\delta} \exp\left\{\int_0^1 \cdots \int_0^1 \log\left|F(e(t_1), \ldots e(t_k), y_{k+1}, \ldots, y_n)\right| \mathrm{d}t_1 \cdots \mathrm{d}t_k\right\}.$$

On conclut en intégrant le logarithme des deux membres sur le polydisque $|y_{k+1}| = \cdots = |y_n| = 1$. □

LEMME 6. — *Soient $u_0, \dots, u_m$ des indéterminées, soit $\underline{\alpha} = (\alpha_1, \dots, \alpha_m)$ un point de $\overline{\mathbb{Q}}^m$ et soit S l'ensemble des plongements de $\mathbb{Q}(\underline{\alpha})$ dans $\mathbb{C}$. On pose*

$$g = a \prod_{\sigma \in S} (u_0 + u_1\sigma(\alpha_1) + \cdots + u_m\sigma(\alpha_m)) \tag{1}$$

où a désigne le plus petit entier positif tel que $g \in \mathbb{Z}[\underline{u}]$. Alors, on a

$$\mu(\underline{\alpha}) \le \log M(g).$$

Preuve. — En effet, pour tout nombre premier rationnel p, on a

$$\sum_{v|p} [\mathbb{K}_v : \mathbb{Q}_p] \log \max\Big(1, |\alpha_1|_v, \dots, |\alpha_m|_v\Big) = -\log|a|_p.$$

Pour la place à l'infini, on utilise le fait que la hauteur d'une forme linéaire est majorée par sa mesure de Mahler, comme le montre la formule (3) de [12] (ou le lemme 1.13 de [14]). On trouve ainsi

$$\begin{aligned}
\sum_{v|\infty} [\mathbb{K}_v : \mathbb{R}] \log \max\Big(1, |\alpha_1|_v, \dots, |\alpha_m|_v\Big) \\
&= \sum_{\sigma\in S} \log H(u_0 + u_1\sigma(\alpha_1) + \cdots + u_m\sigma(\alpha_m)) \\
&\le \sum_{\sigma\in S} \log M(u_0 + u_1\sigma(\alpha_1) + \cdots + u_m\sigma(\alpha_m)) \\
&= -\log|a| + \log M(g).
\end{aligned}$$

On conclut grâce à la formule du produit. □

Voici donc l'estimation dont nous aurons besoin :

LEMME 7. — *Soit $\mathcal{C}$ une courbe algébrique affine dans $\mathbb{C}^m$ définie sur $\mathbb{Q}$, soit d un entier positif, soit $Q \in \mathbb{Z}[X_1, \dots, X_m]$ un polynôme de degré $\le d$ qui ne s'annule pas identiquement sur $\mathcal{C}$, et soit $\underline{\alpha}$ un point de $\mathcal{C}(\overline{\mathbb{Q}})$ tel que $Q(\underline{\alpha}) = 0$. Alors, en désignant par f la forme de Chow de $\overline{\mathcal{C}}$ (définie au §1) et en posant $\delta = \deg(\mathcal{C})$, on a*

$$d(\underline{\alpha}) \le d\delta \quad \text{et} \quad \mu(\underline{\alpha}) \le 2d\delta\log(m+1) + \delta\log L(Q) + d\log H(f).$$

Preuve. — Il n'y a pas de restriction à supposer $d = \deg(Q)$. Soit $I \subset \mathbb{Q}[X_1, \dots, X_m]$ l'idéal de définition de $\mathcal{C}$. On désigne par ${}^hQ \in \mathbb{Z}[X_0, \dots, X_m]$ l'homogénéisé de Q, par ${}^hI \subset \mathbb{Q}[X_0, \dots, X_m]$ celui de I

et, au sens de P. Philippon dans [14], on note F une forme éliminante d'indice $(d,1)$ de ${}^hI$ choisie à coefficients entiers et primitive. En désignant par $\underline{q}$ le vecteur des coefficients de ${}^hQ$ et par $\underline{u} = (u_0, \dots, u_m)$ le vecteur des coefficients d'une forme linéaire générique $L = u_0X_0 + \cdots + u_mX_m$, on pose

$$G = F(\underline{q}, \underline{u}) \in \mathbb{Z}[\underline{u}].$$

Puisque ${}^hQ \notin {}^hI$ et que ${}^hI$ est un idéal premier, la proposition 2.4 de [14] montre que l'ensemble des zéros de $({}^hI, {}^hQ)$ dans $\mathbb{P}^m(\mathbb{C})$ est fini et que G est un produit de puissances des formes de Chow des idéaux premiers homogènes de $\mathbb{Q}[X_0, \dots, X_m]$ qui définissent ces zéros. Chaque zéro de $({}^hI, {}^hQ)$ dans $\mathbb{P}^m(\mathbb{C})$ est représenté par un élément $\underline{\beta} = (\beta_0, \dots, \beta_m)$ de $\overline{\mathbb{Q}}^{m+1}$ dont au moins une coordonnée est égale à 1. Avec cette normalisation, la forme de Chow correspondante h s'écrit $h = b\prod_\sigma L(\sigma(\underline{\beta}))$ où b est un entier et où le produit porte sur tous les plongements de $\mathbb{Q}(\underline{\beta})$ dans $\mathbb{C}$. En particulier, le polynôme g défini au lemme 6 est la forme de Chow de l'idéal premier homogène qui définit le point $(1, \alpha_1, \dots, \alpha_m)$. Donc, G est divisible par g dans $\mathbb{Z}[\underline{u}]$. Le lemme 6 donne $\log M(g) \geq \mu(\underline{\alpha})$ et, en général, $\log M(h) \geq \mu(\underline{\beta})$ pour h et $\underline{\beta}$ comme ci-dessus. Les facteurs irréductibles h de G vérifient donc tous $M(h) \geq 1$. Comme g est de degré $d(\underline{\alpha})$, on obtient ainsi

$$d(\underline{\alpha}) \leq \deg(G) \quad \text{et} \quad \mu(\underline{\alpha}) \leq \log M(g) \leq \log M(G).$$

Le lemme 5 donne

$$M(G) \leq L(Q)^\delta M(F).$$

D'autre part, le lemme 2.8 de [14] permet de comparer $M(F)$ et $M(f)$. Plus précisément, puisque f est une forme éliminante d'indice $(1,1)$ de ${}^hI$, l'argument de récurrence dans la démonstration de ce lemme (voir ligne 2, page 37 de [14]) donne

$$M(F) \leq (m+1)^{d\delta} M(f)^d.$$

Comme la mesure de Mahler d'un polynôme est majorée par sa norme ℓ_2, on trouve aussi

$$M(f) \leq (m+1)^\delta H(f).$$

En combinant les inégalités précédentes et en tenant compte du fait que le degré de G est $d\delta$ (voir la remarque 1, page 15 de [14]), on obtient les majorations annoncées de $d(\underline{\alpha})$ et $\mu(\underline{\alpha})$. Notons toutefois que la majoration de $d(\underline{\alpha})$ découle plus simplement du théorème de Bézout usuel. □

6. Preuve du théorème 1.

Nous sommes maintenant en mesure de déduire le théorème 1 du théorème 2. On peut supposer que la coordonnée θ_1 de $\underline{\theta}$ est un nombre complexe transcendant. Comme $\underline{\theta}$ est un point non singulier de $\mathcal{C}$, la projection $\pi: \mathcal{C} \to \mathbf{A}^1$ définie par $\pi(x_1, \ldots, x_m) = x_1$ constitue alors un isomorphisme local de variétés complexes au voisinage du point $\underline{\theta}$ (cor. 1.26 de [13]). Il existe donc un isomorphisme analytique $\varphi: \mathcal{U} \to \mathcal{V}$ d'un voisinage ouvert $\mathcal{U}$ de θ_1 dans $\mathbb{C}$ dans un voisinage ouvert $\mathcal{V}$ de $\underline{\theta}$ dans $\mathcal{C}(\mathbb{C})$ qui vérifie $\varphi(\theta_1) = \underline{\theta}$ et $\pi \circ \varphi(z) = z$ pour tout $z \in \mathcal{U}$. En particulier, en prenant $\mathcal{V}$ borné, il existe une constante c telle que

$$\log \|\varphi(z) - \underline{\theta}\| \leq \log |z - \theta_1| + c$$

pour tout $z \in \mathcal{U}$. On observe aussi que φ applique $\overline{\mathbb{Q}} \cap \mathcal{U}$ dans $\mathcal{C}(\overline{\mathbb{Q}})$ car, l'idéal de définition de $\mathcal{C}$ dans $\mathbb{Q}[X_1, \ldots, X_m]$ étant premier, tout point de $\mathcal{C}$ qui n'est pas algébrique est $\mathbb{Q}$-générique et par suite sa première coordonnée est transcendante tout comme celle de $\underline{\theta}$.

Pour simplifier l'écriture, on pose $\delta = \deg(\mathcal{C})$ et $\tau = t(\mathcal{C})$. Soit alors

$$d'_n = \left[\frac{d_n}{\delta}\right], \quad t'_n = \frac{t_n}{2\delta}, \quad a' = (1.05)a, \quad b' = b.$$

Sous les hypothèses du théorème 1, il est clair que l'on a l'encadrement

$$(0.96)\frac{d_n}{\delta} \leq d'_n \leq \frac{d_n}{\delta}.$$

Le théorème 2 appliqué au nombre complexe θ_1 avec les données d'_n, t'_n, a' et b', nous fournit pour une infinité d'indices n une approximation algébrique α_1 de θ_1 vérifiant les propriétés

$$c_1^{-1} d_n \leq \gamma_1^{-1} d'_n \leq d(\alpha_1) \leq d'_n, \quad \mu(\alpha_1) \leq t'_n,$$
$$\log |\theta_1 - \alpha_1| \leq -\gamma_2^{-1} d'_n t'_n \leq -(c'_2)^{-1} d_n t_n,$$

avec $c'_2 = 2 \times (0.96)^{-1} \gamma_2 \delta^2 < c_2$.

Supposons que t_n soit suffisamment grand pour que $\alpha_1 \in \mathcal{U}$. Soit alors $\underline{\alpha} = \varphi(\alpha_1)$ et soit $Q \in \mathbb{Z}[X_1]$ le polynôme minimal de α_1. Le lemme 7 nous donne les majorations

$$d(\underline{\alpha}) \leq d'_n \delta \leq d_n, \quad \mu(\underline{\alpha}) \leq 2(\log(m+1)) d'_n \delta + \delta \log L(Q) + d'_n \log H(f).$$

L'inégalité (4) de [12] livre

$$\log L(Q) \leq \mu(\alpha_1) + d(\alpha_1) \log 2 \leq t'_n + d'_n \log 2 \leq \frac{t_n}{2\delta} + \frac{d_n}{\delta} \log(m+1),$$

d'où il s'ensuit que

$$\begin{aligned}\mu(\underline{\alpha}) &\leq 3d_n \log(m+1) + \frac{t_n}{2} + \frac{d_n}{\delta}\log H(f)\\ &\leq 4d_n \max\left\{\frac{\log H(f)}{\delta}, \log(m+1)\right\} + \frac{t_n}{2} = 4d_n\frac{\tau}{\delta} + \frac{t_n}{2} \leq t_n.\end{aligned}$$

Comme $t(\underline{\alpha}) = \max\left\{\mu(\underline{\alpha}), (\log(m+1))d(\underline{\alpha})\right\}$, la majoration $t(\underline{\alpha}) \leq t_n$ est alors automatiquement vérifiée. Récapitulant les estimations obtenues et tenant compte de l'inégalité $c_2' < c_2$, il vient

$$c_1^{-1}d_n \leq d(\alpha_1) \leq d(\underline{\alpha}) \leq d_n, \quad t(\underline{\alpha}) \leq t_n,$$

et

$$\log \|\underline{\theta} - \underline{\alpha}\| \leq \log|\theta_1 - \alpha_1| + c \leq -(c_2')^{-1}d_nt_n + c \leq -c_2^{-1}d_nt_n,$$

pourvu que t_n soit suffisamment grand. Le théorème 1 est donc établi.

7. Un critère d'indépendance algébrique.

On se propose de déduire du théorème 1 un critère d'indépendance algébrique en degré de transcendance 1. Il s'agit de généraliser le critère bien connu de Gel'fond pour le corps des fonctions rationnelles $\mathbb{Q}(\mathcal{C})$ de la courbe $\mathcal{C}$ en tenant compte non seulement des valeurs des fonctions au point $\underline{\theta}$ mais aussi de celles de leurs dérivées. Nous avons déjà établi dans [11] un tel critère pour la droite affine $\mathbf{A}^1$ à partir d'une autre extension du théorème de Wirsing mentionné ci-dessus. Le fait de disposer d'une minoration du degré des approximations algébriques simplifie notablement la démonstration. Le théorème 1 étant un énoncé d'approximation sur une courbe affine $\mathcal{C}$, notre critère est directement utilisable dans une démonstration d'indépendance algébrique sans avoir à introduire une base de transcendance du corps $\mathbb{Q}(\underline{\theta})$ (*cf.* §9.2 de [11]).

Désignons par $\partial : \mathbb{Q}(\mathcal{C}) \to \mathbb{Q}(\mathcal{C})$ une dérivation non triviale du corps des fonctions rationnelles de la courbe $\mathcal{C}$. Pour tout entier $s \geq 1$, on notera $\partial^{[s]} = \partial^s/s!$ le quotient par $s!$ du s-ième itéré de ∂. Si Q est une fraction rationnelle dans $\mathbb{Q}(X_1, \ldots, X_m)$, on désignera encore par le même symbole Q sa restriction à $\mathcal{C}$.

COROLLAIRE 3. — *Soit $\mathcal{C}$ une courbe algébrique affine dans $\mathbb{C}^m$ définie sur $\mathbb{Q}$ et soit $\underline{\theta}$ un point de $\mathcal{C}$ n'appartenant pas à $\mathcal{C}(\overline{\mathbb{Q}})$. Soient a,*

b deux nombres réels ≥ 1, $(s_n)_{n\in\mathbb{N}}$ une suite d'entiers positifs, $(t_n)_{n\in\mathbb{N}}$ et $(d_n)_{n\in\mathbb{N}}$ deux suites à valeurs réelles positives, telles que

$$7m\deg(\mathcal{C}) \leq \frac{d_n}{s_n} \leq \frac{d_{n+1}}{s_{n+1}} \leq a\frac{d_n}{s_n}, \quad \frac{t_n}{s_n} \leq \frac{t_{n+1}}{s_{n+1}} \leq b\frac{t_n}{s_n},$$

et

$$t_n \geq 8\frac{t(\mathcal{C})}{\deg(\mathcal{C})}d_n$$

pour tout $n \geq 0$. On suppose de plus que la suite t_n/s_n tend vers l'infini avec n. Alors, il n'existe pas de suite $(Q_n)_{n\in\mathbb{N}}$ de polynômes de $\mathbb{Z}[X_1,\dots,X_m]$ non identiquement nuls sur $\mathcal{C}$ et vérifiant

$$\deg(Q_n) \leq d_n, \quad \log H(Q_n) \leq t_n,$$

et

$$\log \max_{0\leq\sigma<s_n} \left|\partial^{[\sigma]}Q_n(\underline{\theta})\right| \leq -cd_nt_n/s_n$$

avec $c = 9300(\deg(\mathcal{C}))^2\max\{1,(ab)^2/4\}$, pour tout entier n à partir d'un certain rang.

Il n'y a pas de restriction à supposer que θ_1 est un nombre transcendant. On se donne alors, comme au §6, une fonction holomorphe $\varphi: \mathcal{U} \to \mathcal{V} \subset \mathcal{C}(\mathbb{C})$ qui constitue un inverse local à la projection sur la première coordonnée au voisinage du point $\underline{\theta}$. On note aussi ∂_1 la dérivation de $\mathbb{Q}(\mathcal{C})$ pour laquelle $\partial_1 X_1 = 1$. On utilisera deux représentations de ∂_1.

D'un point de vue analytique, on a, pour tout $Q \in \mathbb{Q}(\mathcal{C})$,

$$(\partial_1 Q)(\varphi(z)) = \frac{\mathrm{d}}{\mathrm{d}z}(Q\circ\varphi)(z), \quad (z\in\mathcal{U}).$$

Par récurrence sur s, on en déduit

$$(\partial_1^s Q)(\varphi(z)) = \frac{\mathrm{d}^s}{\mathrm{d}z^s}(Q\circ\varphi)(z), \quad (z\in\mathcal{U}),$$

pour tout entier $s \geq 1$. En particulier, si on pose $g = Q\circ\varphi$, alors pour tout point $\underline{\alpha} = (\alpha_1,\dots,\alpha_m) \in \mathcal{V}$, on a

$$(\partial_1^{[s]}Q)(\underline{\alpha}) = g^{[s]}(\alpha_1)$$

où $g^{[s]}$ désigne la fonction $(s!)^{-1}(\mathrm{d}^s g/\mathrm{d}z^s)$.

D'un point de vue algébrique, la coordonnée X_1 vue comme une fonction polynomiale sur la courbe $\mathcal{C}$ est une base de transcendance du corps $\mathbb{Q}(\mathcal{C})$. On pose $\delta = \deg(\mathcal{C})$ et, pour $\mu = 2,\dots,m$, on désigne par $P_\mu(X_1,X_\mu)$ l'élément irréductible de $\mathbb{Z}[X_1,X_\mu]$, défini au signe près, qui s'annule identiquement sur $\mathcal{C}$. Alors, P_μ est de degré $\leq \delta$ et on a $\partial P_\mu/\partial X_\mu \neq 0$. On notera aussi par le même symbole ∂_1 la dérivation de $\mathbb{Q}(X_1, \ldots, X_m)$ donnée par la formule

$$\partial_1 = \frac{1}{A_1}\left(\sum_{\mu=1}^{m} A_\mu \frac{\partial}{\partial X_\mu}\right),$$

où

$$A_1 = \prod_{i=2}^{m} \frac{\partial P_i}{\partial X_i} \quad \text{et} \quad A_\mu = -A_1 \frac{\partial P_\mu}{\partial X_1}\left(\frac{\partial P_\mu}{\partial X_\mu}\right)^{-1}, \quad (2 \leq \mu \leq m).$$

Il est clair que $\partial_1 X_1 = 1$ et que $\partial_1 P_\mu = 0$ pour tout $\mu = 2, \ldots, m$. La dérivation ∂_1 annule donc l'idéal de définition de la courbe $\mathcal{C}$ et définit par passage au quotient la dérivation ∂_1 du corps $\mathbb{Q}(\mathcal{C})$ considérée ci-dessus.

Le résultat suivant raffine le lemme 4 du chapitre 2 de [3] :

LEMME 8. — *Pour tout polynôme $Q \in \mathbb{Z}[X_1, \ldots, X_m]$ et tout entier $s \geq 1$, le produit $R_s = A_1^{2s-1}\partial_1^{[s]}Q$ est un élément de $\mathbb{Z}[X_1, \ldots, X_m]$ dont le degré et la longueur vérifient*

$$\deg(R_s) \leq \deg(Q) + (2s-1)m\delta \quad \textit{et} \quad L(R_s) \leq c_3^s\, 2^{\deg(Q)/(4m\delta)}\, L(Q),$$

avec $c_3 = 8m\delta L(A_1)\Big(\sum_{i=1}^{m} L(A_i)\Big)$.

Preuve. — Par dérivation de la formule $\partial_1^{[s]}Q = R_s/A_1^{2s-1}$, il vient la relation de récurrence

$$R_{s+1} = \frac{1}{s+1}\left\{A_1\left(\sum_{\mu=1}^{m} A_\mu \frac{\partial R_s}{\partial X_\mu}\right) - (2s-1)R_s\left(\sum_{\mu=1}^{m} A_\mu \frac{\partial A_1}{\partial X_\mu}\right)\right\}.$$

Comme $R_1 = \sum_{\mu=1}^{m} A_\mu \dfrac{\partial Q}{\partial X_\mu}$, il s'ensuit que R_s est un polynôme de $\mathbb{Q}[X_1, \ldots, X_m]$ de degré $\leq \deg(Q) + (2s-1)m\delta$. On déduit aussi de cette relation de récurrence la majoration de longueur

$$L(R_{s+1}) \leq c_3'\Big(\frac{\deg(Q) + 4ms\delta}{s+1}\Big)L(R_s)$$

avec $c_3' = L(A_1)\sum L(A_i)$. Puisque $L(R_1) \leq c_3' \deg(Q) L(Q)$, on en tire

$$\begin{aligned} L(R_s) &\leq (c_3')^s L(Q) \prod_{j=0}^{s-1} \frac{\deg(Q) + 4mj\delta}{j+1} \\ &\leq (c_3')^s L(Q) (4m\delta)^s \binom{q+s-1}{s} \end{aligned}$$

où q désigne le plus petit entier $\geq \deg(Q)/(4m\delta)$. Majorant $\binom{q+s-1}{s}$ par 2^{q+s-1}, on obtient la majoration annoncée pour $L(R_s)$.

Il nous reste à vérifier que le polynôme R_s est à coefficients entiers lorsque le polynôme Q est à coefficients entiers. En vertu de la formule de Leibniz sur la dérivée d'un produit, il suffit de le montrer pour $Q = X_\mu$ avec $\mu = 2, \ldots, m$. À cet effet fixons μ et posons $X = X_1$, $Y = X_\mu$ et $P = P_\mu$. Alors la restriction de ∂_1 au corps $\mathbb{Q}(X,Y)$ est la dérivation ∂ qui vérifie $\partial X = 1$ et $\partial P(X,Y) = 0$. Remarquant que $\dfrac{\partial P}{\partial Y}(X,Y)$ est non nul dans l'anneau $A := \mathbb{Z}[X,Y]$, le lemme A1 de l'appendice appliqué au polynôme $F(t,u) = P(X+t, Y+u) - P(X,Y) \in A[t,u]$ nous fournit une série de puissances $U = \sum_{s\geq 1} c_s t^s \in \mathbb{Q}(X,Y)[[t]]$ telle que

$$P(X+t, Y+U) = P(X,Y) \quad \text{et} \quad \Big(\frac{\partial P}{\partial Y}(X,Y)\Big)^{2s-1} c_s \in A \qquad \text{pour } s \geq 1.$$

Posons $x = X + t$, $y = Y + U$ et prolongeons la dérivation ∂ au corps $\mathbb{Q}(X,Y)((t))$ par $\partial t = -1$. Ainsi $\partial x = \partial X + \partial t = 0$. Par dérivation de l'équation $P(X,Y) = P(x,y)$, on obtient alors que

$$\frac{\partial P}{\partial Y}(x,y)\partial y = \partial P(X,Y) = 0,$$

d'où il s'ensuit que $\partial y = 0$. Dérivons maintenant dans le corps $\mathbb{Q}(X,Y)((t))$ la relation

$$y = Y + \sum_{s\geq 1} c_s t^s.$$

Il vient l'équation

$$0 = \partial y = \partial Y - c_1 + \sum_{s\geq 1} \Big(\partial c_s - (s+1)c_{s+1}\Big) t^s$$

d'où l'on déduit que

$$c_1 = \partial Y \quad \text{et} \quad c_{s+1} = \partial c_s/(s+1), \quad (s \geq 1),$$

puis que $c_s = \partial^{[s]} Y$. Nous avons ainsi démontré que

$$\Big(\frac{\partial P_\mu}{\partial X_\mu}(X_1, X_\mu)\Big)^{2s-1} \partial_1^{[s]} X_\mu \in \mathbb{Z}[X_1, X_\mu], \quad (s \geq 1).$$

A fortiori le produit $A_1^{2s-1}\partial_1^{[s]} X_\mu$ appartient à $\mathbb{Z}[X_1, \ldots, X_m]$. □

Remarque. — L'assertion d'intégralité contenue dans le lemme 8 n'est pas valable pour une dérivation quelconque ∂_1 du corps $\mathbb{Q}(X_1, \ldots, X_m)$. Ainsi, pour tout entier $s \geq 1$ et $k \geq 0$, on a $\partial_1^{[s]} X_1^k = k^s X_1^k / s!$ lorsque

$\partial_1 = X_1(\partial/\partial X_1)$, alors que $(\partial/\partial X_1)^{[s]}X_1^k = \binom{k}{s}X_1^{k-s}$. Nous avons essentiellement établi dans le lemme 8 qu'une formule de ce dernier type s'étend à une extension algébrique de $\mathbb{Q}(X_1)$ lorsque ∂_1 est l'unique prolongement à cette extension de la dérivation $\partial/\partial X_1$ sur $\mathbb{Q}(X_1)$. Dans cette situation, le lemme A2 de l'appendice permet d'ailleurs plus généralement d'expliciter une telle formule pour $\partial_1^{[s]}(X_1^{k_1}\dots X_m^{k_m})$ quels que soient les entiers $k_1 \geq 0, \dots, k_m \geq 0$.

Regardons de nouveau ∂_1 comme une dérivation du corps $\mathbb{Q}(\mathcal{C})$. Comme ce corps est de degré de transcendance 1 sur $\mathbb{Q}$, les dérivations de $\mathbb{Q}(\mathcal{C})$ forment un espace vectoriel de dimension 1 sur $\mathbb{Q}(\mathcal{C})$. On peut donc écrire $\partial_1 = f\partial$ avec $f \in \mathbb{Q}(\mathcal{C})$, $f \neq 0$. Le lemme suivant permet de comparer les valeurs des opérateurs différentiels $\partial_1^{[s]}$, $(s \geq 0)$, et $\partial^{[t]}$, $(t \geq 0)$.

LEMME 9. — *Pour tout polynôme $Q \in \mathbb{Q}(X_1,\dots,X_m)$ et tout entier $s \geq 1$, on a la majoration*

$$|\partial_1^{[s]}Q(\underline{\theta})| \leq c_4^s\left(\max_{1\leq t\leq s}|\partial^{[t]}Q(\underline{\theta})|\right),$$

où la constante c_4 ne dépend que de f et du point $\underline{\theta}$.

Preuve. — Pour tout couple d'entiers t et s avec $1 \leq t \leq s$, désignons par $\mathcal{F}_{s,t}$ l'ensemble fini formé des suites $\underline{\tau} = (\tau_i)_{i\geq 1}$ d'entiers ≥ 0 vérifiant les conditions suivantes :

$$\sum_{i\geq 1}\tau_i = t \qquad \text{et} \qquad \sum_{i\geq 1} i\tau_i = s.$$

Le lemme A3 de l'appendice nous fournit alors la formule

$$\partial_1^{[s]} = \sum_{t=1}^{s} a_{s,t}\partial^{[t]}, \quad (s \geq 1),$$

avec des coefficients $a_{s,t} \in \mathbb{Q}(\mathcal{C})$ définis par

$$a_{s,t} = \sum_{\underline{\tau}\in\mathcal{F}_{s,t}} \binom{t}{\underline{\tau}} \prod_{i\geq 1}\left(\frac{\partial_1^{i-1}f}{i!}\right)^{\tau_i}, \quad (1 \leq t \leq s),$$

où $\binom{t}{\underline{\tau}} = t!/\prod_{i\geq 1}\tau_i!$ désigne le coefficient multinomial. Par ailleurs, pour tout entier $k \geq 0$, on a $\partial_1^k f(\underline{\theta}) = (f\circ\varphi)^{(k)}(\theta_1)$ et par suite la formule de Cauchy donne les majorations

$$\left|\frac{\partial_1^{i-1}f(\underline{\theta})}{i!}\right| \leq (c_4')^i, \quad (i \geq 1)$$

avec une constante c_4' qui ne dépend que de f et de φ. Comme la courbe $\mathcal{C}$ est entièrement déterminée par son point $\mathbb{Q}$-générique $\underline{\theta}$, la fonction φ et son ouvert de définition $\mathcal{U}$ ne dépendent en dernier ressort que de $\underline{\theta}$. Donc, en fait, c_4' ne dépend que de f et de $\underline{\theta}$. Notant que

$$\sum_{\underline{T}\in\mathcal{F}_{s,t}} \binom{t}{\underline{T}} = \binom{s-1}{t-1}$$

(*cf.* formule (3h), page 146 de [5]), il s'ensuit que

$$|a_{s,t}(\underline{\theta})| \leq \left(\sum_{\underline{T}\in\mathcal{F}_{s,t}} \binom{t}{\underline{T}}\right)(c_4')^s \leq (2c_4')^s, \quad (1 \leq t \leq s),$$

et donc que

$$|\partial_1^{[s]}Q(\underline{\theta})| \leq s(2c_4')^s \left(\max_{1\leq t\leq s} |\partial^{[t]}Q(\underline{\theta})|\right) \leq (4c_4')^s \left(\max_{1\leq t\leq s} |\partial^{[t]}Q(\underline{\theta})|\right).$$

□

Preuve du corollaire 3. — On raisonne par l'absurde en supposant l'existence de la suite $(Q_n)_{n\in\mathbb{N}}$ et l'on pose

$$D_n = 3.4c_2\frac{d_n}{s_n}, \quad T_n = 3.4c_2\frac{t_n}{s_n}, \quad (n \geq 0),$$

où c_2 est la constante définie au théorème 1. Les deux suites D_n et T_n satisfont les conditions requises dans ce théorème. Pour une infinité d'indices n, il existe donc une approximation algébrique $\underline{\alpha}_n = (\alpha_1, \ldots, \alpha_m) \in \mathcal{C}(\overline{\mathbb{Q}})$ du point $\underline{\theta}$ vérifiant

$$\delta c_2^{-1}D_n \leq d(\underline{\alpha}_n) \leq D_n, \quad t(\underline{\alpha}_n) \leq T_n \quad \text{et} \quad \log\|\underline{\theta} - \underline{\alpha}\| \leq -c_2^{-1}D_nT_n.$$

Puisque $A_1(\underline{\theta}) \neq 0$ et que la suite des points $\underline{\alpha}_n$ converge vers $\underline{\theta}$, on a $A_1(\underline{\alpha}_n) \neq 0$ pour tout n suffisamment grand. On peut aussi supposer que $\underline{\alpha}_n$ est un point lisse de la courbe $\mathcal{C}$. Fixons un tel choix de n. La condition $A_1(\underline{\alpha}_n) \neq 0$ assure que les fonctions $\partial_1 Q_n, \partial_1^2 Q_n, \ldots$ sont toutes régulières au point $\underline{\alpha}_n$. La multiplicité d'intersection au point $\underline{\alpha}_n$ de la courbe $\mathcal{C}$ avec l'hypersurface d'équation $Q_n = 0$ est alors égale à l'ordre d'annulation en ce point de la fonction polynomiale Q_n restreinte à la courbe, c'est-à-dire au plus petit entier $s \geq 0$ pour lequel $\partial_1^s Q_n(\underline{\alpha}_n) \neq 0$. Si chacun des nombres $\partial_1^\sigma Q_n(\underline{\alpha}_n)$ avec $0 \leq \sigma \leq s_n/3$ était nul, cette multiplicité d'intersection s serait $> s_n/3$. En vertu du théorème de Bézout (voir par exemple le théorème 7.7 du chapitre 1 de [7]), on aurait alors que $\delta d_n \geq d(\underline{\alpha}_n)s > d(\underline{\alpha}_n)s_n/3$, en contradiction avec la minoration $d(\underline{\alpha}_n) \geq \delta c_2^{-1}D_n$. Il existe donc un entier σ avec $0 \leq \sigma \leq s_n/3$ pour lequel $\partial_1^{[\sigma]} Q_n(\underline{\alpha}_n) \neq 0$. On va montrer que si n est assez grand, cela est impossible. Ce sera la contradiction finale.

Puisque $A_1(\underline{\theta}) \neq 0$, le polynôme $R = A_1^{2\sigma-1}\partial_1^{[\sigma]} Q_n$ ne s'annule pas au point $\underline{\alpha}_n$. Le lemme 8 nous fournit les majorations

$$\deg(R) \leq d_n + \frac{2}{3} m\delta s_n \leq 1.1 d_n$$

et

$$\begin{aligned} L(R) &\leq \binom{d_n+m}{m} e^{t_n} c_3^{s_n/3} 2^{d_n/4} \\ &\leq \exp\left(t_n + \frac{\log 2}{4} d_n + \mathcal{O}(s_n) + \mathcal{O}(\log d_n)\right) \\ &\leq \exp\left(1.1 t_n + o(t_n)\right). \end{aligned}$$

L'inégalité de Liouville (cf. lemme 3.14 de [20]) implique alors la minoration

$$\begin{aligned} \log|R(\underline{\alpha}_n)| &\geq -d(\underline{\alpha}_n) h\big(R(\underline{\alpha}_n)\big) \\ &\geq -d(\underline{\alpha}_n) \log L(R) - \mu(\underline{\alpha}_n)\deg(R) \\ &\geq -(1.1 + o(1))\Big(D_n t_n + T_n d_n\Big) \\ &\geq -7.5 c_2 \frac{d_n t_n}{s_n} \end{aligned}$$

pour tout entier n suffisamment grand.

Il nous reste à majorer $|R(\underline{\alpha}_n)|$. Le lemme 9 entraîne tout d'abord la majoration

$$\begin{aligned} \max_{0\leq s<s_n} |\partial_1^{[s]} Q_n(\underline{\theta})| &\leq c_4^{s_n} \max_{0\leq s<s_n} |\partial^{[s]} Q_n(\underline{\theta})| \\ &\leq \exp\Big(\mathcal{O}(s_n) - c d_n t_n/s_n\Big) \\ &\leq \exp\Big(-(c - o(1))\frac{d_n t_n}{s_n}\Big). \end{aligned}$$

La formule de Taylor nous permet maintenant de majorer la valeur de la fonction $\partial_1^{[\sigma]} Q_n$ sur la courbe $\mathcal{C}$ au point $\underline{\alpha}_n$ voisin du point $\underline{\theta}$. On procède de la façon suivante.

Soit ρ un nombre réel positif ≤ 2 tel que $\mathcal{U}$ contienne le disque $|z-\theta_1| \leq \rho$, et soit $g = Q_n \circ \varphi$. Supposons n suffisamment grand pour qu'on ait à la fois $\underline{\alpha}_n \in \mathcal{V}$ et $|\alpha_1 - \theta_1| \leq \rho/2$. Alors, on a $\partial_1^{[\sigma]} Q_n(\underline{\alpha}_n) = g^{[\sigma]}(\alpha_1)$, où rappelons que α_1 désigne la première coordonnée du point $\underline{\alpha}_n$, ainsi que $\partial_1^{[s]} Q_n(\underline{\theta}) = g^{[s]}(\theta_1)$ pour tout entier $s \geq 0$. Désignons par u le plus petit entier $\geq 2s_n/3$, et développons la fonction $g^{[\sigma]}$ en série de Taylor à l'ordre $u-1$ au point θ_1. On trouve :

$$g^{[\sigma]}(\alpha_1) = \sum_{0\leq\nu<2s_n/3} \binom{\sigma+\nu}{\sigma} g^{[\sigma+\nu]}(\theta_1)(\alpha_1-\theta_1)^\nu$$
$$+\binom{\sigma+u}{u} g^{[\sigma+u]}(\zeta)(\alpha_1-\theta_1)^u$$

où le nombre complexe ζ appartient au segment $[\theta_1, \alpha_1]$. Remarquant que, pour tout entier ν avec $\nu < 2s_n/3$, on a $\sigma+\nu<\sigma+u\leq s_n$, il vient

$$\begin{aligned}
&\left|\partial_1^{[\sigma]} Q_n(\underline{\alpha}_n)\right| \\
&\leq 2^{s_n+1} \max\left\{\max_{0\leq s<s_n} \left|\partial_1^{[s]} Q_n(\underline{\theta})\right|, \left|g^{[\sigma+u]}(\zeta)\right| |\alpha_1-\theta_1|^u\right\} \\
&\leq 2^{s_n+1} \max\left\{\exp\left(-(c-o(1))\frac{d_n t_n}{s_n}\right), \left|g^{[\sigma+u]}(\zeta)\right| \exp\left(-7.7c_2\frac{d_n t_n}{s_n}\right)\right\}.
\end{aligned}$$

Pour majorer $\left|g^{[\sigma+u]}(\zeta)\right|$, on utilise de nouveau la formule de Cauchy. Puisque g est holomorphe sur un ouvert contenant le disque $|z-\theta_1|\leq\rho$ et que ce disque contient le disque $|z-\zeta|\leq\rho/2$, on trouve

$$\left|g^{[\sigma+u]}(\zeta)\right| \leq \left(\frac{2}{\rho}\right)^{\sigma+u} \max_{|z-\zeta|\leq\rho/2} |g(z)| \leq \left(\frac{2}{\rho}\right)^{s_n} \max_{|z-\theta_1|\leq\rho} |g(z)|.$$

Comme

$$\max_{|z-\theta_1|\leq\rho} |g(z)| \leq H(Q_n)\binom{d_n+m}{m}\left(\max_{|z-\theta_1|\leq\rho}\{1, \|\varphi(z)\|\}\right)^{d_n},$$

on obtient ainsi

$$\left|g^{[\sigma+u]}(\zeta)\right| \leq \exp\left(t_n+\mathcal{O}(d_n)+\mathcal{O}(s_n)\right) \leq \exp\left((0.2+o(1))\frac{t_n d_n}{s_n}\right).$$

Reportant cette estimation dans la majoration de $|\partial_1^{[\sigma]} Q_n(\underline{\alpha}_n)|$ et en tenant compte du fait que $|A_1(\underline{\alpha}_n)|$ est borné indépendamment de n, il vient

$$\log|R(\underline{\alpha}_n)| \leq -(7.6c_2-o(1))\frac{d_n t_n}{s_n}$$

en contradiction avec la minoration obtenue précédemment. □

8. Appendice de calcul différentiel.

On se propose d'établir dans cet appendice quelques propriétés ou formules différentielles utilisées précédemment. Commençons par la version suivante du théorème des fonctions implicites.

LEMME A1. — *Soient A un anneau intègre, k son corps des fractions, et $F(t,u) = \sum_{i,j\geq 0} a_{i,j}t^i u^j \in A[[t,u]]$ une série de puissances avec $a_{0,0} = 0$ et $a_{0,1} \neq 0$. Alors, il existe une et une seule série de puissances $U = \sum_{s\geq 1} c_s t^s \in k[[t]]$ telle que $F(t,U) = 0$ dans $k[[t]]$. Les coefficients de cette série vérifient $(a_{0,1})^{2s-1}c_s \in A$ pour tout $s \geq 1$.*

Preuve. — Lorsque $a_{0,1}$ est inversible dans A, l'existence et l'unicité d'une solution formelle U à coefficients dans A est banale ; voir par exemple le corollaire de la proposition 10 du chapitre IV §4 des fascicules d'*Algèbre* de N. Bourbaki. Appliquant alors ce cas particulier à la série

$$(a_{0,1})^{-2}F(a_{0,1}^2 t, a_{0,1}u) = u + \sum_{(i,j)\neq(0,1)} a_{i,j}a_{0,1}^{2i+j-2}t^i u^j$$

de $A[[t,u]]$, on en déduit que $a_{0,1}^{-1}U(a_{0,1}^2 t)$ appartient à $A[[t]]$. □

Le résultat suivant précise le lemme A1. Il fournit une formule fermée pour le s-ième coefficient c_s de U en fonction des coefficients $a_{i,j}$ de F.

Pour tout entier $s \geq 1$, désignons par $\mathcal{E}_s$ l'ensemble des suites $\underline{\sigma} = (\sigma_{i,j})$ d'entiers ≥ 0 indexées par $(i,j) \in \mathbb{N}^2 \setminus \{(0,0),(0,1)\}$ et vérifiant les conditions

$$\sum_{i,j} i\sigma_{i,j} = s, \quad \sum_{i,j}(j-1)\sigma_{i,j} = -1, \quad 1 \leq |\underline{\sigma}| \leq 2s-1,$$

où l'on a posé $|\underline{\sigma}| = \sum_{i,j} \sigma_{i,j}$.

LEMME A2. — *Pour tout $s \geq 1$, on a la formule*

$$c_s = \sum_{\underline{\sigma}\in\mathcal{E}_s} q(\underline{\sigma}) \prod_{i,j} \left(-\frac{a_{i,j}}{a_{0,1}}\right)^{\sigma_{i,j}} \quad \text{avec} \quad q(\underline{\sigma}) = \frac{(|\underline{\sigma}|-1)!}{\prod_{i,j} \sigma_{i,j}!}.$$

De plus les coefficients $q(\underline{\sigma})$ sont des entiers rationnels.

Preuve. — Remarquons tout d'abord que l'intégralité des coefficients $q(\underline{\sigma})$ résulte immédiatement de la formule ci-dessus jointe au lemme A1. Écrivons en effet cette formule sous la forme :

$$a_{0,1}^{2s-1}c_s = \sum_{\underline{\sigma}\in\mathcal{E}_s} (-1)^{|\underline{\sigma}|} q(\underline{\sigma}) a_{0,1}^{2s-1-|\underline{\sigma}|} \prod_{i,j} a_{i,j}^{\sigma_{i,j}}.$$

Si l'on choisit des coefficients génériques $a_{i,j}$, le lemme A1, appliqué à l'anneau A des polynômes à coefficients dans $\mathbb{Z}$ en les indéterminées $a_{i,j}$, montre que le membre de droite dans l'égalité précédente est un polynôme à coefficients entiers en les $a_{i,j}$. Il s'ensuit que ses coefficients $(-1)^{|\underline{\sigma}|}q(\underline{\sigma})$ sont des entiers rationnels.

La preuve de la formule est basée sur l'interprétation différentielle des coefficients c_s déjà rencontrée dans la démonstration du lemme 8. Reprenons ce dernier point. Le lemme A1 appliqué à l'anneau de séries formelles $A[[X,Y]]$ nous fournit une série de puissances, pour laquelle on conservera la même notation $U = \sum_{s\geq 1} c_s t^s$, qui est solution formelle de l'équation $F(X+t, Y+U) = F(X,Y)$. Nous allons montrer que les coefficients $c_s \in k((X,Y))$ sont donnés par la formule

$$(*) \qquad c_s = \sum_{\underline{\sigma}\in\mathcal{E}_s} q(\underline{\sigma}) \prod_{i,j} \left(-\frac{F_{i,j}}{F_{0,1}}\right)^{\sigma_{i,j}}$$

où l'on a noté

$$F_{i,j} = (i!j!)^{-1} \frac{\partial^{i+j} F}{\partial t^i \partial u^j}(X,Y), \quad (i \geq 0, j \geq 0).$$

Pour retrouver la formule du lemme à partir de $(*)$, il suffit de spécialiser X et Y en 0. Désignons par ∂ la dérivation du corps $k((X,Y))$ définie par

$$\partial k = 0, \quad \partial X = 1, \quad \partial F(X,Y) = 0,$$

et reprenons les arguments utilisés dans la preuve du lemme 8 en remplacant l'anneau de base $\mathbb{Z}$ par A et le corps $\mathbb{Q}(X,Y)$ par $k((X,Y))$. On vérifie comme précédemment que

$$c_s = \partial^{[s]} Y, \quad (s \geq 1).$$

On notera cette fois-ci que $\dfrac{\partial F}{\partial u}(X+t, Y+U)$ est non nul car son terme constant $a_{0,1}$ est non nul. Cette interprétation différentielle de c_s nous permet de procéder par récurrence sur s en dérivant la formule $(*)$ au rang s.

Comme $\partial Y = -F_{1,0}/F_{0,1}$, la formule $(*)$ est vérifiée pour $s = 1$. Pour simplifier l'écriture, posons

$$T_{i,j} = -F_{i,j}/F_{0,1}, \quad T^{\underline{\sigma}} = \prod_{i,j} T_{i,j}^{\sigma_{i,j}},$$

et pour tout $(a,b) \in \mathbb{N}^2 \setminus \{(0,0),(0,1)\}$, notons $\underline{1}_{a,b}$ la suite d'entiers $\underline{\sigma}$ où les $\sigma_{i,j}$ sont tous nuls sauf pour $i = a, j = b$ auquel cas $\sigma_{a,b} = 1$.

On vérifie aisément que

$$\partial T_{i,j} = (i+1)T_{i+1,j} + (j+1)T_{1,0}T_{i,j+1} + T_{1,1}T_{i,j} + 2T_{1,0}T_{0,2}T_{i,j}.$$

Supposant que la formule $(*)$ soit établie au rang s, il vient par dérivation

$$\partial c_s = \Sigma_1 + \Sigma_2 + \Sigma_3 + \Sigma_4$$

avec

$$\Sigma_1 = \sum_{\underline{\tau}} \sum_{i,j} (i+1)\tau_{i,j} q(\underline{\tau}) T^{\underline{\tau}+\underline{1}_{i+1,j}-\underline{1}_{i,j}}$$

$$\Sigma_2 = \sum_{\underline{\tau}} \sum_{i,j} (j+1)\tau_{i,j} q(\underline{\tau}) T^{\underline{\tau}+\underline{1}_{1,0}+\underline{1}_{i,j+1}-\underline{1}_{i,j}}$$

$$\Sigma_3 = \sum_{\underline{\tau}} \sum_{i,j} \tau_{i,j} q(\underline{\tau}) T^{\underline{\tau}+\underline{1}_{1,1}}$$

$$\Sigma_4 = 2\sum_{\underline{\tau}} \sum_{i,j} \tau_{i,j} q(\underline{\tau}) T^{\underline{\tau}+\underline{1}_{1,0}+\underline{1}_{0,2}}$$

où les indices de sommation $\underline{\tau}$ et (i,j) décrivent respectivement $\mathcal{E}_s$ et $\mathbb{N}^2 \setminus \{(0,0),(0,1)\}$. On vérifie immédiatement que les exposants

$$\underline{\tau} + \underline{1}_{i+1,j} - \underline{1}_{i,j}, \quad \underline{\tau} + \underline{1}_{1,0} + \underline{1}_{i,j+1} - \underline{1}_{i,j}, \quad \underline{\tau} + \underline{1}_{1,1} \quad \text{et} \quad \underline{\tau} + \underline{1}_{1,0} + \underline{1}_{0,2}$$

appartiennent à $\mathcal{E}_{s+1}$ (notez que l'on peut supposer $\tau_{i,j} \geq 1$ car sinon la contribution du terme indexé par $\underline{\tau}, i, j$ est nulle dans les quatre sommes). Pour chaque $\underline{\sigma} \in \mathcal{E}_{s+1}$, regroupons alors dans $\Sigma_1, \Sigma_2, \Sigma_3$ et Σ_4 les termes contenant le monôme $T^{\underline{\sigma}}$. Tout calcul fait, il vient

$$\begin{aligned}
\Sigma_1 &= \sum_{\underline{\sigma}} \Big(\sum_{i,j} (i+1)\sigma_{i+1,j} \Big) q(\underline{\sigma}) T^{\underline{\sigma}} \\
&= \sum_{\underline{\sigma}} \Big(s+1-\sigma_{1,0}-\sigma_{1,1} \Big) q(\underline{\sigma}) T^{\underline{\sigma}} \\
\Sigma_2 &= \sum_{\underline{\sigma}} \Big(\sum_{i,j} (j+1)\sigma_{i,j+1} \Big) \frac{\sigma_{1,0}}{|\underline{\sigma}|-1} q(\underline{\sigma}) T^{\underline{\sigma}} \\
&= \sum_{\underline{\sigma}} \frac{\sigma_{1,0}(|\underline{\sigma}|-1-2\sigma_{0,2})}{|\underline{\sigma}|-1} q(\underline{\sigma}) T^{\underline{\sigma}} \\
\Sigma_3 &= \sum_{\underline{\sigma}} \sigma_{1,1} q(\underline{\sigma}) T^{\underline{\sigma}} \\
\Sigma_4 &= 2\sum_{\underline{\sigma}} \frac{\sigma_{1,0}\sigma_{0,2}}{|\underline{\sigma}|-1} q(\underline{\sigma}) T^{\underline{\sigma}}.
\end{aligned}$$

Il s'ensuit que

$$\Sigma_1 + \Sigma_2 + \Sigma_3 + \Sigma_4 = (s+1) \sum_{\underline{\sigma} \in \mathcal{E}_{s+1}} q(\underline{\sigma}) T^{\underline{\sigma}},$$

d'où la formule $(*)$ au rang $s+1$. □

Remarque. — Il serait intéressant de donner une interprétation combinatoire des coefficients $q(\underline{\sigma})$. Les *nombres de Catalan* $\binom{2n}{n}/(n+1)$ en sont des cas particuliers obtenus pour $\sigma_{0,2} = n, \sigma_{1,0} = n+1$ et $\sigma_{i,j} = 0$ autrement. Voir à ce sujet les références [8] et [9]. Dans une terminologie différente, le corollaire 2.7 de [9] équivaut notamment à la formule $c_s = \partial^{[s]}Y\Big|_{X=0,Y=0}$ utilisée dans la preuve du lemme A2.

Indiquons maintenant la traduction dans un corps différentiel quelconque de la classique formule de Faa di Bruno qui permet d'exprimer les dérivées successives d'une fonction composée en termes de polynômes de Bell, *cf.* [5].

Soit $\mathbb{K}$ un corps de caractéristique nulle muni d'une dérivation ∂ et soit $f \in \mathbb{K}$. Notons $\partial_1 = f\partial$ et rappelons que pour tout couple d'entiers t et s avec $1 \leq t \leq s$, nous avons désigné par $\mathcal{F}_{s,t}$ l'ensemble des suites $\underline{\sigma} = (\sigma_i)_{i\geq 1}$ d'entiers ≥ 0 vérifiant les conditions

$$\sum_{i\geq 1} \sigma_i = t \qquad \text{et} \qquad \sum_{i\geq 1} i\sigma_i = s.$$

LEMME A3. — *Pour tout entier $s \geq 1$, on a la formule*

$$\partial_1^{[s]} = \sum_{t=1}^{s} a_{s,t}\partial^{[t]} \quad \text{avec} \quad a_{s,t} = \sum_{\underline{\sigma}\in\mathcal{F}_{s,t}} \binom{t}{\underline{\sigma}} \prod_{i\geq 1} \left(\frac{\partial_1^{i-1} f}{i!}\right)^{\sigma_i}.$$

Preuve. — On procède par récurrence sur $s \geq 1$, l'assertion étant évidente pour $s = 1$. Appliquant la dérivation ∂_1 à la formule au rang s, on obtient la relation de récurrence

$$a_{s+1,t} = (s+1)^{-1}\Big(\partial_1 a_{s,t} + tfa_{s,t-1}\Big)$$

avec les conventions $a_{s,s+1} = a_{s,0} = 0$. Il vient

$$\begin{aligned}\partial_1 a_{s,t} &= \sum_{\underline{\tau}\in\mathcal{F}_{s,t}} \sum_{j\geq 1} \binom{t}{\underline{\tau}} \tau_j \frac{\partial_1^j f}{j!} \left(\frac{\partial_1^{j-1} f}{j!}\right)^{\tau_j - 1} \prod_{\substack{i\geq 1\\ i\neq j}} \left(\frac{\partial_1^{i-1} f}{i!}\right)^{\tau_i} \\ &= \sum_{\underline{\sigma}\in\mathcal{F}_{s+1,t}} \binom{t}{\underline{\sigma}} (s+1-\sigma_1) \prod_{i\geq 1} \left(\frac{\partial_1^{i-1} f}{i!}\right)^{\sigma_i}\end{aligned}$$

car pour tout $\underline{\sigma} \in \mathcal{F}_{s+1,t}$, le coefficient du monôme $\prod_{i\geq 1} \left(\frac{\partial_1^{i-1} f}{i!}\right)^{\sigma_i}$ dans la somme double ci-dessus est égal à

$$\binom{t}{\underline{\sigma}}\Big(\sum_{j\geq 1}(j+1)\sigma_{j+1}\Big) = \binom{t}{\underline{\sigma}}(s+1-\sigma_1).$$

On vérifie de même que

$$tfa_{s,t-1} = \sum_{\underline{\sigma}\in\mathcal{F}_{s+1,t}} \binom{t}{\underline{\sigma}}\sigma_1 \prod_{i\geq 1}\left(\frac{\partial_1^{i-1}f}{i!}\right)^{\sigma_i},$$

d'où s'ensuit la formule pour $a_{s+1,t}$. □

BIBLIOGRAPHIE

[1] J.B. Bost, H. Gillet et C. Soulé, Heights of projective varieties and positive Green forms, J. Amer. Math. Soc., 7 (1994), 903–1022.

[2] D. Brownawell, Sequences of Diophantine approximations, J. Number Theory, 6 (1974), 10–21.

[3] M. Chardin, Contributions à l'algèbre commutative effective et à la théorie de l'élimination, Thèse de doctorat de l'Université Pierre et Marie Curie (1990).

[4] G.V. Choodnovsky, Contributions to the theory of transcendental numbers, Math. Surveys and Monographs, 19, A.M.S. (1984).

[5] L. Comtet, Analyse combinatoire, tome premier, Collection Sup. Le mathématicien, Presses Universitaires de France, 1970.

[6] G. Diaz, Une nouvelle propriété d'approximation diophantienne, C. R. Acad. Sci. Paris, 324 (1997), 969–972.

[7] R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics, 52, Springer-Verlag, 1977.

[8] A. Joyal, Une théorie combinatoire des séries formelles, Advance in Math., 42 (1981), 1–82.

[9] G. Labelle, Une combinatoire sous-jacente au théorème des fonctions implicites, J. Comb. Theory Ser. A, 40 (1985), 377–393.

[10] M. Laurent, New methods in algebraic independence, in: Number Theory, Eds.: Györy, Pethö and Sos, Walter de Gruyter, Berlin, 1998, 311–330.

[11] M. Laurent et D. Roy, Criteria of algebraic independence with multiplicities and interpolation determinants, Trans. Amer. Math. Soc., à paraître.

[12] K. Mahler, On some inequalities for polynomials in several variables, J. London Math. Soc., 37 (1962), 341–344.

[13] D. Mumford, Algebraic geometry I: Complex Projective Varieties, 2-ième éd., Springer-Verlag, 1995.

[14] P. Philippon, Critères pour l'indépendance algébrique, Pub. Math. IHES, 64 (1986), 5–52.

[15] P. Philippon, Sur les hauteurs alternatives III, J. Math. Pures Appl., 74 (1994), 345–365.

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

[17] D. Roy et M. Waldschmidt, Approximation diophantienne et indépendance algébrique de logarithmes, Ann. Sci. École Norm. Sup., 30 (1997), 753–796.

[18] D. ROY et M. WALDSCHMIDT, Simultaneous approximation and algebraic independence, Ramanujan Math. J., 1 (1997), 379–430.

[19] M. WALDSCHMIDT, Suites colorées, exposé 21, Séminaire Delange-Pisot-Poitou, (Groupe d'étude de théorie des nombres), 17-ième année, 1975/76, n° G21, 11p.

[20] M. WALDSCHMIDT, Linear independence of logarithms of algebraic numbers, The Institute of Mathematical Sciences, Madras, IMSc. Report 116, 1992, http://www.math.jussieu.fr/~miw.

[21] E. WIRSING, Approximation mit algebraischen Zahlen beschränkten Grades, J. reine angew. Math., 206 (1961), 67–77.

Manuscrit reçu le 23 mars 1998,
accepté le 11 septembre 1998.

M. LAURENT,
Institut de Mathématiques de Luminy, CNRS
163 Avenue de Luminy
Case 930
13288 Marseille Cedex 9 (France).

D. ROY,
Université d'Ottawa
Département de Mathématiques
585 King Edward
Ottawa, Ontario (Canada K1N 6N5).