Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Daniel Bertrand

Transcendance et lois de groupes algébriques

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 18, n° 1 (1976-1977), exp. n° 1, p. 1-10

<http://www.numdam.org/item?id=SDPP_1976-1977__18_1_A1_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
18e année, 1976/77, n° 1, 10 p.

4 octobre 1976

TRANSCENDANCE ET LOIS DE GROUPES ALGÉBRIQUES

par Daniel BERTRAND

Plusieurs énoncés classiques de la théorie des nombres transcendants (tels que les théorèmes de Hermite-Lindemann et de Gel'fond-Schneider, ou les résultats de SCHNEIDER sur les valeurs des fonctions elliptiques de Weierstrass d'invariants algébriques) peuvent être déduits du critère général de transcendance suivant.

THÉORÈME (SCHNEIDER-LANG). - *Soient* f_1 *et* f_2 *deux fonctions méromorphes sur* $\mathbb{C}$, *algébriquement indépendantes, et* K *une extension algébrique de* $\mathbb{Q}$ *plongée dans* $\mathbb{C}$. *On suppose que :*

(A_1) *Il existe* $\ell - 2$ *fonctions méromorphes sur* $\mathbb{C}$: $f_3, \ldots, f_\ell$ *telles que l'algèbre* $K[f_1, \ldots, f_\ell]$ *soit stable par l'opérateur de dérivation* $D = d/dz$;

(A_2) *Les fonctions* f_1 *et* f_2 *sont quotients de fonctions entières d'ordre fini* ;

(A_3) K *est une extension finie de* $\mathbb{Q}$.

Alors, l'ensemble des nombres complexes, où $f_1, \ldots, f_\ell$ *prennent simultanément des valeurs dans* K, *est fini.*

Pour en déduire les résultats de transcendance mentionnés ci-dessus, on fait alors appel aux théorèmes d'addition algébrique qui vérifient la fonction exponentielle ou les fonctions elliptiques.

La traduction p-adique du critère précédent ne pose pas de difficulté. Mais, dans les domaines p-adiques, les fonctions exponentielle et elliptiques ne sont définies qu'au voisinage de l'origine, et si, selon une conjecture de BOMBIERI et de WALDSCHMIDT, l'hypothèse (A_3) est sans doute superflue dans l'énoncé du théorème de Schneider-Lang, l'hypothèse (A_2) semble en revanche fondamentale (voir à ce sujet la remarque 2, § 3.2, ci-dessous).

Pour résoudre cette difficulté, il convient de faire jouer un rôle plus central aux théorèmes d'addition algébrique que vérifient encore les fonctions exponentielle et elliptiques dans les domaines p-adiques. Dans le cas exponentiel, cela avait déjà été remarqué par MAHLER (voir [7] pour l'analogue p-adique du théorème de Hermite-Lindemann, et [8] pour celui du théorème de Gel'fond-Schneider). Le cas des fonctions elliptiques a été traité en toute généralité dans [2], comme conséquence d'un critère de transcendance valable pour des fonctions vérifiant à la fois un système d'équations différentielles algébriques et une suite d'équations fonctionnelles. Nous en obtenons ici une généralisation (voir également [2], remarque 4(b)).

Cette généralisation (I, § 1.2, théorème) porte sur le type d'équations fonction-

nelles que l'on peut considérer. Sa démonstration, qui fait intervenir une suite de "fonctions auxiliaires", est donnée dans la deuxième partie de ce travail. A titre d'illustration, nous indiquons, dans une troisième partie, comment elle permet en particulier de retrouver certains des résultats de [2], en étudiant directement la fonction logarithme associée à certains groupes formels. Mais les énoncés obtenus dépendent bien entendu du choix d'un paramètre sur le groupe formel, et ne semblent pas susceptibles de généralisation.

1. Un nouveau critère de transcendance.

1.1. Ordre arithmétique.

Fixons tout d'abord quelques notations. Soient p un nombre premier, Ω le complété de la clôture algébrique du corps des nombres p-adiques ordinaires, et $|\ |$ la valeur absolue de Ω, normalisée par $|p| = p^{-1}$. Nous notons $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans Ω, et, pour tout élément α de $\overline{\mathbb{Q}}$, nous appelons taille $s(\alpha)$ de α le logarithme du maximum de son dénominateur et de ses différentes valeurs absolues archimédiennes. Si P désigne un polynôme à plusieurs variables à coefficients entiers algébriques, nous appelons taille $s(P)$ de P le maximum de son degré total $\deg P$ et des tailles de ses coefficients.

Soient $\mathcal{D}$ un disque non circonférencié de Ω, centré en 0 (avec les notations habituelles, $\mathcal{D} = D(0, r^-)$, où r désigne un nombre réel > 0), et $\mathcal{K} = \mathcal{K}(\mathcal{D})$ le corps des fonctions méromorphes sur $\mathcal{D}$ (i. e. des quotients de fonctions analytiques strictes sur $\mathcal{D}$). Nous notons D l'opérateur de dérivation d/dz en $\mathcal{K}$. Nous considérons par ailleurs une suite $\tau = \{\tau_n\ ;\ n \in \mathbb{N}\}$ de contractions analytiques sur $\mathcal{D}$, c'est-à-dire d'applications analytiques $\tau_n : \mathcal{D} \longrightarrow \mathcal{D}$ vérifiant : $|\tau_n(z)| \leqslant |z|$ pour $z \in \mathcal{D}$. On associe à cette suite τ la suite $\{T_n\ ;\ n \in \mathbb{N}\}$ d'opérateurs sur $\mathcal{K}$ définis par :

$$\forall\ n \in \mathbb{N},\ \forall\ f \in \mathcal{K} :\ T_n f = f \circ \tau_n .$$

Définition. - On dit qu'un élément f de $\mathcal{K}$ est d'ordre arithmétique fini (relativement à la suite τ) s'il existe un corps de nombres $K = K_f$ d'anneau d'entiers $\mathcal{O}$, et deux nombres réels $c = c_f$ et $\rho = \rho_f$ tels que, pour tout entier $n \geqslant 1$, on ait

$$T_n(f) = P_n(f)/Q_n(f) ,$$

où P_n et Q_n désignent des éléments de $\mathcal{O}[X]$ de taille $< cn^\rho$ (On peut, sans perte de généralité - voir [2], remarque 1 - les supposer premiers entre eux). On appelle alors ordre arithmétique de f la limite inférieure des nombres réels ρ vérifiant cette propriété.

Exemples. - Soit $\tau_{add} = \{\tau_n(z) = nz\ ;\ n \in \mathbb{N}\}$ la suite des multiplications par les entiers positifs. Relativement à τ_{add}, la fonction $f(z) = z$ est d'ordre arithmétique 0 ; la fonction exponentielle p-adique est d'ordre arithmétique 1, et

la fonction elliptique p-adique de Weierstrass associée à une courbe elliptique définie sur un corps de nombre est d'ordre arithmétique 2 (voir [2], I). Des exemples de fonctions d'ordre arithmétique fini relativement à d'autres suites seront donnés dans la troisième partie.

1.2. Enoncé du critère.

L'énoncé qui suit est relatif à la donnée d'un disque $\mathbb{Q}$ et d'une suite τ de contractions.

THÉORÈME. - *Soient* f_1 *et* f_2 *deux fonctions méromorphes sur* $\mathbb{Q}$, *algébriquement indépendantes, et* u *un élément de* $\mathbb{Q}$. *On suppose que :*

(B_1) *Il existe* $\ell - 2$ *fonctions méromorphes sur* $\mathbb{Q}$: $f_3, \dots, f_\ell$ *telles que l'algèbre* $\overline{\mathbb{Q}}[f_1, \dots, f_\ell]$ *soit stable par* D ;

(B_2) *Les fonctions* f_1 *et* f_2 *sont d'ordre arithmétique fini (relativement à* τ) ;

(B_3) ***Si*** n *et* m *sont des entiers* $\geqslant 1$ *distincts, alors* $\tau_n(u) \neq \tau_m(u)$;

(B_4) *La suite* $D\tau_n(u)$ *ne s'annule que pour un nombre fini de valeurs de* n .

Alors, les fonctions $f_1, \dots, f_\ell$ *ne peuvent prendre simultanément de valeurs algébriques au point* u .

Le théorème principal de [2] concernait le cas où τ est la suite τ_{add}. Si u est un élément non nul de $\mathbb{Q}$, la condition (B_3) (ainsi que (B_4)) est alors automatiquement satisfaite. Nous discutons maintenant les hypothèses du nouveau critère de transcendance.

Hypothèse (B_1) : Faisons l'hypothèse plus générale suivante :

(B_1') *La dérivation* D *opère sur le corps* $\overline{\mathbb{Q}}(f_1, \dots, f_\ell)$

Il existe alors $\ell + 1$ éléments $P_1, \dots, P_\ell$ et R de $\overline{\mathbb{Q}}[X_1, \dots, X_\ell]$ tels que

$$\forall\, i = 1, \dots, \ell : \quad Df_i = P_i(f_1, \dots, f_\ell)/R(f_1, \dots, f_\ell) ,$$

et la dérivation D opère sur l'algèbre $\overline{\mathbb{Q}}[f_1, \dots, R^{-1}(\underset{\sim}{f})]$. Le théorème est donc encore valable, si l'on suppose en outre que u n'est pas zéro de $R(f_1, \dots, f_\ell)$.

Hypothèse (B_3) : l'hypothèse (B_3) est en un sens fondamentale. Ainsi, le theorème serait incorrect si la suite $\{\tau_n(u) \ ; \ n \in \underset{\sim}{N}\}$ n'avait qu'un nombre fini de valeurs distinctes (quelques contre-exemples seront développés au § 3.2). Mais on peut l'affaiblir sous la forme suivante :

(B_3') *Pour tout entier* $n \geqslant 1$, *soit* $\nu(n)$ *le cardinal de l'ensemble* $\{\tau_h(u) \ ; \ 1 \leqslant h \leqslant n\}$. *Alors*

$$\limsup_{n \to +\infty} (\log n)/\nu(n) = 0$$

(voir § 2.2, deuxième pas).

Une dernière remarque : Aucune condition de croissance n'est imposée aux fonctions $f_1, \dots, f_\ell$ au voisinage de la frontière de $\mathcal{Q}$. La raison en est que les applications τ_n sont supposées contractantes.

2. Démonstration du critère de transcendance.

2.1. Quelques lemmes.

Au cours de la démonstration du critère, nous serons amenés à étudier des expressions du type $D^k F(\tau_n(u)) = T_n D^k F(u)$, où F est une fonction polynômiale en f_1 et f_2. Comme aucune hypothèse n'est faite sur $T_n f_j$ pour $j = 3, \dots, \ell$, nous considèrerons plutôt $D^k T_n F(u)$ (le lien entre ces expressions est rappelé au lemme 3). L'estimation classique que fournit le lemme 1 peut être améliorée -et c'est crucial- quand u est zéro d'ordre k de $T_n F$ (lemme 2).

Le lemme 2 généralise un énoncé de MASSER ("lemme de Baker-Coates"), obtenu dans le cas où les applications τ_n représentent des endomorphismes d'une courbe elliptique admettant une multiplication complexe. Sa démonstration (ainsi que celle du lemme 1) repose sur des calculs purement algébriques, où la forme des applications τ_n n'intervient pas. Les démonstrations données dans [2] sont donc encore valables, et nous ne les reproduirons pas ici.

Nous reprenons les notations de la première partie, et, pour $i = 1, 2$, et n entier $\geqslant 1$, nous fixons une représentation irréductible $P_{n,i}/Q_{n,i}$ de la fraction rationnelle apparaissant dans l'expression de $T_n f_i$ (§ 1.1). Nous désignons par K le compositum des corps K_{f_1}, K_{f_2} et du corps engendré par les coefficients des équations différentielles satisfaites par $f_1, \dots, f_\ell$ (hypothèse (B_1)). Nous notons $\mathcal{O}$ son anneau d'entiers, et ρ un entier majorant strictement l'ordre arithmétique des fonctions f_1 et f_2.

Soient $h > 0$ et $L > 0$ deux entiers, P un élément de $\mathcal{O}[X_1, X_2]$ de degré total $\leqslant L$, de taille $\leqslant h$, et F la fonction $P(f_1, f_2)$. Alors on a le résultat suivant.

LEMME 1 (voir [2], lemme 1 et formule (5)). - *Il existe un entier γ_1 ne dépendant que de $f_1, \dots, f_\ell$, et vérifiant la propriété suivante : Pour tout couple d'entiers $n \geqslant 1$, $k \geqslant 0$, on a*

$$D^k T_n F = \gamma_1^{-k} R_{k,n,F}(f_1, \dots, f_\ell)/[Q_{n,1}^{L+k}(f_1)\, Q_{n,2}^{L+k}(f_2)],$$

où $R_{k,n,F}$ est un élément de $\mathcal{O}[X_1, \dots, X_\ell]$ tel que

$$\deg R_{k,n,F} \leqslant \gamma_1 (k + L)n^\rho,$$

$$s(R_{k,n,F}) \leqslant h + \gamma_1 k \operatorname{Log}[(k + L)n^\rho] + \gamma_1 (k + L)n^\rho.$$

LEMME 2 (voir [2], lemme 2). - *Il existe un entier γ_2 ne dépendant que de $f_1, \dots, f_\ell$, et vérifiant la propriété suivante : Soient u un point de $\mathcal{Q}$ non*

pôle de $f_1, \dots, f_\ell$, et $n \geqslant 1$, $k \geqslant 0$ deux entiers tels que u soit zéro d'ordre k de $T_n F$ sans être pôle de $T_n f_1$, $T_n f_2$. Alors

$$D^k T_n F(u) = \gamma_2^{-k} S_{k,n,F}(f_1(u), \dots, f_\ell(u)) / [Q_{n,1}^L(f_1(u))\, Q_{n,2}^L(f_2(u))],$$

où $S_{k,n,F}$ est un élément de $\mathcal{O}[X_1, \dots, X_\ell]$ tel que

$$\deg S_{k,n,F} \leqslant \gamma_2 (k + Ln^\rho),$$

$$s(S_{k,n,F}) \leqslant h + \gamma_2 k \operatorname{Log}(k + Ln^\rho) + \gamma_2 (k + Ln^\rho).$$

Remarque 1. - Si $\tau_n(u)$ n'est pas pôle de f_1, f_2, l'hypothèse d'irréductibilité faite sur $P_{n,i}/Q_{n,i}$ entraîne que $Q_{n,i}(f_i(u))$ est non nul, et les expressions ci-dessus sont bien définies.

Le lemme suivant est banal.

LEMME 3. - Soient $k \geqslant 0$ et $n \geqslant 1$ deux entiers, et u un élément de $\mathcal{Q}$ tel que $D\tau_n(u)$ soit non nul. Alors, la fonction $T_n F$ a un zéro d'ordre k au point u si, et seulement si, la fonction F a un zéro d'ordre k au point $\tau_n(u)$, et l'on a, dans ces conditions,

$$D^k T_n F(u) = (D\tau_n(u))^k T_n D^k F(u).$$

2.2. Démonstration du critère.

Supposons qu'en un point u de $\mathcal{Q}$ vérifiant les conditions (B_3) et (B_4), les fonctions $f_1, \dots, f_\ell$ prennent simultanément des valeurs algébriques, que, quitte à augmenter K, on peut supposer appartenir à K. Les fonctions $f_1, \dots, f_\ell$ sont quotients de fonctions analytiques sur le disque non circonférencié $\mathcal{Q}$. D'après l'hypothèse (B_3), et puisque les applications τ_n sont contractantes, il existe donc un entier n_0 tel qu'elles n'admettent aucun des points de la suite $\{\tau_n(u) ; n > n_0\}$ pour pôle. En vertu du lemme 1 et de la remarque 1, les fonctions f_1 et f_2 prennent en ces points des valeurs dans K. Nous allons en déduire une contradiction.

Nous reprenons les notations du § 2.1, et nous posons : $\lambda = 2\rho + 2$, $\sigma = 3\rho + 2$. Nous désignons par m un entier arbitrairement grand, et par $c_1, \dots, c_8$ des nombres réels > 0 ne dépendant que de $f_1, \dots, f_\ell$, p, $\mathcal{Q}$, u et n_0. En vertu de l'hypothèse (B_4), on peut enfin supposer sans perte de généralité que $D\tau_n(u)$ est non nul pour $n > n_0$.

Premier pas (Construction d'un nombre algébrique non nul). - Il existe un élément non nul P de $\mathcal{O}[X_1, X_2]$, de degré $\leqslant L = m^\lambda$, de taille $\leqslant c_1 m^{3\rho+1}$, tel que, si F désigne la fonction $P(f_1, f_2)$, les fonctions $T_{n_0+1} F, \dots, T_m F$ admettent chacune le point u pour zéro d'ordre $> m^\sigma$.

Démonstration. - Il suffit, en vertu du lemme 1, de construire une fonction F telle que

$$\forall\, n = n_0 + 1\ ,\ \dots\ ,\ m\ ;\ k = 0\ ,\dots,\ m^\sigma\ :\qquad R_{k,n,F}(f_1(u)\ ,\ \dots\ ,\ f_\ell(u)) = 0\ ,$$

c'est-à-dire de résoudre un système homogène de $(m - n_0)m^\sigma$ équations linéaires, dont les inconnues sont les $(L + 1)^2$ coefficients de P, et dont les coefficients sont des éléments de K de taille majorée par $c_2(m^\sigma \operatorname{Log} m^\sigma + (m^\sigma + L)m^\rho)$.

Le lemme de Siegel permet d'en obtenir une solution à coefficients dans $\mathcal{O}$, non tous nuls, et de taille majorée par

$$c_3\, m^{\sigma+\rho} \times m^{\sigma+1}/m^{2\lambda} = c_3\, m^{3\rho+1}\ .$$

Puisque f_1 et f_2 sont algébriquement indépendantes, les fonctions $T_n F$ ne sont pas identiquement nulles, et l'on peut définir le plus grand entier M tel que

$$\forall\, n = n_0 + 1\ ,\ \dots\ ,\ M\ ;\ k = 0\ ,\ \dots\ ,\ M^\sigma\ :\qquad D^k T_n F(u) = 0\ .$$

Dans ces conditions, il existe deux entiers $N \leqslant M + 1$ et $K \leqslant (M + 1)^\sigma$ tel que u soit zéro d'ordre K de $T_N F$. Posons

$$\xi = D^K T_N F(u) \neq 0\ .$$

<u>Deuxième pas</u> (<u>Estimations de</u> $|\xi|$). - D'après le lemme 2 et la remarque 1, ξ est un élément de K vérifiant

$$s(\xi) \leqslant c_4\ (m^{3\rho+1} + K \operatorname{Log} K + LN^\rho)\ .$$

Comme ξ est non nul, la formule du produit sur K (voir [8], proposition 1) entraîne

$$|\xi| > \exp(-\,c_5\, M^{3\rho+2} \operatorname{Log} M)\ .$$

Des considérations analytiques permettent par ailleurs de majorer $|\xi|$. En effet, on déduit du lemme 3 et des relations précédentes que la fonction F admet sur le disque circonférencé $\mathcal{Q}_u = D(0\ ,\ |u|^+)$ au moins $(M - n_0)M^\sigma$ zéros (comptés avec leurs ordres de multiplicité). Soient alors δ un nombre réel compris strictement entre $|u|$ et le rayon de $\mathcal{Q}$, et Δ le disque $D(0\ ,\ \delta^+)$. Il existe un polynôme θ ne dépendant que de f_1, f_2 et δ, qui ne s'annule pas aux points de la suite $\{\tau_n(u)\ ;\ n > n_0\}$ et tel que θf_1 et θf_2 soient analytiques sur Δ. La fonction $G = \theta^{2L} F$ est analytique sur Δ, admet sur $\mathcal{Q}_u$ au moins $(M - n_0)M^\sigma$ zéros, et vérifie

$$D^K G(\tau_N(u)) = [\theta(\tau_N(u))]^{2L}\, D^K F(\tau_N(u))\ ,$$

soit, d'après le lemme 3,

$$D^K G(\tau_N(u)) = [D\tau_N(u)]^{-K}\, [\theta(\tau_N(u))]^{2L}\, \xi\ .$$

On déduit du lemme de Schwarz et des inégalités de Cauchy (voir [8], proposition 3) :

$$|D^K G(\tau_N(u))| < (|u|/\delta)^{(M-n_0)M^\sigma}\ c_6^{L+K}\ .$$

Le raisonnement de [1], § 6, entraîne d'autre part

$$|\theta(\tau_N(u))| > \exp[-\sup(s(f_1(\tau_N(u))) , s(f_2(\tau_N(u)))] > \exp(-c_7 M^{\rho}) ;$$

Notant que la relation $|\tau_N(z)| \leqslant |z|$ implique (par exemple au moyen des inégalités de Cauchy) que $|D\tau_N(u)| \leqslant 1$, on obtient en définitive :

$$|\xi| \leqslant \exp(-c_8 M^{3\rho+3}) .$$

La comparaison des inégalités précédentes fournit la contradiction recherchée (sous l'hypothèse (B_3'), il convient de remplacer le terme $(M - n_0)M^{\sigma}$ par $M^{\sigma}\nu(M)$, ce qui permet de conclure).

3. Applications.

Les applications les plus importantes du critère de transcendance concernent l'étude de l'exponentielle p-adique sur certains groupes algébriques [2]. Nous considérons ici les groupes formels qui leurs sont associés. Contrairement (semble-t-il) au cas complexe, on peut, grâce au nouveau critère, étudier directement les propriétés de transcendance de leurs fonctions logarithmes.

3.1. Rappel sur les groupes formels.

Soient A l'anneau des entiers de Ω , $\mathfrak{M}$ son idéal maximal, et $\mathfrak{F}$ une loi de groupe formel (commutative) à un paramètre, à coefficients dans A . Définissons par récurrence la suite $\tau_{\mathfrak{F}} = \{\tau_n ; n \geqslant 1\}$ des "puissances n-ièmes" de $\mathfrak{F}$ par

$$\tau_1(X) = X ; \quad \tau_{n+1}(X) = \mathfrak{F}(X , \tau_n(X)) .$$

Les séries τ_n sont des éléments de $A[[X]]$ vérifiant

$$\tau_n(X) = nX + O(X^2) .$$

Elles définissent des contractions analytiques (notées encore τ_n) de $\mathfrak{M}$ dans lui-même.

A $\mathfrak{F}$ est associée une fonction logarithme $\log_{\mathfrak{F}}$: c'est l'unique isomorphisme de $\mathfrak{F}$ dans le groupe additif tel que $(d/dX)\log_{\mathfrak{F}}(0) = 1$. Comme $\mathfrak{F}$ est définie sur A , la série $d/dX \log_{\mathfrak{F}}(X)$ est un élément de $A[[X]]$ (voir [4], p. 96). Par conséquent, $\log_{\mathfrak{F}}$ définit une fonction analytique sur $\mathfrak{M}$, et l'on a

$$\forall\, n \in N , \quad \forall\, z \in \mathfrak{M} : \quad \log_{\mathfrak{F}}(\tau_n(z)) = n \log_{\mathfrak{F}}(z) .$$

Autrement dit, la fonction $\log_{\mathfrak{F}}$ est, relativement à $\tau_{\mathfrak{F}}$, d'ordre arithmétique 0.

Par ailleurs, l'espace des formes différentielles $\mathfrak{F}$-invariantes sur $\mathfrak{M}$ est de dimension 1. Si $\psi_{\mathfrak{F}}(X)\, dX$ désigne l'un de ses générateurs, on a donc :

$$\psi_{\mathfrak{F}}(X) = \psi_{\mathfrak{F}}(0)\ (d/dX)\log_{\mathfrak{F}}(X) .$$

Afin de satisfaire l'hypothèse (B_1) du critère de transcendance, nous ne pourrons ici considérer que les groupes formels $\mathfrak{F}$ tels que $\psi_{\mathfrak{F}}(X)$ et X soient algébriquement dépendants. Deux cas se présentent (un résultat de HONDA [5] semble en fait

indiquer qu'il n'y en a pas d'autres).

1° Groupe multiplicatif : La loi du produit sur le groupe "standard" $1 + \mathfrak{M}$ permet de munir $\mathfrak{M}$ de la loi de groupe formel :

$$\mathrm{mult}(X , Y) = X + Y + XY .$$

La suite $\tau_{mult} = \{\tau_n ; \ n \geqslant 1\}$ est définie par

$$\tau_n(z) = (1 + z)^n - 1 ,$$

de sorte que la fonction $\xi_{mult}(z) = 1 + z$ est d'ordre arithmétique 1 relativement à τ_{mult}. On peut ici choisir : $\psi_{mult}(z) = \xi_{mult}^{-1}(z)$.

2° Courbe elliptique : Soit E une courbe elliptique définie sur un corps de nombres K par une équation de Weierstrass minimale au sens de [9], § 6 :

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 .$$

Soit E_1 le noyau de la réduction de E modulo $\mathfrak{M} \cap K$. L'application

$$P \longrightarrow z(P) = - x(P)/y(P)$$

est un isomorphisme du groupe "standard" $E_1(\Omega)$ sur $\mathfrak{M}$. Elle permet de munir $\mathfrak{M}$ d'une structure de groupe formel "ell". La suite τ_{ell} est définie par

$$\tau_n(z(P)) = z(nP) .$$

Si $\xi_{ell} = \xi$ et η sont définies sur $\mathfrak{M}$ par

$$\xi(z(P)) = x(P) \ ; \ \ \eta(z(P)) = y(P) ,$$

la loi de groupe sur les points de E montre que la fonction ξ_{ell} est d'ordre arithmétique 2. Enfin, on peut choisir (voir [9], § 3) :

$$\psi_{ell}(z) = [(d/dz)\xi(z)]/(2\eta(z) + a_1 \xi(z) + a_3) .$$

3.2. Résultats de transcendance.

On reprend les notations du critère de transcendance. Après quelques remarques sur les hypothèses (B_3) et (B_4), valables pour tout groupe formel $\mathfrak{F}$ défini sur A, nous considérons les hypothèses (B_1) et (B_2) dans les cas multiplicatif et elliptique.

On tire de l'équation fonctionnelle de $\log_{\mathfrak{F}}$ la relation

$$n D \log_{\mathfrak{F}} = (D\tau_n)(T_n \ D \log_{\mathfrak{F}}) .$$

Comme $(d/dX)\log_{\mathfrak{F}}(X)$ est une série de $A[[X]]$ dont le terme constant est égal à 1, on déduit

$$\forall \ u \in \mathfrak{M} : |n| = |D\tau_n(u)| ,$$

et la condition (B_4) est automatiquement satisfaite.

De façon plus fondamentale, la définition de $\tau_{\mathfrak{F}}$ montre que (B_3) est satisfaite si, et seulement si, le point u de $\mathfrak{M}$ n'appartient pas à l'ensemble $\Lambda(\mathfrak{F})$ des

points de torsion de $\mathfrak{F}$. Ces points (dont l'ordre est nécessairement une puissance de p) forment l'ensemble des zéros de $\log_{\mathfrak{F}}$.

1° Cas multiplicatif : Les fonctions $f_1 = \xi_{mult}^{-1}$ et $f_2 = \log_{mult}$ vérifient les hypothèses (B_1) et (B_2) du critère. En conséquence, si u est un point algébrique de $\mathbb{M}$, $\log_{mult}(u)$ est nul ou transcendant. Désignant par $\mathrm{Log}\, x = \log_{mult}(x - 1)$ la fonction logarithme p-adique ordinaire, on peut alors énoncer le théorème de Mahler [7] sous la forme suivante :

COROLLAIRE 1. - La fonction Log s'annule aux racines (d'ordre une puissance de p) de l'unité, et prend en tout autre point algébrique de $1 + \mathbb{M}$ une valeur transcendante.

2° Cas elliptique : Posons $\varphi = \xi\varphi_2 + \eta\varphi_1$, où

$$\varphi_1 = 2\eta + a_1\,\xi + a_3 \; ; \quad \varphi_2 = 3\xi^2 + 2a_2\,\xi + a_4 - a_1\,\eta \; .$$

Alors (voir [9], § 3), $D\xi/\varphi_1 = D\eta/\varphi_2$, et on déduit de la relation $D\xi/\xi = D\eta/\eta + 1/z$ que $D\eta = \eta^2\,\varphi_2/\varphi$.

Ainsi, les fonctions $f_1 = \xi$ et $f_2 = \log_{ell}$ vérifient les hypothèses (B_1') et (B_2) du critère, avec $f_3(z) = \eta(z)$, $f_4(z) = z$ et $R(f_1, \ldots, f_4) = \varphi\varphi_1$. Le développement de Laurent $1/z^6 + \ldots$ de la fonction φ montre qu'elle ne s'annule pas sur $\mathbb{M}$, et les seuls zéros de φ_1 sont des points d'ordre 2 (qu'on n'aura donc à considérer que si $p = 2$). Enfin, pour tout élément non nul u de $\mathbb{M}$, u et $\xi(u)$ sont simultanément algébriques ou transcendants. Par conséquent, si u est un point algébrique de $\mathbb{M}$, $\log_{ell}(u)$ est nul ou transcendant. Désignant par Log_E la fonction définie sur $E_1(\Omega)$ par

$$\mathrm{Log}_E(P) = \log_{ell}(z(P)) \; ,$$

on peut alors énoncer le corollaire 1 de [2] sous la forme suivante :

COROLLAIRE 2. - La fonction Log_E s'annule aux points de torsion (d'ordre une puissance de p) de E , et prend en tout autre point de $E_1(\overline{\mathbb{Q}})$ une valeur transcendante.

Concluons par quelques remarques sur ces corollaires.

Remarque 2. - Les fonctions logarithmes des deux groupes formels $\mathfrak{F}$ étudiées ci-dessus fournissent des exemples simples de fonctions analytiques sur $\mathbb{M}$, vérifiant une équation différentielle algébrique, et qui prennent des valeurs algébriques en une infinité de points algébriques de $\mathbb{M}$. Néanmoins, on notera, dans l'esprit du théorème de Schneider-Lang, qu'il existe une constante $c = c(\mathfrak{F}) > 0$ telle que, pour tout corps de nombres K , les fonctions z et $\log_{\mathfrak{F}}(z)$ ne prennent simultanément des valeurs dans K qu'en au plus $c[K:\mathbb{Q}]$ points de $\mathbb{M}$. Ceci résulte (le cas d'une courbe elliptique ayant mauvaise réduction en p mis à part) du théorème d'irréductibilité démontré dans [4], page 137, joint aux corollaires 1 et 2 (Pour

le groupe multiplicatif, ou pour une courbe elliptique ayant bonne réduction de hauteur 2, cet énoncé n'est d'ailleurs pas améliorable).

Dans le même ordre d'idée, on notera que, pour tout disque $\mathcal{D}$ strictement inclus dans $\mathfrak{M}$ (et sur lequel $\log_{\mathcal{F}}$ est donc bornée), les fonctions z et $\log_{\mathcal{F}}(z)$ ne prennent simultanément des valeurs algébriques qu'en un nombre fini de points de $\mathcal{D}$.

Remarque 3. - Ainsi que nous le précisions dans l'introduction, les propriétés de transcendance des fonctions $\log_{\mathcal{F}}$ dépendent du choix d'un paramètre du groupe formel $\mathcal{F}$. Ainsi, la méthode exposée ici ne permet pas d'étudier la fonction (voir [3], § 8) :

$$\ell(t) = \sum_{n=1}^{+\infty} t^{p^n}/p^n ,$$

qui représente le logarithme d'une loi de groupe formel isomorphe (sur $\mathbb{Z}_p$) à la loi "mult". Des énoncés de transcendance peuvent néanmoins être obtenus. Par exemple, la version p-adique du théorème de Roth entraîne que, si $p > 2$, le nombre $\ell(p)$ est transcendant. Signalons enfin que la dérivée de la fonction ℓ vérifie une équation fonctionnelle à laquelle s'applique une autre méthode de transcendance, due à MAHLER, et récemment généralisée par KUBOTA, LOXTON et VAN DER POORTEN (voir [6]).

BIBLIOGRAPHIE

[1] BERTRAND (D.). - Algebraic values of p-adic elliptic functions, "Transcendence theory : Advances and applications. Ed. A. Baker and D. Masser", chap. 9. - London, Academic Press, 1977.

[2] BERTRAND (D.). - Sous-groupes à un paramètre p-adique de variétés de groupes, Inventiones Math., t. 40, 1977, p. 171-193.

[3] CARTIER (P.). - Groupes de Lubin-Tate généralisés, Inventiones Math., t. 35, 1976, p. 273-284.

[4] FRÖLICH (A.). - Formal groups. - Berlin, Heidelberg, New York, Springer-Verlag, 1968 (Lecture Notes in Mathematics, 74).

[5] HONDA (T.). - Differential equations and formal groups, "United States-Japan seminar on number theory [1971. Tokyo]".

[6] LOXTON (J. H.) and VAN DER POORTEN (A. J.). - Transcendence and algebraic independence by a method of Mahler, "Transcendence theory : Advances and applications. Ed. A. Baker and D. Masser", chap. 15. - London, Academic Press, 1977.

[7] MAHLER (K.). - Ein Beweis der Transzendenz der P-adischen Exponentialfunktion, J. reine und angew. Math., t. 169, 1932, p. 61-66.

[8] MAHLER (K.). - Über transzendente P-adischen Zahlen, Compositio Math., t. 2, 1935, p. 238-247.

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

(Texte reçu le 7 juillet 1977)

Daniel BERTRAND
Centre de Mathématiques
Ecole Polytechnique
Plateau de Palaiseau
91128 PALAISEAU Cédex