Daniel Bertrand

# Fonctions abéliennes $p$-adiques. Définitions et conjectures

*Groupe de travail d'analyse ultramétrique*, tome 4 (1976-1977), exp. nº 21, p. 1-13
<http://www.numdam.org/item?id=GAU_1976-1977__4__A14_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, D. BARSKI, P. ROBBA)
4e année, 1976/77, n° 21, 13 p. 
9 mai 1977

# FONCTIONS ABÉLIENNES p-ADIQUES. DÉFINITIONS ET CONJECTURES.

par Daniel BERTRAND

Ainsi que l'ont montré LANG [8] et MASSER [9], l'étude des combinaisons linéaires d'intégrales abéliennes permet d'obtenir des résultats de géométrie diophantienne, liés au théorème de Siegel sur les points entiers des courbes algébriques. Nous reprenons ici cette démarche, et nous en développons l'analogue p-adique. La première partie de l'exposé est consacrée à la construction des "fonctions abéliennes v-adiques" associées à une variété abélienne $A$ définie sur un corps de nombres $F$, et à une place $v$ de $F$. Nous nous sommes attachés à préciser les normalisations de l'application exponentielle exigées par les applications à la théorie des nombres transcendants. Dans la deuxième partie, nous discutons une série de conjectures fondées sur des résultats récemment obtenus lorsque $A$ est de type C. M. et pour certaines places $v$ (voir [9], [5], [2]). Ces conjectures fourniraient en particulier une version quantitative du théorème de Siegel-Mahler-Lang [6] sur les dénominateurs des points rationnels d'une courbe algébrique $\Gamma$ de de genre $\geq 1$. L'intérêt principal de cette déduction réside dans la comparaison des distributions (au sens de WEIL) attachées à certaines fonctions rationnelles sur $\Gamma$.

## 1. Fonctions abéliennes v-adiques

1.1. Définitions (les énoncés de ce paragraphe sont classiques ; pour plus de détails, voir [4] et [12]).

Soient $F$ un corps de nombres, et $A$ une variété abélienne (c'est-à-dire une variété algébrique projective irréductible, munie d'une structure de groupe algébrique), définie sur $F$. A tout sur-corps $\Omega$ de $F$, on associe l'ensemble $A(\Omega)$ des points $\Omega$-rationnels de $A$. Ainsi, l'élément neutre $e$ de $A$ appartient au groupe $A(F)$.

Soient $d$ la dimension de $A$, et $\{X_0, \ldots, X_n\}$ un plongement de $A$ dans un espace projectif $\underset{\sim}{P}_n(F)$. On peut, sans perte de généralité, supposer que

$$X_0(e) \neq 0 \;;\quad X_i(e) = 0 \,,\quad \forall\, i = 1, \ldots, n \,.$$

La famille $\{x_i = X_i/X_0 \;;\; i = 1, \ldots, n\}$ définit un système de coordonnées affines $\tilde{x}$ sur l'ouvert $A_0 = \{P \in A \;;\; X_0(P) \neq 0\}$ de $A$. Nous notons $F[A_0]$ l'anneau des fonctions régulières sur $A_0$.

Soit $\mathrm{Lie}_F(A)$ l'espace des dérivations invariantes sur $A$, définies sur $F$. Les éléments $\omega$ de $\mathrm{Lie}_F(A)$ opéront sur le corps $F(A)$ des fonctions rationnelles $\varphi$ sur $A$, définies sur $F$. Plus précisément (voir [7], I, 2), si $\varphi$ est régulière en un point $x$ de $A_0$, il en est de même de $\omega\varphi$.

L'anneau affine $F[A_0]$ étant l'intersection de tous ses anneaux locaux, on a donc

$$\forall\, \omega \in \mathrm{Lie}_F(A) \ , \quad \forall\, \varphi \in F[A_0] : \ \omega\varphi \in F[A_0] \ .$$

En particulier, il existe, pour tout élément $\omega$ de $\mathrm{Lie}_F(A)$, $n$ éléments $P_{1,\omega}, \dots, P_{n,\omega}$ de $F[\tilde{x}]$ tels que

$$\forall\, i = 1, \dots, n : \ \omega x_i = P_{i,\omega}(x_1, \dots, x_n) \ .$$

Nous considérons désormais une place (finie ou non) $v$ de $F$, et le complété $F_v$ de $F$ en $v$. L'ensemble $A(F_v)$ est un groupe de Lie v-adique, d'espace tangent à l'origine $T_e\, A(F_v)$. L'application exponentielle v-adique $\exp_v$ qui lui est associée définit un difféomorphisme local de $T_e\, A(F_v)$ dans $A(F_v)$. Afin de la représenter par des fonctions analytiques, nous fixons une base $(D) = \{D_1, \dots, D_d\}$ de $T_e\, A(F_v)$, formées des restrictions en $e$ d'une base $\{\omega_1, \dots, \omega_d\}$ de $\mathrm{Lie}_F(A)$, ceci est licite, car $\mathrm{Lie}_F(A)$ est une F-structure sur $\mathrm{Lie}\, A(F_v)$ (voir [3], Chap. AG., § 11). Nous appellerons <u>normalisation de l'application exponentielle</u> le choix d'une telle base. Nous identifions alors l'espace vectoriel $F_v^d$ à $T_e\, A(F_v)$ en notant que, la différentielle $d\exp_v$ de $\exp_v$ étant un isomorphisme de $\mathrm{Lie}(T_e\, A(F_v))$ sur $\mathrm{Lie}\, A(F_v)$, il existe un isomorphisme unique $h : F_v^d \dashrightarrow T_e\, A(F_v)$ tel que, si $\{\partial/\partial z_j \ ; \ j = 1, \dots, d\}$ désigne la base canonique de $\mathrm{Lie}(F_v^d)$, on ait

$$d(\exp_v \circ h)(\partial/\partial z_j) = \omega_j \ , \quad \forall\, j = 1, \dots, d \ .$$

Posons, dans ces conditions,

$$f_{i,v} = x_i \circ \exp_v \circ h \qquad (i = 1, \dots, n) \ .$$

Les fonctions $f_{i,v}$ sont appelées <u>fonctions abéliennes</u> v-<u>adiques</u> normalisées associées au triplet $(A, F, (D))$. Elles sont analytiques sur un voisinage $\mathfrak{F}_v$ de l'origine de $F_v^d$, et l'application exponentielle est représentée par le système $\tilde{f}_v = (f_{1,v}, \dots, f_{n,v})$. Lorsqu'aucune confusion n'est à craindre, nous omettrons l'indice $v$ dans les notations précédentes.

Les propriétés qui suivent sont couramment utilisées dans les démonstrations de transcendance.

PROPRIÉTÉ 1. - <u>Soit</u> $\tilde{R}$ <u>le système de fractions rationnelles (à coefficients dans</u> $F$ ) <u>représentant la loi de groupe de</u> $A$ <u>dans les coordonnées</u> $\tilde{x}$. <u>Si</u> $\underset{\sim}{z}$ <u>et</u> $\underset{\sim}{z}'$ <u>sont deux éléments de</u> $\mathfrak{F}_v$, <u>on a</u>

$$\tilde{f}_v(\underset{\sim}{z} + \underset{\sim}{z}') = \tilde{R}(\tilde{f}_v(\underset{\sim}{z}) \ , \ \tilde{f}_v(\underset{\sim}{z}')) \ .$$

Ceci résulte de la commutativité de l'algèbre de Lie $\mathrm{Lie}\, A(F_v)$.

PROPRIÉTÉ 2. - Les fonctions $f_{1,v}, \dots, f_{n,v}$ vérifient le système différentiel :

$$(\partial/\partial z_j)\, f_{i,v} = P_{i,j}(\tilde{f}) \;,\quad \forall\, i = 1, \dots, n \;;\; j = 1, \dots, d \;,$$

où $P_{i,j}$ est un polynôme à coefficients dans $F$. En effet,

$$(\partial/\partial z_j)\, f_i = (\partial/\partial z_j)(x_i \circ \exp \circ h) = (d(\exp \circ h)(\partial/\partial z_j) x_i) \circ \exp \circ h$$
$$= (\mathcal{D}_j\, x_i) \circ \exp \circ h = P_{i,\mathcal{D}_j}(x_1, \dots, x_n) \circ \exp \circ h \;,$$

et on conclut en posant : $P_{i,j} = P_{i,\mathcal{D}_j}$.

REMARQUE. - Dans le cas où $v$ est une place infinie complexe, l'application $\tilde{f}_v$ admet un prolongement méromorphe sur $F_v^d$. On retrouve ainsi la définition des fonctions abéliennes classiques. Le choix de la base (D) décrit plus haut correspond, dans la terminologie de LANG [7], à une normalisation faible. Dans le cas où $v$ est une place finie, l'étude explicite de $\tilde{f}_v$ n'a été faite, à ma connaissance, que lorsque $A$ est la jacobienne d'une courbe algébrique (travaux de WEIL et LUTZ sur les fonctions elliptiques p-adiques, et de CHABAUTY sur les "intégrales abéliennes p-adiques", voir [4], notice historique).

## 1.2. Propriétés métriques.

Précisons tout d'abord quelques notations et conventions, qui seront reprises dans la deuxième partie de l'exposé. Pour toute place finie $v$ de $F$, nous désignons par $\mathcal{O}_v$ l'anneau des entiers v-adiques, par $\mathfrak{p}_v$ son idéal maximal, et par $p_v$ la carastéristique résiduelle du corps $F_v$. Si $v$ est une place infinie, nous posons $p_v = 1$. Nous dirons qu'une propriété $(S_v)$ est vérifiée "pour $v$ suffisamment grand" s'il existe un entier $p_0$, effectivement calculable en fonction des équations de définition de $A$, tel que $(S_v)$ soit vérifiée dès que $p_v > p_0$. Enfin, nous notons $|\;|_v$ la valeur absolue induite par celle de $\underset{\sim}{C}$ si $v$ est infinie, et normalisée par $|p_v|_v = p_v^{-1}$ si $v$ est finie, et nous posons

$$\forall\, \underset{\sim}{z} = (z_1, \dots, z_d) \in F_v^d : \; \|\underset{\sim}{z}\|_v = \sup_{j=1,\dots,d} |z_j|_v \,.$$

D'après le théorème de normalisation de Noether, il existe un système de coordonnées affines $\tilde{x}'$ sur $A_0$ tel que $F[A_0]$ soit entière sur $F[x_1', \dots, x_d']$. Il peut être déduit de $\underset{\sim}{x}$ par une transformation de $GL(n, F)$. Nous fixons le choix d'un tel système, que nous notons de nouveau $\tilde{x}$. Les fonctions $f_1, \dots, f_d$ sont alors algébriquement indépendantes, et l'application

$$\underset{\sim}{f}_v = (f_1, \dots, f_d) : \mathfrak{I}_v \longrightarrow F_v^d$$

est un difféomorphisme. De plus, on a la propriété suivante.

PROPRIETE 3. - Pour $v$ suffisamment grand,

(i) $\tilde{f}_v$ est définie sur le disque $\mathfrak{I}_v = \{z \in F_v^d \;;\; \|z\|_v < r_v\}$, où $r_v = p_v^{-1/(p_v-1)}$,

(ii) $\underset{\sim}{f}_v$ est une isométrie sur $\mathfrak{I}_v$.

<u>Démonstration</u> (l'argument qui suit généralise une idée classique, voir [4]).

(i) Pour $i = 1, \dots, n$, écrivons le développement de Taylor de $f_{i,v}$ en $0$ sous la forme :

$$f_i(\underset{\sim}{z}) = \sum_{\underset{\sim}{m} \in \underset{\sim}{N}^d} (a_{i,\underset{\sim}{m}}/(\underset{\sim}{m}!))\underset{\sim}{z}^{\underset{\sim}{m}} ,$$

où $\underset{\sim}{m}! = m_1! \dots m_d!$ et $\underset{\sim}{z}^{\underset{\sim}{m}} = z_1^{m_1} \dots z_d^{m_d}$, et soient

$$P_{i,j}(\tilde{x}) = \sum_{\tilde{\alpha} \in \underset{\sim}{N}^n} c_{\tilde{\alpha}}^{i,j}\, x^{\tilde{\alpha}} \qquad (\text{avec } \tilde{x} = (x_1, \dots, x_n))$$

les différents polynômes introduits dans l'énoncé de la propriété 2. Nous allons montrer par récurrence que, dès que les coefficients $c_{\tilde{\alpha}}^{i,j}$ sont des éléments de l'anneau $\mathcal{O}_v$, il en est de même des coefficients $a_{i,\underset{\sim}{m}}$.

D'après la construction des coordonnées $\tilde{x}$, on a, pour $i = 1, \dots, n$, $a_{i,0} = 0$. Soit alors $\underset{\sim}{m}$ un multi-indice $(m_1, \dots, m_d)$, et supposons que, pour tout multi-indice $\underset{\sim}{\mu} \leq \underset{\sim}{m}$ (c'est-à-dire tel que, pour $k = 1, \dots, d$, on ait $\mu_k \leq m_k$), les $n$ coefficients $a_{1,\underset{\sim}{\mu}}, \dots, a_{n,\underset{\sim}{\mu}}$ soient des entiers v-adiques. Pour $j = 1, \dots, d$, notons $\underset{\sim}{m}^j$ le multi-indice

$$(m_1, \dots, m_{j-1}, m_j + 1, m_{j+1}, \dots, m_d) .$$

On en déduit des équations différentielles satisfaites par $\tilde{f}$ que, pour $i = 1, \dots, n$ et $j = 1, \dots, d$ :

$$\frac{(m_j + 1)a_{i,\underset{\sim}{m}^j}}{\underset{\sim}{m}^j!} = \frac{a_{i,\underset{\sim}{m}^j}}{\underset{\sim}{m}!} = Q_{i,\underset{\sim}{m}^j}(c_{\tilde{\alpha}}^{i,j}) ,$$

où les coefficients de la forme linéaire $Q_{i,\underset{\sim}{m}^j}$ sont des sommes de monômes s'écrivant, à des facteurs entiers près, sous la forme

$$\prod_{(\sum \underset{\sim}{m}_\ell = \underset{\sim}{m})} a_{k_\ell,\underset{\sim}{m}_\ell}/(\underset{\sim}{m}!) .$$

Comme $\underset{\sim}{m}!/\prod(\underset{\sim}{m}_\ell!)$ est alors entier, on déduit de l'hypothèse de récurrence que, pour tout couple $(i, j)$, le nombre $a_{i,\underset{\sim}{m}^j}$ est un entier v-adique. La récurrence peut donc être poursuivie, et la proposition est démontrée.

L'assertion (i) résulte alors de la minoration :

$$\forall\ m \text{ entier } \geq 1 ,\quad |m!|_v > r_v^{m-1} .$$

(ii) Soit $d\underset{\sim}{f}(0) = (df_1(0), \dots, df_d(0))$ l'application linéaire tangente de $\underset{\sim}{f}$ à l'origine. Sa représentation matricielle $J$ est, d'après les normalisations du § 1.1, un élément de $GL(d, F)$. D'autre part, $J$ est non singulière, puisque $\underset{\sim}{f}$ est un difféomorphisme. En conséquence, $d\underset{\sim}{f}(0)$ est, pour $v$ suffisamment grand, une isométrie. Mais on déduit de l'intégralité des coefficients $a_{i,\underset{\sim}{m}}$, jointe à la minoration rappelée plus haut, et à l'identité

$$X_1 \ldots X_m - Y_1 \ldots Y_m = \sum_{i=1}^{m} (X_i - Y_i)\, Y_1 \ldots Y_{i-1}\, X_{i+1} \ldots X_m ,$$

que, pour $\underset{\sim}{z}$ et $\underset{\sim}{z}'$ éléments de $\mathfrak{F}_v$ :

$$\forall\, i = 1 , \ldots , d , \quad |f_i(\underset{\sim}{z}) - f_i(\underset{\sim}{z}') - df_i(0)(\underset{\sim}{z} - \underset{\sim}{z}')|_v < \|z - z'\|_v .$$

L'inégalité ultramétrique entraîne alors ;

$$\forall\, z , z' \in \mathfrak{F}_v , \quad \|\underset{\sim}{f}(\underset{\sim}{z}) - \underset{\sim}{f}(\underset{\sim}{z}')\|_v = \sup_{i=1,\ldots,d} |f_i(\underset{\sim}{z}) - f_i(\underset{\sim}{z}')|_v = \|z - z'\|_v .$$

### 1.3 Endomorphismes de $A$ .

Soient End $A$ l'anneau des endomorphismes de la variété abélienne $A$ , et $\mathrm{End}_0\, A$ la $\underset{\sim}{Q}$-algèbre $\mathrm{End}\, A \otimes \underset{\sim}{Q}$ . Quitte à faire une extension finie de $F$ , on peut supposer que tous les éléments de End $A$ sont définis sur $F$ . Dans ces conditions (voir [12], I), la différentielle à l'origine $d\lambda(e)$ d'un élément $\lambda$ de End $A$ est un endomorphisme de l'espace vectoriel $T_e\, A(F)$ , restriction en $e$ de $\mathrm{Lie}_F(A)$. Dans la base $(D) = \{D_1 , \ldots , D_d\}$ , décrite au § 1.1, $d\lambda(e)$ admet donc une représentation matricielle $B_\lambda$ à coefficients dans $F$ .

PROPRIÉTÉ 4. - Soit $\tilde{R}_\lambda$ le système de fractions rationnelles (à coefficients dans $F$ ) représentant l'endomorphisme $\lambda$ dans les coordonnées $\tilde{x}$ . Si $\underset{\sim}{z}$ et $B_\lambda \underset{\sim}{z}$ sont des éléments de $\mathfrak{F}_v$ , on a

$$\tilde{f}_v(B_\lambda(\underset{\sim}{z})) = \tilde{R}_\lambda(\tilde{f}_v(\underset{\sim}{z})) .$$

Ceci résulte de la relation : $\lambda \circ \exp_v = \exp_v \circ d\lambda(e)$ .

REMARQUE. - L'algèbre End $A$ étant un $\underset{\sim}{Z}$-module de rang fini, les dénominateurs des coefficients des matrices $B_\lambda$ restent bornés lorque $\lambda$ parcourt End $A$ . Si $v$ est une place finie, l'ensemble des endomorphismes $\lambda$ tels que $B_\lambda \mathfrak{F}_v$ soit inclus dans $\mathfrak{F}_v$ (c'est-à-dire tels que tous les coefficients de $B_\lambda$ soient entiers v-adiques) est donc un ordre $\mathrm{End}_v\, A$ de $\mathrm{End}_0\, A$ . Pour $v$ suffisamment grand, ou si $\mathrm{End}_0\, A$ est une algèbre commutative, $\mathrm{End}_v\, A$ coïncide avec End $A$ .

L'application $\lambda \longmapsto B_\lambda$ s'étend de façon unique en une représentation $\chi = \chi_{(D)}$ de l'algèbre des endomorphismes $\mathrm{End}_0\, A$ . Soient alors $R$ une $\underset{\sim}{Q}$-sous-algèbre de $\mathrm{End}_0\, A$ , unitaire et semi-simple, et $R_{(F)}$ la F-algèbre déduite de $R$ par extension des scalaires à $F$ . La restrictioh de $\chi_{(D)}$ à $R$ est équivalente à une somme directe de représentations irréductibles que, quitte à faire une nouvelle extension de $F$ , on peut supposer absolument irréductibles. Dans ces conditions, nous appellerons R-normalisation de l'application exponentielle le choix d'une base $(D)$ de $T_e\, A(F)$ compatible avec la décomposition de $T_e\, A(F)$ en $R_{(F)}$-modules irréductibles.

EXEMPLE. - Si $A$ est une variété abélienne du type C. M. de Shimura (voir [12], II), il existe un isomorphisme $\iota$ d'un corps de nombres $K$ de type C. M. (extension totalement imaginaire d'un corps totalement réel $K_0$ de degré $d$ ) dans $\mathrm{End}_0 A$. La représentation $\chi_{(D)}$ restreinte à $\iota(K)$ est équivalente à la somme directe $\sigma_1 \oplus \cdots \oplus \sigma_d$, où les $\sigma_i$ désignent des extensions à $K$ des différents plongements de $K_0$ dans $F_v$. Une $\iota(K)$-normalisation correspond ici au choix d'une base $(D)$ telle que :

$$\forall \beta \in K , \quad \chi_{(D)}(\iota(\beta)) = \mathrm{diag}(\sigma_1(\beta) , \ldots , \sigma_d(\beta)) .$$

Si $A$ est de plus une variété abélienne simple (voir [12], II, cas primitif), $\iota(K)$ est égal à $\mathrm{End}_0 A$, et les $(\mathrm{End}_0 A)$-normalisations ne sont autres que les normalisations fortes au sens de LANG [7].

## 2. Approximations diophantiennes

### 2.1. Enoncé des conjectures.

Les conjectures que nous proposons ci-dessous répondent, dans la situation des variétés abéliennes, aux résultats "non homogènes" obtenus dans la théorie des formes linéaires de logarithmes de nombres algébriques. Le rôle de ces logarithmes est ici joué par l'ensemble $\mathcal{L}_v$ des points algébriques des fonctions abéliennes v-adiques, dont nous précisons tout d'abord la définition.

Soit $\tilde{f}_v$ un système de fonctions abéliennes v-adiques associées à un triplet $(A , F , (D))$. Nous appelons point algébrique de $\tilde{f}_v$ tout élément de $\mathfrak{F}_v$ où $\tilde{f}_v$ prend des valeurs dans $F^n$. Lorsque $v$ est une place finie, l'ensemble $\mathcal{L}_v$ est, en vertu de la proposition 4, muni d'une structure de $(\mathrm{End}_v A)$-module, et des éléments de $\mathcal{L}_v$ sont linéairement indépendants sur $\mathrm{End}_v A$ si, et seulement si, leurs images par $\exp_v \circ h$ le sont sur $\mathrm{End}\, A$.

Si $v$ est une place infinie complexe (cas auquel, au moyen d'une extension de $F$ et d'un prolongement de $v$, on peut ramener toutes les places infinies), nous appellerons plus généralement point algébrique de $\tilde{f}_v$ l'ensemble des éléments de $F_v^d$ dont l'image par le prolongement de $\exp_v \circ h$ à $F_v^d$ (voir § 1.1, remarque), est un point de $A(F)$. L'ensemble $\mathcal{L}_v$ est alors muni d'une structure de $(\mathrm{End}_v A)$-module, où $\mathrm{End}_v A = \mathrm{End}\, A$.

Soient $M_d(F)$ l'ensemble des matrices $d \times d$ à coefficients dans $F$, et $\chi(\mathrm{End}_0 A)_{(F)}$ la sous-algèbre de $M_d(F)$ déduite de $\chi(\mathrm{End}_0 A)$ par extension des scalaires à $F$. Si $\beta = (\beta_1 , \ldots , \beta_m)$ désigne une famille d'éléments de $F$, nous appelons hauteur (relativement à $F$ ) de $\beta$ le nombre :

$$H(\beta) = \prod_{v \in \mathfrak{M}_F} \sup(1, |\beta_1|_v , \ldots , |\beta_m|_v)^{\delta_v} ,$$

où $\mathfrak{M}_F$ désigne l'ensemble des places de $F$, et $\delta_v$ le degré local de $F$ en $v$. Ainsi, la hauteur d'un élément de $M_d(F)$ est la hauteur de la famille de ses coefficients. De même, la hauteur $H_{\mathfrak{X}}(Q)$ d'un point $Q$ de $A_0(F)$ est la hauteur de la famille $\tilde{\mathfrak{X}}(Q)$. Enfin, nous notons $\underset{\sim}{1}$ le vecteur de $F_v^d$ dont toutes les composantes sont égales à 1, et $\delta$ le degré du corps $F$.

Les énoncés qui suivent sont relatifs à la donnée d'une place $v$ de $F$, et d'une normalisation (D) de l'application exponentielle.

CONJECTURE 1. - Soient $r$, $H$ et $U$ trois entiers $> 0$, et $\underset{\sim}{u}_1, \dots, \underset{\sim}{u}_r$ des éléments de $\mathcal{L}_v$ dont les images par $\exp_v \circ h$ sont de hauteur $\leq U$. Il existe quatre nombres réels strictement positifs $\varkappa_1$, $\varkappa_2$, $\varkappa_3$ effectivement calculables en fonction de $r$, $d$ et $\delta$, et $C$, effectivement calculable en fonction de $r$, $\delta$ et des équations de définition de $A$, tels que, pour tout $(r+1)$-uple $B_0, \dots, B_r$ d'éléments de $\chi(\mathrm{End}_0\, A)_{(F)}$ de hauteur $\leq H$, la forme linéaire $B_0 \underset{\sim}{1} + B_1 \underset{\sim}{u}_1 + \dots + B_r \underset{\sim}{u}_r$ s'annule ou vérifie :

$$\|B_0 \underset{\sim}{1} + B_1 \underset{\sim}{u}_1 + \dots + B_r \underset{\sim}{u}_r\|_v > \exp(-C(\log H)^{\varkappa_1} p_v^{\varkappa_2} (\log U)^{\varkappa_3}) .$$

Le cas d'annulation de la forme linéaire est précisé par l'énoncé suivant, qui généralise une conjecture de WALDSCHMIDT [13].

CONJECTURE 2. - Soient $u_1, \dots, u_r$ des éléments de $\mathcal{L}_v$ linéairement indépendants sur $\mathrm{End}_v\, A$. Alors, ils sont linéairement indépendants sur $\chi(\mathrm{End}_0\, A)_{(F)}$, et la forme linéaire ne peut s'annuler que si $B_0 \underset{\sim}{1}$ est nul.

La conjecture plus forte qui suit est indépendante du choix de (D) :

CONJECTURE 3. - Soient $u_1, \dots, u_r$ des éléments de $\mathcal{L}_v$ linéairement indépendants sur $\mathrm{End}_v\, A$, et $B_0, B_1, \dots, B_r$ des éléments de $M_d(F)$ tels que $B_0 \underset{\sim}{1}$ ou $B_1$ soit non nul. Alors, $B_0 \underset{\sim}{1} + B_1 \underset{\sim}{u}_1 + \dots + B_r \underset{\sim}{u}_r$ est non nul.

Le corps de nombres $F$ étant arbitraire, il est clair que les conjectures 2 et 3 fournissent des énoncés de transcendance. Ainsi, si $A$ est une variété abélienne simple, tout élément non nul de $\mathcal{L}_v$ est linéairement indépendant sur $\mathrm{End}_v\, A$, et on déduit de la conjecture 3, que, pour toute normalisation de l'application exponentielle v-adique, chacune des composantes de ses points algébriquement non nuls est transcendante (voir [8], § 2, pour le cas des places infinies).

Ces conjectures permettent de retrouver la plupart des énoncés obtenus lorsque $A$ est une courbe elliptique, et nous nous bornerons ici à rappeler une lacune importante dans les connaissances actuelles : le cas $r \geq 3$, $A$ sans multiplication complexe.

Lorsque $A$ est un produit de courbes elliptiques, et que $\tilde{f}_v$ est $(\mathrm{End}_0\, A)$-normalisée, les conjectures 1 et 2 se ramènent au cas de la dimension 1. En effet, si $A = E_1^{n_1} \times \dots \times E_s^{n_s}$, où les $E_i$ désignent des courbes elliptiques non isogènes, l'algèbre $\chi_{(D)}(\mathrm{End}_0\, A)_{(F)}$ s'identifie alors à la somme directe $\oplus_{i=1}^{s} M_{n_i}(F)$.

Mais un choix convenable de la base (D) permet de retrouver certains des résultats de BAKER, COATES et MASSER sur les périodes de deux fonctions elliptiques.

Peu de résultats sont connus dans le cas général. Un énoncé partiel a été obtenu par MASSER [10] lorsque $d = 2$ et $r = 1$. En revanche, si $A$ est une variété abélienne simple de type C. M., et si $\mathcal{L}_v$ est $(\mathrm{End}_0\ A)$-normalisée, les conjectures 1 et 2 ont été établies pour les places suivantes :

- $v$ est une place infinie (complexe) (voir [9], [5]), l'énoncé précis de la conjecture 1 se déduit de ces travaux par la méthode exposée dans [2].

- $v$ est une place finie, le nombre premier $p_v$ se décompose totalement dans le corps totalement réel $K_0$, et les idéaux de $K_0$ au-dessus de $p_v$ ont le même type de décomposition dans $K$ (voir [2]).

(Pour se ramener aux énoncés de ces critères, on notera que si

$$\{\mathrm{diag}(\sigma_j(\beta_i))\ ;\ j = 1, \ldots, d\ ;\ i = 1, \ldots, 2d\}$$

désigne une base de $\chi_{(D)}(\mathrm{End}\ A)$ sur $\mathbb{Z}$, les $2d$ lignes de la matrice $(\sigma_j(\beta_i))$, avec $j = 1, \ldots, d$ ; $i = 1, \ldots, 2d$, apparaissent dans l'écriture du discriminant du corps $K$. Son rang est donc égal à $d$, et l'algèbre $\chi_{(D)}(\mathrm{End}_0\ A)_{(F)}$ s'identifie à l'algèbre des matrices diagonales à coefficients dans $F$).

## 2.2. Une formulation intrinsèque.

Nous ferons désormais l'hypothèse suivante qui correspond, dans la théorie des formes linéaires de logarithmes, au cas "rationnel homogène" :

$(\mathcal{H})$ Il existe une normalisation de l'application exponentielle telle que la conjecture 1 soit vérifiée si $B_0$ est nulle, et $B_1, \ldots, B_r$ appartiennent à $\chi(\mathrm{End}_v\ A)$.

En vertu du théorème de Mordell-Weil, les ensembles $A(F)$ et $\mathcal{L}_v$ sont des $(\mathrm{End}_v\ A)$-modules de type fini. L'hypothèse $(\mathcal{H})$ fournit alors une minoration de la norme de tous les éléments non nuls de $\mathcal{L}_v$, que l'application exponentielle permet de transporter sur la variété. Nous notons $d_v$ la distance définie sur $A_0(F_v)$ par :

$$\forall\ P, Q \in A_0(F_v)\ ,\quad d_v(P, Q) = \sup_{i=1,\ldots,n} |x_i(P) - x_i(Q)|_v\ .$$

COROLLAIRE 1 [sous $(\mathcal{H})$]. - *Il existe un nombre réel $C_1 > 0$, effectivement calculable en fonction d'une base du groupe de Mordell-Weil $A(F)$ (et donc en général non effective), tel que, pour tout point $Q$ de $A_0(F)$ et toute place $v$ de $F$, on ait*

$$d_v(e, Q) > \exp\left(-C_1\, p_v^{\varkappa_4} [\log\log H_{\underline{x}}(Q)]^{\varkappa_1}\right),$$

*où $\varkappa_4 = \varkappa_2 + 2d\delta\varkappa_3$ ($r$ désignant alors le rang de $A(F)$).*

Démonstration. - Nous allons démontrer le corollaire lorsque $v$ est une place finie suffisamment grande. Le raisonnement qui suit s'étend aux "petites" places, à condition de substituer au facteur $C_1\, p_v^{\varkappa_4}$ une constante $C_2$ effectivement calculable en fonction de $C_1$ , $\delta$ et des équations de définitions de $A$ . Enfin, la démarche exposée dans [9], théorème 3, permet de traiter le cas des places infinies, et nous ne ne la reproduirons pas ici.

Soient $A_t(F)$ la $\underset{\sim}{Z}$-torsion de $A(F)$, et $P_1 , \dots , P_r$ des représentants d'une base du $\underset{\sim}{Z}$-module $A(F)/A_t(F)$ . Par $C_3$ , $C_4$ , $C_5$ , nous signifions des nombres réels $> 1$ ne dépendant que de $P_1 , \dots , P_r$ et de $A$ .

Tout élément $Q$ de $A(F)$ s'écrit sous la forme $Q = \beta_1 P_1 + \dots + \beta_r P_r + P_t$ , où $P_t \in A_t(F)$ , et $\beta_1 , \dots , \beta_r$ sont des éléments de $\mathrm{End}\, A$ . Si (D) désigne la normalisation définie par ($\mathcal{H}$), et $H$ le maximum des hauteurs des matrices $\chi_{(D)}(\beta_i)$ , la quadraticité de la hauteur de Néron-Tate sur $A$ entraîne

$$H_{\tilde{X}}(Q) > C_3^{H^2} .$$

Dès que $A$ a bonne réduction en la place $v$ , le noyau $A_v$ de la réduction de $A(F_v)$ modulo $\wp_v$ est un sous-groupe de $A(F_v)$ d'indice $\mu_v < C_4\, p_v^{\delta d}$ , puisque (voir [1], lemme 13) le cardinal de la variété réduite est $< C_4 (N_{F/\underset{\sim}{Q}}\, \wp_v)^d$ .

D'autre part, dès que $p_v$ ne se ramifie pas dans $F$ , le sous-groupe $\mathfrak{a}_v = \exp_v \circ h(\mathfrak{F}_v)$ de $A$ coïncide avec $A_v$ . En effet, la propriété 3(ii) (§ 1.2) montre que :

$$\mathfrak{a}_v = \{Q \in A_0(F_v) \ ; \ \forall\ i = 1 , \dots , n , \ |x_i(Q)|_v < p_v^{-1/(p_v-1)}\}$$

tandis que, par définition,

$$A_v = \{Q \in A_0(F_v) \ ; \ \forall\ i = 1 , \dots , n , \ |x_i(Q)|_v < 1\} .$$

En conséquence, les points $\mu_v Q$ , $\mu_v P_1$ , $\dots$ , $\mu_v P_r$ appartiennent à $\mathfrak{a}_v$ , le point $\mu_v P_t$ , élément de $A_t(F) \cap \mathfrak{a}_v$ , est nul, et l'on a, en notant $\ell_v$ l'application réciproque de $\exp_v \circ h$ sur $\mathfrak{a}_v$ ,

$$\|\ell_v(\mu_v Q)\|_v = \|\chi(\beta_1)\, \ell_v(\mu_v P_1) + \dots + \chi(\beta_r)\, \ell_v(\mu_v P_r)\|_v$$

(cf. propriété 4).

Comme $H_{\tilde{X}}(\mu_v P_i) < C_5^{\mu_v^2}$ , l'hypothèse ($\mathcal{H}$) entraîne donc :

$$\|\ell_v(\mu_v Q)\|_v > \exp(- C(\log \log H_{\tilde{X}}(Q))^{\varkappa_1}\, p_v^{\varkappa_2}\, \mu_v^{2\varkappa_3}\, (\log C_5)^{\varkappa_3}) .$$

Or on a, pour tout élément $Q$ de $A_0(F)$ , $d_v(e , Q) \geqslant d_v(e , \mu_v Q)$ . La propriété 3(ii) permet alors de conclure.

## 2.3. Dénominateurs des points rationnels des courbes algébriques.

Soient $\Gamma$ une courbe algébrique projective irréductible de genre $\geqslant 1$, définie sur un corps de nombres $F$ , et $\varphi$ un élément non constant du corps $F(\Gamma)$ des fonctions rationnelles sur $\Gamma$ , définies sur $F$ . Pour tout point $Q$ de $\Gamma(F)$ non

Pôle de $\varphi$ , nous notons $P(\text{dén}\,\varphi(Q))$ le plus grand facteur premier du dénominateur de $\varphi(Q)$ , et $H_\varphi(Q)$ la hauteur (relativement à $F$ ) de $\varphi(Q)$ . D'après le théorème de Siegel-Mahler-Lang [6], les points $Q$ de $\Gamma(F)$ , tels que $P(\text{dén}\,\varphi(P))$ soit borné, sont de hauteur $H_\varphi$ bornée, et forment donc un ensemble fini. Le corollaire 1 permet de préciser ce théorème sous la forme suivante.

COROLLAIRE 2 [sous (*)]. - Il existe deux nombres réels $c$ et $\varkappa > 0$ , ne dépendant que de $\Gamma$ , $F$ et $\varphi$ , tels que, pour tout point $Q$ de $\Gamma(F)$ non pôle de $\varphi$ , on ait :

$$P(\text{dén}\,\varphi(Q)) > c(\log H_\varphi(Q))^{\varkappa} .$$

Démonstration. - Supposons tout d'abord l'assertion établie lorsque $\Gamma$ est non singulière. Elle sera alors vraie pour toute courbe $\Gamma$ . Soit, en effet $\pi : \tilde{\Gamma} \mapsto \Gamma$ une normalisation de $\Gamma$ . La normalisée $\tilde{\Gamma}$ est non singulière, et définie sur une extension finie $F'$ de $F$ . Le corollaire 2, appliqué à l'élément $\tilde{\varphi} = \varphi \circ \pi$ de $F'(\tilde{\Gamma})$ , entraîne, pour tout point $\tilde{Q}$ de $\tilde{\Gamma}(F')$ non pôle de $\tilde{\varphi}$ ,

$$P(\text{dén}(\varphi \circ \pi\ (\tilde{Q}))) > c'(\log H'_{\varphi\circ\pi}\ (\tilde{Q}))^{\varkappa'} ;$$

la hauteur $H'$ est ici prise relativement à $F'$ , et vérifie, pour tout élément $\beta$ de $F$ : $H'(\beta) = H(\beta)^{[F':F]}$ . On conclut en notant que le morphisme $\pi$ est surjectif.

Soit donc $\varphi$ une fonction rationnelle non constante sur la courbe lisse $\Gamma$ . Ses différents pôles $P_1 , \dots , P_m$ sont définis sur une extension finie $F''$ de $F$ . D'après la formule sur les hauteurs rappelée plus haut, on peut, sans perte de généralité, supposer que $F'' = F$ . Soit par ailleurs $A$ la jacobienne de la courbe $\Gamma$ . C'est une variété abélienne définie sur $F$ , et pour laquelle nous reprenons les notations du § 1.1. Pour $j = 1 , \dots , m$ , nous notons $\psi_j$ le plongement de $\Gamma$ dans $A$ tel que $\psi_j(P_j) = e$ , et $\nu_j$ l'ordre du pôle $P_j$ de $\varphi$ . Nous allons associer à toute place $v$ de $F$ un nombre réel $\gamma_v$ ne dépendant que de $F$ , $\Gamma$ et $\varphi$ , et tel que, pour tout point $Q$ de $\Gamma(F)$ :

(i) $|\varphi(Q)|_v > \gamma_v \Rightarrow |\varphi(Q)|_v \leq \gamma_v \sup_{j=1,\dots,m} (\inf_{i=1,\dots,n} |x_i \circ \psi_j(Q)^{-\nu_j}|_v)$.

(ii) $\gamma_v = 1$ pour $v$ suffisamment grand.

Cette seconde condition, qui est fondamentale pour l'application que nous avons en vue, signifie que, pour un entier $p_0$ effectivement calculable en fonction de $\Gamma$ , $\varphi$ et $F$ , on a $\gamma_v = 1$ dès que $p_v > p_0$ , et ce indépendamment du point $Q$ .

Le corollaire 2 se déduit aisément de (i) et (ii) ; posons :

$$P = P(\text{dén}\,\varphi(Q)) \ ; \quad \gamma = \prod_{v\in\mathfrak{M}_F} \gamma_v = \prod_{p_v\leq p_0} \gamma_v \ ; \ \nu = \sup_{j=1,\dots,m} \nu_j .$$

Dès que $p_v > P$ (voir [1], III), $\varphi(Q)$ est un entier $v$-adique. En conséquence (i) entraîne :

$$H_\varphi(Q) = \prod_{v\in\mathfrak{M}_F} \sup(1 , |\varphi(Q)|_v)^{\delta_v} \leq \gamma \prod_{p_v\leq P} \sup[1 , \sup_{j=1,\dots,m} d_v(e , \psi_j(Q)^{-\nu_j}]^{\delta_v} .$$

Désignons par $c_1$ , $c_2$ , $c_3$ des nombres réels $> 0$ ne dépendant que de $\Gamma$ , $\varphi$ et $F$ . Les hauteurs associées à $\varphi$ et au plongement $\tilde{x} \circ \psi_j$ étant, à une puissance près, quasi équivalentes (voir [6], propriété 5 et § 5), on déduit du corollaire 1, appliqué à la jacobienne de $\Gamma$ :

$$H_\varphi(Q) \leqslant c_1 \exp(c_2 \, \nu\delta \, (\log\log H_\varphi(Q))^{\varkappa_1} \textstyle\sum_{p_v \leqslant P} p_v^{\varkappa_4}) ,$$

soit

$$H_\varphi(Q) \leqslant \exp(c_3 \, (\log\log H_\varphi(Q))^{\varkappa_1} \, (P(\text{dén}\, \varphi(Q)))^{\varkappa_4+1}) .$$

L'inégalité du corollaire 2 en résulte.

Les propriétés (i) et (ii) peuvent s'interpréter dans le langage des distributions de Weil. Nous en donnons ci-dessous une démonstration directe.

Les points $P_1 , \dots , P_m$ étant simples, il existe un élément $t$ de $F(\Gamma)$ les admettant chacun pour zéro d'ordre 1 (autrement dit, $t$ est une uniformisante locale en chacun de ces points). Si $f \in K(\Gamma)$ , et si, pour $j = 1 , \dots , m$ , on désigne par $\omega_j$ l'ordre de $f$ au point $P_j$ , il existe une série de Laurent à coefficients dans $K$ :

$$f_j(T) = \textstyle\sum_{n \geqslant \omega_j} a_{j,n} T^n ,$$

et, pour toute place $v$ de $F$ , un voisinage $V_{j,v}$ de $P_j$ dans $\Gamma(F_v)$ , tels que

$$\forall \; Q \in V_{j,v} , \quad f_j(t(Q)) = f(Q) .$$

On déduit de ces relations (appliquées aux fonctions $\varphi$ et $x_i \circ \psi_j$) l'existence de trois constantes $\gamma'_v$ , $\gamma''_v$ , $\gamma'''_v$ telles que :

- si $Q \in \bigcup_{j=1,\dots,m} V_{j,v}$ : $|\varphi(Q)|_v < \gamma'_v$
- dans le cas contraire, $\exists \; j \in [1, \dots , m]$ tel que $|\varphi(Q)|_v < \gamma''_v \, |t(Q)|_v^{-\nu_j}$ , et, $\forall \; i = 1 , \dots , n$ , $|x_i \circ \psi_j(Q)|_v < \gamma'''_v \; |t(Q)|_v$ .

La propriété (i) en résulte. Pour établir (ii), nous faisons appel au <u>théorème d'Eisenstein</u> (voir [11], VIII, exercice n° 236), en vertu duquel, pour $v$ suffisamment grand (en fonction de $\Gamma$ , $f$ et $t$ ), les coefficients $a_{j,n}$ des développements mentionnés plus haut sont tous entiers $v$-adiques ; les fonctions $f$ et $t$ appartiennent à $F(\Gamma)$ , les séries $f_j$ sont en effet algébriques sur $F(t)$ . Pour $v$ suffisamment grand, $a_{j,\omega_j}$ est de plus une unité $p$-adique , et l'on a :

$$0 < |t(Q)|_v < 1 \Longrightarrow |f_j(t(Q))|_v = |t(Q)|_v^{\omega_j} .$$

D'autre part, tous les pôles de $\varphi$ étant par construction pôles de la fonction $t^{-1}$ , la fonction $\varphi$ est entière sur $F[t^{-1}]$ , et donc, pour $v$ suffisamment grand sur $\mathcal{O}_v[t^{-1}]$ . Par conséquent, la relation $|\varphi(Q)|_v > 1$ entraîne $|t(Q)|_v < 1$ . Mais, si $S_\varphi(t , X)$ désigne le polynôme minimal de $X$ sur $F(t)$ , et si $|t(Q)|_v < 1$ , les seuls zéros de l'équation $S_\varphi(t(Q) , X) = 0$ , de valeur absolue $v$-adique $> 1$ , sont les nombres $\varphi_1(t(Q))$ , $\dots$ , $\varphi_m(t(Q))$ , où $\varphi_j$ désigne le développement de Laurent de $\varphi$ en $P_j$ . Lorsque $|\varphi(Q)|_v > 1$ , il existe donc un indice $j \in [1, \dots, m]$ tel que :

$$\varphi(Q) = \varphi_j(t(Q)) ,$$

d'où

$$|\varphi(Q)|_v = |t(Q)|_v^{-\nu_j} .$$

Un raisonnement similaire permettrait de montrer que, sous les mêmes hypothèses,

$$\forall\ i = 1, \dots, n,\ j = 1, \dots, m,\ |x_i \circ \psi_j(Q)|_v \leqslant |t(Q)|_v .$$

Ainsi, pour $v$ suffisamment grand, l'inégalité $|\varphi(Q)|_v > 1$ entraîne :

$$\exists\ j \in [1, \dots, m] ;\ \forall\ i = 1, \dots, n,\ |\varphi(Q)|_v \leqslant |x_i \circ \psi_j(Q)|_v^{-\nu_j} .$$

La condition (ii) est donc bien vérifiée, et le corollaire 2 est démontré.

EXEMPLE (courbes de Fermat ; voir également [9], [2]). - Soit $\ell$ un nombre prêmier impair. D'après le corollaire 2, il existe deux nombres réels $c_\ell$ et $\varkappa_\ell > 0$, ne dependant que de $\ell$, tels que, si $x_1$, $x_2$, $x_3$ désignent trois entiers dont la somme des puissances $\ell$-ièmes est nulle, leurs plus grands facteurs premiers $P(x_i)$ vérifient :

$$\forall\ i = 1, 2, 3,\ P(x_i) > c_\ell\ (\log X)^{\varkappa_\ell} ,$$

où $X = \max_{i=1,2,3} |x_i|_\infty$.

On notera que le seul point ineffectif de la démarche présentée ici réside dans la détermination des générateurs du groupe des points rationnels de la jacobienne de $\Gamma$, la constante $c$ étant fonction de leurs hauteurs (la constante $\varkappa$ ne dépend elle-même que du rang du groupe).

BIBLIOGRAPHIE


[1] BERTRAND (D.). - Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe, Compositio Math. (à paraître).

[2] BERTRAND (D.) and FLICKER (Y.). - Linear forms on abelian varieties over local fields (en préparation).

[3] BOREL (A.). - Linear algebraic groups. - New York, W. A. Benjamin, 1969 (Mathematics Lecture Note Series).

[4] BOURBAKI (N.). - Groupes et algèbres de Lie, Chap. 2 et 3. - Paris, Hermann, 1972 (Act. scient. et ind. 1349 ; Bourbaki, 37).

[5] COATES (J.) and LANG (S.). - Diophantine approximation on abelian varieties with complex multiplication, Invent. Math., Berlin, t. 34, 1976, p. 129-133.

[6] LANG (S.). - Integral points on curves. - Paris, Presses Universitaires de France, 1960 (Institut des Hautes Etudes Scientifiques, Publications mathématiques, 6, p. 27-43).

[7] LANG (S.). - Diophantine approximation on abelian varieties with complex multiplication, Advances in Math., t. 17, 1975, p. 281-336.

[8] LANG (S.). - Higher dimensional diophantine problems, Bull. Amer. math. Soc., t. 80, 1974, p. 779-787.

[9] MASSER (D.). - Linear forms in algebraic points of abelian functions, III,

Proc. London math. Soc., series 3, t. 33, 1976, p. 549-564.

[10] MASSER (D.). - On the period of abelian functions in two variables, Mathematika, London, t. 22, 1975, p. 97-107.

[11] POLYA (G.) und SZEGO (G.). - Aufgaben und Lehrsätze aus der Analysis, II. - Berlin, Springer-Verlag, 1925 (Grundlehren der mathematischen Wissenschaften, 20).

[12] SHIMURA (G.) and TANIYAMA (Y.). - Complex multiplication of abelian varieties and its applications to number theory. - Tokyo, The Mathematical Society of Japan, 1961 (Publications of the Mathematical Society of Japan, 6).

[13] WALDSCHMIDT (M.). - Nombres transcendants et groupes algébriques, Cours Peccot, Collège de France, 1977.

(Texte reçu le 17 octobre 1977)

Daniel BERTRAND
Centre de Mathématiques
Ecole polytechnique
91128 PALAISEAU CEDEX