ANNALES DE L'INSTITUT FOURIER

JOHN L. BOXALL

p-adic interpolation of logarithmic derivatives associated to certain Lubin-Tate formal groups

Annales de l'institut Fourier, tome 36, nº 3 (1986), p. 1-27

<http://www.numdam.org/item?id=AIF_1986__36_3_1_0>

Ann. Inst. Fourier, Grenoble
36, 3 (1986), 1-27

p-ADIC INTERPOLATION OF LOGARITHMIC DERIVATIVES ASSOCIATED TO CERTAIN LUBIN-TATE FORMAL GROUPS

by John L. BOXALL

Introduction.

The purpose of this paper is to study the p-adic interpolation properties of the values of logarithmic derivatives of power series at 0 attached to certain one-dimensional formal groups over p-adic integer rings. The earliest results at this kind were given in Iwasawa [3], following the then unpublished work of Kubota and Leopoldt [9], who applied them to the construction of p-adic L-functions attached to Dirichlet characters. They were subsequently used to construct p-adic L-functions in other contexts, notably those attached to abelian extensions of totally real fields [1] and to elliptic curves with complex multiplication, at least when p splits in the field of complex multiplication. We first recall the interpolation results of Iwasawa, Kubota and Leopoldt in a form similar to that in Lichtenbaum [10, §1]. Fix an odd prime p and let $\mathbf{C}_p$ be the completion of the algebraic closure of $\mathbf{Q}_p$. We denote by $v : \mathbf{C}_p^* \longrightarrow \mathbf{Q}$ the valuation normalised so that $v(p) = 1$. Let Q_0 be the ring of power series

$$\left\{ f(T) = \sum_{n=0}^{\infty} \frac{c_n T^n}{n!} \in C_p [[T]] \mid v(c_n) \longrightarrow \infty \text{ as } n \longrightarrow \infty \right\}. \quad (1)$$

For $\beta \in \mathbf{Z}/(p-1)\mathbf{Z}$ and $f \in Q_0$ define f_β to the power series

Key-words: p-adic interpolation – Formal groups.

$$f_\beta(\mathrm{T}) = f(\mathrm{T}) - \frac{1}{p} \sum_{c=0}^{p-1} f(\xi^c(1+\mathrm{T}) - 1) \quad \text{if} \quad \beta = 0,$$

$$= \frac{\tau(\beta)}{p} \sum_{c=1}^{p-1} f(\xi^c(1+\mathrm{T}) - 1)\, \omega^{-\beta}(c) \quad \text{if} \quad \beta \neq 0. \tag{2}$$

Here ξ is a fixed primitive p-th root of unity, $\omega : \mathbf{Z}_p^* \longrightarrow \mathbf{Z}_p^*$ is the Teichmuller character (i.e. for each $a \in \mathbf{Z}_p^*$ $\omega(a)$ is the unique $p-1-$ st root of unity such that $\omega(a) \equiv a \pmod p$) and the Gauss sum $\tau(\beta)$ is defined by

$$\tau(\beta) = \sum_{a=1}^{p-1} \omega^\beta(a)\, \xi^a .$$

Let $\mathfrak{O}$ be the ring of integers of $\mathbf{C}_p$ and u a topological generator of the $\mathbf{Z}_p$-module $(1 + p\,\mathbf{Z}_p)^{\mathrm{X}}$; then the interpolation theorem may be stated as follows.

THEOREM A. – (i) *Let* $f \in \mathrm{Q}_0$ *and* $\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}$. *Then there exists a unique continuous function* $\mathrm{C}_f^{(\alpha)} : \mathbf{Z}_p \longrightarrow \mathbf{C}_p$ *such that for each* $\beta \in \mathbf{Z}/(p-1)\,\mathbf{Z}$

$$\mathrm{C}_f^{(\alpha)}(k) = (-1)^{\alpha-\beta} \left((1+\mathrm{T}) \frac{d}{d\mathrm{T}} \right)^k f_{\alpha-\beta}(\mathrm{T})\,|_{\mathrm{T}=0}$$

whenever $k \geqslant 0$ *and* $k \in \beta$.

(ii) *If* $f \in \mathfrak{O}[[\mathrm{T}]]$ *then* $f_\beta \in \mathfrak{O}[[\mathrm{T}]]$ *for each* β *and there is a unique power series* $\mathrm{G}_f^{(\alpha)}(\mathrm{X}) \in \mathfrak{O}[[\mathrm{X}]]$ *such that*

$$\mathrm{G}_f^{(\alpha)}(u^s - 1) = \mathrm{C}_f^{(\alpha)}(s)$$

for all $s \in \mathbf{Z}_p$.

The existence of the power series $\mathrm{G}_f^{(\alpha)}$ in (ii) is equivalent to the assertion that $\mathrm{C}_f^{(\alpha)}$ is an Iwasawa function (see Serre [14]), or that it is p-adic Mellin transform of a Mazur measure (see Lang [8, Chapter 4] or Mazur and Swinnerton-Dyer [12]).

We now explain the generalisation of Theorem A to which this article is devoted. Let $\mathfrak{F}$ be a (commutative) one dimensional formal group over the ring of integers $\mathfrak{O}_{\mathrm{F}_p}$ of a finite extension F_p of $\mathbf{Q}_p$.

Let K_p be another finite extension of $\mathbf{Q}_p$, of degree h and ramification index e, let $\mathcal{O}_{K_p}$ be the ring of integers of K_p, π a uniformising parameter for K_p, and q (a power of p) the cardinality of the residue class field k_{K_p}. We suppose that $\mathfrak{F}$ is isomorphic over $\mathcal{O}$ to the basic Lubin-Tate group $\mathfrak{F}_0$ associated to the polynomial $\pi T + T^q$, so that in particular the height of $\mathfrak{F}$ is h. Let η_0 be a fixed non-trivial element of ker $[\pi]$, the π-division points of $\mathfrak{F}$, and write λ for the logarithm of $\mathfrak{F}$. The Teichmuller character $\omega : \mathcal{O}^*_{K_p} \longrightarrow \mathcal{O}^*_{K_p}$ is defined by taking $\omega(a)$ to be the unique $q-1-$ st root of unity in K_p which satisfies $\omega(a) \equiv a (\mathrm{mod}\, \pi)$. Also, for each residue class $\beta \in \mathbf{Z}/(q-1)\mathbf{Z}$ we denote by $\tau(\beta)$ the Gauss sum to be defined in § 1. If $f \in \mathcal{O}\,[[T]]$, we define $\Delta^{(\beta)}_{\mathfrak{F}} f$ by

$$(\Delta^{(\beta)}_{\mathfrak{F}} f(T) = f(T) - \frac{1}{q} \sum_{c} f(T + {}_{\mathfrak{F}}[c]\,(\eta_0)) \quad \text{if} \quad \beta = 0,$$

$$= \frac{\tau(\beta)}{q} \sum_{c \neq 0} f(T + {}_{\mathfrak{F}}[c]\,(\eta_0))\, \omega^{-\beta}(c) \quad \text{if} \quad \beta \neq 0. \tag{3}$$

Here the sum is taken over a complete set of representatives $\{c\}$ of k_{K_p} in $\mathcal{O}_{K_p}$ if $\beta = 0$ and of $k^*_{K_p}$ if $\beta = 0$. Let e be the ramification degree of K_p over $\mathbf{Q}_p$. We shall prove

THEOREM B. — *Suppose that* $e \leqslant p-1$. *Let* $f \in \mathcal{O}\,[[T]]$ *and* $\alpha \in \mathbf{Z}/(q-1)\mathbf{Z}$. *Then there exists a constant* $\Omega_p \in \mathbf{C}_p$ *with* $v(\Omega_p) = \dfrac{1}{p-1} - \dfrac{1}{e(q-1)}$ *and a unique locally analytic function* $C^{(\alpha)}_f : \mathbf{Z}_p \longrightarrow \mathbf{C}_p$ *such that for each* $\beta \in \mathbf{Z}/(q-1)\mathbf{Z}$

$$C^{(\alpha)}_f(k) = \frac{(-1)^{\alpha-\beta}}{\Omega_p^k} \left(\frac{1}{\lambda'(T)} \frac{d}{dT}\right)^k (\Delta^{(\alpha-\beta)}_{\mathfrak{F}} f)(T)\,|_{T=0} \tag{4}$$

whenever $k \geqslant 0$ *and* $k \in \beta$.

(Locally analytic means that $C^{(\alpha)}_f$ can be expanded in a Taylor series about every $s_0 \in \mathbf{Z}_p$).

If $\mathfrak{F}$ is the multiplicative group $\mathbf{G}_m$ (so that $h = 1$), it is easy to see that Theorem B reduces to a weaker form of Theorem A (iii);

more generally, if $\mathfrak{F}$ is an arbitrary formal group of height 1 the results of Lubin [11] imply that $\mathfrak{F}$ is isomorphic to $\mathbf{G}_m$ and so it is possible to deduce a much stronger form of Theorem B from Theorem A ; thus we shall only regard Theorem B as being of interest when the height of $\mathfrak{F}$ is $\geqslant 2$. After some preliminaries in § 1, we define in § 2 a subring B_0 of $\mathbf{C}_p[[T]]$ which is the analogue of Q_0 and prove the existence of a continuous function interpolating the right hand side of (4). In § 3 we describe a condition on the $f \in B_0$ which ensures that $C_f^{(\alpha)}$ is locally analytic while in § 4 we show that this condition is satisfied if $f \in \mathfrak{O}\,[[T]]$.

A weaker form of Theorem B in the case when the height of $\mathfrak{F}$ is 2 has been proved by Katz [6], [7] and also by Rubin [13], but our argument is more in the line of Lichtenbaum's proof of Theorem A, and in fact there is more than a germ of these ideas in Kummer's note [4].

In a subsequent paper we shall show how these results can be used to construct p-adic L-functions attached to elliptic curves with complex multiplication, even if p is inert or ramified in the field of complex multiplication. It would be interesting to find applications of our results to other situations. For example the power series studied by Coleman [2] and to generalise Theorem B to other kinds of formal groups.

Acknowledgements.

The work in this paper first appeared as part of my Oxford D Phil Thesis, and I would like to thank the SERC for its financial support furing its preparation. My thanks also go to Dr B.J. Birch for suggesting this area of research and giving me his constant support and encouragement.

1. Preliminaries.

Let p be an odd prime. The symbols $\mathbf{Z}$, $\mathbf{Z}_p$, $\mathbf{Q}$, $\mathbf{Q}_p$ have their usual meaning and we write $\mathbf{Z}_+$ for the non-negative integers. Let $\mathbf{C}_p$ denote the completion of the algebraic closure of $\mathbf{Q}_p$, $\mathfrak{O}$ its ring of integers and $\mathfrak{m}$ its maximal ideal. We denote by $v : \mathbf{C}_p^* \longrightarrow \mathbf{Q}$ the p-adic valuation normalised so that $v(p) = 1$.

If L_p is a subfield of $\mathbf{C}_p$ we write $\mathcal{O}_{L_p}$ for its ring of integers, $\mathfrak{m}_{L_p}$ for its maximal ideal, and k_{L_p} for the residue class field; $\mu_n(L_p)$ is the group of n-th roots of unity in L_p and $\mu(L_p)$ the group of all roots of unity in L_p. Let $\omega : \mathcal{O}^* \longrightarrow \mu(\mathbf{C}_p)$ be the Teichmuller character; if $a \in \mathcal{O}^*$ then $\omega(a)$ is the unique prime-to-p-th root of unity congruent to $a \pmod{\mathfrak{m}}$; we also use ω for its restriction to $\mathcal{O}^*_{L_p}$ for any subfield L_p. Let K_p denote an extension of $\mathbf{Q}_p$ of degree h and residue class degree e, and q (a power of p) the cardinality of k_{K_p}. We consider a one-dimensional (commutative) formal group $\mathfrak{F}$ defined over $\mathcal{O}_{F_p}$, where F_p is another finite extension of $\mathbf{Q}_p$, and as in the Introduction we assume that $\mathfrak{F}$ is $\mathcal{O}$-isomorphic to the Lubin-Tate group associated to the polynomial $\pi T + T^q$, where π is a uniformising parameter for K_p (for the theory and basic properties of such groups see Lang [8, Chapter 8]). This implies that the absolute endomorphism ring of $\mathfrak{F}$ is isomorphic to $\mathcal{O}_{K_p}$, and we may suppose that all the elements of End $(\mathfrak{F})$ are defined over F_p, and that $K_p \subseteq F_p$. Let $\lambda(T)$ be the logarithm of $\mathfrak{F}$, i.e. the unique element of $F_p[[T]]$ satisfying

$$\lambda(X +_{\mathfrak{F}} Y) = \lambda(X) + \lambda(Y) \quad \text{and} \quad \lambda(T) = T + O(T^2).$$

It is well-known that $\lambda'(T) \in 1 + T\mathcal{O}[[T]]$ and in fact that

$$\frac{1}{\lambda'(T)} = \frac{\delta}{\delta Y}\mathfrak{F}(X, Y)\,|_{X=T, Y=0} \tag{5}$$

(see Lang [8, Chapter 7]). We denote by ker $[\pi]$ the group of order q which is the kernel of multiplication by π in the group law of $\mathfrak{F}$, and fix a non-trivial element η_0 of ker $[\pi]$, so that ker $[\pi] = \{[c](\eta_0)\}$ as c runs over a set of representatives for k_{K_p} in $\mathcal{O}_{K_p}$ (here $[c] \in$ End $(\mathfrak{F})$ denotes the element corresponding to $c \in \mathcal{O}_{K_p}$).

Let

$$\mathcal{H} = \{f \in \mathcal{O}[[T]] \mid f(X +_{\mathfrak{F}} Y) = f(X)f(Y) \quad \text{and} \quad f(0) = 1\}. \tag{6}$$

Then $\mathcal{H}$ can be identified with $\mathrm{Hom}_{\mathcal{O}}(\mathfrak{F}, \mathbf{G}_m)$. It is evident that every $f \in \mathcal{H}$ induces an element of Hom $(T_p\mathfrak{F}, T_p\mathbf{G}_m)$, $T_p\mathfrak{F}$ and

$T_p \mathbf{G}_m$ being the Tate modules of $\mathfrak{F}$ and $\mathbf{G}_m$ respectively. According to an important result of Tate [15] the induced map

$$\mathrm{Hom}_{\mathcal{O}}(\mathfrak{F}, \mathbf{G}_m) \longrightarrow \mathrm{Hom}(T_p\mathfrak{F}, T_p\mathbf{G}_m)$$

is an isomorphism of $\mathbf{Z}_p$-modules. From this we deduce the following facts which are vital to the following discussion.

FACT 1 : $\mathcal{H}$ is a free $\mathbf{Z}_p$-module of rang h.

FACT 2 : For each non-zero element η of $\ker[\pi]$ there exists $t \in \mathcal{H}$ such that $t(\eta)$ is a *primitive* p-th root of unity.

In our case, if $t \in \mathcal{H}$ then also $t \circ [a] \in \mathcal{H}$ whenever $a \in \mathcal{O}_{K_p}$, and so $\mathcal{H}$ acquires the structure of an $\mathcal{O}_{K_p}$-module, which must necessarily be free of rank one: we fix a generator t_1 and write t_a for $t_1 \circ [a]$. Define a constant Ω_p by

$$t_a(T) = 1 + \Omega_p aT + O(T^2). \tag{7}$$

We denote by Diff $(\mathfrak{F})$ the $\mathcal{O}$-algebra of all $\mathfrak{F}$-invariant differential operators taking $\mathcal{O}[[T]]$ into itself (recall that $\mathfrak{F}$-invariant means that $(Df)(T +_{\mathfrak{F}} w) = D(f(T +_{\mathfrak{F}} w))$ for all $D \in \mathrm{Diff}(\mathfrak{F})$, $f \in \mathcal{O}[[T]]$ and $w \in \mathfrak{m}$). It is known that Diff $(\mathfrak{F})$ is the free $\mathcal{O}$-module on the operators D_n, $n \in \mathbf{Z}_+$ defined by the "Taylor expansion"

$$f(X +_{\mathfrak{F}} Y) = \sum_{n=0}^{\infty} (D_n f)(X)\, Y^n. \tag{8}$$

We now recall some properties of $\mathcal{H}$ and Diff $(\mathfrak{F})$ (cf. [6], [7]).

LEMMA 1. – (i) *Each* $t \in \mathcal{H}$ *is a simultaneous eigenfunction for all the* $D \in \mathrm{Diff}(\mathfrak{F})$; *in fact* $(Dt)(T) = Dt(0)\, t(T)$.

(ii) *We have the expansion*

$$t(T) = \sum_{n=0}^{\infty} (D_n t)(0)\, T^n .$$

(iii) $(D_0 f)(T) = f(T)$ *and* $(D_1 f)(T) = \dfrac{1}{\lambda'(T)} f'(T)$ *for all* $f \in \mathbf{C}_p[[T]]$, *i.e.* D_1 *is the logarithmic derivative of* $\mathfrak{F}$.

(iv) *If* $a, b \in \mathcal{O}_{K_p}$ *then* $t_{a+b}(T) = t_a(T)\, t_b(T)$, $t_0(T) = 1$, $t_{ab}(T) = t_a([b](T)) = t_b([a](T))$, *and if* $b \in \mathbf{Z}_p$ *then*

$$t_{ab}(T) = t_a(T)^b = \sum_{n=0}^{\infty} (t_a(T) - 1)^n \binom{b}{n}.$$

Proof. – (i) We have

$$Dt(T +_{\mathcal{F}} w) = D(t(T +_{\mathcal{F}} w)) = D(t(T)\, t(w)) = (Dt)(T)\, t(w)$$

for all $w \in m$. Putting $T = 0$ we obtain $(Dt)(w) = (Dt)(0)\, t(w)$ and since w is arbitrary the assertion follows.

(ii) This is the special case $X = 0$, $Y = T$ of (8).

(iii) Since

$$f(X +_{\mathcal{F}} Y) = f(\mathcal{F}(X, Y)) = \sum_{n=0}^{\infty} \frac{Y^n}{n!} \left. \frac{\delta^n f(\mathcal{F}(X, Y))}{\delta Y^n} \right|_{Y=0}$$

by the "usual" Taylor expansion, we find that $D_0 f = f$ and

$$(D_1 f)(T) = \left. \frac{\delta f(\mathcal{F}(X, Y))}{\delta Y} \right|_{X=T,\, Y=0} = \frac{1}{\lambda'(T)} f'(T)$$

using the chain rule together with (5).

(iv) This is obvious from the definition of $\mathcal{H}$; note that the last expression is well-defined since $t_a(T) - 1$ has no constant term.

Our next task is to define the Gauss sum $\tau(\beta)$ appearing in Theorem B. Fact 2 above together with part (iv) of Lemma 1 tell us that t_a induces a homomorphism from $\ker[\pi]$ *onto* $\mu_p(\mathbf{C}_p)$ if and only if $a \not\equiv 0 \pmod{\pi}$. In particular $t_a = t_b$ (restricted to $\ker[\pi]$) if and only if $a \equiv b \pmod{\pi}$.

LEMMA 2. – (ii) *Let* $\eta \in \ker[\pi]$. *Then*

$$\sum_{a \bmod \pi} t_a(\eta) = 0 \quad \text{if} \quad \eta \neq 0$$
$$= q \quad \text{if} \quad \eta = 0.$$

(ii) *Let* $a \in \mathcal{O}_{K_p}$. *Then*

$$\sum_{\eta \in \ker \pi} t_a(\eta) = 0 \quad \text{if} \quad a \not\equiv 0 \pmod{\pi}$$
$$= q \quad \text{if} \quad a \equiv 0 \pmod{\pi}.$$

Proof. – (i) If $\eta \neq 0$ then $\sum\limits_a t_a(\eta) = qp^{-1} \sum\limits_{\xi \in \eta_p} \xi = 0$ while if $\eta = 0$ then $\sum\limits_a t_a(\eta) = \sum\limits_a 1 = q$ by Fact 2. The proof of (ii) is similar.

Now let $\beta \in \mathbf{Z}/(q-1)\mathbf{Z}$ with $\beta \neq 0$ and recall that η_0 is a fixed non-trivial element of $\ker[\pi]$. Define

$$\tau_a(\beta) = \sum_u{}' \omega^\beta(u)\, t_a([u](\eta_0)),$$

where Σ' indicates that the sum is taken over a complete set of representatives of $k^*_{K_p}$ in $\mathcal{O}_{K_p}$ (i.e. omitting the term $u \equiv 0 \pmod{\pi}$); and write $\tau(\beta)$ for $\tau_1(\beta)$. The $\tau_a(\beta)'s$ may be thought of as Gauss sums and we have

LEMMA 3. – (i) $\tau_a(\beta) = \omega^{-\beta}(a)\,\tau(\beta)$ *if* $a \in \mathcal{O}^*_{K_p}$.

(ii) $\tau(\beta)\,\tau(-\beta) = (-1)^\beta q$.

Proof. – (i) We have

$$\begin{aligned}\tau_a(\beta) &= \sum_u{}' \omega^\beta([u](\eta_0)) \\ &= \sum_u{}' \omega^\beta(u)\, t_1([au](\eta_0)) \\ &= \omega^{-\beta}(a) \sum_u{}' \omega^\beta(au)\, t_1([au](\eta_0))\end{aligned}$$

and (i) follows.

(ii) we have

$$\begin{aligned}\tau(\beta)\,\tau(-\beta) &= \sum_{u,v}{}' \omega^\beta(u)\,\omega^{-\beta}(v)\, t_1([u](\eta_0))\, t_1([v](\eta_0)) \\ &= \sum_{u,x}{}' \omega^\beta(u)\,\omega^{-\beta}(-xu)\, t_1([u-xu](\eta_0))\end{aligned}$$

(on writing $v = -xu$)

$$= (-1)^\beta \sum_x{}' \omega^{-\beta}(x) \sum_u{}' t_1([u-xu](\eta_0)).$$

But by Lemma 2 (ii) $\sum_u' t_1([u - xu](\eta_0)) = q - 1$ if $x \equiv 1 \pmod{\pi}$ and -1 otherwise. Therefore

$$\begin{aligned}\tau(\beta)\,\tau(-\beta) &= (-1)^\beta\,[(q-1) + \sum_{x \not\equiv 1\,(\pi)} \omega^{-\beta}(x)\,(-1)] \\ &= (-1)^\beta\,[(q-1) + (-1)(-1)] \\ &= (-1)^\beta\, q\,,\end{aligned}$$

as claimed.

2. An interpolation theorem.

In this section we define a ring of power series $B_0 \subseteq \mathbf{C}_p[[T]]$ and a "twisting operator" $\Delta_{\mathfrak{F}}^{(\beta)}$ for each residue class β mod $(q-1)$ of $\mathbf{Z}$, and prove an interpolation theorem for the quantities $(D_1^k\,\Delta_{\mathfrak{F}}^{(\beta)} f)(0)$, $k = 0, 1, 2, \ldots,$ where $D_1 = \dfrac{1}{\lambda'(T)}\dfrac{d}{dT}$ and $f \in B_0$.

We first introduce a notational convention which will be in constant use throughtout this and the next section : if $x \in \mathbf{C}_p^h$ (resp. K_p^h, resp. $\mathbf{Z}_+^h$ etc.) then we denote the i-th component of x by x_i. Conversely, if a system of h elements of $\mathbf{C}_p$ (resp. K_p, resp. $\mathbf{Z}_+$ etc.) has been denoted by a letter with suffices $i = 1, 2, \ldots, h$ then the same letter (without a suffix) is used for the corresponding element of $\mathbf{C}_p^h$ (resp. K_p^h, resp. $\mathbf{Z}_+^h$ etc.). If $n \in \mathbf{Z}_+^h$ we write $n!$ for $\prod_{i=1}^h n_i!$. If $X_1, X_2, \ldots, X_h$ are indeterminates, the monomial $X_1^{n_1} X_2^{n_2} \ldots X_h^{n_h}$ is abbreviated to X^n; however the letter T will always stand for a single indeterminate.

Let $x \in \mathcal{O}_{K_p}^h$ be a basis for $\mathcal{O}_{K_p}$ over $\mathbf{Z}_p$, and Q_0 the ring

$$\left\{ F(X) = \sum_{n \in \mathbf{Z}_+^h} \frac{c_n X^n}{n!} \in \mathbf{C}_p[[X_1, X_2, \ldots, X_h]] \mid v(c_n) \longrightarrow \infty \text{ as } n \longrightarrow \infty \right\}.$$

Define a homomorphism $\epsilon : Q_0 \longrightarrow \mathbf{C}_p[[T]]$ by setting

$$\epsilon(X_i) = t_{X_i}(T) - 1$$

for each $i = 1, 2, \ldots, h$. This is well-defined since $t_a(T) - 1$ has no constant term.

DEFINITION. — *B_0 is the image of ϵ in $\mathbf{C}_p[[T]]$. If $a \in \mathcal{O}_{K_p}$ we can write $a = \sum_{i=1}^{h} v_i x_i$ where $v_i \in \mathbf{Z}_p$ and so (using Lemma 1 (iv)) $t_a(T) = \prod_{i=1}^{h} t_{X_i}(T)^{v_i} = \epsilon\left(\prod_{i=1}^{h} (1 + X_i)^{v_i}\right)$. This implies at once that B_0 does not depend on the choice of basis x.*

Let $\beta \in \mathbf{Z}/(q-1)\mathbf{Z}$. One would like to define the $\mathcal{O}$-linear operator $\Delta_{\mathfrak{f}}^{(\beta)} : B_0 \longrightarrow \mathbf{C}_p[[T]]$ by

$$(\Delta_{\mathfrak{f}}^{(\beta)} f)(T) = f(T) - \frac{1}{q}\sum_{u} f(T) +_{\mathfrak{f}} [u](\eta_0)) \qquad \text{if} \quad \beta = 0,$$

$$= \frac{\tau(\beta)}{q} \sum_{u}{}' f(T) +_{\mathfrak{f}} [u](\eta_0))\, \omega^{-\beta}(u) \qquad \text{if} \quad \beta \neq 0.$$

However at first sight it is not clear whether this is well-defined owing to the possible presence of denominators in the coefficients of f. The fact that it is follows from

LEMMA 4. — *Let $\eta \in \ker[\pi]$ and $f \in B_0$. Then $f(T +_{\mathfrak{f}} \eta)$ is a well-defined element of B_0, whence $\Delta_{\mathfrak{f}}^{(\beta)}$ is a well-defined operator taking values in B_0.*

Proof. — Let $f = \epsilon(F)$ with $F \in Q_0$. Define $\zeta \in (\mu_p(\mathbf{C}_p))^h$ by $\zeta_i = t_{X_i}(\eta)$ for each $i = 1, 2, \ldots, h$. It is well-known that

$$v(\zeta_i - 1) \geqslant \frac{1}{p-1} \quad \text{and} \quad v(n!) \leqslant \frac{\sum n_i}{p-1} \quad \text{if } n \in \mathbf{Z}_+^h.$$ These estimates imply that

$$F_\zeta(X_1, \ldots, X_h) := F((\zeta_1 - 1) + \zeta_1 X_1, \ldots, (\zeta_h - 1) + \zeta_h X_h)$$

is an element of Q_0. Now since

$$t_a(\mathrm{T} +_{\mathfrak{s}} \eta) - 1 = t_a(\mathrm{T})\, t_a(\eta) - 1 = t_a(\eta) - 1 + t_a(\eta)\,(t_a(\mathrm{T}) - 1)$$

we have

$$\mathrm{F}(t_{x_1}(\mathrm{T} +_{\mathfrak{s}} \eta) - 1, \dots, t_{x_h}(\mathrm{T} +_{\mathfrak{s}} \eta) - 1) = \mathrm{F}_\zeta(t_{x_1}(\mathrm{T}) - 1, \dots, t_{x_h}(\mathrm{T}) - 1) \quad (9)$$

and so we would like to define $f(\mathrm{T} +_{\mathfrak{s}} \eta)$ by the right hand side of (9). To do this we need to check that this is independent of the choice of F. One way to do this is as follows; – it suffices to consider the case $f = 0$: now $\mathrm{F} \in \mathrm{Q}_0$ implies that F converges at all $z \in \mathbf{C}_p^h$ with $v(z_i) \geqslant \dfrac{1}{p-1}$ and $y \longmapsto t_{x_i}(y) - 1$ defines a homeomorphism from an open subset $\mathfrak{N}$ of $\mathbf{C}_p$ containing the origin into $\mathbf{C}_p$. Hence

$$\mathrm{F}(t_{x_1}(\mathrm{T}) - 1, \dots, t_{x_h}(\mathrm{T}) - 1) = 0 \quad \text{in} \quad \mathbf{C}_p[[\mathrm{T}]]$$

implies that

$$\mathrm{F}(t_{x_1}(y) - 1, \dots, t_{x_h}(y) - 1) = 0$$

for all $y \in \mathfrak{N}$, i.e.

$$\mathrm{F}((\zeta_1 - 1) + \zeta_1(t_{x_1}(y') - 1), \dots, (\zeta_h - 1) + \zeta_h(t_{x_h}(y') - 1)) = 0$$

and therefore

$$\mathrm{F}_\zeta(t_{x_1}(y') - 1, \dots, t_{x_h}(y') - 1) = 0$$

for all y' such that $y' +_{\mathfrak{s}} \eta \in \mathfrak{N}$. Since a power series that vanishes on an open set on which it converges vanishes identically, we conclude that

$$\mathrm{F}_\zeta(t_{x_1}(\mathrm{T}) - 1, \dots, t_{x_1}(\mathrm{T}) - 1) = 0$$

which is what is required.

The following lemma shows that any $f \in \mathrm{B}_0$ can be decomposed as a sum of functions on which the $\Delta_{\mathfrak{s}}^{(\beta)}$'s act especially simply.

LEMMA 5. – *Let* $f \in \mathrm{B}_0$ *and for* $a \in \mathcal{O}_{\mathrm{K}_p}$ *define*

$$\mathrm{F}_a(\mathrm{T}) = \sum_{\eta \in \ker[\pi]} f(\mathrm{T} +_{\mathfrak{s}} \eta)\, t_a(\eta)\,; \quad (10)$$

then (i) $(\Delta_{\mathfrak{g}}^{(\beta)} F_a)(T) = \omega^\beta(a) F_a(T)$ *if* $a \not\equiv 0 \pmod{\pi}$

$= 0$ *if* $a \equiv 0 \pmod{\pi}$.

(ii) *We have* $f(T) = \frac{1}{q} \sum_{a \bmod \pi} F_a(T)$.

(iii) *If* $\beta \neq 0$ *then*

$$(\Delta_{\mathfrak{g}}^{(\beta)} f)(T) = \frac{1}{q} \sum_a{}' \omega^\beta(a) F_a(T) = \frac{1}{q} \sum_a{}' (\Delta_{\mathfrak{g}}^{(\beta)} F_a)(T).$$

Proof. – (i) Suppose that $\beta \neq 0$. Then

$$(\Delta_{\mathfrak{g}}^{(\beta)} F_a)(T)$$

$$= \sum_{\eta \in \ker[\pi]} (\Delta_{\mathfrak{g}}^{(\beta)} f(T +_{\mathfrak{g}} \eta) t_a(\eta)$$

$$= \frac{\tau(\beta)}{q} \sum_\eta \sum_u{}' f(T +_{\mathfrak{g}} [u](\eta_0) +_{\mathfrak{g}} \eta) t_a(\eta) \omega^{-\beta}(u)$$

$$= \frac{\tau(\beta)}{q} \sum_v \sum_u{}' f(T +_{\mathfrak{g}} [u + v](\eta_0)) t_a([v](\eta_0)) \omega^{-\beta}(u)$$

$$= \frac{\tau(\beta)}{q} \sum_x \sum_u{}' f(T +_{\mathfrak{g}} [x](\eta_0)) t_a([x - u](\eta_0)) \omega^{-\beta}(u)$$

(writing $u + v = x$)

$$= \frac{\tau(\beta)}{q} \Big(\sum_x f(T +_{\mathfrak{g}} [x](\eta_0)) t_a([x](\eta_0))\Big) \Big(\sum_u{}' t_a([-u](\eta_0)) \omega^{-\beta}(u)\Big)$$

$$= \frac{\tau(\beta)}{q} F_a(T) (-1)^\beta \tau_a(-\beta)$$

$$= \omega^\beta(a) F_a(T)$$

by Lemma 3. The case $\beta = 0$ of (i) as well as parts (ii) and (iii) require similar calculations and will be omitted.

We shall now state and prove the main result of this section.

THEOREM 6. – *Let* $f \in \mathrm{B}_0$ *and* $\alpha \in \mathbf{Z}/(q-1)\mathbf{Z}$. *Then there exists a unique continuous function* $\mathrm{C}_f^{(\alpha)} : \mathbf{Z}_p \longrightarrow \mathbf{C}_p$ *such that for each* $\beta \in \mathbf{Z}/q-1)\mathbf{Z}$

$$\mathrm{C}_f^{(\alpha)}(k) = (-1)^{\alpha-\beta} \frac{\mathrm{D}_1^k(\Delta_{\mathfrak{s}}^{(\alpha-\beta)} f)(0)}{\Omega_p^k}$$

whenever $k \geqslant 0$ *and* $k \in \beta$.

Proof. – The uniqueness is clear, since $\mathbf{Z}_+$ is dense in $\mathbf{Z}_p$. Evidently $t_a \in \mathrm{B}_0$ for all $a \in \mathcal{O}_{\mathrm{K}_p}$, and we claim that

$$(\Delta_{\mathfrak{s}}^{(\beta)} t_a)(\mathrm{T}) = (-1)^\beta \, \omega^\beta(a) \, t_a(\mathrm{T}) \quad \text{if} \quad a \not\equiv 0 \pmod{\pi}$$

$$= 0 \quad \text{if} \quad a \equiv 0 \pmod{\pi}$$

for each $\beta \in \mathbf{Z}/(q-1)\mathbf{Z}$. Indeed suppose that $a \not\equiv 0 \pmod{\pi}$ and $\beta \neq 0$. Then we compute

$$\begin{aligned}(\Delta_{\mathfrak{s}}^{(\beta)} t_a)(\mathrm{T}) &= \frac{\tau(\beta)}{q} \sum_u{}' \, t_a(\mathrm{T} + {}_{\mathfrak{s}}[u](\eta_0)) \, \omega^{-\beta}(u) \\ &= \frac{\tau(\beta)}{q} \, t_a(\mathrm{T}) \sum_u{}' \, t_a([u](\eta_0)) \, \omega^{-\beta}(u) \\ &= \frac{\tau(\beta)}{q} \, t_a(\mathrm{T}) \, \tau_a(-\beta) \\ &= \omega^\beta(a) \, t_a(\mathrm{T}) \, (-1)^\beta \end{aligned}$$

by Lemma 3. The other cases are similar.

Now $(\mathrm{D}_1 t_a)(0) = \Omega_p a$ by (7) and Lemma 1 (ii). Hence

$$(-1)^{\alpha-\beta} \frac{(\mathrm{D}_1^k \, \Delta_{\mathfrak{s}}^{(\alpha-\beta)} t_a)(0)}{\Omega_p^k} = \omega^{\alpha-\beta}(a) \, a^k \quad \text{if} \quad a \not\equiv 0 \pmod{\pi}$$

$$= 0 \qquad \text{if} \quad a \equiv 0 \pmod{\pi}.$$

Define $\langle a \rangle$, for $a \in \mathcal{O}_{\mathrm{K}_p}$, by $\langle a \rangle \, \omega(a) = a$ if $a \not\equiv 0 \pmod{\pi}$ and $\langle a \rangle = 0$ if $a \equiv 0 \pmod{\pi}$. Then $\langle a \rangle \equiv 1 \pmod{\pi}$ if $a \not\equiv 0 \pmod{\pi}$ and so $\langle a \rangle^s$ is well-defined for all $s \in \mathbf{Z}_p$; we interpret $\omega^\alpha(a)$ and $\langle a \rangle^s$ as 0 if $a \equiv 0 \pmod{\pi}$. With these conventions, we have

$$\mathrm{C}_{t_a}^{(\alpha)}(s) = \omega^\alpha(a) \, \langle a \rangle^s .$$

Now let $f \in \mathrm{B}_0$. Then we can write

$$f = \sum_{n \in \mathbf{Z}_+^h} \frac{c_n (t_x - 1)^n}{n\,!} \tag{11}$$

where $(t_x - 1)^n$ is an abbreviation for

$$(t_{x_1}(\mathrm{T}) - 1)^{n_1} \dots (t_{x_h}(\mathrm{T}) - 1)^{n_h},$$

and $v(c_n) \longrightarrow \infty$ *as* $n \longrightarrow \infty$. If $\binom{n}{r} = \prod_{i=1}^{h} \binom{n_i}{r_i}$ for each $n, r \in \mathbf{Z}_+^h$ then

$$(t_x - 1)^n = \sum_{r=0}^{n} (-1)^{\sum_i n_i - r_i} \binom{n}{r} t_{x \cdot r}$$

where $x \cdot r = \sum_{i=1}^{h} x_i r_i$, so that

$$\mathrm{C}^{(\alpha)}_{(t_x - 1)^n}(s) = \sum_{r=0}^{n} (-1)^{\sum_i n_i - r_i} \binom{n}{r} \omega^\alpha (x \cdot r) \langle x \cdot r \rangle^s . \tag{12}$$

In view of this, and the fact that $v(c_n) \longrightarrow \infty$, the theorem will be proved if we can show that

$$\mathrm{C}^{(\alpha)}_{(t_x - 1)^n}(s) \equiv 0 \pmod{n\,!} \tag{13}$$

whenever $n \in \mathbf{Z}_+^h$. Let $k \in \mathbf{Z}_+$ satisfy $k \in \alpha$, and $ev(n\,!) \leqslant k$, where e is the ramification degree of K_p over $\mathbf{Q}_p$; then

$$\mathrm{C}^{(\alpha)}_{(t_x - 1)^n}(k) = \sum_{r=0}^{n} (-1)^{\sum_i n_i - r_i} \binom{n}{r} \omega^\alpha (x \cdot r) \langle x \cdot r \rangle^k$$

$$\equiv \sum_{r=0}^{n} (-1)^{\sum_i n_i - r_i} \binom{n}{r} (x \cdot r)^k \pmod{\pi^k}$$

(so that this congruence also holds modulo $n\,!$) and

$$\sum_{r=0}^{n} (-1)^{\sum n_i - r_i} \binom{n}{r} (x \cdot r)^k = \left[\left(\frac{d}{dz}\right)^k \prod_{i=1}^{h} (\exp(x_i z) - 1)^{n_i} \right]_{z=0} .$$

Since the set of integers k described above is dense in $\mathbf{Z}_p$, the theorem follows from the following lemma (cf. [3 § 3.5]) :

LEMMA 7. — *For all* $k \in \mathbf{Z}_+$ *we have the congruence*

$$\delta_k(n) := \left[\left(\frac{d}{dz}\right)^k \prod_{i=1}^{h} (\exp(x_i z) - 1)^{n_i} \right]_{z=0} \equiv 0 \ (\mathrm{mod}\ n\,!) .$$

Proof. — If $k < \Sigma\, n_i$ then $\delta_k(n) = 0$ and the assertion is trivial. On the other hand

$$\delta_{k+1}(n) = \left[\left(\frac{d}{dz}\right)^k \left(\frac{d}{dz}\right) \prod_{i=1}^{h} (\exp(x_i z) - 1)^{n_i} \right]_{z=0}$$

$$= \sum_{i=1}^{h} x_i n_i (\delta_k(n^{(i)}) + \delta_k(n))$$

where $n^{(i)}$ is obtained from n by replacing n_i by $n_i - 1$. Hence if $\delta_k(n) \equiv 0 \ (\mathrm{mod}\ n\,!)$ and $\delta_k(n^{(i)}) \equiv 0 \ (\mathrm{mod}\ n^{(i)}\,!)$ then

$$\delta_{k+1}(n) \equiv 0 \ (\mathrm{mod}\ n\,!)$$

as required.

3. An analyticity theorem

The function $C_f^{(\alpha)}$ introduced in the previous section does not appear to have any analyticity properties for an arbitrary $f \in B_0$; however we can prove that $C_f^{(\alpha)}$ is locally analytic if the coefficients c_n in (11) can be chosen to tend to zero sufficiently fast. More precisely we have

THEOREM 8. — *Let notation be as in Theorem 6. Suppose that there exist real numbers* A, B *with* B > 0 *such that*

$$v(c_n) \geqslant A + Bv(n\,!)$$

for all $n \in \mathbf{Z}_+^h$. *Then* $C_f^{(\alpha)}$ *is locally analytic on* $\mathbf{Z}_p$ *in the following sense : at every* $s_0 \in \mathbf{Z}_p$, *it has a power series expansion*

$$C_f^{(\alpha)}(s) = \sum_{k=0}^{\infty} \sigma_k(s_0)(s-s_0)^k$$

with non-zero radius of convergence.

Proof. – Suppose first that $f(T) = t_a(T)$ for some $a \in \mathcal{O}_{K_p}$. We saw in the proof of Theorem 6 that $C_f^{(\alpha)}(s) = \omega^\alpha(a)\langle a\rangle^s$ if $a \not\equiv 0 \pmod{\pi}$ while $C_f^{(\alpha)}(s) = 0$ if $a \equiv 0 \pmod{\pi}$. Hence

$$\begin{aligned} C_f^{(\alpha)}(s) &= \sum_{k=0}^{\infty} \frac{\omega^\alpha(a)(\log_p\langle a\rangle)^k \langle a\rangle^{s_0}}{k!}(s-s_0)^k \quad \text{if} \quad a \not\equiv 0 \bmod \pi) \\ &= 0 \quad \text{if} \quad a \equiv 0 \pmod{\pi} \end{aligned} \tag{14}$$

so that if we now take $f(T) = (t_x(T)-1)^n = \prod_{i=1}^{h} (t_{x_i}(T)-1)^{n_i}$

then by (12) and (14)

$$C_f^{(\alpha)}(s) = \sum_{k=0}^{\infty} \delta(n,k,s_0)(s-s_0)^k$$

where

$$\begin{aligned} \delta(n,k,s_0) &= \sum_{r=0}^{n} (-1)^{\sum_i n_i - r_i} \binom{n}{r} \omega^\alpha(x\cdot r)\langle x\cdot r\rangle^{s_0} \\ &\qquad \frac{(\log_p\langle x\cdot r\rangle)^k}{k!} \quad \text{if} \quad x\cdot r \not\equiv 0 \pmod{\pi} \\ &= 0 \quad \text{if} \quad x\cdot r \equiv 0 \pmod{\pi}. \end{aligned} \tag{15}$$

Now suppose that $f(T) = \sum_{n\in\mathbf{Z}_+^h} c_n \frac{(t_x(T)-1)^n}{n!}$ as in (11). Then Theorem 8 will be proved if we can show that

$$\sum_{n\in\mathbf{Z}_+^h} c_n \frac{\delta(n,k,s_0)}{n!} \tag{16}$$

converges for all $k \in \mathbf{Z}_+$ and, if its sum is denoted by $\sigma_k(s_0)$, then

$$v(\sigma_k(s_0)) \geqslant A + B'k \tag{17}$$

for some constant B' depending only on B.

If $F : \mathbf{Z}_p^h \longrightarrow \mathbf{C}_p$ is any function and $n \in \mathbf{Z}_+^h$ we define $M(n, F)$ to be the expression

$$M(n,F) = \sum_{r=0}^{n} (-1)^{\sum_i n_i - r_i} \binom{n}{r} F(r)$$

where the sum is taken over all $r \in \mathbf{Z}_+^h$ with $0 \leqslant r_i \leqslant n_i$ for each i. In particular

$$\delta(n, k, s_0) = M(n, G) \tag{18}$$

where G is defined by

$$G(\rho) = \omega^\alpha(x \cdot \rho) \langle x \cdot \rho \rangle^{s_0} \frac{(\log_p < x \cdot \rho >)^k}{k\,!} \qquad \text{if } x \cdot \rho \not\equiv 0 \pmod{\pi}$$

$$= 0 \quad \text{if} \quad x \cdot \rho \equiv 0 \pmod{\pi}.$$

The proof of assertions (16) and (17) will require a couple of lemmas.

LEMMA 9. – (i) *The map* $F \longmapsto M(n, F)$ *is* $\mathbf{C}_p$*-linear and if* F *takes values in* $\mathfrak{O}$ *then* $M(n, F) \in \mathfrak{O}$.

(ii) *If* F *and* F′ *take values in* $\mathfrak{O}$ *and* $F(\rho) \equiv F'(\rho) \pmod{\pi^m}$ *for some* $m \geqslant 0$ *and all* $\rho \in \mathbf{Z}_p^h$ *then*

$$M(n, F) \equiv M(n, F') \pmod{\pi^m}$$

for all $n \in \mathbf{Z}_+^h$.

(iii) *Let* F *be defined by*

$$F(\rho) = (\langle x \cdot \rho \rangle - 1)^\ell \, \omega^\alpha(x \cdot \rho) \langle x \cdot \rho \rangle^s$$

if $x \cdot \rho \not\equiv 0 \pmod{\pi}$ *and* $F(\rho) = 0$ *if* $x \cdot \rho \equiv 0 \pmod{\pi}$. *Then* $v(M(n, F)) \geqslant \max\left(\frac{\ell}{e}, v(n\,!)\right)$, *where* e *is the ramification degree of* K_p *over* $\mathbf{Q}_p$.

Proof. – Assertion (i) is trivial. (ii) follows from (i) by considering the function $\frac{1}{\pi^m}(F - F')$. To prove (iii) observe first that if $F_0(\rho) = \omega^\alpha(x \cdot \rho) \langle x \cdot \rho \rangle^s$ for $x \cdot \rho \not\equiv 0 \pmod{\pi}$ and $F_0(\rho) = 0$ otherwise, then $v(M(n, F_0)) \geqslant v(n\,!)$; indeed this is just the content of equation (13) of the previous section. But F is an $\mathfrak{O}$-linear combination of functions of this form so that $v(\mathrm{M}(n,\mathrm{F})) \geqslant v(n!)$ also. On the other hand $\langle x \cdot \rho \rangle \equiv 1 \pmod{\pi}$ if $x \cdot \rho \not\equiv 0 \pmod{\pi}$ and so $\mathrm{F}(\rho) \equiv 0 \pmod{\pi^{\ell}}$ for all ρ so that $v(\mathrm{M}(n,\mathrm{F})) \geqslant \ell e^{-1}$ by (ii).

LEMMA 10. – *For* $k, \ell \in \mathbf{Z}_+$ *let* $\epsilon_{k,\ell}$ *be defined by the expansion*

$$(\log(1+\mathrm{T}))^k = \sum_{\ell=0}^{\infty} \epsilon_{k,\ell}\,\mathrm{T}^{\ell},$$

where $\log(1+\mathrm{T}) = \sum_{\ell=1}^{\infty} (-1)^{\ell+1} \frac{\mathrm{T}^{\ell}}{\ell}$. *Then we have* $\epsilon_{k,\ell} = 0$ *if* $\ell < k$ *and* $v(\epsilon_{k,\ell}) \geqslant -k\,\frac{\log \ell - \log k}{\log p}$ *if* $\ell \geqslant k$.

Proof. – It is clear that $\epsilon_{k,\ell} = 0$ if $\ell < k$. On the other hand if $\ell \geqslant k$ then

$$\epsilon_{k,\ell} = \sum_{\substack{m_i \geqslant 1 \\ m_1+\dots+m_k=\ell}} \frac{(-1)^{m_1+m_2+\dots+m_k-k}}{m_1 m_2 \dots m_k}$$

and so

$$v(\epsilon_{k,\ell}) \geqslant \min_{\substack{m_i \geqslant 1 \\ m_1+\dots+m_k=\ell}} v\left(\frac{1}{m_1 m_2 \dots m_k}\right).$$

Therefore we need to estimate $\max v(m_1 m_2 \dots m_k)$. Now by an elementary inequality $\left(\prod_{i=1}^{k} m_i\right)^{\frac{1}{k}} \leqslant \frac{1}{k} \sum_{i=1}^{k} m_i = \frac{\ell}{k}$ and so

$$\sum_{i=1}^{k} \log m_i \leqslant k\left(\log \frac{\ell}{k}\right).$$

But $v(m_i) \leqslant \frac{\log m_i}{\log p}$ for all i and so

$$v(m_1 m_2 \dots m_k) = \sum_{i=1}^{k} v(m_i) \leqslant \frac{\sum_{i=1}^{k} \log m_i}{\log p} \leqslant k\left(\frac{\log(\ell/k)}{\log p}\right)$$

and the result follows.

We can now estimate $\delta(n, k, s_0) = M(n, G)$ where G is the function in (18). In fact

$$G(\rho) = \frac{1}{k!}\omega^\alpha(x \cdot \rho)\langle x \cdot \rho\rangle^{s_0} \sum_{\ell=k}^{\infty} \epsilon_{k,\ell}(\langle x \cdot \rho\rangle - 1)^\ell \quad \text{if } x \cdot \rho \not\equiv 0$$

$$= 0 \quad \text{if } x \cdot \rho \equiv 0 \pmod{\pi},$$

and so combining Lemmas 9 (iii) and 10 we find that

$$v(\delta(n, k, s_0)) \geqslant \min_{\ell \geqslant k} \left\{\max\left(\frac{\ell}{e} + v(\epsilon_{k,\ell}), v(n!) + v(\epsilon_{k,\ell})\right)\right\} - v(k!)$$

whence

$$v\left(\frac{\delta(n, k, s_0)}{n!}\right) \geqslant \min_{\ell \geqslant k}$$

$$\left\{\max\left(\frac{\ell}{e} - v(n!) - k\left(\frac{\log \ell - \log k}{\log p}\right), -k\left(\frac{\log \ell - \log k}{\log p}\right)\right)\right\} - v(k!).$$

It is easy to see that the minimum is attained at

$$\ell = \frac{e}{\log p} k \qquad \text{if } e \geqslant \log p \text{ and } (\log p)\, v(n!) \leqslant k,$$

$$\ell = k \qquad \text{if } e \leqslant \log p \text{ and } ev(n!) \leqslant k,$$

and $\ell = ev(n!)$ if $\inf(e, \log p)\, v(n!) \geqslant k$.

Taking each of these cases in turn, we have

$$v\left(\frac{\delta(n, k, s_0)}{n!}\right) \geqslant \frac{k}{\log p} - v(n!) - k\left(\frac{\log(e/\log p)}{\log p}\right) - v(k!),$$

or

$$\geqslant \frac{k}{e} - v(n!) - v(k!),$$

or

$$\geqslant -k\left(\frac{\log(ev(n!)) - \log k}{\log p}\right) - v(k!).$$

Hence if $v(c_n) \geqslant \mathrm{A} + \mathrm{B}v(n\,!)$ for some $\mathrm{B} > 0$, then

$$v\left(c_n \frac{\delta(n, k, s_0)}{n\,!}\right) \longrightarrow \infty \quad \text{as} \quad n \longrightarrow \infty,$$

(k fixed) and so (16) is proved.

We now turn to the proof of (17). For $\xi > 0$ and $k \in \mathbf{Z}_+$ define

$$y_k(\xi) = \mathrm{A} + \mathrm{B}\xi + \frac{k}{\log p} - \xi - k\,\frac{\log(e/\log p)}{\log p} - v(k\,!)$$

$$\text{if } e \geqslant \log p \text{ and } (\log p)\,\xi \leqslant k,$$

$$= \mathrm{A} + \mathrm{B}\xi + \frac{k}{e} - \xi - v(k\,!) \qquad \text{if } e \leqslant \log p \text{ and } e\,\xi \leqslant k,$$

$$= \mathrm{A} + \mathrm{B}\xi - k\left(\frac{\log e\xi - \log k}{\log p}\right) - v(k\,!)$$

$$\text{if } \inf(e, \log p)\,\xi \geqslant k.$$

Then if $\sigma_k(s_0) = \sum_{n \in \mathbf{Z}_+^h} c_n \dfrac{\delta(n, k, s_0)}{n\,!}$ we have

$$v(\sigma_k(s_0)) \geqslant \min_{n \in \mathbf{Z}_+^h} (y_k(v(n\,!))) \geqslant \inf_{\xi > 0} y_k(\xi).$$

We may suppose that $\mathrm{B} \leqslant \dfrac{\inf(\log p, e)}{\log p}$. Then $y_k(\xi)$ is decreasing in $0 \leqslant \xi \leqslant \dfrac{k}{\inf(\log p, e)}$ and a routine computation shows that $y_k(\xi)$ has a unique minimum at $\xi = \dfrac{k}{\mathrm{B}\log p}$ which is greater than $\dfrac{k}{\inf(\log p, e)}$. Hence

$$\inf_{\xi > 0} y_k(\xi) = y_k\left(\frac{k}{\mathrm{B}\log p}\right)$$

$$= \mathrm{A} + k\left(\frac{1 + \log \mathrm{B} + \log\log p - \log e}{\log p}\right) - v(k\,!).$$

Recalling that $v(k\,!) \leqslant \dfrac{k}{p-1}$ we see that

$$v(\sigma_k(s_0)) \geqslant \mathrm{A} + k\left(\frac{1+\log \mathrm{B} + \log\log p - \log e}{\log p}\right) - \frac{k}{p-1}$$

for all k, and so we may take

$$\mathrm{B}' = \frac{1+\log \mathrm{B} + \log\log p - \log e}{\log p} - \frac{1}{p-1}$$

in (17) and so complete the proof of Theorem 8.

4. Power series with integral coefficients.

We preserve the notation of the previous sections. The purpose of this section is to prove

THEOREM 11. – *Suppose that the ramification index* e *of* K_p *over* $\mathbf{Q}_p$ *is less than or equal to* $p-1$. *Then there exists a constant* $\delta > 0$ *with the following property: if* $f(\mathrm{T}) = \sum_{n=0}^{\infty} a_n \mathrm{T}^n \in \mathbf{C}_p[[\mathrm{T}]]$ *satisfies* $v(a_n) \geqslant \mathrm{A} - n\delta$ *for some* $\mathrm{A} \in \mathbf{R}$, *then* $f(\mathrm{T}) \in \mathrm{B}_0$ *and the function* $s \longmapsto \mathrm{C}_f^{(\alpha)}(s)$ *is locally analytic for every* $\alpha \in \mathbf{Z}/(q-1)\mathbf{Z}$.

In particular since $\lambda'(\mathrm{T}) \in \mathcal{O}[[\mathrm{T}]]$, it is easy to see that if $f \in \mathbf{C}_p[[\mathrm{T}]]$ satisfies $\mathrm{D}_1^k f(\mathrm{T}) \in \mathcal{O}[[\mathrm{T}]]$ for some $k \geqslant 0$, then Theorem 11 can be applied to it, and so we have

COROLLARY 12. – *Let* $f \in \mathbf{C}_p[[\mathrm{T}]]$ *be such that*

$$(\mathrm{D}_1^k f)(\mathrm{T}) \in \mathcal{O}[[\mathrm{T}]]$$

for some $k \geqslant 0$. *Then* $f \in \mathrm{B}_0$ *and* $s \mapsto \mathrm{C}_f^{(\alpha)}(s)$ *is a locally analytic function for every* $\alpha \in \mathbf{Z}/(q-1)\mathbf{Z}$.

Theorem B of the introduction is evidently the special case $k = 0$ of Corollary 12 (except for the statement

$$v(\Omega_p) = \frac{1}{p-1} - \frac{1}{e(q-1)}$$

which is Lemma 13 below).

We now begin the proof of Theorem 11. Recall our hypothesis that $\mathcal{F}$ is isomorphic to the Lubin-Tate group $\mathcal{F}_0$. If $h = 1$, then Lubin [11, Theorem 4.3.2] tells us that $\mathcal{F}$ is isomorphic to $\mathbf{G}_m$ and so a much stronger result can be deduced from Theorem A (ii); and we shall therefore suppose that $h > 1$.

Let $\tau : \mathcal{F} \longrightarrow \mathcal{F}_0$ be an isomorphism. Then

$$\tau(\mathrm{T}) = \tau_0 \mathrm{T} + \mathrm{O}(\mathrm{T}^2) \in \mathcal{O}[[\mathrm{T}]]$$

with τ_0 a unit of $\mathcal{O}$. Thus $\mathcal{O}[[\mathrm{T}]] = \mathcal{O}[[\tau(\mathrm{T})]]$ and so $\tau(\mathrm{B}_0) = \mathrm{B}'_0 (= \mathrm{B}_0$ defined with $\mathcal{F}_0$ in place of $\mathcal{F})$. Also if λ_0 denotes the logarithm of $\mathcal{F}_0$, and $\mathrm{W} = \tau(\mathrm{T})$ then $\lambda(\mathrm{T}) = \tau_0^{-1} \lambda_0(\mathrm{W})$ and so by the chain rule

$$\frac{1}{\lambda'(\mathrm{T})} \frac{df(\mathrm{T})}{d\mathrm{T}} = \frac{1}{\tau_0^{-1} \lambda'_0(\mathrm{W})} \frac{df o \tau^{-1}(\mathrm{W})}{d\mathrm{W}}.$$

Since $f(\mathrm{T} +_{\mathcal{F}} \eta) = f(\tau^{-1}(\mathrm{W}) +_{\mathcal{F}_0} \tau^{-1}(\eta))$ it suffices to prove the theorem for the group $\mathcal{F}_0$ and we assume that $\mathcal{F} = \mathcal{F}_0$ for the rest of this section; thus in what follows λ, t_a etc are associated to $\mathcal{F}_0$.

We write $\lambda(\mathrm{T}) = \sum_{n=1}^{\infty} \lambda_n \mathrm{T}^n$ with $\lambda_1 = 1$.

We need

Lemma 13. – (i) $\lambda_n = 0$ *unless* $n \equiv 1 \pmod{q-1}, \lambda_n \in \mathcal{O}_{\mathrm{K}_p}$ *except perhaps when* $n \equiv 0 \pmod{q}$, *and* $v(\lambda_q) = -e^{-1}$.

(ii) *The map* $(\Omega_p a) \longmapsto (\mathrm{D}_n t_a)(0)\ (a \in \mathcal{O}_{\mathrm{K}_p})$ *is a polynomial in* $\Omega_p a$ *of degree* n *with coefficient in* K_p; *the coefficient of* $(\Omega_p a)^k$ *being* 0 *unless* $k \equiv n \pmod{q-1}$.

(iii) *We have*

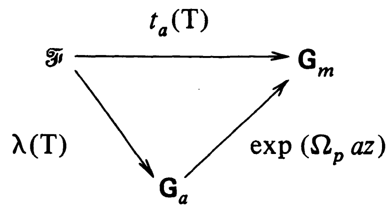
$$t_a(\mathrm{T}) = \sum_{k=0}^{q-1} \frac{(\Omega_p a)^k}{k!} \mathrm{T}^k + \left[\frac{(\Omega_p a)^q}{q!} + \lambda_q \Omega_p a\right] \mathrm{T}^q + \mathrm{O}(\mathrm{T}^{q+1}).$$

(iv) $v(\Omega_p) = \dfrac{1}{p-1} - \dfrac{1}{e(q-1)}$.

Remark. – Part (iv) of this lemma is true for any $\mathcal{F}$ (so long as $e \leqslant p-1$). Indeed, once the assertion has been proven for $\mathcal{F}_0$ the isomorphism $\tau : \mathfrak{F} \longrightarrow \mathfrak{F}_0$ above shows that, with suitable normalisation and obvious notation, we have $\tau_0 \, \Omega_p \, (\mathfrak{F} = \Omega_p (\mathfrak{F}_0)$.

Proof. – (i) For the proof of this see Lang [8, Chapter 8]. The final statement follows from the proof given there.

(ii) We have the commutative triangle



where z is a local parameter for the additive group $\mathbf{G}_a$). This says precisely that $t_a(\mathrm{T}) = \exp(\Omega_p a\lambda(\mathrm{T}))$. Expanding $\exp(\Omega_p a\lambda(\mathrm{T}))$ in powers of T and using (i) we obtain (ii).

(iii) This follows easily from parts (i) and (ii).

(iv) Put $x = \dfrac{1}{p-1} - \dfrac{1}{e(q-1)}$. We first claim that $v(\Omega_p) \leqslant x$. Indeed Fact 2 of § 1 tells us that there exists $\eta \in \ker[\pi]$ and $\zeta \in \mu_p(\mathbf{C}_p)$ with $\zeta \neq 1$ such that $t_1(\eta) = \zeta$. Suppose that $v(\Omega_p) > x$. Since $v(\eta) = \dfrac{1}{e(q-1)}$ and $v(n\,!) \leqslant \dfrac{n-1}{p-1}$ we have

$$v\left(\frac{(\Omega_p \eta)^n}{n\,!}\right) > \frac{1}{p-1}$$

for any $n > 0$. But one has $v(\eta^q) = \dfrac{q}{e(q-1)} > \dfrac{1}{e}$; so, using our hypothesis $e \leqslant p-1$ and referring to the expression

$$t_1(\eta) = \sum_{k=0}^{q-1}{}' \frac{(\Omega_p \eta)^k}{k\,!} + \eta^q u, \quad \text{with} \quad u \in \mathfrak{O}$$

obtained by substituting $a = 1$ and $\mathrm{T} = \eta$ in part (iii) we find that

$$v(\zeta - 1) = v(t_1(\eta) - 1) > \frac{1}{p-1}$$

which is false. Hence $v(\Omega_p) \leqslant x$ and so $v(\lambda_q \, \Omega_p) < 0$ by (i). But the coefficient of T^q in $t_1(\mathrm{T})$ is

$$\frac{\Omega_p^q}{q\,!} + \lambda_q \Omega_p$$

which lies in $\mathcal{O}$, so that $v\left(\frac{\Omega_p^q}{q\,!}\right) = v(\lambda_q \Omega_p) = -\frac{1}{e} + v(\Omega_p)$. Since it is easy to see that $v(q\,!) = \frac{q-1}{p-1}$ it follows that

$$v(\Omega_p) = \frac{1}{p-1} - \frac{1}{e(q-1)}$$

as asserted.

We now begin the proof of Theorem 11 itself. Consider the auxiliary function

$$\Phi(\mathrm{T}) = \frac{1}{q-1} \sum_{\zeta \in \mu_{q-1}} t_\zeta(\mathrm{T})\, \zeta^{-1}$$

where the sum is taken over all $\zeta \in \mu_{q-1}(\mathrm{K}_p)$. In view of parts (i) and (ii) of Lemma 13, and the fact that $\sum_{\zeta \in \mu_{q-1}} \zeta^n = q - 1$ or 0 according as to whether $n \equiv 0 \pmod{q-1}$ or not, we find that the coefficient of T^n in $\Phi(\mathrm{T})$ is 0 unless $n \equiv 1 \pmod{q-1}$, in which case it is the same as the coefficient of T^n in $t_1(\mathrm{T})$.

Now consider the case $f(\mathrm{T}) = \mathrm{T}$. We can certainly write $\mathrm{T} = \sum_{n=0}^{\infty} a_n \frac{\Phi(\mathrm{T})^n}{n\,!}$ with $a_n \in \mathbf{C}_p$ and $a_n = 0$ if $n \not\equiv 1 \pmod{q-1}$. Now

$$\frac{\Phi(\mathrm{T})}{\Omega_p} = \mathrm{T} + \frac{\mathrm{T}^q}{\Omega_p} \Psi(\mathrm{T}^{q-1})$$

for some $\Psi(\mathrm{T}) \in \mathcal{O}[[\mathrm{T}]]$ and therefore if $k \in \mathbf{Z}_+$,

$$\left(\frac{\Phi(\mathrm{T})}{\Omega_p}\right)^{k(q-1)+1} = \mathrm{T}^{k(q-1)+1} + \frac{\beta_1^{(k)}}{\Omega_p}\mathrm{T}^{(k+1)(q-1)+1} + \dots + \frac{\beta_r^{(k)}}{\Omega_p}\mathrm{T}^{(k+r)(q-1)+1} + \dots$$

with $\beta_r^{(k)} \in \mathcal{O}$ and in fact $\beta_r^{(k)}\, \Omega_p^{(k(q-1)+1)-r} \in \mathcal{O}$ if

$$r \geqslant k(q-1)+1 .$$

Thus, proceeding inductively we find that if we write

$$\mathrm{T} = \sum_{k=0}^{\infty} d_k \frac{\Phi(\mathrm{T})^{k(q-1)+1}}{\Omega_p^{k(q-1)+1}}$$

then

$$d_0 = 1 , \quad \Omega_p d_1 \in \mathfrak{O} , \quad \Omega_p^2 d_2 \in \mathfrak{O} , \ldots$$

and in general $\Omega_p^k d_k \in \mathfrak{O}$. For simplicity we write Λ for $\Omega_p^{\frac{1}{q-1}}$. Then

$$\frac{\mathrm{T}}{\Lambda} \in \mathfrak{O}\left[\left[\frac{\Phi(\mathrm{T})}{\Lambda^q}\right]\right]$$

and therefore, if we take

$$\delta = v(\Lambda) = \left(\frac{1}{p-1} - \frac{1}{e(q-1)}\right)\frac{1}{q-1},$$

then any f satisfying the hypotheses of Theorem 11 will lie in $\mathbf{C}_p \cdot \mathfrak{O}\left[\left[\frac{\Phi(\mathrm{T})}{\Lambda^q}\right]\right]$. Hence to complete the proof of Theorem 11 it suffices to show that every $f \in \mathfrak{O}\left[\left[\frac{\Phi(\mathrm{T})}{\Lambda^q}\right]\right]$ satisfies the hypothesis of Theorem 8. Now clearly $\Phi(\mathrm{T}) \in \mathfrak{O}\ [[t_{x_1}(\mathrm{T}) - 1 , \ldots , t_{x_h}(\mathrm{T}) - 1]]$ from which it follows that any $f \in \mathfrak{O}\left[\left[\frac{\Phi(\mathrm{T})}{\Lambda^q}\right]\right]$ can be written in the form $\sum_{n \in \mathbf{Z}_+^h} c_n \frac{(t_x - 1)^n}{n!}$ with

$$v\left(\frac{c_n}{n!}\right) \geqslant v\left(\Lambda^{-(\sum_i n_i)(q-1)}\right) = -\frac{q}{q-1}\left(\sum_{i=1}^{h} n_i\right)\left(\frac{1}{p-1} - \frac{1}{e(q-1)}\right).$$

Recalling that $v(n!) \geqslant \frac{\sum_i n_i}{p-1} + \mathrm{O}\left(\log \prod_{i=1}^{h} n_i\right)$ we find that $v(c_n) \geqslant \mathrm{A} + \mathrm{B}v(n!)$ for any

$$B < 1 - \frac{q(p-1)}{p-1}\left[\frac{1}{p-1} - \frac{1}{e(q-1)}\right] = \frac{1}{q-1}\left[\frac{(p-1)q}{e(q-1)} - 1\right]$$

and suitable A depending on B. Now $\frac{(p-1)q}{e(q-1)} > 1$ since $e \leqslant p - 1$ and so the hypotheses of Theorem 8 are satisfied and the proof of Theorem 11 is complete.

BIBLIOGRAPHIE

[1] P. Cassou-Nogues, Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques, *Inventiones Math.*, 51 (1979), 29-59.

[2] R.F. Coleman, Division values in local fields, *Inventiones Math.*, 53 (1979), 91-116.

[3] K. Iwasawa, Lectures on p-adic L-functions, *Annals of Math. Studies*, 74 P.U.P. (1972).

[4] E.E. Kummer, Uber eine allgemeine Eigenschaft der rationale Entwicklungscoefficienten eines bestimmten Gattung analytischer Functionen, *Crelle's J.*, 41 (1851) 368-372, (= collected works vol. 1, pp. 358-362, Springer-Verlag (1975)).

[5] T. Kubota and H.W. Leopoldt, Eine p-adische Theorie der Zetawerte, *Crelle's J*, 214/215 (1964), 328-339.

[6] N. Katz, Formal groups and p-adic interpolation, *Astérisque*, 41-42 (1977) 55-65.

[7] N. Katz, Divisibilities, congruences and Cartier duality, *J. Fac. Sci. Univ. Tokyo*, Ser. 1 A, 28 (1982), 667-678.

[8] S. Lang, Cyclotomic fields, *Graduate texts in Math*, Springer-Verlag (1978).

[9] H.W. Leopoldt, Eine p-adiche Theorie der Zetewerte II, *Crelle's J.*, 274/275 (1975), 225-239.

[10] S. Lichtenbaum, On p-adic L-functions associated to elliptic curves, *Inventiones Math.*, 56 (1980), 19-55.

[11] J. LUBIN, One-parameter formal Lie groups over *p*-adic integer rings, *Annals of Math.*, 80 (1964), 464-484.

[12] B. MAZUR and P. SWINNERTON-DYER, Arithmetic of Weil curves, *Inventiones Math.*, 25 (1974), 1-61.

[13] K. RUBIN, Congruences for special values of L-functions of elliptic curves with complex multiplication, *Inventiones Math.*, 71(1983), 339-364.

[14] J.P. SERRE, Formes modulaires et fonction zêta *p*-adiques, In *Springer Lecture Notes in Math.*, 350 (1973), 191-268.

[15] J. TATE, *p*-divisible groups, *Proc. Conf. On local fields*, ed. T. Springer, Springer-Verlag, (1967), 153-183.

Manuscrit reçu le 16 novembre 1984
révisé le 11 mars 1985.

John L. BOXALL,
Université de Caen
Dépt. de Mathématiques et de Mécanique
14032 Caen Cedex
&
The University of Manchester Institute of Science & Technology
P.O. Box 88
Manchester M60 1QD (G.B.).