Daniel Bertrand

Points algébriques sur les courbes elliptiques p-adiques de Tate

Groupe de travail d'analyse ultramétrique, tome 2 (1974-1975), exp. n° 1, p. 1-13
<http://www.numdam.org/item?id=GAU_1974-1975__2__A1_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, P. ROBBA)
2e année, 1974/75, n° 1, 13 p.

14 octobre 1974

POINTS ALGÉBRIQUES SUR LES COURBES ELLIPTIQUES p-ADIQUES DE TATE

par Daniel BERTRAND

En 1949, SCHNEIDER [5] démontrait un critère de transcendance sur les valeurs de fonctions méromorphes sur $\underset{\sim}{C}$, qui admet comme corollaires les propositions suivantes, où $\wp$ (resp. $\wp^*$) désigne une fonction elliptique de Weierstrass, d'invariants g_2 et g_3 (resp. g_2^* et g_3^*) , et t un nombre complexe non pôle de $\wp$ (resp. $\wp^*$) :

PROPOSITION A. - <u>L'un au moins des quatre nombres</u> g_2 , g_3 , t , $\wp(t)$ <u>est transcendant</u>.

PROPOSITION B. - <u>L'un au moins des quatre nombres</u> g_2 , g_3 , e^t , $\wp(t)$ <u>est transcendant</u>.

PROPOSITION C. - <u>Si</u> $\wp$ <u>et</u> $\wp^*$ <u>sont algébriquement indépendants sur</u> $\underset{\sim}{C}$, <u>l'un au moins des six nombres</u> g_2 , g_3 , g_2^* , g_3^* , $\wp(t)$, $\wp^*(t)$ <u>est transcendant</u>.

Aucune de ces proposition ne connaît, pour l'instant, de traduction dans le domaine p-adique. Nous nous proposons d'aborder ce problème au moyen d'un critère "local" de transcendance bien adapté à l'étude des fonctions elliptiques p-adiques.

I. Un critère de transcendance

1. Enoncé.

Nous utiliserons les notations suivantes.

- p désigne un nombre premier, C_p un corps valué non archimédien complet, algébriquement clos, de caractéristique 0 et de caractéristique résiduelle p (par exemple, $C_p = \underset{\sim}{C}_p$, complété de la clôture algébrique de $\underset{\sim}{Q}_p$). On note $|.|$ la valeur absolue de C_p , normalisée par $|p| = p^{-1}$.

- K est une extension algébrique de $\underset{\sim}{Q}$, de degré fini, plongée dans C_p . On appelle taille d'un élément x de K , et on note $s(x)$, le logarithme du maximum de son plus petit dénominateur et des valeurs absolues archimédiennes de ses conjugués.

- soient $\mathbb{D}$ un disque non circonférencié de C_p , et $\underset{\sim}{f} = (f_1 , \ldots , f_\ell)$ une application méromorphe de $\mathbb{D}$ dans C_p^ℓ ; on appelle <u>point algébrique</u> (resp. <u>K-point</u>) de $\underset{\sim}{f}$ tout élément u de $\mathbb{D}$ tel que $\underset{\sim}{f}(u)$ ait des coordonnées algébriques sur $\underset{\sim}{Q}$ (resp. des coordonnées dans K) . Sur l'ensemble des K-points de $\underset{\sim}{f}$, on définit la fonction :

$$t(u) = \sup_{1 \leq i \leq \ell} s(f_i(u)) .$$

Ces définitions étant posées, nous pouvons énoncer le critère de transcendance suivant :

"CRITÈRE LOCAL". - Si l'application $\underset{\sim}{f}$ vérifie les conditions suivantes :

(C_1) la dérivation d/dz opère sur le corps $K(\underset{\sim}{f})$.

(C_2) il existe une suite $\{u_n\}_{n \in \mathbb{N}}$ de K-points distincts de $\underset{\sim}{f}$, situés dans un disque Δ strictement inclus dans Ω , telle que la suite $t(u_n)/n$ soit bornée,

alors, le degré de transcendance du corps $K(\underset{\sim}{f})$ sur K est inférieur ou égal à 1.

ADAMS [1] a démontré ce critère local dans le cas particulier où la dérivation d/dz opère sur l'espace vectoriel engendré sur K par $1, f_1, \dots, f_\ell$ (On obtient alors comme corollaire de traduction p-adique des théorèmes de Hermite-Lindemann et de Gel'fond-Schneider). Dans le cas où la dérivation opère sur l'algèbre $K[f_1, \dots, f_\ell]$ (cas auquel nous ramènerons la condition (C_1)), il imposait à la suite $\{u_n\}$ la condition : $t(u_n)/n \longrightarrow 0$.

Remarquons que l'hypothèse (C_2) peut être formulée sous la forme plus maniable suivante : il existe un disque Δ strictement inclus dans Ω tel que, pour tout réel X positif suffisamment grand, le cardinal $\nu(X)$ de l'ensemble :

$$\{u \in \Delta \ ; u \text{ K-point de } \underset{\sim}{f} , \ t(u) \leq X\}$$

vérifie : $\nu(X)/X$ est minoré par une constante strictement positive.

Enfin, la condition (C_1) peut être remplacée par la condition :

(C_1') la dérivation $z(d/dz)$ opère sur le corps $K(\underset{\sim}{f})$.

C'est cette condition que vérifieront les fonctions elliptiques p-adiques de Tate étudiées au III, 1.

2. Esquisse de la démonstration.

Nous raisonnerons par l'absurde, en supposant que deux des fonctions $f_1, \dots, f_\ell$, soient f_1 et f_2 , sont algébriquement indépendantes sur K .

Posons $T_n = \max(n , \sup_{1 \leq j \leq n} t(u_j))$, et soit N un entier arbitrairement grand.

1er pas : le lemme de Siegel permet de construire une fonction $F = F_N$ s'exprimant comme un polynôme non nul en f_1 et f_2 à coefficients entiers algébriques dans K soumis à certaines majorations $(\mathfrak{M}_N)$, et qui vérifie :

$$F^{(k)}(u_N) = 0 , \quad \forall\ k = 0 , \dots , S - 1 \quad \text{avec} \quad S = [\exp T_N] + 1 .$$

2e pas : f_1 et f_2 étant algébriquement indépendants sur K , la fonction F n'est pas identiquement nulle, et on peut définir, pour tout $n \geq N$, le plus petit ordre de dérivation, soit σ_n , tel que :

$$\gamma_n = F^{(\sigma_n)}(u_n) \neq 0 .$$

3e pas : un "lemme de Schwarz" p-adique permet, pour tout $n \geq N$, de relier le nombre de zéros de F (comptés avec leur ordre de multiplicité) à $|\gamma_n|$, donc, γ_n étant un élément de K, à $s(\gamma_n)$. Plus précisément, on montre au moyen de la condition (C_1) (resp. (C_1')) et des majorations $(\mathfrak{M}_N)$, qu'il existe une constante α, indépendante de N et n, telle que les inégalités

$$(\mathfrak{I}_n) \qquad \sum_{i\geq N} \sigma_i \leq \alpha(\sigma_n \log(\sigma_n + S^{3/4}) + (\sigma_n + S^{3/4})T_n)$$

soient satisfaites pour tout $n \geq N$.

4e pas : la fonction non nulle F, étant méromorphe dans Ω, et la suite $\{u_n\}$ contenue dans Δ, la suite σ_n est nulle pour n suffisamment grand (cf. LAZARD [4]). Les conditions initiales $S^{3/4} < S = [\exp T_N] + 1 \leq \sigma_N$ et le fait que la suite $\{\exp T_n\}$ soit croissante permettent donc de définir le plus petit entier, soit $M \geq N$ tel que :

$$\forall\, n > M , \quad \sigma_n < \exp T_n ,$$

et le plus petit entier, soit $L \geq M$, tel que :

$$\forall\, n , \quad M < n \leq L , \quad S^{3/4} < \sigma_n < \exp T_n .$$

5e pas : le but essentiel de ce qui suit consiste à montrer que l'intervalle (M , L) est grand par rapport à M. Les inégalités $(\mathfrak{I}_N)$ entraînent,

pour $n = L + 1$

$$\exp T_M < \sigma_M \leq \sum_{i\geq N} \sigma_i \leq \alpha(\sigma_{L+1} \log(\sigma_{L+1} + S^{3/4}) + (\sigma_{L+1} + S^{3/4})T_{L+1})$$
$$\leq 3\alpha S^{3/4}\, T_{L+1} \leq 3\alpha \exp(3T_M/4)\, T_{L+1} ,$$

d'après la définition de S et L. D'où :

$$(*) \qquad \exp(T_M/4) \leq 3\alpha T_{L+1} ;$$

pour $n \in [M + 1 , L]$:

$$\sum_{i=M+1}^{L} \sigma_i \leq \alpha \times 4\sigma_n T_n ,$$

d'où l'on tire :

$$(**) \qquad \sum_{n=M+1}^{L} 1/T_n \leq 4\alpha .$$

6e pas : la condition (C_2) montre qu'il existe une constante $\beta \geq 1$ telle que, pour tout entier n, on ait :

$$n \leq T_n \leq \beta n .$$

D'après $(*)$, on a alors $\exp(M/4) \leq 3\alpha\beta(L + 1)$, soit

$$\log(L + 1) \geq \frac{M}{4} - \log(3\alpha\beta) .$$

D'autre part, $(**)$ entraîne

$$\sum_{M+1}^{L} \frac{1}{n} = \log L - \log M + O(\tfrac{1}{M}) \leq 4\alpha\beta .$$

La comparaison de ces deux dernières inégalités fournit pour N, donc M, suffisamment grand, une contradiction.

II. Démonstration du critère

En vue des applications, nous allons démontrer le critère en supposant remplie la condition (C_1'). Par ailleurs, on peut alors se ramener à l'hypothèse :

(C_1'') la dérivation $D = z(d/dz)$ opère sur l'algèbre $K[\underset{\sim}{f}]$.

En effet, il existe, en vertu de (C_1'), $\ell + 1$ polynômes de $K[X_1, \dots, X_\ell]$, soient Q et P_i, $i = 1, \dots, \ell$, tels que :

$$Df_i = \frac{P_i(f_1, \dots, f_\ell)}{Q(f_1, \dots, f_\ell)}, \quad i = 1, \dots, \ell .$$

Posons alors $f_{\ell+1} = Q(f_1, \dots, f_\ell)^{-1}$. Il est facile de voir que D opère sur l'algèbre $K[f_1, \dots, f_{\ell+1}]$. Mais la fonction $Q(f_1, \dots, f_\ell)$, méromorphe dans $\mathbb{C}$, et non nulle, n'admet qu'un nombre fini de zéros dans tout disque strictement inclus dans $\mathbb{C}$ (cf. LAZARD [4]), et tous les points de la suite $\{u_n\}$, sauf un nombre fini, sont encore des K-points de $\{f_1, \dots, f_{\ell+1}\}$. La condition (C_2) permet enfin de vérifier que $s(f_{\ell+1}(u_n))/n$ est bornée. Nous pourrons donc désormais nous placer sous l'hypothèse (C_1'').

Nous reprenons dans ce qui suit les notations de I,2.

1. Construction de la fonction auxiliaire F_N.

Le résultat suivant regroupe toutes les majorations dont nous aurons besoin.

LEMME 1. - Soit τ un réel supérieur à 1, P un polynôme non nul à deux variables, de degré R en chaque variable, à coefficients entiers algébriques dans le corps de nombres K, de tailles majorées par τ. Alors la fonction F, définie par $F = P(f_1, f_2)$, vérifie, en tout point u_n de la suite de K-points de $\underset{\sim}{f}$, et pour tout entier k,

(i) $D^k F(u_n) \in K$,

(ii) il existe une constante γ_1 ne dépendant que des équations différentielles (C_1') telle que :

$$s(D^k F(u_n)) \leq \tau + k \log \gamma_1(k + R) + \ell T_n(\gamma_1 k + R) + 2 \log(1 + R) .$$

Démonstration. - Elle se fait par récurrence à partir de cas $k = 0$ (cf. LANG [3], lemme 1 ; WALDSCHMIDT [10], exercice 3.3.e).

Le principe des tiroirs de Dirichlet permet alors de construire la fonction F_N définie au 1er pas. De façon précise, on a le lemme suivant.

LEMME 2. - Soit $R = [S^{3/4}]$. Il existe une constante γ_2 indépendante de N, et un polynôme non nul $P_N(X_1, X_2) = \sum_{0\leq\lambda_1,\lambda_2\leq R} p_{\lambda_1,\lambda_2} X_1^{\lambda_1} X_2^{\lambda_2}$, dont les coefficients sont des entiers de K, de taille majorée par τ_N, avec

$$\tau_N < \gamma_2 S^{1/2} \log S$$

et tel que la fonction $F_N : P_N(f_1, f_2)$ vérifie :

$$D^k F_N(u_n) = 0 , \quad \forall k = 0, \dots, S-1 , \text{ avec } S = [\exp T_N] + 1 .$$

Démonstration. - Il s'agit de résoudre, dans l'anneau des entiers de K, un système de S équations à $(R+1)^2$ inconnues p_{λ_1,λ_2}, dont les coefficients $D^k f_1^{\lambda_1} f_2^{\lambda_2}(u_n)$, $k = 0, \dots, S-1$, $0 \leq \lambda_1, \lambda_2 \leq R$, sont des nombres algébriques dans K, de tailles majorées, d'après le lemme 1, par

$$S \log \gamma_1(S+R) + \ell T_N(\gamma_1 S + R) .$$

Or $(R+1)^2 = ([S^{3/4}]+1)^2$ est supérieur à S pour N, donc S suffisamment grand. D'après un lemme classique de Siegel, il existe alors une solution non triviale p_{λ_1,λ_2} dans l'anneau des entiers de K, vérifiant :

$$\sup_{\lambda_1,\lambda_2;\sigma:K\subseteq\underset{\sim}{C}} |\sigma(p_{\lambda_1,\lambda_2})|_\infty \leq [\sqrt{2}(R+1)^2 (\gamma_1 S)^{2(\ell+1)\gamma_1 S}]^{S/((R+1)^2-S)}$$

(car $S = [\exp T_N] + 1$). D'où

$$s(p_{\lambda_1,\lambda_2}) \leq \frac{2(\ell+1)\gamma_1 S.\log S}{S^{1/2}} < \gamma_2 S^{1/2} \log S .$$

2. Démonstration des inégalités $(\mathfrak{J}_N)$.

Ces inégalités traduisent un principe du maximum, que nous rappelons sous la forme suivante :

LEMME 3. - Soient $r > \rho > 0$ deux réels, a un élément de C_p non nul, φ une fonction non identiquement nulle, analytique sur le disque circonférencié

$$B = B(a, r^+) ,$$

ν le nombre de ses zéros (comptés avec leur ordre de multiplicité) dans le disque circonférencié $\Delta^\circ = B(a, \rho^+)$. Soit k le plus petit entier tel que $D^k \varphi(a)$ soit non nul. Alors :

(i) k est le plus petit entier tel que $(d^k/dz^k)\varphi(a)$ soit non nul (i. e. c'est l'ordre de φ en a).

(ii) on a, en posant : $|\varphi|_B = \sup_{|z-a|\leq r} |\varphi(z)|$:

$$\nu \leq \frac{1}{\log(r/\rho)} [\log|\varphi|_B - \log|D^k \varphi(a)| + k(\log|a| - \log \rho)] .$$

Démonstration. - On démontre aisément par récurrence que, si a est non nul, les assertions

$$\langle\!\langle (z(d/dz))^h \varphi(a) = 0 , \quad \forall h = 0, \dots, k-1 \rangle\!\rangle$$

et

$$\ll (d/dz)^h \varphi(a) = 0 \ , \ \forall\ h = 0 \ , \ \ldots \ , \ k-1 \gg$$

sont équivalentes. On a alors :

$$D^k \varphi(a) = a^k (d^k/dz^k)\ \varphi(a) \ ,$$

d'où

$$(d^k/dz^k)\varphi(a) = a^{-k}\ D^k\ \varphi(a) \neq 0 \ .$$

La fonction φ ayant ainsi un zéro d'ordre k au point a, la fonction

$$\Psi(z) = \varphi(z)/(z-a)^k$$

est encore analytique sur B. Elle admet $\nu - k$ zéros dans Δ°. D'après le lemme de Schwarz p-adique (cf. SERRE [8]), on a donc :

$$|\Psi(a)| \leqslant (\frac{\rho}{r})^{\nu-k}\ |\Psi|_B \ .$$

Or $(d^k/dz^k)\ \varphi(a) = k!\ \Psi(a)$, et $|\varphi|_B = r^k\ |\Psi|_B$ d'après l'inégalité ultramétrique. Ainsi :

$$|a|^{-k}.|D^k\ \varphi(a)| \leqslant (\frac{r}{\rho})^{-\nu}\ (\frac{1}{\rho})^k\ |\varphi|_B \ ,$$

ce qui est l'inégalité désirée.

Nous allons appliquer le lemme 3 à une fonction analytique déduite de F_N, et en chacun des points u_n, $n \geq N$.

En vertu de la densité du groupe de valeurs de C_p dans $\underset{\sim}{R}^+$, il existe deux disques circonférenciés $\Delta^\circ \subsetneqq B$ de rayons respectifs ρ et r, contenant le disque Δ défini par la condition (C_2), et strictement inclus dans le disque non circonférencié $\mathbb{D}$. Les fonctions f_1 et f_2 étant méromorphes dans $\mathbb{D}$ n'ont qu'un nombre fini de zéros et de pôles dans B. Pour N suffisamment grand, elles n'admettent donc pas les points de la suite $\{u_n\}_{n\geqslant N}$ comme zéros (ni comme pôles, par hypothèse). Pour $i = 1, 2$, soit θ_i le polynôme diviseur des pôles de f_i dans B. Alors les fonctions θ_i et $\theta_i\ f_i$ sont analytiques dans B, n'admettent pas les points $\{u_n\}_{n\geqslant N}$ comme zéros, et n'ont aucun zéro commun. Ceci permet de définir les constantes réelles :

$$A_i = \log|\theta_i\ f_i|_B \ ; \quad B_i = \log|\theta_i|_\Delta$$

$$C_i = \inf_{z\in B}(|\theta_i\ f_i(z)| + |\theta_i(z)|) \ , \quad C_i > 0 \ .$$

Dans ces conditions, considérons la fonction $G_N = \theta_1^R\ \theta_2^R\ F_N$. Elle est analytique sur B, et si σ_n désigne l'ordre de F_N en u_n, c'est aussi l'ordre de G_N en u_n, donc, par le lemme 3, (i), le plus petit entier tel que : $D^{\sigma_n}\ G_N(u_n) \neq 0$.

Soit ν le nombre de zéros de G_N (comptés avec leur multiplicité) de G_N dans Δ°. La construction précédente entraîne :

$$\Sigma_{i\geqslant N}\ \sigma_i \leqslant \nu \ .$$

Pour N suffisamment grand, les points $\{u_n\}_{n\geq N}$ sont non nuls. Par ailleurs, ils sont tous centres des disques $\overset{\circ}{\Delta}$ et B. Soit alors n un entier supérieur ou égal à N. Le lemme 3, appliqué à la fonction $\varphi = G_N$ au point $a = u_n$, entraîne :

$$\nu \leq \frac{1}{\log(r/\rho)} [\log|\theta_1^R \theta_2^R F_N|_B - \log|\theta_1^R \theta_2^R D^{\sigma_n} F_N(u_n)| + \sigma_n(\log|u_n| - \log r)] .$$

(En effet, la définition de σ_n montre que $D^{\sigma_n} G_N(u_n) = \theta_1^R(u_n)\ \theta_2^R(u_n)\ D^{\sigma_n} F_N(u_n)$.)

Il reste à majorer le terme de droite de cette inégalité. Les constantes $\gamma_3, \dots, \gamma_6$ et α, écrites ci-dessous, sont aisément calculables à partir de $\gamma_1, \gamma_2, A_i, B_i$ et C_i. <u>Elles sont donc indépendantes de</u> N <u>et</u> n.

(α) $\log|\theta_1^R \theta_2^k F_N|_B \leq R(A_1 + A_2 + B_1 + B_2) \leq \gamma_3\, S^{3/4}$.

(β) On a, d'après la définition de C_i,

$$|\theta_i(u_n)| \geq C_i/[2 \sup(1, |f_i(u_n)|)] , \text{ pour } i = 1, 2 .$$

Mais $f_i(u_n)$ est un élément de K. Si δ désigne son dénominateur, on a

$$|\delta . f(u_n)| \leq 1 .$$

La formule du produit dans $\underset{\sim}{Q}$ entraîne $\delta.|\delta| \geq 1$, d'où $|f(u_n)| \leq \delta$, ce qui implique, d'après la définition de la taille d'un élément de K :

$$\log|f(u_n)| \leq \log \delta \leq s(f(u_n)) \leq t(u_n) \leq T_n .$$

En conséquence

$$- \log|\theta_1^R(u_n)\ \theta_2^R(u_n)| \leq R(-\log \frac{C_1 C_2}{4} + 2T_n)$$
$$\leq \gamma_4\, S^{3/4}\, T_n .$$

(γ) $D^{\sigma_n} F_N(u_n)$ est un élément de K non nul par définition. Il vérifie donc l'inégalité fondamentale (cf. SERRE [7], §1)

$$- 2[K : \underset{\sim}{Q}]\, s(D^{\sigma_n} F_N(u_n)) \leq \log|D^{\sigma_n} F_N(u_n)| .$$

D'où, en vertu du lemme 2,

$$- \log|D^{\sigma_n} F_N(u_n)| \leq 2[K:\underset{\sim}{Q}][T_N + \sigma_n \log \gamma_1(\sigma_n + R) + \ell T_n(\gamma_1 \sigma_n + R) + 2\log(1+R)]$$
$$\leq \gamma_5(\sigma_n \log(\sigma_n + S^{3/4}) + (\sigma_n + S^{3/4})T_n) .$$

(δ) Enfin, $\sigma_n(\log|u_n| - \log r) \leq \sigma_n(\log \delta - \log r) \leq \gamma_6\, \sigma_n$.

En regroupant ces différentes inégalités, on obtient :

$$\nu \leq \frac{1}{\log(r/\rho)} [(\gamma_3 + \gamma_4 T_n)S^{3/4} + \gamma_5(\sigma_n \log(\sigma_n + S^{3/4}) + (\sigma_n + S^{3/4})T_n) + \gamma_6\, \sigma_n].$$

Ainsi,

$$\sum_{i\geq N} \sigma_i \leq \alpha(\sigma_n \log(\sigma_n + S^{3/4}) + (\sigma_n + S^{3/4})T_n) ,$$

ce qui, pour n décrivant l'ensemble des entiers supérieurs à N, fournit les inégalites $(\mathfrak{J}_N)$, et permet, au moyen des 4e, 5e et 6e pas, de conclure la démonstration de critère de transcendance local.

III. Application aux fonctions elliptiques p-adiques

Un premier type de "fonctions elliptiques" p-adiques a été introduit par Elisabeth LUTZ ([5], §2) pour paramétrer, au voisinage de son élément neutre, une courbe elliptique définie sur un corps ultramétrique complet C_p. Pour $p \neq 2, 3$, un isomorphisme de C_p-groupe de Lie permet de se ramener à l'étude des courbes algébriques planes (Γ) d'équation :

$$Y^2 = 4X^3 - g_2 X - g_3 \text{ , avec } \Delta = g_2^3 - 27g_3^2 \neq 0 \text{ .}$$

Si g_2 et g_3 sont des éléments de C_p algébriques sur $\underset{\sim}{Q}$, la démarche formelle suivante permet de retrouver les "fonctions elliptiques" de Lutz. Soit σ un plongement de $\overline{\underset{\sim}{Q}}$ dans $\underset{\sim}{C}$, et $\wp$ la fonction elliptique de Weierstrass complexe d'invariants $\sigma(g_2)$ et $\sigma(g_3)$. L'application $\underset{\sim}{C}$-méromorphe

$$z \longrightarrow (\wp(z) \text{ , } \wp'(z))$$

définit une représentation paramétrique de $\Gamma_{\underset{\sim}{C}}$, ensemble des points $\underset{\sim}{C}$-rationnels de (Γ). Au développement de Laurent de $\wp$ au voisinage de 0 :

$$\wp(z) = \frac{1}{z^2} + \frac{\sigma(g_2)}{20} z^2 + \frac{\sigma(g_3)}{28} z^4 + \dots \text{ ,}$$

on associe l'élément de $C_p((z))$:

$$\wp_p(z) = \frac{1}{z^2} + \frac{g_2}{20} z^2 + \frac{g_3}{28} z^4 + \dots \text{ ,}$$

qui définit une fonction méromorphe sur un disque $\mathfrak{D}_{g_2,g_3}$ de C_p, de rayon strictement positif. C'est la fonction elliptique de Lutz.

Les applications $(z , \wp(z) , \wp'(z))$, $(e^z , \wp(z) , \wp'(z))$, $(\wp(z) , \wp'(z) , \wp^*(z) , \wp^{*\prime}(z))$ vérifient la condition (C_1) du critère de transcendance local, que l'on peut alors appliquer à l'étude de leurs points algébriques sur $\mathfrak{D}_{g_2,g_3}$.

Ce point de vue permet, dans le cas de multiplication complexe, de démontrer l'équivalent p-adique de la proposition A de Schneider. Nous y reviendrons ailleurs.

Nous donnons ici des corollaires du critère local concernant un autre type de fonctions elliptiques p-adiques, introduit par John TATE ([9], §6).

1. Rappels sur les courbes et les fonctions elliptiques de Tate.

Soient L une extension algébrique (finie ou non) de $\underset{\sim}{Q}_p$, H_L l'ensemble des fonctions holomorphes sur $\underset{\sim}{C}_p^*$, dont le développement de Laurent à l'origine a ses coefficients dans L, M_L son corps des fractions, et $F_L(q)$ le sous-corps de M_L formé par les fonctions multiplicativement périodiques de période q, où q désigne un élément de L^*, $|q| < 1$.

PROPOSITION 1. - Le corps $F_L(q)$ est un corps de fonctions sur L, de genre égal à 1.

La démonstration de cette proposition suit celle de l'énoncé similaire concernant les fonctions méromorphes sur $\underset{\sim}{C}$ admettant un réseau de période donné (voir à ce sujet ROQUETTE [4], §2).

Si x_0 (resp. y_0) désigne un élément de $F_L(q)$ admettant 1 comme pôle d'ordre 2 (resp. 3) , le théorème de Riemann-Roch entraîne que les 7 éléments

$$1 , x_0 , y_0 , x_0^2 , x_0 y_0 , y_0^2 , x_0^3$$

sont L-linéairement dépendants. Lorsque la caractéristique résiduelle p est différente de 2 ou 3 , on peut mettre la relation de dépendance sous la forme de Weierstrass :

$$(W) \qquad y^2 = 4x^3 - g_2 x - g_3 ,$$

où x et y sont les L-combinaisons linéaires de x_0 et y_0 . On a alors

$$F_L(q) = L(x_0 , y_0) = L(x , y) .$$

Comme dans le cas classique, les seuls générateurs de $F_L(q)$, liés par une relation de dépendance algébrique de la forme (W), sont du type : $x^* = \lambda^2 x$, $y^* = \lambda^3 y$, où λ désigne un élément de L^* . La relation s'écrit alors :

$$(W^*) \qquad y^{*2} = 4x^{*3} - g_2^* x^* - g_3^* , \text{ avec } g_2^* = \lambda^4 g_2 , \quad g_3^* = \lambda^6 g_3 .$$

Nous allons maintenant expliciter des générateurs x et y de $F_L(q)$. Soit Θ la fonction théta fondamentale :

$$\Theta(Z) = \prod_{n\geq 0}(1 - q^n Z^{-1}) \prod_{n<0}(1 - q^{-n} Z) .$$

On a $\Theta(q^{-1} Z) = - Z\Theta(Z)$.

Introduisons l'opérateur de dérivation $D = Z(d/dZ)$, qui laisse stable le corps $F_L(q)$. La fonction $\zeta(Z) = D\Theta(Z)/\Theta(Z)$ vérifie $\zeta(q^{-1} Z) = \zeta(Z) + 1$.

Posons alors $P(Z) = - D\zeta(Z)$. On vérifie aisément que la fonction P est un élément de $F_L(q)$, admettant 1 comme pôle d'ordre 2 . Le calcul donne :

$$P(Z) = \sum_{n\in\underset{\sim}{Z}} \frac{q^n Z}{(1 - q^n Z)^2} ,$$

et nous introduisons la fonction :

$$P_q(Z) = \sum_{n\in\underset{\sim}{Z}} \frac{q^n Z}{(1 - q^n Z)^2} + \frac{1}{12} - 2 \sum_{n\geq 1} \frac{q^n}{(1 - q^n)^2} .$$

D'où : $DP_q(Z) = \sum_{n\in\underset{\sim}{Z}} (q^n Z + q^{2n} Z^2)/(1 - q^n Z)^3$.

DP_q admet 1 comme pôle d'ordre 3 . Nous allons montrer que la relation liant P_q et DP_q est de la forme (W). Pour l'obtenir, introduisons l'uniformisante locale $T = \mathrm{Lg}\, Z$ au voisinage $D(1 , 1^-)$ de l'élément neutre de L^* . (Lg désigne dans toute la suite le logarithmique p-adique, et Exp l'exponentielle p-adique.)

On a $D = Z(d/dZ) = d/dT$, et un calcul explicite montre que le développement de $P_q(\mathrm{Exp}\, T)$ en série de fonctions méromorphes n'est autre, formellement, que celui de la fonction $(1/2i\pi)^2\, \wp_{1,\tau}(T/2i\pi)$, où $\wp_{1,\tau}$ désigne la fonction elliptique de

Weierstrass associée au réseau $(1\ ,\ \tau)$, avec $q = \exp 2i\pi\tau$. De

$$(\wp'_{1,\tau})^2 = 4(\wp_{1,\tau})^3 - g_2(1\ ,\ \tau)\wp - g_3(1\ ,\ \tau)\ ,$$

on tire

$$(DP_q)^2 = 4P_q^3 - g_2(q)\ P_q - g_3(q)$$

avec

$$g_2(q) \equiv (1/(2i\pi)^4)\ g_2(1\ ,\ \tau) = (1/12)E_4(q)$$
$$g_3(q) \equiv (1/(2i\pi)^6)\ g_3(1\ ,\ \tau) = -\ (1/216)E_6(q)$$

(le signe $\equiv$ désigne une égalité formelle ; le signe $=$, une égalité dans L), où $E_4(q)$ et $E_6(q)$ sont les séries d'Eisenstein normalisées d'ordre 2 et 3 .

L'invariant modulaire

$$J(q) = 1728(g_2(q)^3)/(g_2(q)^3 - 27g_3(q)^2) = 1728(E_4(q)^3)/(E_4(q)^3) - (E_6(q)^2)$$

est donc donné par la série convergente

$$J(q) = \frac{1}{q} + 744 + \sum_{n=1}^{+\infty} c(n)q^n\ ,$$

où les coefficients $c(n)$ sont les entiers rationnels intervenant dans le développement classique de $J(q)$. Ceci permet de montrer la proposition suivante.

PROPOSITION 2. – <u>L'invariant modulaire</u> J <u>définit une bijection</u> L-<u>analytique de l'ensemble</u> $\{q \in L^*\ ;\ |q| < 1\}$ <u>dans l'ensemble</u> $\{j \in L\ ,\ |j| > 1\}$.

Appelons <u>courbe elliptique de Tate</u> $\mathcal{E}_q$ le quotient $\overline{L}/q^{\mathbb{Z}}$, où $L = \mathbb{Q}_p(q)$, et $\overline{L}$ est la clôture algébrique de L . Nous avons vu que l'ensemble de ses points L-rationnels est isomorphe à l'ensemble des points L-rationnels de la cubique (Γ) , définie par (W). Pour $p \neq 2\ ,\ 3$, on démontre que l'invariant de Hasse de (Γ) : $-\frac{1}{2}\ g_2(q)/g_3(q)$ $(\mathrm{mod}\ L^{*2})$ est toujours égal à 1 (cf. ROQUETTE [7], §A1). On en déduit que deux «cubiques de Tate», définies sur L , sont isomorphes sur L ,si, et seulement si, elles ont même invariant modulaire $g_2^3/(g_2^3 - 27g_3^2)$.

Nous allons maintenant nous intéresser aux points $\overline{\mathbb{Q}}$-rationnels des courbes elliptiques d'<u>invariant modulaire algébrique sur</u> $\mathbb{Q}$. De façon précise, <u>nous pourrons choisir, pour de telles courbes, une équation de la forme</u> (W^*) <u>définie sur</u> $\overline{\mathbb{Q}}$. <u>Ce sont les points</u> $\overline{\mathbb{Q}}$-<u>rationnels de la cubique</u> (Γ^*) <u>associée à</u> (W^*) <u>que nous étudierons</u>.

2. Points algébriques des fonctions elliptiques p-adiques.

Soient J un élément de $\mathbb{C}_p$ algébrique sur $\mathbb{Q}$, $|J| > 1$, et $\mathcal{E}_q$ la courbe elliptique de Tate d'invariant modulaire J (q est obtenu par application de la proposition 2). Posons $L = \mathbb{Q}_p(J) = \mathbb{Q}_p(q)$.

Les fonctions elliptiques $(P_q\ ,\ DP_q)$ qui paramètrent la courbe $\mathcal{E}_q$ vérifient l'équation :

(W) $$DP_q^2 = 4P_q^3 - \frac{1}{12} E_4(q)\, P_q + \frac{1}{216} E_6(q)\ .$$

Les nombres $g_2(1\ ,\ \tau)$ et $g_3(1\ ,\ \tau)$ correspondant, dans le domaine complexe, à $E_4(q)$, et $E_6(q)$ ne peuvent être simultanément algébriques, d'après le théorème classique de Schneider (proposition A, appliquée au point $t = \frac{1}{2}$). On conjecture qu'il en est de même des nombres $E_4(q)$ et $E_6(q)$. Le critère de transcendance, démontré dans la première partie de ce travail, ne permettant d'étudier que des fonctions satisfaisant des équations différentielles algébriques, nous allons définir une nouvelle fonction, notée P_q^* , à laquelle il sera applicable.

Soit λ un élément de L^* , $|\lambda| < 1$, tel que $E_4^*(q) = \lambda^4 E_4(q)$ soit algébrique sur $\underset{\sim}{Q}$. Alors $E_6^*(q) = \lambda^6 E_6(q)$ est algébrique sur $\underset{\sim}{Q}$, en vertu de l'hypothèse faite sur J . La cubique (Γ^*) d'équation :

(W^*) $$y^2 = 4x^3 - \frac{1}{12} E_4^*(q)\ x + \frac{1}{216} E_6^*(q)$$

est L-isomorphe à $\mathcal{E}_q$.

La fonction Z^λ est définie sur le disque $\mathcal{D} = \{z \in \underset{\sim}{C}_p\ ;\ \ |z-1| < p^{-1/(p-1)}\}$.

Posons alors $P_q^*(Z) = \lambda^2\, P_q(Z^\lambda)$. On a

$$DP_q^*(Z) = \lambda^2\ Z.\lambda Z^{\lambda-1} \frac{d}{dZ} P_q\Big|_{Z^\lambda} = \lambda^3\ Z^\lambda \frac{d}{dZ} P_q\Big|_{Z^\lambda} = \lambda^3\ DP_q(Z)\ ,$$

d'où l'on tire l'équation différentielle :

(W^*) $$DP_q^{*2} = 4P_q^{*3} - \frac{1}{12} E_4^*(q)\ P_q^* - \frac{1}{216} E_6^*(q)\ .$$

En conclusion, les fonctions $(P_q^*\ ,\ DP_q^*)$ définissent un paramétrage de W^* au voisinage de son élément neutre (voir [2]).

Ces définitions étant posées, on peut énoncer la proposition suivante.

PROPOSITION B'. – <u>Deux éléments de $\mathcal{D}$, multiplicativement indépendants, ne peuvent être simultanément points algébriques de</u> $(Z\ ,\ P_q^*(Z))$.

<u>Démonstration</u>. – Supposons qu'il existe deux nombres algébriques U_1 et U_2 de $\mathcal{D}$, multiplicativement indépendants, tels que $P_q^*(U_1)$ et $P_q^*(U_2)$ soient algébriques, et soient K le corps de nombre engendré sur $\underset{\sim}{Q}$ par $E_4^*(q)$, $E_6^*(q)$, $P_q^*(U_1)$, $DP_q^*(U_1)$, $P_q^*(U_2)$, $DP_q^*(U_2)$, U_1 et U_2 . Posons $V_i = U_i^p$ pour $i=1,2$, et considérons les N^2 points algébriques $\{V_1^{n_1}\ V_2^{n_2}\}$, $0 < n_1\ ,\ n_2 \leqslant N$, situés dans le disque $\Delta = \{z \in \underset{\sim}{C}_p\ ;\ \ |z-1| < p^{-p/(p-1)}\}$ strictement inclus dans $\mathcal{D}$. En vertu du théorème de multiplication algébrique de P_q^* (déduit formellement du théorème d'addition des fonctions elliptiques de Weierstrass $\wp$), les points $\{V_1^{n_1}\ V_2^{n_2}\}$, $0 < n_1\ ,\ n_2 \leqslant N$, sont des K-points des fonctions P_q^* , DP_q^* , et vérifient

$$\sup_{0<n_1,n_2\leqslant N}(s(P_q^*(V_1^{n_1}\ V_2^{n_2})\ ,\ s(DP_q^*(V_1^{n_1}\ V_2^{n_2})) < A.N^2$$

(cette dernière inégalité traduit d'ailleurs une propriété classique de la hauteur sur les variétés abéliennes).

L'application $(Z, P_q^*(Z), DP_q^*(Z))$ vérifie la condition (C_1'') du critère local, et, d'après ce qui précède, on a en notant $\nu(N^2)$ le cardinal de l'ensemble $\{u \in \Delta, u$ K-point de $(Z, P_q^*, DP_q^*) ; t(u) < N^2\}$:

$$\nu(N^2)/N^2 > \frac{1}{A} > 0 .$$

Le critère local contredit alors l'indépendance algébrique des fonctions Z et $P_q^*(Z)$.

Signalons pour conclure deux corollaires du critère local dont la démonstration est similaire à la précédente.

PROPOSITION A'. - Deux éléments de $\mathfrak{O}$ multiplicativement indépendants ne peuvent être simultanément points algébriques de $(\mathrm{Lg}\ Z, P_q^*(Z))$.

PROPOSITION C'. - Soit $\mathcal{E} = \mathcal{E}_{q_1} \times \mathcal{E}_{q_2}$ la variété abélienne produit de deux courbes elliptiques de Tate, non isogènes, d'invariants modulaires algébriques. L'application

$$\Psi^* : Z \longrightarrow (P_{q_1}^*(Z), DP_{q_1}^*(Z) ; P_{q_2}^*(Z), DP_{q_2}^*(Z))$$

définit un paramétrage de $\mathcal{E}$ au voisinage de son élément neutre. Si U_1 et U_2 sont deux éléments de $\mathfrak{O}$ multiplicativement indépendants, les points $\Psi^*(U_1)$ et $\Psi^*(U_2)$ de $\mathcal{E}$ ne peuvent être simultanément algébriques sur $\underset{\sim}{Q}$.

On conjecture (cf. LANG [3], Appendice) que, comme dans le cas complexe, il n'y a pas de point algébrique "exceptionnel" pour les fonctions méromorphes p-adiques considérées ci-dessus.

BIBLIOGRAPHIE

[1] ADAMS (W. W.). - Transcendental numbers in the p-adic domain, Amer. J.of Math., t. 88, 1966, p. 279-308.

[2] BERTRAND (D.). - Points algébriques sur les courbes elliptiques p-adiques de Tate, C. R. Acad. Sc. Paris, t. 279, 1974, Série A, p. 809-812.

[3] LANG (S.). - Introduction to transcendental numbers. - Reading, Palo Alto, London [etc.], Addison-Wesley publishing Company, 1966 (Addison-Wesley Series in Mathematics).

[4] LAZARD (M.). - Les zéros d'une fonction analytique d'une variable sur un corps valué complet. - Paris, Presses universitaires de France, 1962 (Institut des Hautes Etudes Scientifiques. Publications mathématiques, 14, p. 47-75).

[5] LUTZ (E.). - Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques, J. für reine und angew. Math., t. 177, 1937, p. 238-247.

[6] ROQUETTE (P.). - Analytic theory of elliptic functions over local fields. - Göttingen, Vandenhoeck und Ruprecht, 1970 (Hamburger math. Einzelschriften, Neue Folge, 1).

[7] SCHNEIDER (T.). - Ein Satz über ganzwertige Funktionen als Prinzip für Transzendenzbeweise, Math. Ann., t. 121, 1949, p. 131-140.

[8] SERRE (J.-P.). - Dépendance d'exponentielles p-adiques, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 7e année, 1965/66, n° 15, 14 p.

[9] TATE (J.). - The arithmetic of elliptic curves, Invent. Math., t. 23, 1974, p. 179-206.

[10] WALDSCHMIDT (M.). - Nombres transcendants. - Berlin, Heidelberg, New York, Springer-Verlag, 1974 (Lecture Notes in Mathematics, 402).

(Texte reçu le 11 mars 1975)

Daniel BERTRAND
Centre de Mathématiques de l'Ecole Polytechnique
17 rue Descartes
75230 PARIS CEDEX 05